Aplicativo IBM QRadar User Behavior Analytics (UBA)
Versão 3.2.0

Guia do usuário

Comunicado

Antes de usar estas informações e o produto que ela suporta, leia as informações em “Avisos” na página 207.

Informações sobre o produto

Este documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.8 e a liberações subsequentes, a menos que seja substituído por uma versão atualizada deste documento.

Índice

1 Analítica de Comportamento do Usuário para QRadar

O aplicativo User Behavior Analytics for QRadar ajuda a determinar os perfis de risco de usuários dentro de sua rede e a executar ação quando o aplicativo alerta quanto a comportamento ameaçador.

O aplicativo User Behavior Analytics for QRadar (UBA) é uma ferramenta para a detecção de ameaças internas em sua organização. Ele foi desenvolvido sobre a estrutura do aplicativo para usar dados existentes no QRadar para gerar novos insights em torno de usuários e riscos. O UBA inclui duas funções principais no QRadar: criação de perfil de risco e identidades de usuários unificadas.

A criação de perfil de risco é feita atribuindo o risco a diferentes casos de uso de segurança. O exemplo pode incluir regras simples e verificações como websites inválidos ou análises de dados stateful mais avançadas que usam aprendizado de máquina. O risco é atribuído a cada um dependendo da gravidade e da confiabilidade do incidente detectado. O UBA usa os dados de evento e de fluxo existentes no sistema QRadar para gerar esses insights e riscos de perfil de usuários. O UBA usa três tipos de tráfego: 1. O tráfego em torno do acesso, da autenticação e de mudanças de conta. 2. O comportamento do usuário na rede, portanto, dispositivos como: proxies, firewalls, IPS, VPNs. 3. Logs de terminal e de aplicativo, como a partir do Windows ou Linux e de aplicativos SAAS. Todos os três tipos de tráfego enriquecem o UBA e permitem que mais casos de uso criem o perfil de risco.

A unificação de identidades do usuário é realizada pela combinação de contas diferentes para um usuário no QRadar. Ao importar dados de um arquivo do Active Directory, LDAP ou CSV, o UBA pode ser ensinado sobre quais contas pertencem a uma identidade do usuário. Isso ajuda a combinar o risco e o tráfego entre os diferentes nomes de usuário no QRadar para UBA.

Aprendizado de Máquina (ML) é uma ferramenta complementar que aumenta o aplicativo UBA. Ele permite casos de uso mais ricos e detalhados que executam a criação de perfil e o armazenamento em cluster da série temporal. Ele é instalado a partir do aplicativo UBA, na página de configurações de Aprendizado de Máquina. O ML inclui mais visualizações no aplicativo UBA existente que mostram o comportamento aprendido (modelos), o comportamento atual e os alertas. O aprendizado de máquina usa até quatro semanas de dados históricos no QRadar para criar os modelos preditivos e as linhas de base do que é normal para um usuário.

Para obter mais informações sobre como usar o aplicativo Reference Data Import LDAP, consulte 8, “Aplicativo Reference Data Import - LDAP”, na página 161.

Para obter mais informações sobre como usar o aplicativo Machine Learning Analytics, consulte 9, “App Machine Learning Analytics”, na página 173.

Atenção: Deve-se instalar o IBM® QRadar V7.2.8 ou mais recente antes de instalar o aplicativo QRadar UBA.

Conceitos relacionados:

7, “Regras e ajuste para o aplicativo UBA”, na página 45
O aplicativo IBM QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

“Configurando o aplicativo User Behavior Analytics” na página 23
Para poder usar o aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar definições adicionais.

8, “Aplicativo Reference Data Import - LDAP”, na página 161
Use o aplicativo Reference Data Import - LDAP para reunir informações de identificação contextuais de múltiplas fontes LDAP no seu QRadar Console.

9, “App Machine Learning Analytics”, na página 173
O app Machine Learning Analytics (ML) estende os recursos do seu sistema QRadar e do app QRadar User Behavior Analytics (UBA) ao incluir os casos de uso para análise de aprendizado de máquina. Com os casos de uso do Machine Learning Analytics, é possível obter mais insight sobre o comportamento do usuário com a modelagem preditiva. O aplicativo ML ajuda o seu sistema a aprender o comportamento esperado dos usuários em sua rede.

Tarefas relacionadas:

“Instalando o aplicativo User Behavior Analytics” na página 17
Use a ferramenta IBM QRadar Extension Management para fazer upload e instalar seu archive do aplicativo diretamente no QRadar Console.

“Fazendo upgrade do aplicativo User Behavior Analytics” na página 21
Utilize a ferramenta IBM QRadar Extension Management para fazer upgrade do seu aplicativo.

O que há de novo no aplicativo User Behavior Analytics

Aprenda sobre os novos recursos em cada liberação do aplicativo User Behavior Analytics (UBA).

O que há de novo na V3.2.0

- Identificar usuários com contas inativas no painel e nas páginas de perfil do usuário. Para obter informações adicionais, consulte “Contas inativas” na página 39.
- Criar listas de observação de contas de serviços com base em uma propriedade de usuário ausente. Para obter informações adicionais, consulte “Criando watchlists” na página 35.
- Aprimorado o aplicativo LDAP para que você possa selecionar os atributos LDAP a serem usados em UBA. Nota: ao configurar o LDAP, agora é necessário selecionar uma chave externa na seção Mapeamento de atributo. Para obter informações adicionais, consulte “Configurando o aplicativo Reference Data Import LDAP” na página 23.
- Incluída a capacidade de importar informações sobre o usuário a partir de um arquivo CSV. Para obter informações adicionais, consulte “Importando dados do usuário de um arquivo CSV” na página 162.
- Incluído caso de uso UBA: acesso do usuário a partir de múltiplos hosts. Para obter informações adicionais, consulte “UBA: acesso do usuário a partir de múltiplos hosts” na página 58.
- Incluído caso de uso UBA: possível enumeração de serviços de diretório. Para obter informações adicionais, consulte “UBA: possível enumeração de serviços de diretório” na página 94.
- Incluído caso de uso UBA: Possível Enumeração de Sessão SMB em um Controlador de Domínio. Para obter informações adicionais, consulte “UBA: possível enumeração de sessão SMB em um controlador de domínio” na página 94.
- Incluído caso de uso UBA: acesso suspeito seguido pela exfiltração de dados. Para obter informações adicionais, consulte “UBA: acesso suspeito seguido pela exfiltração de dados” na página 110.
- Incluído caso de uso UBA: tentativa de uso de conta inativa. Para obter informações adicionais, consulte “UBA: tentativa de uso de conta inativa” na página 73.

O que há de novo na V3.1.0

- Agora é possível customizar a exibição de métricas na linha de tempo do usuário e visualizar os dados que compõem as métricas.
- Incluída a capacidade de configurar um limite de risco dinâmico.
- Incluídas duas novas categorias de casos de uso na página Regras e Ajuste: Nuvem e Controlador de Domínio. Para obter informações adicionais, consulte 7, “Regras e ajuste para o aplicativo UBA”, na página 45.
- Incluído caso de uso UBA: usuário não padrão acessando recursos do AWS. Para obter informações adicionais, consulte “UBA: usuário não padrão acessando recursos do AWS” na página 90.
- Incluído caso de uso UBA: console do AWS acessado por usuário não autorizado. Para obter informações adicionais, consulte “UBA: console do AWS acessado por usuário não autorizado” na página 89.

- Incluído caso de uso UBA: solicitação de replicação de um controlador não de domínio. Para obter informações adicionais, consulte “UBA: solicitação de replicação de um controlador não de domínio” na página 96.
- Incluído caso de uso UBA: enumeração de conta do Kerberos detectada. Para obter informações adicionais, consulte “UBA: enumeração de conta do Kerberos detectada” na página 91.
- Incluído caso de uso UBA: possível falsificação de TGT PAC. Para obter informações adicionais, consulte “UBA: possível falsificação de TGT PAC” na página 96.
- Incluído caso de uso UBA: tentativa de recuperação de chave mestra de backup DPAPI. Para obter informações adicionais, consulte “UBA: tentativa de recuperação de chave mestra de backup DPAPI” na página 90.
- Incluído caso de uso UBA: ataque DoS por exclusão de conta. Para obter informações adicionais, consulte “UBA: ataque DoS por exclusão de conta” na página 68.
- Incluído caso de uso UBA: diversas transferências de arquivos bloqueadas seguidas por uma transferência de arquivo. Para obter informações adicionais, consulte “UBA: várias transferências de arquivos bloqueadas seguidas por uma transferência de arquivo” na página 108.

O que há de novo na V3.0.1

- Incluído um caso de uso para suportar a detecção de Tunelamento de DNS pelo aplicativo IBM QRadar DNS Analyzer. Para obter mais informações, consulte “UBA : Possível acesso ao domínio de tunelamento” na página 129.
- Corrigido um problema que pode impedir a capacidade de alimentar os usuários de uma tabela de referência.

O que há de novo na V3.0.0

- Agora é possível criar e gerenciar listas de observação para que seja possível monitorar grupos customizados de usuários. Para obter informações adicionais, consulte “Criando watchlists” na página 35.
- Agora é possível visualizar, filtrar e ajustar casos de uso do UBA com a nova página Regras e Ajuste. Para obter informações adicionais, consulte 7, “Regras e ajuste para o aplicativo UBA”, na página 45.
- Agora é possível visualizar eventos de risco e métricas na linha de tempo da atividade do usuário por sessões de atividade. Para obter informações adicionais, consulte “Painel do UBA e detalhes do usuário” na página 9.
- Incluída uma analítica de aprendizado de máquina que detecta um volume anormal de dados para domínios externos. Para obter informações adicionais, consulte “Configurando a analítica *Abnormal Volume of Data to External Domains*” na página 183.
- Incluído o UBA de caso de uso: transferência de saída grande por usuário de alto risco. Para obter informações adicionais, consulte “UBA : Transferência grande de saída por usuário de alto risco” na página 107.
- Incluído o UBA de caso de uso: atividade Honeytoken. Para obter informações adicionais, consulte “UBA: Atividade Honeytoken” na página 125.
- Incluído o UBA de caso de uso: tentativas de autenticação de Bruteforce. Para obter informações adicionais, consulte “UBA: Novas Tentativas de Autenticação Bruteforce” na página 45.
- Incluído o UBA de caso de uso: conta do usuário criada e excluída em um período de tempo curto. Para obter informações adicionais, consulte “UBA : A conta do usuário foi criada e excluída em um curto período de tempo” na página 72.
- Incluído o UBA de caso de uso: acesso de usuário de alto risco ao ativo crítico. Para obter informações adicionais, consulte “UBA : Acesso de usuário de alto risco para o ativo crítico” na página 48.
- Incluído o UBA de caso de uso: conta anômala criada a partir do novo local. Para obter informações adicionais, consulte “UBA : Conta defeituosa criada a partir de um novo local” na página 111.

- Incluído o UBA de caso de uso: conta de nuvem anômala criada a partir do novo local. Para obter informações adicionais, consulte “UBA : Conta em nuvem defeituosa criada a partir de um novo local” na página 115.

O que há de novo na V2.8.0

- Agora é possível filtrar por consultas AQL com o campo **Filtro de procura avançada** ao configurar as definições de analítica de aprendizado de máquina. Para obter informações adicionais, consulte “Definindo configurações do Machine Learning Analytics” na página 176.
- Agora é possível visualizar estatísticas do painel para Usuários descobertos por meio de eventos e Usuários importados do diretório. Para obter informações adicionais, consulte “Painel do UBA e detalhes do usuário” na página 9.
- Agora é possível especificar os usuários que você deseja controlar com aprendizado de máquina. Para obter mais informações, consulte “Painel do UBA e detalhes do usuário” na página 9
- Agora você pode configurar se deve exibir gráficos para cada analítica de aprendizado de máquina. Para obter informações adicionais, consulte “Definindo configurações do Machine Learning Analytics” na página 176.
- Agora é possível configurar se você deve instalar ou fazer upgrade de pacotes de conteúdo do UBA (regras do QRadar, propriedades customizadas e dados de referência para casos de uso). Para obter informações adicionais, consulte “Configurando Definições do Pacote de Conteúdo” na página 29.
- Incluída uma analítica de aprendizado de máquina que é possível ativar para detectar tentativas de transferência de saída anormais. Para obter informações adicionais, consulte “Configurando a analítica *Abnormal Outbound Transfer Attempts*” na página 178.
- Incluídas configurações de memória de aprendizado de máquina para suportar mais usuários quando você executa o UBA com o Aprendizado de máquina em um nó do aplicativo.
- Incluído um conjunto de referência para identificar os Usuários de alto risco. Para obter informações adicionais, consulte “Conjuntos de referência” na página 43.
- Incluídos casos de uso para as categorias Procurados no Website a seguir: Negócios/Serviço, LifeStyle e Não Categorizados. Para obter informações adicionais, consulte “Comportamento de navegação” na página 82.
- Incluído o UBA de caso de uso: compartilhamento de rede acessado. Para obter informações adicionais, consulte “UBA: Acesso de Rede Acessado” na página 145.
- Incluído o UBA de caso de uso: acesso não administrativo ao controlador de domínio. Para obter informações adicionais, consulte “UBA: acesso que não é de administrador ao controlador de domínio” na página 92.
- Incluído o UBA de caso de uso: acesso ao usuário por meio do local proibido. Para obter informações adicionais, consulte “UBA: acesso de usuário de local proibido” na página 117.
- Incluído o UBA de caso de uso: acesso de usuário por meio do local restrito. Para obter mais informações, consulte “UBA: uso de programa restrito” na página 103
- Incluído o UBA de caso de uso: múltiplas falhas do Kerberos Authentication do mesmo usuário. Para obter informações adicionais, consulte “UBA: diversas falhas de autenticação Kerberos do mesmo usuário” na página 91.
- Incluído o UBA de caso de uso: chamado do TGT usado por múltiplos hosts. Para obter mais informações, consulte “UBA: chamado TGT usado por diversos hosts” na página 97

O que há de novo na V2.7.0

Atenção: Se estiver fazendo upgrade para V2.7.0, você deve concluir as instruções na nota técnica a seguir: http://www.ibm.com/support/docview.wss?uid=swg22005489.

V2.7.0 do aplicativo User Behavior Analytics inclui os novos recursos a seguir:

- Agora é possível investigar os usuários no aplicativo QRadar Advisor com o aplicativo Watson. Nota: você deve ter QRadar Advisor com o Watson V1.13.0 instalado. Para obter informações adicionais, consulte "Investigando os usuários no QRadar Advisor com o Watson" na página 14.
- Agora é possível gerar um relatório de conformidade com o General Data Protection Regulation (GDPR) para um usuário e impedir que um usuário seja rastreado.
- Agora é possível marcar o status da investigação de um usuário e visualizar todos os usuários que estão sob investigação no painel **Análise de dados do usuário**.
- Agora é possível configurar se você deseja exibir bandeiras de país e região para endereços IP.
- Incluído suporte para eventos de acesso de domínio que são gerados pelo aplicativo IBM QRadar DNS Analyzer. Para obter informações adicionais, consulte "Analisador QRadar DNS" na página 128.
- Incluídos 19 novos casos de uso de varredura incomuns. Para obter informações adicionais, consulte "Reconhecimento" na página 135.
- Incluídos três novos casos de uso de aplicativo suspeitos. Para obter informações adicionais, consulte "Nó de extremidade" na página 97.
- Incluídos dez novos casos de uso de procura de risco. Para obter informações adicionais, consulte "Comportamento de navegação" na página 82.
- Incluídos 13 novos casos de uso de monitoramento de sistema (Sysmon). Para obter informações adicionais, consulte "Monitoramento do sistema (sysmon)" na página 144.

O que há de novo na V2.6.0

Atenção: Se você estiver fazendo upgrade para a V2.6.0, deverá concluir as instruções na nota técnica a seguir: http://www.ibm.com/support/docview.wss?uid=swg22005489.

A V2.6.0 do aplicativo User Behavior Analytics inclui os novos recursos a seguir:

- Aplicativo Machine Learning Analytics (ML) estendido para analisar anomalias com base em grupos de peers definidos no LDAP e no Active Directory.
- O analítico do grupo de peers para o aplicativo ML foi renomeado para Learned Peer Group.
- Caso de uso incluído: UBA: processo executado fora da lista de desbloqueio de disco gold (Windows/Linux)
- Caso de uso incluído: UBA: comportamento ransomware detectado
- Caso de uso incluído: UBA: detecção de processo de Netcat (Windows/Linux)
- Caso de uso incluído: UBA: múltiplas contas do VPN que falharam ao efetuar login de IP único
- Caso de uso incluído: UBA: cópia de sombra de volume criada
- Caso de uso incluído: UBA: detecção de protocolo inseguro ou não padrão
- Caso de uso incluído: UBA: atividade de malware - registro modificado em massa
- Caso de uso incluído: UBA: configurações de Internet modificadas
- Caso de uso incluído: UBA: múltiplas contas do VPN com login efetuado de IP único
- Caso de uso incluído: UBA: atividade suspeita de PowerShell (ativo)
- Caso de uso incluído: UBA: atividade suspeita de PowerShell
- Caso de uso incluído: UBA: atividade suspeita de shell de comando
- Caso de uso incluído: UBA: processo malicioso detectado

O que há de novo no V2.5.0

Atenção: Se está fazendo upgrade para a V2.5.0, deve-se concluir as instruções na seguinte nota técnica: http://www.ibm.com/support/docview.wss?uid=swg22005489.

A V2.5.0 do app User Behavior Analytics inclui as seguintes melhorias:

- Incluída a capacidade de investigar rapidamente o comportamento arriscado de um usuário com o visualizador de eventos contextuais sequenciais. Para obter informações adicionais, consulte “Painel do UBA e detalhes do usuário” na página 9.
- Incluída uma página de ajuda e suporte que fornece links para a documentação, os tutoriais e as informações de suporte, além de fornecer funções administrativas. Para obter informações adicionais, consulte “Página de Ajuda e suporte para UBA” na página 201.
- Aumento da precisão e da escalabilidade para o Machine Learning e melhoria no sistema de mensagens na seção Status dos modelos do Machine Learning do painel. Para obter informações adicionais, consulte “Painel do UBA com o Machine Learning Analytics” na página 190.
- Incluído o caso de uso: UBA: usuário executando um novo processo. Para obter informações adicionais, consulte “UBA: usuário executando novo processo” na página 105.
- Incluído o caso de uso: UBA: usuário instalando aplicativo suspeito. Para obter informações adicionais, consulte “UBA: usuário instalando aplicativo suspeito” na página 104.
- Incluído o caso de uso: UBA: Unix/Linux acessado com a conta de serviço ou de máquina. Para obter informações adicionais, consulte “UBA: sistema Unix/Linux acessado com conta de serviço ou máquina” na página 54.
- Incluído o caso de uso: UBA: acesso de usuário ao servidor interno do servidor de salto. Para obter informações adicionais, consulte “UBA: acesso de usuário ao servidor interno por meio do servidor de salto” na página 59.
- Incluído o caso de uso: UBA: ativo somente executivo acessado por usuário não executivo. Para obter informações adicionais, consulte “UBA: ativo somente executivo acessado por usuário não executivo” na página 47.

O que há de novo na V2.4.0

Atenção: Se você está fazendo upgrade para a V2.4.0, deve-se concluir as instruções na nota técnica a seguir: http://www.ibm.com/support/docview.wss?uid=swg22005489.

A V2.4.0 do aplicativo User Behavior Analytics inclui as melhorias a seguir:

- Exiba o status de recuperação do LDAP no aplicativo LDAP.
- Importe até 400.000 usuários pelo aplicativo LDAP. Antes de mudar a configuração, veja Problemas conhecidos.
- Integração e mapeamento de dados de LDAP/AD aperfeiçoados e simplificados.
- Capacidade para mapear um número ilimitado de aliases para um ID do usuário principal.
- Definições de configuração de memória foram incluídas em Configurações de Machine Learning para suportar mais usuários quando você executar o Machine Learning em um Nó do aplicativo.
- Incluída a pesquisa de feedback.
- Incluído UBA de caso de uso: acesso ao Windows com a conta de serviço ou máquina. Para obter mais informações, consulte “UBA: Windows Access com conta de serviço ou máquina” na página 66
- Incluído UBA de caso de uso: ataque D/DoS detectado. Para obter mais informações, consulte “UBA: ataque D/DoS detectado” na página 124
- Incluído UBA de caso de uso: detectar sessão SSH persistente. Para obter mais informações, consulte “UBA: detectar sessão SSH persistente” na página 98
- Incluído UBA de caso de uso: volume de dados anormais para o domínio externo. Para obter mais informações, consulte “UBA: volume de dados anormais para o domínio externo (regra do ADE)” na página 106
- Incluído UBA de caso de uso: tentativas de saída anormal. Para obter mais informações, consulte “UBA: tentativas de transferência de saída anormal (regra ADE)” na página 107

Problemas conhecidos

O aplicativo User Behavior Analytics tem informações necessárias para upgrade e problemas conhecidos.

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Problemas conhecidos para a V3.2.0

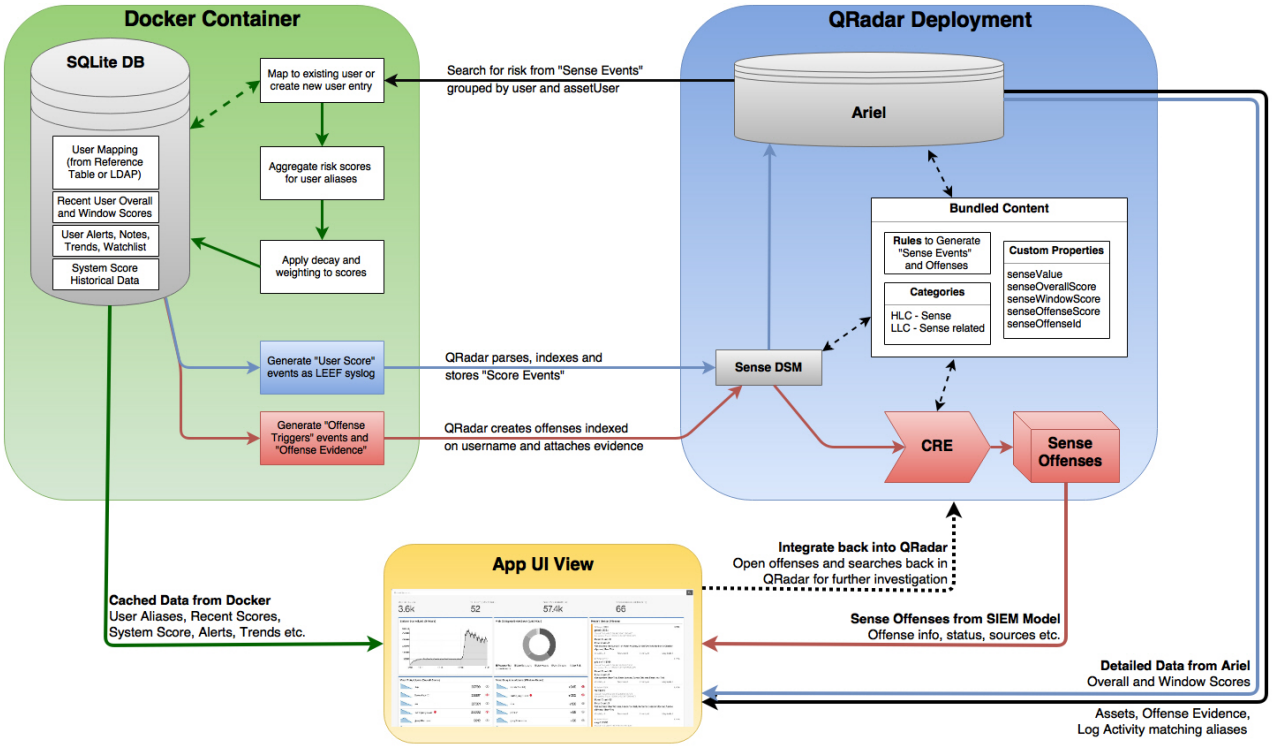
O app User Behavior Analytics tem os seguintes problemas conhecidos:

- O agrupamento de usuários de uma tabela de referência gerará informações incompletas do usuário nos registros do usuário do UBA, se você estiver executando no QRadar 7.2.8 Patch 13, no QRadar 7.2.8 Patch 13 IF1, no QRadar 7.3.1 Patch 3 ou no QRadar 7.3.1 Patch 4. O problema é resolvido no V7.3.1 Patch 4 IF1. Consulte o APAR IJ06032 para obter mais informações.
- Se você estiver fazendo upgrade do aplicativo UBA e receber um erro de exceção de notificação do QRadar informando que um conjunto de regras falhou ao ser carregado, será possível ignorá-lo e continuar. Se o erro persistir, entre em contato com o Suporte ao Cliente IBM.
- Devido a problemas conhecidos com o QRadar V7.2.8 Patch 12 e QRadar V7.3.1 Patch 3, é necessário fazer upgrade para QRadar V7.2.8 Patch 13 e QRadar V7.3.1 Patch 4.
- Depois de fazer upgrade do UBA para a V3.2.0, o gráfico Distribuição de Atividade de Aprendizado de Máquina na página Detalhes do Usuário pode levar até um dia para ser exibido.
- Ao visualizar uma página do perfil do usuário, o botão **Incluir na lista de desbloqueio** poderá falhar na exibição. Se isso ocorrer, será possível atualizar a página para resolver o problema.
- Importar mais de 100.000 usuários no LDAP para UBA pode afetar gravemente o sistema QRadar e a instalação do app UBA. O problema é causado devido a um problema conhecido no APAR IV98655. Importar mais de 200.000 usuários não é recomendado, a menos que você use o QRadar 7.3.0 ou mais recente em um console de 128 GB.
- Em raras instâncias do QRadar V7.2.8 e V7.3.0, é possível encontrar um problema com um token SEC recém-criado, no qual o token SEC parece funcionar e, posteriormente, se torna inválido. Para corrigir esse problema, conclua uma das ações a seguir:
  - Reinicie o serviço Apache Tomcat por meio de uma linha de comandos em seu Console do QRadar.
  - Implemente qualquer ação na guia Administrador no QRadar.
- No gráfico Pontuação do Sistema, ao selecionar um intervalo de data de mais de um dia e com uma data de encerramento do dia atual, os primeiros 8 pontos de dados são mostrados como 0s.
- Sequências em inglês ou texto corrompido são exibidos em algumas partes da interface com o usuário ao usar o QRadar V7.2.8 e em alguns códigos de idioma.

Visão Geral do Processo

O aplicativo User Behavior Analytics funciona com seu sistema QRadar para coletar dados sobre os usuários dentro de sua rede.

Como o UBA funciona



1. Os logs enviam dados para o QRadar.
2. As regras específicas do UBA procuram certos eventos (dependendo de quais regras do UBA estão ativadas) e acionam um novo evento de verificação que é lido pelo aplicativo UBA.
3. As regras do UBA requerem que os eventos tenham um nome do usuário e outros testes (revise as regras para ver o que eles estão procurando).
4. O UBA puxa o *senseValue* e o nome do usuário do evento de verificação e, em seguida, aumenta essa *pontuação de risco* do usuário pela quantia de *senseValue*.
5. Quando uma *pontuação de risco* do usuário exceder o limite que você configurar na página Configurações do UBA, o UBA enviará um evento que acionará a regra "UBA: criar ofensa" e uma ofensa será criada para esse usuário.

Pontuação de

Uma pontuação de risco é a adição de todos os eventos de risco que são detectados por regras do UBA. Quanto maior a pontuação de risco, maior a probabilidade de um usuário interno ser um risco de segurança e isso garante a revisão adicional da atividade de rede do usuário. A pontuação de risco será reduzida ao longo do tempo se nenhum evento novo ocorrer. A quantia da redução é controlada por meio do valor em **Risco de queda por esse fator por hora** na página Configurações do UBA.

Como os senseValues são usados para criar pontuações de risco do usuário

Cada regra e análise de dados tem um valor designado a ela que indica a severidade do problema localizado. Cada vez que as ações de um usuário fazem uma regra ser acionada, o usuário tem esse valor incluído na pontuação. Quanto mais o usuário "viola" uma regra, maior a pontuação será.

Regras e eventos de verificação

As regras, quando acionadas, geram eventos de verificação para determinar a pontuação de risco do usuário.

É possível atualizar as regras existentes no QRadar para produzir eventos de verificação. Para obter informações adicionais, consulte “Integrando o conteúdo do QRadar novo ou existente com o aplicativo UBA” na página 42.

Machine Learning Analytics e eventos de verificação

É possível instalar o aplicativo Machine Learning Analytics e ativar a análise de dados de aprendizado de máquina para identificar o comportamento anômalo do usuário. A análise de dados, quando acionada, gerará eventos de verificação que também aumentam a pontuação de risco de um usuário.

Demonstrações e tutoriais de vídeo

Saiba mais sobre o aplicativo IBM QRadar User Behavior Analytics (UBA), o aplicativo Reference Data Import - LDAP e o aplicativo Machine Learning Analytics (ML).

IBM Security Learning Academy

Inscreva-se nos cursos do User Behavior Analytics (UBA) no website do IBM Security Learning Academy.

Dica: Deve-se ter uma conta IBMid para se inscrever e assistir aos vídeos.

Tutoriais de Vídeo no YouTube

Demonstração do app User Behavior Analytics com o Machine Learning V2.0.0: https://www.youtube.com/watch?v=RgF1RztR1yg.

Demonstração para configurar o aplicativo Reference Data Import - LDAP: https://www.youtube.com/watch?v=ER-wYxS6wFk.

Visão geral do aplicativo User Behavior Analytics:

- https://www.youtube.com/watch?v=bf_DODl8Ehs
- https://www.youtube.com/watch?v=ARVsuQaSF9E

Painel do UBA e detalhes do usuário

O aplicativo IBM QRadar User Behavior Analytics (UBA) mostra a você os dados de risco gerais para usuários em sua rede.

Dashboard

Após você instalar e configurar o aplicativo do UBA, clique na guia **Analítica do usuário** para abrir o Painel.

Nota: O número suportado de usuários que o aplicativo do UBA pode monitorar é 400.000 usuários.

No campo **Procurar por usuário**, é possível procurar usuários por nome, endereço de e-mail e nome do usuário. Conforme você insere um nome, o aplicativo mostra os cinco principais resultados.

O Painel é automaticamente atualizado a cada minuto e mostra os dados de risco a seguir:

Usuários Monitorados	Exibe o número total de usuários que o aplicativo UBA está monitorando ativamente.
Usuários de Alto Risco	Exibe o número de usuários que estão atualmente excedendo a pontuação de risco. O valor para determinar a pontuação de risco é configurado no "Limite de risco para acionar ofensas" em Configurações do UBA.
Usuários Descobertos de Eventos	Exibe o número de usuários que são descobertos por meio de eventos, excluindo os usuários importados.
Usuários Importados do Diretório	Exibe o número de usuários que foram importados das tabelas de referência.
Analítica ativa	• Regras do UBA: indicam o status do conteúdo de regras. Um status verde indica que as regras estão instaladas e ativas. Cinza indica que as regras estão desativadas. Amarelo indica que a instalação está em andamento. • Regras de fluxo: indicam o status das regras do QNI. Um status verde indica que as regras do QNI estão instaladas e ativas. Cinza indica que as regras do QNI não estão instaladas. • Anomalia comportamental: um status verde indica que as regras do ADE estão instaladas e ativas. Cinza indica que as regras do ADE não estão instaladas. • Analítica de aprendizado de máquina: um status verde indica que o aplicativo da Machine Learning Analytics está instalado. Cinza indica que o aplicativo Machine Learning Analytics não está instalado.
Usuários Monitorados	Exibe os 10 principais usuários mais risquiados. A primeira coluna lista o nome de exibição, o título da tarefa e a cidade, se disponível. • Risco recente: mostra o risco acumulado para o respectivo usuário para os últimos 5 minutos. • Pontuação de risco: mostra um gráfico que ilustra a tendência geral de pontuação de risco do usuário para a última hora e a pontuação de risco atual. A cor do gráfico indica o risco geral. • Ícone de lista de observação: inclua o usuário em uma lista de observação ou crie uma lista de observação. O número indica de quantas listas de observação o usuário é membro. • É possível visualizar todos os usuários rastreados na página Procurar.
Ofensas recentes	Ofensas de detecção mais recentes por usuário.
[User] Watchlist	Watchlists que você criou. É possível criar tantas listas de observação quanto você desejar, e elas serão exibidas no Painel. É possível visualizar todos os usuários rastreados na lista de observação customizada criada na página **Procurar**. **Dica:** Para incluir um usuário em uma lista de observação, clique no ícone **Lista de observação**  . O número indica de quantas listas de observação o usuário é membro.
Pontuação do sistema	Pontuação de risco acumulada geral para todos os usuários em um momento especificado. Clique no ícone **Calendário** para especificar um intervalo de dados maior que um dia. A duração máxima que pode ser selecionada é de 30 dias a qualquer momento durante o último ano.
Detalhamento da categoria de risco	Categorias de risco de alto nível ao longo da última hora. Clique no gráfico para ver as subcategorias e, em seguida, clique para ver uma exibição de eventos.
Usuários com contas inativas	Lista de observação de usuários que estão sinalizados como tendo contas inativas. A lista Usuários com Contas Inativas é gerada automaticamente. Disponível na V3.2.0 e mais recente.
Investigações ativas	Os usuários que estão atualmente sob investigação. Marque a caixa de seleção **Minhas Investigações** para mostrar apenas as investigações que você iniciou. Disponível na V2.7.0 e mais recente.

Status dos modelos de aprendizado de máquina	O status da Machine Learning Analytics será visível se o aplicativo do Machine Learning estiver instalado. Para obter informações adicionais, consulte “Painel do UBA com o Machine Learning Analytics” na página 190.

Página de detalhes do usuário

É possível clicar em um nome do usuário em qualquer lugar no aplicativo para ver detalhes para o usuário selecionado.

É possível aprender mais sobre as atividades do usuário com a área de janela do *visualizador de eventos*. A área de janela do visualizador de eventos mostra informações sobre uma atividade ou um momento selecionado. Clicar em um evento na área de janela *visualizador de eventos* revela mais detalhes, como eventos de syslog e informações de carga útil. A área de janela do visualizador de eventos está disponível para todos os gráficos de rosca e de linha e as atividades na Linha de tempo de atividade de risco na página Detalhes do Usuário.

A página Detalhes do Usuário inclui as seguintes informações do usuário:

- Mostra o nome e os aliases do usuário selecionado e quaisquer detalhes adicionais dos atributos que são importados do LDAP.
- Na V3.2.0 e mais recente, é possível visualizar o status (inativo, ativo, nunca usado) de todas as contas que foram localizadas associadas ao usuário.
- Se você tiver o QRadar Advisor com o Watson V1.13.0 ou mais recente instalado, será possível procurar informações que estão relacionadas ao usuário. Deve-se ter privilégios de administrador do QRadar. Clique no ícone **Procurar Watson**. (Disponível na V2.7.0 ou posterior.)
- Para iniciar uma investigação sobre o usuário, clique no ícone **Iniciar Investigação** . Quando sua investigação for concluída, clique no ícone **Terminar Investigação**. (Disponível na V2.7.0 ou posterior.)
- Para incluir o usuário em uma lista de observação ou criar uma lista de observação, clique no ícone **Lista de observação** .

A lista **Ações Avançadas** inclui as seguintes ações:

Incluir alerta customizado	É possível configurar um alerta customizado que é exibido pelo nome do usuário. Clique em **Incluir alerta customizado**, insira uma mensagem de alerta e, então, clique em **Configurar**. Para remover o alerta customizado para o usuário selecionado, clique em **Remover alerta customizado**.
Incluir na lista de desbloqueio	Deve-se ter privilégios de administrador do QRadar. É possível incluir o usuário selecionado na lista de desbloqueio para que o usuário não gere pontuações de risco e ofensas. Para remover o usuário selecionado da lista de desbloqueio, clique em **Incluído na lista de desbloqueio**. Para revisar a lista completa de usuários que foram incluídos na lista de desbloqueio, consulte “Visualizando a lista de desbloqueio de usuários confiáveis” na página 37.
Gerar relatório de conformidade com o GDPR para o usuário	É possível gerar um relatório de conformidade com o General Data Protection Regulation (GDPR) para o usuário. **Importante:** Gere o relatório antes de clicar em **Excluir e Parar Rastreamento de Usuário**.
Excluir e Parar Rastreamento de Usuário	Deve-se ter privilégios de administrador do QRadar. Você pode clicar em **Excluir e Parar Rastreamento de Usuário** para obedecer o General Data Protection Regulation (GDPR). Selecione **Sim** para excluir permanentemente e parar o rastreamento do usuário. Para começar a rastrear o usuário novamente, exclua os alias do usuário do conjunto de referência **UBA : Usuários Não Rastreados**. Para visualizar todos os alias de usuário, faça download do relatório GDPR antes de excluir o usuário.

Sempre rastree com o Machine Learning	Deve-se ter privilégios de administrador do QRadar. É possível clicar em **Sempre rastrear com o Machine Learning** para incluir o usuário no conjunto de referência *UBA: ML Always Tracked Watchlist*. A inclusão do usuário no conjunto de referência fornece a mais alta probabilidade de que o usuário seja incluído em um modelo de aprendizado de máquina. Para obter mais informações sobre conjuntos de referência no UBA, veja “Conjuntos de referência” na página 43. Para remover o usuário selecionado do conjunto de referência, clique em **Rastreado com o Machine Learning**. **Nota:** Disponível na V2.8.0 ou mais recente e somente se o Aprendizado de Máquina estiver instalado e você tiver privilégios do administrador do QRadar.

É possível visualizar as seguintes informações sobre o usuário selecionado:

Contagem de Risco Geral	A pontuação de risco geral mostra as tendências de risco para o usuário.
Linha de Tempo	O gráfico de linha de tempo mostra Eventos Riscos e Eventos do Usuário. Eventos de risco são eventos de risco que contribuem para a pontuação de risco. Os eventos do usuário são eventos não de risco. O eixo Y é a contagem de eventos e o eixo X é o tempo. É possível clicar em qualquer atividade na linha de tempo para abrir a área de janela do visualizador de eventos, que lista os eventos de log de apoio que estão associados à atividade do usuário. Clique em um evento para visualizar mais detalhes, como eventos syslog e informações de carga útil. • Na V2.8.0 ou anterior, na seção Linha de tempo de atividade de risco, é possível clicar em **Agrupar por atividade** ou **Agrupar por hora** para ver uma lista de atividades do usuário e, em seguida, filtrar e procurar por qualquer coluna na linha de tempo. • Na V3.0.0 e mais recente, a atividade de linha de tempo é agrupada por sessões e dias. As sessões são definidas na seção Configurações do aplicativo da página **Configurações do UBA**. As cores representam o risco geral de uma sessão. Clique no ícone **Calendário** para especificar o intervalo de data (1 - 14 dias). • Na V3.1.0 e mais recente, é possível customizar as configurações de métrica que são exibidas para a linha de tempo, clicando no ícone **Configurações de métrica**. É possível incluir e remover as categorias que você deseja ver. Os dados mostrados na seção Métricas de exemplo da tela Configurações de métrica não representam valores reais. **Nota:** "Eventos Riscos" e "Casos de Uso" serão mostrar os mesmos dados em que "Eventos Riscos" é o número total de eventos para os casos de uso fornecidos. “Categorias de URL“ e “URLs“ mostrarão os mesmos dados em que “URLs“ é o número total de eventos para as Categorias de URL“ fornecidas. “IDs de Eventos“ e “Eventos“ mostrarão os mesmos dados em que “Eventos“ é o número total de eventos para os IDs de Eventos fornecidos.
Ofensas recentes	Mostra qualquer ofensa do tipo de usuário, no qual o nome do usuário correspondeu a quaisquer aliases do usuário selecionado. As últimas cinco ofensas são exibidas. Clique em uma ofensa para abrir a guia **Ofensas** no QRadar.
Detalhamento da categoria de risco	Mostra as categorias de risco do usuário selecionado durante a última hora.
Adicionar notas	Clique no ícone **Incluir** + para incluir notas para o usuário selecionado. As notas são excluídas automaticamente após o período de retenção de 30 dias. **Dica:** Para salvar a nota indefinidamente, marque a nota como importante clicando no ícone **Sinalização**.

Os gráficos a seguir serão exibidos na página Detalhes do usuário se o aplicativo Machine Learning estiver instalado e a analítica especificada estiver ativada. Para obter informações adicionais, consulte “Painel do UBA com o Machine Learning Analytics” na página 190.

Atividade total	Mostra a quantia real e a aprendida de atividade de usuários durante todo o dia agrupada por hora.
Atividade do usuário por categoria	Mostra os padrões de comportamento de atividade do usuário reais e os esperados por categoria de alto nível.
Variação de risco	Mostra se a pontuação de risco de um usuário se desvia do padrão de pontuação de risco esperado.
Tentativas de Transferência de Saída Anormal	Mostra o uso do tráfego de saída para cada usuário e alertas sobre comportamento anormal. Observe que o gráfico para esta analítica não está ativado por padrão. A analítica de Tentativas de transferência de saída anormal será visível no painel apenas se o aplicativo do Machine Learning estiver instalado, a analítica estiver ativada e **a página Mostrar gráfico nos Detalhes do usuário** for selecionada nas configurações do Machine Learning. Disponível na V2.8.0 ou mais recente.
Volume anormal de dados para domínios externos	Mostra o uso de dados do domínio externo para cada usuário e os alertas sobre comportamento anormal. A analítica Volume anormal de dados para domínios externos só será visível no painel se o aplicativo Machine Learning estiver instalado, a analítica estiver ativada e **Mostrar gráfico na página Detalhes do usuário** estiver selecionado nas configurações do Machine Learning. Disponível na V3.0.0 ou mais recente.
Distribuição de atividade	Mostra clusters de comportamento dinâmico para todos os usuários que são monitorados por aprendizado de máquina. Disponível na V2.2.0 ou posterior.
Grupo de Peer Aprendeu	Mostra quanto o usuário se desviou do grupo de peers inferido no qual ele deveria estar. Disponível na V2.2.0 ou posterior.
Grupo de Peer Definido	Mostra quanto uma atividade de evento do usuário se desvia do seu grupo de pares definido. Disponível na V2.6.0 ou mais recente.

Para retornar ao painel principal, clique em **Painel**.

Conceitos relacionados:

"Painel do UBA com o Machine Learning Analytics" na página 190
O aplicativo IBM QRadar User Behavior Analytics (UBA) com o Machine Learning Analytics inclui o status do Machine Learning Analytics e detalhes adicionais para o usuário selecionado.

"Contas inativas" na página 39
É possível ver usuários em seu sistema que possuem contas inativas, contas ativas ou contas que nunca foram usadas.

Tarefas relacionadas:

"Criando watchlists" na página 35
É possível incluir um usuário em uma nova lista de observação ou em uma lista de observação existente.

"Visualizando a lista de desbloqueio de usuários confiáveis" na página 37
É possível visualizar a lista de usuários confiáveis que estão incluídos na lista de desbloqueio na lista de gerenciamento de conjunto de referência.

"Incluindo origens de log no grupo de origens de log confiáveis" na página 39
Se você não desejar que o aplicativo UBA monitore e relate determinadas origens de log, será possível incluí-las no **UBA: grupo de origens de log confiáveis**. A inclusão de origens de log no grupo para o monitoramento delas pelo aplicativo UBA.

"Instalando o aplicativo Machine Learning Analytics" na página 174
Instale o app Machine Learning Analytics depois de ter instalado o app UBA no Extension Manager.

"Investigando os usuários no QRadar Advisor com o Watson" na página 14
Você pode selecionar usuários do aplicativo User Behavior Analytics (UBA) para enviar ao QRadar Advisor com o Watson para investigação.

Investigando os usuários no QRadar Advisor com o Watson

Você pode selecionar usuários do aplicativo User Behavior Analytics (UBA) para enviar ao QRadar Advisor com o Watson para investigação.

Antes de Iniciar

- Deve-se ter o aplicativo User Behavior Analytics (UBA) V2.7.0 ou mais recente instalado e configurado com dados do usuário.
- Você deve ter privilégios de Administrador.
- Deve-se ter o QRadar Advisor com o Watson V 1.13.0 ou mais recente instalado.

Para obter informações adicionais, consulte https://developer.ibm.com/qradar/advisor.

Sobre Esta Tarefa

Nota: Este recurso está disponível somente no User Behavior Analytics V2.7.0 e posterior e no QRadar Advisor com o Watson V1.13.0 e posterior.

Procedimento

1. Clique na guia **Análise de dados do usuário** para abrir o Painel do UBA.
2. Selecione um usuário ou procure um usuário para abrir a página Detalhes do Usuário.
3. Clique no ícone **Procurar Watson**. Quando o ícone parar de girar, será possível revisar seus resultados no QRadar Advisor com o aplicativo Watson.
4. Na guia **Watson**, na página Visão Geral do Incidente, selecione a investigação do usuário.

   Investigações do usuário são indicadas com o ícone do  **Investigação Iniciada a partir do UBA**.

Pré-requisitos para instalar o aplicativo User Behavior Analytics

Antes de instalar o aplicativo User Behavior Analytics (UBA), assegure-se de atender aos requisitos.

- Verifique se você tem o IBM Security QRadar V7.2.8 ou mais recente instalado.

  Para ter a melhor experiência, faça upgrade de seu sistema QRadar para as versões a seguir:
  - QRadar 7.2.8 Correção 13 (7.2.8.20180529210357) ou posterior
  - QRadar 7.3.1 Correção 6 (7.3.1.20180912181210) ou posterior
- Instale os pacotes de conteúdo por meio do IBM App Exchange
- Inclua o IBM Sense DSM para o aplicativo User Behavior Analytics (UBA).

Dependências de conteúdo

Diversas regras foram projetadas para alimentar eventos para o UBA por meio de outros aplicativos. Essas regras requerem que o conteúdo para os outros aplicativos seja instalado para que elas funcionem corretamente.

Para obter mais informações sobre o conteúdo do UBA e os aplicativos necessários, consulte a tabela a seguir.

Conteúdo do UBA	Apps necessários
"Analisador QRadar DNS" na página 128	IBM QRadar DNS Analyzer
UBA QRadar Network Insights	QRadar Network Insights Content v7.2.8 Conteúdo do QRadar Network Insights para V7.3.0+
Reconhecimento	IBM Security Reconnaissance Content

Conteúdo do UBA	Apps necessários
Monitoramento do sistema (sysmon)	IBM QRadar Content para Sysmon

Nota: Se você editar essas regras, elas podem não funcionar conforme o esperado.

Instalando o IBM Sense DSM manualmente

O aplicativo User Behavior Analytics (UBA) usa o IBM Sense DSM para incluir pontuações de risco do usuário e ofensas para o QRadar. É possível instalar o DSM por meio de atualizações automáticas ou é possível fazer upload para o QRadar e instalá-lo manualmente.

Nota: Se o seu sistema estiver desconectado da Internet, poderá ser necessário instalar o RPM do DSM manualmente.

Restrição: A desinstalação de um Device Support Module (DSM) não é suportada no QRadar.

1. Faça download do arquivo RPM do DSM no website Suporte IBM:
   - Para o QRadar V7.2.8: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
   - Para o QRadar V7.3.1 e mais recente: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`
2. Copie o arquivo RPM para o QRadar Console.
3. Use SSH para efetuar login no host do QRadar como usuário raiz.
4. Acesse o diretório que inclui o arquivo transferido por download.
5. Digite o seguinte comando:
   `rpm -Uvh <rpm_filename>`
6. Nas configurações de **Administrador**, clique em**Implementar mudanças**.
7. Nas configurações de **Administrador**, selecione **Avançado** > **Reiniciar serviços da web**.

Navegadores suportados para o aplicativo UBA

Para que os recursos nos produtos IBM Security QRadar funcionem adequadamente, deve-se usar um navegador da web suportado.

A tabela a seguir lista as versões suportadas de navegadores da web.

Navegador web	Versões suportadas
Mozilla Firefox	Liberação do suporte estendido 45.2
Google Chrome	Último

Nota: Para maximizar sua experiência com o UBA, é necessário executar um dos procedimentos a seguir:

- Desativar o bloqueador de pop-up para seu navegador
- Configurar o navegador para permitir exceções para pop-ups que vêm do endereço IP do QRadar Console

Tipos de origem de log relevantes para o aplicativo UBA

O app User Behavior Analytics (UBA) e o app ML podem aceitar e analisar eventos de determinadas origens de log.

Em geral, o app UBA e o app ML requerem origens de log que forneçam um nome do usuário. Para o UBA, se não houver nenhum nome do usuário, ative a caixa de seleção **Procurar ativos para nome do usuário quando nenhum nome de usuário estiver disponível para dados de evento ou de fluxo** em

Configurações do UBA para que o UBA possa tentar consultar o usuário na tabela de ativos. Se nenhum usuário puder ser determinado, o UBA não processará o evento.

Para obter mais detalhes sobre casos de uso específicos e os tipos de origem de log correspondentes, veja 7, “Regras e ajuste para o aplicativo UBA”, na página 45.

Tarefas relacionadas:

“Definindo as configurações do UBA” na página 28
Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar as definições do aplicativo UBA.

2 Instalando e Desinstalando

Instalando o aplicativo User Behavior Analytics

Use a ferramenta IBM QRadar Extension Management para fazer upload e instalar seu archive do aplicativo diretamente no QRadar Console.

Antes de Iniciar

Conclua o "Pré-requisitos para instalar o aplicativo User Behavior Analytics" na página 14.

Importante: Antes de instalar o aplicativo, assegure-se de que o IBM QRadar atenda aos requisitos mínimos de memória (RAM). O aplicativo UBA requer 1 GB de memória livre do conjunto de aplicativos da memória. O aplicativo do UBA falhará ao ser instalado se o conjunto de aplicativos não tiver memória livre suficiente.

Sobre Esta Tarefa

A instalação foi mudada iniciando com a V2.8.0. Os pacotes de conteúdo específicos do UBA, que contêm regras para acionar ofensas, agora são instalados como extensões separadas. Os pacotes de conteúdo são instalados por padrão. Se você escolher criar as suas próprias regras customizadas para acionar ofensas no UBA, será possível mudar a configuração **Instalar e fazer upgrade de pacotes de conteúdo** ao definir as Configurações do UBA.

Atenção: Após a instalação do app, você deverá:

- Ativar índices
- Implemente a configuração integral.
- Limpe o seu cache do navegador e atualize a janela do navegador.
- Configure permissões para os usuários que requerem acesso para visualizar a guia Análise de dados do usuário. As permissões a seguir devem ser designadas para cada função de usuário que requer acesso ao aplicativo:
  - Análise de dados do usuário
  - Ofensas
  - Atividade do Log

Depois de fazer download de seu aplicativo por meio do IBM Security App Exchange, use a ferramenta IBM QRadar Extension Management para instalá-lo em seu QRadar Console.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação (☰) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique em **Configuração do Sistema** > **Gerenciamento de Extensões** .
3. Na janela Gerenciamento de extensões, clique em **Incluir** e selecione o archive do aplicativo do UBA do qual você deseja fazer upload para o console.
4. Marque a caixa de seleção **Instalar imediatamente** e clique em **Incluir**.
5. No prompt, selecione **Sobrescrever**.

Importante: Você pode ter que esperar alguns minutos para que o aplicativo se torne ativo. Após o aplicativo do UBA ser instalado, os pacotes de conteúdo serão instalados no segundo plano. O conteúdo pode não estar visível no QRadar imediatamente após a instalação do aplicativo.

6. Nas configurações de **Administrador**, clique em **Configuração do sistema** > **Gerenciamento de índice** e, em seguida, ative os índices a seguir:
   - Categoria de Alto Nível
   - Categoria de Baixo Nível
   - Nome de usuário
   - senseValue
7. Nas configurações de **Administrador**, clique em **Avançado** > **Implementar configuração integral**.

   Nota: Os pacotes de conteúdo a seguir são instalados após a instalação do UBA ser concluída e o UBA estar configurado.
   - Conteúdo de autenticação e acesso do User Behavior Analytics
   - Conteúdo de privilégios e contas do User Behavior Analytics
   - Conteúdo do Comportamento Navegação do User Behavior Analytics
   - Conteúdo DNS do User Behavior Analytics DNS Analyzer
   - Conteúdo do Nó de Extremidade do User Behavior Analytics
   - Conteúdo de exfiltração do User Behavior Analytics Exfiltration
   - Conteúdo de Geografia do User Behavior Analytics
   - Conteúdo de ataques e de tráfego de rede do User Behavior Analytics
   - Conteúdo do QRadar Network Insights para o User Behavior Analytics
   - Conteúdo de Reconciliação do User Behavior Analytics
   - Conteúdo Sysmon do User Behavior Analytics Sysmon
   - Conteúdo do User Behavior Analytics Threat Intelligence

O que Fazer Depois

- Quando a instalação estiver concluída, limpe o cache do navegador e atualize a janela do navegador antes de usar o aplicativo.
- Gerenciar permissões para funções de usuário do aplicativo UBA.

Tarefas relacionadas:

"Ativando índices para melhorar o desempenho" na página 41
Para melhorar o desempenho de seu aplicativo IBM QRadar User Behavior Analytics (UBA), ative os índices no IBM QRadar.

"Gerenciando permissões para o aplicativo QRadar UBA" na página 35
Os administradores usam o recurso Gerenciamento de função de usuário no IBM QRadar para configurar e gerenciar contas de usuários. Como um administrador, deve-se ativar as permissões Análise de dados do usuário, Ofensas e Atividade de log para cada função do usuário que estiver autorizado a usar o aplicativo QRadar UBA.

Desinstalando o app UBA

Utilize a ferramenta IBM QRadar Extension Management para desinstalar seu aplicativo do seu QRadar Console.

Antes de Iniciar

Se você tiver um app Machine Learning Analytics (ML) instalado, deverá desinstalar o app ML da página de Configurações do Machine Learning antes de desinstalar o app UBA da janela Gerenciamento de

extensão. Se você não remove o aplicativo ML antes de desinstalar o UBA, deve removê-lo da interface da documentação da API interativa.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique em **Extension Management**.
3. Na guia **INSTALLED** da janela Gerenciamento de extensão, selecione o aplicativo User Behavior Analytics e clique em **Desinstalar**.

   Quando você desinstala um aplicativo, ele é removido do sistema. Se quiser reinstalá-lo, deve-se incluí-lo novamente.
4. Iniciando com a V2.8.0, os pacotes de conteúdo a seguir são instalados quando você configura o aplicativo do UBA. Deve-se desinstalar cada pacote de conteúdo para remover completamente o aplicativo.
   - Conteúdo de autenticação e acesso do User Behavior Analytics
   - Conteúdo de privilégios e contas do User Behavior Analytics
   - Conteúdo do Comportamento Navegação do User Behavior Analytics
   - Conteúdo DNS do User Behavior Analytics DNS Analyzer
   - Conteúdo do Nó de Extremidade do User Behavior Analytics
   - Conteúdo de exfiltração do User Behavior Analytics Exfiltration
   - Conteúdo de Geografia do User Behavior Analytics
   - Conteúdo de ataques e de tráfego de rede do User Behavior Analytics
   - Conteúdo do QRadar Network Insights para o User Behavior Analytics
   - Conteúdo de Reconciliação do User Behavior Analytics
   - Conteúdo Sysmon do User Behavior Analytics Sysmon
   - Conteúdo do User Behavior Analytics Threat Intelligence

3 Fazendo o upgrade

Fazendo upgrade do aplicativo User Behavior Analytics

Utilize a ferramenta IBM QRadar Extension Management para fazer upgrade do seu aplicativo.

Antes de Iniciar

Importante: Os requisitos de memória aumentaram a partir da V2.8.0. Antes de fazer upgrade do aplicativo, assegure-se de que o IBM QRadar atenda aos requisitos mínimos de memória (RAM). O aplicativo UBA requer 1 GB de memória livre do conjunto de aplicativos da memória. O aplicativo do UBA falhará ao fazer upgrade se o conjunto de aplicativos não tiver memória livre suficiente.

Para ter a melhor experiência, faça upgrade de seu sistema QRadar para as versões a seguir:

- QRadar 7.2.8 Correção 13 (7.2.8.20180529210357) ou posterior
- QRadar 7.3.0 Correção 7 (7.3.0.20171205025101) ou mais recente
- QRadar 7.3.1 Correção 6 (7.3.1.20180912181210) ou posterior

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique em **Extension Management**.
3. Na janela Gerenciamento de extensão, clique em **Incluir** e selecione o archive do aplicativo UBA que você deseja fazer upload para o console.
4. No prompt, selecione **Sobrescrever**. Todos os dados existentes do seu aplicativo UBA permanecem intactos.

   Importante: Você pode ter que esperar alguns minutos para que o aplicativo se torne ativo. Após o aplicativo do UBA ser atualizado, os pacotes de conteúdo serão atualizados em segundo plano. O conteúdo pode não estar visível no QRadar imediatamente após o aplicativo ser atualizado.

   Nota: Os pacotes de conteúdo a seguir são atualizados após o upgrade do UBA ser concluído e o UBA ser configurado.
   - Conteúdo de autenticação e acesso do User Behavior Analytics
   - Conteúdo de privilégios e contas do User Behavior Analytics
   - Conteúdo do Comportamento Navegação do User Behavior Analytics
   - Conteúdo DNS do User Behavior Analytics DNS Analyzer
   - Conteúdo do Nó de Extremidade do User Behavior Analytics
   - Conteúdo de exfiltração do User Behavior Analytics Exfiltration
   - Conteúdo de Geografia do User Behavior Analytics
   - Conteúdo de ataques e de tráfego de rede do User Behavior Analytics
   - Conteúdo do QRadar Network Insights para o User Behavior Analytics
   - Conteúdo de Reconciliação do User Behavior Analytics
   - Conteúdo Sysmon do User Behavior Analytics Sysmon
   - Conteúdo do User Behavior Analytics Threat Intelligence

O que Fazer Depois

Quando o upgrade estiver concluído, limpe o cache do navegador e atualize a janela do navegador antes de usar o aplicativo.

4 Configurando o

Configurando o aplicativo User Behavior Analytics

Para poder usar o aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar definições adicionais.

Quando você instalar o aplicativo do UBA, o aplicativo do IBM QRadar Reference Data Import LDAP (LDAP) também será instalado. Se você escolher usar o aplicativo LDAP, deverá configurar aplicativo LDAP antes de configurar o aplicativo do UBA. Os dados que o aplicativo UBA usa são de uma consulta LDAP. A consulta LDAP recupera a lista de usuários que é usada para preencher o aplicativo UBA.

Tanto o aplicativo do UBA quanto o aplicativo LDAP requerem tokens de autorização separados. Será possível criar os tokens de autorização ao configurar cada aplicativo.

Conclua os procedimentos de configuração a seguir:

- Configure o aplicativo Reference Data Import se você estiver usando LDAP
- Defina as configurações do UBA para o aplicativo do UBA

Configurando o aplicativo Reference Data Import LDAP

Quando você instala o aplicativo IBM® QRadar® User Behavior Analytics (UBA), o aplicativo Reference Data Import LDAP também é instalado. É possível usar o aplicativo LDAP para importar dados do usuário de um servidor LDAP/AD ou de um arquivo CSV para uma tabela de referência do QRadar. A tabela de referência é, então, consumida pelo aplicativo UBA ou pode ser usada para procuras ou regras do QRadar.

Antes de Iniciar

Atenção: Se você instalou anteriormente o aplicativo Reference Data Import LDAP, ele será substituído quando o aplicativo UBA for instalado. Suas configurações serão incluídas na versão atualizada do aplicativo Reference Data Import LDAP.

Sobre Esta Tarefa

Nota: Certifique-se de anotar o nome da tabela de referência e, se fornecido, um alias customizado para qualquer um dos atributos. Ao configurar o aplicativo UBA, selecione a tabela de referência criada no aplicativo Reference Data Import LDAP.

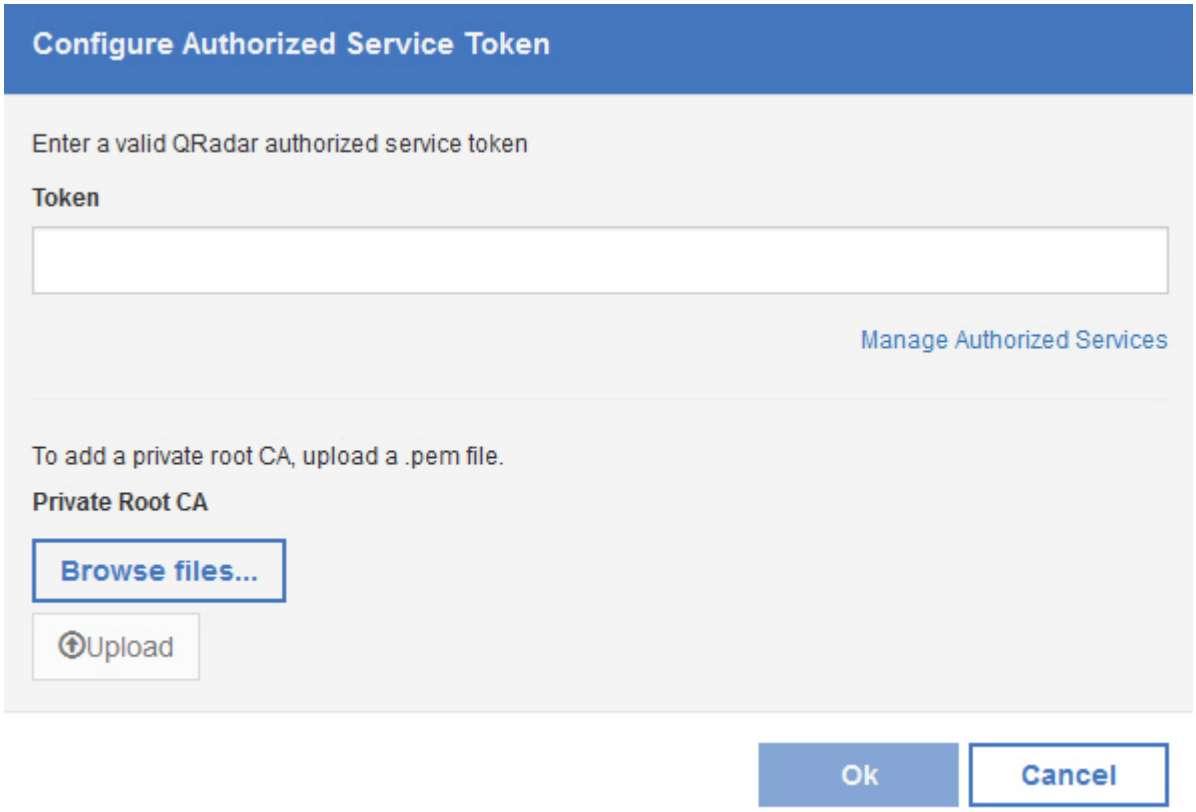
Para obter mais informações sobre o aplicativo Reference Data Import LDAP, consulte a seção a seguir do IBM Knowledge Center: http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.apps.doc/c_Qapps_LDAP_intro.html

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Importação de dados de referência - LDAP**.
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.

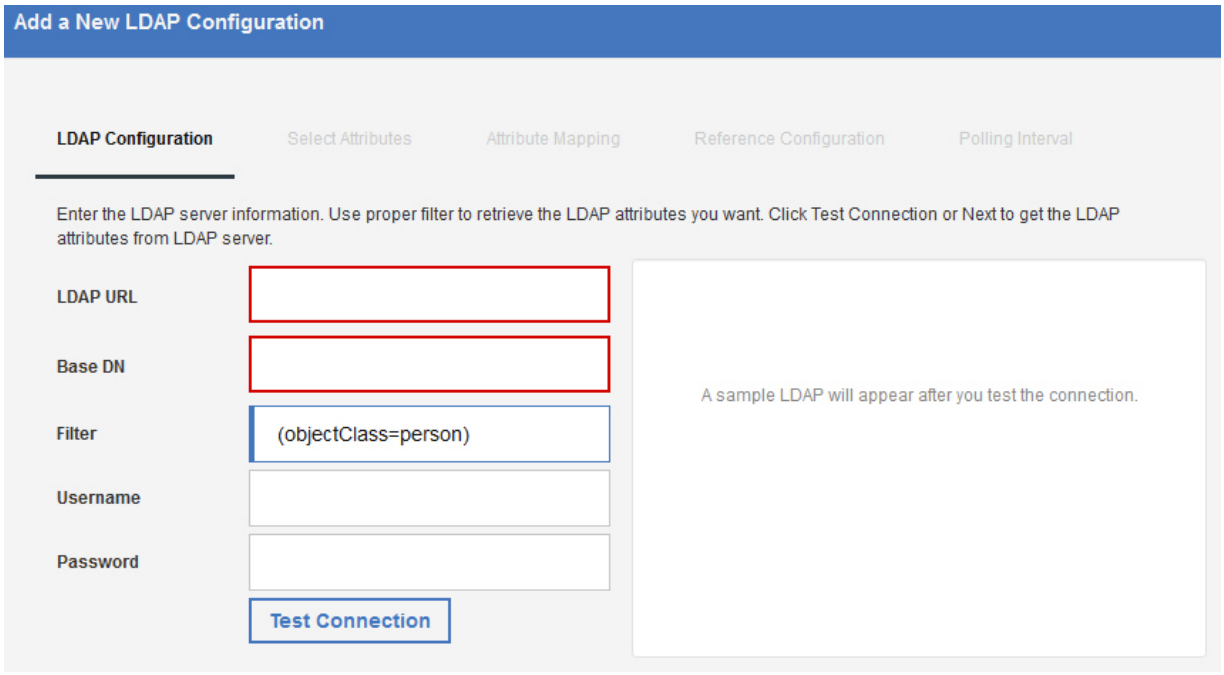
- No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Importação de dados de referência - LDAP** > **Importação de dados de referência - LDAP**.

3. Clique em **Configurar** para criar um token de serviço autorizado para LDAP. A caixa Configurar token de serviço autorizado é aberta.
   a. Clique no link **Gerenciar serviços autorizados** e, em seguida, clique em **Incluir serviço autorizado**.
   b. No campo **Nome do serviço**, digite `LDAP`. Este é o usuário como o qual as solicitações de API do aplicativo LDAP são executadas.
   c. Na lista **Função de usuário**, selecione a função de usuário **Administrador**.
   d. Na lista **Perfil de segurança**, selecione o perfil de segurança que você deseja designar a esse serviço autorizado. O perfil de segurança determina as redes e fontes de log às quais esse serviço pode acessar na interface com o usuário do QRadar.
   e. Na lista **Data de validade**, digite ou selecione uma data para esse serviço expirar. Caso uma data de validade não seja necessária, selecione **Sem expiração**.
   f. Clique em **Criar Serviço**.
   g. Clique na linha que contém o serviço LDAP que você criou e, em seguida, selecione e copie a sequência de token do campo **Token selecionado** na barra de menus.
   h. Na caixa Configurar token de serviço autorizado, cole a sequência de token de serviço autorizado no campo **Token**.
4. Opcional: Para incluir um arquivo de autoridade de certificação raiz privada, clique em **Procurar arquivos**, abra um arquivo suportado, clique em **Abrir** e, em seguida, clique em **Fazer upload**. O tipo de arquivo a seguir é suportado: `.pem`.
5. Clique em **OK**.

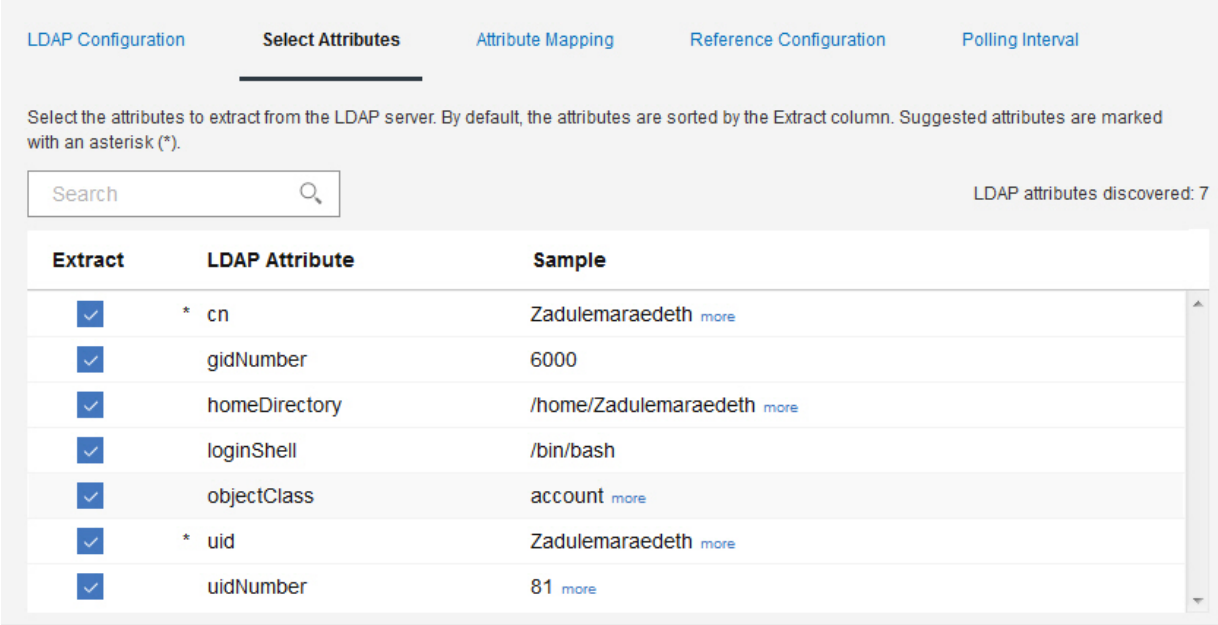


6. Na janela principal do aplicativo Importação de dados de referência (LDAP), clique em **Incluir importação**. A caixa de diálogo Incluir uma nova configuração LDAP é aberta.

7. Na guia **Configuração LDAP**, inclua informações de conexão para o servidor LDAP. O campo **Filtro** é preenchido automaticamente a partir de seus atributos do Active Directory.
   a. Insira uma URL que comece com `ldap://` ou `ldaps://` (para TLS) no campo **URL do LDAP**.
   b. Insira o ponto na árvore do diretório LDAP do qual o servidor deve procurar usuários no campo **DN base**. Por exemplo, se o seu servidor LDAP estava no domínio example.com, você poderia ver: `dc=example,dc=com`.
   c. Insira o atributo ou atributos que deseja usar para classificar os dados que são importados na tabela de referência no campo **Filtro**. Por exemplo: `cn=*; uid=*; sn=*`. Os valores padrão a seguir funcionarão com o Active Directory: `(&(sAMAccountName=*)(samAccountType=805306368))`.
   d. Insira o nome do usuário que é usado para autenticar o servidor LDAP no campo **Nome do usuário**.
   e. Insira a senha para o servidor LDAP no campo **Senha**.
8. Clique em **Conexão de teste** ou em **Avançar** para confirmar que o IBM QRadar pode conectar-se ao servidor LDAP. Se a sua tentativa de conexão for bem-sucedida, as informações do seu servidor LDAP serão exibidas na guia **Configuração de LDAP**.



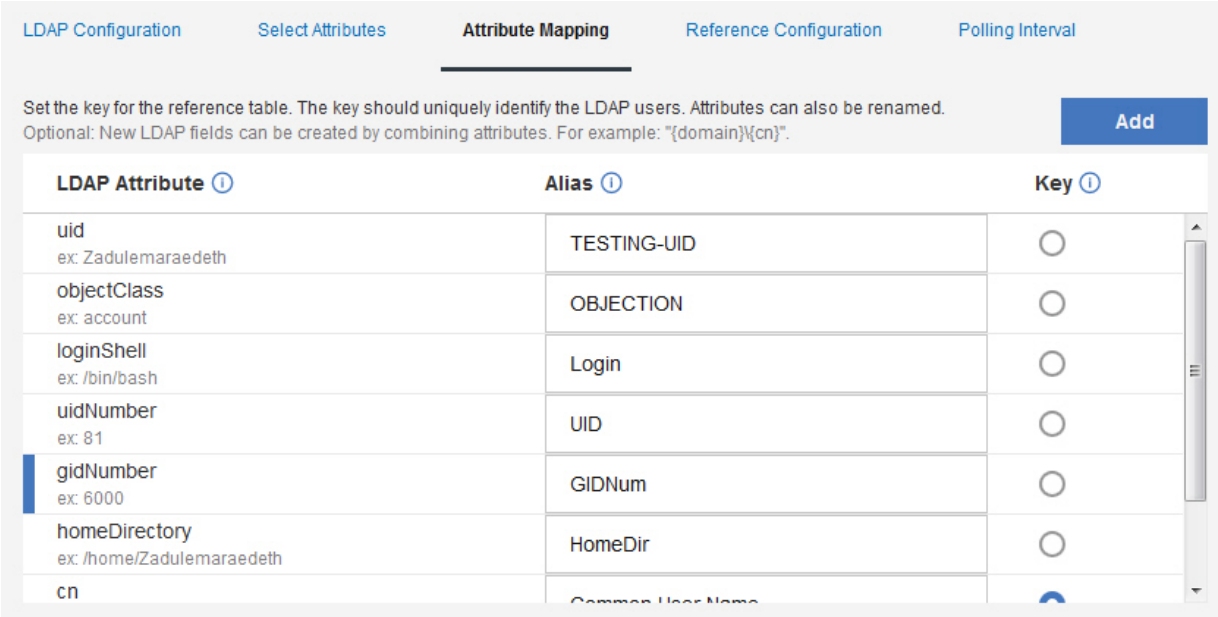
9. Na guia **Selecionar atributos**, selecione os atributos que você deseja extrair do servidor LDAP. Os valores padrão a seguir funcionarão com o Active Directory: `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.



10. Opcional: Na guia **Mapeamento de atributo**, configure a chave para a tabela de referência.

    Dica: É possível criar novos campos LDAP clicando em **Incluir** e combinando dois atributos. Por exemplo, é possível usar a sintaxe a seguir: `"Último: {ln}, Primeiro: {fn}"`.

    Dica: Se desejar mesclar dados do LDAP de diversas origens na mesma tabela de referência, será possível usar aliases customizados para diferenciar atributos LDAP com o mesmo nome em diferentes origens.

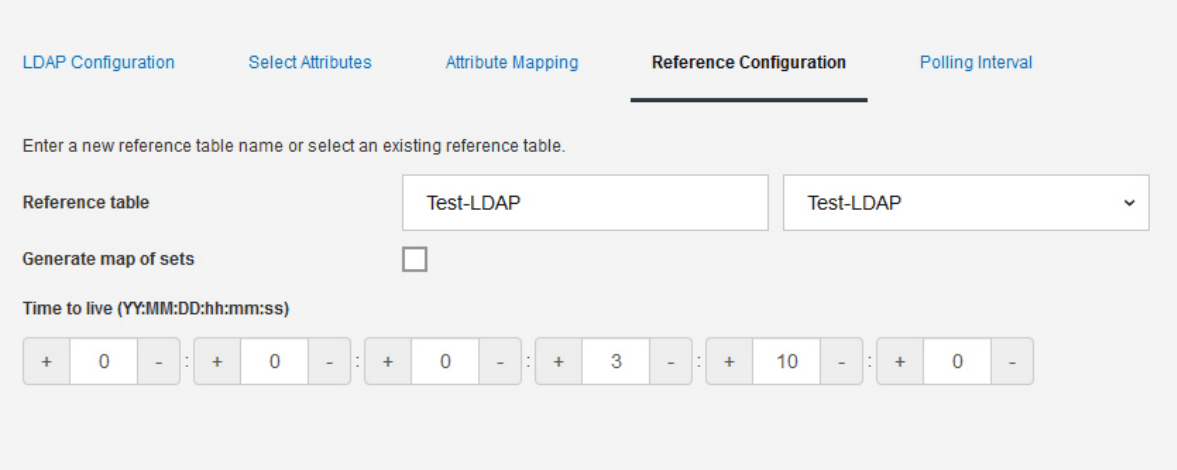


11. Na guia **Configuração de referência**, crie um novo mapa de referência de mapas ou designe um mapa de referência de mapas existente nos quais deseja incluir dados LDAP.
    a. No campo **Tabela de referência**, insira o nome para uma nova tabela de referência. Como alternativa, inclua o nome de uma tabela de referência existente à qual você deseja anexar os dados LDAP da lista.

b. A caixa de seleção **Gerar mapa de conjuntos** está desativada por padrão. Se você ativar a caixa de seleção, ela enviará dados para um formato de conjunto de referência para melhorar a procura do QRadar, no entanto isso poderá afetar o desempenho.

c. Na seção **Tempo de vida**, defina quanto tempo você deseja que os dados persistam no mapa de referência de mapas. Por padrão, os dados que você inclui nunca expiram. Quando o período de tempo de vida é excedido, um evento *ReferenceDataExpiry* é acionado.

Nota: Se você anexar dados a um mapa de referência de mapas existente, o aplicativo usará os parâmetros de tempo de vida originais. Esses parâmetros não podem ser substituídos na guia **Configuração de referência**.



12. Na guia **Pesquisa**, defina a frequência com que deseja que o aplicativo pesquise dados no servidor LDAP.

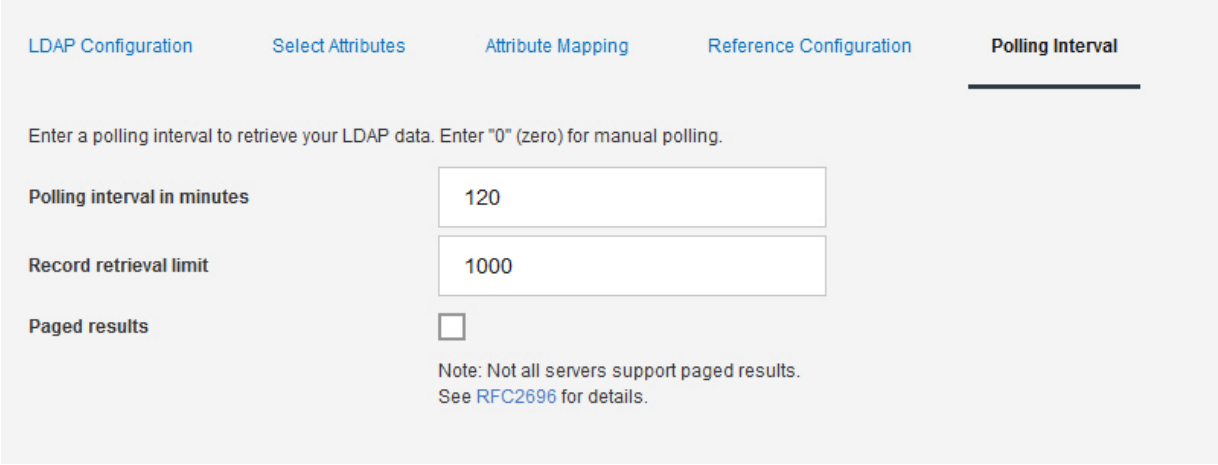
a. No campo **Intervalo de pesquisa em minutos**, defina em minutos com que frequência deseja que o aplicativo pesquise dados no servidor LDAP.

Nota: O valor mínimo do intervalo de pesquisa é 120. Também é possível inserir um intervalo de pesquisa de zero. Se você inserir um intervalo de pesquisa de zero, deverá pesquisar o aplicativo manualmente com a opção de pesquisa exibida no feed.

b. No campo **Limite de recuperação de registro**, insira um valor para o número de registros que você deseja que a pesquisa retorne. Por padrão, 100.000 registros são retornados. O número máximo de registos que podem ser retornados é 200.000.

c. Opcional: A caixa de seleção **Resultados paginados** é selecionada por padrão para evitar a limitação do número de registros que o servidor LDAP retorna para cada pesquisa.

Nota: Os resultados paginados não são suportados por todos os servidores LDAP.



13. Clique em **Salvar**.

Definindo as configurações do UBA

Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar as definições do aplicativo UBA.

Configurando o token de autorização nas configurações do QRadar

Para visualizar informações no aplicativo do IBM QRadar User Behavior Analytics (UBA), deve-se configurar um token de autorização do UBA em Configurações do UBA.

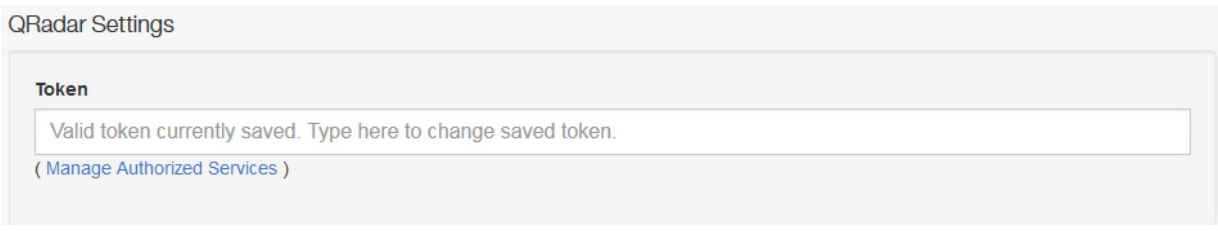
Sobre Esta Tarefa

Atenção: Os administradores do QRadar on Cloud não podem criar um token de serviço autorizado para aplicativos QRadar devido a recursos limitados do administrador. Se você for um cliente do QRadar on Cloud, entre em contato com o Suporte ao Cliente para criar um token de serviço autorizado para você.

Deve-se concluir as etapas a seguir para criar um token de autorização. Não salve a configuração até que você tenha configurado todas as Configurações do UBA.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações do UBA** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações UBA**.
3. Na seção Configurações do QRadar, clique no link **Gerenciar serviços autorizados**.



4. Clique em **Incluir Serviço Autorizado**
5. No campo **Nome do serviço**, digite UBA.
6. Na lista **Função de usuário**, selecione a função de usuário **Administrador**.
7. Na lista **Perfil de segurança**, selecione o perfil de segurança que você deseja designar a esse serviço autorizado. O perfil de segurança determina as redes e fontes de log às quais esse serviço pode acessar na interface com o usuário do QRadar.
8. Na lista **Data de validade**, digite ou selecione uma data para esse serviço expirar. Caso uma data de validade não seja necessária, selecione **Sem expiração**.
9. Clique em **Criar Serviço**.
10. Clique na linha que contém o serviço UBA criado e, em seguida, selecione e copie a sequência de token do campo **Token selecionado** na barra de menus.
11. Retorne para a seção Configurações do QRadar e cole a sequência de token de serviço autorizado no campo **Token**.

O que Fazer Depois

"Configurando Definições do Pacote de Conteúdo"

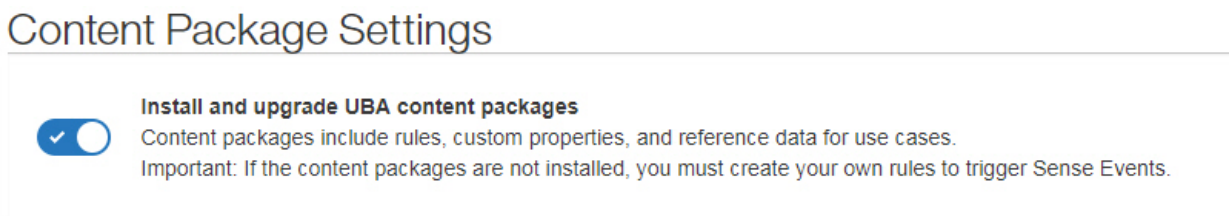
Configurando Definições do Pacote de Conteúdo

Para visualizar informações no aplicativo do IBM QRadar User Behavior Analytics (UBA), deve-se definir as configurações do pacote de conteúdo.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações do UBA** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações UBA**.
3. Na seção Configurações do pacote de conteúdo, a caixa de seleção **Instalar e fazer upgrade dos pacotes de conteúdo do UBA** é ativada por padrão. Se você não desejar instalar os pacotes de conteúdo do UBA, limpe a caixa de seleção e salve a configuração. Se você decidir não instalar os pacotes de conteúdo do UBA, deve-se criar as suas próprias regras para acionar eventos de verificação que enviam eventos para o UBA.

   Nota: Se você desmarcar a caixa de seleção **Instalar e fazer upgrade dos pacotes de conteúdo do UBA** e salvar a configuração e, em seguida, retornar para a página Configurações do UBA e decidir selecionar a caixa de seleção e salvar a configuração, o conteúdo será instalado e atualizado.



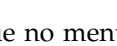
O que Fazer Depois

"Definindo configurações do aplicativo" na página 30

Definindo configurações do aplicativo

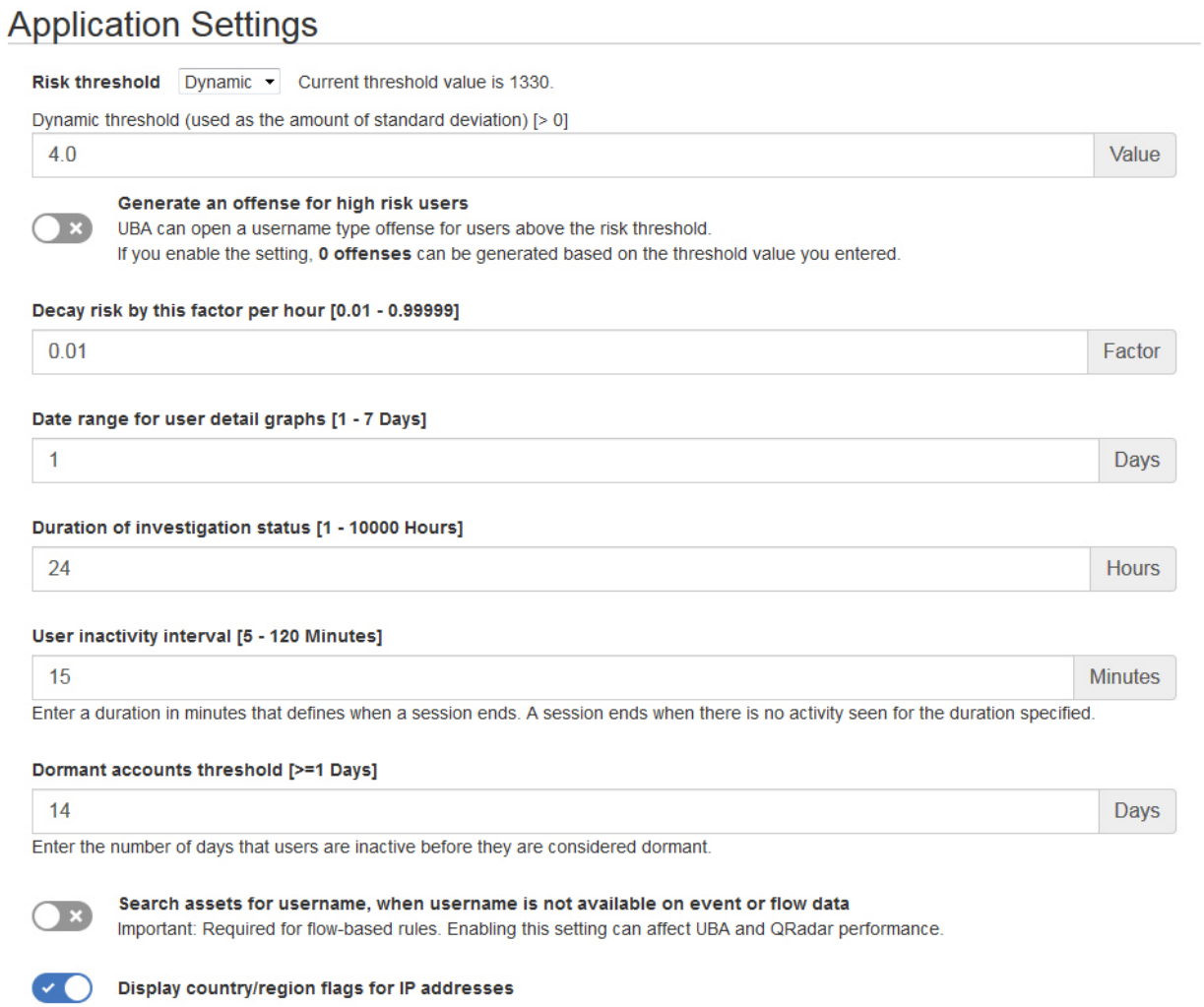
Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar as definições do aplicativo UBA.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações do UBA** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações UBA**.
3. Na seção Configurações do aplicativo, configure as definições a seguir:

Opção	Descrição
Limite de risco	Indica o limite máximo até o qual a pontuação de risco de um usuário deve chegar para que uma ofensa seja acionada com relação a esse usuário. Uma *pontuação de risco* é a adição de todos os eventos de risco detectados por regras do UBA. Selecione uma das seguintes opções: • **Dinâmico**: O valor padrão é 4.0. Quanto mais alto for o valor, maior será o limite dinâmico, resultando em menos ofensas. Você deve desligar **Gerar uma ofensa para usuários de alto risco**até que as configurações sejam executadas por pelo menos um dia. O valor do limite dinâmico é atualizado de hora em hora com base na distribuição de pontuação de risco no sistema. É possível determinar se você deseja ativar a configuração com base no número de ofensas que podem ser acionadas. Consulte a Dica para obter mais informações. **Nota:** Se não houver variedade suficiente em suas pontuações, a pontuação de risco será configurada como +10 do usuário de risco mais alto. Ela permanece assim para evitar que um grande número de ofensas seja gerado desnecessariamente. • **Estático**: o valor padrão é 100.000. O valor é configurado para um valor alto por padrão para evitar que delitos sejam acionados antes de o ambiente ser analisado. É possível ativar a opção **Gerar uma ofensa para usuários de alto risco** para abrir uma ofensa com um tipo de nome de usuário para usuários acima do limite de risco. É possível determinar se você deseja ativar a configuração com base no número de ofensas que podem ser acionadas. **Dica:** Considere configurar o UBA e deixar o valor padrão. Permita que as configurações sejam executadas por pelo menos um dia para ver o tipo das pontuações que são retornadas. Após alguns dias, revise os resultados no painel para determinar um padrão. É possível então ajustar o limite. Por exemplo, se você vê uma ou duas pessoas com pontuações no 500, mas a maioria está no 100, considere configurar o limite para 200 ou 300. Portanto, "normal" para seu ambiente pode ser aproximadamente 100 e qualquer pontuação acima que possa requerer sua atenção.
Reduzir risco por este fator por hora	Declínio de risco é a porcentagem que a pontuação de risco é reduzida a cada hora. O valor padrão é 0,5. **Nota:** Quanto maior o número, mais rapidamente a pontuação de risco decairá; quanto menor o número, mais lentamente a pontuação de risco decairá.
Intervalo de Data para Gráficos de Detalhes do Usuário	O intervalo de datas que é exibido para os gráficos de detalhes do usuário na página Detalhes do usuário. O valor padrão é 1.
Duração do status de investigação	O número de horas (1 - 10.000) designado para que uma investigação seja concluída.

Opção	Descrição
Intervalo de inatividade do usuário	A página Detalhes do usuário mostra uma linha de tempo com a atividade agrupada por sessões. Se um usuário estiver inativo pela quantia de tempo inserida no campo **Intervalo de inatividade do usuário**, a sessão terminará. O valor-padrão é de 15 minutos.
Limite de conta ociosa	O número de dias que os usuários ficam inativos antes de serem considerados inativos. O valor padrão é 14 dias. Para obter informações adicionais, consulte “Contas inativas” na página 39.(Disponível na V3.2.0 e mais recente).
Procurar ativos para nome do usuário, quando o nome do usuário não está disponível para dados de evento ou de fluxo	Selecione a caixa de seleção para procurar nomes de usuário na tabela de ativos. O aplicativo UBA usa ativos para consultar um usuário para um endereço IP quando nenhum usuário está listado em um evento. **Importante:** Esse recurso pode causar problemas de desempenho no aplicativo UBA e seu sistema QRadar. **Dica:** Se o limite de tempo limite de consulta for excedido, o aplicativo não retornará nenhum dado. Se você receber uma mensagem de erro no Painel UBA, desmarque a caixa de seleção e clique em **Atualizar**.
Exibir bandeiras do país/região para endereços IP	Limpe a caixa de seleção se você não deseja exibir bandeiras de país e região para endereços IP.



O que Fazer Depois

"Configurando a importação de dados do usuário e a união de usuários"

Configurando a importação de dados do usuário e a união de usuários

Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), é possível importar dados do usuário de uma tabela de referência.

Antes de Iniciar

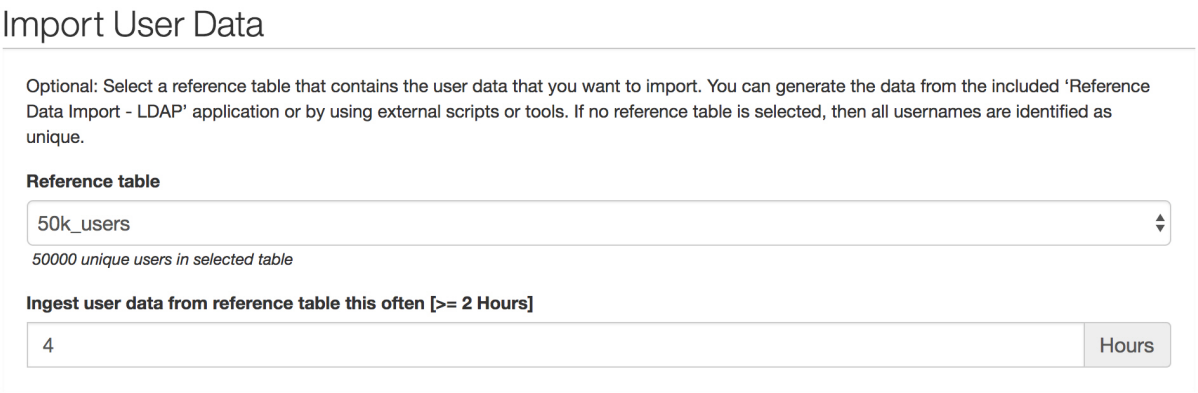
Conclua as instruções para o "Definindo configurações do aplicativo" na página 30.

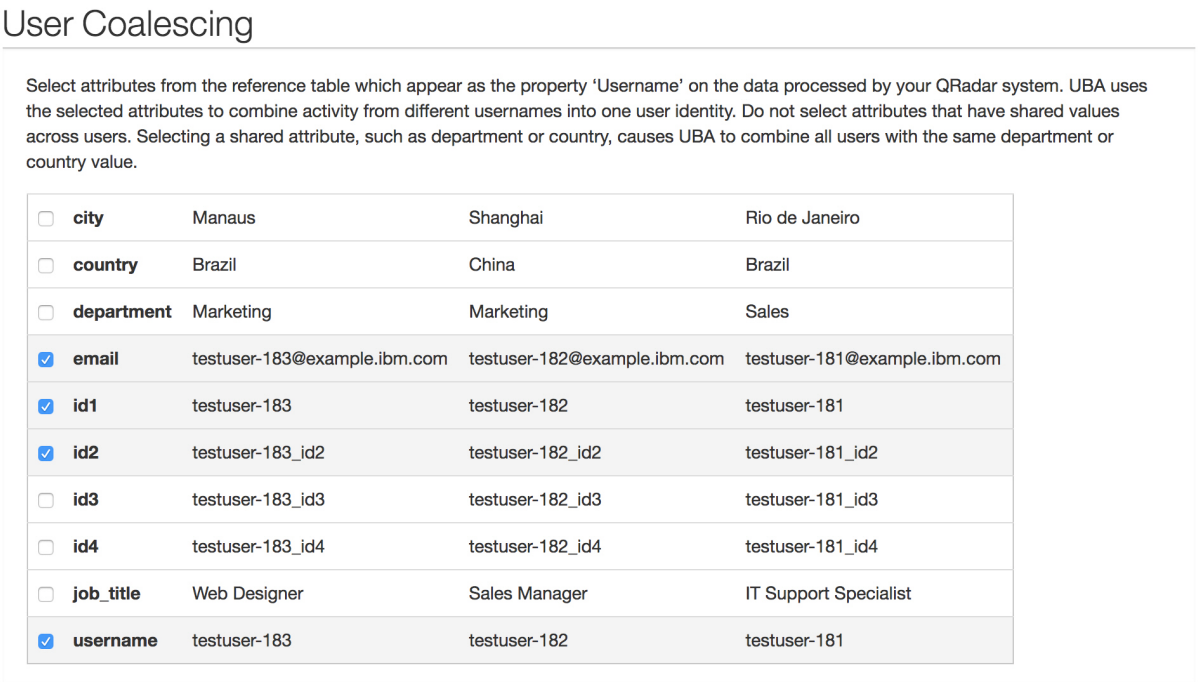
Sobre Esta Tarefa

A importação de dados do usuário e a união de usuários são opcionais.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações do UBA** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações UBA**.
3. Na seção Importar dados do usuário, selecione uma **Tabela de referência**.
4. Insira o número de horas para determinar com que frequência você deseja referenciar a tabela para alimentar os dados.
5. Na seção União de usuários, selecione os atributos que são puxados da tabela de referência selecionada e que aparecem como "Nome do usuário" em seu sistema QRadar. As pontuações de risco desses identificadores são incluídas e também associadas ao identificador primário. Não selecione atributos que tenham valores compartilhados entre usuários. Por exemplo, se houver muitas pessoas do mesmo departamento, não selecione "Departamento" como um nome de usuário. Selecionar um atributo compartilhado como "Departamento" ou "País" faz o UBA combinar todos os usuários com o mesmo valor de departamento ou país.





O que Fazer Depois

"Configurando Atributos de Exibição"

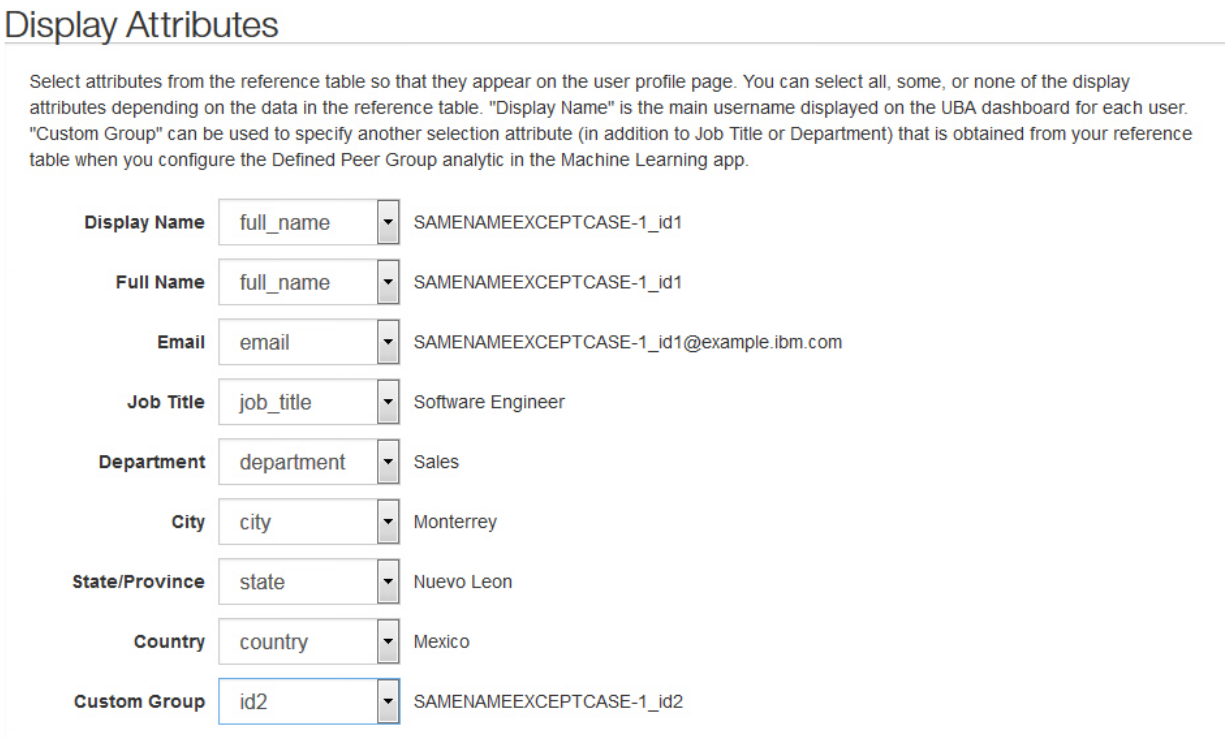
Configurando Atributos de Exibição

Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), é possível selecionar atributos da tabela de referência que você deseja exibir na página Detalhes do usuário.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações do UBA** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações UBA**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações UBA**.

3. Na seção Atributos de exibição, selecione os atributos que você deseja exibir na página Detalhes do usuário.



4. Clique em **Salvar Configuração**.

5 Administração

Gerenciando permissões para o aplicativo QRadar UBA

Os administradores usam o recurso Gerenciamento de função de usuário no IBM QRadar para configurar e gerenciar contas de usuários. Como um administrador, deve-se ativar as permissões Análise de dados do usuário, Ofensas e Atividade de log para cada função do usuário que estiver autorizado a usar o aplicativo QRadar UBA.

Sobre Esta Tarefa

Depois de instalar o aplicativo QRadar UBA, as permissões **Análise de dados do usuário**, **Ofensas** e **Atividade de log** devem ser ativadas para as funções de usuário que são designadas a usuários que pretendem usar o aplicativo QRadar UBA.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Na seção Configuração do sistema, clique em **Gerenciamento do usuário** e, em seguida, clique no ícone **Funções do usuário**.
3. Selecione uma função de usuário existente ou crie uma nova função.
4. Marque as caixas de seleção a seguir para incluir as permissões na função.
   - **Análise de dados do usuário**
   - **Ofensas**
   - **Atividade do Log**
5. Clique em **Salvar**.

Criando watchlists

É possível incluir um usuário em uma nova lista de observação ou em uma lista de observação existente.

Sobre Esta Tarefa

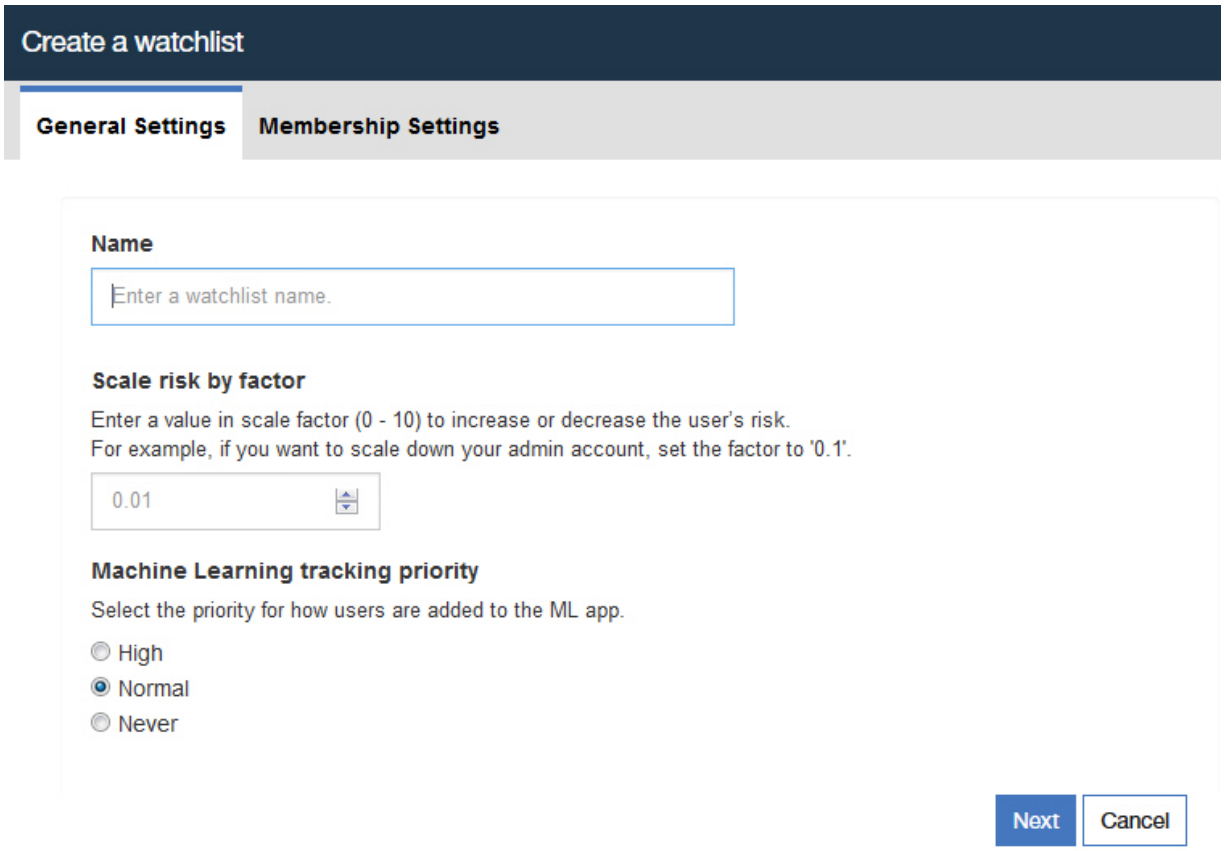
É possível incluir um usuário em uma nova lista de observação ou em uma lista de observação existente no UBA Painel, a página Detalhes do usuário ou a página Resultados da Procura. Um único usuário pode ser um membro de várias listas de observação.

Procedimento

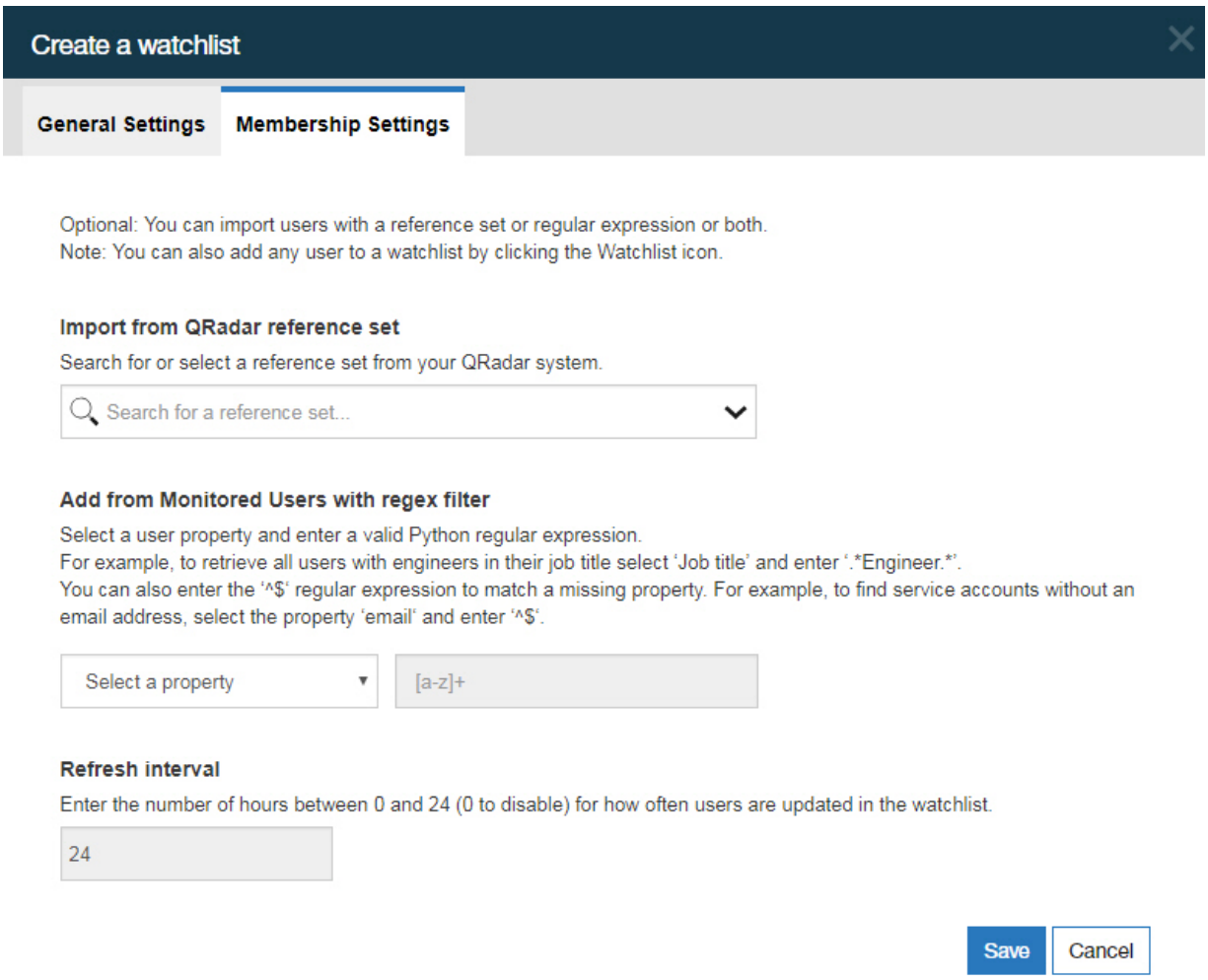
1. Na página Painel do UBA ou Detalhes do usuário, clique no ícone **Lista de observação**  .
2. No menu, selecione **Criar nova lista de observação**. Para incluir um usuário em uma lista de observação existente, clique em **Incluir em** em sua lista de observação.
3. Na guia **Configurações gerais**, insira um nome da lista de observação.
4. É possível aumentar ou diminuir artificialmente a pontuação de risco do usuário, mudando o valor no campo **Escala de risco por fator**. O fator padrão de '1' deixa a pontuação de risco inalterada.

Nota: Se um usuário estiver em mais de uma lista de observação, o fator de maior escala será aplicado.

5. Na seção **Prioridade de rastreamento de aprendizado de máquina**, selecione a prioridade para como os usuários são controlados pelo Machine Learning Analytics.
   - Alto - Os usuários são sempre rastreados até o máximo de usuários por Machine Learning Analytics.
   - Normal - Os usuários são rastreados por risco mais alto após todos os usuários altos serem incluídos.
   - Nunca - Os usuários não são rastreados pelo Machine Learning.
6. Clique em **Avançar**.



7. Na guia **Configurações de associação**, é possível preencher automaticamente a lista de observação com os usuários de um conjunto de referência, uma expressão regular ou ambos.
8. Opcional: No campo **Importar do conjunto de referência do QRadar**, procure um conjunto de referência ou clique para selecionar um conjunto de referência na lista, para importar todas as entradas do conjunto de referência. Observação: a lista pode conter conjuntos de referência que não têm nomes de usuário. Depois de selecionar um conjunto de referência, clique no link para revisar.
9. Opcional: No campo **Incluir de Usuários monitorados com filtro Regex**, é possível selecionar uma propriedade de usuário e inserir uma expressão regular Python válida para selecionar usuários que já estão localizados no banco de dados UBA.
10. No campo **Intervalo de atualização**, insira o número de horas para a frequência com que você deseja que a lista de usuários seja atualizada. Por exemplo, se você inserir 10, a lista de usuários será atualizada a cada 10 horas. Se o **Intervalo de atualização** for configurado para um valor de 0 (zero), será possível atualizar manualmente a lista de observação clicando em **Atualizar**.
11. Clique em **Salvar**.



Visualizando a lista de desbloqueio de usuários confiáveis

É possível visualizar a lista de usuários confiáveis que estão incluídos na lista de desbloqueio na lista de gerenciamento de conjunto de referência.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação (☰) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Na seção Configuração do sistema, clique em **Gerenciamento de conjunto de referência**.
3. Na janela Gerenciamento de conjunto de referência, selecione o conjunto de referência **UBA: nomes de usuários confiáveis**.
4. Clique em **Visualizar Conteúdo**.

Gerenciando ferramentas de monitoramento de rede

É possível gerenciar ferramentas de monitoramento de rede para o aplicativo IBM QRadar User Behavior Analytics (UBA).

Sobre Esta Tarefa

Se você desejar monitorar o uso do programa de captura, monitoramento ou análise de rede, certifique-se de que os programas estejam listados no conjunto de referência UBA: nomes de arquivos do programa de captura, monitoramento e análise de rede. Deve-se então ativar a regra **UBA: nomes de arquivos do programa de captura, monitoramento e análise de rede**.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Na seção Configuração do sistema, clique em **Gerenciamento de conjunto de referência**.
3. Na janela Gerenciamento de conjunto de referência, selecione o conjunto de referência **UBA: nomes de arquivos do programa de captura, monitoramento e análise de rede**.
4. Clique em **Visualizar Conteúdo**.
5. Para incluir um aplicativo para gerenciamento, clique em **Incluir** e insira os valores na caixa.
6. Para remover um aplicativo, selecione um aplicativo e clique em **Excluir**.

O que Fazer Depois

Ative a regra **UBA: nomes de arquivos do programa de captura, monitoramento e análise de rede**.

Gerenciando programas restritos

É possível gerenciar programas restritos para o aplicativo IBM QRadar User Behavior Analytics (UBA).

Sobre Esta Tarefa

Se houver quaisquer aplicativos que você deseja monitorar para uso, acesse o conjunto de referência UBA: nomes de arquivos do programa restrito e insira os aplicativos que desejar monitorar. Deve-se então ativar a regra UBA: nomes de arquivos do programa restrito.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Na seção Configuração do sistema, clique em **Gerenciamento de conjunto de referência**.
3. Na janela Gerenciamento de conjunto de referência, selecione o conjunto de referência **UBA: nomes de arquivos do programa restrito**.
4. Clique em **Visualizar Conteúdo**.
5. Para incluir um aplicativo para gerenciamento, clique em **Incluir** e insira os valores na caixa.
6. Para remover um aplicativo, selecione um aplicativo e clique em **Excluir**.

O que Fazer Depois

Ative a regra **UBA: nomes de arquivos do programa restrito**.

Incluindo origens de log no grupo de origens de log confiáveis

Se você não desejar que o aplicativo UBA monitore e relate determinadas origens de log, será possível incluí-las no **UBA: grupo de origens de log confiáveis**. A inclusão de origens de log no grupo para o monitoramento delas pelo aplicativo UBA.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Origens de Log**.
3. Clique em **Incluir (Add)**.
4. Configure os parâmetros comuns para sua fonte de log.
5. Configure os parâmetros específicos de protocolo para sua fonte de log.
6. Marque a caixa de seleção **UBA: grupo de origens de log confiáveis**.
7. Clique em **Salvar**.
8. Na guia **Administrador**, clique em **Implementar mudanças**.

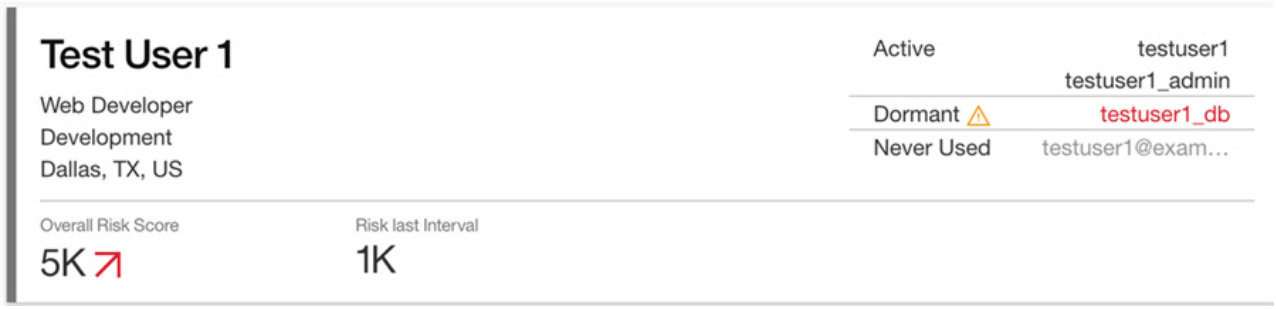
Contas inativas

É possível ver usuários em seu sistema que possuem contas inativas, contas ativas ou contas que nunca foram usadas.

Visualizando contas inativas na página Detalhes do Usuário

Na V3.2.0 e mais recente, é possível ver o status das contas que estão associadas ao usuário selecionado na página Detalhes do Usuário.

Status de conta do usuário	**Descrição**
Ativa	Uma conta da qual UBA viu eventos a partir de uma origem de log do QRadar dentro do período limite configurado de conta inativa.
Inativa	Uma conta da qual UBA viu pelo menos um evento no passado, mas não viu nenhum novo evento durante o período limite de conta inativa.
Nunca usada	Uma conta para a qual UBA nunca viu um evento com esse nome de usuário em uma origem de log do QRadar. As contas identificadas como "Nunca Usadas" podem ser causadas pelas atividades a seguir: • Contas que nunca foram registradas por uma origem de log do QRadar para a conta de nome de usuário associada. • O evento ocorreu antes do UBA V3.2.0 ser instalado. Nota: quando você instala o aplicativo UBA pela primeira vez, apenas os eventos que ocorreram na última hora são analisados para determinar quando uma conta foi acessada pela última vez. Após a análise inicial, o aplicativo UBA consulta eventos que ocorreram entre as execuções de a tarefa em segundo plano que vigia o uso da conta. Nota: as contas que são categorizadas como "Nunca usada" provavelmente foram importadas a partir do aplicativo LDAP.



Lista de observação Usuários com Contas Inativas

A lista de observação Usuários com Contas Inativas é gerada automaticamente à medida que o aplicativo UBA extrai os dados do usuário. É possível visualizar a lista de observação Usuários com Contas Inativas no Painel do UBA.

Se você excluir a lista de observação, ela não será recriada automaticamente. Se você precisar criá-la novamente, selecione a referência **UBA: contas inativas** configurada na guia **Configurações de associação** na tela Criar uma lista de observação.

Configurando o limite de contas inativas

O valor padrão para o limite de contas inativas é de 14 dias. É possível mudar o número de dias que os usuários ficam inativos antes de serem considerados inativos na seção Configurações do Aplicativo na página Configurações do UBA (**Configurações de administrador** > **Análise de dados do usuário** > **Configurações do UBA**).

Respostas para contas inativas ou usuários

É possível gerar respostas para contas inativas a partir das regras fornecidas. Também é possível criar respostas customizadas usando os eventos que são acionados a partir do aplicativo.

Para usar as regras fornecidas para que a pontuação de um usuário seja aumentada quando uma conta que estava inativa for usada ou houver tentativa de usá-la, certifique-se de que as regras a seguir estejam ativadas:

- "UBA: tentativa de uso de conta inativa" na página 73
- "UBA: conta inativa usada" na página 72

Para criar respostas customizadas, é possível usar os eventos gerados a seguir em uma regra ou consulta:

- Conta inativa localizada (QID 104000012)
- Conta inativa usada (QID 104000013)

Conceitos relacionados:

"Painel do UBA e detalhes do usuário" na página 9
O aplicativo IBM QRadar User Behavior Analytics (UBA) mostra a você os dados de risco gerais para usuários em sua rede.

Tarefas relacionadas:

"Definindo configurações do aplicativo" na página 30
Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar as definições do aplicativo UBA.

"Criando watchlists" na página 35
É possível incluir um usuário em uma nova lista de observação ou em uma lista de observação existente.

6 Ajustar

Ativando índices para melhorar o desempenho

Para melhorar o desempenho de seu aplicativo IBM QRadar User Behavior Analytics (UBA), ative os índices no IBM QRadar.

Sobre Esta Tarefa

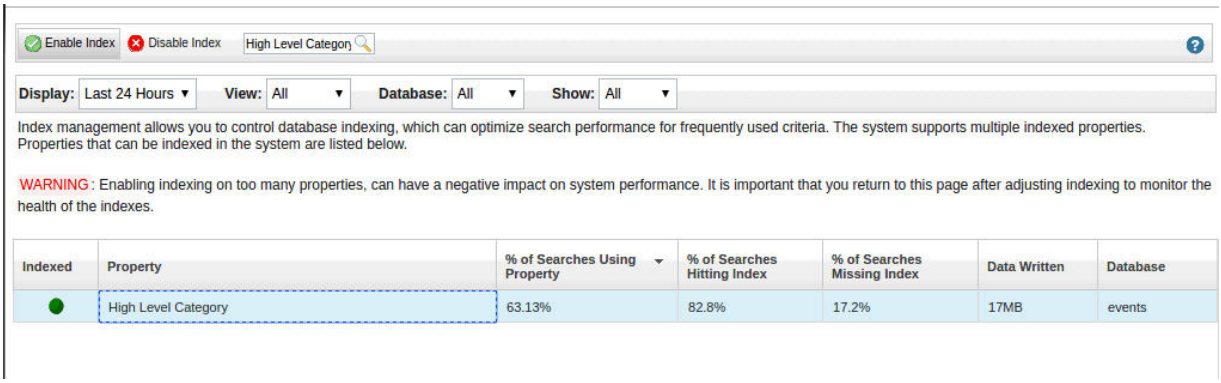
Para melhorar a velocidade de procuras no IBM QRadar e no aplicativo UBA, limite os dados gerais incluindo os campos indexados a seguir em sua consulta de procura:

- Categoria de Alto Nível
- Categoria de Baixo Nível
- senseValue
- senseOverallScore
- Nome de usuário

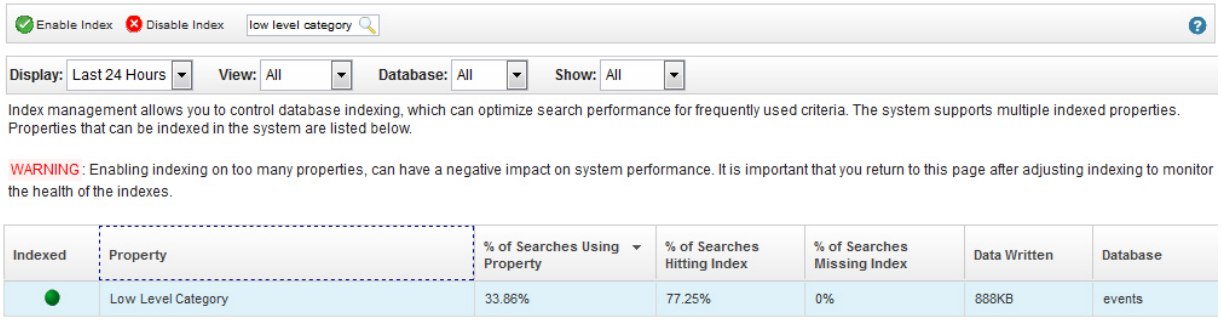
Para obter mais informações sobre a indexação, veja a seção a seguir do IBM Knowledge Center em https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_index_mgmt.html.

Procedimento

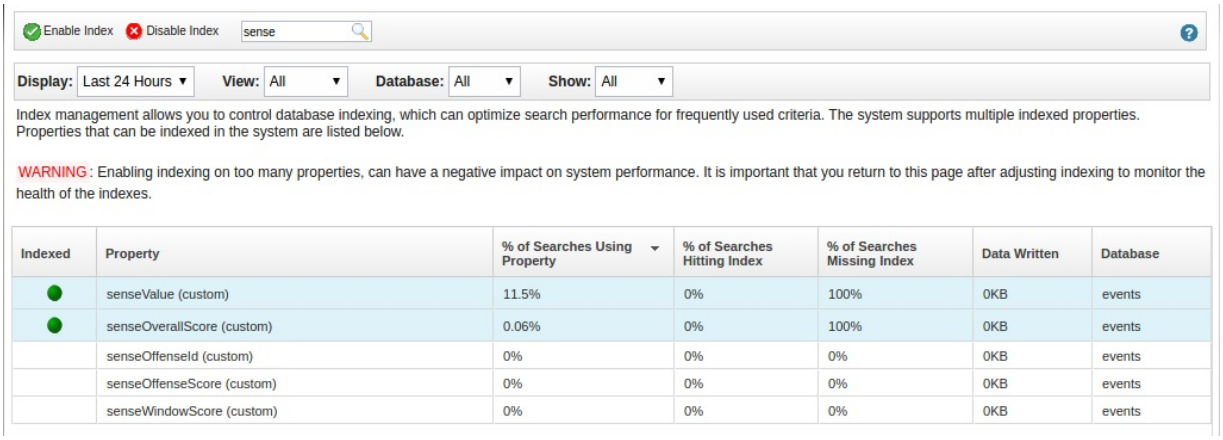
1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Na seção Configuração do sistema, clique no ícone **Gerenciamento de índice**.
3. Na página Gerenciamento de índice, na caixa de procura, insira `Categoria de alto nível`.
4. Selecione **Categoria de alto nível** e, em seguida, clique em **Ativar índice**.



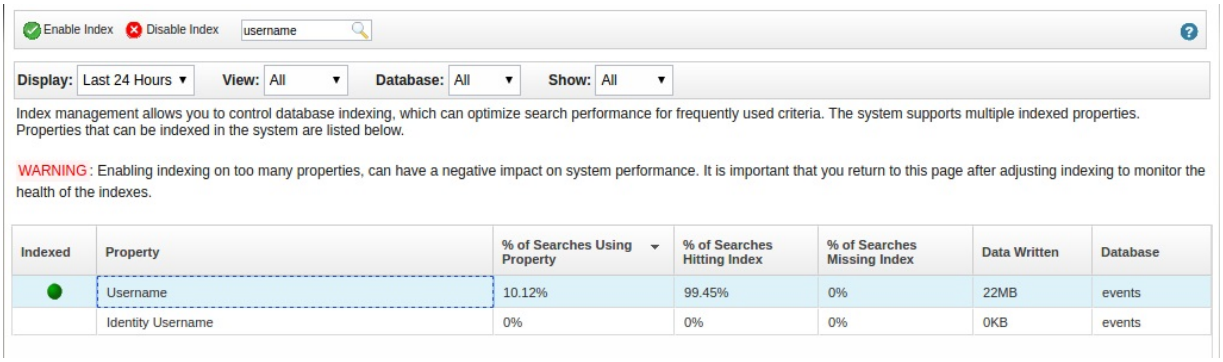
5. Clique em **Salvar**.
6. Selecione **Categoria de baixo nível** e, em seguida, clique em **Ativar índice**.



7. Clique em **Salvar**.
8. Na página Gerenciamento de índice, na caixa de procura, insira `sense`.
9. Selecione **senseValue** e **senseOverallScore** e, em seguida, clique em **Ativar índice**.



10. Clique em **Salvar**.
11. Na página Gerenciamento de índice, na caixa de procura, insira `username`.
12. Selecione **Nome do usuário** e, em seguida, clique em **Ativar índice**.



13. Clique em **Salvar**.

Integrando o conteúdo do QRadar novo ou existente com o aplicativo UBA

Use o Assistente de regras no QRadar para integrar as regras customizadas ou existentes do QRadar com o aplicativo UBA.

Sobre Esta Tarefa

Para atender suas necessidades específicas, é possível usar os recursos construídos no QRadar integrando as regras existentes do QRadar com o aplicativo UBA.

Restrição: Não customize suas regras para usar o UBA e conjuntos de referência de Aprendizado por Máquina. A tentativa de usar conjuntos de referência em regras customizadas pode levar a falhas no aplicativo UBA.

Procedimento

1. Crie uma cópia da regra existente. Isso evita que as atualizações para a regra base afetem as edições feitas na nova regra.
2. Abra a regra no Assistente de regras e, em seguida, navegue para a seção Resposta de regra.
3. Ative ou edite a opção **Despachar novo evento** certificando-se de que o texto de **Descrição do evento** seja formatado da maneira a seguir: `senseValue=#,senseDesc='sometext',usecase_id='rule UUID'`
4. Configure a **Categoria de alto nível** para **Verificação**.
5. Clique em **Concluir** para salvar as alterações.

   Nota: Se a regra funciona em dados de fluxo, deve-se ativar a opção **Procurar ativos para nome do usuário, quando o nome do usuário não está disponível para dados de evento ou de fluxo** para que eventos sem nomes de usuários possam tentar uma consulta para mapeamento de usuário.

Conjuntos de referência

O aplicativo do User Behavior Analytics e o aplicativo do Machine Learning usam conjuntos de referência para armazenar informações do usuário. Alguns conjuntos de referência são reservados para uso do aplicativo apenas e não é necessário modificá-los ou usá-los na criação de regras customizadas.

Conjuntos de referência que você pode customizar

Conjunto de referência	Descrição
UBA: Usuários de Alto Risco	O conjunto de referência *UBA : High Risk Users* é construído por meio do valor **Limite de risco para acionar ofensas** na página Configurações do UBA. O número máximo de usuários é 10.000 e o conjunto de referência é reconstruído a cada 5 minutos
UBA : Trusted Usernames	É possível incluir nomes de usuários no conjunto de referência *UBA : Trusted Usernames*, mas não usar para regras ou relatórios. Nenhuma ofensas é gerada para os usuários no conjunto de referência *UBA : Trusted Usernames*.
UBA: ML Watchlist Sempre Rastreado	O conjunto de referência *UBA : ML Always Tracked Watchlist* é construído por meio dos usuários que você seleciona para **Controlar com o Machine Learning** na seção **Configurações avançadas** na página Detalhes do usuário. É possível incluir nomes de usuários no conjunto de referência *UBA : ML Always Tracked Watchlist*, mas não usar para regras ou relatórios.

Conjuntos de referência que você não pode customizar

Restrição: Não modifique ou use os conjuntos de referência a seguir para criação de regra customizada.

- UBA-Usuários Rastreados por ML Atuais
- UBA-Usuários Rastreados ML Anteriores
- UBA - usuários rastreados por ML abreviados atuais
- UBA - usuários rastreados por ML abreviados prévios
- UBA - usuários rastreados por ML do peer atual
- UBA - usuários rastreados por ML do grupo de peers prévio

7 Regras e ajuste para o aplicativo UBA

O aplicativo IBM QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

O aplicativo User Behavior Analytics (UBA) inclui casos de uso que são baseados em regras customizadas. Essas regras são usadas para gerar dados para o painel de aplicativos UBA. Iniciando com a V3.0.0 do aplicativo UBA, é possível visualizar, filtrar e ajustar regras dentro do aplicativo UBA. Na V2.8.0 ou anterior, é possível visualizar e modificar as regras no Grupo do User Behavior Analytics na Lista de Regras no QRadar.

Nota:

- Por padrão, nem todas as regras do aplicativo UBA são ativadas.
- Uma ou mais das origens de log devem fornecer informações para a regra específica do UBA. As origens de log não são priorizadas em nenhuma ordem específica.

Restrição: Não customize suas regras para usar o UBA e conjuntos de referência de Aprendizado por Máquina. A tentativa de usar conjuntos de referência em regras customizadas pode levar a falhas no aplicativo UBA. Para obter informações adicionais, consulte "Conjuntos de referência" na página 43.

Para obter mais informações sobre como trabalhar com regras no QRadar, veja https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html

Regras e Página Ajuste

O aplicativo UBA V3.0.0 introduz a página Regras e Ajuste (**Configurações administrativas** > **Analíticas de usuário** > **Regras e Ajuste**).

A página Regras e Ajuste inclui uma lista de todas as regras que estão incluídas com o da versão do aplicativo UBA. Junto com o status atual ativado e os conjuntos de referência correspondentes.

Na página Regras e Ajuste, é possível:

- Ativar ou desativar regras
- Acessar rapidamente o Assistente de Regras do QRadar para revisar ou editar regras
- Acessar rapidamente os conjuntos de referência para revisar ou editar o conteúdo
- Filtrar a tabela de regras por categoria, status, pontuação de risco padrão, conjuntos de referência requeridos e dependências de conteúdo
- Classificar a tabela de regras por nome de regra, conjunto de referência ou status
- Procurar itens na tabela ou palavras que estão localizadas na dica de ferramenta de descrição da regra
- Acessar a documentação da ajuda para regras individuais

Acesso e autenticação

UBA: Novas Tentativas de Autenticação Bruteforce

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: Novas Tentativas de Autenticação Bruteforce

Ativado por Padrão

True

senseValue padrão

5

Descrição

Detecta força bruta na falha de autenticação (horizontal e vertical).

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Falhas de Autenticação
- BB:UBA: detectando tentativas de Bruteforce de autenticação (horizontal)
- BB:UBA: detectando tentativas de Bruteforce de autenticação (vertical)

Origens de dados

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT,Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform,Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch,Nortel Contivity VPN Switch (obsolete),

Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager,Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure,RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security,Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: ativo somente executivo acessado por usuário não executivo

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: ativo somente executivo acessado por usuário não executivo

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta quando um usuário não executivo efetua logon em um ativo que é somente para uso executivo. Dois conjuntos de referência vazios serão importados com esta regra: "UBA: Usuários executivos" e "UBA: Ativos executivos". Edite os conjuntos de referência para incluir ou remover quaisquer contas e endereços IP que são sinalizados em seu ambiente. Ative esta regra depois de configurar os conjuntos de referência.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
- BB:CategoryDefinition: Aceitação de Firewall ou ACL

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: "UBA: usuários executivos" e "UBA: ativos executivos".

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE

System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Acesso de usuário de alto risco para o ativo crítico

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Acesso de usuário de alto risco para o ativo crítico

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta quando um usuário envolvido em incidentes (ofensas) acessa o ativo crítico.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação

Configuração necessária

Inclua os valores apropriados no seguinte conjunto de referência: "Ativos Críticos".

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA,

Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: múltiplas contas VPN com falha de login de IP único

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: múltiplas contas VPN com falha de login de IP único

Ativado por Padrão

True

senseValue padrão

5

Descrição

Detecta qualquer falha de login da conta do VPN do conjunto de referência "UBA: múltiplas contas do VPN falharam ao efetuar login de um IP único".

Regras de suporte

- UBA: preencher múltiplas contas do VPN que falharam ao efetuar login de IP único
- BB:UBA: falha de login de VPN

Configuração necessária

Ative a regra a seguir: "UBA: preencher várias contas VPN com falha de login a partir de IP único"

Origens de dados

Cisco Adaptive Security Appliance (ASA)

UBA: múltiplas contas VPN com login efetuado de IP único

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: múltiplas contas VPN com login efetuado de IP único

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Mapeia múltiplos usuários do VPN provenientes do mesmo endereço IP e depois aumenta a pontuação de risco. Quando a regra detecta os usuários do VPN provenientes do mesmo endereço IP, o endereço IP é incluído no "UBA: múltiplas contas do VPN com login efetuado de IP único". Antes de ativar essa regra, certifique-se de que a regra "UBA: preencher múltiplas contas do VPN com login efetuado de IP único" esteja ativada e que o conjunto de referência "UBA: múltiplas contas do VPN com login efetuado de IP único" tenha dados.

Regras de suporte

- UBA: preencher várias contas VPN conectadas a partir de um único IP
- BB:UBA: Login VPN com Êxito

Configuração necessária

Ative a regra a seguir: "UBA: preencher várias contas VPN conectadas a partir de um único IP"

Origens de dados

Cisco Adaptive Security Appliance (ASA)

UBA: repetir acesso não autorizado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: repetir acesso não autorizado

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica que atividades repetir acesso não autorizado foram localizadas.

Regra de suporte

UBA: acesso não autorizado

Configuração necessária

Ative a regra a seguir: "UBA: acesso não autorizado"

Origens de dados

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus,Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform,Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

UBA: acesso não autorizado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: acesso não autorizado

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica que atividades de acesso não autorizado foram localizadas.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:UBA: Acesso Negado
- BB:UBA: Negações de Aplicativo

Origens de dados

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus,Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication

Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform,Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

UBA: sistema Unix/Linux acessado com conta de serviço ou máquina

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: sistema Unix/Linux acessado com conta de serviço ou máquina

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta qualquer sessão interativa (por meio da GUI e da CLI, tanto login local como remoto) que é iniciada por uma conta de serviço ou de máquina nos servidores UNIX e Linux. Contas e sessões interativas permitidas são listadas no UBA: Conta de serviço e de máquina e o UBA: conjuntos de referência da sessão de interação permitida. Edite o conjunto de referência para incluir ou remover qualquer sessão interativa que você deseja sinalizar em seu ambiente.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Aceitação de Firewall ou ACL
- BB:CategoryDefinition: Sucesso de Autenticação

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: "UBA: serviço, conta de máquina" e "UBA: sessão interativa permitida".

Origens de dados

S.O. Linux

UBA: acesso de usuário - Falha de acesso a ativos críticos

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: acesso de usuário - Falha de acesso a ativos críticos

Ativado por Padrão

True

senseValue padrão

5

Descrição

Esta regra detecta falhas de autenticação para sistemas localizados no conjunto de referência Ativos críticos.

Regras de Suporte

- BB:UBA : Filtros de Evento Comum
- BB:CategoryDefinition: Falhas de Autenticação

Configuração Necessária

Inclua os valores apropriados no seguinte conjunto de referência: "Ativos Críticos".

Origens de dados

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT,Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform,Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch,Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel

Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager,Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure,RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security,Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso de usuário - primeiro acesso a ativos críticos

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Suporta:

- UBA: acesso de usuário, primeiro acesso a ativos críticos
- UBA: atualização vista de usuários de sistemas críticos

Ativado por Padrão

True

senseValue padrão

10

Descrição

UBA: acesso de usuário, primeiro acesso a ativos críticos: Indica que essa é a primeira vez que o usuário acessou um ativo crítico. A coleção de referências "Usuários de sistemas críticos vistos" governa o tempo de vida de uma observação. Por padrão, essa regra detecta o primeiro acesso em três meses.

UBA: atualização de sistemas críticos vistos por usuários: atualiza o último valor visto na coleção de referência "Sistemas críticos vistos por usuários" para correspondências de IP de destino/nome do usuário que já existem.

Regras de suporte

- BB:CategoryDefinition: Sucessos na Autenticação
- BB:UBA : Filtros de Evento Comum

Configuração Necessária

Inclua os valores apropriados no seguinte conjunto de referência: "Ativos Críticos".

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass

Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso do usuário a partir de múltiplos hosts

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: UBA: Acesso do usuário a partir de múltiplos hosts

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta quando um único usuário efetua login por meio de mais de um número permitido de dispositivos.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman

Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso de usuário ao servidor interno por meio do servidor de salto

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: acesso de usuário ao servidor interno por meio do servidor de salto

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta quando um usuário usa um servidor de salto para acessar a VPN ou os servidores internos.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: "UBA: servidores Jump" e "UBA: servidores internos".

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: anomalia de login de acesso de usuário

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: anomalia de login de acesso de usuário

Ativado por Padrão

True

senseValue padrão

5

Descrição

Indica uma sequência de falhas de login em um ativo local. A regra também pode indicar um compromisso de conta ou atividade de movimento lateral. Assegure-se de que a regra Múltiplas falhas de login para um único nome de usuário esteja ativada. Ajuste os parâmetros de correspondência e de duração de tempo para essa regra para ajustar a responsividade.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- Falhas de Login Múltiplas para Nome de Usuário Único

Configuração necessária

Ative a regra a seguir: "Múltiplas falhas de login para nome do usuário único"

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando conta de origem anônima

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando conta de origem anônima

Ativado por Padrão

True

senseValue padrão

15

Descrição

Indica que um usuário está acessando recursos internos de uma origem anônima como TOR ou VPN.

Regras de Suporte

- BB:CategoryDefinition: Sucessos na Autenticação
- BB:UBA : Filtros de Evento Comum

Configuração Necessária

Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase

ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: tempo do usuário, acesso em horários incomuns

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: tempo do usuário, acesso em horários incomuns

Ativado por Padrão

True

senseValue padrão

5

Descrição

Indica que os usuários estão se autenticando com sucesso em horários que são incomuns para sua rede, conforme definido por "UBA: horários incomuns, %" de blocos de construção.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
- BB:UBA: Horários Incomuns, Evening
- BB:UBA: Horários Incomuns, Overnight

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2,

IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso à VPN por conta de máquina ou de serviço

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: acesso à VPN por conta de máquina ou de serviço

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta quando um Cisco VPN é acessado por uma conta de serviço ou de máquina. As contas são listadas no conjunto de referência 'UBA: conta de serviço, máquina'. Edite a lista para incluir ou remover quaisquer contas para sinalizar de seu ambiente.

Regra de suporte

BB:UBA : Mapeamento de VPN (lógica)

Configuração Necessária

Inclua os valores apropriados nos seguintes conjuntos de referência: "UBA: Serviço e Conta de Máquina".

Origens de dados

Cisco Adaptive Security Appliance (ASA)

UBA: compartilhamento de certificado do VPN

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: compartilhamento de certificado do VPN

Ativado por Padrão

True

Nota: Se você planeja usar a regra do UBA: compartilhamento de certificado VPN, deve-se atualizar o Cisco DSM Firewall para o seguinte:

- Para a V7.2.8: `DSM-CiscoFirewallDevices-7.2-20170619124928.noarch.rpm`
- Para a V7.3.0 e mais recente: `DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm`

senseValue padrão

15

Descrição

Essa regra detecta quando o nome do usuário do evento de uma VPN não é igual a 'VPNSubjectcn'. Isso poderá indicar que há um compartilhamento de certificado do VPN ocorrendo. O compartilhamento do certificado ou de outro token de autenticação pode dificultar a identificação de quem fez o quê. Isso poderá complicar a tomada das próximas etapas no caso de um compromisso.

Regras de suporte

- BB:UBA: Mapeamento de VPN (lógica)
- UBA: Subject_CN e atualização de mapa de nome do usuário
- UBA: Subject_CN e mapeamento de nome do usuário

Essas regras atualizam os conjuntos de referência associados com os dados necessários.

Configuração necessária

Ative as regras a seguir:

- UBA: Subject_CN e atualização de mapa de nome do usuário
- UBA: Subject_CN e mapeamento de nome do usuário

Origens de dados

Cisco Adaptive Security Appliance (ASA)

UBA: Windows Access com conta de serviço ou máquina

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: Windows Access com conta de serviço ou máquina

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta qualquer sessão interativa (RDP, login local) que é iniciada por uma conta de serviço ou de máquina no Windows Server. As contas são listadas no conjunto de referências UBA: serviço, conta de máquina. Edite a lista para incluir ou remover quaisquer contas para sinalização de seu ambiente.

Regras de suporte

BB:UBA : Filtros de Evento Comum

Configuração Necessária

Inclua os valores apropriados nos seguintes conjuntos de referência: "UBA: Serviço e Conta de Máquina".

Origens de dados

Microsoft Windows Security Event Log (EventID: 4776)

Contas e Privilégios

UBA: conta ou grupo ou privilégios incluídos

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: conta ou grupo ou privilégios incluídos (anteriormente chamado de UBA: conta, grupo ou privilégios incluídos ou modificados)

Ativado por Padrão

True

senseValue padrão

5

Descrição

Detecta eventos que um usuário executa e que se ajustam a uma das categorias a seguir. A regra despacha um evento do IBM Sense para incrementar a pontuação de risco do usuário originador.

- Authentication.Group Added

- Authentication.Group Changed
- Authentication.Group Member Added
- Authentication.Computer Account Added
- Authentication.Computer Account Changed
- Authentication.Policy Added
- Authentication.Policy Change
- Authentication.Trusted Domain Added
- Authentication.User Account Added
- Authentication.User Account Changed
- Authentication.User Right Assigned

Nota: Para ajustar o impacto dessa regra nas pontuações de risco geral dos usuários, considere modificar a regra de bloco de construção "CategoryDefinition: usuário ou grupo de autenticação incluído ou mudado" incluindo categorias de eventos de interesse para sua organização.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:UBA: usuário, grupo ou política de autenticação incluído

Origens de dados

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System,Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400,Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X,McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA

Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss,genua genugate, iT-CUBE agileSI

UBA: conta, grupo ou privilégios modificados

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: conta, grupo ou privilégios modificados (anteriormente chamado de UBA: mudança de conta do usuário)

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica quando uma conta do usuário foi afetada por uma ação que muda os privilégios efetivos do usuário, para cima ou para baixo.

Nota de falso positivo: Esse evento pode atribuir incorretamente as modificações em um nome da conta ao usuário que está fazendo mudanças. Se desejar reduzir essa possibilidade de positivo falso, será possível incluir o teste 'e quando o Username for igual a AccountName'.

Nota de falso negativo: Esse evento pode não detectar todos os casos de modificações de conta para um usuário.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:UBA: usuário, grupo ou política de autenticação mudado

Origens de dados

Microsoft Windows Security Event Log (EventID: 626, 642, 644, 1300, 1317, 625, 629, 4672, 4722, 4725, 4738, 4765, 4767, 4781, 4737, 4755)

UBA: ataque DoS por exclusão de conta

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: ataque DoS por exclusão de conta

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta o ataque DoS verificando o número de eventos de exclusão de conta em um limite fixo na amplitude de tempo fixa.

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA: Conta do Usuário Excluída

Origens de dados

Amazon AWS CloudTrail (EventID: DeleteUser)

Application Security DbProtect (EventID: Login revogado - Windows, Login descartado - padrão, Função do banco de dados - descartada, Usuário do banco de dados revogado)

Aruba Mobility Controller (EventID: authmgr_user_del)

Box (EventID: DELETE_USER)

Brocade FabricOS (EventID: SEC-1181, SEC-3028)

CA ACF2 (EventID: ACF2-L)

Check Point (EventID: user_deleted, device_deleted, User Deleted)

Cilasoft QJRN/400 (EventID: C20020)

Cisco Adaptive Security Appliance (ASA) (EventID: %PIX|ASA-5-502102, %ASA-5-502102)

Cisco FireSIGHT Management Center (EventID: USER_REMOVED_CHANGE_EVENT)

Cisco Firewall Services Module (FWSM) (EventID: 502102)

Cisco Identity Services Engine (EventID: 86008, 86028)

Cisco NAC Appliance (EventID: CCA-1453, CCA-1502)

Cisco Nexus (EventID: SECURITYD-6-DELETE_STALE_USER_ACCOUNT)

Cisco Wireless LAN Controllers (EventID: 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo (EventID: Usuário Halo excluído, Conta local excluída (apenas linux))

CorreLog Agent for IBM zOS (EventID: RACF DELUSER: Sem Violações)

Mecanismo de regra customizada (EventID: 3035, 3043)

Cyber-Ark Vault (EventID: 276)

EMC VMWare (EventID: AccountRemovedEvent)

Extreme Dragon Network IPS (EventID: HOST:LINUX:USER-DELETED, HOST:WIN:ACCOUNT-DELETED)

Extreme Matrix K/N/S Series Switch (EventID: Evento excluído pelo usuário, foi excluído)

Extreme NAC (EventID: Usuário registrado excluído)

Extreme NetsightASM (EventID: UserRemove)

Flow Classification Engine (EventID: 3035, 3043)

Forcepoint Sidewinder (EventID: exclusão do passaporte, todos os passaportes revogados)

HBGary Active Defense (EventID: DeleteUser)

HP Network Automation (EventID: Usuário Excluído)

Huawei S Series Switch (EventID: SSH/6/DELUSER_SUCCESS)

Auditoria do IBM AIX (EventID: USER_Remove SUCCEEDED)

IBM AIX Server (EventID: USER_Remove)

IBM DB2 (EventID: DROP_USER SUCCESS)

IBM DataPower (EventID: 0x81000136)

IBM IMS (EventID: USER DELETED)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: Delete User)

IBM QRadar Packet Capture (EventID: UserDeleted)

IBM Resource Access Control Facility (RACF) (EventID: 80 17.2, DELUSER_SUCCESS, 80 17.0)

IBM Security Access Manager for Enterprise Single Sign-On (EventID: REVOKE_IMS_ID, DELETE_IMS_ID)

IBM Security Directory Server (EventID: Auditoria do SDS)

IBM Security Identity Governance (EventID: 50, 43, 70005)

IBM Security Identity Manager (EventID: Delete SUCCESS, Delete SUBMITTED, Delete Success)

IBM SmartCloud Orchestrator (EventID: usuário)

IBM Tivoli Access Manager for e-business (EventID: 13408 - Bem-sucedido, 13408 Comando Bem-sucedido)

IBM i (EventID: GSL2502, M250100, DO_USRPRF, GSL2602, GSL2601, M260100, MC@0400, GSL2501)

IBM z/OS (EventID: 80 1.35)

Juniper Networks Network and Security Manager (EventID: adm24473)

S.O. Linux (EventID: userDel, Conta Excluída, DEL_USER)

McAfee Application/Change Control (EventID: USER_ACCOUNT_DELETED)

McAfee ePolicy Orchestrator (EventID: 20793)

Microsoft ISA (EventID: usuário removido)

Microsoft Office 365 (EventID: Delete User-PartiallySucceded, Delete user-success, Delete Usuário-sucesso, Excluir usuário-PartiallySucceded)

Microsoft SQL Server (EventID: 24129, DR - US, DR - SL, DR - LX, DR - AR,DR - SU, 24076, 24123, 38)

Microsoft Windows Security Event Log (EventID: 4743, 630, 1327, 647, 4726)

Netskope Active (EventID: Excluir Administrador, Administrador Excluído)

Nortel Application Switch (EventID: Excluído pelo Usuário)

Novell eDirectory (EventID: DELETE_ACCOUNT)

Qidmap de Serviços do S.O. (EventID: Conta Excluída, Usuário Excluído)

OSSEC (EventID: 18112)

Okta (EventID: core.user_group_member.user_remove, app.generic.import.details.delete_user)

Oracle Enterprise Manager (EventID: Exclusão do Computador (bem-sucedida), Exclusão de Usuário (bem-sucedida))

Registro de Auditoria RDBMS do Oracle (EventID: DROP USER-Padrão:1, 53:1, 53:0, DROP USER-Padrão:0, 53)

PGP Universal Server (EventID: ADMIN_DELETED_USER)

Palo Alto Endpoint Security Manager (EventID: Excluído pelo Usuário)

Pulse Secure Pulse Connect Secure (EventID: SYN24849, ADM20722, ADM24473, SYN24745, SYN24850)

RSA Authentication Manager (EventID: desconhecido, Usuário excluído, REMOVE_ORPHANED_PRINCIPALS, REMOTE_PRINCIPAL_DELETE, DELETE_PRINCIPAL)

SIM Audit (EventID: Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT (EventID: DirectorycomputerObject DeletedTrueFalse ativo, DirectoryuserObject DeletedTrueFalse ativo, Excluído pelo usuário/grupo do console, Excluído pelo usuário/grupo do console)

SafeNet DataSecure/KeySecure (EventID: Usuário removido)

Skyhigh Networks Cloud Security Platform (EventID: 10017)

Solaris BSM (EventID: excluir usuário)

SonicWALL SonicOS (EventID: 559, 1157, 1158)

Trend Micro Deep Security (EventID: 651)

DSM Universal (EventID: Conta do Computador Removida, Conta do Usuário Removida)

VMware vCloud Director (EventID: com/vmware/vcloud/event/user/remove, com/vmware/vcloud/event/user/delete)

Vormetric Data Security (EventID: DAO0090I)

iT-CUBE agileSI (EventID: AU8, U0)

UBA : A conta do usuário foi criada e excluída em um curto período de tempo

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : A conta do usuário foi criada e excluída em um curto período de tempo

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta quando uma conta do usuário é criada e excluída em um período de tempo curto.

Regras de suporte

- BB:UBA: Conta do Usuário Criada
- BB:UBA: Conta do Usuário Excluída
- BB:UBA: Filtros de Eventos Comuns

Origens de dados

UBA: conta inativa usada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: conta inativa usada

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta o login bem-sucedido a partir de uma conta que foi determinada para estar inativa.

Regra de suporte

- BB:UBA : Filtros de Evento Comum
- BB:CategoryDefinition: Falhas de Autenticação

Origens de dados

Qualquer origem de log suportada que forneça um nome do usuário no evento.

UBA: tentativa de uso de conta inativa

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: tentativa de uso de conta inativa

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta o log com falha em tentativa a partir de uma conta que foi determinada como estando inativa.

Regra de suporte

- BB:UBA : Filtros de Evento Comum
- BB:CategoryDefinition: Falhas de Autenticação

Origens de dados

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway,Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Identity Platform, Centrify Infrastructure Services, Check Point,Cilasoft QJRN/400, Cisco ACS,Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center,Cisco Firewall Services Module (FWSM),Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS,CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,Event CRE Injected,Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Matrix K/N/S Series Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine,

Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem,Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM Bluemix Platform, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta,OpenBSD OS, Open LDAP Software, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Palo Alto PA Series, Pirean Access: One, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Sybase ASE,Symantec Encryption Management Server, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: Conta Expirada Usada

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: Conta Expirada Usada. (anteriormente chamado de UBA: conta órfã, revogada ou suspensa usada)

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica que um usuário tentou efetuar login em uma conta desativada ou expirada em um sistema local. Essa regra também pode sugerir que uma conta foi comprometida.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: autenticação para a conta expirada

Origens de dados

Cisco CatOS for Catalyst Switches, Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Juniper Junos WebApp Secure, Microsoft IAS Server, Microsoft Windows Security Event Log

UBA: primeira escalada de privilégio

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: primeira escalada de privilégio

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica que um usuário executou acesso privilegiado pela primeira vez. Essa regra de relatório pode ser desativada para permitir o rastreamento de comportamentos do usuário para propósitos de determinação de linha de base.

Regra de suporte

BB:UBA: usuário privilegiado, uso de privilégio do usuário pela primeira vez (lógica)

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM

Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: uso de nova conta detectado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: uso de nova conta detectado

Ativado por Padrão

True

senseValue padrão

5

Descrição

Fornece funções de relatório que indicam que um usuário efetuou login com sucesso pela primeira vez. Essa regra de relatório pode ser desativada temporariamente para propósitos de determinação de linha de base.

Regra de suporte

BB:UBA: primeiro acesso do usuário (lógica)

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X

Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: atividade privilegiada suspeita (primeiro uso de privilégio observado)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: atividade privilegiada suspeita (primeiro uso de privilégio observado)

Ativado por Padrão

True

senseValue padrão

5

Descrição

Indica que um usuário executou uma ação privilegiada que nunca executou antes. As observações são mantidas em mapas de conjuntos "UBA: atividades observadas por categoria de nível baixo e nome do usuário".

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA : Atividade Privilegiada

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud

Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: atividade privilegiada suspeita (privilégio raramente usado)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: atividade privilegiada suspeita (privilégio raramente usado)

Ativado por Padrão

True

senseValue padrão

10

Descrição

Indica que um usuário executou uma ação privilegiada que não havia executado recentemente. As observações são mantidas em mapas de conjuntos "UBA: atividades recentes por categoria de nível baixo e nome do usuário". A sensibilidade desse evento pode ser modificada mudando o TTL (tempo de vida) do Mapa de conjuntos de referência para "UBA: atividades recentes por categoria de nível baixo e nome do usuário". Aumentar o TTL reduz a sensibilidade. Diminuir o TTL aumenta a sensibilidade.

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA : Atividade Privilegiada

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: tentativa do usuário de usar uma conta suspensa

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: tentativa do usuário de usar uma conta suspensa

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta que um usuário tentou acessar uma conta suspensa ou desativada.

Regras de suporte

- BB:CategoryDefinition: Autenticação para Conta Desativada
- BB:UBA: Filtros de Eventos Comuns

Origens de dados

Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Microsoft ISA, Microsoft Windows Security Event Log

UBA: o usuário ficou inativo (regra do ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada. As informações da conta inativa podem ser visualizadas no UBA Painel a partir do V3.2.0. Para obter informações adicionais, consulte “Contas inativas” na página 39.

UBA: o usuário ficou inativo (nenhuma regra de anomalia de atividade)

UBA: conta inativa localizada (privilegiada)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Certifique-se de que "UBA: o usuário ficou inativo (nenhuma regra de anomalia de atividade)" esteja ativado para ativar essa regra.

Esta regra indica que a contagem de atividades de um nome de usuário mudou mais que 80%. "UBA: conta inativa do usuário localizada (privilegiada)" e "UBA: o usuário ficou inativo (nenhuma regra de anomalia de atividade)" são destinadas a mostrar quando um usuário parou de produzir atividade por

um período estendido. Esta condição pode indicar que o usuário não mais requer acesso, conforme indicado por uma longa ausência de atividade associada ao seu nome de usuário. Alarmes falsos serão possíveis se a atividade de um Nome de usuário cair para zero durante o período de intervalo curto (14 dias por padrão) e se antes de zero estiver a nova linha de base (28 dias por padrão). Eles não afetarão a pontuação de risco de um usuário se o limite de frequência de resposta para "UBA: conta inativa do usuário localizada (privilegiada)" for configurado para um período de tempo igual ou maior que o intervalo longo por nome de usuário.

Nota: Alarmes falsos serão possíveis para 'UBA: o usuário ficou inativo (nenhuma regra de anomalia de atividade)' se a atividade de um Nome de usuário diminuir para zero durante o período de intervalo curto (14 dias por padrão) e antes de zero ser a nova linha de base (28 dias por padrão). Os alarmes falsos não afetarão a pontuação de risco de um usuário se o limite de frequência de resposta para "UBA: conta inativa do usuário localizada (privilegiada)" for configurado para um período de tempo igual ou maior que o intervalo longo por Nome de usuário.

Regra de suporte

UBA: conta inativa localizada (privilegiada)

Configuração necessária

Ative a regra a seguir: "UBA: conta inativa localizada (privilegiado)".

Origens de dados

Todas as origens de log suportadas.

Comportamento de navegação

UBA: procurado para o website de negócios/serviço

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: procurado para o website de negócios/serviço

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar um risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA: Procura para o Website de Comunicações

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: Procura para o Website de Comunicações

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Entretenimento

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Entretenimento

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Apostas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Apostas

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Tecnologia da Informação

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Tecnologia da Informação

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Procura por Emprego

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Procura por Emprego

Ativado por Padrão

True

senseValue padrão

15

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA: procurado para o website LifeStyle

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: procurado para o website LifeStyle

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar um risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website Malicioso

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website Malicioso

Ativado por Padrão

True

senseValue padrão

15

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Conteúdo Misto/Potencialmente Adulto

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Conteúdo Misto/Potencialmente Adulto

Ativado por Padrão

True

senseValue padrão

10

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Phishing

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Phishing

Ativado por Padrão

True

senseValue padrão

15

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Pornografia

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Pornografia

Ativado por Padrão

True

senseValue padrão

10

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Procura para Website de Fraude/Questionável/Ilegal

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Procura para Website de Fraude/Questionável/Ilegal

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA: procurado para o website sem categoria

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: procurado para o website sem categoria

Ativado por Padrão

True

senseValue padrão

5

Descrição

Um usuário acessou uma URL que pode indicar um risco de segurança ou jurídico elevado.

Regra de suporte

BB:UBA : Filtro da Categoria da URL

Origens de dados

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA: usuário acessando URL arriscada

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando a URL de risco (anteriormente chamada de URL X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um usuário local está acessando o conteúdo on-line questionável.

Regras de suporte

- URL arriscada de X-Force
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ativar a regra a seguir: URL X-Force de risco.

Origens de dados

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

Controlador de

UBA: console do AWS acessado por usuário não autorizado

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: console do AWS acessado por usuário não autorizado

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta uma tentativa desautorizada de acessar o console do Amazon Web Services (AWS) por um usuário que está fora da lista autorizada no conjunto de referência 'AWS - Usuários padrão'.

Regras de suporte

BB:UBA : Filtros de Evento Comum

Configuração Necessária

- Instale o pacote a seguir a partir do IBM Security App Exchange: IBM QRadar Content Extension for Monitoring Amazon AWS.
- Inclua os valores apropriados no conjunto de referência a seguir: "UBA: Administradores do Controlador de Domínio". Configure a origem de log a seguir: Amazon AWS Cloudtrail

Origens de dados

Amazon AWS CloudTrail (ID de evento: ConsoleLogin)

UBA: usuário não padrão acessando recursos do AWS

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: usuário não padrão acessando recursos do AWS

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta um usuário não padrão que está tentando acessar recursos do Amazon Web Services (AWS).

Origem de dados

Extensão do Amazon Web Services

Controlador do domínio

UBA: tentativa de recuperação de chave mestra de backup DPAPI

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: tentativa de recuperação de chave mestra de backup DPAPI

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta quando a recuperação será tentada para uma Chave mestra DPAPI.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origem de Dados

Log de eventos de segurança do Microsoft Windows (ID de evento: 4693)

UBA: enumeração de conta do Kerberos detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: enumeração de conta do Kerberos detectada

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta a enumeração de conta do Kerberos, detectando alto número de nomes de usuários que estão sendo usados para fazer solicitações do Kerberos a partir do mesmo IP de origem.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origem de Dados

Microsoft Windows Security Event Log (EventID: 4768)

UBA: diversas falhas de autenticação Kerberos do mesmo usuário

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: diversas falhas de autenticação Kerberos do mesmo usuário

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta múltiplas rejeições ou falhas do chamado de autenticação do Kerberos.

Regra de suporte

- BB:UBA: Filtros de Origem de Log Comuns
- BB:UBA: falhas de autenticação do Kerberos

Origens de dados

Log de eventos de segurança do Microsoft Windows

UBA: acesso que não é de administrador ao controlador de domínio

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: acesso que não é de administrador ao controlador de domínio

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta tentativas de acesso a contas não administrativas para o controlador de domínio.

Regra de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
- BB:CategoryDefinition: Falhas de Autenticação

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: "UBA: controladores de domínio" e "UBA: administradores de controlador de domínio"

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks

ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: passar o hash

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: passar o hash

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta os eventos de logon do Windows que são possivelmente gerados durante explorações passar o hash.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Configuração necessária:

Inclua os valores apropriados no conjunto de referência a seguir: UBA: domínios confiáveis.

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4624)

UBA: possível enumeração de serviços de diretório

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: possível enumeração de serviços de diretório

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta tentativas de reconhecimento para a Enumeração de Serviço de Diretório.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Configuração Necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: Administradores do Controlador de Domínio"

Origem de dados

Log de eventos de segurança do Microsoft Windows (ID de evento: 4661)

UBA: possível enumeração de sessão SMB em um controlador de domínio

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: possível enumeração de sessão SMB em um controlador de domínio

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta tentativas na enumeração de SMB com relação a um controlador de domínio.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Configuração Necessária

Inclua os valores apropriados nos conjuntos de referência a seguir:

- UBA: Controladores de Domínio
- UBA: Administradores do Controlador de Domínio

Origem de dados

Log de eventos de segurança do Microsoft Windows (ID de evento: 5140)

UBA: possível falsificação de TGT

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: possível falsificação de TGT

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta TGTs do Kerberos que contêm anomalias de Nome de domínio. Eles possivelmente indicam chamados que são geradas usando explorações passar o chamado.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: UBA: domínios confiáveis.

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4768)

UBA: possível falsificação de TGT PAC

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: possível falsificação de TGT PAC

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta o uso de um certificado PAC falsificado para obter um ticket de serviço do Kerberos TGS.

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA: Falsificação de TCT PAC do Servidor Corrigida
- BB:UBA: Falsificação de TCT PAC do Servidor Não Corrigida

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: Administradores do Controlador de Domínio".

Origem de dados

Log de eventos de segurança do Microsoft Windows (ID de evento: 4672, 4769)

UBA: solicitação de replicação de um controlador não de domínio

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: solicitação de replicação de um controlador não de domínio

Ativado por Padrão

True

senseValue padrão

5

Descrição

Detecta solicitações de replicação de um Controlador de Domínio ilegítimo

Regras de suporte

BB:UBA : Filtros de Evento Comum

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: Administradores do Controlador de Domínio".

Origem de dados

Log de eventos de segurança do Microsoft Windows (ID de evento: 4662)

UBA: chamado TGT usado por diversos hosts

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: chamado TGT usado por diversos hosts

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta que o chamado do Kerberos TGT está sendo usado em dois (ou mais) computadores diferentes.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

UBA: Mapeamento de Conta do Kerberos

Essa regra atualiza os conjuntos de referência associados com os dados necessários.

Configuração necessária

Ative as regras a seguir: "UBA: mapeamento de conta do Kerberos

Origens de dados

Microsoft Windows Security Event Log (EventID: 4768)

Nó de extremidade

UBA: detecção de protocolo não seguro ou não padrão

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: detecção de protocolo não seguro ou não padrão

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta qualquer usuário que esteja se comunicando com protocolos não autorizados que são considerados protocolos inseguros ou não padrão. Protocolos autorizados são listados no UBA: conjunto de referência de portas de protocolos autorizados com valor padrão 0, que é a porta de eventos do QRadar. Edite o UBA: conjunto de referência de portas de protocolos autorizados para sinalizar de seu ambiente antes de ativar esta regra.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:UBA: Portas Inseguras
-

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: UBA: portas de protocolos autorizados.

Origens de dados

Todas as origens de log suportadas.

UBA: detectar sessão SSH persistente

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: detectar sessão SSH persistente

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta sessões SSH que estão ativas por mais de 10 horas.

Regras de suporte

- BB:UBA : Filtros de Eventos Comuns
- BB:UBA: Sessão SSH fechada
- BB:UBA: Sessão SSH Aberta

Configuração Necessária

Esta regra requer que os eventos SSH Aberto e SSH Fechado ocorram para uma detecção precisa. Se a origem de log que é usada não tiver um eventID para ambos os eventos, você poderá receber resultados imprecisos. Consulte as Origens de dados para determinar os eventIDs para a origem de log em uso.

Origens de dados (SSH aberto)

Centrificar serviços de infraestrutura (EventID: 27100, 27104)

Cisco IOS (EventID: %SSH-5-SSH2_SESSION, %SSH-SW2-5-SSH2_SESSION)

Mecanismo de regra customizada (EventID: 18037, 3071)

Cyber-Ark Vault (EventID: 378)

Roteadores de segurança do Extreme XSR (EventID: NEW_SSH_CONNECTION)

Flow Classification Engine (EventID: 3071, 18037)

Huawei S Series Switch (EventID: SSH/4/SFTP_REQ_RECORD)

HyTrust CloudControl (EventID: AUN0120, desconhecido)

IBM AIX Server (EventID: conexão sshd2 estabelecida, conexão ssh-server, sessão ssh-server abrir)

IBM DataPower (EventID: 0x8100011e, 0x810001e4, 0x810001e5)

Juniper MX Series Ethernet Services Router (EventID: SSH)

Juniper Networks AVT (EventID: SSH)

Mac OS X (EventID: sessão ssh do OSX iniciada)

Qidmap de serviços do S.O. (EventID: conexão a partir de, pam_open_session, pam_sm_open_session)

Mensagens de autenticação do sistema operacional Solaris (EventID: sessão ssh aberta)

DSM Universal (EventID: SSH aberto, sessão SSH iniciada)

Origens de dados (SSH fechado)

Aruba Mobility Controller (EventID: sshd_disconnect)

Centrificar serviços de infraestrutura (EventID: 27102)

Cisco IOS (EventID: %SSH-5-SSH_CLOSE, %SSH-SW2-5-SSH2_CLOSE, %SSH-5-SSH2_CLOSE)

Mecanismo de regra customizada (EventID: 3072, 18038, 18040)

Cyber-Ark Vault (EventID: 380, 381)

Flow Classification Engine (EventID: 3072, 18038, 18040)

Huawei S Series Switch (EventID: SSH/6/RECV_DISCONNECT)

IBM AIX Server (EventID: desconexão do servidor ssh, conexão sshd2 perdida, desconexão de SSH, desconexão local do sshd2, encerramento de sessão do servidor ssh)

Qidmap de serviços do S.O. (EventID: concluído com conexão, pam_sm_close_session, pam_close_session, não recebeu sequência de identificação, tempo de conexão esgotado, desconexão recebida do IP, conexão fechada)

Pulse Secure Pulse Connect Secure (EventID: GWE24572)

DSM Universal (EventID: SSH finalizado, sessão SSH concluída, SSH fechado)

UBA: configurações da Internet modificadas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: configurações da Internet modificadas

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta modificações de configurações da Internet no sistema.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4657)

UBA: atividade de malware - registro modificado em massa

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: atividade de malware - registro modificado em massa

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta processos que modificam múltiplos valores de registro em massa em um intervalo mais curto.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4657)

UBA: detecção de processo Netcat (Linux)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: detecção de processo Netcat (Linux)

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta o processo netcat em um sistema Linux.

Regra de suporte

BB:UBA: Filtros de Origem de Log Comuns

Origens de dados

Linux OS (EventID: SYSCALL)

UBA: detecção de processo Netcat (Windows)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: detecção de processo Netcat (Windows)

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta o processo Netcat em um sistema Windows.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4688)

UBA: processo executado fora da lista de desbloqueio de disco Gold (Linux)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: processo executado fora da lista de desbloqueio de disco Gold (Linux)

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta processos que são criados em um sistema Linux e alerta quando o processo está fora da lista de desbloqueio de processo de disco gold.

Nota: A regra está desativada por padrão. Ative a regra somente depois de preencher ou modificar os nomes de processo para que sejam incluídos na lista de desbloqueio no conjunto de referência 'UBA: lista de desbloqueio de processo de disco gold - Linux'.

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: lista de desbloqueio de processo de disco Gold - Linux".

Regra de suporte

BB:UBA: Filtros de Origem de Log Comuns

Origens de dados

Linux OS (EventID: SYSCALL)

UBA: processo executado fora da lista de desbloqueio de disco Gold (Windows)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: processo executado fora da lista de desbloqueio de disco Gold (Windows)

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta processos que são criados em um sistema Windows e alerta quando o processo está fora da lista de desbloqueio de processo de disco gold.

Nota: A regra está desativada por padrão. Ative a regra somente depois de preencher ou modificar os nomes de processo para que sejam incluídos na lista de desbloqueio no conjunto de referência 'UBA: lista de desbloqueio de processo de disco gold - Windows'.

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: lista de desbloqueio de processos de disco Gold - Windows".

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4688)

UBA: comportamento Ransomware detectado

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: comportamento Ransomware detectado

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta o comportamento que geralmente é visto durante uma infecção de ransomware.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: processos comuns do Windows".

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4663)

UBA: uso de programa restrito

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: uso de programa restrito

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Indica que um processo foi criado e seu nome corresponde a um dos nomes binários listados no conjunto de referência "UBA: nomes de arquivos de programa restrito". Esse conjunto de referência está em branco por padrão para que seja possível customizá-lo. É possível preencher o conjunto de referência com nomes de arquivos que você deseja monitorar para gerenciamento de risco.

Para obter mais informações sobre como incluir ou remover programas para monitoramento, veja Gerenciando programas restritos.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: nomes de arquivos de programa restritos".

Origens de dados

Log de eventos de segurança do Microsoft Windows

UBA: usuário instalando aplicativo suspeito

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

Suporta as regras a seguir:

- UBA: usuário instalando aplicativo suspeito
- UBA: preencher aplicativos autorizados

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta eventos de instalação do aplicativo e, em seguida, alerta quando aplicativos suspeitos são vistos. Observação: preencha o conjunto de referência "UBA: Aplicativos Autorizados" com os nomes de aplicativos que estão autorizados na organização. Regra "UBA: Preencher Aplicativos Autorizados" pode ser ativada para uma curta duração para preencher esse conjunto de referência.

Regra "UBA: Preencher Aplicativos Autorizados" preenche o conjunto de referência "UBA: Aplicativos Autorizados" com os nomes dos aplicativos que são instalados enquanto essa regra está ativada. Nota: a regra está desativada por padrão. Ative uma duração mais curta para preencher os nomes enquanto os usuários estão instalando aplicativos.

Origens de dados

Microsoft Windows Security Event Logs

UBA: usuário executando novo processo

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

Suporta as regras a seguir:

- UBA: usuário executando novo processo
- UBA: Preencher nomes de arquivos de processos

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta processos que são criados pelo usuário e, em seguida, alerta quando um usuário executa um novo processo.

Regra "UBA: Preencher nomes de arquivos do processo" preenche o conjunto de referência "UBA : Nomes de arquivos do processo" usado como uma regra de utilitário para "UBA: usuário executando novo processo." Nota: a regra está desativada por padrão. Ative a regra para uma duração mais curta para preencher os nomes de arquivos.

Regra de suporte

BB:UBA: filtros de evento comum, UBA: preencher nomes de arquivo de processo

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: "UBA: nomes de arquivos de processo".

Origens de dados

Microsoft Windows System Event Logs (EventID:4688)

UBA: cópia de sombra de volume criada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: cópia de sombra de volume criada

Ativado por Padrão

True

senseValue padrão

15

Descrição

Detecta cópias de sombra que foram criadas usando vssadmin.exe ou o Windows Management Instrumentation Command-line (WMIC).

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

Microsoft Windows Security Event Logs (EventID: 1 ou 4688)

Exfiltração

UBA: volume de dados anormais para o domínio externo (regra do ADE)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

Nota: Esta regra foi substituída pela Analítica de aprendizado de máquina a seguir: volume anormal de dados para domínios externos.

- UBA: volume de dados anormais para o domínio externo
- UBA: volume anormal de dados para domínio externo localizado

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

UBA: volume de dados anormais para o domínio externo Essa regra usa o mecanismo de detecção de anomalias para monitorar o uso de tráfego do usuário e alertar sobre volumes de dados anormais de tráfego para domínios externos.

UBA: volume de dados anormais para o domínio externo localizado Essa é uma regra do CRE que suporta a respectiva regra do ADE idêntica: UBA: volume de dados anormais para o domínio externo, que usa o mecanismo de detecção de anomalias para monitorar o uso de tráfego do usuário e alertar sobre volumes de dados anormais de tráfego para domínios externos.

Origens de dados

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

UBA: tentativas de transferência de saída anormal (regra ADE)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

Nota: Esta regra foi substituída pela Analítica de aprendizado de máquina a seguir: tentativas de transferência de saída anormal. Para obter informações adicionais, consulte "Configurando a analítica *Abnormal Outbound Transfer Attempts*" na página 178.

UBA: tentativas de transferência de saída anormal (UBA chamado: tentativas de saída anormal na V2.4.0)

UBA: tentativas de transferência de saída anormal localizadas

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

UBA: tentativas de transferência de saída anormal (regra ADE) Essa regra usa o mecanismo de detecção de anomalias para monitorar o uso de tráfego de saída e para alertar sobre o número anormal de tentativas.

UBA: tentativas de transferência de saída anormal localizadas Essa é uma regra do CRE que suporta a respectiva regra do ADE idêntica: UBA: tentativas de saída anormal, que usa o mecanismo de detecção de anomalias para monitorar o uso de tráfego de saída e alertar sobre o número anormal de tentativas.

Origens de dados

Todas as origens de logs suportadas.

UBA : Transferência grande de saída por usuário de alto risco

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Transferência grande de saída por usuário de alto risco

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta uma transferência de saída de 200.000 bytes ou mais por um usuário de alto risco.

Regras de suporte

BB:UBA: Filtros de Eventos Comuns

Origens de dados

Origens de log que têm o CEP BytesSent definido.

UBA: várias transferências de arquivos bloqueadas seguidas por uma transferência de arquivo

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: várias transferências de arquivos bloqueadas seguidas por uma transferência de arquivo

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta a exfiltração verificando uploads de arquivos que foram inicialmente bloqueados, mas foram seguidos por um upload bem-sucedido dentro de um período de 5 minutos.

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA: Transferência de Arquivos Bloqueada
- BB:UBA: Transferência de Arquivos Bem-sucedida

Configuração necessária

Esta regra requer que ambos os eventos, de Transferências de arquivo bloqueadas e de Transferências de arquivo bem-sucedidas, ocorram para uma detecção precisa. Se a origem de log que é usada não tiver um eventID para ambos os eventos, você poderá receber resultados imprecisos. Consulte as Origens de dados para determinar os eventIDs para a origem de log em uso.

Origens de dados (Transferências de arquivos bloqueadas)

Cilasoft QJRN/400 (EventID: C21020)

Cisco Call Manager (EventID: %UC_DRF-3-DRFSftpFailure)

Cisco IOS (EventID: %UPDATE-3-SFTP_TRANSFER_FAIL)

Mecanismo de regra customizada (EventID: 18014, 18071, 18187, 4032)

Comutadores Extreme Empilháveis e Independentes (EventID: Solicitação de FFTP com Falha)

Flow Classification Engine (EventID: 4032, 18187, 18014, 18071)

Forcepoint Sidewinder (EventID: Permissões de FTP, comando ftp negado)

IBM i (EventID: UNR0907, UNR0908, UNR2302, GSL0118, GSL0119, GSL0318, GSL0319, GSL3718, GSL3719, GSL0618,UNR0701, UNR0707, UNR0901, UNR0910, UNR2301, UNR0705, UNR0706, UNR0708, UNR0710, UNR0801, UNR0802, UNR0905, UNR0906, GSL0619)

Juniper Networks Intrusion Detection and Prevention (IDP) (EventID: TFTP:AUDIT:READ-FAILED)

Microsoft IIS (EventID: 530)

Microsoft Operations Manager (EventID: 22095)

OSSEC (EventID: 11504, 11512)

DSM Universal (EventID: Ação de FTP Negada, Sessão de TFTP Negada, FTP Negado, Transferência de Arquivos Negada)

WatchGuard Fireware OS (EventID: 1CFF0002, 1CFF0006, 1CFF0007, 1CFF0009, 1CFF0001, 1CFF0019, 1CFF0000, 1CFF0003)

Origens de dados (Transferências de arquivos bem-sucedidas)

Cilasoft QJRN/400 (EventID: C21031)

Cisco FireSIGHT Management Center (EventID: FILE_EVENT, FILE_EVENT_0)

Cisco IOS (EventID: %FTPSERVER-6-NEWCONN)

Cisco IronPort (EventID: FTP_connection)

Mecanismo de regra customizada (EventID: 18010, 4031, 18431, 18183)

DG Technology MEAS (EventID: 119-003, 119-070)

Flow Classification Engine (EventID: 18010, 4031,18431, 18183)

Tipo de Dispositivo de Fluxo (EventID: 21984, 21879, 51337, 51336, 35159, 21910)

Huawei S Series Switch (EventID: FTPS/5/REQUEST)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: FTP, TFTP)

IBM i (EventID: MLD1200, MLD2100, MO10300, MO10400, MO11800, MO12100, MO12400, MO20200, MO20300. MO21300, MO21800, MO21900, GSL0101, GSL0102, GSL0301, GSL0302, GSL3701,GSL3702, M090100, UNA0705, UNA0706, UNA0708, UNA0710, UNA0801, UNA0802, UNA0905, UNA0906, UNA0907,UNA0908, UNA2302,UNA0601, UNA0604, UNA0605, UNA0607, UNA0701, UNA0707, UNA0901, UNA0902, UNA0910, UNA2301, M030100, MLD1100)

Juniper MX Series Ethernet Services Router (EventID: TFTP, FTP)

Juniper Networks AVT (EventID: TFTP, FTP)

Microsoft IIS (EventID: 150, 125, 225)

ProFTPD Server (EventID: sessão FTP aberta)

Mensagens de Autenticação do Sistema Operacional Solaris (EventID: conexão de ftp)

SonicWALL SonicOS (EventID: 1112, 1113)

Proxy da Web Squid (EventID: 3C0002_ALLOWED)

Trend InterScan VirusWall (EventID: Trend ftpconnect)

DSM Universal (EventID: Transferência de Arquivos, FTP Aberto, Ação de FTP Permitida, Sessão de TFTP Aberta)

Verdasys Digital Guardian (EventID: Upload de Transferência de Rede, Download de Transferência de Rede)

WatchGuard Fireware OS (EventID: 2AFF0004, 1CFF0019)

UBA: acesso suspeito seguido pela exfiltração de dados

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: acesso suspeito seguido pela exfiltração de dados

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta acesso a partir de locais incomuns, restritos ou proibidos, seguido por uma tentativa de exfiltração de dados.

Regra de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA: Exfiltração de Dados
- UBA: acesso de usuário de local restrito
- UBA: acesso de usuário de local proibido
- UBA: geografia do usuário, acesso de locais incomuns

Configuração Necessária

Ative as regras a seguir:

- UBA: acesso de usuário de local restrito
- UBA: acesso de usuário de local proibido
- UBA: geografia do usuário, acesso de locais incomuns

Origem de Dados

Cisco Stealthwatch (ID de evento: 45)

IBM Security Trusteer Apex Advanced Malware Protection (ID de evento: ConnectionCreate.Connection_Test, CerberusNG.ent_create_remote_thread, ConnectionCreate.in_suspend_state, ConnectionCreate.orphant_thread_connect, close.file_inspection, processcreate.file_inspection)

Plataforma Skyhigh Networks Cloud Security (ID de evento: 10003, 10004)

UBA: anomalia de atividade de volume do usuário - tráfego para domínios externos (regra do ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada.

- UBA: anomalia de volume de atividade do usuário - tráfego para domínios externos
- UBA: anomalia de volume de atividade do usuário - tráfego para domínios externos localizados

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

UBA: anomalia de atividade do volume do usuário - tráfego para domínios externos Esta é uma regra CRE que suporta a regra ADE idêntica respectiva: UBA: anomalia de atividade do volume do usuário - tráfego que usa o mecanismo de Detecção de anomalias para monitorar o uso do tráfego do usuário e alertar sobre volumes incomuns de tráfego.

UBA: anomalia de atividade do volume do usuário - tráfego para domínios externos localizados Esta é uma regra CRE que suporta o UBA respectivo idêntico: anomalia de atividade do volume do usuário - Regra de tráfego para domínios externos, que usa o mecanismo de Detecção de anomalias para monitorar o uso do tráfego de saída e para alertar sobre o número anormal de tentativas.

Origens de dados

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

Geografia

UBA : Conta defeituosa criada a partir de um novo local

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Conta defeituosa criada a partir de um novo local

Ativado por Padrão

True

senseValue padrão

5

Descrição

Detecta atividade de criação de conta anômala de um novo local.

Regras de suporte

- BB:UBA: Terminais de Nuvem
- BB:UBA: Conta do Usuário Criada
- BB:UBA : Filtros de Eventos Comuns
- UBA: mudança de geografia do usuário

Configuração necessária

Ative a regra a seguir: "UBA: Mudança Geográfica do Usuário".

Origens de dados

APC do AhnLab Policy Center (EventID: Inclusão da Conta do Administrator: Bem-Sucedida, ADD_ADMIN_ACCOUNT_SUCCESS)

Application Security DbProtect (EventID: Usuário do banco de dados criado, Login criado - padrão, Login incluído - Windows, Função do banco de dados - criado)

Aruba Mobility Controller (EventID: authmgr_user_add)

Bit9 Security Platform (EventID: User_group_created, User_group_modified, User_group_deleted, Console_user_created, Console_user_modified, Console_user_deleted)

Box (EventID: NEW_USER)

Brocade FabricOS (EventID: SEC-1180, SEC-3025, SEC-1182)

CA ACF2 (EventID: ACF2-L)

Check Point (EventID: Usuário Incluído, device_added)

Cilasoft QJRN/400 (EventID: C20010, C20011)

Cisco Adaptive Security Appliance (ASA) (EventID: %PIX|ASA-5-502101, %ASA-5-502101)

Cisco Firewall Services Module (FWSM) (EventID: 502101, 504001)

Cisco IOS (EventID: %APF-6-USER_NAME_CREATED)

Cisco Identity Services Engine (EventID: 86006)

Cisco NAC Appliance (EventID: CCA-1500)

Cisco PIX Firewall (EventID: %PIX-0-502101, %PIX-1-502101, %PIX-2-502101, %PIX-3-502101, %PIX-4-502101, %PIX-5-502101, %PIX-6-502101, %PIX-7-502101)

Cisco PIX Firewall (EventID: 502101)

Cisco Wireless LAN Controllers (EventID: %APF-6-USER_NAME_CREATED, 1.3.6.1.4.1.9.9.515.0.2)

Cisco Wireless Services Module (WiSM) (EventID: %AAA-6-GUEST_ACCOUNT_CREATE, %APF-6-USER_NAME_CREATED)

CloudPassage Halo (EventID: Usuário Halo incluído, Usuário Halo incluído novamente, Conta local criada (apenas Linux))

CorreLog Agent for IBM zOS (EventID: RACF ADDUSER: Sem Violações)

Cyber-Ark Vault (EventID: 180, 2)

EMC VMWare (EventID: AccountCreatedEvent)

Extreme Dragon Network IPS (EventID: HOST:WIN:ACCOUNT-CREATED)

Extreme Matrix K/N/S Series Switch (EventID: criado com, Evento Criado pelo Usuário)

Extreme NAC (EventID: Usuário registrado incluído, Incluir Usuário Registrado)

Flow Classification Engine (EventID: 3031, 3041)

Forcepoint Sidewinder (EventID: adição de passaporte)

Fortinet FortiGate Security Gateway (EventID: incluir, auth-logon)

Foundry Fastiron (EventID: SNMP_USER_ADDED)

HBGary Active Defense (EventID: CreateUser)

HP Network Automation (EventID: Usuário Incluído)

Auditoria do IBM AIX (EventID: USER_Create SUCCEEDED)

IBM AIX Server (EventID: USER_Create)

IBM DB2 (EventID: ADD_USER SUCCESS)

IBM IMS (EventID: USER CREATED)

IBM QRadar Packet Capture (EventID: UserAdded)

IBM Resource Access Control Facility (RACF) (EventID: 80 10.0, 80 10.2)

IBM Security Access Manager for Enterprise Single Sign-On (EventID: PRE_PROVISION_IMS_USER, AA_SCR_REGISTRATION, REGISTER_MAC_IDENTITY, REGISTER_IDENTITY)

IBM Security Directory Server (EventID: Auditoria do SDS)

IBM Security Identity Governance (EventID: 49, 70004, 42)

IBM Security Identity Manager (EventID: Inclusão Bem-Sucedida, Inclusão ENVIADA, Inclusão BEM-SUCEDIDA)

IBM SmartCloud Orchestrator (EventID: usuário)

IBM Tivoli Access Manager for e-business (EventID: 13402 - Bem-Sucedido, 13401 - Bem-Sucedido, 13402 Comando Bem-Sucedido, 13401 Comando Bem-Sucedido)

IBM i (EventID: GSL2401, MC@0300, GSL2402, M240100, CP_CRT)

Imperva SecureSphere (EventID: NEW_USERS_ACCOUNT, SOX_NEW_USERS, SOX - Novos usuários, Conta de Novos Usuários)

Itron Smart Meter (EventID: CEUI-AUDIT-27, CEUI.AUDIT.26)

Juniper Networks Network and Security Manager (EventID: adm23303, aut20167, adm30407, aut20168, adm20716, adm20717)

S.O. Linux (EventID: ADD_USER)

McAfee Application/Change Control (EventID: USER_ACCOUNT_CREATED)

McAfee ePolicy Orchestrator (EventID: 20792)

Microsoft ISA (EventID: usuário incluído)

Microsoft SQL Server (EventID: CR - SU, CR - US, CR - SL, CR - LX, CR - AR, CR - WU, 24127, 24121, 24075)

Microsoft SharePoint (EventID: 37)

Log de Eventos de Segurança do Microsoft Windows (EventID: 624, 645, 1318, 4720, 4741)

NCC Group DDos Secure (EventID: 1003)

Netskope Active (EventID: Criar Administrador, Criado novo administrador)

Novell eDirectory (EventID: CREATE_ACCOUNT)

Qidmap de Serviços do S.O. (EventID: Conta do Usuário Incluída)

OSSEC (EventID: 5902, 18110)

Okta (EventID: app.user_management.push_new_user_success, app.generic.import.details.add_user, app.generic.import.new_user, app.user_management.provision_user, app.user_management.push_new_user, app.user_management.push_profile_success, core.user.config.user_creation.success, core.user_group_member.user_add, cvd.user_profile_bootstrapped, cvd.appuser_profile_bootstrapped)

OpenBSD OS (EventID: incluir usuário)

Oracle Enterprise Manager (EventID: Criação de Usuário (bem-sucedida), Criação do Computador (bem-sucedida))

Registro de Auditoria RDBMS do Oracle (EventID: 51:1, 51:0, CRIAR USUÁRIO-Padrão:1, CRIAR USUÁRIO-Padrão:0)

Registro de Auditoria do S.O. do Oracle RDBMS (EventID: 51)

Pirean Access: Um (EventID: IsimUserRegistration;*;1)

Pulse Secure Pulse Connect Secure (EventID: ADM23303, ADM20265, AUT20167, ADM30407, AUT20168)

RSA Authentication Manager (EventID: Usuário incluído, desconhecido, REMOTE_PRINCIPAL_CREATE, CREATE_PRINCIPAL, CREATE_AM_PRINCIPAL)

Auditoria do SIM (EventID: Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT (EventID: DirectorycomputerObject AddedTrueFalse ativo, Console? usuário/grupo incluído, Console ⌂ usuário/grupo incluído, DirectoryuserObject AddedTrueFalse ativo, Console - usuário/grupo incluído)

SafeNet DataSecure/KeySecure (EventID: Usuário Incluído)

Salesforce Security Auditing (EventID: Novo Usuário do Cliente Criado, Novo Usuário Criado)

Skyhigh Networks Cloud Security Platform (EventID: 10016)

Solaris BSM (EventID: criar usuário)

SonicWALL SonicOS (EventID: 558)

Symantec Encryption Management Server (EventID: ADMIN_IMPORTED_USER)

ThreatGRID Malware Threat Intelligence Platform (EventID: user-account-creation)

Trend Micro Deep Discovery Email Inspector (EventID: SYSTEM_EVENT_ACCOUNT_CREATED)

Trend Micro Deep Security (EventID: 650)

DSM Universal (EventID: Conta do Computador Incluída, Conta do Usuário Incluída)

VMware vCloud Director (EventID: com/vmware/vcloud/event/user/create, com/vmware/vcloud/event/user/import)

Vormetric Data Security (EventID: DAO0089I)

iT-CUBE agileSI (EventID: U0, AU7)

UBA : Conta em nuvem defeituosa criada a partir de um novo local

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Conta em nuvem defeituosa criada a partir de um novo local

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta atividades de criação de conta de nuvem por meio de um novo local.

Regras de suporte

- BB:UBA : Filtros de Evento Comum
- BB:UBA: Terminais de Nuvem
- BB:UBA: Conta do Usuário Criada
- UBA: mudança de geografia do usuário

Configuração Necessária

Ative a regra a seguir: "UBA: Mudança Geográfica do Usuário".

Origens de dados

Amazon AWS CloudTrail (ID de evento: CreateUser)

Microsoft Office 365 (ID de evento: Add User-success, Add user-PartiallySucceded)

UBA: acesso de usuário de diversos locais

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: acesso de usuário de diversos locais

Ativado por Padrão

True

senseValue padrão

5

Descrição

Indica que múltiplos locais ou origens estão usando a mesma conta do usuário simultaneamente. Ajuste os parâmetros de correspondência e duração para ajustar a responsividade.

Regra de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC

Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso de usuário de local proibido

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: acesso de usuário de local proibido

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta acesso de usuário de um local não no "UBA: lista de locais permitidos."

Regras de suporte:

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
-

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: UBA: lista de localização permitida

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel

Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: acesso de usuário de local restrito

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: acesso de usuário de local restrito

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta acesso de usuário de um local no "UBA: lista de locais restritos." É possível incluir países do "local geográfico" no "UBA: lista de locais restritos."

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
-

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: UBA: lista de localização restrita

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point,

Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: mudança de geografia do usuário

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: mudança de geografia do usuário

Ativado por Padrão

True

senseValue padrão

5

Descrição

Uma correspondência indica que um usuário efetuou login remotamente de um país que é diferente do país do último login remoto do usuário. Essa regra também pode indicar um comprometimento da conta, particularmente se as correspondências da regra ocorreram em um tempo aproximado.

Regras de suporte

- BB:UBA: Filtros de Eventos Comuns
- BB:CategoryDefinition: Sucesso de Autenticação
- UBA: mapa de geografia do usuário

Configuração necessária

Ative a regra a seguir: UBA: mapa geográfico do usuário

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman

Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Regra de suporte

Mapa de geografia do usuário

Essa regra atualiza os conjuntos de referência associados com os dados necessários.

UBA: geografia do usuário, acesso de locais incomuns

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: geografia do usuário, acesso de locais incomuns

Ativado por Padrão

True

senseValue padrão

15

Descrição

Indica que os usuários foram capazes de se autenticar em países que são incomuns para sua rede, conforme definido pela regra de bloco de construção "UBA: BB: locais de origem incomuns".

Regras de suporte

- BB:UBA: Locais de Origem Incomuns
- BB:CategoryDefinition: Sucesso de Autenticação
- BB:UBA: Filtros de Eventos Comuns

Origens de dados

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam e Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Tráfego e ataques de rede

UBA: ataque D/DoS detectado

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: ataque D/DoS detectado

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta ataques de Negação de Serviço (DoS) da rede por um usuário.

Nota: Antes de poder usar essa regra, conclua as etapas a seguir:

1. Na guia **Administrador**, clique em **Configurações do UBA**.
2. Marque a caixa de seleção **Procurar ativos para o nome do usuário, quando o nome do usuário não está disponível para dados de evento ou de fluxo** para procurar nomes de usuários na tabela de ativos. O aplicativo UBA usa ativos para consultar um usuário para um endereço IP quando nenhum usuário está listado em um evento.
3. A regra de evento precisa da Origem de log "IDS do software livre Snort" para funcionar.

Regras de suporte

- BB:UBA: Filtros de Origem de Log Comuns
- BB:CategoryDefinition: Eventos de Ataque DDoS
- BB:CategoryDefinition: Ataque de DoS de Rede
- BB:CategoryDefinition: DoS de Serviço

Origens de dados

Akamai KONA, Application Security DbProtect, Aruba Mobility Controller, Barracuda Web Application Firewall, Brocade FabricOS, CRE System, Check Point, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Intrusion Prevention System (IPS), Cisco PIX Firewall, Cisco Stealthwatch, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Custom Rule Engine, CyberGuard TSP Firewall/VPN, Enterprise-IT-Security.com SF-Sherlock, Event CRE Injected, Extreme Dragon Network IPS, Extreme HiPath, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Fair Warning, FireEye, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, Huawei AR Series Router, IBM Proventia Network Intrusion Prevention System (IPS), IBM Security Network IPS (GX), Imperva Incapsula, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Motorola SymbolAP, NCC Group DDos Secure, Niksun 2005 v3.5, Nortel Application Switch, OS Services Qidmap, OSSEC, Palo Alto PA Series, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, SonicWALL SonicOS, Squid Web Proxy, Stonesoft Management Center, Symantec Endpoint

Protection, TippingPoint Intrusion Prevention System (IPS), Top Layer IPS, Trend Micro Deep Security, Universal DSM, Vectra Networks Vectra, Venustech Venusense Security Platform, WatchGuard Fireware OS

UBA: Atividade Honeytoken

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: Atividade Honeytoken

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividade usando uma conta Honeytoken.

Regras de suporte

BB:UBA : Filtros de Eventos Comuns

Configuração necessária

Inclua os valores apropriados nos conjuntos de referência a seguir: UBA: contas Honeytoken.

Inclua as origens de log apropriadas nos grupos de origens de log a seguir: UBA: sistemas com contas Honeytoken.

Origens de dados

Todas as origens de log incluídas no UBA: sistemas com o grupo de origem de log de Contas Honeytoken.

UBA: tráfego de rede: uso do programa de captura, monitoramento e análise

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: tráfego de rede: uso do programa de captura, monitoramento e análise

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Indica que um processo é criado e o nome do processo corresponde a um dos nomes binários que são listados no conjunto de referência "UBA: nomes de arquivos do programa de captura, monitoramento e análise de rede". Esse conjunto de referência lista os nomes binários de software de captura de pacote de rede. O conjunto de referência é preenchido previamente com os nomes de alguns nomes de arquivos comuns do software de análise de protocolo de rede.

Para obter mais informações sobre como incluir ou remover programas para monitoramento, veja Gerenciando ferramentas de monitoramento de rede.

Regra de suporte

BB:UBA: Filtros de Eventos Comuns

Configuração necessária

Inclua os valores apropriados no conjunto de referência a seguir: UBA: captura de rede, monitoramento e análise de nomes de arquivos de programa.

Origens de dados

Log de eventos de segurança do Microsoft Windows

UBA: comportamento do usuário, anomalia de sessão por destino (regra ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada.

UBA: comportamento do usuário, anomalia de sessão por destino

UBA: comportamento do usuário, anomalia de sessão por destino localizada

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

UBA: comportamento do usuário, anomalia de sessão por destino Indica que um usuário está acessando endereços IP de destino significantemente diferentes daqueles que foram acessados pelo usuário no passado. O evento não é necessariamente uma indicação de comprometimento. A mudança no comportamento pode indicar uma mudança significativa nos hábitos de trabalho ou responsabilidades de tarefa do usuário.

UBA: comportamento do usuário, anomalia de sessão por destino localizada Essa é uma regra do CRE que suporta a respectiva regra do ADE idêntica: UBA: comportamento do usuário, anomalia de sessão

por destino, que indica que um usuário está acessando endereços IP de destino significativamente diferentes daqueles que foram acessados pelo usuário no passado. O evento não é necessariamente uma indicação de comprometimento. A mudança no comportamento pode indicar uma mudança significativa nos hábitos de trabalho ou responsabilidades de tarefa do usuário.

Origens de dados

Todas as origens de log suportadas.

UBA: categorias de anomalia de frequência de evento do usuário (regra ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Esta regra foi substituída pela Analítica de aprendizado de máquina a seguir: atividade por categoria. Para obter informações adicionais, consulte "Configurando a Analítica *Activity by Category*" na página 180.

UBA: categorias de anomalia de frequência de evento do usuário (regra ADE)

UBA: anomalia de frequência de evento do usuário - categorias localizadas

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

UBA: categorias de anomalia de frequência de evento do usuário Usa o mecanismo de detecção de anomalias para monitorar a distribuição de categoria de eventos de um usuário. Ele alerta sobre mudanças de frequência incomuns.

UBA: anomalia de frequência de evento do usuário - categorias localizadas Essa é uma regra do CRE que suporta a respectiva regra do ADE idêntica: UBA: anomalia de frequência de evento do usuário - categorias, que usa o mecanismo de detecção de anomalias para monitorar a distribuição de categoria de eventos de um usuário. Ela alertará sobre mudanças de frequência incomuns.

Origens de dados

Todas as origens de log suportadas.

UBA: anomalia de atividade de volume do usuário - tráfego para domínios internos (regra do ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada.

- UBA: anomalia de volume de atividade do usuário - tráfego para domínios internos

- UBA: anomalia de volume de atividade do usuário - tráfego para domínios internos localizados

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Esta é uma regra CRE que suporta a regra respectiva idêntica: UBA: anomalia do volume de atividade do usuário - tráfego para domínios internos que usam o mecanismo de Detecção de anomalias para monitorar o uso do tráfego do usuário e alertar sobre volumes incomuns de tráfego.

Origens de dados

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

Analisador QRadar DNS

Para obter mais informações, veja IBM QRadar DNS Analyzer.

UBA : Acesso Potencial para Domínio de Lista de Bloqueio

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Acesso Potencial para Domínio de Lista de Bloqueio

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta eventos que indicam que possivelmente o usuário acessou um domínio da lista de bloqueio. Requer o aplicativo IBM QRadar DNS Analyzer.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o aplicativo IBM QRadar DNS Analyzer. Para obter mais informações, veja IBM QRadar DNS Analyzer.

Origens de dados

IBM QRadar DNS Analyzer

UBA : Acesso Potencial para Domínio DGA

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Acesso Potencial para Domínio DGA

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta eventos que indicam que possivelmente o usuário acessou um domínio DGA (Domain Generated by Algorithm). Requer o aplicativo IBM QRadar DNS Analyzer.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o aplicativo IBM QRadar DNS Analyzer. Para obter mais informações, veja IBM QRadar DNS Analyzer.

Origens de dados

IBM QRadar DNS Analyzer

UBA : Acesso Potencial para Domínio Squatting

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Acesso Potencial para Domínio Squatting

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta eventos que indicam que possivelmente o usuário acessou um domínio Squatting. Requer o aplicativo IBM QRadar DNS Analyzer.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o aplicativo IBM QRadar DNS Analyzer. Para obter mais informações, veja IBM QRadar DNS Analyzer.

Origens de dados

IBM QRadar DNS Analyzer

UBA : Possível acesso ao domínio de tunelamento

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Possível acesso ao domínio de tunelamento

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta eventos que indicam que o usuário potencialmente acessou um domínio de tunelamento. Requer o aplicativo IBM DNS Analyzer.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o aplicativo IBM QRadar DNS Analyzer. Para obter mais informações, veja IBM QRadar DNS Analyzer.

Origens de dados

IBM QRadar DNS Analyzer

QRadar Network Insights (QNI)

Para obter mais informações sobre a instalação de regras QNI no QRadar V7.2.8, consulte QRadar Network Insights Content v7.2.8.

Para o QRadar V7.3.0 e mais recente, consulte QRadar Network Insights Content v7.3.0+.

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado expirado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado expirado

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

O QRadar Network Insights (QNI) detectou uma sessão SSL/TLS que usa um certificado expirado. Os servidores e clientes usam os certificados ao estabelecer a comunicação usando Secure Sockets Layer (SSL) ou Segurança da Camada de Transporte (TLS). Os certificados são emitidos com uma data de expiração que indica por quanto tempo o certificado permanece válido.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado inválido

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado inválido

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

O QRadar Network Insights (QNI) detectou uma sessão SSL/TLS que usa um certificado inválido. Os servidores e clientes usam certificados X.509 ao estabelecer a comunicação usando Secure Sockets Layer (SSL). Os certificados são emitidos com uma data Não anterior a, que indica a data mais antiga em que o certificado é válido.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Acesso ao serviço protegido incorretamente - Comprimento da chave pública fraco

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Acesso ao serviço protegido incorretamente - Comprimento da chave pública fraco

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

O QRadar Network Insights (QNI) detectou uma sessão SSL/TLS que usa um certificado com uma contagem de bits da chave pública baixa de menos de 2.048. Um servidor que fornece um Certificado de chave pública fraco (menos de 1.024 bits) pode representar um risco de segurança. De acordo com a publicação NIST 800-57, a chave RSA mínima recomendada a partir de 2011 é a de 2.048 bits.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado autoassinado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Acesso ao serviço protegido incorretamente - Certificado autoassinado

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

O QRadar Network Insights (QNI) detectou uma sessão SSL/TLS que usa um certificado autoassinado. Um certificado autoassinado em um aplicativo público ou de servidor de produção pode permitir que um invasor remoto inicie um ataque man-in-the-middle.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA : QNI - Há conteúdo confidencial sendo transferido para um local no exterior

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : QNI - Há conteúdo confidencial sendo transferido para um local no exterior

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Detecta o conteúdo confidencial que está sendo transferido para países e regiões com acesso restrito. Observe que esses países e regiões são definidos no bloco de construção a seguir: "Países/Regiões com acesso restrito". Antes de ativar essa regra, certifique-se de que o bloco de construção esteja configurado de acordo com seu caso de uso de negócios.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Hash de arquivo observado associado à ameaça de malware

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Hash de arquivo observado associado à ameaça de malware

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Esta regra é acionada quando o conteúdo do fluxo inclui um hash de arquivo que corresponde a hashes de arquivo inválido conhecidos incluídos em um feed de dados do Threat Intelligence. Indica que alguém transferiu malware na rede.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Hash de arquivo observado em vários hosts

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Hash de arquivo observado em vários hosts

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Esta regra é acionada quando o mesmo hash de arquivo associado a malware é visto sendo transferido para diversos destinos.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Tentativa de spam/phishing possível detectada no destinatário de e-mail rejeitado

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Tentativa de spam/phishing possível detectada no destinatário de e-mail rejeitado

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Esta regra é acionada quando eventos de e-mail rejeitados enviados para um endereço de destinatário inexistente são vistos no sistema. Isso pode indicar uma tentativa de spam ou de phishing. Configure o bloco de construção BB:CategoryDefinition: destinatário de e-mail rejeitado para incluir QIDs relevantes à sua organização. Ele é preenchido previamente com os QIDs a seguir que são bons para monitoramento: Microsoft Exchange; Linux OS [executando sendmail]; Logs Sendmail do Sistema Operacional Solaris e Barracuda Spam and Virus Firewall.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

UBA: QNI - Assunto de spam/phishing em potencial detectado de diversos servidores de envio

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: QNI - Assunto de spam/phishing em potencial detectado de diversos servidores de envio

Ativado por Padrão

Falso

senseValue padrão

5

Descrição

Esta regra é acionada quando diversos servidores de envio enviam o mesmo assunto de e-mail em um período de tempo que pode indicar spam ou phishing.

Configuração Necessária

Antes de ativar essa regra de QNI, é necessário instalar o pacote de conteúdo do QRadar Network Insights e ativar seus conteúdos de regra. Para o QRadar 7.2.8, consulte QRadar Network Insights Content v7.2.8. Para o QRadar 7.3.0 ou mais recente, consulte QRadar Network Insights Content v7.3.0+.

Origens de dados

QRadar Network Insights (QNI)

Reconhecimento

Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores DHCP Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores DHCP Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores DHCP.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores de Banco de Dados Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores de Banco de Dados Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores de banco de dados.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores DNS Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores DNS Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores DNS.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores FTP Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores FTP Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para o servidor FTP.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores de Jogos Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores de Jogos Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores de jogos.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de ICMP Genérico Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de ICMP Genérico Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede em servidores que utilizam o protocolo ICMP.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de TCP Genérico Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de TCP Genérico Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede em servidores usando portas TCP comuns.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de UDP Genérico Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de UDP Genérico Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede em servidores usando portas UDP comuns.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores IRC Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores IRC Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores IRC.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores LDAP Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores LDAP Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores LDAP.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores de Correio Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores de Correio Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores de correio.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores de Mensagens Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores de Mensagens Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para os servidores de mensagens.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores P2P Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores P2P Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores P2P.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores Proxy Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores Proxy Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores proxy.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores RPC Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores RPC Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores RPC.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores SNMP Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores SNMP Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores SNMP.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores SSH Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores SSH Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores SSH.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores da Web Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores da Web Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores da web.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

UBA : Varredura Incomum de Servidores Windows Detectada

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Varredura Incomum de Servidores Windows Detectada

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Detecta varredura incomum na rede para servidores Windows.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o IBM Security Reconnaissance Content Pack e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM Security Reconnaissance Content.

Monitoramento do sistema (sysmon)

Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

UBA : Ferramentas de Exploração Comuns Detectadas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Ferramentas de Exploração Comuns Detectadas

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta o uso de ferramentas de exploração comumente utilizadas, como keyloggers e PsExec.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Ferramentas de Exploração Comuns Detectadas (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Ferramentas de Exploração Comuns Detectadas

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta o uso de ferramentas de exploração comumente utilizadas, como keyloggers e PsExec.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA: processo malicioso detectado

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: processo malicioso detectado

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta processos que indicam o comportamento malicioso em hosts do Windows.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA: Acesso de Rede Acessado

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: Acesso de Rede Acessado

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades suspeitas que envolvem compartilhamentos de rede.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Regras do Sysmon

UBA : Processo Criando Encadeamentos Remotos Suspeitos Detectado (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Processo Criando Encadeamentos Remotos Suspeitos Detectado (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta processos que estão criando encadeamentos de forma suspeita em uma máquina remota.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades Suspeitas em Hosts Comprometidos

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades Suspeitas em Hosts Comprometidos

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades que são executadas em um host comprometido.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades Suspeitas em Hosts Comprometidos (Ativos)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades Suspeitas em Hosts Comprometidos (Ativos)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades que são executadas em um host comprometido.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades Administrativas Suspeitas Detectadas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades Administrativas Suspeitas Detectadas

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades administrativas raramente executadas que parecem suspeitas.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA: atividade suspeita de prompt de comandos

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: atividade suspeita de prompt de comandos

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades nos scripts do prompt de comandos.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Entradas Suspeitas no Registro do Sistema (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Entradas Suspeitas no Registro do Sistema (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades suspeitas que envolvem modificações ou atualizações do Windows Registry.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Carregamento de Imagem Suspeita Detectado (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Carregamento de Imagem Suspeita Detectado (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta imagens suspeitas que são transferidas por upload em locais sensíveis.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades do Canal Suspeitas (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades do Canal Suspeitas (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detectar atividades suspeitas que envolvam canais de processo em hosts Windows.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA: atividade suspeita de PowerShell

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: atividade suspeita de PowerShell

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detectar atividades nos scripts do Microsoft PowerShell.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA: atividade suspeita de PowerShell (ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA: atividade suspeita de PowerShell (ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades em scripts do Microsoft PowerShell. Essa regra requer que a funcionalidade "Procurar ativos para nome do usuário quando o nome do usuário não estiver disponível para dados de evento ou de fluxo" seja ativada.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades de Tarefa Planejada Suspeitas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades de Tarefa Planejada Suspeitas

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta a criação suspeita de tarefas planejadas em hosts Windows

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades de Serviço Suspeitas

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades de Serviço Suspeitas

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades de serviço suspeitas em computadores Windows.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Atividades de Serviço Suspeitas (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Atividades de Serviço Suspeitas (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades de serviço suspeitas em computadores Windows.

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

UBA : Bypass do User Access Control Detectado (Ativo)

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Bypass do User Access Control Detectado (Ativo)

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta atividades de processo que indicam bypass do User Access Control (UAC).

Configuração Necessária

Antes de ativar essa regra, é necessário instalar o pacote do IBM QRadar Content Extension for Sysmon e ativar seus conteúdos de regra. Para obter mais informações, consulte IBM QRadar Content Extension for Sysmon.

Origens de dados

Microsoft Windows Security Event Logs

Inteligência de ameaça

UBA: visitas anormais para recursos arriscados (regra do ADE)

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada.

- UBA: visitas anormais para recursos arriscados
- UBA: visitas anormais a recursos arriscados localizadas

Nota: A ativação de regras ADE pode afetar o desempenho do aplicativo UBA e seu sistema QRadar.

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

UBA: visitas anormais a recursos arriscados localizadas Essa regra usa o mecanismo de detecção de anomalias para monitorar o número de vezes que um usuário acessa um recurso arriscado (como URLs suspeitas, anonymizers e hosts de malware) e alerta quando o número de visitas muda de forma anormal.

UBA: visitas anormais a recursos arriscados localizadas Essa é uma regra do CRE que suporta a respectiva regra do ADE idêntica: UBA: visitas anormais a recursos arriscados, que usa o mecanismo de detecção de anomalias para monitorar o número de vezes que um usuário acessa recursos arriscados (como URLs suspeitas, anonymizers, hosts de malware) e alerta quando o número de visitas muda de forma anormal.

Origens de dados

Todas as origens de log suportadas.

UBA : Detectar IOCs para Locky

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Detectar IOCs para Locky

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta os computadores do usuário que mostram Indicators of Compromise (IOCs) para Locky usando URLs ou IPs que são preenchidos a partir de feeds de campanha do X-Force.

Regras de suporte

- BB:UBA: Filtros de Origem de Log Comuns
- BB:UBA: Detect Locky Utilizando IP
- BB:UBA: Detectar Locky Usando URL

Configuração necessária

- Inclua os valores apropriados nos conjuntos de referência a seguir: UBA: IP IOCs-Locky e UBA: URL IOCs-Locky.
- Ative a "Consulta de Usuário do Ativo" em **Configurações do Administrador** > **Configurações UBA**.

Origens de dados

Todas as origens de log suportadas.

UBA : Detectar IOCs para WannaCry

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : Detectar IOCs para WannaCry

Ativado por Padrão

Falso

senseValue padrão

10

Descrição

Detecta os computadores do usuário que mostram Indicators of Compromise (IOCs) para WannaCry usando URLs, IPs ou hashes que são preenchidos a partir de feeds de campanha do X-Force.

Regras de suporte

- BB:UBA: Filtros de Origem de Log Comuns
- BB:UBA: Detectar WannaCry Usando Hashes
- BB:UBA: Detectar WannaCry Usando IP
- BB:UBA: Detectar WannaCry usando URL

Configuração necessária:

- Inclua os valores apropriados nos conjuntos de referência a seguir: UBA: Malware Activity WannaCry - Hash, UBA: Malware Activity WannaCry - IP e UBA: Malware Activity WannaCry - URL.
- Ative a "Consulta de Usuário do Ativo" em **Configurações do Administrador** > **Configurações UBA**.

Origens de dados

Todas as origens de log suportadas.

UBA : ShellBags Modificados por Ransomware

O app QRadar User Behavior Analytics (UBA) suporta casos de uso com base em regras para determinadas anomalias comportamentais.

UBA : ShellBags Modificados por Ransomware

Ativado por Padrão

True

senseValue padrão

10

Descrição

Detecta modificações de registros ShellBag que indicam malware típico ou comportamento ransomware.

Regras de suporte

BB:UBA : Filtros de Evento Comum

Origens de dados

Microsoft Windows Security Event Logs (EventID: 4657)

UBA: usuário acessando recursos arriscados

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

Nota: Essa regra não é mais suportada.

UBA: usuário acessando recursos arriscados é desativado por padrão iniciando com a V2.3.0. As regras são agora listadas pelos tipos a seguir e ativadas por padrão:

- UBA: usuário acessando IP arriscado, anonimização
- UBA: usuário acessando IP arriscado, botnet
- UBA: usuário acessando IP arriscado, dinâmico
- UBA: usuário acessando IP arriscado, malware
- UBA: usuário acessando IP arriscado, spam

Ativado por Padrão

Falso

senseValue padrão

15

Descrição

Indica que um usuário acessou um recurso externo que é considerado inapropriado ou arriscado ou que mostra sinais de infecção.

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando IP arriscado, anonimização

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando IP, anonimização de risco (anteriormente chamado de IP, anonimização X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um usuário ou host local está se conectando a um serviço de anonimização externo.

Regras de suporte

- IP arriscado de X-Force, anonimização
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ative a regra a seguir: IP, anonimização X-Force de risco.

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando IP arriscado, botnet

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando IP, Bonet de risco (anteriormente chamado de IP, Bonet X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um usuário ou host local está se conectando a um comando botnet e a um servidor de controle.

Regras de suporte

- IP arriscado de X-Force, botnet
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ative a regra a seguir: IP, Bonet X-Force de risco.

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando IP arriscado, dinâmico

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando IP, dinâmico de risco (anteriormente chamado de IP, dinâmico X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um host ou usuário local está se conectando a um endereço IP designado dinamicamente.

Regras de suporte

- IP arriscado de X-Force, dinâmico
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ative a regra a seguir: IP, dinâmico X-Force de risco.

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando IP arriscado, malware

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando IP, malware de risco (anteriormente chamado de IP, malware X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um usuário ou host local está se conectando a um host de malware.

Regras de suporte

- IP arriscado de X-Force, malware
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ative a regra a seguir: IP, malware X-Force de risco.

Origens de dados

Todas as origens de log suportadas.

UBA: usuário acessando IP arriscado, spam

O aplicativo QRadar User Behavior Analytics (UBA) suporta casos de uso baseados em regras para determinadas anomalias comportamentais.

UBA: usuário acessando IP de risco, Spam (anteriormente chamado de IP, Spam X-Force de risco)

Ativado por Padrão

True

Descrição

Esta regra detecta quando um usuário ou host local está se conectando a um host de envio de spam.

Regras de suporte

- IP arriscado de X-Force, spam
- BB:UBA: Filtros de Eventos Comuns

Configuração necessária

- Configure "Ativar o Feed de Inteligência de Ameaça do X-Force" para Sim em **Configurações do Administrador** > **Configurações do Sistema**.
- Ative a regra a seguir: IP, Spam X-Force de risco.

Origens de dados

Todas as origens de log suportadas.

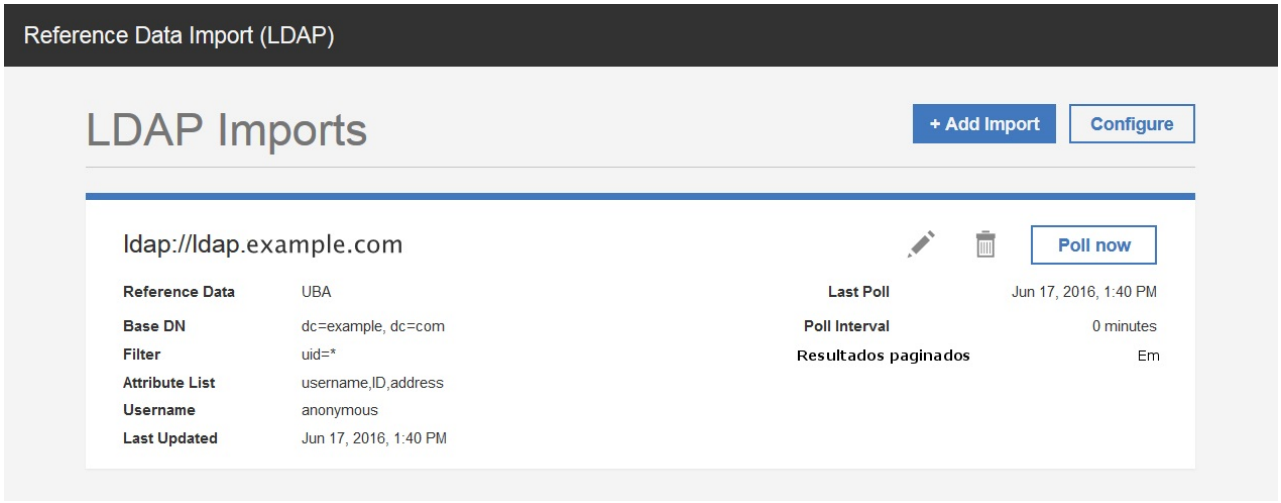
8 Aplicativo Reference Data Import - LDAP

Use o aplicativo Reference Data Import - LDAP para reunir informações de identificação contextuais de múltiplas fontes LDAP no seu QRadar Console.

Atenção: O aplicativo Reference Data Import - LDAP não é suportado no QRadar on Cloud.

Quando você instala o aplicativo IBM® QRadar® User Behavior Analytics (UBA), o aplicativo Reference Data Import LDAP também é instalado. É possível usar o aplicativo LDAP para importar dados do usuário de um servidor LDAP/AD ou de um arquivo CSV para uma tabela de referência do QRadar. A tabela de referência é, então, consumida pelo aplicativo UBA ou pode ser usada para procuras ou regras do QRadar.

Nota: O aplicativo Reference Data Import - LDAP requer o QRadar V7.2.8 ou mais recente.



Usando os dados LDAP no QRadar

Sempre que a tabela de referência é atualizada, um evento `ReferenceDataUpdated` é acionado. É possível configurar um valor de tempo de vida para os dados LDAP na tabela de referência. Quando o período de tempo de vida é excedido, um evento `ReferenceDataExpiry` é acionado. É possível criar regras que respondam a esses eventos ou criar procuras para consultar as cargas úteis desses eventos na guia QRadar **Atividade de log**.

Acessando o aplicativo Reference Data Import - LDAP

Acesse o aplicativo QRadar Reference Data Import - LDAP clicando no ícone **Reference Data Import LDAP** nas configurações de **Administrador**.

Para obter informações adicionais sobre coleções de dados de referência no QRadar, consulte *IBM QRadar SIEM Administration Guide*.

Navegadores suportados para o aplicativo LDAP

Para que os recursos nos produtos IBM Security QRadar funcionem adequadamente, deve-se usar um navegador da web suportado.

A tabela a seguir lista as versões suportadas de navegadores da web.

Tabela 1. Navegadores da web suportados para o aplicativo QRadar Reference Data Import LDAP

Navegador web	Versões suportadas
Mozilla Firefox	Liberação do suporte estendido 45.2
Google Chrome	Último

Importando dados do usuário de um arquivo CSV

É possível fazer upload de um arquivo CSV que contenha dados do usuário com o aplicativo Reference Data Import - LDAP

Sobre Esta Tarefa

Se você tiver dados do usuário em um formato CSV padrão, será possível importar os dados de um arquivo CSV para o aplicativo UBA.

Procedimento

1. No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia do administrador.
2. No QRadar 7.3.1 ou mais recente, clique em **Aplicativos** > **Importação de dados de referência - LDAP** > **Importação de dados de referência - Arquivo**.

3. Na janela Importação de dados de referência (arquivo), clique em **Configurar** para criar um token de serviço autorizado.
4. Na janela Importação de dados de referência (arquivo), clique em **Importar**.
5. Na tela Incluir dados do usuário, procure um arquivo CSV que contenha dados do usuário.

   Nota:

   O arquivo deve ter 5 MB ou menos, conter uma linha de cabeçalho com os nomes de colunas e deve ter pelo menos uma coluna que contenha dados exclusivos.
6. Clique em **Avançar** e selecione se você deseja mesclar dados com uma tabela de referência existente ou criar uma tabela de referência.
   - Se você optar por se mesclar em uma tabela de referência existente, clique em **Avançar** e selecione uma tabela de referência existente.
   - Se você optar por criar uma tabela de referência, clique em **Avançar** e crie uma tabela de referência.
7. Clique em **Avançar**.

8. Na tela Mapeamento de atributo, configure os nomes de atributos e a chave para a tabela de referência e clique em **Importar**.

Criando um token de serviço autorizado

Para poder configurar o servidor LDAP para incluir dados em uma tabela de referência, deve-se criar um token de serviço autorizado.

Antes de Iniciar

Atenção: Os administradores do QRadar on Cloud não podem criar um token de serviço autorizado para aplicativos QRadar devido a recursos limitados do administrador. Se você for um cliente do QRadar on Cloud, entre em contato com o Suporte ao Cliente para criar um token de serviço autorizado para você.

Sobre Esta Tarefa

Nota: Depois de enviar o token de serviço autorizado, deve-se implementar mudanças para o novo token de serviço autorizado entrar em vigor.
O IBM QRadar requer que você use um token de autenticação para autenticar as chamadas API que o aplicativo Reference Data Import - LDAP faz. Você usa a janela Gerenciar serviços autorizados nas configurações de **Administrador** para criar o token de serviço autorizado.

Procedimento

1. Na janela do aplicativo Reference Data Import - LDAP, clique em **Configurar**.
2. Na caixa de diálogo Configurar token de serviço autorizado, clique em **Gerenciar serviços autorizados**.
3. Na janela Gerenciar serviços autorizados, clique em **Incluir serviço autorizado**.
4. Inclua as informações relevantes nos campos a seguir e clique em **Criar serviço**:
   a. No campo **Nome do Serviço** , digite um nome para este serviço autorizado. O nome pode ter até 255 caracteres de comprimento.
   b. Na lista **Função de usuário**, selecione **Administrador**.
   c. Na lista **Perfil de segurança**, selecione o perfil de segurança que você deseja designar a esse serviço autorizado. O perfil de segurança determina as redes e fontes de log às quais esse serviço pode acessar na interface com o usuário do QRadar.
   d. Na lista **Data de validade**, digite ou selecione uma data para esse serviço expirar. Caso uma data de validade não seja necessária, selecione **Sem expiração**.
5. Clique na linha que contém o serviço que você criou, selecione e copie a sequência de caracteres do token no campo **Token selecionado** na barra de menus e feche a janela Gerenciar serviços autorizados.
6. Na caixa de diálogo Configurar token de serviço autorizado, cole a sequência de caracteres do token no campo **Token** e clique em **OK**.
7. Implemente mudanças para que o novo token de serviço autorizado entre em vigor.

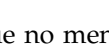
O que Fazer Depois

"Incluindo uma configuração LDAP" na página 164

Incluindo uma autoridade de certificação raiz privada

É possível fazer upload de um pacote configurável de autoridade de certificação (CA) raiz privada para o IBM QRadar para uso com o aplicativo LDAP.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **LDAP de importação de dados de referência**.
3. Na janela principal do aplicativo Reference Data Import LDAP, clique em **Configurar**.
4. Clique em **Escolher arquivo** e clique em **Upload**. Somente o tipo de arquivo `.pem` tem suporte.
5. Clique em **OK**.

Incluindo uma configuração LDAP

Inclua as informações do servidor LDAP usado para inserir dados do usuário em um mapa de referência de mapas.

Antes de Iniciar

Deve-se criar e incluir um token de autenticação no aplicativo Reference Data Import - LDAP antes de poder incluir uma configuração LDAP.

Procedimento

1. Na janela do aplicativo Reference Data Import - LDAP, clique em **Incluir importação**.
2. Insira as informações a seguir na guia **Configuração de LDAP**:
   a. Insira uma URL que comece com `ldap://` ou `ldaps://` (para TLS) no campo **URL do LDAP**.
   b. Insira o ponto na árvore do diretório LDAP do qual o servidor deve procurar usuários no campo **DN base**.

      Por exemplo, se o seu servidor LDAP estava no domínio `example.com`, você poderá usar: `dc=example,dc=com`
   c. Insira o atributo ou atributos que deseja usar para classificar os dados que são importados na tabela de referência no campo **Filtro**. Por exemplo:

      `cn=*; uid=*; sn=*`

      Os valores padrão a seguir funcionarão com o Active Directory: `(&(sAMAccountName=*)(samAccountType=805306368))`.
   d. Insira os atributos que deseja importar na tabela de referência no campo **Lista de atributos**.

      Os valores padrão a seguir funcionarão com o Active Directory: `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.
   e. Insira o nome do usuário que é usado para autenticar o servidor LDAP no campo **Nome do usuário**.
   f. Insira a senha para o servidor LDAP no campo **Senha**.
3. Clique em **Conexão de teste** para confirmar que o IBM QRadar pode se conectar com o servidor LDAP antes de você continuar.

   Se a sua tentativa de conexão for bem-sucedida, as informações do seu servidor LDAP serão exibidas na guia **Configuração de LDAP**.
4. Clique em **Avançar**.

O que Fazer Depois

"Selecionando atributos" na página 165.

Tarefas relacionadas:

“Incluindo uma autoridade de certificação raiz privada” na página 163
É possível fazer upload de um pacote configurável de autoridade de certificação (CA) raiz privada para o IBM QRadar para uso com o aplicativo LDAP.

“Criando um token de serviço autorizado” na página 163
Para poder configurar o servidor LDAP para incluir dados em uma tabela de referência, deve-se criar um token de serviço autorizado.

“Incluindo mapeamentos de atributo LDAP”
É possível incluir aliases e configurar a chave para a tabela de referência.

Selecionando atributos

Selecione os atributos a serem extraídos do servidor LDAP.

Procedimento

1. Na guia Selecionar **atributos**, procure atributos específicos e selecione os atributos que você deseja extrair do servidor LDAP.
2. Clique em **Avançar**.

O que Fazer Depois

Incluir mapeamentos de atributo de LDAP.

Incluindo mapeamentos de atributo LDAP

É possível incluir aliases e configurar a chave para a tabela de referência.

Sobre Esta Tarefa

Se desejar mesclar dados LDAP de múltiplas fontes na mesma tabela de referência, será possível usar aliases customizados para diferenciar atributos LDAP com o mesmo nome em diferentes fontes.

Procedimento

1. Na guia **Mapeamento de atributo**, configure a chave para a tabela de referência.

   Dica: É possível criar novos campos de Atributo LDAP clicando em **Incluir** e combinando dois atributos. Por exemplo, é possível usar a sintaxe a seguir: `"Último: {ln}, Primeiro: {fn}"`.
2. Clique em **Avançar**.

O que Fazer Depois

Configure uma tabela de dados de referência para armazenar dados LDAP..

Tarefas relacionadas:

“Incluindo uma configuração de dados de referência” na página 166
Use a guia Configuração de referência para configurar uma tabela de dados de referência para armazenar dados LDAP.

“Criando uma regra que responda às atualizações de dados LDAP” na página 168
Após ter configurado o aplicativo IBM QRadar Reference Data Import - LDAP para armazenar dados do seu servidor LDAP em uma tabela de referência no QRadar, é possível usar os dados para criar regras de evento.

Incluindo uma configuração de dados de referência

Use a guia Configuração de referência para configurar uma tabela de dados de referência para armazenar dados LDAP.

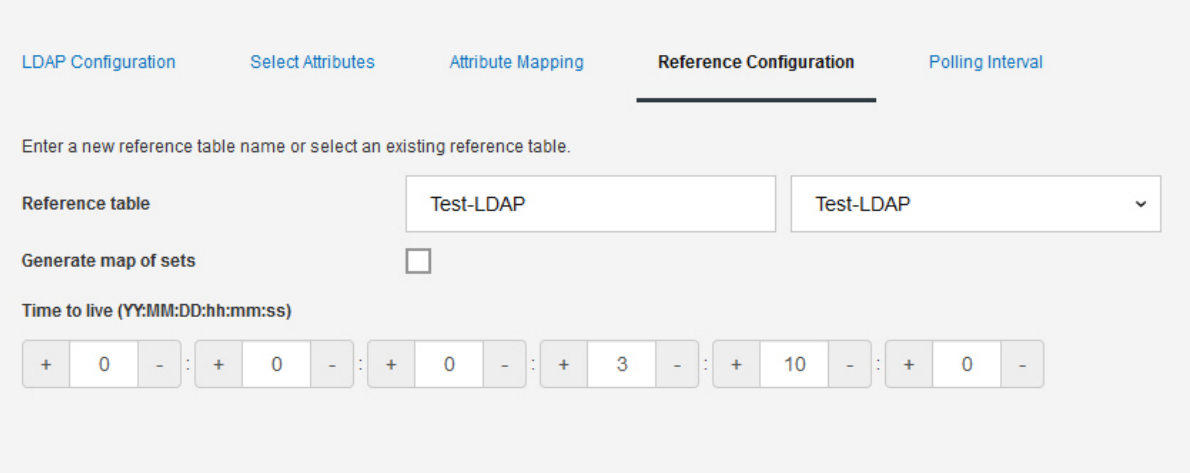
Antes de Iniciar

Após configurar as informações do seu servidor LDAP, deve-se configurar uma tabela de referência para armazenar os dados LDAP que são passados para o aplicativo. Então, é possível usar os dados armazenados para construir regras no QRadar ou criar procuras e relatórios.

Procedimento

1. Use a guia **Configuração de referência** para inserir uma nova tabela de referência ou designar uma tabela de referência existente na qual você deseja incluir dados LDAP.
   a. Insira um nome para a coleção de dados de referência no campo **Dados de referência** ou selecione uma coleção de dados de referência existente na lista.
   b. A caixa de seleção **Gerar mapa de conjuntos** está desativada por padrão. Se você ativar a caixa de seleção, ela enviará dados para um formato de conjunto de referência para melhorar a procura do QRadar e poderá afetar o desempenho.
   c. Use os campos **Tempo de vida** para definir por quanto tempo você deseja que os dados persistam na tabela de referência. Por padrão, os dados que você inclui nunca expiram. Quando o período de tempo de vida é excedido, um evento `ReferenceDataExpiry` é acionado.

      Nota: Se você anexar dados a um mapa de referência de mapas existente, o aplicativo usará os parâmetros de tempo de vida originais. Esses parâmetros não podem ser substituídos na guia **Configuração de referência**.



2. Clique em **Avançar**.

O que Fazer Depois

Configure o intervalo de pesquisa.

Tarefas relacionadas:

"Configurando a pesquisa" na página 167
Use a guia **Intervalo de pesquisa** para configurar com que frequência o aplicativo pesquisará o seu servidor LDAP para informações novas.

Configurando a pesquisa

Use a guia **Intervalo de pesquisa** para configurar com que frequência o aplicativo pesquisará o seu servidor LDAP para informações novas.

Antes de Iniciar

Após configurar as informações e a coleção de dados de referência do seu servidor LDAP, configure com qual frequência deseja que o aplicativo extraia dados do servidor LDAP.

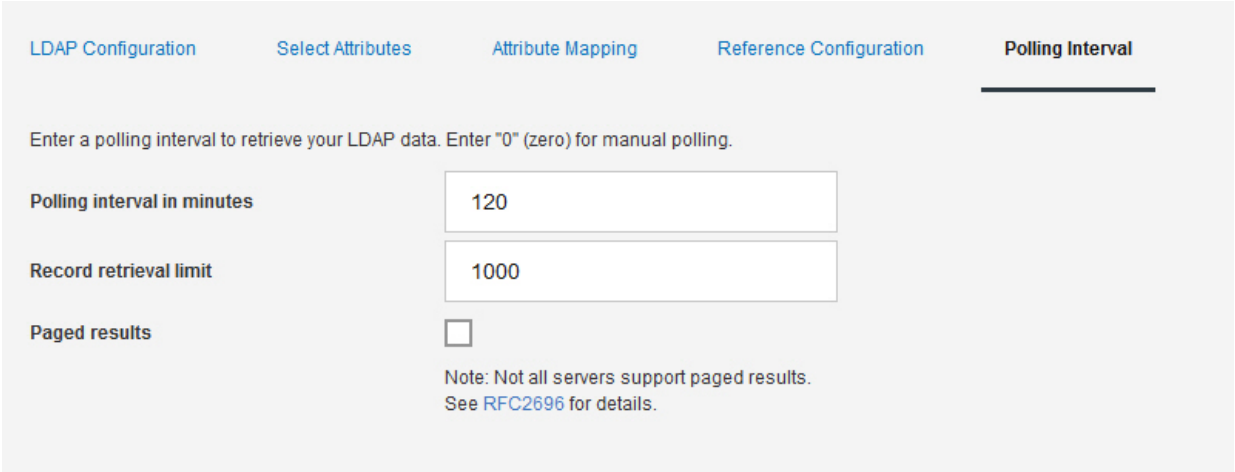
Procedimento

1. Use o campo **Intervalo de pesquisa em minutos** para definir em minutos com que frequência você deseja que o aplicativo pesquise dados no seu servidor LDAP.

   O valor mínimo do intervalo de pesquisa permitido é `120`.
2. Insira um valor para o número de registros que deseja que a pesquisa retorne no campo **Limite de recuperação de registro**.

   Por padrão, 100.000 registros são retornados. O número máximo de registos que podem ser retornados é 200.000.
3. A caixa de seleção **Resultados paginados** é selecionada por padrão para evitar a limitação do número de registros que o servidor LDAP retorna para cada pesquisa.

   Nota: Os resultados paginados não são suportados por todos os servidores LDAP.
4. Clique em **Salvar**.



Resultados

Dados do seu servidor LDAP são incluídos na coleção de dados de referência selecionada no intervalo que você configurou. É possível usar a página da API no console do IBM QRadar para verificar se os dados foram incluídos na coleção de dados de referência.

Tarefas relacionadas:

"Verificando se os dados estão incluídos na coleção de dados de referência" na página 168
Será possível usar a página de documentação da API do IBM QRadar para testar se os dados foram incluídos na coleção de dados de referência que você criou.

Verificando se os dados estão incluídos na coleção de dados de referência

Será possível usar a página de documentação da API do IBM QRadar para testar se os dados foram incluídos na coleção de dados de referência que você criou.

Sobre Esta Tarefa

A página Documentação da API em seu QRadar Console pode mostrar os dados que estão armazenados na tabela de referência que você criou no aplicativo Reference Data Import - LDAP. É possível usar a página Documentação da API para verificar se as informações de LDAP foram atualizadas pelo aplicativo.

Procedimento

1. Efetue login na página QRadar Documentação da API.
   `https://<Console_IP>/api_doc`
2. Na árvore de navegação, abra a API mais recente.
3. Acesse **/reference_data** > **/table** > **/name** > **GET**
4. No campo **Valor** do parâmetro **`Name`**, insira o nome da coleção de dados de referência criada para armazenar as informações de LDAP e clique em **Experimente!**.
   Os dados incluídos pelo aplicativo são retornados no campo **Corpo de resposta**.

Criando uma regra que responda às atualizações de dados LDAP

Após ter configurado o aplicativo IBM QRadar Reference Data Import - LDAP para armazenar dados do seu servidor LDAP em uma tabela de referência no QRadar, é possível usar os dados para criar regras de evento.

Sobre Esta Tarefa

Quando você pesquisa o seu servidor LDAP e os dados estão incluídos na tabela de referência, os eventos `ReferenceDataUpdated` são acionados. Quando o período de tempo de vida configurado na guia **Configuração de referência** é excedido, um evento `ReferenceDataExpiry` é acionado. É possível criar regras que respondam ao conteúdo dentro de uma carga útil do evento `ReferenceDataUpdated` ou `ReferenceDataExpiry`.

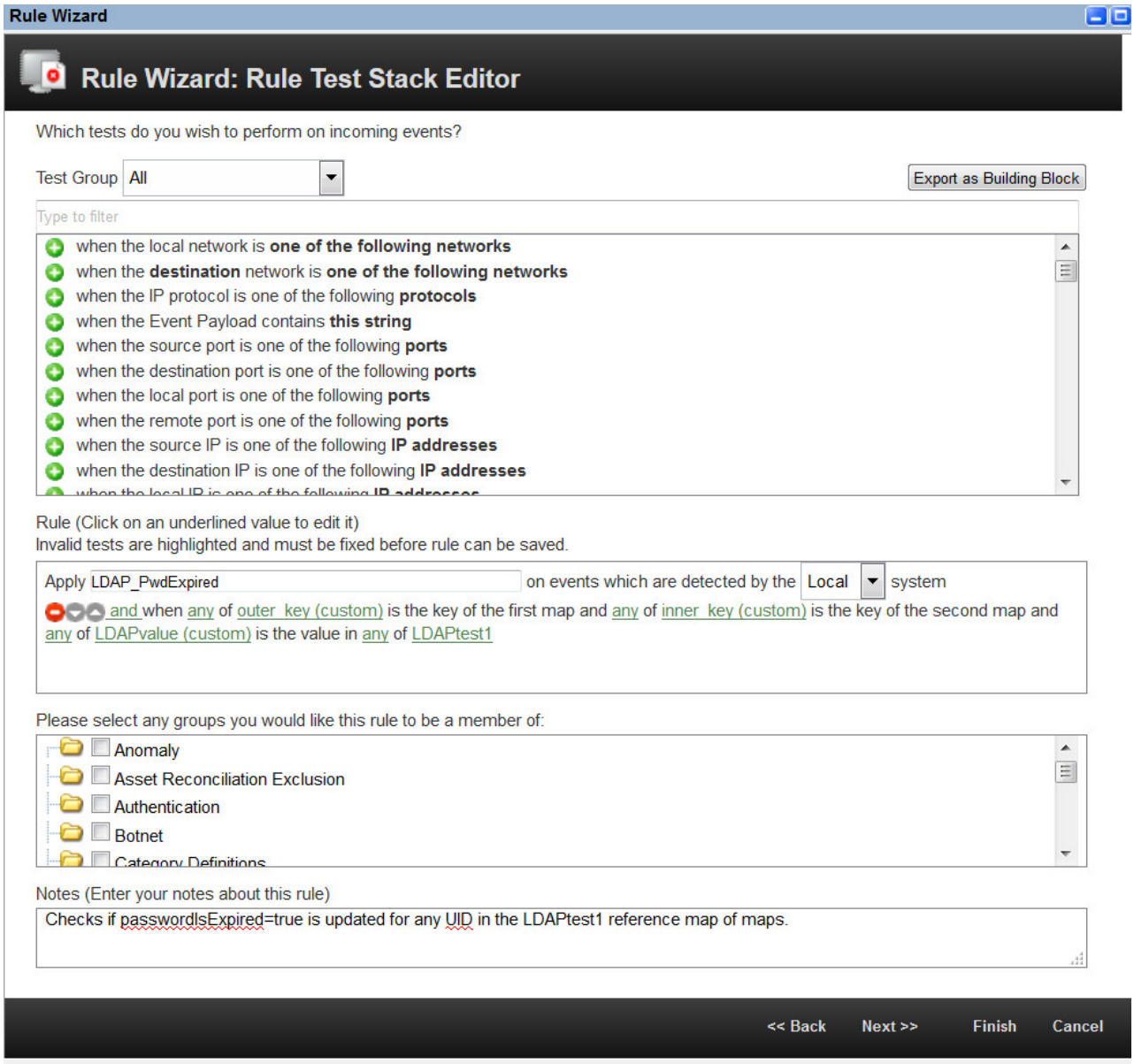
Dados LDAP armazenados pelo aplicativo em uma coleção de dados de referência estão disponíveis para regras que podem ser configuradas usando o QRadar **Assistente de regras**. O **Assistente de regras** pode ser acessado das guias **Ofensas**, **Atividade de log** ou **Atividade de rede**.

Procedimento

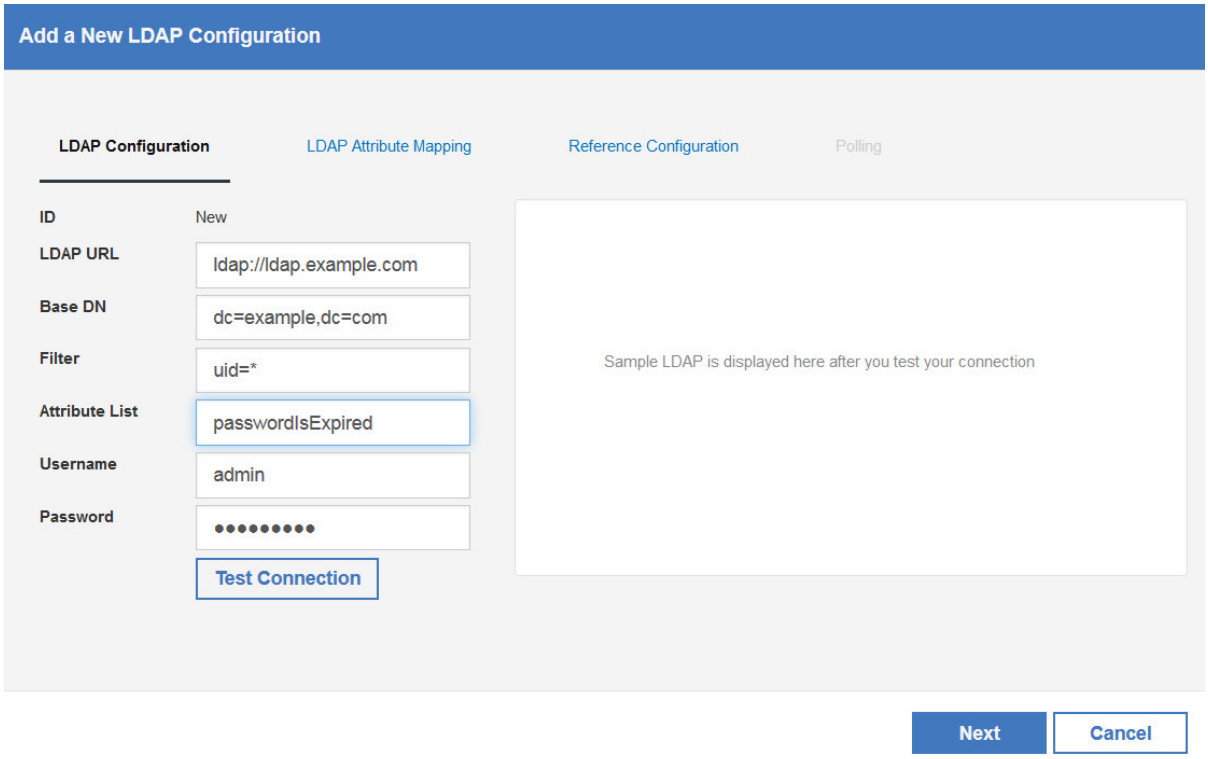
1. Clique em **Atividade de log** > **Regras** > **Ações** > **Nova regra de evento**.
2. Na página de introdução **Assistente de regra**, clique em **Avançar**.
3. Certifique-se de que o botão de opções **Eventos** esteja selecionado e clique em **Avançar**.
4. Insira um nome para a regra no campo fornecido.
5. Selecione um teste na lista **Grupo de testes** e clique no ícone + ao lado do teste que deseja usar:
   O teste de regra que você selecionar dependerá das informações que deseja recuperar da coleção de dados de referência que retém seus dados LDAP.
   O teste de propriedade de mapas de referência de evento de mapas a seguir é projetado para testar eventos que são acionados quando a tabela de referência do aplicativo Reference Data Import - LDAP é atualizada:

```
Quando qualquer uma dessas propriedades de evento é a chave no primeiro mapa
 e qualquer uma dessas propriedades de evento é a chave do segundo mapa
 e qualquer uma dessas propriedades de evento é o valor
 em qualquer um desses mapas de referência de mapas.
```

Uma regra será configurada para testar a carga útil do evento `ReferenceDataExpiry` se o atributo LDAP **`PasswordIsExpired`** for atualizado para `true` para qualquer UID em uma coleção de dados de referência **LDAPtest1**.



Para usar esse teste de propriedade de evento, deve-se criar propriedades de evento customizadas para os campos **`outer key`** (a chave do primeiro mapa), **`inner key`** (a chave do segundo mapa) e **`value`**. No exemplo a seguir, o aplicativo Reference Data Import - LDAP foi configurado para importar informações sobre usuários cuja senha foi expirada de um servidor LDAP em `example.com`.



A outer key

Essa propriedade contém os dados inseridos nos campos LDAP especificados nos campos **DN base** e **Filtro** na guia de configuração LDAP do aplicativo. A expressão regular para a propriedade do evento customizado pode ser parecer com isso:

```
(uid=(.*?),dc=example,dc=com)
```

A inner key

Essa propriedade contém os dados inseridos nos campos LDAP especificados no campo **Atributo** na guia de configuração LDAP do aplicativo. É possível usar aliases de atributo nesse campo A expressão regular para a propriedade do evento customizado pode ser parecer com isso:

```
(passwordIsExpired)
```

O campo Valor

Essa propriedade contém os dados recuperados para o atributo LDAP **passwordIsExpired** para cada usuário. A expressão regular para a propriedade do evento customizado pode ser parecer com isso:

```
(\['true'\])
```

Para obter informações adicionais sobre as propriedades de evento customizadas, consulte o *IBM QRadar SIEM Users Guide*.

6. Clique em **Avançar**.
7. Selecione a ação de regra, a resposta de regra e o limitador de regra que deseja aplicar à regra e clique em **Concluir**.

   Para obter informações adicionais sobre regras de evento customizadas, consulte o *IBM QRadar SIEM Users Guide*.

Resultados

Da próxima vez que você pesquisar o seu servidor LDAP e a coleção de dados de referência que você criou for atualizada, a sua regra será acionada.

Tarefas relacionadas:

"Incluindo mapeamentos de atributo LDAP" na página 165
É possível incluir aliases e configurar a chave para a tabela de referência.

"Incluindo uma configuração de dados de referência" na página 166
Use a guia Configuração de referência para configurar uma tabela de dados de referência para armazenar dados LDAP.

9 App Machine Learning Analytics

O app Machine Learning Analytics (ML) estende os recursos do seu sistema QRadar e do app QRadar User Behavior Analytics (UBA) ao incluir os casos de uso para análise de aprendizado de máquina. Com os casos de uso do Machine Learning Analytics, é possível obter mais insight sobre o comportamento do usuário com a modelagem preditiva. O aplicativo ML ajuda o seu sistema a aprender o comportamento esperado dos usuários em sua rede.

Atenção: Deve-se instalar o IBM QRadar V7.2.8 ou mais recente antes de instalar o aplicativo UBA e o aplicativo ML.

Importante:

- É melhor ativar as Configurações do Machine Learning Analytics um dia depois de configurar inicialmente o aplicativo UBA. Esse período de espera assegura que o app UBA tenha tempo suficiente para criar perfis de risco para os usuários.
- O modelo é atualizado a cada sete dias. Isso garante que o app Machine Learning Analytics monitore os usuários com risco mais recentes.
- O console do QRadar limita a quantia de memória que pode ser usada por aplicativos. As opções de tamanho da instalação do aplicativo do ML são baseadas na quantidade de memória que o QRadar tem atualmente para os aplicativos.
  - A quantia mínima de memória livre necessária para instalar o aplicativo do ML é de 2 GB em um console do QRadar e de 5 GB em um nó do aplicativo.
  - O número de usuários monitorados pelo aplicativo do ML depende do tamanho da instalação do aplicativo do ML e da analítica específica do Machine Learning. O número máximo de usuários monitorados por qualquer analítica do Machine Learning é de 500 usuários por GB do tamanho da instalação do Machine Learning. Por exemplo, 2 GB seriam de até 1000 usuários e 50 GB seriam até 25000 usuários.
- A instalação poderá falhar devido a uma falta de memória disponível. Essa situação poderá ocorrer se a quantia de memória disponível para aplicativos diminuir em decorrência da instalação de outros aplicativos.

Problemas conhecidos para o Machine Learning Analytics

O aplicativo Machine Learning Analytics tem as informações necessárias para instalação e problemas conhecidos.

O aplicativo Machine Learning Analytics tem os problemas conhecidos a seguir:

- O app Machine Learning pode mostrar mensagens de aviso na seção Status do Machine Learning. Para obter informações adicionais, consulte “O status do app Machine Learning mostra um aviso no painel” na página 202.
- A instalação poderá falhar devido a uma falta de memória disponível. Essa situação poderá ocorrer em consoles de 128 GB se vários outros aplicativos já estiverem instalados e restarem menos de 10 GB para o aplicativo ML usar. Se a instalação falhar, a mensagem de erro "FAILED" será exibida. Para corrigir essa situação, desinstale alguns dos outros aplicativos e, em seguida, tente novamente.

Pré-requisitos para instalar o aplicativo Machine Learning Analytics

Antes de instalar o aplicativo Machine Learning Analytics, assegure-se de atender aos requisitos.

Deve-se atender aos requisitos do sistema a seguir e instalar e configurar totalmente o aplicativo User Behavior Analytics (UBA) antes de poder instalar o aplicativo Machine Learning Analytics.

Componente	Requisitos mínimos
Memória do sistema	• Console: 64 GB • Nó do aplicativo: 5 GB
Versão do IBM QRadar	V7.2.8 ou mais recente
Sense DSM	Instale o arquivo RPM do DSM.
Aplicativo UBA	• Instale o aplicativo UBA V3.1.0. • Configure as Configurações do UBA. • Clique na guia **Análise de dados do usuário** e confirme se o Painel do UBA contém dados do usuário.

Instalando o IBM Sense DSM manualmente

O aplicativo UBA e o aplicativo Machine Learning Analytics usam os arquivos do IBM Sense DSM para incluir pontuações de risco e ofensas do usuário no QRadar.

- Para V7.2.8: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
- Para o QRadar V7.3.1 e mais recente: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`

Restrição: A desinstalação de um Device Support Module (DSM) não é suportada no QRadar.

1. Copie o arquivo DSM RPM para o seu console QRadar.
2. Use SSH para efetuar login no host do QRadar como usuário raiz.
3. Acesse o diretório que inclui o arquivo transferido por download.
4. Digite o seguinte comando:
   `rpm -Uvh <rpm_filename>`
5. Nas configurações de **Administrador**, clique em **Avançado** > **Implementar configuração integral**.

Nota: Instruções para instalar e configurar o aplicativo UBA estão no IBM Knowledge Center.

Tarefas relacionadas:

"Instalando o aplicativo User Behavior Analytics" na página 17
Use a ferramenta IBM QRadar Extension Management para fazer upload e instalar seu archive do aplicativo diretamente no QRadar Console.

"Definindo as configurações do UBA" na página 28
Para visualizar informações no aplicativo IBM QRadar User Behavior Analytics (UBA), deve-se configurar as definições do aplicativo UBA.

Instalando o aplicativo Machine Learning Analytics

Instale o app Machine Learning Analytics depois de ter instalado o app UBA no Extension Manager.

Antes de Iniciar

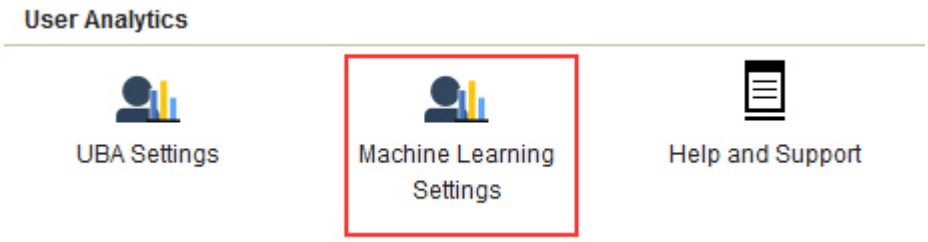
Certifique-se de ter concluído todos os Pré-requisitos para instalar o aplicativo Machine Learning Analytics.

Sobre Esta Tarefa

Depois de instalar seu aplicativo User Behavior Analytics (UBA) V2.1.0 ou mais recente, é possível instalar o aplicativo Machine Learning Analytics na página Configurações de Machine Learning.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.



3. Na página Configurações de aprendizado de máquina, clique em **Instalar App do ML**.
4. No prompt, clique em **Sim** para instalar o aplicativo. O aplicativo ML leva vários minutos para ser instalado.

O que Fazer Depois

Quando a instalação for concluída, será possível ativar os casos de uso do ML e, em seguida, clicar em **Salvar configuração**.

Atualizando o aplicativo Machine Learning Analytics

Faça upgrade do app Machine Learning Analytics na página Configurações do Machine Learning.

Antes de Iniciar

Iniciando com o UBA com o ML V2.2.0, não há procedimentos de upgrade. O aplicativo Machine Learning é automaticamente submetido a upgrade com o aplicativo UBA. Depois de instalar ou fazer upgrade de seu aplicativo User Behavior Analytics (UBA), é possível fazer upgrade seu aplicativo Machine Learning Analytics existente na página Configurações de Machine Learning.

Atenção: Se você tiver o app Machine Learning Analytics (ML) V2.0.0 instalado e fizer upgrade para a versão mais recente do app UBA, não desinstale o app Machine Learning Analytics do QRadar Extension Manager. Se você tentar desinstalar o app Machine Learning Analytics do Extension Manager, poderá encontrar problemas ao instalar o app ML.

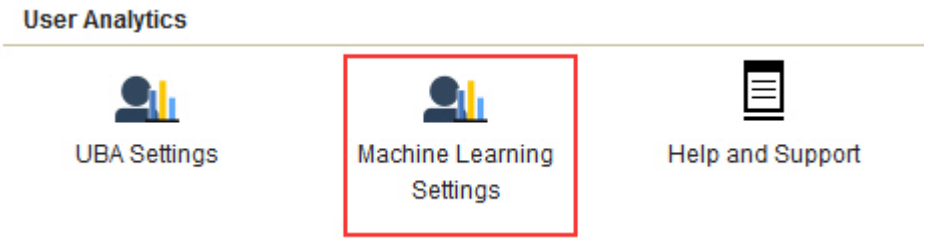
Nota: Se você estiver fazendo upgrade do app Machine Learning Analytics V2.1.0 ou inferior, o **Valor de risco do evento de verificação** para cada Analítica do usuário será atualizado para o valor padrão atual de Aprendizado de máquina.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.

- No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.

2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.



3. Na página Configurações de aprendizado de máquina, clique em **Fazer upgrade do App do ML**.
4. No prompt, clique em **Sim**. O aplicativo ML leva vários minutos para fazer o upgrade.
5. Após o upgrade ser concluído, a construção de modelo será reiniciada.

O que Fazer Depois

Verifique se as Configurações do Machine Learning estão definidas corretamente. Se você mudar alguma configuração, certifique-se de **Salvar a configuração**.

Definindo configurações do Machine Learning Analytics

Para visualizar informações no aplicativo Machine Learning Analytics, deve-se definir configurações do aplicativo Machine Learning Analytics.

Configurando a Analítica *Total Activity*

Configure a analítica de aprendizado de máquina *Total Activity* para exibir a quantia real e esperada (aprendida) da atividade de usuários durante todo o dia no Painel do UBA.

Sobre Esta Tarefa

Atenção: Após você configurar ou modificar as suas configurações, será necessário um mínimo de 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Importante: Iniciando com a V2.2.0, os valores padrão para **Valor de risco de evento de verificação** mudaram. Como os novos valores padrão são significativamente menores que os valores padrão anteriores, os novos valores padrão sobrescrevem os valores padrão existentes ou qualquer valor modificado anteriormente.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .

- No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
- No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.

3. Na página Configurações de aprendizado de máquina, clique em **Atividade total**.
4. Clique em **Ativado**  para ativar a analítica *Atividade total*.

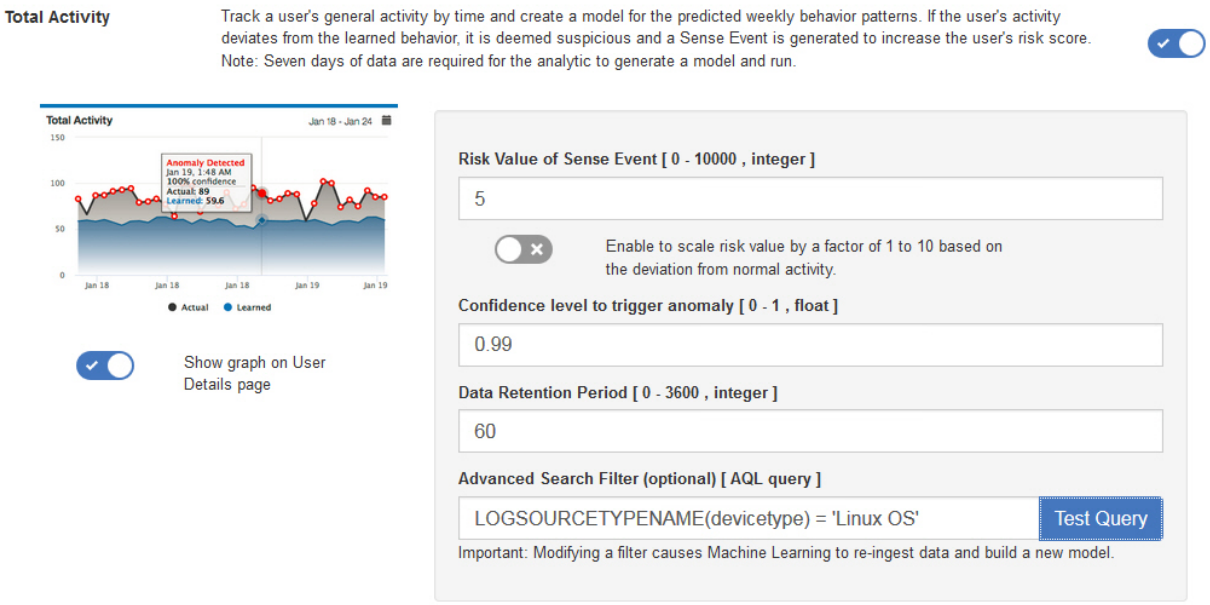
   Importante: Deve-se ter 7 dias de dados disponíveis para que a análise de dados gere um modelo.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Total Activity* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Total Activity* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a analítica *Abnormal Outbound Transfer Attempts*

Configure a analítica de aprendizado de máquina *Abnormal Outbound Transfer Attempts* para exibir o uso do tráfego de saída para cada usuário no Painel do UBA.

Sobre Esta Tarefa

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

A analítica de aprendizado de máquina *Abnormal Outbound Transfer Attempts* está disponível na V2.8.0 e mais recente.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em **Tentativas de transferência de saída anormal**.
4. Clique em **Ativado** para ativar a analítica *Abnormal Outbound Transfer Attempts*.

Importante: Deve-se ter 7 dias de dados após o conteúdo do UBA ser ativado no sistema.

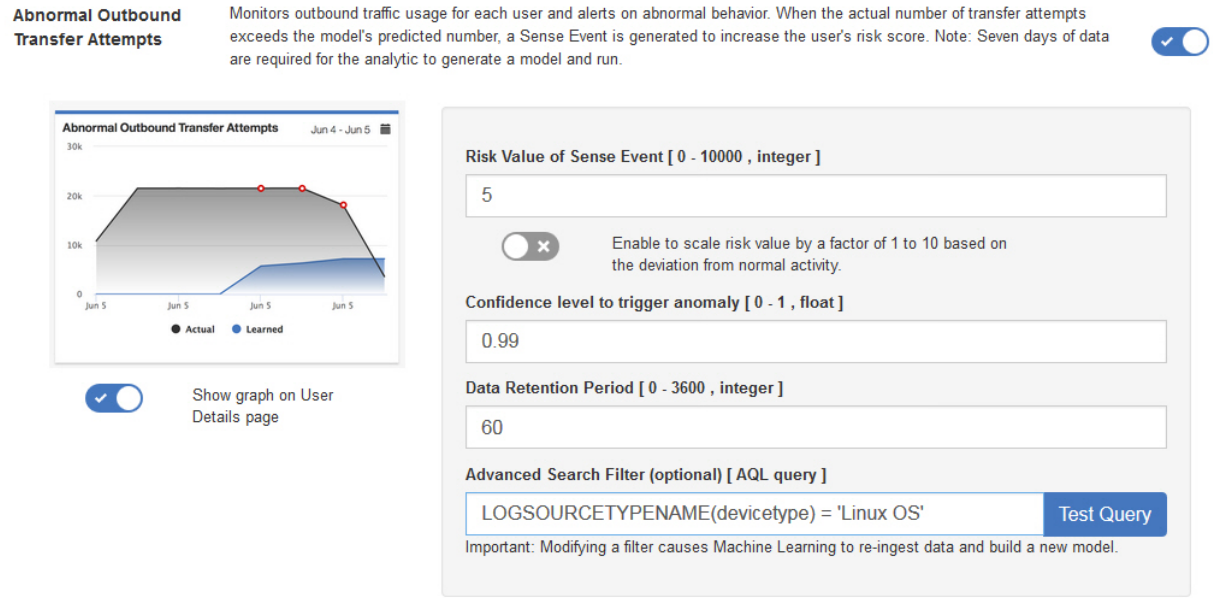
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é desativada por padrão. Para exibir o gráfico *Abnormal Outbound Transfer Attempts* na página Detalhes do Usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a Analítica *Activity by Category*

Configure a analítica de aprendizado de máquina *Activity by Category* para exibir os padrões de comportamento de atividade do usuário reais e esperados por categoria de alto nível no Painel do UBA.

Sobre Esta Tarefa

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Importante: Iniciando com a V2.2.0, os valores padrão para **Valor de risco de evento de verificação** mudaram. Como os novos valores padrão são significativamente menores que os valores padrão anteriores, os novos valores padrão sobrescrevem os valores padrão existentes ou qualquer valor modificado anteriormente.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em **Atividade por categoria**.
4. Clique em **Ativado**  para ativar a analítica *Activity by Category* e para exibir o gráfico *Activity by Category* na página Detalhes do usuário.

   Importante: Deve-se ter 7 dias de dados disponíveis para a análise de dados gerar um modelo inicial. Se você tiver menos de 7 dias de dados do usuário para esse sistema do QRadar, então, o modelo inicial será gerado após 7 dias de dados do usuário serem acumulados.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Activity by Category* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Activity by Category* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 1.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. Na seção **Categorias para rastrear**, as categorias de eventos de alto nível são ativadas por padrão. Clique em qualquer categoria para desativar seu monitoramento. Para obter mais informações sobre categorias, consulte o tópico Categorias de alto nível no IBM Knowledge Center.

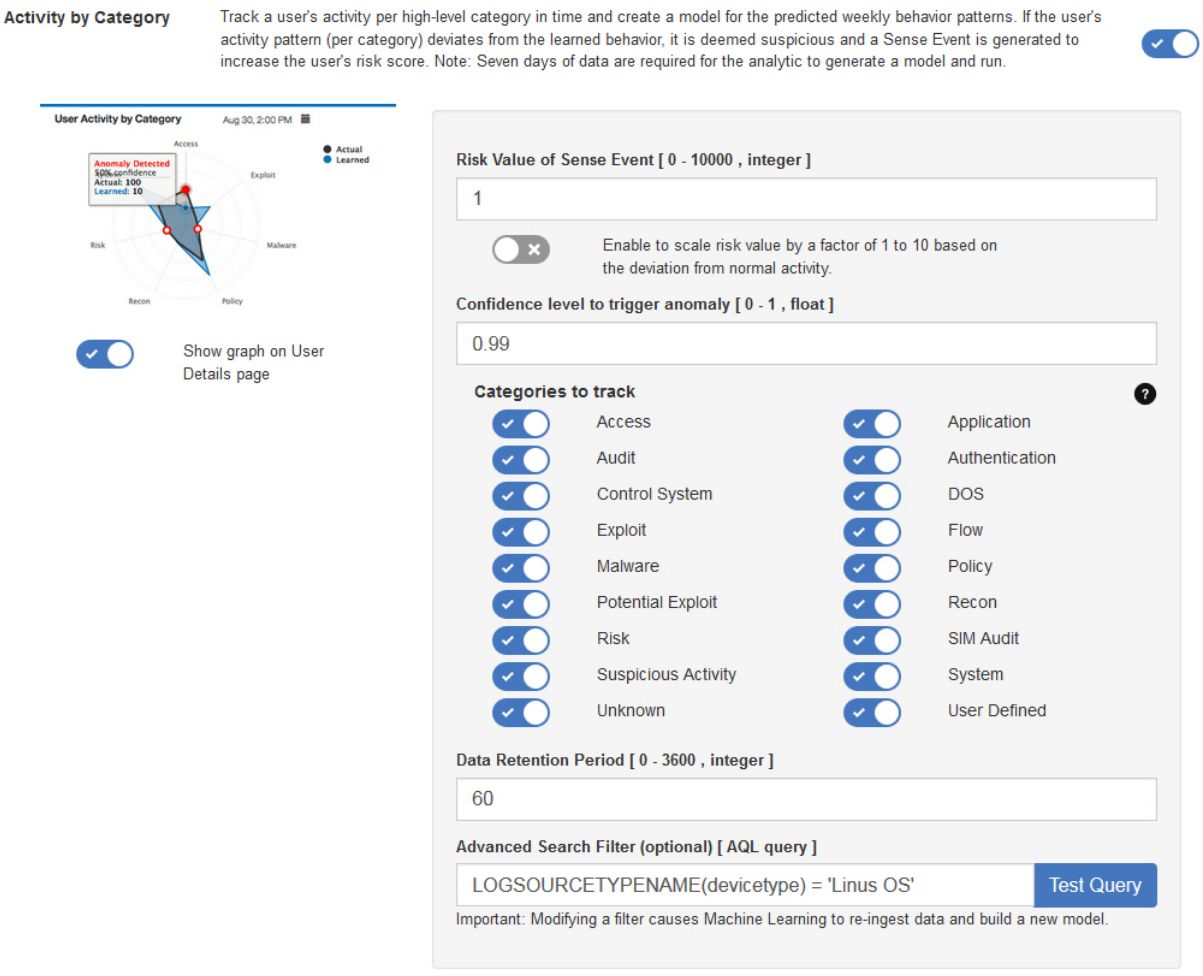
10. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
11. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
12. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a Analítica *Risk Posture*

Configure a analítica de aprendizado de máquina *Risk Posture* para exibir o desvio de pontuação de risco do usuário no Painel do UBA.

Sobre Esta Tarefa

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Importante: Iniciando com a V2.2.0, os valores padrão para **Valor de risco de evento de verificação** mudaram. Como os novos valores padrão são significativamente menores do que os valores padrão anteriores, os novos valores padrão sobrescreverão os valores padrão existentes ou qualquer valor modificado anteriormente.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em **Variação de risco**.
4. Clique em **Ativado** para ativar a analítica *Risk Posture*.

   Importante: Deve-se ter 7 dias de dados disponíveis para que a análise de dados gere um modelo.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Risk Posture* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Risk Posture* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco básico será multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o

número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

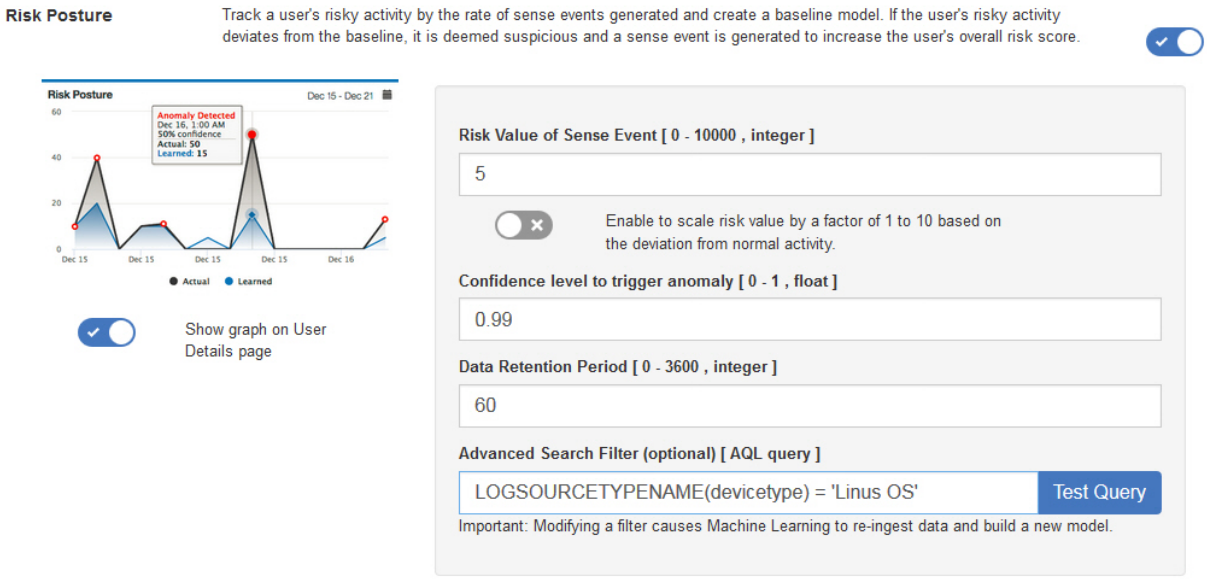
Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

- `REFERENCESETCONTAINS('Important People', username)`
- `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
- `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

Para obter mais informações, consulte Lingaguem da Consulta Ariel.

11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo uma hora para o aplicativo alimentar dados e construir um modelo inicial.

Configurando a analítica *Abnormal Volume of Data to External Domains*

Configure a analítica de aprendizado de máquina *Abnormal Volume of Data to External Domains* para exibir a quantidade real e esperada (informada) do volume de upload local para remoto para cada usuário no Painel do UBA.

Sobre Esta Tarefa

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

A analítica de aprendizado de máquina *Abnormal Volume of Data to External Domains* está disponível na V3.0.0 e mais recente.

Procedimento

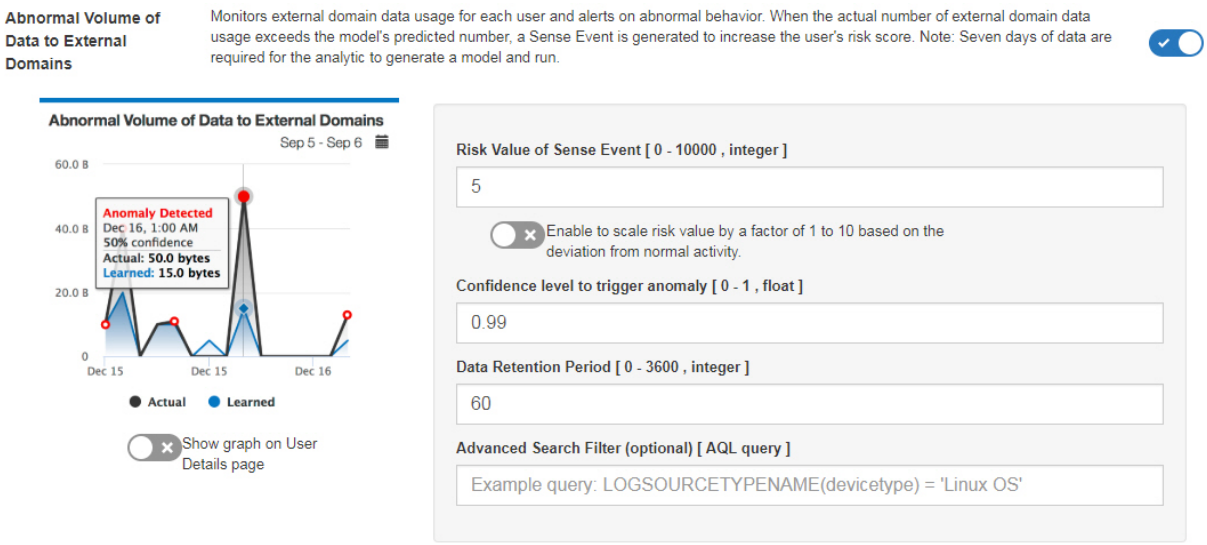
1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de Machine Learning**.
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações do Machine Learning, clique em **Volume anormal de dados para domínios externos**.
4. Clique em **Ativado**  para ativar a analítica *Abnormal Volume of Data to External Domains*.

   Importante: Deve-se ter 7 dias de dados após o conteúdo do UBA ser ativado no sistema.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é desativada por padrão. Para exibir o gráfico *Abnormal Volume of Data to External Domains* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 1.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:
    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a Analítica *Activity Distribution*

Configure a analítica de aprendizado de máquina *Activity Distribution* para exibir os clusters de comportamento dinâmico para todos os usuários que são monitorados por aprendizado de máquina no Painel do UBA.

Sobre Esta Tarefa

A analítica de aprendizado de máquina *Activity Distribution* está disponível na V2.2.0 e mais recente.

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em **Distribuição de atividade**.
4. Clique em **Ativado** para ativar a analítica *Activity Distribution* e para exibir o gráfico *Activity Distribution* na página Detalhes do usuário.

   Importante: Deve-se ter 7 dias de dados disponíveis para que a análise de dados gere um modelo.

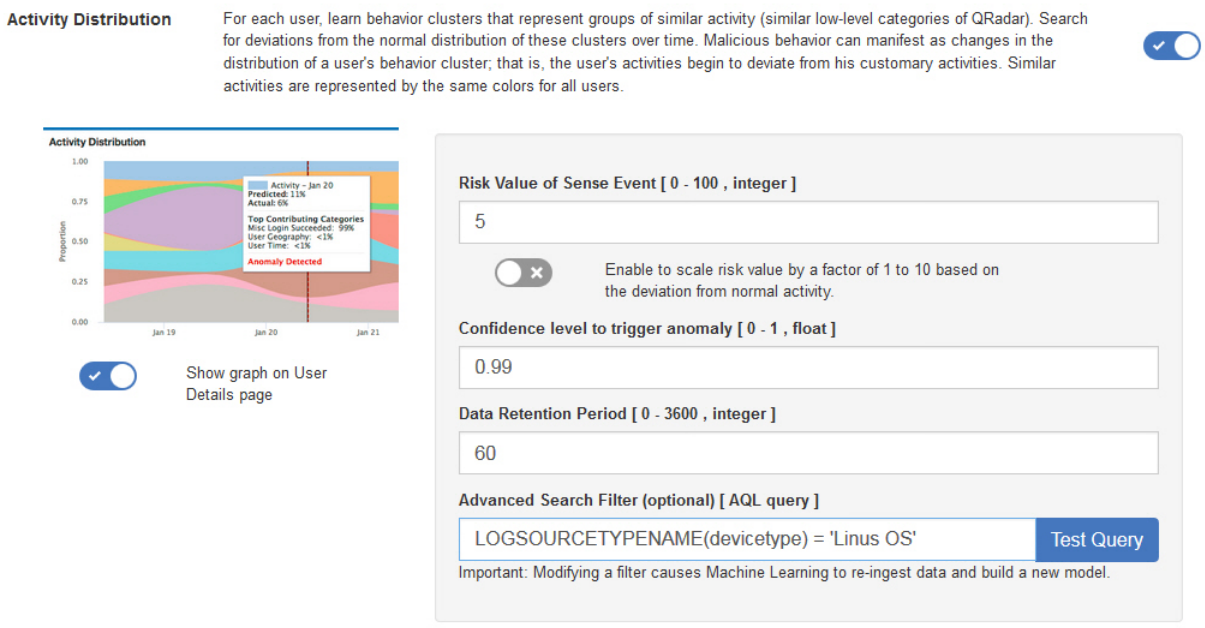
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Activity Distribution* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Activity Distribution* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a Analítica *Defined Peer Group*

Configure a analítica de aprendizado de máquina *Defined Peer Group* para exibir quanto a atividade de evento de um usuário se desvia da atividade de evento de seu grupo de peers definido no Painel do UBA.

Antes de Iniciar

- Para ativar a analítica *Defined Peer Group*, deve-se ter grupos de usuários válidos em uma tabela de referência e, em seguida, definir **Configurações do UBA** > **Exibir atributos** > **Grupos customizados** para usar a tabela de referência. Para obter informações adicionais, consulte "Grupos de usuários para a analítica do Defined Peer Group" na página 197.
- Deve-se ter sete dias de dados de eventos disponíveis para que a análise gere um modelo.

Sobre Esta Tarefa

A analítica de aprendizado de máquina *Defined Peer Group* está disponível na V2.6.0 e mais recente.

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em *Defined Peer Group*.
4. Clique em **Ativado**  para ativar a analítica *Defined Peer Group*.

   Importante: Deve-se ter 7 dias de dados disponíveis para que a análise de dados gere um modelo.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Defined Peer Group* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Defined Peer Group* na página Detalhes do Usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.

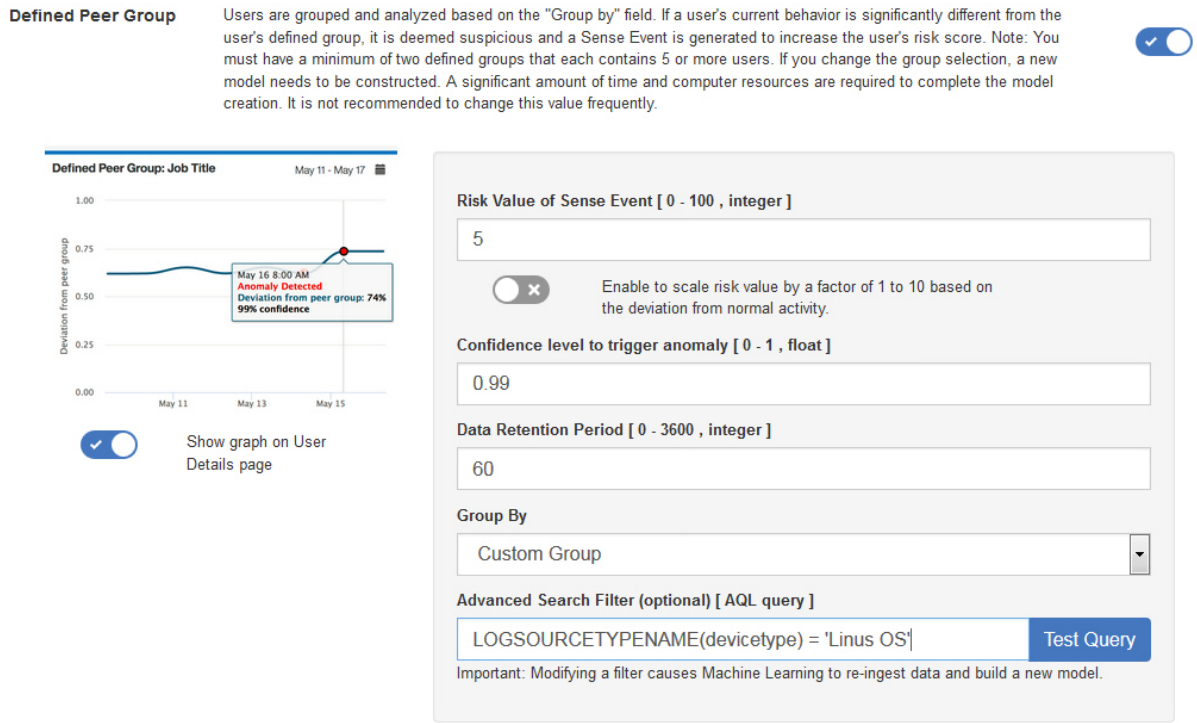
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. No campo **Agrupar por**, selecione o grupo que você deseja que a analítica *Defined Peer Group* use.
11. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

    Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

    É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    Para obter mais informações, consulte Lingaguem da Consulta Ariel.
12. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Configurando a analítica *Learned Peer Group*

Configure a analítica de aprendizado de máquina *Learned Peer Group* para exibir quanto o usuário desviou do grupo de peers inferido que ele esperava estar no Painel do UBA.

Antes de Iniciar

- Deve-se instalar um Nó do aplicativo para ativar a analítica *Learned Peer Group*. Para obter mais informações, consulte https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_adm_appnode_intro.html
- Deve-se ter 7 dias de dados do evento disponíveis para a analítica *Learned Peer Group* para gerar um modelo.

Sobre Esta Tarefa

A analítica de aprendizado de máquina *Learned Peer Group* está disponível na V2.2.0 e mais recente.

Atenção: Depois de definir suas configurações, leva no mínimo 1 hora para alimentar os dados, construir um modelo inicial e ver os resultados iniciais para os usuários.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação () e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de aprendizado de máquina** .
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.
3. Na página Configurações de aprendizado de máquina, clique em *Learned Peer Group*.
4. Clique em **Ativado**  para ativar a analítica *Learned Peer Group*.

   Importante: Deve-se ter 7 dias de dados disponíveis para que a análise de dados gere um modelo.
5. A alternância **Mostrar gráfico na página Detalhes do usuário** é ativada por padrão para exibir o gráfico *Learned Peer Group* na página Detalhes do usuário. Se você não desejar exibir o gráfico *Learned Peer Group* na página Detalhes do usuário, clique na alternância.
6. No campo **Valor de risco de evento de verificação**, insira a quantia para aumentar a pontuação de risco do usuário quando um evento de verificação for acionado. O valor padrão é 5.
7. Ative a alternância para escalar o valor de risco. Quando ativado, o valor de risco base é multiplicado por um fator (intervalo de 1 a 10). Esse fator é determinado por quanto o usuário se desvia do comportamento esperado e não somente pelo fato de ter desviado.
8. No campo **Intervalo de confiança para acionar anomalia**, insira a porcentagem para o nível de confiança que o algoritmo de aprendizado de máquina deve estar antes de acionar um evento anômalo. O valor padrão é 0,99.
9. No campo **Período de retenção de dados**, configure o número de dias pelos quais você deseja salvar o modelo de dados. O valor padrão é 60. Se desejar desativar a limpeza automática de dados, configure o valor para 0 (zero).
10. Opcional: No campo **Filtro de Procura Avançada**, é possível incluir um filtro AQL para limitar os dados consultados pela análise no QRadar. Ao filtrar uma consulta AQL, é possível reduzir o

número de usuários ou os tipos de dados analisados pela análise. Antes de salvar a configuração, clique em **Testar consulta** para ativar uma consulta AQL completa no QRadar para que seja possível revisar a consulta e verificar os resultados.

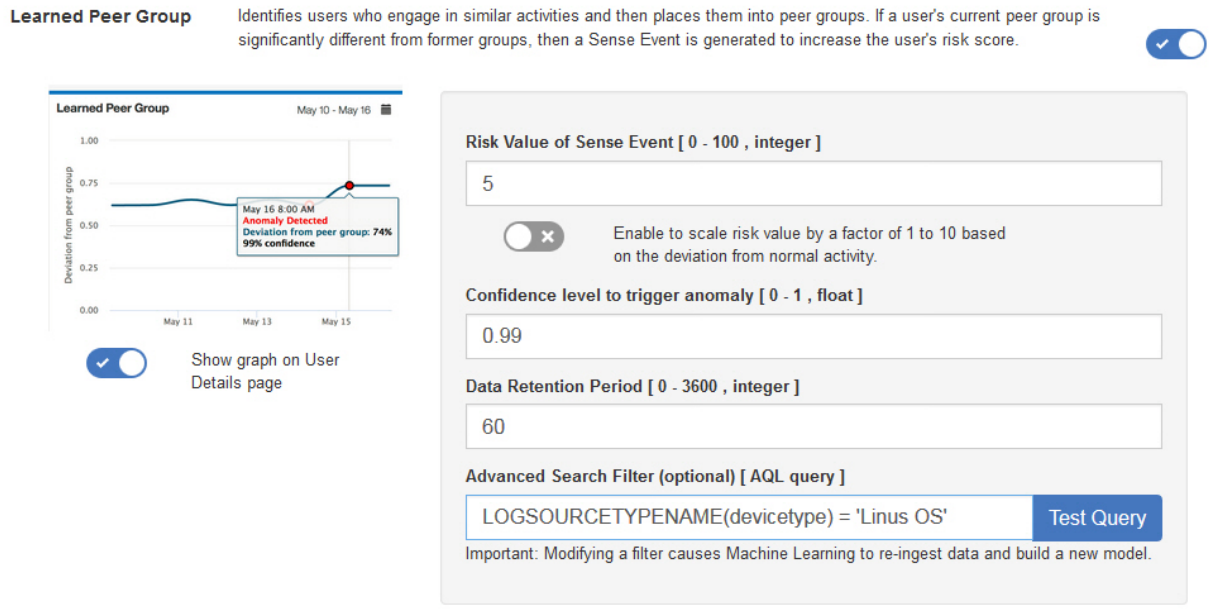
Importante: Ao modificar o filtro AQL, o modelo existente para a análise será marcado como inválido e será reconstruído. O período de tempo da reconstrução depende da quantidade de dados retornada pelo filtro modificado.

É possível filtrar origens de log específicas, nomes de rede ou conjuntos de referência que contenham usuários específicos. Consulte os exemplos a seguir:

- `REFERENCESETCONTAINS('Important People', username)`
- `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
- `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

Para obter mais informações, consulte Lingaguem da Consulta Ariel.

11. Clique em **Salvar Configuração**.



Resultados

Pode levar no mínimo 1 hora para o aplicativo ingerir dados e construir um modelo inicial.

Painel do UBA com o Machine Learning Analytics

O aplicativo IBM QRadar User Behavior Analytics (UBA) com o Machine Learning Analytics inclui o status do Machine Learning Analytics e detalhes adicionais para o usuário selecionado.

Dashboard

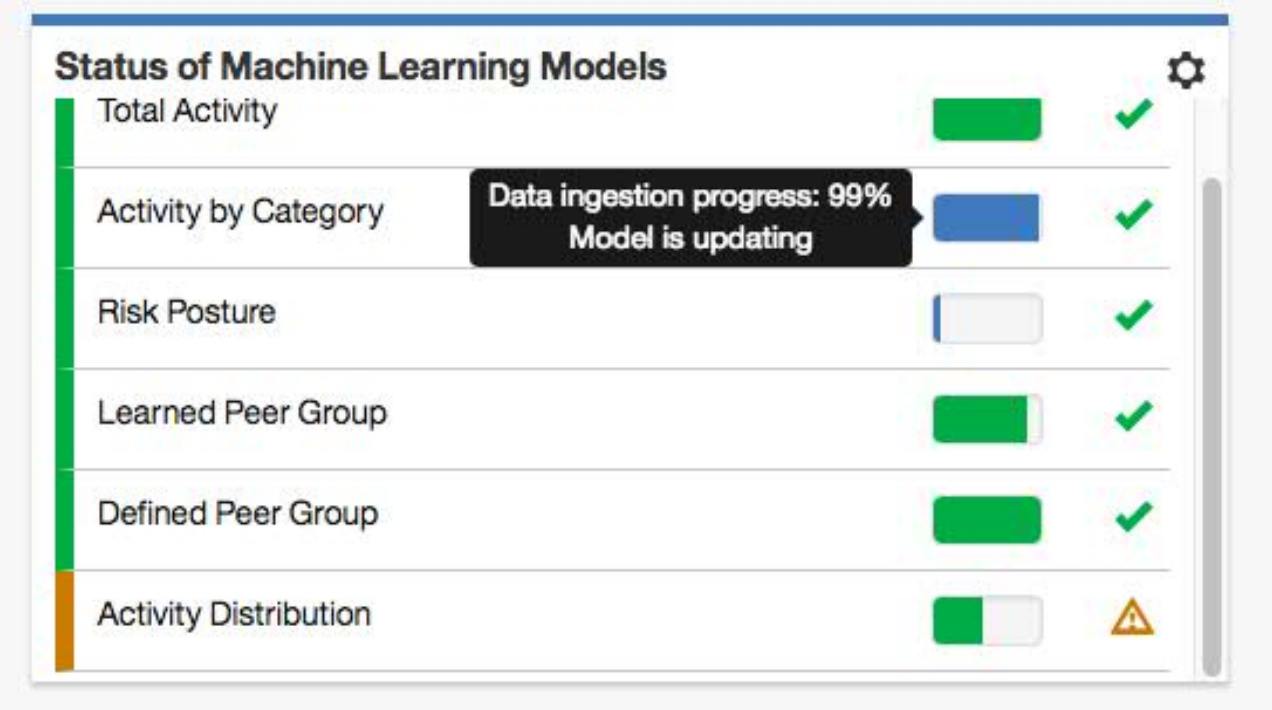
Depois de ativar o Machine Learning Analytics, clique na guia **Análise de dados do usuário** para abrir o painel.

A seção Status dos modelos do Machine Learning mostra a ingestão de modelo e o progresso da construção de modelo para cada analítica que você ativou. Observe que os modelos são atualizados a cada sete dias.

- A barra de progresso azul indica que a analítica está ingerindo dados.
- A barra de progresso verde indica que a analítica está construindo o modelo.
- A marca de seleção verde indica que a analítica está ativada.
- O ícone de aviso amarelo indica que um problema foi encontrado durante a fase de construção de modelo. Consulte “O status do app Machine Learning mostra um aviso no painel” na página 202

Clique no ícone **Configurações de ML** para abrir a página Machine Learning Analytics e editar a configuração para os casos de uso do Machine Learning Analytics.

Nota: Se você editar a configuração após ela ser salva, um novo modelo será construído e o tempo de espera para a ingestão e a construção de modelo será reconfigurado.

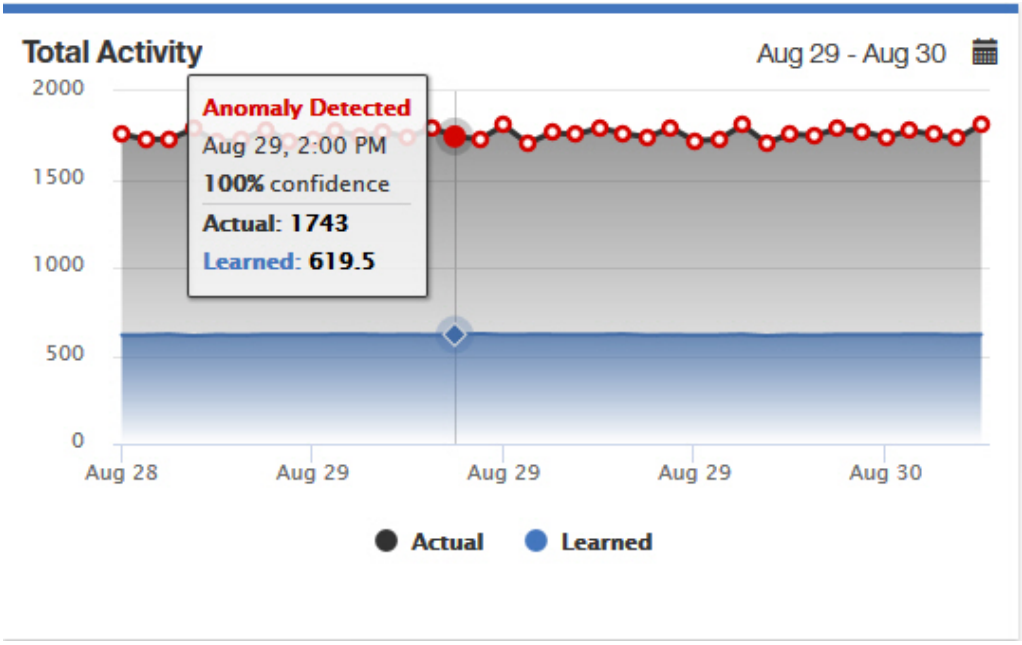


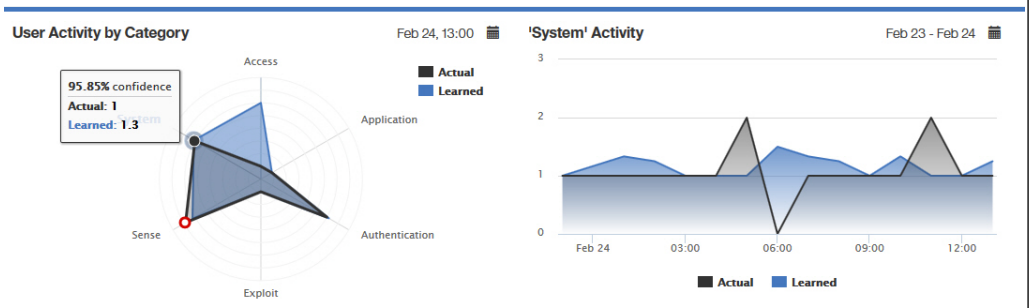
Página de detalhes do usuário

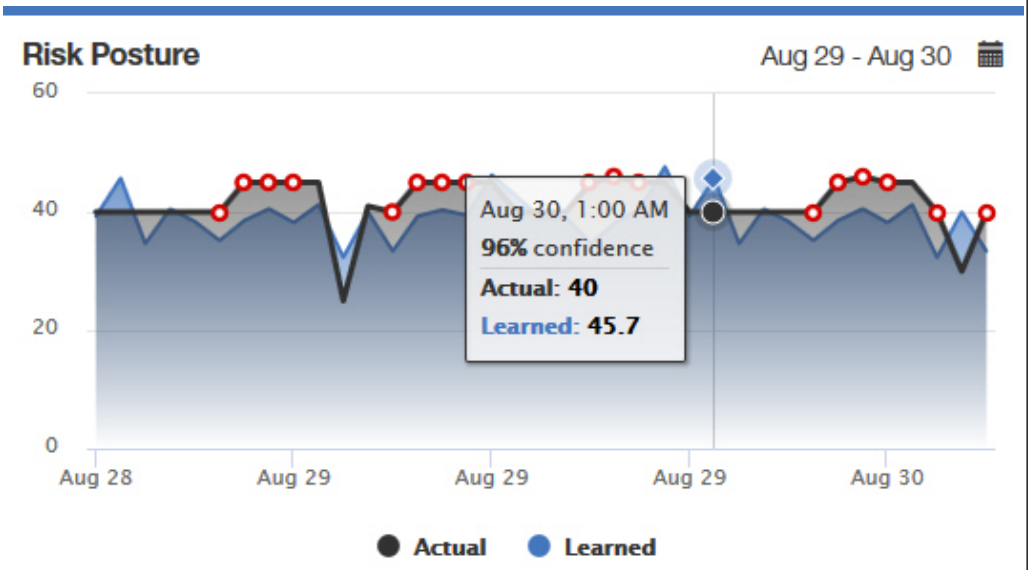
É possível clicar em um nome do usuário em qualquer lugar no aplicativo para ver detalhes para o usuário selecionado.

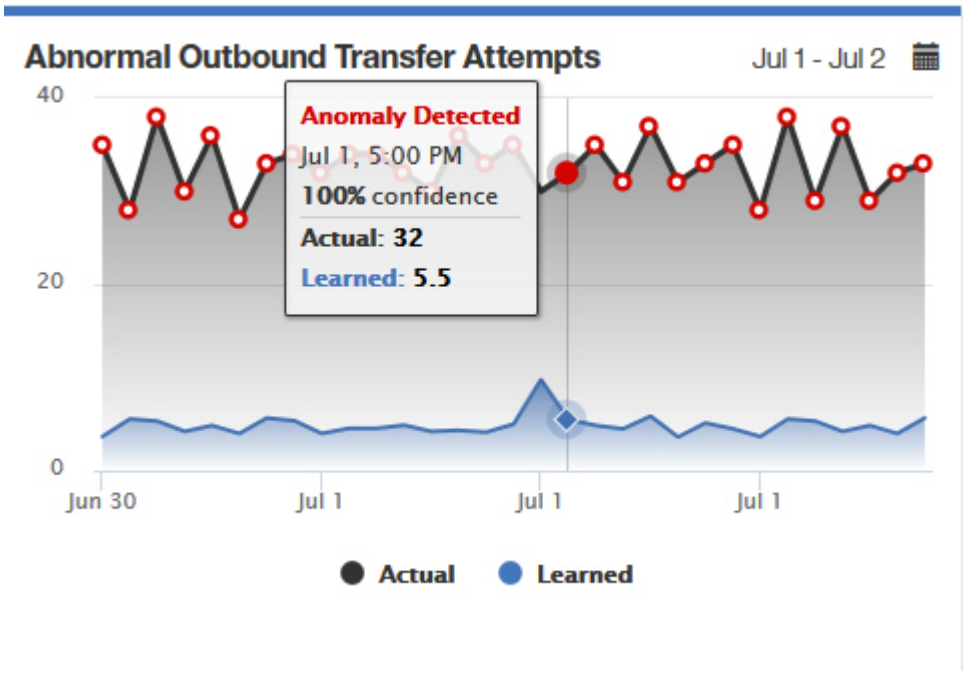
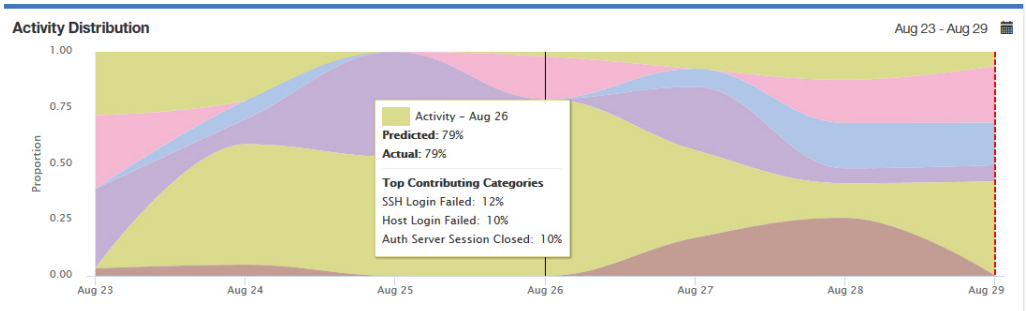
Iniciando com a V2.5.0, é possível aprender mais sobre as atividades do usuário com a área de janela *Visualizador de eventos*. A área de janela do visualizador de eventos mostra informações sobre uma atividade ou um momento selecionado. Clicar em um evento na área de janela visualizador de eventos revela mais detalhes, como eventos de syslog e informações de carga útil. A área de janela do visualizador de eventos está disponível para todos os gráficos de rosca e de linha na página Detalhes do Usuário.

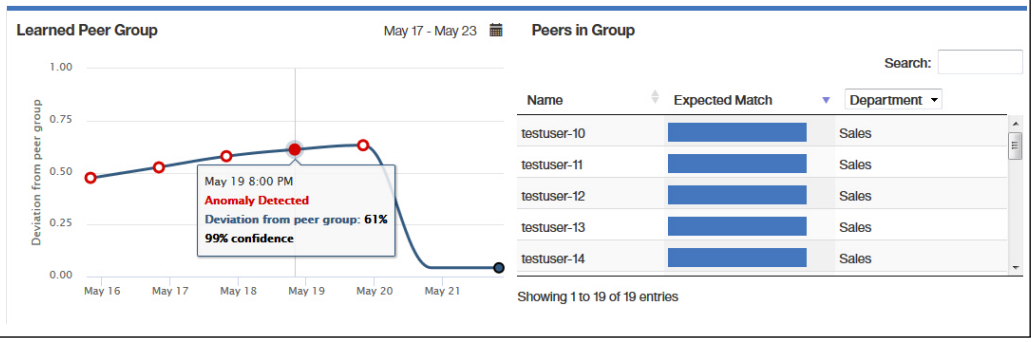
A tabela a seguir descreve os gráficos do Machine Learning Analytics disponíveis na página Detalhes do usuário.

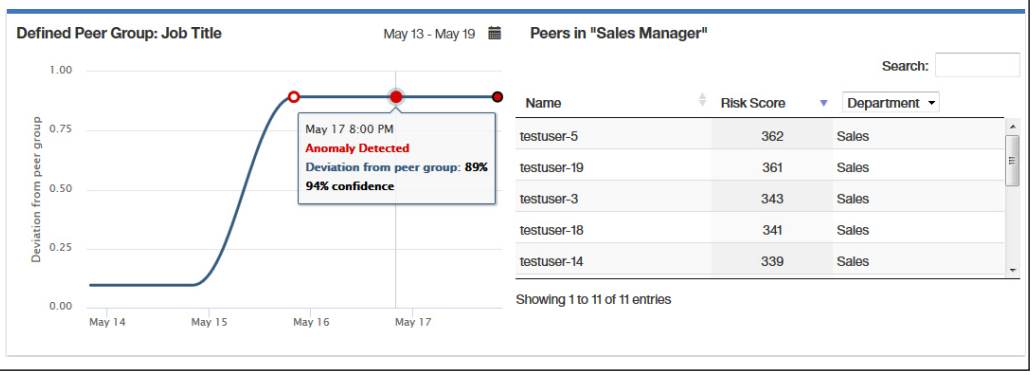
Atividade total	Mostra a quantidade real e a esperada (aprendida) de atividade de usuários durante todo o dia. Os valores reais são o número de eventos para esse usuário durante o período selecionado. Os valores esperados são o número de eventos preditos para esse usuário durante o período selecionado. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. No gráfico Atividade total, é possível: • Clique em um nó de dados e obtenha uma listagem de consulta dos eventos que compõem a anomalia. • Clique no ícone **Calendário** para especificar um intervalo de data customizado. 

Atividade do usuário por categoria	Mostra padrões de comportamento de atividade de usuário reais e esperados por categoria de alto nível. Os valores reais são o número de eventos por categoria de alto nível para esse usuário durante o período selecionado. Os valores esperados são o número predito de eventos por categoria de alto nível para esse usuário durante o período selecionado. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. No gráfico Atividade do usuário por categoria, é possível: • Clicar no ícone **Calendário** para especificar uma hora e uma data. • Clicar em uma categoria para abrir o gráfico de linha de tempo para a categoria selecionada. No gráfico de linha de tempo para a categoria selecionada, é possível: • Clicar em um nó de dados e obter uma listagem de consulta dos eventos que representam esse nó. • Clique no ícone **Calendário** para especificar um intervalo de data customizado. 

Variação de risco	Mostra se a pontuação de risco de um usuário se desvia do padrão de pontuação de risco esperado. Os valores reais são a soma dos valores de verificação para os eventos de verificação para esse usuário durante o período selecionado. Os valores esperados são a soma predita dos valores de verificação para os eventos de verificação para esse usuário durante o período selecionado. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. No gráfico Variação de risco, é possível: • Clique em um nó e obtenha uma listagem de consulta dos eventos. • Clique no ícone **Calendário** para especificar um intervalo de data customizado. 

Tentativas de Transferência de Saída Anormal	Mostra se um uso de tráfego de saída do usuário foi desviado de seu comportamento esperado. Os valores reais são o número de tentativas de transferência para esse usuário durante o período selecionado. Os valores aprendidos são o número previsto do modelo de tentativas de transferência. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. No gráfico de Tentativas de transferência de saída anormal, é possível: • Clique em um nó e obtenha uma listagem de consulta dos eventos. • Clique no ícone **Calendário** para especificar um intervalo de data customizado. 
Distribuição de atividades (V2.2.0 ou mais recente)	Mostra clusters de comportamento dinâmico para todos os usuários que são monitorados por aprendizado de máquina. Os clusters são inferidos pelas categorias de atividade de baixo nível para todos os usuários que são monitorados pelo aprendizado de máquina. Os valores reais são a correspondência de percentual para esse cluster. Os valores esperados são a correspondência de percentual predito para esse cluster. Cada cor no gráfico representa um cluster de comportamento dinâmico exclusivo para todos os usuários monitorados pelo aprendizado de máquina. Uma cor usada para denotar um grupo específico é a mesma para todos os usuários. Uma linha vertical vermelha indica que uma anomalia foi detectada e um evento de verificação foi gerado pelo aprendizado de máquina. No gráfico Distribuição de atividade, é possível: • Passar o mouse sobre cada cluster para visualizar os percentis real e predito de atividade e as 3 principais categorias de baixo nível de contribuição. • Clique no ícone **Calendário** para especificar um intervalo de data. 

Grupo de peers aprendido (V2.2.0 ou mais recente)	Mostra quanto o usuário se desviou do grupo de peers inferido no qual ele deveria estar. O Learned Peer Group é inferido pelas categorias de atividade de baixo nível para o usuário. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. **Desvio do grupo de peers** significa a porcentagem que um usuário desviou de seu grupo de peers inferido. **Confiança** é o percentil do desvio no contexto de dados históricos sobre os quais o modelo foi construído. Um alerta é acionado se o desvio e a confiança excederem seus limites. No gráfico do Learned Peer Group, é possível: • Clicar em um ponto de dados para visualizar a tabela Peers no grupo. • Clique no ícone **Calendário** para especificar um intervalo de data. A tabela Peers no grupo mostra todos os usuários que são esperados e que estão realmente no grupo. É possível: • Clique no nome de um usuário para abrir a página Detalhes do Usuário • **Correspondência esperada** mostra o quão confiante a analítica é para esse usuário estar no grupo • Clicar na lista suspensa para selecionar os atributos do usuário para exibição • Procurar para filtrar os nomes de usuários 

Defined Peer Group (V2.6.0 ou mais recente)	Mostra quanto a atividade de eventos de um usuário se desvia daquela de seu grupo de peers definido. A analítica usa as categorias de atividade de baixo nível de eventos dos usuários para determinar o desvio dos usuários do seu grupo de peers definido. Um círculo vermelho indica que uma anomalia foi detectada e um evento de verificação foi gerado por aprendizado de máquina. **Desvio do grupo de peers** significa a porcentagem que um usuário desviou de seu grupo de peers definido. **Confiança** é o percentil do desvio no contexto de dados históricos sobre os quais o modelo foi construído. Um alerta é acionado se o desvio e a confiança excederem seus limites. Para visualizar a analítica do Defined Peer Group, deve-se definir grupos de usuários. Para obter informações adicionais, consulte “Grupos de usuários para a analítica do Defined Peer Group”. No gráfico Defined Peer Group, é possível: • Clique em um ponto de dados para visualizar os Peers na tabela "o seu grupo de peers definido". • Clique no ícone **Calendário** para especificar um intervalo de data. Os Peers na tabela "o seu grupo de peers definido" mostram a você os usuários mais arriscados no grupo de usuários atual. É possível: • Clique no nome de um usuário para abrir a página Detalhes do Usuário • Clicar na lista suspensa para selecionar os atributos do usuário para exibição • Procurar para filtrar os nomes de usuários 

Grupos de usuários para a analítica do Defined Peer Group

É possível ativar a analítica do Defined Peer Group no aplicativo Machine Learning se o UBA estiver configurado para usar uma tabela de referência que contenha pelo menos dois agrupamentos com um mínimo de cinco usuários usando uma das seleções de Agrupar por.

Nota: Na V2.6.0 ou mais recente, é possível extrair grupos de usuários no UBA e ativar a analítica de Defined Peer Group.

As seleções de agrupamento são **Título da tarefa**, **Departamento** ou uma propriedade customizada que você define na página Configurações do UBA no campo **Grupo customizado** em Atributos de exibição. Quando o UBA detecta mais de dois grupos distintos com cinco ou mais usuários cada um, a analítica do Defined Peer Group pode ser ativada. Para ter grupos de usuários válidos, é possível configurar o aplicativo Reference Data Import LDAP para que as propriedades do usuário (Título da tarefa, Departamento ou outro agrupamento de atributos LDAP) possam ser extraídas como uma tabela de referência. É possível, então, configurar o UBA para usar a tabela de referência que você criou.

A analítica do Defined Peer Group pode monitorar até 20 grupos. Os maiores 20 grupos no campo **Agrupar por** são escolhidos. O número de usuários para monitorar é proporcionalmente reduzido de cada grupo para atender ao limite do usuário monitorado para o tamanho de instalação do seu Machine Learning.

Lembre-se: A importação da tabela de referência tem um planejamento de repetição de no mínimo 2 horas conforme configurado na página Configurações do UBA. Quaisquer novos atributos de agrupamento de usuário serão importados quando a execução da importação for planejada.

Desinstalando o aplicativo Machine Learning Analytics

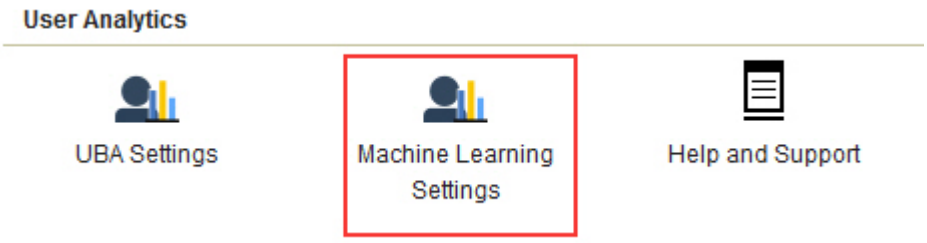
Desinstale o app Machine Learning Analytics na página Configurações do Machine Learning.

Sobre Esta Tarefa

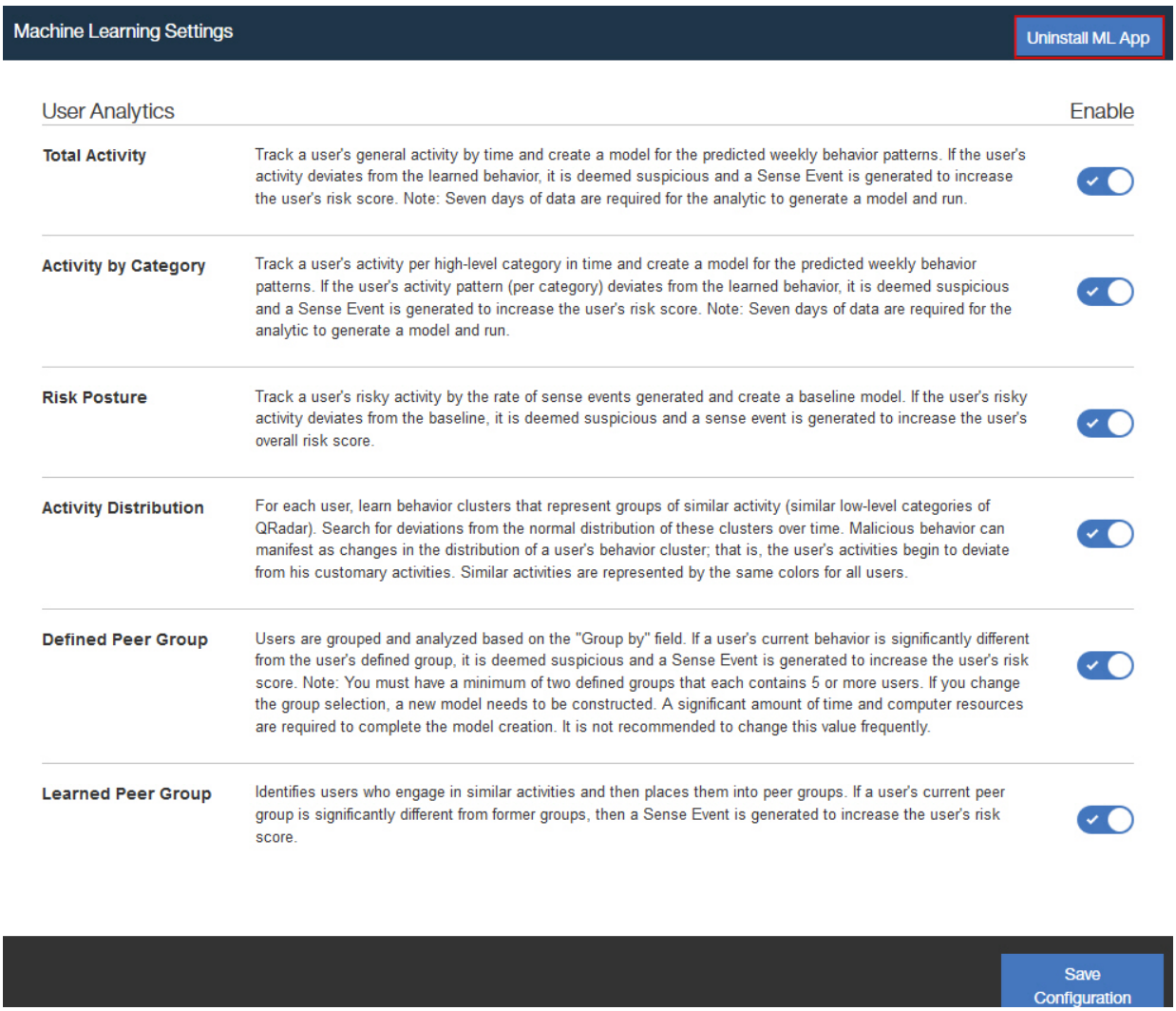
Antes de desinstalar o aplicativo UBA, deve-se concluir o procedimento a seguir para desinstalar o aplicativo ML. Se você não desinstala o aplicativo ML antes de desinstalar o UBA, deve removê-lo da interface da documentação da API interativa.

Procedimento

1. Abra as configurações de **Administrador**:
   - No IBM QRadar V7.3.0 ou anterior, clique na guia **Administrador**.
   - No IBM QRadar V7.3.1 e mais recente, clique no menu de navegação ( ) e, em seguida, clique em **Administrador** para abrir a guia Administrador.
2. Clique no ícone **Configurações de Machine Learning**.
   - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Análise do Usuário** > **Configurações de Machine Learning**.
   - No QRadar 7.3.1 ou posterior, clique em **Aplicativos** > **Análise do Usuário** > **Configurações de Machine Learning**.



3. Na tela Configurações do Machine Learning, clique em **Desinstalar app ML**.



4. No prompt de desinstalação, clique em **Sim**.

O que Fazer Depois

Deve-se limpar seu cache do navegador antes de se registrar novamente no console QRadar.

10 Resolução de problemas e suporte

Para isolar e resolver problemas com o seu produto IBM, é possível usar as informações de resolução de problemas e de suporte.

Para obter respostas a perguntas comuns de suporte sobre o aplicativo User Behavior Analytics e o aplicativo Machine Learning Analytics, veja https://developer.ibm.com/answers/topics/uba/

Página de Ajuda e suporte para UBA

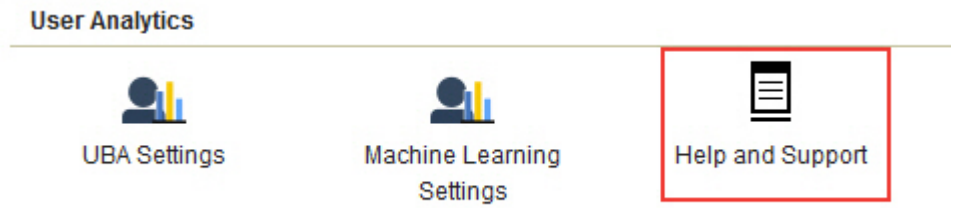
O app UBA (V2.5.0) inclui uma seção Ajuda e Suporte para usar o app UBA, o app LDAP e o app Machine Learning Analytics.

Acessando a página Ajuda e suporte para o UBA

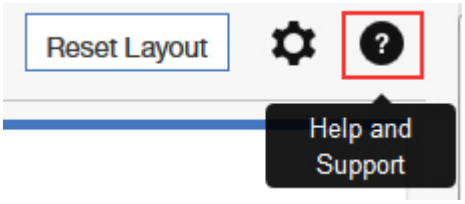
A página Ajuda e suporte fornece links para a documentação, resolução de problemas e suporte, tutoriais de vídeo, arquivos de log e funções administrativas. Deve-se ter privilégios de administrador do QRadar® para visualizar arquivos de log e concluir funções administrativas da página Ajuda e Suporte.

Após você instalar o aplicativo do UBA, será possível acessar a página Ajuda e suporte por meio dos locais a seguir:

- A partir das configurações do **Administrador** :
  - No QRadar V7.3.0 ou anterior, clique em **Plug-ins** > **Analítica do usuário** > **Ajuda e suporte**.
  - No QRadar 7.3.1 ou mais recente, clique em **Aplicativos** > **Analítica do usuário** > **Ajuda e suporte**.



- Na guia **Analítica do Usuário**, clique no ícone **Ajuda e Suporte**.



Funções Administrativas

Deve-se ter privilégios de administrador do QRadar® para visualizar arquivos de log e executar funções administrativas.

As funções administrativas incluem a capacidade de concluir as seguintes ações:

- Clicar em **Limpar dados do UBA** para remover todos os dados do usuário do UBA, mas manter todas as suas definições de configuração atuais do UBA. Limpar os dados do UBA faz com que o app UBA

se comporte como se você tivesse acabado de instalar e definir as **Configurações do UBA**. Se o app Machine Learning estiver instalado, o botão **Limpar dados do UBA** também reconfigurará o aplicativo ML.

- Clique em **Reconfigurar Configuração do ML** se o aplicativo de Machine Learning estiver instalado e você desejar reconfigurar todas as definições do Machine Learning e desativar todas as analíticas que estão ativadas.

Pedidos de Serviços

As solicitações de serviço também são conhecidas como Problem Management Records (PMRs).

Existem diversos métodos para enviar as informações de diagnóstico ao Suporte técnico de software IBM. Para abrir uma solicitação de serviço ou para trocar informações com o suporte técnico, visualize no Suporte de software IBM a página Trocando informações com o suporte técnico (http://www.ibm.com/software/support/exchangeinfo.html). As solicitações de serviço também podem ser enviadas diretamente usando a ferramenta de Solicitações de serviço (PMRs) (http://www.ibm.com/support/entry/portal/Open_service_request).

O status do app Machine Learning mostra um aviso no painel

Se o status de modelos do Machine Learning no painel do UBA mostrar mensagens de aviso, revise os procedimentos para resolver o problema.

Se o status dos modelos do Machine Learning mostrar **Modelo falhou ao construir** para uma analítica, será possível tentar as seguintes sugestões para resolver o problema:

- Consulte os logs de erros para o app ML.
- Verifique o espaço em disco no sistema que está executando o app Machine Learning.
- Verifique se o app UBA tem usuários com eventos.
- Entre em contato com o Suporte ao Cliente da IBM.

Conceitos relacionados:

"Extraindo os logs do UBA e do Machine Learning" na página 204
Use os arquivos de log do UBA e do Machine Learning para ajudar a solucionar problemas.

O status do app Machine Learning não mostra nenhum progresso para a ingestão de dados

Se o status dos modelos do Machine Learning no painel do UBA parecer estar preso durante a fase de ingestão de dados, revise o procedimento para resolver o problema.

Se o status dos modelos do Machine Learning não mostrar progresso para ingestão de dados para uma analítica, será possível tentar as seguintes sugestões para resolver o problema:

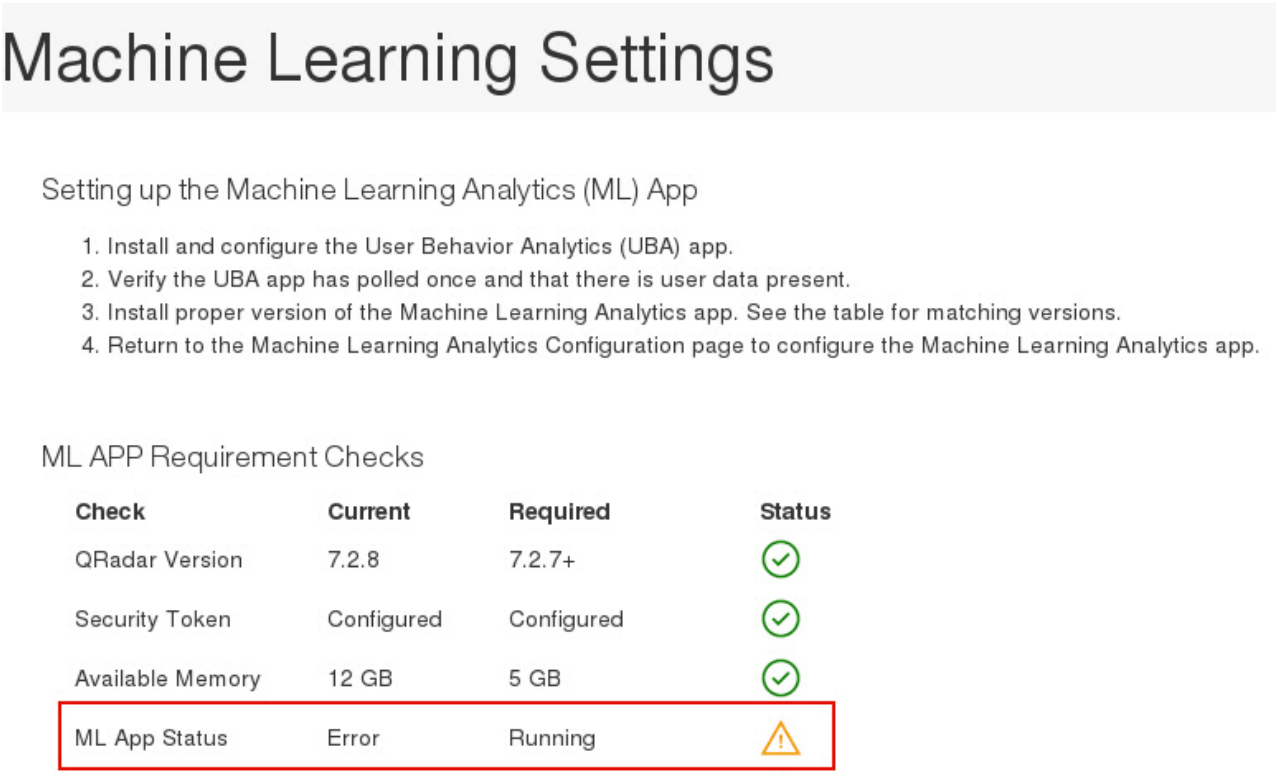
- Reinicie o serviço do Servidor Ariel
- Verifique o espaço em disco no sistema que executa o app Machine Learning.
- Verifique dentro do contêiner ML para ver se o processo **UBAController** está em execução.
- Entre em contato com o Suporte ao Cliente da IBM.

O status do aplicativo ML está em um estado de erro

Se a instalação do aplicativo Machine Learning Analytics (ML) falha e as Configurações de Machine Learning mostram um status de Erro, é possível usar a ferramenta de linha de comandos **cURL** e as configurações da Documentação da API para desinstalar o aplicativo ML.

Procedimento

Se o Status do aplicativo ML na página Configurações de Machine Learning mostra Erro, conclua o procedimento para desinstalar o app com falha.



Nota: Deve-se ter um token de autenticação válido. É possível ver a lista de tokens de autenticação configurados na seção Serviços autorizados nas configurações de Administrador do QRadar Console.

1. Usando SSH, efetue login no QRadar Console.
2. Execute o comando a seguir:

   # psql -U qradar -c 'select id,name,status from installed_application'

   Saída de Exemplo:

```
 id  |  name  |  status
-----+--------------------------------+---------
1356 | User Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. Localize e registre o valor *id* para o Machine Learning Analytics da saída do comando.
4. Usando um token de autenticação válido no lugar de <*valid token*> e o valor do ID registrado no lugar de <*id*>, execute o comando a seguir para desinstalar o aplicativo Machine Learning com falha: **# curl -k -H -X DELETE 'SEC:<valid token>' https://127.0.0.1/api/gui_app_framework/applications/<id>**

Removendo o aplicativo Machine Learning

Para remover o aplicativo Machine Learning usando a API gui_app_framework, conclua as etapas a seguir:

1. Abra o QRadar Console e navegue para a página de doc da API no local a seguir: https://<*host_address_port*>/api_doc

2. Abra a pasta para o maior número da versão da API (o número é diferente com base na versão do QRadar; por exemplo, 7.0 no QR 7.2.8).
3. Abra a pasta `/gui_app_framework` e, em seguida, `select /applications`.
4. Neste ponto, é necessário estar na **API GET**. Clique no botão **"Experimente!"** para obter a lista de aplicativos instalados.
5. Procure por `Machine Learning Analytics` nos resultados da etapa 4 e obtenha o valor de atributo `application_id`.
6. Expanda o menu `/applications` nos docs de API (mesmo local que na etapa 3), selecione a API `/application_id` e clique na guia **EXCLUIR**.
7. Insira o valor do ID do aplicativo da etapa 5 e, em seguida, clique no botão **"Experimente!"** para remover o aplicativo.
8. A API deve retornar um código de status HTTP 204 para indicar que o aplicativo foi removido com êxito.

Extraindo os logs do UBA e do Machine Learning

Use os arquivos de log do UBA e do Machine Learning para ajudar a solucionar problemas.

Fazendo download de arquivos de log do app

É possível fazer download facilmente de arquivos de log para o app UBA e o app Machine Learning no "Página de Ajuda e suporte para UBA" na página 201.

Arquivos de log do aplicativo UBA

Siga estas etapas para extrair manualmente os arquivos de log do app UBA do contêiner docker.

1. No host QRadar que está executando o UBA, navegue até um diretório que tenha espaço suficiente para criar um arquivo zip que inclua todos os arquivos de log do app.
2. Execute o comando a seguir:

   find /store/docker/v* -name uba.db
3. Copie o caminho do diretório que precede `uba.db`

   Por exemplo, no caminho do diretório a seguir
   /store/docker/volumes/qapp-1001/uba.db
   você copiaria
   /store/docker/volumes/qapp-1001/
4. Execute o comando a seguir, substituindo o caminho do diretório na etapa 1:

   zip -qr uba_logs.zip <your_path_here>log*

   Por
   exemplo:
   zip -qr uba_logs.zip /store/docker/volumes/qapp-1001/log*

Arquivos de log do aplicativo Machine Learning

Siga estas etapas para extrair manualmente os arquivos de log do app Machine Learning do contêiner docker.

1. No host QRadar que está executando o UBA, navegue até um diretório que tenha espaço suficiente para criar um arquivo zip que inclua todos os arquivos de log do app.
2. Execute o comando a seguir:

find /store/docker/v* -name itproot

3. Copie o caminho do diretório que precede `itproot`.

   Por exemplo, no caminho do diretório a seguir:
   /store/docker/volumes/qapp-1003/itproot
   você copiaria
   /store/docker/volumes/qapp-1003/

4. Execute o comando a seguir, substituindo o caminho do diretório na etapa 1:

   zip -qr ml_logs.zip <your_path_here>log*

   Por
   exemplo:
   zip -qr ml_logs.zip /store/docker/volumes/qapp-1003/log*

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licenças devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE MERCADO OU DE ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Todas as referências a websites não IBM contidas nestas informações são fornecidas apenas por conveniência e não representam, de forma alguma, um endosso a esses websites. Os materiais nesses websites não fazem parte dos materiais para este produto IBM e o uso desses websites é de inteira responsabilidade do Cliente.

A IBM pode usar ou distribuir as informações fornecidas da forma que julgar apropriada, sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Os exemplos de clientes e dados de desempenho citados são apresentados com propósitos meramente ilustrativos. Os resultados de desempenho reais podem variar, dependendo de configurações e condições operacionais específicas.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços dos revendedores podem variar.

Essas informações contêm exemplos de dados e relatórios utilizados em operações diárias de negócios. Para ilustrá-las da forma mais completa possível, os exemplos incluem os nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com pessoas ou empresas reais é mera coincidência.

Marcas registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corp., registradas em várias jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou outras empresas. Uma lista atual de marcas comerciais da IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Adobe, o logotipo Adobe, PostScript e o logotipo PostScript são marcas ou marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada de The Open Group nos Estados Unidos e em outros países.

Java™ e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou suas afiliadas.

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Termos e condições da documentação do produto

As permissões para uso destes documentos são concedidas de acordo com os termos e condições a seguir.

Aplicabilidade

Esses termos e condições são em adição a quaisquer termos de uso para o website da IBM.

utilizar o Personal

É possível reproduzir estas publicações para uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou fazer trabalho derivativo dessas publicações ou qualquer porção destas, sem o expresso consentimento da IBM.

Uso comercial

É possível reproduzir, distribuir e exibir estas publicações exclusivamente dentro de sua empresa desde que todos os avisos do proprietário sejam preservados. Você não pode fazer trabalhos derivativos dessas publicações ou reproduzir, distribuir ou exibir essas publicações ou qualquer parte destas fora da sua empresa, sem o expresso consentimento da IBM.

Direitas

Exceto conforme concedido expressamente nesta permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, às publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida aqui.

A IBM reserva-se o direito de retirar as permissões aqui concedidas sempre que, a seu critério, o uso das publicações for prejudicial aos seus interesses ou, conforme determinado pela IBM, as instruções acima não estiverem sendo seguidas adequadamente.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto se elas estiverem totalmente em conformidade com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação dos Estados Unidos.

A IBM NÃO FORNECE GARANTIA QUANTO AO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Declaração de Privacidade Online da IBM

Os produtos de software IBM, incluindo software como soluções de serviço (“Ofertas de software”), podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de software podem ajudá-lo a coletar informações de identificação pessoal. Se esta Oferta de software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de autenticação e gerenciamento de sessões. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, veja a Política de privacidade IBM em http://www.ibm.com/privacy e a Declaração de privacidade on-line da IBM em http://www.ibm.com/privacy/details, a seção intitulada "Cookies, web beacons e outras tecnologias", e a "Declaração de privacidade de produtos de software IBM e software como serviço" em http://www.ibm.com/software/info/product-privacy.

Regulamento Geral de Proteção de Dados

Os clientes são responsáveis por assegurar sua própria conformidade com várias leis e regulamentações, inclusive com a General Data Protection Regulation da União Europeia. Os clientes são unicamente responsáveis por obter consultoria jurídica competente quanto à identificação e interpretação de quaisquer leis e regulamentos relevantes que possam afetar seus negócios e de quaisquer ações que possam precisar tomar para estar em conformidade com tais leis e regulamentos. Os produtos, serviços e outros recursos descritos neste documento não são adequados para todas as situações dos clientes e podem ter disponibilidade restringida. A IBM não fornece assessoria jurídica, contábil ou de auditoria nem declara ou garante que seus serviços ou produtos irão assegurar que os clientes estejam em conformidade com qualquer lei ou regulamentação.

Para saber mais sobre a própria jornada de preparação do GDPR da IBM e os nossos recursos e ofertas do GDPR, veja as informações a seguir: https://ibm.com/gdpr.

Impresso no Brasil