IBM QRadar User Behavior Analytics(UBA) 앱

버전 3.2.0

사용자 안내서

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 239 페이지의 『주의사항』의 정보를 읽으십시오.

제품 정보

본 문서는 본 문서의 업데이트된 버전에서 달리 대체되지 않는 한 IBM QRadar Security Intelligence Platform V7.2.8 및 후속 릴리스에 적용됩니다.

목차

1 User Behavior Analytics for QRadar

User Behavior Analytics for QRadar 앱은 사용자가 네트워크 내부 사용자의 위험 프로파일을 판별하고 앱이 위협적인 작동을 경고하면 적절한 조치를 취할 수 있도록 도와줍니다.

User Behavior Analytics for QRadar(UBA) 앱은 조직의 내부자 위협을 탐지하는 데 필요한 도구입니다. QRadar에서 기존 데이터를 사용하여 사용자와 위험에 대한 새 인사이트를 생성하도록 앱 프레임워크의 맨 위에 빌드됩니다. UBA은 다음 두 가지 주요 기능을 QRadar에 추가합니다. 위험 프로파일링 및 통합된 사용자 ID.

위험 프로파일링은 다른 보안 유스 케이스에 위험을 지정하여 수행됩니다. 예제에는 올바르지 않은 웹 사이트 또는 기계 학습을 사용하는 보다 향상된 Stateful 분석과 같은 단순 룰과 검사가 포함될 수 있습니다. 위험은 발견된 인시던트의 심각도와 신뢰성에 따라 각각 지정됩니다. UBA는 이러한 인사이트와 사용자의 프로파일 위험을 생성하기 위해 사용자의 QRadar 시스템에서 기존 이벤트 및 플로우 데이터를 사용합니다. UBA은 세 가지 유형의 트래픽을 사용합니다. 1. 액세스, 인증 및 계정 변경사항에 따른 트래픽. 2. 네트워크에서의 사용자 동작(프록시, 방화벽, IPS, VPN프록시, 방화벽, IPS, VPN 등과 같은 디바이스). 3. Windows, Linux 및 SAAS 애플리케이션과 같은 엔드포인트와 애플리케이션 로그. 모든 세 가지 유형의 트래픽은 UBA를 강화하고 더 많은 유스 케이스를 사용하여 위험을 프로파일링합니다.

QRadar에서 사용자에 대한 서로 다른 계정을 결합하여 사용자 ID 통합이 수행됩니다. UBA는 Active Directory, LDAP 또는 CSV 파일에서 데이터를 가져와 사용자 ID에 속한 계정을 학습할 수 있습니다. 이는 UBA를 위한 QRadar에서 다른 사용자 이름 전체에 걸쳐 위험과 트래픽을 결합하는 데 도움이 됩니다.

Machine Learning(ML)은 UBA 앱을 보강하는 추가 도구입니다. 이를 통해 시계열 프로파일링 및 클러스터링을 수행하는 보다 다양하고 심도 깊은 유스 케이스를 사용할 수 있습니다. 기계 학습 설정 페이지의 UBA 앱 내부에서 설치됩니다. ML은 학습된 동작(모델), 현재 동작 및 경보를 표시하는 기존 UBA 앱에 더 많은 시각화를 추가합니다. 기계 학습은 사용자에게 예측 모델과 일반적인 기준선을 작성하기 위해 최대 4주 간의 QRadar의 히스토리 데이터를 사용합니다.

참조 데이터 가져오기 LDAP 앱 사용에 대한 자세한 정보는 191 페이지의 8, 『참조 데이터 가져오기 - LDAP 앱』의 내용을 참조하십시오.

Machine Learning Analytics 앱 사용에 대한 자세한 정보는 203 페이지의 9, 『Machine Learning Analytics 앱』의 내용을 참조하십시오.

주의: QRadar® UBA 앱을 설치하기 전에 IBM® QRadar V7.2.8 이상을 설치해야 합니다.

관련 개념:

51 페이지의 7, 『UBA 앱에 대한 룰 및 튜닝』
IBM QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

25 페이지의 『User Behavior Analytics 앱 구성』
IBM QRadar User Behavior Analytics(UBA) 앱을 사용할 수 있으려면 먼저 추가 설정을 구성해야 합니다.

191 페이지의 8, 『참조 데이터 가져오기 - LDAP 앱』
참조 데이터 가져오기 - LDAP 앱을 사용하여 여러 LDAP 소스의 컨텍스트 ID 정보를 QRadar Console에 수집합니다.

203 페이지의 9, 『Machine Learning Analytics 앱』
Machine Learning Analytics(ML) 앱은 기계 학습 분석에 대한 유스 케이스를 추가하여 QRadar User Behavior Analytics(UBA) 앱 및 QRadar 시스템의 기능을 확장합니다. Machine Learning Analytics 유스 케이스를 사용하면 예측 모델링을 통해 사용자 행위패턴에 대한 추가적인 통찰을 얻을 수 있습니다. ML 앱을 통해 네트워크에 있는 사용자의 예상 행위패턴을 파악할 수 있습니다.

관련 태스크:

19 페이지의 『User Behavior Analytics 앱 설치』
IBM QRadar 확장 관리 도구를 사용하여 QRadar Console에 직접 앱 아카이브를 업로드하고 설치합니다.

23 페이지의 『User Behavior Analytics 앱 업그레이드』
IBM QRadar 확장 관리 도구를 사용하여 앱을 업그레이드합니다.

User Behavior Analytics 앱의 새로운 기능

각 User Behavior Analytics(UBA) 앱 릴리스의 새 기능에 대해 알아봅니다.

V3.2.0의 새로운 기능

- 대시보드 및 사용자 프로파일 페이지에서 비활성 계정이 있는 사용자를 식별합니다. 추가 정보는 44 페이지의 『비활성 계정』의 내용을 참조하십시오.
- 누락된 사용자 특성을 기반으로 서비스 계정의 관심 목록을 작성합니다. 추가 정보는 39 페이지의 『관심 목록 작성』의 내용을 참조하십시오.
- UBA에서 사용할 LDAP 속성을 선택할 수 있도록 LDAP 앱이 향상되었습니다. 참고: LDAP을 구성할 때 이제 속성 맵핑 섹션에서 외부 키를 선택해야 합니다. 추가 정보는 25 페이지의 『참조 데이터 가져오기 LDAP 앱 구성』의 내용을 참조하십시오.
- CSV 파일에서 사용자 정보를 가져올 수 있는 기능이 추가되었습니다. 추가 정보는 192 페이지의 『CSV 파일에서 사용자 데이터 가져오기』의 내용을 참조하십시오.
- UBA : User Access from Multiple Hosts 유스 케이스가 추가되었습니다. 추가 정보는 68 페이지의 『UBA : User Access from Multiple Hosts』의 내용을 참조하십시오.

- UBA : Possible Directory Services Enumeration 유스 케이스가 추가되었습니다. 추가 정보는 113 페이지의 『UBA : Possible Directory Services Enumeration』의 내용을 참조하십시오.
- UBA : Possible SMB Session Enumeration on a Domain Controller 유스 케이스가 추가되었습니다. 추가 정보는 114 페이지의 『UBA : Possible SMB Session Enumeration on a Domain Controller』의 내용을 참조하십시오.
- UBA : Suspicious Access Followed by Data Exfiltration 유스 케이스가 추가되었습니다. 추가 정보는 132 페이지의 『UBA : Suspicious Access Followed by Data Exfiltration』의 내용을 참조하십시오.
- UBA : Dormant Account Use Attempted 유스 케이스가 추가되었습니다. 추가 정보는 87 페이지의 『UBA : Dormant Account Use Attempted』의 내용을 참조하십시오.

V3.1.0의 새로운 기능

- 이제 사용자 타임라인에서 지표의 표시장치를 사용자 정의하고 지표를 구성하는 데이터를 볼 수 있습니다.
- 동적 위험 임계값을 설정하는 기능이 추가되었습니다.
- 룰 및 튜닝 페이지에 두 개의 새 유스 케이스(클라우드 및 도메인 컨트롤러) 카테고리가 추가되었습니다. 추가 정보는 51 페이지의 7, 『UBA 앱에 대한 룰 및 튜닝』의 내용을 참조하십시오.
- UBA : Non-Standard User Accessing AWS Resources 유스 케이스가 추가되었습니다. 추가 정보는 108 페이지의 『UBA : Non-Standard User Accessing AWS Resources』의 내용을 참조하십시오.
- UBA : AWS Console Accessed by Unauthorized User 유스 케이스가 추가되었습니다. 추가 정보는 107 페이지의 『UBA : AWS Console Accessed by Unauthorized User』의 내용을 참조하십시오.
- UBA : Replication Request from a Non-Domain Controller 유스 케이스가 추가되었습니다. 추가 정보는 116 페이지의 『UBA : Replication Request from a Non-Domain Controller』의 내용을 참조하십시오.
- UBA : Kerberos Account Enumeration Detected 유스 케이스가 추가되었습니다. 추가 정보는 109 페이지의 『UBA : Kerberos Account Enumeration Detected』의 내용을 참조하십시오.
- UBA : Possible TGT PAC Forgery 유스 케이스가 추가되었습니다. 추가 정보는 115 페이지의 『UBA : Possible TGT PAC Forgery』의 내용을 참조하십시오.
- UBA : DPAPI Backup Master Key Recovery Attempted 유스 케이스가 추가되었습니다. 추가 정보는 109 페이지의 『UBA : DPAPI Backup Master Key Recovery Attempted』의 내용을 참조하십시오.
- UBA : DoS Attack by Account Deletion 유스 케이스가 추가되었습니다. 추가 정보는 82 페이지의 『UBA : DoS Attack by Account Deletion』의 내용을 참조하십시오.
- UBA : Multiple Blocked File Transfers Followed by a File Transfer 유스 케이스가 추가되었습니다. 추가 정보는 129 페이지의 『UBA : Multiple Blocked File Transfers Followed by a File Transfer』의 내용을 참조하십시오.

V3.0.1의 새로운 기능

- IBM QRadar DNS Analyzer 앱을 통한 DNS 터널링 발견을 지원하는 유스 케이스가 추가되었습니다. 자세한 정보는 156 페이지의 『UBA : Potential Access to Tunneling Domain』의 내용을 참조하십시오.
- 참조 테이블에서 사용자를 유입할 수 없게 하는 문제를 수정했습니다.

V3.0.0의 새로운 기능

- 이제 사용자 정의 사용자 그룹을 모니터할 수 있도록 관심 목록을 작성하고 관리할 수 있습니다. 추가 정보는 39 페이지의 『관심 목록 작성』의 내용을 참조하십시오.
- 이제 새 룰 및 튜닝 페이지를 사용하여 UBA 유스 케이스를 보고 필터링하고 튜닝할 수 있습니다. 추가 정보는 51 페이지의 7, 『UBA 앱에 대한 룰 및 튜닝』의 내용을 참조하십시오.
- 이제 활동의 세션별로 사용자 활동 타임라인에서 위험한 이벤트 및 지표를 볼 수 있습니다. 추가 정보는 12 페이지의 『UBA 대시보드 및 사용자 세부사항』의 내용을 참조하십시오.
- 외부 도메인에 대한 비정상 데이터 볼륨을 발견하는 기계 학습 분석이 추가되었습니다. 추가 정보는 215 페이지의 『외부 도메인에 대한 비정상 데이터 볼륨 분석 구성』의 내용을 참조하십시오.
- UBA : Large Outbound Transfer by High Risk User 유스 케이스가 추가되었습니다. 추가 정보는 129 페이지의 『UBA : Large Outbound Transfer by High Risk User』의 내용을 참조하십시오.
- UBA : Honeytoken Activity 유스 케이스가 추가되었습니다. 추가 정보는 151 페이지의 『UBA : Honeytoken Activity』의 내용을 참조하십시오.
- UBA : Bruteforce Authentication Attempts 유스 케이스가 추가되었습니다. 추가 정보는 52 페이지의 『UBA : Bruteforce Authentication Attempts』의 내용을 참조하십시오.
- UBA : User Account Created and Deleted in a Short Period of Time 유스 케이스가 추가되었습니다. 추가 정보는 86 페이지의 『UBA : User Account Created and Deleted in a Short Period of Time』의 내용을 참조하십시오.
- UBA : High Risk User Access to Critical Asset 유스 케이스가 추가되었습니다. 추가 정보는 56 페이지의 『UBA : High Risk User Access to Critical Asset』의 내용을 참조하십시오.
- UBA : Anomalous Account Created From New Location 유스 케이스가 추가되었습니다. 추가 정보는 133 페이지의 『UBA : Anomalous Account Created From New Location』의 내용을 참조하십시오.
- UBA : Anomalous Cloud Account Created From New Location 유스 케이스가 추가되었습니다. 추가 정보는 138 페이지의 『UBA : Anomalous Cloud Account Created From New Location』의 내용을 참조하십시오.

V2.8.0의 새로운 기능

- 이제 기계 학습 분석 설정을 구성하는 경우 **고급 검색 필터** 필드를 사용하여 AQL 조회로 필터링할 수 있습니다. 추가 정보는 207 페이지의 『Machine Learning Analytics 설정 구성』의 내용을 참조하십시오.

- 이제 이벤트에서 발견된 사용자와 디렉토리에서 가져온 사용자에 대한 대시보드 통계를 볼 수 있습니다. 추가 정보는 12 페이지의 『UBA 대시보드 및 사용자 세부사항』의 내용을 참조하십시오.
- 기계 학습으로 추적하려는 사용자를 이제 지정할 수 있습니다. 추가 정보는 12 페이지의 『UBA 대시보드 및 사용자 세부사항』의 내용을 참조하십시오.
- 각 기계 학습 분석에 대한 그래프를 표시할지 여부를 구성할 수 있습니다. 추가 정보는 207 페이지의 『Machine Learning Analytics 설정 구성』의 내용을 참조하십시오.
- 이제 UBA 컨텐츠 패키지(QRadar 룰, 사용자 정의 특성 및 유스 케이스의 참조 데이터)를 설치하거나 업그레이드를 할지 여부를 구성할 수 있습니다. 추가 정보는 32 페이지의 『컨텐츠 패키지 설정 구성』의 내용을 참조하십시오.
- 비정상 아웃바운드 전송 시도를 발견할 수 있는 기계 학습 분석이 추가되었습니다. 추가 정보는 209 페이지의 『비정상 아웃바운드 전송 시도 분석 구성』의 내용을 참조하십시오.
- 앱 노드에서 Machine Learning을 사용하여 UBA를 실행하는 경우, 추가 사용자를 지원하는 기계 학습 메모리 구성이 추가되었습니다.
- 고위험 사용자를 식별하는 참조 세트가 추가되었습니다. 추가 정보는 50 페이지의 『참조 세트』의 내용을 참조하십시오.
- 찾아보기된 웹 사이트(비즈니스/서비스, LifeStyle 및 카테고리화되지 않음) 카테고리에 대한 유스 케이스가 추가되었습니다. 추가 정보는 99 페이지의 『찾아보기 동작』의 내용을 참조하십시오.
- UBA : Network Share Accessed 유스 케이스가 추가되었습니다. 추가 정보는 175 페이지의 『UBA : Network Share Accessed』의 내용을 참조하십시오.
- UBA : Non-Admin Access to Domain Controller 유스 케이스가 추가되었습니다. 추가 정보는 110 페이지의 『UBA : Non-Admin Access to Domain Controller』의 내용을 참조하십시오.
- UBA : User Access from Prohibited Location 유스 케이스가 추가되었습니다. 추가 정보는 141 페이지의 『UBA : User Access from Prohibited Location』의 내용을 참조하십시오.
- UBA : User Access from Restricted Location 유스 케이스가 추가되었습니다. 추가 정보는 124 페이지의 『UBA : Restricted Program Usage』의 내용을 참조하십시오.
- UBA : Multiple Kerberos Authentication Failures from Same User 유스 케이스가 추가되었습니다. 추가 정보는 110 페이지의 『UBA : Multiple Kerberos Authentication Failures from Same User』의 내용을 참조하십시오.
- UBA : TGT Ticket Used by Multiple Hosts 유스 케이스가 추가되었습니다. 추가 정보는 116 페이지의 『UBA : TGT Ticket Used by Multiple Hosts』의 내용을 참조하십시오.

V2.7.0의 새로운 기능

주의: V2.7.0으로 업그레이드하는 경우 http://www.ibm.com/support/docview.wss?uid=swg22005489 기술 노트의 지시사항을 완료해야 합니다.

User Behavior Analytics 앱의 V2.7.0에 포함된 새 기능은 다음과 같습니다.

- QRadar Advisor with Watson 앱에서 사용자를 조사할 수 있습니다. 참고: QRadar Advisor with Watson V1.13.0이 설치되어 있어야 합니다. 추가 정보는 16 페이지의 『QRadar Advisor with Watson에서 사용자 조사』의 내용을 참조하십시오.
- 이제 사용자에 대한 GDPR(General Data Protection Regulation) 준수 보고서를 생성하고 사용자 추적을 중지할 수 있습니다.
- 사용자의 검사 상태를 표시할 수 있으며 **사용자 분석** 대시보드에서 조사 중인 모든 사용자를 볼 수 있습니다.
- IP 주소의 국가 및 지역 플래그 표시 여부를 구성할 수 있습니다.
- IBM QRadar DNS Analyzer 앱에서 생성한 도메인 액세스 이벤트에 대한 지원이 추가되었습니다. 추가 정보는 154 페이지의 『QRadar DNS Analyzer』의 내용을 참조하십시오.
- 19개의 비정상 스캐닝 유스 케이스가 새로 추가되었습니다. 추가 정보는 163 페이지의 『탐색』의 내용을 참조하십시오.
- 3개의 의심스러운 애플리케이션 유스 케이스가 새로 추가되었습니다. 추가 정보는 117 페이지의 『엔드포인트』의 내용을 참조하십시오.
- 10개의 위험 찾아보기 유스 케이스가 새로 추가되었습니다. 추가 정보는 99 페이지의 『찾아보기 동작』의 내용을 참조하십시오.
- 13개의 시스템 모니터링(Sysmon) 유스 케이스가 새로 추가되었습니다. 추가 정보는 173 페이지의 『시스템 모니터링(Sysmon)』의 내용을 참조하십시오.

V2.6.0의 새로운 기능

주의: V2.6.0으로 업그레이드하는 경우 http://www.ibm.com/support/docview.wss?uid=swg22005489 기술 노트의 지시사항을 완료해야 합니다.

User Behavior Analytics 앱의 V2.6.0에는 다음과 같은 새 기능이 포함되어 있습니다.

- LDAP 및 Active Directory에서 정의된 피어 그룹을 기반으로 비정상을 분석하도록 Machine Learning Analytics(ML) 앱이 확장되었습니다.
- ML 앱의 피어 그룹 분석이 학습된 피어 그룹이라는 이름으로 바뀌었습니다.
- 추가된 유스 케이스: UBA : Process Executed Outside Gold Disk Whitelist(Windows/Linux)
- 추가된 유스 케이스: UBA : Ransomware Behavior Detected
- 추가된 유스 케이스: UBA : Netcat Process Detection(Windows/Linux)
- 추가된 유스 케이스: UBA : Multiple VPN Accounts Failed Login from Single IP
- 추가된 유스 케이스: UBA : Volume Shadow Copy Created
- 추가된 유스 케이스: UBA : Detect Insecure Or Non-Standard Protocol
- 추가된 유스 케이스: UBA : Malware Activity - Registry Modified In Bulk
- 추가된 유스 케이스: UBA : Internet Settings Modified
- 추가된 유스 케이스: UBA : Multiple VPN Accounts Logged In from Single IP

- 추가된 유스 케이스: UBA : Suspicious PowerShell Activity(Asset)
- 추가된 유스 케이스: UBA : Suspicious PowerShell Activity
- 추가된 유스 케이스: UBA : Suspicious Command shell Activity
- 추가된 유스 케이스: UBA : Malicious Process Detected

V2.5.0의 새로운 기능

주의: V2.5.0으로 업그레이드하는 경우 http://www.ibm.com/support/docview.wss?uid=swg22005489 기술 노트의 지시사항을 완료해야 합니다.

User Behavior Analytics 앱의 V2.5.0에는 다음 개선사항이 포함되어 있습니다.

- 인라인 컨텍스트 이벤트 뷰어를 사용하여 사용자의 위험한 작동을 신속하게 조사하는 기능이 추가되었습니다. 추가 정보는 12 페이지의 『UBA 대시보드 및 사용자 세부사항』의 내용을 참조하십시오.
- 문서, 학습서 및 지원 정보에 대한 링크를 제공하고 관리 기능도 제공하는 도움말 및 지원 페이지가 추가되었습니다. 추가 정보는 233 페이지의 『UBA에 대한 도움말 및 지원 페이지』의 내용을 참조하십시오.
- Machine Learning에 대한 정확도와 확장성이 증가되었으며 대시보드의 Machine Learning 모델 상태 섹션에서 메시징 기능이 개선되었습니다. 추가 정보는 224 페이지의 『Machine Learning Analytics가 있는 UBA 대시보드』의 내용을 참조하십시오.
- UBA : User Running New Process 유스 케이스가 추가되었습니다. 추가 정보는 126 페이지의 『UBA : User Running New Process』의 내용을 참조하십시오.
- UBA : User Installing Suspicious Application 유스 케이스가 추가되었습니다. 추가 정보는 125 페이지의 『UBA : User Installing Suspicious Application』의 내용을 참조하십시오.
- UBA : Unix/Linux System Accessed With Service or Machine Account 유스 케이스가 추가되었습니다. 추가 정보는 63 페이지의 『UBA : Unix/Linux System Accessed With Service or Machine Account』의 내용을 참조하십시오.
- UBA : User Access to Internal Server From Jump Server 유스 케이스가 추가되었습니다. 추가 정보는 70 페이지의 『UBA : User Access to Internal Server From Jump Server』의 내용을 참조하십시오.
- UBA : Executive Only Asset Accessed by Non-Executive User 유스 케이스가 추가되었습니다. 추가 정보는 54 페이지의 『UBA : Executive Only Asset Accessed by Non-Executive User』의 내용을 참조하십시오.

V2.4.0의 새로운 기능

주의: V2.4.0으로 업그레이드하는 경우 http://www.ibm.com/support/docview.wss?uid=swg22005489 기술 노트의 지시사항을 완료해야 합니다.

User Behavior Analytics 앱의 V2.4.0에는 다음 개선사항이 포함되어 있습니다.

- LDAP 앱에 LDAP 검색 상태가 표시됩니다.
- LDAP 앱을 통해 최대 400,000명의 사용자를 가져옵니다. 구성을 변경하기 전에 알려진 문제점을 참조하십시오.
- LDAP/AD 데이터의 통합과 맵핑이 단순화되었습니다.
- 기본 사용자 ID에 별명을 무제한으로 맵핑할 수 있습니다.
- 앱 노드에서 Machine Learning을 실행하는 경우 추가 사용자를 지원하기 위해 Machine Learning 설정에 메모리 구성 설정이 추가되었습니다.
- 피드백 설문조사가 추가되었습니다.
- UBA : Windows access with Service or Machine Account 유스 케이스가 추가되었습니다. 추가 정보는 78 페이지의 『UBA : Windows Access with Service or Machine Account』의 내용을 참조하십시오.
- UBA : D/DoS Attack Detected 유스 케이스가 추가되었습니다. 추가 정보는 149 페이지의 『UBA : D/DoS Attack Detected』의 내용을 참조하십시오.
- UBA : Detect Persistent SSH session 유스 케이스가 추가되었습니다. 추가 정보는 118 페이지의 『UBA : Detect Persistent SSH session』의 내용을 참조하십시오.
- UBA : Abnormal data volume to external domain 유스 케이스가 추가되었습니다. 추가 정보는 127 페이지의 『UBA : Abnormal data volume to external domain(ADE 룰)』의 내용을 참조하십시오.
- UBA : Abnormal Outbound Attempts 유스 케이스가 추가되었습니다. 추가 정보는 128 페이지의 『UBA : Abnormal Outbound Transfer Attempts(ADE 룰)』의 내용을 참조하십시오.

알려진 문제점

User Behavior Analytics 앱에는 업그레이드를 위한 필수 정보 및 알려진 문제점이 있습니다.

참고: ADE 룰을 사용하면 UBA 앱과 QRadar시스템의 성능에 영향을 미칠 수 있습니다.

V3.2.0의 알려진 문제점

User Behavior Analytics 앱에는 다음과 같은 알려진 문제점이 있습니다.

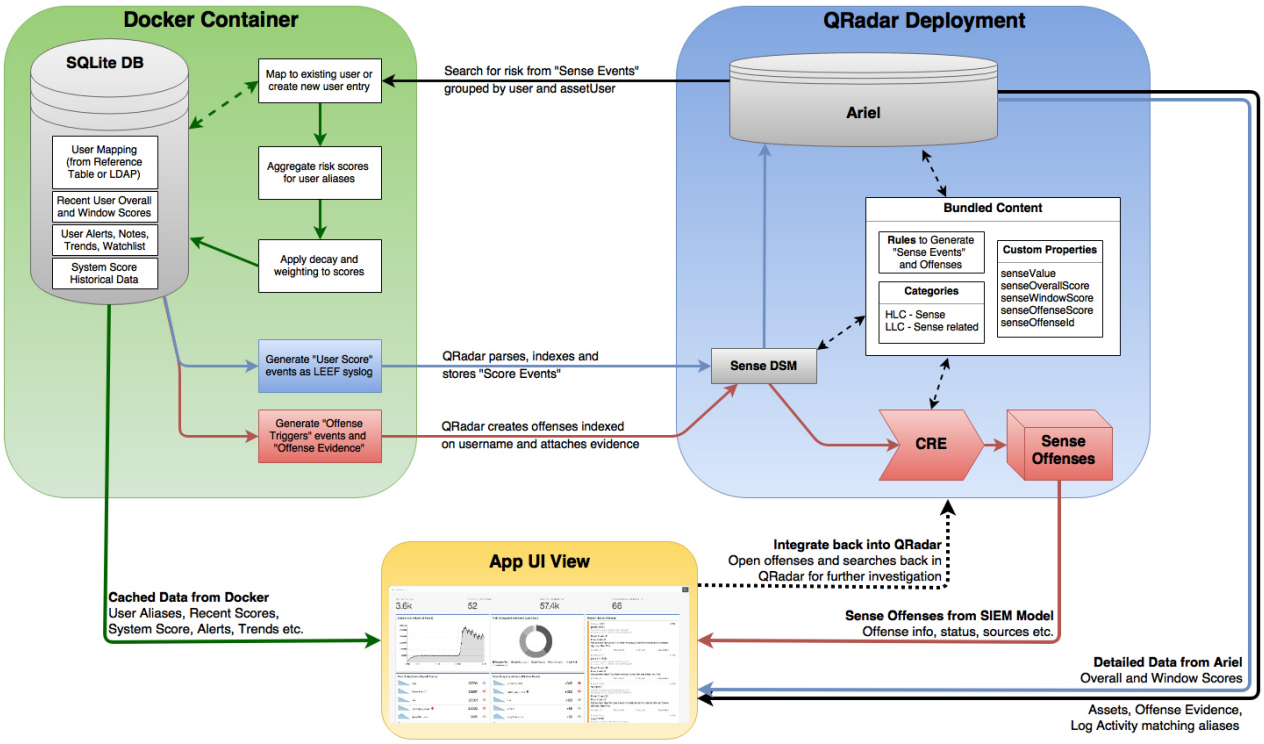
- QRadar 7.2.8 패치 13, QRadar 7.2.8 패치 13 IF1, QRadar 7.3.1 패치 3 또는 QRadar 7.3.1 패치 4에서 실행 중인 경우 참조 테이블에서의 사용자 통합으로 UBA 사용자 레코드에 불완전한 사용자 정보가 생성됩니다. 이 문제점은 V7.3.1 패치 4 IF1에서 해결되었습니다. 자세한 정보는 APAR IJ06032를 참조하십시오.
- UBA 앱을 업그레이드하는 중에 룰 세트 로드에 실패했음을 알리는 QRadar 알림 예외 오류를 수신하는 경우 이 오류를 무시하고 업그레이드를 계속할 수 있습니다. 오류가 지속되는 경우 IBM 고객 지원 부서에 문의하십시오.
- QRadar V7.2.8 패치 12 및 QRadar V7.3.1 패치 3의 알려진 문제점으로 인해 QRadar V7.2.8 패치 13 및 QRadar V7.3.1 패치 4로 업그레이드해야 합니다.

- UBA를 V3.2.0으로 업그레이드하고 나면 사용자 세부사항 페이지의 Machine Learning 활동 분포 그래프가 표시되는 데 최대 하루가 걸릴 수 있습니다.
- 사용자 프로파일 페이지를 볼 때 **화이트리스트에 추가** 단추가 표시되지 않을 수 있습니다. 이 경우 페이지를 새로 고쳐서 문제를 해결할 수 있습니다.
- 100,000명을 초과하는 사용자를 UBA용 LDAP으로 가져오는 것은 QRadar 시스템과 UBA 앱 설치에 심각한 영향을 줄 수 있습니다. 이 문제는 APAR IV98655의 알려진 문제로 인해 발생합니다. 128GB 콘솔에서 QRadar 7.3.0 이상을 사용하지 않는 한, 200,000명을 초과하는 사용자를 가져오는 것은 권장하지 않습니다.
- 간혹 QRadar V7.2.8 및 V7.3.0에서 새로 작성된 SEC 토큰이 작동하는 것처럼 보이지만 나중에 올바르지 않게 되는 SEC 토큰 관련 문제가 발생할 수 있습니다. 이 문제를 수정하려면 다음 조치 중 하나를 완료하십시오.
  - QRadar Console의 명령행에서 Apache Tomcat 서비스를 다시 시작하십시오.
  - QRadar의 관리 탭에서 조치를 배치하십시오.
- 시스템 점수 그래프에서 이틀 이상의 날짜 범위를 선택하고 현재 날짜로 종료 날짜를 선택하면 처음 8개의 데이터 점은 0으로 표시됩니다.
- QRadar V7.2.8을 사용하는 경우 일부 로케일에서 사용자 인터페이스의 일부분에 영문 문자열 또는 손상된 텍스트가 표시됩니다.

프로세스 개요

User Behavior Analytics 앱은 QRadar 시스템과 함께 작동하여 네트워크 내부의 사용자에 대한 데이터를 수집합니다.

UBA 작동 방식



1. 로그는 QRadar에 데이터를 전송합니다.
2. UBA 특정 룰이 특정 이벤트를 검색하고(사용으로 설정된 UBA 룰에 따라) UBA 앱이 읽은 새 감지 데이터를 트리거합니다.
3. UBA 룰을 사용하려면 이벤트에 사용자 이름 및 기타 테스트가 있어야 합니다(룰이 검색하는 항목을 확인하려면 룰을 검토하십시오).
4. UBA는 감지 이벤트에서 *senseValue*와 사용자 이름을 가져온 다음 *senseValue* 크기만큼 해당 사용자의 위험성 점수를 증가시킵니다.
5. 사용자의 위험성 점수가 UBA 설정 페이지에 설정된 임계값을 초과하면 UBA에서 "UBA : Create Offense" 룰을 트리거하는 이벤트를 전송하고 해당 사용자에 대한 오펜스가 작성됩니다.

위험성 점수

위험성 점수는 UBA 룰에 의해 발견된 모든 위험 이벤트의 합계입니다.위험성 점수가 높을수록 내부 사용자가 보안 위험이 될 가능성이 높아지며 사용자의 네트워크 활동에 대한 추가 검토가 필요하게 됩니다. 새로운 이벤트가 발생하지 않으면 위험성 점수는 시간이 지남에 따라 감소합니다. 감소량은 UBA 설정 페이지의 **시간당 이 인수 단위로 위험 감소**의 값에 의해 제어됩니다.

senseValues가 사용자 위험성 점수를 작성하는 데 사용되는 방식

각각의 룰 및 분석에는 발견된 문제의 심각도를 표시하는 값이 지정되어 있습니다. 사용자의 조치로 인해 룰이 트리거될 때마다 사용자의 점수에는 이 값이 추가됩니다. 사용자가 룰을 더 많이 "위반"할수록 점수는 더 높아집니다.

룰 및 감지 이벤트

룰은 트리거되면 사용자의 위험성 점수를 판별하는 데 사용되는 감지 이벤트를 생성합니다.

QRadar의 기존 룰을 업데이트하여 감지 이벤트를 작성할 수 있습니다. 추가 정보는 49 페이지의 『기존 또는 새 QRadar 컨텐츠를 UBA 앱과 통합』의 내용을 참조하십시오.

Machine Learning Analytics 및 감지 이벤트

Machine Learning Analytics 앱을 설치하고 기계 학습 분석을 사용으로 설정하여 비정상적인 사용자 행위패턴을 식별할 수 있습니다. 분석은 트리거되는 경우 사용자의 위험성 점수도 높이는 감지 이벤트를 생성합니다.

비디오 데모 및 학습서

IBM QRadar User Behavior Analytics(UBA) 앱, 참조 데이터 가져오기 - LDAP 앱 및 Machine Learning Analytics(ML) 앱에 대해 자세히 알아봅니다.

IBM Security Learning Academy

IBM Security Learning Academy 웹 사이트에서 User Behavior Analytics(UBA) 과정에 등록하십시오.

팁: 비디오를 등록하고 시청하려면 IBM ID 계정이 있어야 합니다.

유튜브의 비디오 학습서

Machine Learning V2.0.0이 포함된 User Behavior Analytics 앱 데모: https://www.youtube.com/watch?v=RgF1RztR1yg

참조 데이터 가져오기 - LDAP 앱 구성 데모: https://www.youtube.com/watch?v=ER-wYxS6wFk

User Behavior Analytics 앱의 일반 개요:

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

UBA 대시보드 및 사용자 세부사항

IBM QRadar User Behavior Analytics(UBA) 앱은 네트워크에서 사용자에 대한 전체적인 위험 데이터를 표시합니다.

대시보드

UBA 앱을 설치하고 구성한 후 **사용자 분석** 탭을 클릭하여 대시보드를 여십시오.

참고: UBA 앱에서 모니터할 수 있는 지원되는 사용자 수는 40만 명입니다.

사용자 검색 필드에서 이름, 이메일 주소 또는 사용자 이름으로 사용자를 검색할 수 있습니다. 이름을 입력하면 앱은 상위 다섯 개의 결과를 표시합니다.

대시보드는 1분마다 자동으로 새로 고쳐지며 다음과 같은 위험 데이터를 표시합니다.

모니터되는 사용자	UBA 앱에서 능동적으로 모니터하고 있는 총 사용자 수를 표시합니다.
고위험 사용자	현재 위험성 점수를 초과하는 사용자 수를 표시합니다. 위험성 점수를 판별하는 데 필요한 값은 UBA 설정의 "오펜스 트리거 위험 임계값"에 설정됩니다.
이벤트에서 발견된 사용자	가져온 사용자를 제외한 이벤트에서 발견된 사용자 수를 표시합니다.
디렉토리에서 가져온 사용자	참조 테이블에서 가져온 사용자 수를 표시합니다.
활성 분석	• UBA 룰: 룰 컨텐츠 상태를 표시합니다. 초록색 상태는 룰이 설치되어 있고 활성 상태임을 표시합니다. 회색은 룰이 사용 안함으로 설정되어 있음을 표시합니다. 노란색은 설치가 진행 중임을 표시합니다. • 플로우 룰: QNI 룰의 상태를 표시합니다. 초록색 상태는 QNI 룰이 설치되어 있고 활성 상태임을 표시합니다. 회색은 QNI 룰이 설치되어 있지 않음을 표시합니다. • 작동 이상 항목: 초록색 상태는 ADE 룰이 설치되어 있고 활성 상태임을 표시합니다. 회색은 ADE 룰이 설치되어 있지 않음을 표시합니다. • Machine Learning Analytics: 초록색 상태는 Machine Learning Analytics 앱이 설치되어 있음을 표시합니다. 회색은 Machine Learning Analytics 앱이 설치되어 있지 않음을 표시합니다.
모니터되는 사용자	가장 위험한 사용자 상위 10명을 표시합니다. 첫 번째 컬럼은 표시 이름과 직책 및 구/군/시(있는 경우)를 나열합니다. • 최근 위험: 각 사용자에 대해 지난 5분 동안 누적된 위험을 표시합니다. • 위험성 점수: 지난 1시간 동안 사용자의 전체 위험성 점수 경향 및 현재 위험성 점수를 표시합니다. 그래프의 색상은 전체 위험도를 표시합니다. • 관심 목록 아이콘: 사용자를 관심 목록에 추가하거나 관심 목록을 작성합니다. 숫자는 사용자가 구성원으로 속한 관심 목록의 수를 표시합니다. • 검색 페이지에서 추적된 모든 사용자를 볼 수 있습니다.
최근 오펜스	사용자별 가장 최근 감지 오펜스입니다.

[사용자] 관심 목록	사용자가 작성한 관심 목록입니다. 원하는 수만큼 관심 목록을 작성할 수 있으며 해당 관심 목록은 대시보드에 표시됩니다. **검색** 페이지에서 사용자가 작성한 사용자 정의 관심 목록에서 추적된 모든 사용자를 볼 수 있습니다. **팁:** 사용자를 관심 목록에 추가하려면 **관심 목록**() 아이콘을 클릭하십시오. 숫자는 사용자가 구성원으로 속한 관심 목록의 수를 표시합니다.
시스템 점수	지정된 시점에서 모든 사용자에 대한 전체적인 누적 위험성 점수입니다. 1일보다 더 길게 날짜 범위를 지정하려면 **캘린더** 아이콘을 클릭하십시오. 선택할 수 있는 최대 기간은 작년 중에 임의의 30일입니다.
위험 카테고리 분류	지난 1시간 동안의 상위 레벨 위험 카테고리입니다. 하위 카테고리를 보려면 그래프를 클릭한 다음 이벤트가 표시되도록 클릭하십시오.
비활성 계정이 포함된 사용자	비활성 계정으로 플래그 지정된 사용자의 관심 목록입니다. 비활성 계정이 있는 사용자는 자동으로 생성됩니다. V3.2.0 이상 버전에서 사용이 가능합니다.
활성 조사	현재 조사 중인 사용자입니다. 시작한 조사만 표시하려면 **내 조사** 선택란을 선택하십시오. V2.7.0 이상 버전에서 사용이 가능합니다.
Machine Learning 모델의 상태	Machine Learning 앱이 설치된 경우, Machine Learning Analytics의 상태가 표시됩니다. 추가 정보는 224 페이지의 『Machine Learning Analytics가 있는 UBA 대시보드』의 내용을 참조하십시오.

사용자 세부사항 페이지

앱의 어디서든 사용자 이름을 클릭하여 선택한 사용자에 대한 세부사항을 볼 수 있습니다.

이벤트 뷰어 분할창에서 사용자 활동에 대한 자세한 정보를 볼 수 있습니다. 이벤트 뷰어 분할창은 선택한 활동 또는 시점에 대한 정보를 표시합니다. 이벤트 뷰어 분할창에서 이벤트를 클릭하면 syslog 이벤트 및 페이로드 정보와 같은 세부사항이 표시됩니다. 이벤트 뷰어 분할창은 사용자 세부사항 페이지에서 모든 원 및 선 그래프와 위험한 활동 타임라인의 활동에 사용할 수 있습니다.

사용자 세부사항 페이지에 들어 있는 사용자 정보는 다음과 같습니다.

- 선택한 사용자의 이름과 별명 및 LDAP에서 가져온 속성의 추가 세부사항을 표시합니다.
- V3.2.0 이상에서는 사용자와 연관된 것으로 발견된 모든 계정의 상태(비활성, 활성, 사용되지 않음)를 볼 수 있습니다.
- QRadar Advisor with Watson V1.13.0 이상이 설치되어 있는 경우 사용자와 관련된 정보를 검색할 수 있습니다. QRadar 관리자 권한이 있어야 합니다. **Watson 검색** 아이콘을 클릭하십시오(V2.7.0 이상에서 사용 가능).
- 사용자에 대한 조사를 시작하려면 **조사 시작**  아이콘을 클릭하십시오. 조사가 완료되면 **조사 종료** 아이콘을 클릭하십시오(V2.7.0 이상에서 사용 가능).
- 사용자를 관심 목록에 추가하거나 관심 목록을 작성하려면 **관심 목록**() 아이콘을 클릭하십시오.

고급 조치 목록에 있는 조치는 다음과 같습니다.

사용자 정의 경보 추가	사용자 이름별로 표시되는 사용자 정의 경보를 설정할 수 있습니다. **사용자 정의 경보 추가**를 클릭하고 경보 메시지를 입력한 다음 **설정**을 클릭하십시오. 선택한 사용자에 대한 사용자 정의 경보를 제거하려면 **사용자 정의 경보 제거**를 클릭하십시오.
화이트리스트에 추가	QRadar 관리자 권한이 있어야 합니다. 사용자가 위험성 점수 및 오펜스를 생성하지 않도록 선택한 사용자를 화이트리스트에 추가할 수 있습니다. 화이트리스트에서 선택한 사용자를 제거하려면 **화이트리스트에 있음**을 클릭하십시오. 화이트리스트에 추가된 사용자의 전체 목록을 검토하려면 41 페이지의 『신뢰할 수 있는 사용자를 위한 화이트리스트 보기』의 내용을 참조하십시오.
사용자에 대한 GDPR 준수 보고서 생성	사용자에 대한 GDPR(General Data Protection Regulation) 준수 보고서를 생성할 수 있습니다. **중요사항: 사용자 추적 삭제 및 중지**를 클릭하기 전에 보고서를 생성하십시오.
사용자 추적 삭제 및 중지	QRadar 관리자 권한이 있어야 합니다. GDPR(General Data Protection Regulation)을 준수하도록 **사용자 추적 삭제 및 중지**를 클릭할 수 있습니다. 사용자 추적을 영구적으로 삭제 및 중지하려면 **예**를 선택하십시오. 사용자 추적을 다시 시작하려면 참조 세트 **UBA : Users Not Tracked**에서 사용자의 별명을 삭제하십시오. 사용자의 별명을 모두 보려면 사용자를 삭제하기 전에 GDPR 보고서를 다운로드하십시오.
Machine Learning으로 항상 추적	QRadar 관리자 권한이 있어야 합니다. **Machine Learning으로 추적**을 클릭하여 사용자를 *UBA: ML Always Tracked Watchlist* 참조 세트에 추가할 수 있습니다. 참조 세트에 사용자를 추가하면 해당 사용자가 기계 학습 모델에 포함될 가능성이 가장 높아집니다. UBA의 참조 세트에 대한 자세한 정보는 50 페이지의 『참조 세트』의 내용을 참조하십시오. 선택한 사용자를 참조 세트에서 제거하려면 **Machine Learning으로 추적됨**을 클릭하십시오. **참고:** Machine Learning이 설치되고 QRadar 관리자 권한이 있는 경우에만 V2.8.0 이상에서 사용 가능합니다.

선택한 사용자에 대해 다음과 같은 정보를 볼 수 있습니다.

전체 위험성 점수	전체 위험성 점수는 사용자에 대한 위험 경향을 표시합니다.
타임라인	타임라인 그래프가 위험한 이벤트 및 사용자 이벤트를 표시합니다. 위험한 이벤트는 위험성 점수에 기여하는 위험 이벤트입니다. 사용자 이벤트는 위험하지 않은 이벤트입니다. Y축은 이벤트 수이고 X축은 시간입니다. 타임라인의 활동을 클릭하여 사용자 활동과 연관된 지원 로그 이벤트를 나열하는 이벤트 뷰어 분할창을 열 수 있습니다. 이벤트를 클릭하여 syslog 이벤트 및 페이로드 정보와 같은 세부사항을 표시하십시오. • V2.8.0 이상에서는 위험한 활동 타임라인 섹션에서 **활동별 그룹화** 또는 **시간별 그룹화**를 클릭하여 사용자의 활동 목록을 보고 타임라인의 컬럼 기준으로 필터링하고 검색할 수 있습니다. • V3.0.0 이상에서는 타임라인 활동이 세션별 및 일별로 그룹화됩니다. 세션은 **UBA 설정** 페이지의 애플리케이션 설정 섹션에서 정의됩니다. 색상은 세션의 전체 위험도를 나타냅니다. **캘린더** 아이콘을 클릭하여 날짜 범위(1 - 14일)를 지정하십시오. • 3.1.0 이상에서는 **지표 설정** 아이콘을 클릭하여 타임라인에 대해 표시되는 지표 설정을 사용자 정의할 수 있습니다. 보려는 카테고리를 추가하고 제거할 수 있습니다. 지표 설정 화면의 예제 지표 섹션에 표시된 데이터는 실제 값을 표시하지 않습니다. **참고:** "위험한 이벤트" 및 "유스 케이스"는 "위험한 이벤트"가 제공된 유스 케이스의 총 이벤트 수와 동일한 데이터를 표시합니다. "URL 카테고리" 및 "URL"은 "URL"이 제공된"URL 카테고리"의 총 이벤트 수와 동일한 데이터를 표시합니다. "이벤트 ID" 및 "이벤트"는 제공된 이벤트 ID의 총 이벤트 수와 동일한 데이터를 표시합니다.

최근 오펜스	사용자 유형 오펜스를 표시합니다. 여기서 사용자 이름은 선택한 사용자의 별명과 일치합니다. 마지막 5개 오펜스가 표시됩니다. QRadar에서 **오펜스** 탭을 열려면 오펜스를 클릭하십시오.
위험 카테고리 분류	지난 1시간 동안에 선택한 사용자의 위험 카테고리를 표시합니다.
참고 추가	선택한 사용자에 대한 참고를 추가하려면 **추가** 아이콘(+)을 클릭하십시오. 참고는 30일의 보존 기간 후에 자동 삭제됩니다. **팁:** 참고를 무기한으로 저장하려면 **플래그** 아이콘을 클릭하여 참고에 중요 표시를 하십시오.

Machine Learning 앱이 설치되고 지정된 분석이 사용으로 설정된 경우 다음 그래프가 사용자 세부사항 페이지에 표시됩니다. 추가 정보는 224 페이지의 『Machine Learning Analytics가 있는 UBA 대시보드』의 내용을 참조하십시오.

총 활동	하루동안 시간별로 그룹화된 사용자의 실제 및 학습된 활동량을 표시합니다.
카테고리별 사용자 활동	상위 레벨 카테고리별로 실제 및 예상되는 사용자 활동의 작동 패턴을 표시합니다.
위험 관리 태세	사용자의 위험성 점수가 예상 위험성 점수 패턴에서 벗어나는지 여부를 표시합니다.
비정상 아웃바운드 전송 시도	각 사용자의 아웃바운드 트래픽 사용량 및 비정상적인 작동에 대한 경보를 표시합니다. 이 분석에 대한 그래프는 기본적으로 사용으로 설정되어 있지 않음을 유의하십시오. 비정상 아웃바운드 전송 시도 분석은 Machine Learning 앱이 설치되고 분석이 사용으로 설정되어 있고 **사용자 세부사항 페이지에 그래프 표시**가 Machine Learning 설정에서 선택된 경우에만 대시보드에 표시됩니다. V2.8.0 이상 버전에서 사용이 가능합니다.
외부 도메인에 대한 비정상 데이터 볼륨	각 사용자의 외부 도메인 데이터 사용량 및 비정상적인 작동에 대한 경보를 표시합니다. 외부 도메인에 대한 비정상 데이터 볼륨 분석은 Machine Learning 앱이 설치되고, 분석이 사용으로 설정되어 있고, **사용자 세부사항 페이지에 그래프 표시**가 Machine Learning 설정에서 선택된 경우에만 대시보드에 표시됩니다. V3.0.0 이상 버전에서 사용이 가능합니다.
활동 분포	기계 학습에서 모니터하는 모든 사용자에 대한 동적 작동 클러스터를 표시합니다. V2.2.0 이상 버전에서 사용이 가능합니다.
학습된 피어 그룹	사용자가 속한 것으로 예상했던 유추된 피어 그룹에서 벗어난 정도를 표시합니다. V2.2.0 이상 버전에서 사용이 가능합니다.
정의된 피어 그룹	사용자의 이벤트 활동이 정의된 피어 그룹의 이벤트 활동에서 벗어난 정도를 표시합니다. V2.6.0 이상 버전에서 사용이 가능합니다.

기본 대시보드로 돌아가려면 **대시보드**를 클릭하십시오.

관련 개념:

224 페이지의 『Machine Learning Analytics가 있는 UBA 대시보드』

Machine Learning Analytics가 있는 IBM QRadar User Behavior Analytics(UBA) 앱에는 선택된 사용자의 Machine Learning Analytics 상태 및 추가 세부사항이 포함되어 있습니다.

44 페이지의 『비활성 계정』

비활성 계정, 활성 계정 또는 사용되지 않은 계정이 있는 시스템의 사용자를 볼 수 있습니다.

관련 태스크:

39 페이지의 『관심 목록 작성』

새 관심 목록 또는 기존 관심 목록에 사용자를 추가할 수 있습니다.

41 페이지의 『신뢰할 수 있는 사용자를 위한 화이트리스트 보기』
참조 세트 관리 목록에서 화이트리스트에 포함된 신뢰할 수 있는 사용자의 목록을 볼 수 있습니다.

43 페이지의 『신뢰할 수 있는 로그 소스 그룹에 로그 소스 추가』
UBA 앱에서 특정 로그 소스를 모니터링하고 보고하지 않게 하려는 경우, **UBA : Trusted Log Source Group**에 추가할 수 있습니다. 로그 소스를 그룹에 추가하면 UBA 앱은 그에 대한 모니터링을 중지합니다.

205 페이지의 『Machine Learning Analytics 앱 설치』
확장 관리자에서 UBA 앱을 설치한 후에 Machine Learning Analytics 앱을 설치하십시오.

『QRadar Advisor with Watson에서 사용자 조사』
QRadar Advisor with Watson으로 보내 조사할 사용자를 User Behavior Analytics(UBA) 앱에서 선택할 수 있습니다.

QRadar Advisor with Watson에서 사용자 조사

QRadar Advisor with Watson으로 보내 조사할 사용자를 User Behavior Analytics(UBA) 앱에서 선택할 수 있습니다.

시작하기 전에

- User Behavior Analytics(UBA) 앱 V2.7.0 또는 이후 버전을 설치하고 사용자 데이터로 구성해야 합니다.
- 관리 권한이 있어야 합니다.
- QRadar Advisor with Watson V 1.13.0 또는 이후 버전을 설치해야 합니다.

추가 정보는 https://developer.ibm.com/qradar/advisor의 내용을 참조하십시오.

이 태스크 정보

참고: 이 기능은 User Behavior Analytics V2.7.0 이상 및 QRadar Advisor with Watson V1.13.0 이상에서만 사용할 수 있습니다.

프로시저

1. **사용자 분석** 탭을 클릭하여 UBA 대시보드를 여십시오.
2. 사용자를 선택하거나 검색하여 사용자 세부사항 페이지를 여십시오.
3. **Watson 검색** 아이콘을 클릭하십시오. 아이콘이 회전을 중지하면 QRadar Advisor with Watson 앱에서 결과를 검토할 수 있습니다.
4. **Watson** 탭의 인시던트 개요 페이지에서 사용자 조사를 선택하십시오. 사용자 조사는 **UBA에서 시작된 조사**  아이콘으로 표시됩니다.

User Behavior Analytics 앱 설치의 전제조건

User Behavior Analytics(UBA) 앱을 설치하기 전에 요구사항이 충족되는지 확인하십시오.

- IBM Security QRadar V7.2.8 이상이 설치되었는지 확인하십시오.

  우수한 사용 환경을 위해 QRadar 시스템을 다음 버전으로 업그레이드하십시오.

  – QRadar 7.2.8 패치 13(7.2.8.20180529210357) 이상
  – QRadar 7.3.1 패치 6(7.3.1.20180912181210) 이상
- IBM App Exchange의 컨텐츠 팩을 설치하십시오.
- User Behavior Analytics(UBA) 앱에 대한 IBM Sense DSM을 추가하십시오.

컨텐츠 종속 항목

여러 룰이 기타 앱에서 UBA로 이벤트를 피드하도록 고안되었습니다. 이러한 룰이 올바르게 작동하려면 기타 앱의 컨텐츠가 설치되어야 합니다.

UBA 컨텐츠 및 필수 앱에 대한 자세한 정보는 다음 표를 참조하십시오.

UBA 컨텐츠	필수 앱
154 페이지의 『QRadar DNS Analyzer』	IBM QRadar DNS Analyzer
UBA QRadar Network Insights	QRadar Network Insights Content v7.2.8 QRadar Network Insights Content for V7.3.0+
탐색	IBM Security Reconnaissance Content
시스템 모니터링(Sysmon)	IBM QRadar Content for Sysmon

참고: 이 룰을 편집하면 예상대로 작동하지 않을 수 있습니다.

수동으로 IBM Sense DSM 설치

User Behavior Analytics(UBA) 앱은 IBM Sense DSM을 사용하여 QRadar에 사용자 위험성 점수 및 오펜스를 추가합니다. 자동 업데이트를 통해 DSM을 설치하거나 QRadar에 업로드하고 수동으로 설치할 수 있습니다.

참고: 시스템이 인터넷에서 연결이 끊어진 경우에는 수동으로 DSM RPM을 설치해야 합니다.

제한사항: DSM(Device Support Module) 설치 제거는 QRadar에서 지원되지 않습니다.

1. IBM 지원 센터 웹 사이트에서 DSM RPM 파일을 다운로드하십시오.
   - QRadar V7.2.8의 경우: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
   - QRadar V7.3.1 이상의 경우: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`
2. RPM 파일을 사용자의 QRadar Console로 복사하십시오.
3. SSH를 사용하여 root 사용자로 QRadar 호스트에 로그인하십시오.
4. 다운로드한 파일이 있는 디렉토리로 이동하십시오.

5. 다음 명령을 입력하십시오.

   ```
   rpm -Uvh <rpm_filename>
   ```

6. **관리** 설정에서 **변경사항 배치**를 클릭하십시오.
7. **관리** 설정에서 **고급** > **웹 서비스 다시 시작**을 선택하십시오.

UBA 앱에 지원되는 브라우저

IBM Security QRadar 제품의 기능이 올바르게 작동하려면 지원되는 웹 브라우저를 사용해야 합니다.

다음 표에는 지원되는 웹 브라우저 버전이 나열되어 있습니다.

웹 브라우저	지원되는 버전
Mozilla Firefox	45.2 확장 지원 릴리스
Google Chrome	최신

참고: UBA에 대한 경험을 최대화하려면 다음 중 하나를 수행해야 합니다.

- 브라우저의 팝업 차단기 사용 안함
- QRadar Console IP 주소에서 생성되는 팝업에 대한 예외를 허용하도록 브라우저 구성

UBA 앱과 관련된 로그 소스 유형

User Behavior Analytics(UBA) 앱 및 ML 앱은 특정 로그 소스로부터 이벤트를 채택하고 분석할 수 있습니다.

일반적으로 UBA 앱 및 ML 앱은 사용자 이름을 제공하는 로그 소스가 필요합니다. UBA의 경우 사용자 이름이 없으면 UBA 설정에서 **이벤트 또는 플로우 데이터에 대한 사용자 이름이 사용 불가능한 경우 자산에서 사용자 이름 검색** 선택란을 사용으로 설정하여 UBA가 자산 테이블에서 사용자를 검색할 수 있도록 설정하십시오. 사용자를 판별할 수 없는 경우 UBA는 이벤트를 처리하지 않습니다.

특정 유스 케이스 및 해당 로그 소스 유형에 대한 세부사항은 51 페이지의 7, 『UBA 앱에 대한 룰 및 튜닝』의 내용을 참조하십시오.

관련 태스크:

30 페이지의 『UBA 설정 구성』
IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 애플리케이션 설정을 구성해야 합니다.

2 설치 및 설치 제거

User Behavior Analytics 앱 설치

IBM QRadar 확장 관리 도구를 사용하여 QRadar Console에 직접 앱 아카이브를 업로드하고 설치합니다.

시작하기 전에

17 페이지의 『User Behavior Analytics 앱 설치의 전제조건』을 완료하십시오.

중요사항: 앱을 설치하기 전에 IBM QRadar가 최소 메모리(RAM) 요구사항을 충족하는지 확인하십시오. UBA 앱에는 메모리의 애플리케이션 풀에서 1GB의 사용 가능한 메모리가 필요합니다. 애플리케이션 풀에서 사용 가능한 메모리가 충분하지 않으면 UBA 앱은 설치되지 않습니다.

이 태스크 정보

설치가 V2.8.0부터 변경되었습니다. 오펜스 트리거에 사용하는 룰을 포함하는 UBA 특정 컨텐츠 패키지가 이제 별도의 확장으로 설치됩니다. 컨텐츠 패키지는 기본적으로 설치됩니다. UBA에서 사용자만의 사용자 정의 룰을 작성하기로 선택한 경우 UBA 설정을 구성할 때 **컨텐츠 패키지 설치 및 업그레이드** 설정을 변경할 수 있습니다.

주의: 앱이 설치된 후에 다음을 수행해야 합니다.

- 인덱스를 사용으로 설정하십시오.
- 전체 구성을 배치하십시오.
- 브라우저 캐시를 지우고 브라우저 창을 새로 고치십시오.
- 사용자 분석 탭을 볼 수 있는 액세스 권한이 필요한 사용자에 대한 권한을 설정하십시오. 앱에 대한 액세스 권한이 필요한 각 사용자 역할에 다음 권한을 지정해야 합니다.
  - 사용자 분석
  - 오펜스
  - 로그 보기

IBM Security App Exchange에서 앱을 다운로드한 후에 IBM QRadar 확장 관리 도구를 사용하여 QRadar Console에 설치하십시오.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.

- IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.

2. **시스템 구성** > **확장 관리**를 클릭하십시오.
3. 확장 관리 창에서 **추가**를 클릭하고 콘솔에 업로드하려는 UBA 앱 아카이브를 선택하십시오.
4. **즉시 설치** 선택란을 선택하고 **추가**를 클릭하십시오.
5. 프롬프트가 표시되면 **겹쳐쓰기**를 선택하십시오.

   중요사항: 앱이 활성 상태가 되려면 몇 분을 기다려야 할 수 있습니다. UBA 앱을 설치하면 컨텐츠 패키지가 백그라운드에서 설치됩니다. 컨텐츠는 앱이 설치된 후 QRadar에 즉시 표시되지 않을 수 있습니다.
6. **관리** 설정에서 **시스템 구성** > **인덱스 관리**를 클릭한 후 다음 인덱스를 사용으로 설정하십시오.
   - 상위 레벨 카테고리
   - 하위 레벨 카테고리
   - 사용자 이름
   - senseValue
7. **관리** 설정에서 **고급** > **전체 구성 배치**를 클릭하십시오.

   참고: UBA 설치를 완료하고 UBA를 구성하고 나면 다음과 같은 컨텐츠 패키지가 설치됩니다.
   - User Behavior Analytics 액세스 및 인증 컨텐츠
   - User Behavior Analytics 계정 및 권한 컨텐츠
   - User Behavior Analytics 찾아보기 동작 컨텐츠
   - User Behavior Analytics DNS Analyzer 컨텐츠
   - User Behavior Analytics 엔드포인트 컨텐츠
   - User Behavior Analytics 탈출 컨텐츠
   - User Behavior Analytics 지역 컨텐츠
   - User Behavior Analytics 네트워크 트래픽 및 공격 컨텐츠
   - User Behavior Analytics QRadar Network Insights 컨텐츠
   - User Behavior Analytics 탐색 컨텐츠
   - User Behavior Analytics Sysmon 컨텐츠
   - User Behavior Analytics 위협 인텔리전스 컨텐츠

다음에 수행할 작업

- 설치가 완료되면 브라우저 캐시를 지우고 앱을 사용하기 전에 브라우저 창을 새로 고치십시오.
- UBA 앱 사용자 역할에 대한 권한을 관리하십시오.

관련 태스크:

47 페이지의 『성능 개선을 위한 인덱스 사용』
IBM QRadar User Behavior Analytics(UBA) 앱의 성능을 개선하려면 IBM QRadar에서 인덱스를 사용으로 설정하십시오.

39 페이지의 『QRadar UBA 앱에 대한 권한 관리』
관리자는 IBM QRadar의 사용자 역할 관리 기능을 사용하여 사용자 계정을 구성하고 관리합니다. 관리자로서 QRadar UBA 앱을 사용하도록 허용된 각 사용자 역할에 대해 사용자 분석, 오펜스 및 로그 보기 권한을 사용으로 설정해야 합니다.

UBA 앱 설치 제거

IBM QRadar 확장 관리 도구를 사용하여 QRadar Console에서 애플리케이션을 설치 제거합니다.

시작하기 전에

Machine Learning Analytics(ML) 앱을 설치한 경우, 확장 관리 창에서 UBA 앱을 설치 제거하기 전에 Machine Learning 설정 페이지에서 ML 앱을 설치 제거해야 합니다. UBA를 설치 제거하기 전에 ML 앱을 제거하지 않은 경우에는 대화식 API 문서 인터페이스에서 ML 앱을 제거해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **확장 관리**를 클릭하십시오.
3. 확장 관리 창의 **설치됨** 탭에서 User Behavior Analytics 앱을 선택하고 **설치 제거**를 클릭하십시오.

   앱을 설치 제거할 때 시스템에서 확장이 제거됩니다. 확장을 다시 설치하려면 이를 다시 추가해야 합니다.
4. V2.8.0부터 UBA 앱을 구성할 때 다음 컨텐츠 패키지가 설치됩니다. 앱을 완전히 제거하려면 각 컨텐츠 패키지를 설치 제거해야 합니다.
   - User Behavior Analytics 액세스 및 인증 컨텐츠
   - User Behavior Analytics 계정 및 권한 컨텐츠
   - User Behavior Analytics 찾아보기 동작 컨텐츠
   - User Behavior Analytics DNS Analyzer 컨텐츠
   - User Behavior Analytics 엔드포인트 컨텐츠
   - User Behavior Analytics 탈출 컨텐츠
   - User Behavior Analytics 지역 컨텐츠

- User Behavior Analytics 네트워크 트래픽 및 공격 컨텐츠
- User Behavior Analytics QRadar Network Insights 컨텐츠
- User Behavior Analytics 탐색 컨텐츠
- User Behavior Analytics Sysmon 컨텐츠
- User Behavior Analytics 위협 인텔리전스 컨텐츠

3 업그레이드

User Behavior Analytics 앱 업그레이드

IBM QRadar 확장 관리 도구를 사용하여 앱을 업그레이드합니다.

시작하기 전에

중요사항: V2.8.0부터 메모리 요구사항이 증가되었습니다. 앱을 업그레이드하기 전에 IBM QRadar가 최소 메모리(RAM) 요구사항을 충족하는지 확인하십시오. UBA 앱에는 메모리의 애플리케이션 풀에서 1GB의 사용 가능한 메모리가 필요합니다. 애플리케이션 풀에서 사용 가능한 메모리가 충분하지 않으면 UBA 앱은 업그레이드되지 않습니다.

우수한 사용 환경을 위해 QRadar 시스템을 다음 버전으로 업그레이드하십시오.

- QRadar 7.2.8 패치 13(7.2.8.20180529210357) 이상
- QRadar 7.3.0 패치 7(7.3.0.20171205025101) 이상
- QRadar 7.3.1 패치 6(7.3.1.20180912181210) 이상

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **확장 관리**를 클릭하십시오.
3. 확장 관리 창에서 **추가**를 클릭하고 콘솔에 업로드하려는 UBA 앱 아카이브를 선택하십시오.
4. 프롬프트가 표시되면 **겹쳐쓰기**를 선택하십시오. 기존 UBA 앱 데이터는 모두 원래대로 남아 있습니다.

   중요사항: 앱이 활성 상태가 되려면 몇 분을 기다려야 할 수 있습니다. UBA 앱을 업그레이드하면 컨텐츠 패키지가 백그라운드에서 업그레이드됩니다. 컨텐츠는 앱이 업그레이드된 후 QRadar에 즉시 표시되지 않을 수 있습니다.

   참고: UBA 업그레이드를 완료하고 UBA를 구성하고 나면 다음과 같은 컨텐츠 패키지가 업그레이드됩니다.

   - User Behavior Analytics 액세스 및 인증 컨텐츠
   - User Behavior Analytics 계정 및 권한 컨텐츠
   - User Behavior Analytics 찾아보기 동작 컨텐츠

- User Behavior Analytics DNS Analyzer 컨텐츠
- User Behavior Analytics 엔드포인트 컨텐츠
- User Behavior Analytics 탈출 컨텐츠
- User Behavior Analytics 지역 컨텐츠
- User Behavior Analytics 네트워크 트래픽 및 공격 컨텐츠
- User Behavior Analytics QRadar Network Insights 컨텐츠
- User Behavior Analytics 탐색 컨텐츠
- User Behavior Analytics Sysmon 컨텐츠
- User Behavior Analytics 위협 인텔리전스 컨텐츠

다음에 수행할 작업

업그레이드가 완료되면 브라우저 캐시를 지우고 앱을 사용하기 전에 브라우저 창을 새로 고치십시오.

4 구성

User Behavior Analytics 앱 구성

IBM QRadar User Behavior Analytics(UBA) 앱을 사용할 수 있으려면 먼저 추가 설정을 구성해야 합니다.

UBA 앱을 설치할 때 IBM QRadar 참조 데이터 가져오기 LDAP(LDAP) 앱도 설치됩니다. LDAP 앱 사용을 선택하는 경우, UBA 앱을 설정하기 전에 LDAP 앱을 구성해야 합니다. UBA 앱에서 사용하는 데이터의 출처는 LDAP 조회입니다. LDAP 조회는 UBA 앱을 채우는 데 사용되는 사용자의 목록을 검색합니다.

UBA 앱 및 LDAP 앱 모두 별도의 인증 토큰이 필요합니다. 각 앱을 구성할 때 인증 토큰을 작성할 수 있습니다.

다음 설정 프로시저를 완료하십시오.

- LDAP을 사용 중인 경우 참조 데이터 가져오기 LDAP 앱 구성
- UBA 앱에 대한 UBA 설정 구성

참조 데이터 가져오기 LDAP 앱 구성

IBM® QRadar® User Behavior Analytics(UBA) 앱을 설치할 때 참조 데이터 가져오기 LDAP 앱도 설치됩니다. LDAP 앱을 사용하여 LDAP/AD 서버 또는 CSV 파일에서 QRadar 참조 테이블로 사용자 데이터를 가져올 수 있습니다. 그런 다음 참조 테이블은 UBA 앱에 의해 사용되거나, QRadar 검색 또는 룰에 사용될 수 있습니다.

시작하기 전에

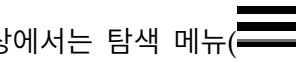
경고: 이전에 독립형 참조 데이터 가져오기 LDAP 앱을 설치한 경우에는 UBA 앱을 설치할 때 대체됩니다. 구성은 참조 데이터 가져오기 LDAP 앱의 업데이트된 버전에 추가됩니다.

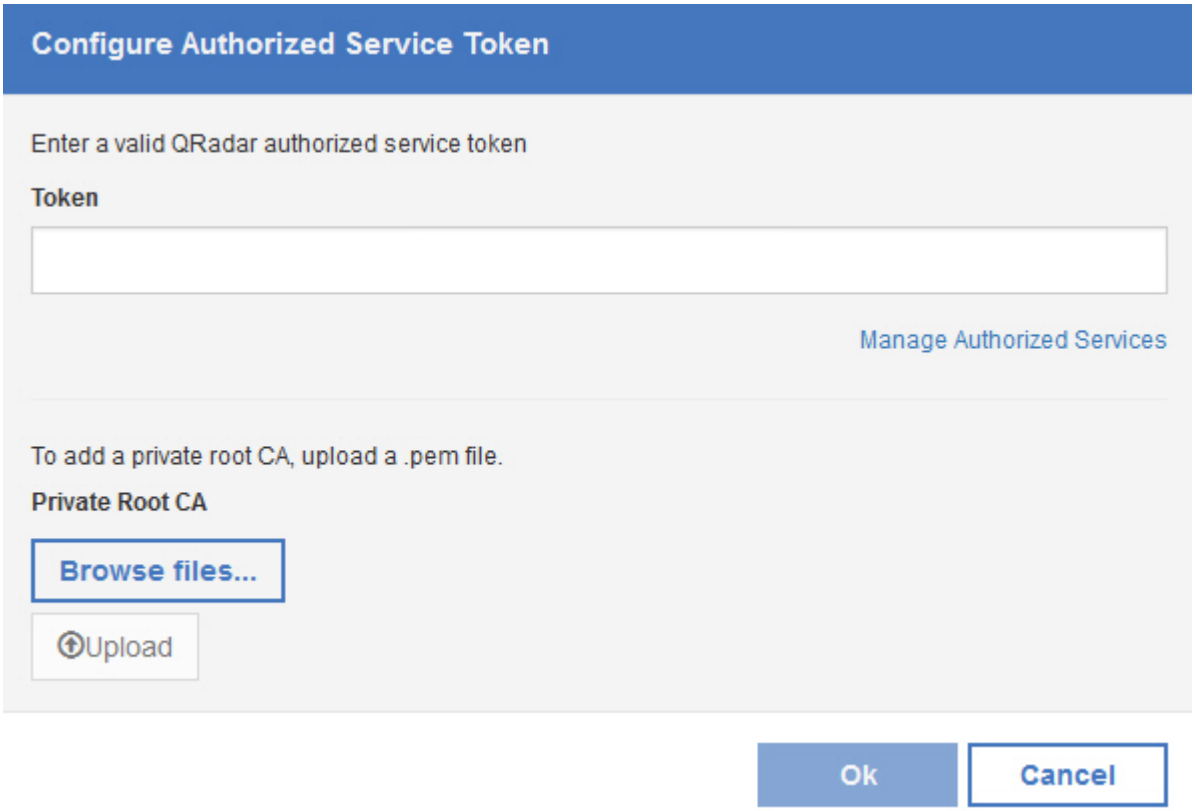
이 태스크 정보

참고: 참조 테이블 이름을 기록하도록 하고 속성에 사용자 정의 별명을 제공하는지 여부를 확인하십시오. UBA 앱을 설정할 때 참조 데이터 가져오기 LDAP 앱에서 작성한 참조 테이블을 선택하십시오.

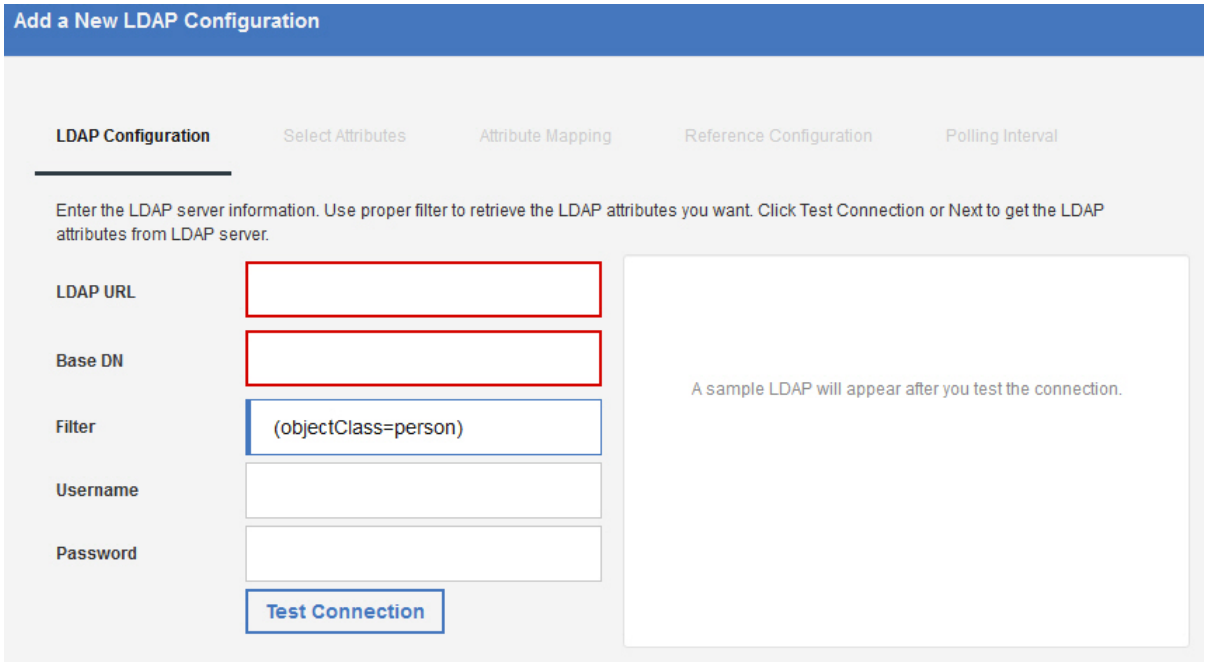
참조 데이터 가져오기 LDAP 앱에 대한 자세한 정보는 IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.apps.doc/c_Qapps_LDAP_intro.html)의 다음 섹션을 참조하십시오.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **참조 데이터 가져오기 - LDAP** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1이상 버전에서는 **앱** > **참조 데이터 가져오기 - LDAP** > **참조 데이터 가져오기 - LDAP**를 클릭하십시오.
3. **구성**을 클릭하여 LDAP용 권한 서비스 토큰을 작성하십시오. 권한 서비스 토큰 구성 대화 상자가 열립니다.
   a. **권한 서비스 관리** 링크를 클릭한 다음 **권한 서비스 추가**를 클릭하십시오.
   b. **서비스 이름** 필드에 LDAP를 입력하십시오. LDAP 앱에서 API 요청을 실행하는 사용자입니다.
   c. **사용자 역할** 목록에서 **관리** 사용자 역할을 선택하십시오.
   d. **보안 프로파일** 목록에서 이 권한 서비스에 지정할 보안 프로파일을 선택하십시오. 보안 프로파일은 이 서비스가 QRadar 사용자 인터페이스에 액세스할 수 있는 네트워크 및 로그 소스를 판별합니다.
   e. **만료 날짜** 목록에서 이 서비스가 만료될 날짜를 입력하거나 선택하십시오. 만료 날짜가 필요하지 않은 경우 **만료되지 않음**을 선택하십시오.
   f. **서비스 작성**을 클릭하십시오.
   g. 작성한 LDAP 서비스가 포함된 행을 클릭한 다음에 메뉴 표시줄의 **선택된 토큰** 필드에서 토큰 문자열을 선택하고 복사하십시오.
   h. 권한 서비스 토큰 구성 대화 상자에서 권한 서비스 토큰 문자열을 **토큰** 필드에 붙여넣으십시오.
4. 옵션: 개인용 루트 인증 기관 파일을 추가하려면 **파일 찾아보기**를 클릭하고 지원 되는 파일을 열고 **열기**를 클릭한 후 **업로드**를 클릭하십시오. 파일 유형 **.pem**이 지원됩니다.
5. **확인**을 클릭하십시오.

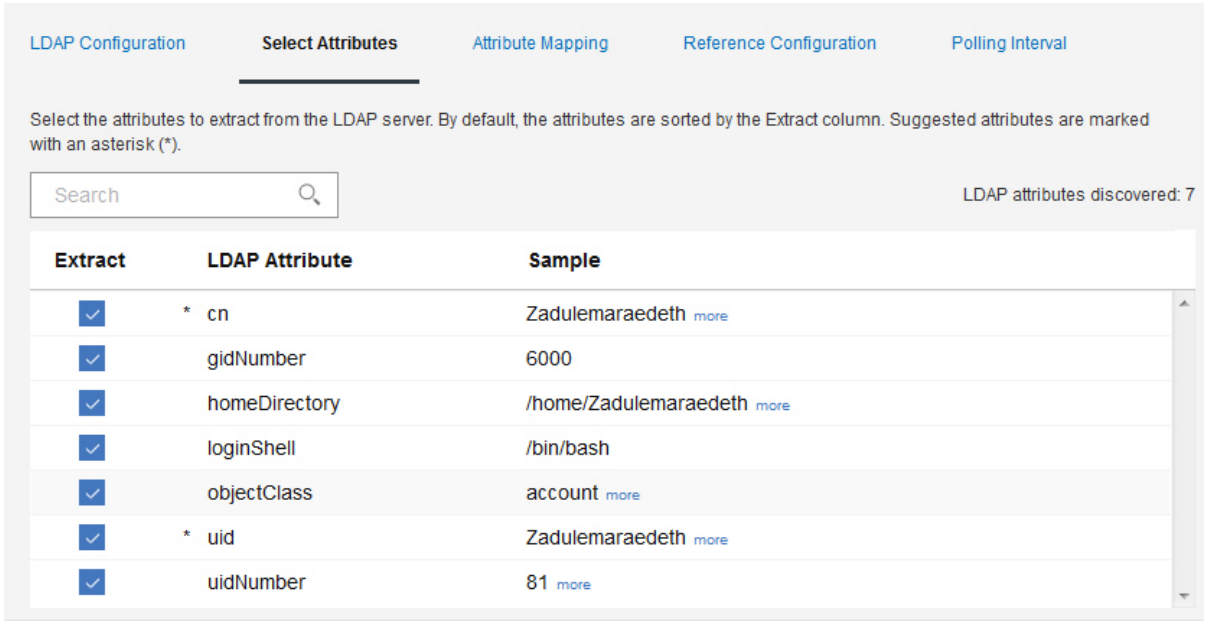


6. 참조 데이터 가져오기(LDAP) 앱 기본 창에서 **가져오기 추가**를 클릭하십시오. 새 LDAP 구성 추가 대화 상자가 열립니다.
7. **LDAP 구성** 탭에서 LDAP 서버에 대한 연결 정보를 추가하십시오. **필터** 필드가 Active Directory 속성에서 자동으로 채워집니다.
   a. **LDAP URL** 필드에 `ldap://` 또는 `ldaps://`(TLS의 경우)로 시작하는 URL을 입력하십시오.
   b. **기본 DN** 필드에 서버가 사용자를 검색해야 하는 LDAP 디렉토리 트리의 지점을 입력하십시오. 예를 들어, LDAP 서버가 도메인 example.com에 있다면 `dc=example,dc=com`을 사용할 수 있습니다.
   c. 참조 테이블로 가져온 데이터를 정렬하려면 사용하려는 속성을 **필터** 필드에 입력하십시오. 예: `cn=*; uid=*; sn=*`. Active Directory로 작업하는 기본값은 다음과 같습니다. `(&(sAMAccountName=*)(samAccountType=805306368))`.
   d. **사용자 이름** 필드에 LDAP 서버를 인증하는 데 사용되는 사용자 이름을 입력하십시오.
   e. **비밀번호** 필드에 LDAP 서버의 비밀번호를 입력하십시오.
8. **연결 테스트** 또는 **다음**을 클릭하여 IBM QRadar가 LDAP 서버에 연결할 수 있는지 확인하십시오. 연결 시도가 성공적이면 LDAP 서버의 정보가 **LDAP 구성** 탭에 표시됩니다.



9. **속성 선택** 탭에서, LDAP 서버에서 추출하려는 속성을 선택하십시오. Active Directory로 작업하는 기본값은 다음과 같습니다.

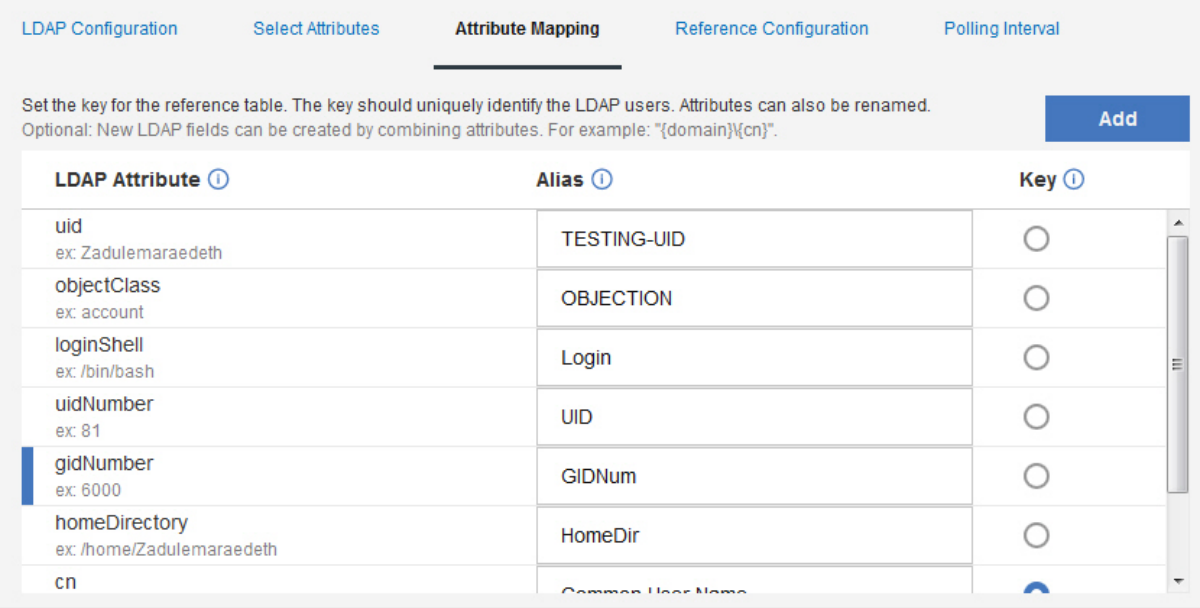
   `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.



10. 옵션: **속성 맵핑** 탭에서 참조 테이블에 대한 키를 설정하십시오.

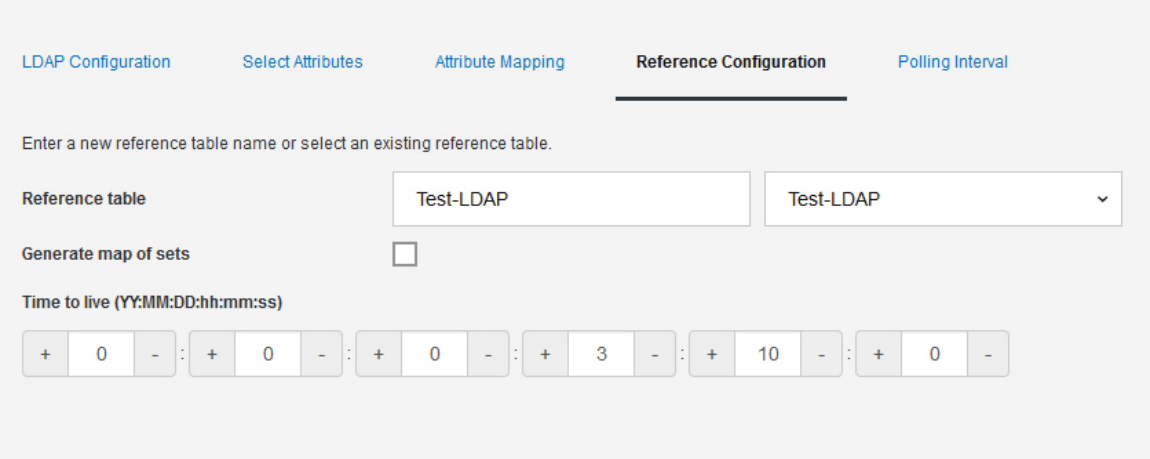
    팁: 추가를 클릭하고 두 개의 속성을 결합하여 새 LDAP 필드를 작성할 수 있습니다. 다음과 같은 구문을 작성할 수 있습니다. 예: `"Last: {ln}, First: {fn}"`.

팁: 같은 참조 테이블의 여러 소스에서 LDAP 데이터를 병합하려면 다른 소스에서 동일한 이름을 가진 LDAP 속성을 구별하기 위해 사용자 정의 별명을 사용할 수 있습니다.



11. **참조 구성** 탭에서 맵의 새 참조 맵을 작성하거나 LDAP 데이터를 추가하려는 맵의 기존 참조 맵을 지정하십시오.
    a. **참조 테이블** 필드에 새 참조 테이블의 이름을 입력하십시오. 또는 목록에서 LDAP 데이터를 추가하려는 기존 참조 테이블의 이름을 추가하십시오.
    b. 기본적으로 **세트의 맵 생성** 선택란은 사용 안함으로 설정됩니다. 이 선택란을 사용으로 설정하면 데이터를 참조 세트 형식으로 전송하여 QRadar 검색을 개선하지만 성능에 영향을 미칠 수 있습니다.
    c. **TTL(Time to live)** 섹션에서 데이터를 맵의 참조 맵에서 지속시키려는 기간을 정의하십시오. 기본적으로 사용자가 추가하는 데이터는 만료되지 않습니다. TTL 기간이 초과되면 *ReferenceDataExpiry* 이벤트가 트리거됩니다.

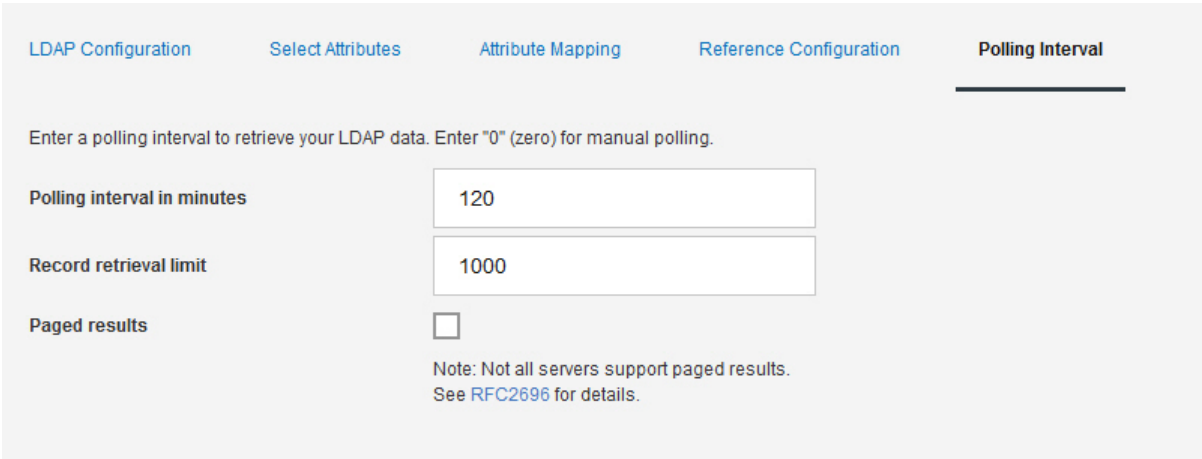
    참고: 맵의 기존 참조 맵에 데이터를 추가하면 앱은 원래 TTL 매개변수를 사용합니다. 이러한 매개변수는 **참조 구성** 탭에서 대체될 수 없습니다.



12. **폴링** 탭에서 데이터를 위한 LDAP 서버를 앱이 폴링하는 빈도를 정의하십시오.
    a. **폴링 간격(분)** 필드에서 데이터를 위한 LDAP 서버를 앱이 폴링하는 빈도를 정의하십시오.

       참고: 최소 폴링 간격 값은 120입니다. 0의 폴링 간격을 입력할 수도 있습니다. 0의 폴링 간격을 입력하면 피드에 표시된 폴링 옵션으로 앱을 수동으로 폴링해야 합니다.
    b. **레코드 검색 한계** 필드에 폴링으로 리턴하기 원하는 레코드 수의 값을 입력하십시오. 기본적으로 100,000개의 레코드가 리턴됩니다. 리턴 가능한 최대 레코드 수는 200,000입니다.
    c. 옵션: 각 폴링에 대해 LDAP 서버가 리턴하는 레코드 수가 제한되지 않도록 **페이징된 결과** 선택란은 기본적으로 선택됩니다.

       참고: 페이징된 결과가 모든 LDAP 서버에서 지원되지는 않습니다.



13. **저장**을 클릭하십시오.

UBA 설정 구성

IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 애플리케이션 설정을 구성해야 합니다.

QRadar 설정에서 인증 토큰 구성

IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 설정에서 UBA 인증 토큰을 구성해야 합니다.

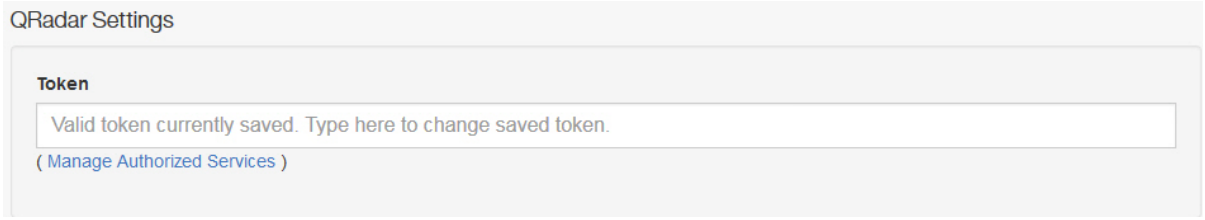
이 태스크 정보

경고: QRadar on Cloud 관리자는 제한된 관리자 기능으로 인해 QRadar 앱에 대한 권한 서비스 토큰을 작성할 수 없습니다. QRadar on Cloud 고객인 경우, 고객 지원에 문의하여 권한 서비스 토큰을 작성하십시오.

인증 토큰을 작성하려면 다음 단계를 완료해야 합니다. 모든 UBA 설정을 구성할 때까지 구성을 저장하지 마십시오.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **UBA 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
3. QRadar 설정 섹션에서 **권한 서비스 관리** 링크를 클릭하십시오.



4. **권한 서비스 추가**를 클릭하십시오.
5. **서비스 이름** 필드에 UBA를 입력하십시오.
6. **사용자 역할** 목록에서 **관리** 사용자 역할을 선택하십시오.
7. **보안 프로파일** 목록에서 이 권한 서비스에 지정할 보안 프로파일을 선택하십시오. 보안 프로파일은 이 서비스가 QRadar 사용자 인터페이스에 액세스할 수 있는 네트워크 및 로그 소스를 판별합니다.
8. **만료 날짜** 목록에서 이 서비스가 만료될 날짜를 입력하거나 선택하십시오. 만료 날짜가 필요하지 않은 경우 **만료되지 않음**을 선택하십시오.
9. **서비스 작성**을 클릭하십시오.

10. 작성한 UBA 서비스가 포함된 행을 클릭한 다음에 메뉴 표시줄의 **선택된 토큰** 필드에서 토큰 문자열을 선택하고 복사하십시오.
11. QRadar 설정 섹션으로 돌아가서 권한 서비스 토큰 문자열을 **토큰** 필드에 붙여넣으십시오.

다음에 수행할 작업

『컨텐츠 패키지 설정 구성』

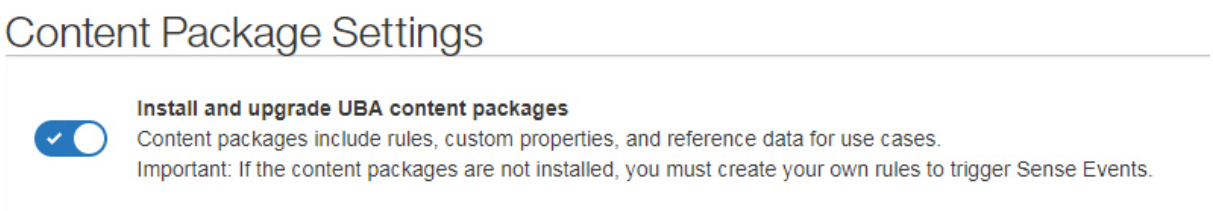
컨텐츠 패키지 설정 구성

IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 컨텐츠 패키지 설정을 구성해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **UBA 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
3. 컨텐츠 패키지 설정 섹션에서 **UBA 컨텐츠 패키지 설치 및 업그레이드** 선택란은 기본적으로 사용으로 설정되어 있습니다. UBA 컨텐츠 패키지를 설치하지 않으려면 선택란을 선택 취소하고 구성을 저장하십시오. UBA 컨텐츠 패키지를 설치하지 않기로 결정한 경우 자체 룰을 작성하여 UBA에 이벤트를 보내는 감지 이벤트를 트리거해야 합니다.

   참고: UBA 컨텐츠 패키지 설치 및 업그레이드 선택란을 선택 취소하고 구성을 저장한 다음 UBA 설정 페이지로 돌아가서 선택란을 선택하고 구성을 저장하기로 결정한 경우 컨텐츠가 설치되고 업그레이드됩니다.



다음에 수행할 작업

33 페이지의 『애플리케이션 설정 구성』

애플리케이션 설정 구성

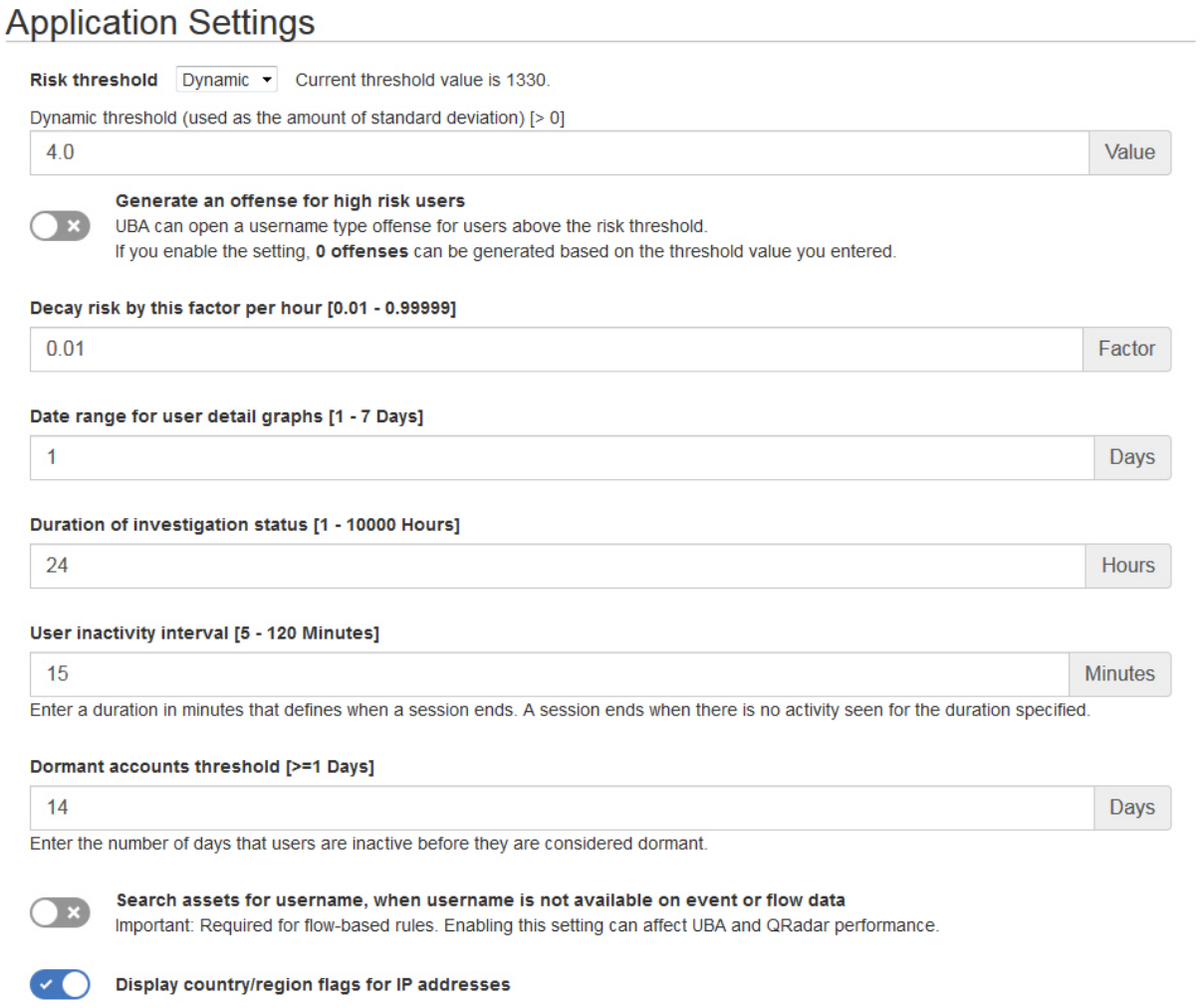
IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 애플리케이션 설정을 구성해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **UBA 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
3. 애플리케이션 설정 섹션에서 다음 설정을 구성하십시오.

옵션	설명
위험 임계값	사용자에 대해 오펜스가 트리거되기 전에 해당 사용자의 위험성 점수가 도달해야 하는 값을 표시합니다. 위험성 점수는 UBA 룰에 의해 발견된 모든 위험 이벤트의 합계입니다. 다음 옵션 중 하나를 선택하십시오. • **동적**: 기본값은 4.0입니다. 값이 높을수록 동적 임계값이 높아져 오펜스가 줄어듭니다. 설정이 최소 하루 이상 실행될 때까지 **고위험 사용자에 대한 오펜스 생성**을 꺼야 합니다. 동적 임계값은 시스템에서 위험성 점수 분포에 따라 매시간 업데이트됩니다. 트리거될 수 있는 오펜스 수에 따라 설정을 사용할지 여부를 결정할 수 있습니다. 자세한 정보는 팁을 참조하십시오. **참고:** 점수가 충분히 다양하지 않을 경우 위험성 점수는 최고 위험 사용자의 +10으로 설정됩니다. 많은 수의 오펜스가 불필요하게 생성되지 않도록 해당 방법을 유지합니다. • **정적**: 기본값은 100,000입니다. 환경이 분석되기 전에 오펜스를 트리거하지 않도록 값은 기본적으로 높은 값으로 설정됩니다. **고위험 사용자에 대한 오펜스 생성**을 켜서 위험 임계값보다 높은 사용자에 대해 사용자 이름 유형의 오펜스를 열 수 있습니다. 트리거될 수 있는 오펜스 수에 따라 설정을 사용할지 여부를 결정할 수 있습니다. **팁:** UBA를 설정하고 기본값을 그대로 두는 것을 고려하십시오. 리턴되는 점수 유형을 확인하려면 하루 이상 설정이 실행되도록 허용하십시오. 며칠 후에 대시보드에서 결과를 검토하여 패턴을 판별하십시오. 그러면 임계값을 조정할 수 있습니다. 예를 들어, 점수가 500점대인 사용자가 1~2명 있지만 대부분은 100점대인 경우에는 임계값을 200 또는 300으로 설정하는 것을 고려하십시오. 따라서 사용자 환경에 대한 "보통"은 100 정도가 될 수 있으며 그 이상의 점수에는 주의가 필요할 수 있습니다.
시간당 이 인수 단위로 위험 감소	위험 감소는 위험성 점수가 1시간마다 감소되는 백분율입니다. 기본값은 0.5입니다. **참고:** 숫자가 높을수록 위험성 점수가 더 빠르게 감소되며 숫자가 낮을수록 위험성 점수가 느리게 감소됩니다.
사용자 세부사항 그래프의 날짜 범위	사용자 세부사항 페이지의 사용자 세부사항 그래프에 표시되는 날짜 범위입니다. 기본값은 1입니다.
조사 상태 지속 기간	조사 완료를 위해 지정된 시간(1 - 10,000)입니다.

옵션	설명
사용자 비활성 간격	사용자 세부사항 페이지는 세션별로 그룹화된 활동이 포함된 타임라인을 보여줍니다. 사용자가 **사용자 비활성 간격** 필드에 입력된 시간 동안 비활성 상태인 경우 세션이 종료됩니다. 기본값은 15분입니다.
비활성 계정 임계값	비활성으로 간주되기 전에 사용자가 비활성 상태인 일 수. 기본값은 14일입니다. 추가 정보는 44 페이지의 『비활성 계정』의 내용을 참조하십시오.(V3.2.0 이상에서 사용 가능).
이벤트 또는 플로우 데이터에 대한 사용자 이름이 사용 불가능한 경우 자산에서 사용자 이름 검색	자산 테이블에서 사용자 이름에 대해 검색하려면 선택란을 선택하십시오. UBA 앱은 이벤트에 사용자가 나열되지 않은 경우 IP 주소에 대한 사용자를 검색하기 위해 자산을 사용합니다. **중요사항:** 이 기능은 UBA 앱 및 QRadar 시스템에서 성능 문제를 일으킬 수 있습니다. **팁:** 조회 제한시간 임계값을 초과하면 앱이 데이터를 리턴하지 않습니다. UBA 대시보드에 오류 메시지가 표시되면 선택란을 선택 취소하고 **새로 고치기**를 클릭하십시오.
IP 주소의 국가/지역 플래그 표시	IP 주소의 국가 및 지역 플래그를 표시하지 않으려면 선택란을 선택 취소하십시오.



다음에 수행할 작업

35 페이지의 『사용자 데이터 가져오기 및 사용자 통합 구성』

사용자 데이터 가져오기 및 사용자 통합 구성

IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 참조 테이블에서 사용자 데이터를 가져올 수 있습니다.

시작하기 전에

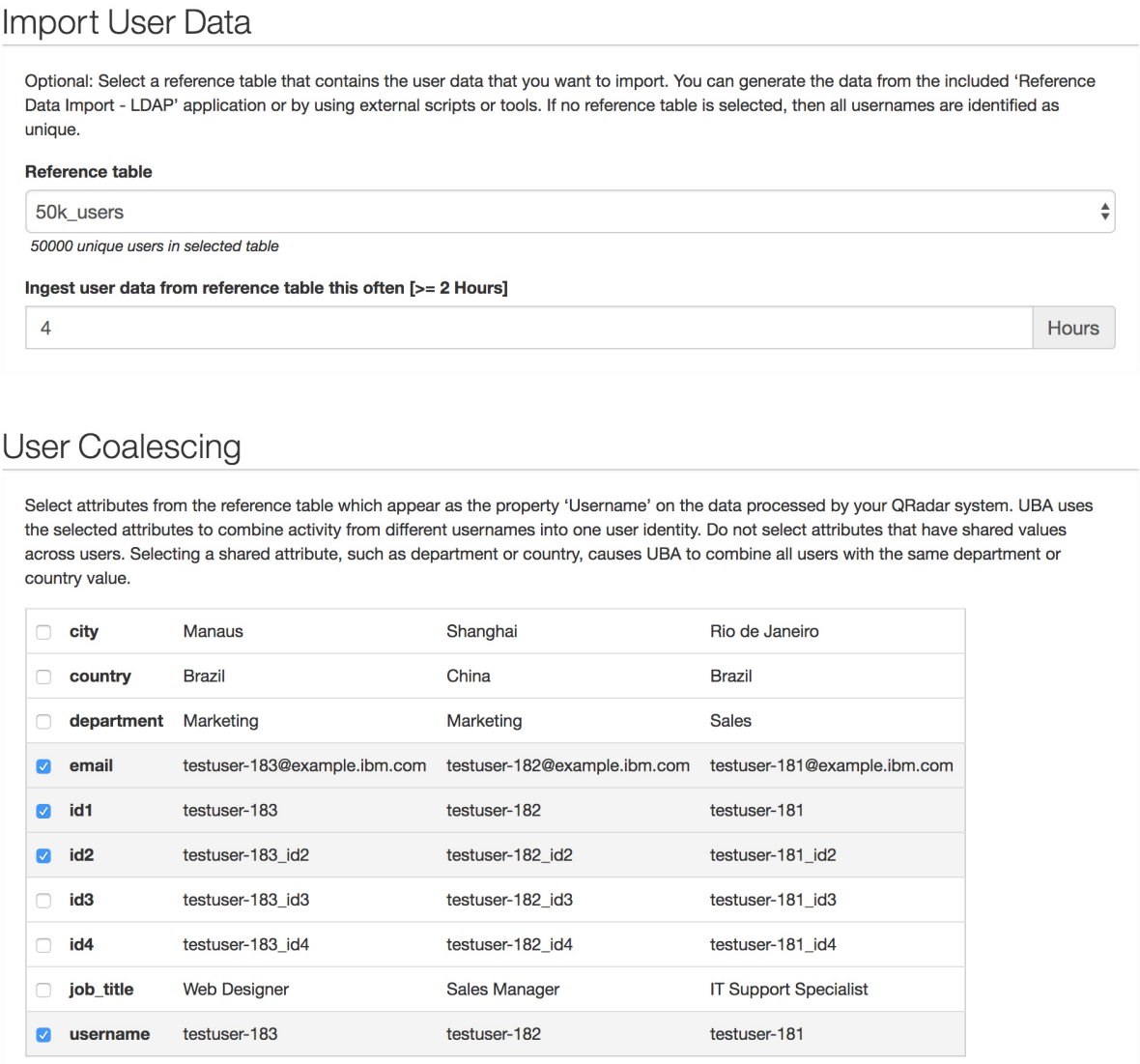
33 페이지의 『애플리케이션 설정 구성』에 대한 지시사항을 완료하십시오.

이 태스크 정보

사용자 데이터 가져오기 및 사용자 통합은 선택사항입니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **UBA 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
3. 사용자 데이터 가져오기 섹션에서 **참조 테이블**을 선택하십시오.
4. 참조 테이블이 데이터를 수집하는 빈도를 판별할 시간 수를 입력하십시오.
5. 사용자 통합 섹션에서 선택된 참조 테이블에서 가져오고 QRadar 시스템에 의해 "사용자 이름"으로 표시되는 속성을 선택하십시오. 해당 ID의 위험성 점수가 추가되며 기본 ID와 연관됩니다. 사용자 간에 공유되는 값이 있는 속성은 선택하지 마십시오. 예를 들어 동일한 부서에 사람이 많은 경우 "Department"를 사용자 이름으로 선택하지 마십시오. "Department" 또는 "Country"와 같은 공유되는 속성을 선택하면 UBA가 동일한 부서나 국가 값을 가지는 모든 사용자를 결합합니다.



다음에 수행할 작업

『속성 표시 구성』

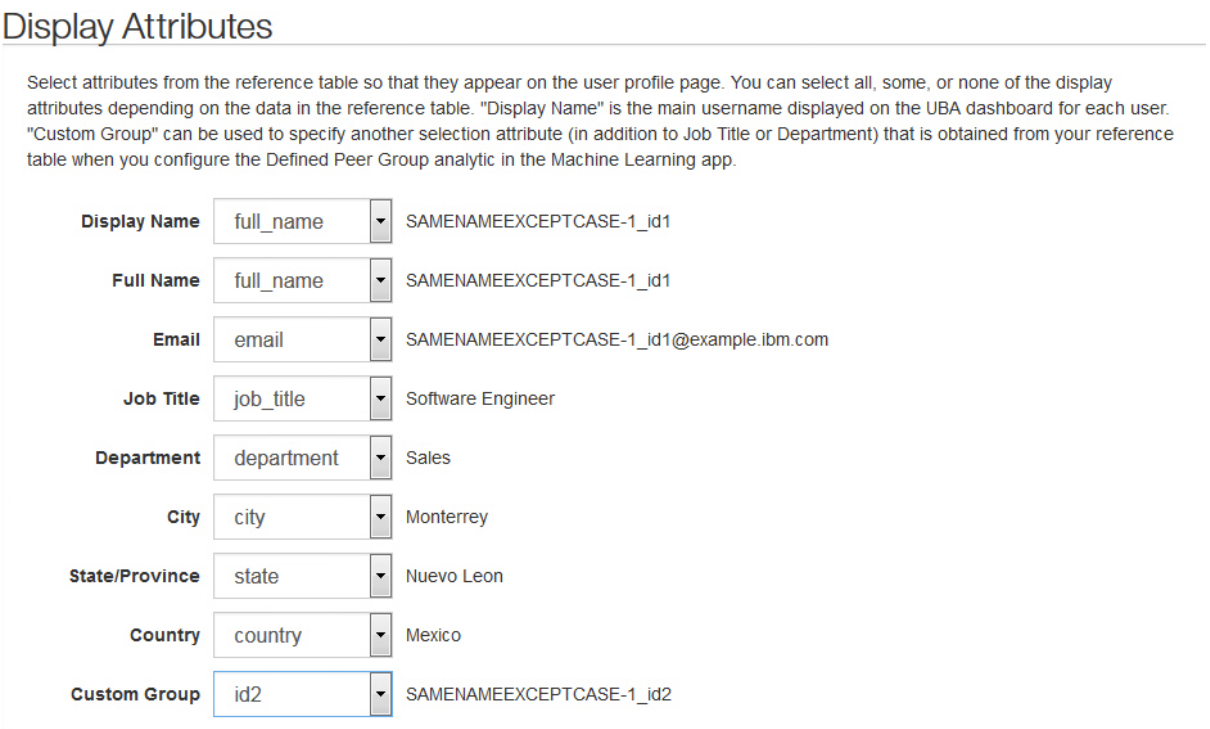
속성 표시 구성

IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 사용자 세부사항 페이지에 표시하려는 참조 테이블에서 속성을 선택할 수 있습니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.

2. **UBA 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **UBA 설정**을 클릭하십시오.
3. 속성 표시 섹션에서 사용자 세부사항 페이지에 표시하려는 속성을 선택하십시오.



4. **구성 저장**을 클릭하십시오.

5 관리

QRadar UBA 앱에 대한 권한 관리

관리자는 IBM QRadar의 사용자 역할 관리 기능을 사용하여 사용자 계정을 구성하고 관리합니다. 관리자로서 QRadar UBA 앱을 사용하도록 허용된 각 사용자 역할에 대해 사용자 분석, 오펜스 및 로그 보기 권한을 사용으로 설정해야 합니다.

이 태스크 정보

QRadar UBA 앱을 설치한 후, QRadar UBA 앱을 사용하려는 사용자에게 지정된 사용자 역할에 대해 **사용자 분석**, **오펜스** 및 **로그 보기** 권한을 사용으로 설정해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. 시스템 구성 섹션에서 **사용자 관리**를 클릭한 다음 **사용자 역할** 아이콘을 클릭하십시오.
3. 기존 사용자 역할을 선택하거나 새 역할을 작성하십시오.
4. 역할에 권한을 추가하려면 다음 선택란을 선택하십시오.
   - **사용자 분석**
   - **오펜스**
   - **로그 보기**
5. **저장**을 클릭하십시오.

관심 목록 작성

새 관심 목록 또는 기존 관심 목록에 사용자를 추가할 수 있습니다.

이 태스크 정보

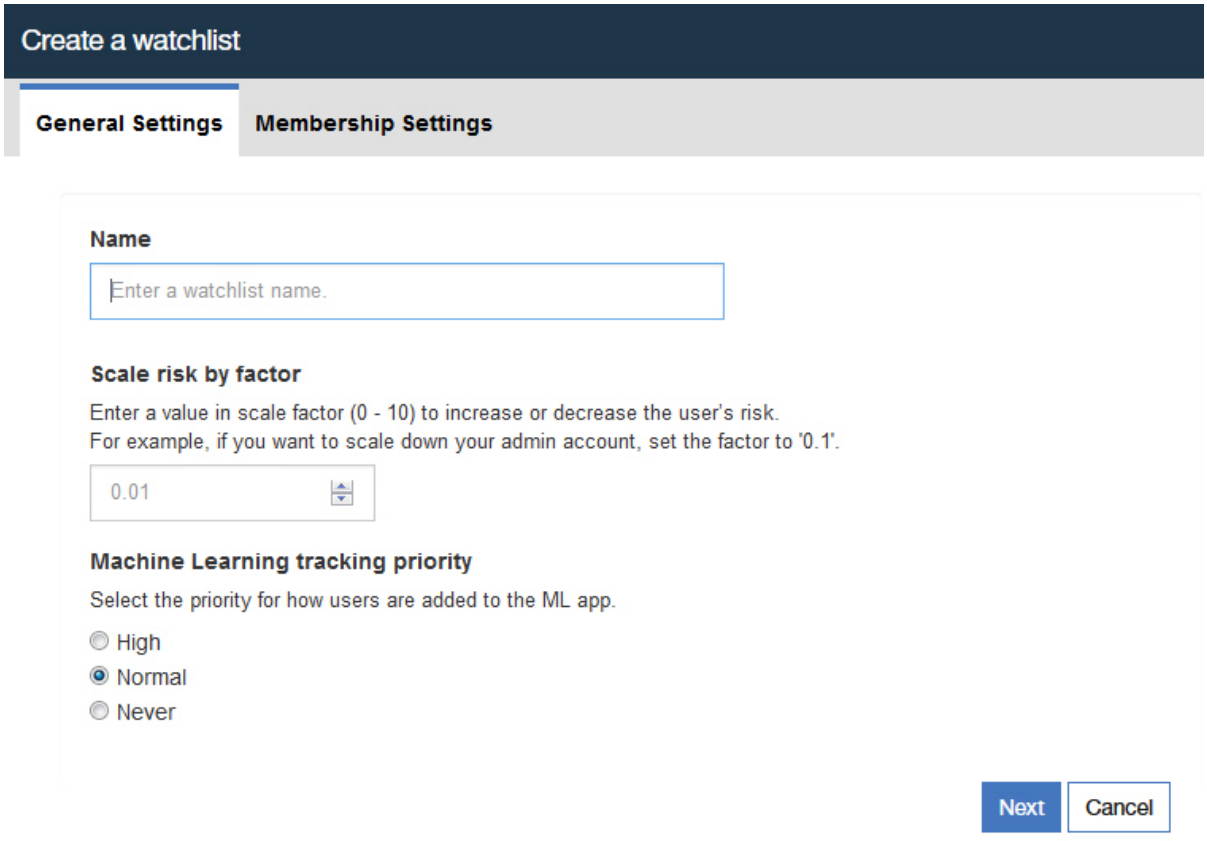
UBA 대시보드, 사용자 세부사항 페이지 또는 Search 결과 페이지에서 새 관심 목록 또는 기존 관심 목록에 사용자를 추가할 수 있습니다. 단일 사용자가 여러 관심 목록의 구성원일 수 있습니다.

프로시저

1. UBA 대시보드 또는 사용자 세부사항 페이지에서 **관심 목록**() 아이콘을 클릭하십시오.

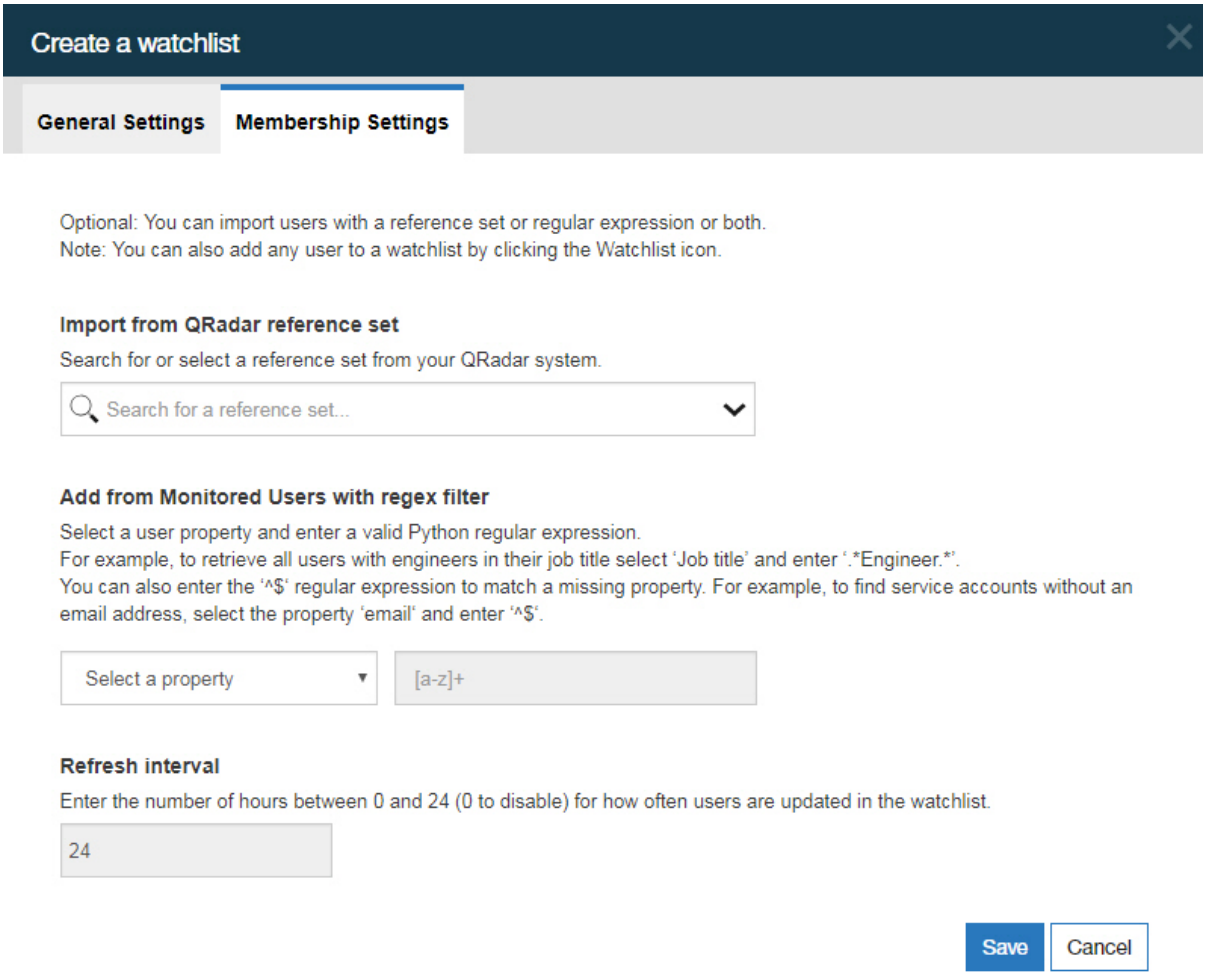
2. 메뉴에서 **새 관심 목록 작성**을 선택하십시오. 기존 관심 목록에 사용자를 추가하려면 관심 목록에 **추가**를 클릭하십시오.
3. **일반 설정** 탭에서 관심 목록 이름을 입력하십시오.
4. **위험 스케일링 인수** 필드의 값을 변경하여 사용자의 위험성 점수를 인위적으로 늘리거나 줄일 수 있습니다. 기본 인수 '1'은 위험성 점수를 변경되지 않은 상태로 유지합니다.

   참고: 사용자가 둘 이상의 관심 목록에 있는 경우 가장 큰 스케일링 인수가 적용됩니다.
5. **Machine Learning 추적 우선순위** 섹션에서 Machine Learning 분석이 사용자를 추적하는 우선순위를 선택하십시오.
   - 높음 - 항상 Machine Learning 분석당 최대 사용자 수까지 사용자가 추적됩니다.
   - 보통 - 우선순위가 높음인 모든 사용자가 포함된 이후 가장 높은 위험에 의해 사용자가 추적됩니다.
   - 없음 - Machine Learning에서 사용자가 추적되지 않습니다.
6. **다음**을 클릭하십시오.



7. **멤버십 설정** 탭에서 참조 세트, 정규식 또는 둘 다를 통해 자동으로 관심 목록을 사용자로 채울 수 있습니다.

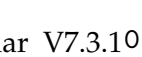
8. 옵션: **QRadar 참조 세트에서 가져오기** 필드에서 참조 세트를 검색하거나 목록에서 참조세트를 선택하여 참조세트의 모든 항목을 가져오십시오. 참고: 이 목록은 사용자 이름이 없는 참조 세트를 포함할 수 있습니다. 참조 세트를 선택한 후 검토할 링크를 클릭하십시오.
9. 옵션: **regex 필터를 사용하여 모니터 대상 사용자에서 추가** 필드에서 사용자 특성을 선택하고 유효한 Python 정규식을 입력하여 UBA 데이터베이스에서 이미 찾은 사용자를 선택할 수 있습니다.
10. **새로 고치기 간격** 필드에 사용자 목록을 업데이트할 빈도를 시간 단위로 입력하십시오. 예를 들어, 10을 입력하면 사용자 목록은 10시간마다 업데이트됩니다. **새로 고치기 간격**이 값 0으로 설정되는 경우 **새로 고치기**를 클릭하여 관심 목록을 수동 업데이트할 수 있습니다.
11. **저장**을 클릭하십시오.



신뢰할 수 있는 사용자를 위한 화이트리스트 보기

참조 세트 관리 목록에서 화이트리스트에 포함된 신뢰할 수 있는 사용자의 목록을 볼 수 있습니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. 시스템 구성 섹션에서 **참조 세트 관리**를 클릭하십시오.
3. 참조 세트 관리 창에서 **UBA : Trusted Usernames** 참조 세트를 선택하십시오.
4. **컨텐츠 보기**를 클릭하십시오.

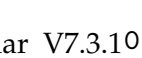
네트워크 모니터링 도구 관리

IBM QRadar User Behavior Analytics(UBA) 앱에 대한 네트워크 모니터링 도구를 관리할 수 있습니다.

이 태스크 정보

네트워크 캡처, 모니터링 또는 분석 프로그램 사용의 사용을 모니터하려는 경우, UBA : Network Capture, Monitoring and Analysis Program Filenames 참조 세트에 프로그램이 나열되어 있는지 확인하십시오. 그리고 나서 **UBA : Network Capture, Monitoring and Analysis Program Filenames** 룰을 사용으로 설정해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. 시스템 구성 섹션에서 **참조 세트 관리**를 클릭하십시오.
3. 참조 세트 관리 창에서 **UBA : Network Capture, Monitoring and Analysis Program Filenames** 참조 세트를 선택하십시오.
4. **컨텐츠 보기**를 클릭하십시오.
5. 관리할 애플리케이션을 추가하려면 상자에서 **추가**를 클릭하고 값을 입력하십시오.
6. 애플리케이션을 제거하려면 애플리케이션을 선택하고 **삭제**를 클릭하십시오.

다음에 수행할 작업

UBA : Network Capture, Monitoring and Analysis Program Filenames 룰을 사용으로 설정하십시오.

제한된 프로그램 관리

IBM QRadar User Behavior Analytics(UBA) 앱에 대한 제한된 프로그램을 관리할 수 있습니다.

이 태스크 정보

사용을 모니터하려는 애플리케이션이 있으면 UBA : Restricted Program Filenames 참조 세트로 이동하여 모니터하려는 애플리케이션을 입력하십시오. 그리고 나서 UBA : Restricted Program Filenames 룰을 사용으로 설정해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. 시스템 구성 섹션에서 **참조 세트 관리**를 클릭하십시오.
3. 참조 세트 관리 창에서 **UBA : Restricted Program Filenames** 참조 세트를 선택하십시오.
4. **컨텐츠 보기**를 클릭하십시오.
5. 관리할 애플리케이션을 추가하려면 상자에서 **추가**를 클릭하고 값을 입력하십시오.
6. 애플리케이션을 제거하려면 애플리케이션을 선택하고 **삭제**를 클릭하십시오.

다음에 수행할 작업

UBA : Restricted Program Filenames 룰을 사용으로 설정하십시오.

신뢰할 수 있는 로그 소스 그룹에 로그 소스 추가

UBA 앱에서 특정 로그 소스를 모니터링하고 보고하지 않게 하려는 경우, **UBA : Trusted Log Source Group**에 추가할 수 있습니다. 로그 소스를 그룹에 추가하면 UBA 앱은 그에 대한 모니터링을 중지합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **로그 소스** 아이콘을 클릭하십시오.
3. **추가**를 클릭하십시오.
4. 로그 소스에 대한 공통 매개변수를 구성하십시오.

5. 로그 소스에 대한 프로토콜 특정 매개변수를 구성하십시오.
6. **UBA : Trusted Log Source Group** 선택란을 선택하십시오.
7. **저장**을 클릭하십시오.
8. **관리** 탭에서 **변경사항 배치**를 클릭하십시오.

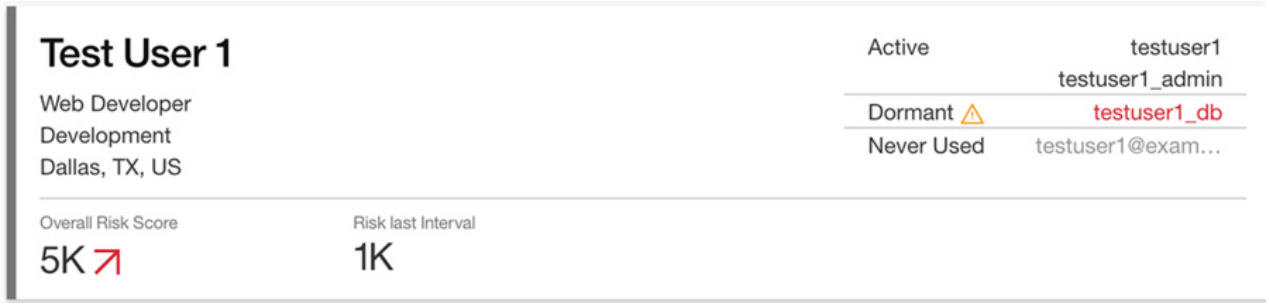
비활성 계정

비활성 계정, 활성 계정 또는 사용되지 않은 계정이 있는 시스템의 사용자를 볼 수 있습니다.

사용자 세부사항 페이지에서 비활성 계정 보기

V3.2.0 이상에서는 사용자 세부사항 페이지에서 선택한 사용자와 연관된 계정의 상태를 볼 수 있습니다.

사용자 계정 상태	설명
활성	UBA가 구성된 비활성 계정 임계값 기간 내에 QRadar 로그 소스에서 이벤트를 확인한 계정.
비활성 상태	UBA가 과거에 한 개 이상의 이벤트를 보았지만 비활성 계정 임계값 기간 동안 새 이벤트를 보지 못한 계정.
사용되지 않음	UBA가 QRadar 로그 소스에서 해당 사용자 이름이 포함된 이벤트를 보지 못한 계정. "사용되지 않음"으로 식별된 계정은 다음 활동에 의해 초래될 수 있습니다. • 연관된 사용자 이름 계정에 대해 QRadar 로그 소스에 의해 로깅된 적이 없는 계정. • UBA V3.2.0이 설치되기 전에 이벤트가 발생했습니다. 참고: UBA 앱을 처음 설치하면 최근 1시간 동안 발생한 이벤트만 분석되어 계정에 마지막으로 액세스한 시간을 식별합니다. 초기 분석 후에 UBA 앱은 계정 사용량을 감시하는 백그라운드 태스크의 실행 사이에 발생한 이벤트를 조회합니다. 참고: "사용되지 않음"으로 분류된 계정은 LDAP 앱에서 가져왔을 수 있습니다.



비활성 계정 관심 목록에 포함된 사용자

UBA 앱이 사용자 데이터를 가져올 때 비활성 계정 관심 목록에 포함된 사용자가 자동으로 생성됩니다. UBA 대시보드에 비활성 계정 관심 목록으로 사용자가 표시될 수 있습니다.

관심 목록을 삭제한 경우, 자동으로 다시 작성되지 않습니다. 다시 작성해야 하는 경우, 관심 목록 작성 화면의 **멤버십 설정** 탭에서 **UBA : 비활성 계정** 참조 세트를 선택하십시오.

비활성 계정 임계값 구성

비활성 계정 임계값의 기본값은 14일입니다. UBA 설정 페이지(**관리 설정** > **사용자 분석** > **UBA 설정**)의 애플리케이션 설정 섹션에서 비활성 상태로 간주되는 사용자가 비활성 상태인 일 수를 변경할 수 있습니다.

비활성 계정 또는 사용자에 대한 응답

제공된 룰에서 비활성 계정에 대한 응답을 생성할 수 있습니다. 앱에서 트리거되는 이벤트를 사용하여 사용자 정의 응답을 작성할 수도 있습니다.

비활성 계정이 사용되거나 사용이 시도될 때 사용자의 점수가 증가되도록 제공된 룰을 사용하려면 다음 룰이 사용으로 설정되어 있는지 확인하십시오.

- 87 페이지의 『UBA : Dormant Account Use Attempted』
- 86 페이지의 『UBA : Dormant Account Used』

사용자 정의 응답을 작성하려면 룰 또는 조회에서 다음 생성된 이벤트를 사용할 수 있습니다.

- 비활성 계정이 발견됨(QID 104000012)
- 비활성 계정이 사용됨(QID 104000013)

관련 개념:

12 페이지의 『UBA 대시보드 및 사용자 세부사항』
IBM QRadar User Behavior Analytics(UBA) 앱은 네트워크에서 사용자에 대한 전체적인 위험 데이터를 표시합니다.

관련 태스크:

33 페이지의 『애플리케이션 설정 구성』
IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 애플리케이션 설정을 구성해야 합니다.

39 페이지의 『관심 목록 작성』
새 관심 목록 또는 기존 관심 목록에 사용자를 추가할 수 있습니다.

6 튜닝

성능 개선을 위한 인덱스 사용

IBM QRadar User Behavior Analytics(UBA) 앱의 성능을 개선하려면 IBM QRadar에서 인덱스를 사용으로 설정하십시오.

이 태스크 정보

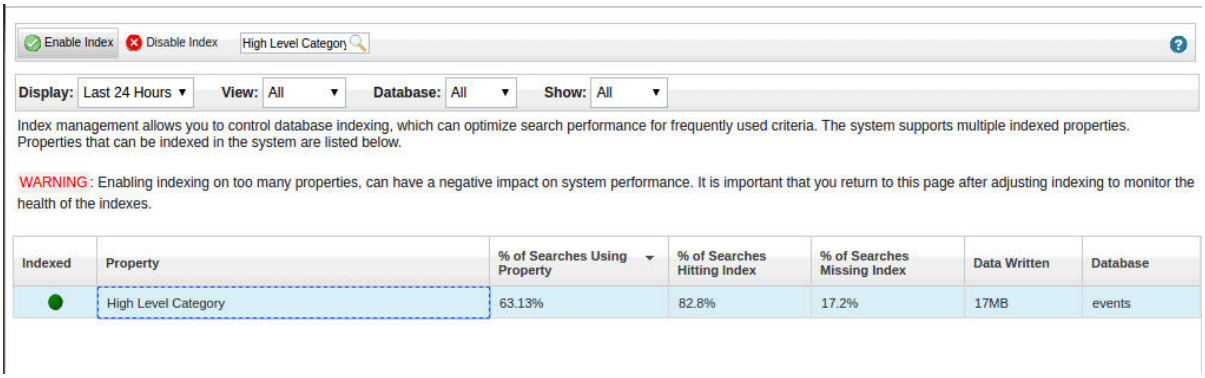
IBM QRadar 및 UBA 앱에서 검색 속도를 개선하려면 검색 조회에 인덱싱된 다음 필드를 추가하여 전체 데이터의 범위를 좁히십시오.

- 상위 레벨 카테고리
- 하위 레벨 카테고리
- senseValue
- senseOverallScore
- 사용자 이름

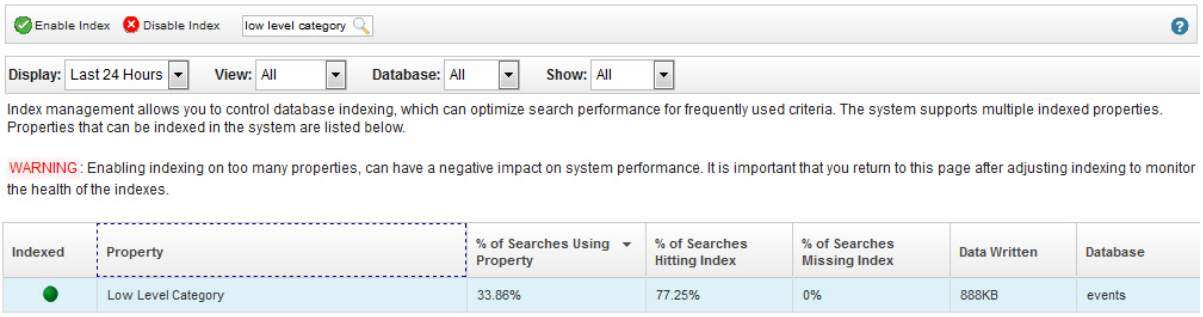
인덱싱에 대한 자세한 정보는 IBM Knowledge Center(https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_index_mgmt.html)의 다음 섹션을 참조하십시오.

프로시저

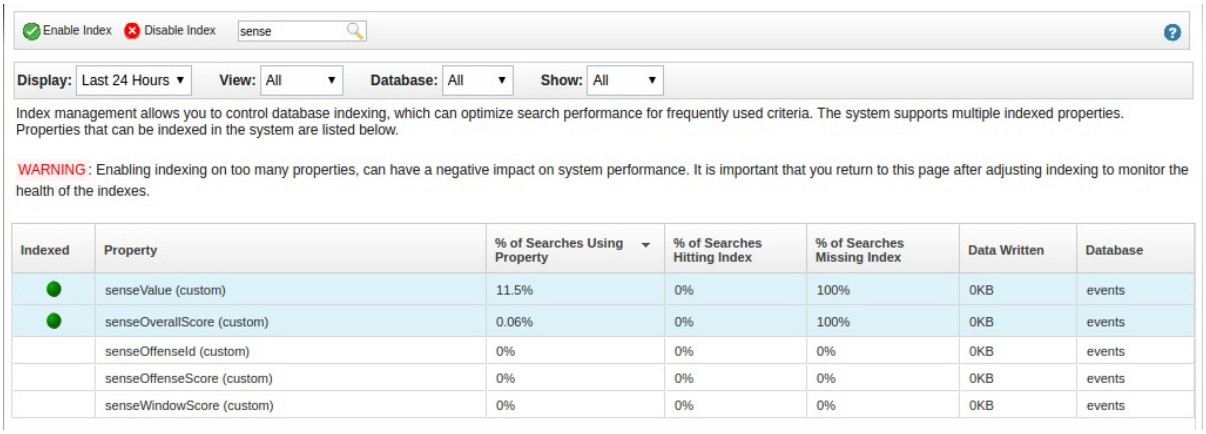
1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. 시스템 구성 섹션에서 **인덱스 관리** 아이콘을 클릭하십시오.
3. 인덱스 관리 페이지의 검색 상자에서 상위 레벨 카테고리를 입력하십시오.
4. **상위 레벨 카테고리**를 선택한 다음 **인덱스 사용**을 클릭하십시오.



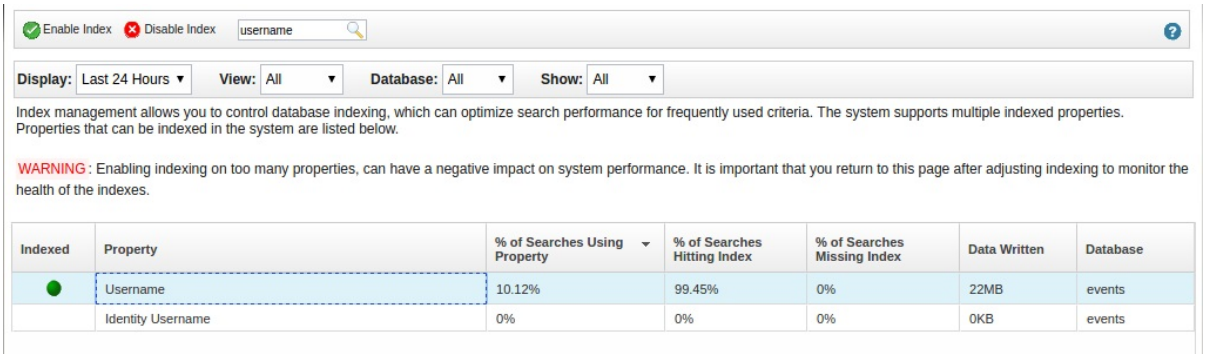
5. **저장**을 클릭하십시오.
6. **하위 레벨 카테고리**를 선택한 다음 **인덱스 사용**을 클릭하십시오.



7. **저장**을 클릭하십시오.
8. 인덱스 관리 페이지의 검색 상자에 sense를 입력하십시오.
9. **senseValue** 및 **senseOverallScore**를 선택한 다음 **인덱스 사용**을 클릭하십시오.



10. **저장**을 클릭하십시오.
11. 인덱스 관리 페이지의 검색 상자에 사용자 이름을 입력하십시오.
12. **사용자 이름**을 선택한 다음 **인덱스 사용**을 클릭하십시오.



13. **저장**을 클릭하십시오.

기존 또는 새 QRadar 컨텐츠를 UBA 앱과 통합

QRadar의 룰 마법사를 사용하여 기존 또는 사용자 정의 QRadar 룰을 UBA 앱과 통합할 수 있습니다.

이 태스크 정보

특정한 요구사항을 충족시키기 위해 기존 QRadar 룰을 UBA 앱과 통합하여 QRadar에 빌드된 기능을 사용할 수 있습니다.

제한사항: UBA 및 Machine Learning 참조 세트를 사용하도록 룰을 사용자 정의하지 마십시오. 사용자 정의 룰에서 참조 세트를 사용하려고 하면 UBA 앱에 장애가 발생할 수 있습니다.

프로시저

1. 기존 룰의 사본을 작성하십시오. 이렇게 하면 기본 룰에 대한 업데이트가 새 룰에 적용된 편집에 영향을 미치지 않습니다.
2. 룰 마법사에서 룰을 연 후 룰 응답 섹션을 탐색하십시오.
3. **이벤트 설명** 텍스트가 다음과 같이 형식화되어 있는지 확인하여 **새 이벤트 디스패치** 옵션을 사용으로 설정하거나 편집하십시오. `senseValue=#,senseDesc='sometext',usecase_id='rule UUID'`
4. **상위 레벨 카테고리**를 **감지**로 설정하십시오.
5. **완료**를 클릭하여 변경사항을 저장하십시오.

   참고: 룰이 플로우 데이터에서 작동하는 경우 사용자 이름이 없는 이벤트가 사용자 맵핑 검색을 시도할 수 있도록 **이벤트 또는 플로우 데이터에 대한 사용자 이름이 사용 불가능한 경우 자산에서 사용자 이름 검색** 옵션을 사용으로 설정해야 합니다.

참조 세트

User Behavior Analytics 앱 및 Machine Learning 앱에서는 사용자 정보를 저장하는 데 참조 세트를 사용합니다. 일부 참조 세트는 앱 전용으로 예약되어 있으므로 수정하거나 사용자 정의 룰을 작성할 때 사용해서는 안됩니다.

사용자 정의할 수 있는 참조 세트

참조 세트	설명
UBA : High Risk Users	*UBA : High Risk Users* 참조 세트는 UBA 설정 페이지의 **오펜스 트리거 위험 임계값** 값에서 빌드됩니다. 최대 사용자 수는 10,000명이며 참조 세트는 5분마다 다시 작성됩니다.
UBA : Trusted Usernames	*UBA : Trusted Usernames* 참조 세트에 사용자 이름을 추가할 수 있지만 룰 또는 보고서에는 사용하지 않습니다. *UBA : Trusted Usernames* 참조 세트의 사용자에 대해서는 오펜스가 생성되지 않습니다.
UBA : ML Always Tracked Watchlist	*UBA : ML Always Tracked Watchlist* 참조 세트는 사용자 세부사항 페이지의 **고급 설정** 섹션에서 **Machine Learning으로 추적**하도록 선택한 사용자에서 빌드됩니다. *UBA : ML Always Tracked Watchlist* 참조 세트에 사용자 이름을 추가할 수 있지만 룰 또는 보고서에는 사용하지 않습니다.

사용자 정의할 수 없는 참조 세트

제한사항: 사용자 정의 룰 작성을 위해 다음 참조 세트를 수정하거나 사용하지 마십시오.

- UBA - Current ML Tracked Users
- UBA - Previous ML Tracked Users
- UBA - Current Abridged ML Tracked Users
- UBA - Previous Abridged ML Tracked Users
- UBA - Current Peer Group ML Tracked Users
- UBA - Previous Peer Group ML Tracked Users

7 UBA 앱에 대한 룰 및 튜닝

IBM QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

User Behavior Analytics(UBA) 앱에는 사용자 정의 룰을 기반으로 하는 유스 케이스가 포함되어 있습니다. 이러한 룰은 UBA 앱 대시보드에 대한 데이터를 생성하는 데 사용됩니다. UBA 앱 V3.0.0부터는 UBA 앱 내에서 룰을 보고 필터링하고 튜닝할 수 있습니다. V2.8.0 이상에서는 QRadar의 룰 목록의 User Behavior Analytics 그룹에서 룰을 보고 수정할 수 있습니다.

참고:

- 기본적으로 모든 UBA 앱 룰이 사용 가능하게 설정되지는 않습니다.
- 하나 이상의 로그 소스는 특정 UBA 룰에 대한 정보를 제공해야 합니다. 로그 소스는 특정한 순서로 우선순위가 지정되지 않습니다.

제한사항: UBA 및 Machine Learning 참조 세트를 사용하도록 룰을 사용자 정의하지 마십시오. 사용자 정의 룰에서 참조 세트를 사용하려고 하면 UBA 앱에 장애가 발생할 수 있습니다. 추가 정보는 50 페이지의 『참조 세트』의 내용을 참조하십시오.

QRadar에서 룰에 대한 작업과 관련한 자세한 정보는 https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html의 내용을 참조하십시오.

룰 및 튜닝 페이지

UBA 앱 V3.0.0에서는 룰 및 튜닝 페이지(**관리 설정** > **사용자 분석** > **룰 및 튜닝**)가 도입됩니다.

룰 및 튜닝 페이지에는 설치된 UBA 앱 버전에 포함된 모든 룰 목록이 포함되어 있습니다. 현재 사용 설정 상태 및 해당 참조 세트도 함께 포함되어 있습니다.

룰 및 튜닝 페이지에서 다음을 수행할 수 있습니다.

- 룰을 사용 또는 사용 안함으로 설정
- QRadar 룰 마법사에 빠르게 액세스하여 결과를 검토하거나 편집
- 참조 세트에 빠르게 액세스하여 해당 컨텐츠를 검토하거나 편집
- 카테고리, 상태, 기본 위험성 점수, 필요한 참조 세트 및 컨텐츠 종속 항목별로 룰 테이블 필터링
- 룰 이름, 참조 세트 또는 상태별로 룰 테이블 정렬
- 테이블에 있는 항목 또는 룰 설명 도구 팁에서 찾은 단어 검색
- 개별 룰의 도움말 문서에 액세스

액세스 및 인증

UBA : Bruteforce Authentication Attempts

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Bruteforce Authentication Attempts

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

인증 실패 무작위 대입 공격(수평 및 수직)을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures
- BB:UBA : Detecting Authentication Bruteforce Attempts (Horizontal)
- BB:UBA : Detecting Authentication Bruteforce Attempts (Vertical)

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : Executive Only Asset Accessed by Non-Executive User

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Executive Only Asset Accessed by Non-Executive User

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

임원이 아닌 사용자가 임원만 사용할 수 있는 자산에 로그온하는 경우를 발견합니다. 이 룰을 사용하여 두 개의 비어 있는 참조 세트 "UBA : Executive Users" 및 "UBA : Executive Assets"를 가져옵니다. 참조 세트를 편집하여 사용자 환경에서 플래그 지정된 계정 및 IP 주소를 추가하거나 제거하십시오. 참조 세트를 구성한 후 이 룰을 사용으로 설정하십시오.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:CategoryDefinition: Firewall or ACL Accept

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Executive Users" 및 "UBA : Executive Assets"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : High Risk User Access to Critical Asset

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : High Risk User Access to Critical Asset

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

인시던트(오펜스)와 관련된 사용자가 중요 자산에 액세스하는 경우를 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "Critical Assets"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : Multiple VPN Accounts Failed Login From Single IP

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Multiple VPN Accounts Failed Login From Single IP

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

"UBA : Multiple VPN Accounts Failed Login From Single IP" 참조 세트에서 VPN 계정 로그인 실패를 발견합니다.

지원 룰

- UBA : Populate Multiple VPN Accounts Failed Login From Single IP
- BB:UBA : VPN Login Failed

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : Populate Multiple VPN Accounts Failed Login From Single IP"

데이터 소스

Cisco Adaptive Security Appliance(ASA)

UBA : Multiple VPN Accounts Logged In From Single IP

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Multiple VPN Accounts Logged In From Single IP

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

동일한 IP 주소를 사용하는 여러 VPN 사용자를 맵핑한 다음 위험성 점수를 높입니다. 룰이 동일한 IP 주소를 사용하는 VPN 사용자를 발견하면 IP 주소가 "UBA : Multiple VPN Accounts Logged In From Single IP"에 추가됩니다. 이 룰을 사용으로 설정하기 전에 룰 "UBA : Populate Multiple VPN Accounts Logged In From Single IP"가 사용 가능하고 "UBA : Multiple VPN Accounts Logged In From Single IP" 참조 세트에 데이터가 있는지 확인하십시오.

지원 룰

- UBA : Populate Multiple VPN Accounts Logged In from Single IP
- BB:UBA : VPN Login Successful

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : Populate Multiple VPN Accounts Logged In from Single IP"

데이터 소스

Cisco Adaptive Security Appliance(ASA)

UBA : Repeat Unauthorized Access

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Repeat Unauthorized Access

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

권한이 없는 액세스 활동이 반복되었음을 표시합니다.

지원 룰

UBA : Unauthorized Access

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : Unauthorized Access"

데이터 소스

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 & 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 및 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 : Unauthorized Access

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unauthorized Access

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

권한 없는 액세스 활동이 발견되었음을 표시합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Access Denies
- BB:UBA : Application Denies

데이터 소스

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 & 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 및 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 : Unix/Linux System Accessed With Service or Machine Account

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unix/Linux System Accessed With Service or Machine Account

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

UNIX 및 Linux 서버의 서비스 또는 시스템 계정에서 시작하는 대화식 세션(GUI 및 CLI 사용, 로컬 및 원격 로그인 모두 해당)을 발견합니다. 계정 및 허용되는 대화식 세션은 UBA : Service, Machine Account 및 UBA : Allowed Interaction Session 참조 세트에 나열됩니다. 참조 세트를 편집하여 사용자 환경에서 플래그 지정할 대화식 세션을 추가 또는 제거하십시오.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Firewall or ACL Accept
- BB:CategoryDefinition: Authentication Success

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Service, Machine Account" 및 "UBA : Allowed Interactive Session"

데이터 소스

Linux OS

UBA : User Access - Failed Access to Critical Assets

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access - Failed Access to Critical Assets

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

이 룰은 위험 자산 참조 세트에 위치한 시스템에 대한 인증 실패를 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "Critical Assets"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access - First Access to Critical Assets

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

다음을 지원합니다.

- UBA : User Access First Access to Critical Assets
- UBA : Critical Systems Users Seen Update

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

UBA : User Access First Access to Critical Assets: 사용자가 중요 자산에 액세스한 것이 이번이 처음임을 표시합니다. "Critical Systems Users Seen" 참조 콜렉션은 관찰의 TTL(time-to-live)을 관리합니다. 기본적으로 이 룰은 3개월의 첫 번째 액세스를 발견합니다.

UBA : Critical Systems Users Seen Update: 이미 존재하는 대상 IP/사용자 이름 일치 항목에 대한 "Critical Systems Users Seen" 참조 콜렉션에서 마지막으로 확인된 값을 업데이트합니다.

지원 룰

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "Critical Assets"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access from Multiple Hosts

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : UBA : User Access from Multiple Hosts

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

단일 사용자가 허용된 수보다 많은 디바이스에서 로그인하는 경우를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access to Internal Server From Jump Server

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access to Internal Server From Jump Server

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

사용자가 점프 서버를 사용하여 VPN 또는 내부 서버에 액세스할 때 발견됩니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Jump Servers" 및 "UBA : Internal Servers"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access Login Anomaly

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access Login Anomaly

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

로컬 자산에서 일련의 로그인 실패를 표시합니다. 룰은 계정 손상 또는 측면 이동 활동을 표시할 수도 있습니다. 하나의 사용자 이름 룰에 대한 다중 로그인 실패가 사용으로 설정되어 있는지 확인하십시오. 이 룰에 대한 일치 및 시간 지속 기간 매개변수를 조정하여 반응성을 조정하십시오.

지원 룰

- BB:UBA : Common Event Filters
- Multiple Login Failures for Single Username

필수 구성

다음 룰을 사용으로 설정하십시오. "Multiple Login Failures for Single Username"

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Account from Anonymous Source

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Account from Anonymous Source

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

사용자가 TOR 또는 VPN과 같은 익명 소스에서 내부 자원에 액세스하고 있음을 표시합니다.

지원 룰

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

필수 구성

관리 설정 > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Time, Access at Unusual Times

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Time, Access at Unusual Times

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

"UBA: Unusual Times, %" 빌딩 블록에 의해 정의된 대로 사용자가 사용자의 네트워크에 일반적이지 않은 시간에 정상적으로 인증하고 있음을 표시합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Unusual Times, Evening
- BB:UBA : Unusual Times, Overnight

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : VPN Access By Service or Machine Account

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : VPN Access By Service or Machine Account

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

서비스 또는 시스템 계정에서 Cisco VPN에 액세스하는 경우를 발견합니다. 계정은 'UBA : Service, Machine Account' 참조 세트에 나열됩니다. 이 목록을 편집하여 사용자 환경에서 플래그를 지정할 계정을 추가하거나 제거하십시오.

지원 룰

BB:UBA : VPN Mapping(로직)

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Service, Machine Account"

데이터 소스

Cisco Adaptive Security Appliance(ASA)

UBA : VPN Certificate Sharing

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : VPN Certificate Sharing

기본적으로 사용 가능

True

참고: UBA : VPN Certificate Sharing 룰을 사용하려는 경우 Cisco 방화벽 DSM을 다음과 같이 업데이트해야 합니다.

- V7.2.8의 경우: `DSM-CiscoFirewallDevices-7.2-20170619124928.noarch.rpm`
- V7.3.0 이상의 경우: `DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm`

senseVaule 기본값

15

설명

이 룰은 VPN 이벤트의 사용자 이름이 'VPNSubjectcn'과 같지 않은 경우를 발견합니다. 이는 VPN 인증서 공유가 발생했음을 표시할 수 있습니다. 인증서가 공유되거나 기타 인증 토큰이 공유되면 작업자 및 작업자가 수행한 작업을 식별하기 어려울 수 있습니다. 이는 침해가 발생하는 경우에 다음 단계를 수행하는 것을 복잡하게 만들 수 있습니다.

지원 룰

- BB:UBA : VPN Mapping(로직)
- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

이러한 룰은 필수 데이터로 연관된 참조 세트를 업데이트합니다.

필수 구성

다음 룰을 사용으로 설정하십시오.

- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

데이터 소스

Cisco Adaptive Security Appliance(ASA)

UBA : Windows Access with Service or Machine Account

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Windows Access with Service or Machine Account

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

Windows Server의 서비스 또는 시스템 계정에서 시작하는 대화식 세션(RDP, 로컬 로그인)을 발견합니다. 계정은 UBA : Service, Machine Account 참조 세트에 나열됩니다. 목록을 편집하여 사용자 환경에서 플래그를 지정할 계정을 추가하거나 제거하십시오.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Service, Machine Account"

데이터 소스

Microsoft Windows Security Event Log (이벤트 ID: 4776)

계정 및 권한

UBA : Account or Group or Privileges Added

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Account or Group or Privileges Added(이전에는 UBA : Account, Group or Privileges Added or Modified라고 함)

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 수행하고 있으며 다음 카테고리 중 하나에 맞는 이벤트를 발견합니다. 룰은 원래 사용자의 위험성 점수를 늘리기 위해 IBM Sense 이벤트를 디스패치합니다.

- Authentication.Group 추가됨
- Authentication.Group 변경됨

- Authentication.Group Member 추가됨
- Authentication.Computer Account 추가됨
- Authentication.Computer Account 변경됨
- Authentication.Policy 추가됨
- Authentication.Policy 변경
- Authentication.Trusted Domain 추가됨
- Authentication.User Account 추가됨
- Authentication.User Account 변경됨
- Authentication.User Right 지정됨

참고: 사용자의 전체 위험성 점수에 대한 이 룰의 영향을 조정하려면 사용자의 조직에 해당하는 이벤트 카테고리를 추가하여 빌딩 블록 룰 "CategoryDefinition: Authentication User or Group Added / Changed"를 수정하는 것을 고려하십시오.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Added

데이터 소스

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 & 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 및 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 : Account or Group or Privileges Modified

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Account or Group or Privileges Modified(이전에는 UBA : User Account Change라고 함)

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

사용자의 유효 권한을 위 또는 아래로 변경하는 조치에 의해 사용자 계정이 언제 영향을 받았는지를 표시합니다.

False Positive 참고: 이 이벤트는 계정 이름에 대한 수정을 변경사항을 작성하는 사용자에게 잘못 지정할 수 있습니다. 이 False Positive를 줄이려는 경우, 테스트 'and when Username equals AccountName'을 추가할 수 있습니다.

False Negative 참고: 이 이벤트는 사용자에 대한 계정이 수정된 경우를 모두 발견할 수는 없습니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Changed

데이터 소스

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

UBA : DoS Attack by Account Deletion

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : DoS Attack by Account Deletion

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

일정한 기간 내의 고정 임계값에 대해 계정 삭제 이벤트 수를 확인하여 DoS 공격을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : User Account Deleted

데이터 소스

Amazon AWS CloudTrail(이벤트 ID: DeleteUser)

Application Security DbProtect(이벤트 ID: Login revoked - Windows, Login dropped - standard, Database role - dropped, Database user revoked)

Aruba Mobility Controller(이벤트 ID: authmgr_user_del)

Box(이벤트 ID: DELETE_USER)

Brocade FabricOS(이벤트 ID: SEC-1181, SEC-3028)

CA ACF2(이벤트 ID: ACF2-L)

Check Point(이벤트 ID: user_deleted, device_deleted, User Deleted)

Cilasoft QJRN/400(이벤트 ID: C20020)

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

Cisco FireSIGHT Management Center(이벤트 ID: USER_REMOVED_CHANGE_EVENT)

Cisco Firewall Services Module(FWSM)(이벤트 ID: 502102)

Cisco Identity Services Engine(이벤트 ID: 86008, 86028)

Cisco NAC Appliance(이벤트 ID: CCA-1453, CCA-1502)

Cisco Nexus(이벤트 ID: SECURITYD-6-DELETE_STALE_USER_ACCOUNT)

Cisco Wireless LAN Controllers(이벤트 ID: 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo(이벤트 ID: Halo user deleted, Local account deleted(linux에만 해당))

CorreLog Agent for IBM zOS(이벤트 ID: RACF DELUSER: No Violations)

Custom Rule Engine(이벤트 ID: 3035, 3043)

Cyber-Ark Vault(이벤트 ID: 276)

EMC VMWare(이벤트 ID: AccountRemovedEvent)

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

Extreme Matrix K/N/S Series Switch(이벤트 ID: User Deleted Event, has been deleted)

Extreme NAC(이벤트 ID: Deleted registered user)

Extreme NetsightASM(이벤트 ID: UserRemove)

Flow Classification Engine(이벤트 ID: 3035, 3043)

Forcepoint Sidewinder(이벤트 ID: passport deletion, all passports revoked)

HBGary Active Defense(이벤트 ID: DeleteUser)

HP Network Automation(이벤트 ID: User Deleted)

Huawei S Series Switch(이벤트 ID: SSH/6/DELUSER_SUCCESS)

IBM AIX Audit(이벤트 ID: USER_Remove SUCCEEDED)

IBM AIX Server(이벤트 ID: USER_Remove)

IBM DB2(이벤트 ID: DROP_USER SUCCESS)

IBM DataPower(이벤트 ID: 0x81000136)

IBM IMS(이벤트 ID: USER DELETED)

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

IBM QRadar Packet Capture(이벤트 ID: UserDeleted)

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

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

IBM Security Directory Server(이벤트 ID: SDS Audit)

IBM Security Identity Governance(이벤트 ID: 50, 43, 70005)

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

IBM SmartCloud Orchestrator(이벤트 ID: user)

IBM Tivoli Access Manager for e-business(이벤트 ID: 13408 - Succeeded, 13408 Command Succeeded)

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

IBM z/OS(이벤트 ID: 80 1.35)

Juniper Networks Network and Security Manager(이벤트 ID: adm24473)

Linux OS(이벤트 ID: userDel, Account Deleted, DEL_USER)

McAfee Application/Change Control(이벤트 ID: USER_ACCOUNT_DELETED)

McAfee ePolicy Orchestrator(이벤트 ID: 20793)

Microsoft ISA(이벤트 ID: user removed)

Microsoft Office 365(이벤트 ID: Delete User-PartiallySucceded, Delete user-success, Delete User-success, Delete user-PartiallySucceded)

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

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

Netskope Active(이벤트 ID: Delete Admin, Deleted admin)

Nortel Application Switch(이벤트 ID: User Deleted)

Novell eDirectory(이벤트 ID: DELETE_ACCOUNT)

OS Services Qidmap(이벤트 ID: Account Deleted, User Deleted)

OSSEC(이벤트 ID: 18112)

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

Oracle Enterprise Manager(이벤트 ID: Computer Delete (successful), User Delete (successful))

Oracle RDBMS Audit Record(이벤트 ID: DROP USER-Standard:1, 53:1, 53:0,DROP USER-Standard:0, 53)

PGP Universal Server(이벤트 ID: ADMIN_DELETED_USER)

Palo Alto Endpoint Security Manager(이벤트 ID: User Deleted)

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

RSA Authentication Manager(이벤트 ID: unknown, Deleted user, REMOVE_ORPHANED_PRINCIPALS, REMOTE_PRINCIPAL_DELETE, DELETE_PRINCIPAL)

SIM Audit(이벤트 ID: Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT(이벤트 ID: Active DirectorycomputerObject DeletedTrueFalse, Active DirectoryuserObject DeletedTrueFalse, Console user/group deleted, Console user/group deleted)

SafeNet DataSecure/KeySecure(이벤트 ID: Removed user)

Skyhigh Networks Cloud Security Platform(이벤트 ID: 10017)

Solaris BSM(이벤트 ID: delete user)

SonicWALL SonicOS(이벤트 ID: 559, 1157, 1158)

Trend Micro Deep Security(이벤트 ID: 651)

Universal DSM(이벤트 ID: Computer Account Removed, User Account Removed)

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

Vormetric Data Security(이벤트 ID: DAO0090I)

iT-CUBE agileSI(이벤트 ID: AU8, U0)

UBA : User Account Created and Deleted in a Short Period of Time

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Account Created and Deleted in a Short Period of Time

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

사용자 계정이 짧은 시간 내에 작성되고 삭제되는 상황을 발견합니다.

지원 룰

- BB:UBA : User Account Created
- BB:UBA : User Account Deleted
- BB:UBA : Common Event Filters

데이터 소스

UBA : Dormant Account Used

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Dormant Account Used

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

비활성 상태인 것으로 판별된 계정에서의 정상적인 로그인을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

데이터 소스

이벤트에 사용자 이름을 제공하는 지원되는 로그 소스.

UBA : Dormant Account Use Attempted

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Dormant Account Use Attempted

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

비활성 상태인 것으로 판별된 계정에서의 실패한 로그인을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : Expired Account Used

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Expired Account Used(이전에는 UBA : Orphaned or Revoked or Suspended Account Used라고 함)

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

로컬 시스템에서 사용 안함으로 설정되었거나 만료된 계정에 사용자가 로그인을 시도했음을 표시합니다. 이 룰은 계정이 손상되었음을 암시할 수도 있습니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication to Expired Account

데이터 소스

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 : First Privilege Escalation

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : First Privilege Escalation

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

사용자가 처음으로 권한이 필요한 액세스를 실행했음을 표시합니다. 기준선 설정 목적으로 사용자 행위패턴의 추적을 허용하도록 이 보고 룰을 사용 안함으로 설정할 수 있습니다.

지원 룰

BB:UBA : Privileged User, First Time Privilege Use(로직)

데이터 소스

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 및 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 : New Account Use Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : New Account Use Detected

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 처음으로 로그인했음을 표시하는 보고 기능을 제공합니다. 이 보고 룰은 기준선 설정 목적으로 임시로 사용 안함으로 설정될 수 있습니다.

지원 룰

BB:UBA : User First Time Access(로직)

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : Suspicious Privileged Activity (First Observed Privilege Use)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Privileged Activity (First Observed Privilege Use)

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 이전에 실행한 적이 없는 권한이 필요한 조치를 실행했음을 표시합니다. 관찰이 "UBA : Observed Activities by Low Level Category and Username" 맵 세트에 보관됩니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

데이터 소스

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 및 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 : Suspicious Privileged Activity (Rarely Used Privilege)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Privileged Activity (Rarely Used Privilege)

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

사용자가 최근에 실행하지 않은 권한이 필요한 조치를 실행했음을 표시합니다. 관찰이 "UBA : Recent Activities by Low Level Category and Username" 맵 세트에 보관됩니다. 이 이벤트의 민감도는 "UBA : Recent Activities by Low Level Category and Username"에 대한 참조 맵 세트의 TTL(time-to-live)을 변경하여 수정할 수 있습니다. TTL을 증가시키면 민감도가 감소됩니다. TTL을 줄이면 민감도가 증가됩니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

데이터 소스

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 및 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 : User Attempt to Use a Suspended Account

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Attempt to Use a Suspended Account

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

일시중단되었거나 사용 안함으로 설정된 계정에 사용자가 액세스를 시도했음을 발견합니다.

지원 룰

- BB:CategoryDefinition: Authentication to Disabled Account
- BB:UBA : Common Event Filters

데이터 소스

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

UBA : User Has Gone Dormant(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다. 비활성 계정 정보는 V3.2.0부터 UBA 대시보드에 표시됩니다. 추가 정보는 44 페이지의 『비활성 계정』의 내용을 참조하십시오.

UBA : User Has Gone Dormant(활동 비정상 룰 없음)

UBA : Dormant Account Found(권한 부여됨)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

이 룰을 활성화하려면 "UBA : User Has Gone Dormant(활동 비정상 룰 없음)"가 사용으로 설정되었는지 확인하십시오.

이 룰은 사용자 이름의 활동 수가 80%를 초과하여 변경되었음을 표시합니다. "UBA : User Dormant Account Found(권한 부여됨)" 및 "UBA : User Has Gone Dormant(활동 비정상 룰 없음)"는 사용자가 연장된 기간에 대해 생산 활동을 중지했음을 나타내고자 합니다. 이 조건은 사용자가 해당 사용자 이름과 연관된 활동의 장기간 부재에 따라 더 이상 액세스 권한이 필요하지 않음을 나타낼 수 있습니다. 사용자 이름의 활동이 짧은 간격 기간(기본값 14일) 동안에 0으로 떨어지고 0 이전이 새 기준선(기본값 28일)인 경우 잘못된 알람이 발생할 수 있습니다. "UBA : User Dormant Account Found(권한 부여됨)"에 대한 응답 빈도 한계가 사용자 이름별 긴 간격보다 크거나 같은 기간으로 설정된 경우 이는 사용자의 위험성 점수에 영향을 주지 않습니다.

참고: 사용자 이름의 활동이 짧은 간격 기간(기본값 14일) 동안에 0으로 줄어들고 0 이전이 새 기준선(기본값 28일)인 경우 'UBA : User Has Gone Dormant(활동 비정상 룰 없음)'에 대해 잘못된 알람이 발생할 수 있습니다. "UBA : User Dormant Account Found(권한 부여됨)"에 대한 응답 빈도 제한이 사용자 이름별 긴 간격보다 크거나 같은 기간의 시간으로 설정된 경우 잘못된 알람은 사용자의 위험성 점수에 영향을 미치지 않습니다.

지원 룰

UBA : Dormant Account Found(권한 부여됨)

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : Dormant Account Found(권한 부여됨)"

데이터 소스

지원되는 모든 로그 소스.

찾아보기 동작

UBA : Browsed to Business/Service Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Browsed to Business/Service Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Communications Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Communications Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Entertainment Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Entertainment Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Gambling Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Gambling Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Information Technology Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Information Technology Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Job Search Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Job Search Website

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to LifeStyle Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to LifeStyle Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Malicious Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Malicious Website

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Mixed Content/Potentially Adult Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Mixed Content/Potentially Adult Website

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Phishing Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Phishing Website

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Pornography Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Pornography Website

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Scam/Questionable/Illegal Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Scam/Questionable/Illegal Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : Browsed to Uncategorized Website

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Browsed to Uncategorized Website

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

사용자가 강화된 보안 또는 법적 위험을 표시할 수 있는 URL에 액세스했습니다.

지원 룰

BB:UBA : URL Category Filter

데이터 소스

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

UBA : User Accessing Risky URL

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA: User Accessing Risky URL(이전에는 X-Force Risky URL이라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자가 의심스러운 온라인 컨텐츠에 액세스하는 경우를 발견합니다.

지원 룰

- X-Force Risky URL
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky URL

데이터 소스

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

---

클라우드

UBA : AWS Console Accessed by Unauthorized User

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : AWS Console Accessed by Unauthorized User

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

'AWS - 표준 사용자' 참조 세트의 권한 부여 목록에 포함되지 않은 사용자가 AWS(Amazon Web Services) 콘솔에 액세스하려는 무단 시도를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

- IBM Security App Exchange(IBM QRadar Content Extension for Monitoring Amazon AWS)에서 다음 패키지를 설치하십시오.
- 적절한 값을 다음 참조 세트에 추가하십시오. "UBA : Domain Controller Administrators"는 Amazon AWS Cloudtrail 로그 소스를 구성합니다.

데이터 소스

Amazon AWS CloudTrail(이벤트 ID: ConsoleLogin)

UBA : Non-Standard User Accessing AWS Resources

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Non-Standard User Accessing AWS Resources

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

AWS(Amazon Web Services) 리소스에 액세스를 시도하고 있는 비표준 사용자를 발견합니다.

데이터 소스

Amazon Web Services Extension

도메인 컨트롤러

UBA : DPAPI Backup Master Key Recovery Attempted

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : DPAPI Backup Master Key Recovery Attempted

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

DPAPI 마스터 키에 대한 복구가 시도되는 경우를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Log(이벤트 ID: 4693)

UBA : Kerberos Account Enumeration Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Kerberos Account Enumeration Detected

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

동일한 소스 IP에서 Kerberos 요청을 수행하는 데 사용되는 많은 사용자 이름을 발견하여 Kerberos 계정 열거를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Log (이벤트 ID: 4768)

UBA : Multiple Kerberos Authentication Failures from Same User

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Multiple Kerberos Authentication Failures from Same User

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

여러 Kerberos 인증 티켓 거부 또는 실패를 발견합니다.

지원 룰

- BB:UBA : Common Log Source Filters
- BB:UBA : Kerberos Authentication Failures

데이터 소스

Microsoft Windows Security Event Log

UBA : Non-Admin Access to Domain Controller

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Non-Admin Access to Domain Controller

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

도메인 컨트롤러에 대한 비관리 계정 액세스 시도를 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:CategoryDefinition: Authentication Failures

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Domain Controllers" 및 "UBA : Domain Controller Administrators"

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : Pass the Hash

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Pass the Hash

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

pass the hash 악용 중에 생성되었을 수 있는 Windows 로그온 이벤트를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성:

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Trusted Domains

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4624)

UBA : Possible Directory Services Enumeration

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Possible Directory Services Enumeration

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

디렉토리 서비스 열거에 대한 탐색 시도를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Domain Controller Administrators"

데이터 소스

Microsoft Windows Security Event Log(이벤트 ID: 4661)

UBA : Possible SMB Session Enumeration on a Domain Controller

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Possible SMB Session Enumeration on a Domain Controller

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

도메인 컨트롤러에 대한 SMB 열거 시도를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오.

- UBA : Domain Controllers
- UBA : Domain Controller Administrators

데이터 소스

Microsoft Windows Security Event Log(이벤트 ID: 5140)

UBA : Possible TGT Forgery

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Possible TGT Forgery

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

도메인 이름 비정상이 포함된 Kerberos TGT를 발견합니다. 이는 Pass-the-Ticket 악용을 사용하여 생성된 티켓을 나타낼 수 있습니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Trusted Domains

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4768)

UBA : Possible TGT PAC Forgery

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Possible TGT PAC Forgery

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Kerberos TGS에서의 서비스 티켓을 가져오기 위해 위조된 PAC 인증서의 사용을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : TCT PAC Forgery Patched Server
- BB:UBA : TCT PAC Forgery Unpatched Server

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Domain Controller Administrators"

데이터 소스

Microsoft Windows Security Event Log(이벤트 ID: 4672, 4769)

UBA : Replication Request from a Non-Domain Controller

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Replication Request from a Non-Domain Controller

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

불법 도메인 컨트롤러에서의 복제 요청 발견

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Domain Controller Administrators"

데이터 소스

Microsoft Windows Security Event Log(이벤트 ID: 4662)

UBA : TGT Ticket Used by Multiple Hosts

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : TGT Ticket Used by Multiple Hosts

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

두 대(또는 그 이상)의 다른 컴퓨터에서 사용되는 Kerberos TGT 티켓을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

UBA : Kerberos Account Mapping

이 룰은 필수 데이터로 연관된 참조 세트를 업데이트합니다.

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : Kerberos Account Mapping"

데이터 소스

Microsoft Windows Security Event Log (이벤트 ID: 4768)

엔드포인트

UBA : Detect Insecure Or Non-Standard Protocol

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Detect Insecure Or Non-Standard Protocol

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

비보안 또는 비표준 프로토콜로 간주되는 권한 없는 프로토콜을 통해 통신하는 사용자를 발견합니다. 권한 있는 프로토콜은 UBA : Ports of Authorized Protocols 참조 세트에 나열되며 기본값은 0이고 이는 QRadar 이벤트의 포트입니다. 이 룰을 사용하려면 먼저 사용자 환경에서 플래그를 지정하도록 UBA : Ports of Authorized Protocols 참조 세트를 편집하십시오.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Insecure Ports
-

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Ports Of Authorized Protocols

데이터 소스

지원되는 모든 로그 소스.

UBA : Detect Persistent SSH session

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Detect Persistent SSH session

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

10시간 이상 활성 상태인 SSH 세션을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : SSH Session Closed
- BB:UBA : SSH Session Opened

필수 구성

이 룰에는 정확한 발견을 위해 발생하는 SSH 열림 및 SSH 닫힘 이벤트가 필요합니다. 사용되는 로그 소스에 두 이벤트에 해당하는 이벤트 ID가 없으면 부정확한 결과가 수신될 수 있습니다. 사용 중인 로그 소스의 이벤트 ID를 판별하려면 데이터 소스를 참조하십시오.

데이터 소스(SSH 열림)

Centrify Infrastructure Services(이벤트 ID: 27100, 27104)

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

Custom Rule Engine(이벤트 ID: 18037, 3071)

Cyber-Ark Vault(이벤트 ID: 378)

Extreme XSR Security Routers(이벤트 ID: NEW_SSH_CONNECTION)

Flow Classification Engine(이벤트 ID: 3071, 18037)

Huawei S Series Switch(이벤트 ID: SSH/4/SFTP_REQ_RECORD)

HyTrust CloudControl(이벤트 ID: AUN0120, 알 수 없음)

IBM AIX Server(이벤트 ID: sshd2 connection established, ssh-server connect, ssh-server session open)

IBM DataPower(이벤트 ID: 0x8100011e, 0x810001e4, 0x810001e5)

Juniper MX Series Ethernet Services Router(이벤트 ID: SSH)

Juniper Networks AVT(이벤트 ID: SSH)

Mac OS X(이벤트 ID: OSX ssh session started)

OS Services Qidmap(이벤트 ID: Connection from, pam_open_session, pam_sm_open_session)

Solaris Operating System Authentication Messages(이벤트 ID: ssh session opened)

Universal DSM(이벤트 ID: SSH Opened, SSH Session Started)

데이터 소스(SSH 닫힘)

Aruba Mobility Controller(이벤트 ID: sshd_disconnect)

Centrify Infrastructure Services(이벤트 ID: 27102)

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

Custom Rule Engine(이벤트 ID: 3072, 18038, 18040)

Cyber-Ark Vault(이벤트 ID: 380, 381)

Flow Classification Engine(이벤트 ID: 3072, 18038, 18040)

Huawei S Series Switch(이벤트 ID: SSH/6/RECV_DISCONNECT)

IBM AIX Server(이벤트 ID: ssh-server disconnect, sshd2 connection lost, SSH Disconnect, sshd2 local disconnect, ssh-server session close)

OS Services Qidmap(이벤트 ID: Done with connection, pam_sm_close_session, pam_close_session, Did not receive identification string, Connection timed out, Received disconnect from IP, Connection closed)

Pulse Secure Pulse Connect Secure(이벤트 ID: GWE24572)

Universal DSM(이벤트 ID: SSH Terminated, SSH Session Finished, SSH Closed)

UBA : Internet Settings Modified

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Internet Settings Modified

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

시스템에서 인터넷 설정 수정을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4657)

UBA : Malware Activity - Registry Modified In Bulk

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Malware Activity - Registry Modified In Bulk

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

짧은 간격 내에 다중 레지스트리 값을 한꺼번에 수정하는 프로세스를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4657)

UBA : Netcat Process Detection(Linux)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Netcat Process Detection(Linux)

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

Linux 시스템에서 netcat 프로세스를 발견합니다.

지원 룰

BB:UBA : Common Log Source Filters

데이터 소스

Linux OS (이벤트 ID: SYSCALL)

UBA : Netcat Process Detection(Windows)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Netcat Process Detection(Windows)

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

Windows 시스템에서 netcat 프로세스를 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4688)

UBA : Process Executed Outside Gold Disk Whitelist(Linux)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Process Executed Outside Gold Disk Whitelist(Linux)

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

Linux 시스템에서 작성된 프로세스를 발견하고 프로세스가 골든 디스크 프로세스 화이트리스트 외부에 있는 경우 이를 알립니다.

참고: 기본적으로 룰은 사용 불가능합니다. 참조 세트 'UBA : Gold Disk Process Whitelist - Linux'에서 화이트리스트에 추가할 프로세스 이름을 입력하거나 수정한 후에만 룰을 사용으로 설정하십시오.

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Gold Disk Process Whitelist - Linux"

지원 룰

BB:UBA : Common Log Source Filters

데이터 소스

Linux OS (이벤트 ID: SYSCALL)

UBA : Process Executed Outside Gold Disk Whitelist(Windows)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Process Executed Outside Gold Disk Whitelist(Windows)

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

Windows 시스템에서 작성된 프로세스를 발견하고 프로세스가 골든 디스크 프로세스 화이트리스트 외부에 있는 경우 이를 알립니다.

참고: 기본적으로 룰은 사용 불가능합니다. 참조 세트 'UBA : Gold Disk Process Whitelist - Windows'에서 화이트리스트에 추가할 프로세스 이름을 입력하거나 수정한 후에만 룰을 사용으로 설정하십시오.

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Gold Disk Process Whitelist - Windows"

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4688)

UBA : Ransomware Behavior Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Ransomware Behavior Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

랜섬웨어 감염 시 일반적으로 나타나는 동작을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Windows Common Processes"

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4663)

UBA : Restricted Program Usage

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Restricted Program Usage

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

프로세스가 작성되었으며 그 프로세스 이름이 참조 세트 "UBA : Restricted Program Filenames"에 나열된 2진 이름 중 하나와 일치함을 표시합니다. 이 참조 세트는 사용자가 사용자 정의할 수 있도록 기본적으로 공백입니다. 위험 관리를 위해 모니터하려는 파일 이름으로 참조 세트를 채울 수 있습니다.

모니터링을 위한 프로그램 추가 또는 제거에 대한 자세한 정보는 제한된 프로그램 관리를 참조하십시오.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Restricted Program Filenames"

데이터 소스

Microsoft Windows Security Event Log

UBA : User Installing Suspicious Application

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

다음 룰을 지원합니다.

- UBA : User Installing Suspicious Application
- UBA : Populate Authorized Applications

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

애플리케이션 설치 이벤트를 발견하고 의심스러운 애플리케이션이 표시되면 경보를 전송합니다. 참고: 조직에서 권한 부여된 애플리케이션 이름으로 참조 세트 "UBA : Authorized Applications"를 채우십시오. 짧은 기간 동안 이 참조 세트를 채우기 위해 룰 "UBA : Populate Authorized Applications"를 사용할 수있습니다.

룰 "UBA : Populate Authorized Applications"는 이 룰을 사용하는 동안 설치되는 애플리케이션 이름으로 참조 세트 "UBA : Authorized Applications"를 채웁니다. 참고: 기본적으로 룰이 표시됩니다.

사용자가 애플리케이션을 설치하는 중에 짧은 기간 동안 해당 이름을 채울 수 있도록 설정합니다.

데이터 소스

Microsoft Windows Security Event Logs

UBA : User Running New Process

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

다음 룰을 지원합니다.

- UBA : User Running New Process
- UBA : Populate Process Filenames

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

사용자가 작성한 프로세스를 발견하고 사용자가 새 프로세스를 실행하는 경우 경보를 전송합니다.

룰 "UBA: Populate Process Filenames"는 "UBA: User Running New Process"에 대한 유틸리티 룰로 사용되는 참조 세트 "UBA: Process Filenames"를 채웁니다. 참고: 기본적으로 룰이 표시됩니다. 짧은 기간 동안 파일 이름을 채울 수 있도록 룰을 설정합니다.

지원 룰

BB:UBA : Common Event Filters, UBA : Populate Process Filenames

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. "UBA : Process Filenames"

데이터 소스

Microsoft Windows System Event Logs (이벤트 ID:4688)

UBA : Volume Shadow Copy Created

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Volume Shadow Copy Created

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

vssadmin.exe 또는 WMIC(Windows Management Instrumentation Command-line)를 사용하여 작성된 새도우 사본을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 1 또는 4688)

탈출

UBA : Abnormal data volume to external domain(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 다음 기계 학습 분석: 외부 도메인에 대한 비정상 데이터 볼륨(Abnormal Volume of Data to External Domains)으로 대체되었습니다.

- UBA : Abnormal data volume to external domain
- UBA : Abnormal data volume to external domain Found

참고: ADE 룰을 사용하면 UBA 앱과 QRadar 시스템의 성능에 영향을 미칠 수 있습니다.

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

UBA : Abnormal data volume to external domain 이 룰은 Anomaly Detection Engine을 사용하여 사용자의 트래픽 사용량을 모니터하고 외부 도메인에 대한 트래픽의 비정상 데이터 볼륨에 대한 경보를 전송합니다.

UBA : Abnormal data volume to external domain Found Anomaly Detection Engine을 사용하여 사용자의 트래픽 사용량을 모니터하고 외부 도메인에 대한 트래픽의 비정상 데이터 볼륨에 대한 경보를 전송하는 동일한 개별 ADE 룰 UBA : Abnormal data volume to external domain을 지원하는 CRE 룰입니다.

데이터 소스

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

UBA : Abnormal Outbound Transfer Attempts(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 다음 기계 학습 분석: 비정상 아웃바운드 전송 시도(Abnormal Outbound Transfer Attempts)로 대체되었습니다. 추가 정보는 209 페이지의 『비정상 아웃바운드 전송 시도 분석 구성』의 내용을 참조하십시오.

UBA : Abnormal Outbound Transfer Attempts(V2.4.0의 경우 UBA : Abnormal Outbound Attempts)

UBA : Abnormal Outbound Transfer Attempts Found

참고: ADE 룰을 사용하면 UBA 앱과 QRadar 시스템의 성능에 영향을 미칠 수 있습니다.

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

UBA : Abnormal Outbound Transfer Attempts(ADE 룰) 이 룰은 Anomaly Detection Engine을 사용하여 아웃바운드 트래픽 사용량을 모니터하고 비정상 시도 수에 대한 경보를 전송합니다.

UBA : Abnormal Outbound Transfer Attempts Found Anomaly Detection Engine을 사용하여 아웃바운드 트래픽 사용량을 모니터하고 비정상 시도 수에 대한 경보를 전송하는 동일한 개별 ADE 룰 UBA : Abnormal Outbound Attempts를 지원하는 CRE 룰입니다.

데이터 소스

지원되는 모든 로그 소스.

UBA : Large Outbound Transfer by High Risk User

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Large Outbound Transfer by High Risk User

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

고위험 사용자가 200,000바이트 이상을 아웃바운드 전송하는 것을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

CEP BytesSent가 정의되어 있는 로그 소스입니다.

UBA : Multiple Blocked File Transfers Followed by a File Transfer

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Multiple Blocked File Transfers Followed by a File Transfer

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

처음에는 차단되었지만 5분 내에 정상적으로 업로드가 수행된 파일 업로드를 확인하여 유출을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Blocked File Transfer
- BB:UBA : Successful File Transfer

필수 구성

이 룰에는 정확한 발견을 위해 차단된 파일 전송 및 정상적인 파일 전송 이벤트가 모두 필요합니다. 사용되는 로그 소스에 두 이벤트에 해당하는 이벤트 ID가 없으면 부정확한 결과가 수신될 수 있습니다. 사용 중인 로그 소스의 이벤트 ID를 판별하려면 데이터 소스를 참조하십시오.

데이터 소스(차단된 파일 전송)

Cilasoft QJRN/400(이벤트 ID: C21020)

Cisco Call Manager(이벤트 ID: %UC_DRF-3-DRFSftpFailure)

Cisco IOS(이벤트 ID: %UPDATE-3-SFTP_TRANSFER_FAIL)

Custom Rule Engine(이벤트 ID: 18014, 18071, 18187, 4032)

Extreme Stackable and Standalone Switches(이벤트 ID: FFTP request failed)

Flow Classification Engine(이벤트 ID: 4032, 18187, 18014, 18071)

Forcepoint Sidewinder(이벤트 ID: FTP Permits, denied ftp command)

IBM i(이벤트 ID: 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)(이벤트 ID: TFTP:AUDIT:READ-FAILED)

Microsoft IIS(이벤트 ID: 530)

Microsoft Operations Manager(이벤트 ID: 22095)

OSSEC(이벤트 ID: 11504, 11512)

Universal DSM(이벤트 ID: FTP Action Denied, TFTP Session Denied,FTP Denied,FileTransfer Denied)

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

데이터 소스(정상적인 파일 전송)

Cilasoft QJRN/400(이벤트 ID: C21031)

Cisco FireSIGHT Management Center(이벤트 ID: FILE_EVENT, FILE_EVENT_0)

Cisco IOS(이벤트 ID: %FTPSERVER-6-NEWCONN)

Cisco IronPort(이벤트 ID: FTP_connection)

Custom Rule Engine(이벤트 ID: 18010, 4031,18431, 18183)

DG Technology MEAS(이벤트 ID: 119-003, 119-070)

Flow Classification Engine(이벤트 ID: 18010, 4031,18431, 18183)

Flow Device Type(이벤트 ID: 21984, 21879, 51337, 51336, 35159, 21910)

Huawei S Series Switch(이벤트 ID: FTPS/5/REQUEST)

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

IBM i(이벤트 ID: 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(이벤트 ID: TFTP, FTP)

Juniper Networks AVT(이벤트 ID: TFTP, FTP)

Microsoft IIS(이벤트 ID: 150, 125, 225)

ProFTPD Server(이벤트 ID: FTP session opened)

Solaris Operating System Authentication Messages(이벤트 ID: ftp connection)

SonicWALL SonicOS(이벤트 ID: 1112, 1113)

Squid Web Proxy(이벤트 ID: 3C0002_ALLOWED)

Trend InterScan VirusWall(이벤트 ID: Trend ftpconnect)

Universal DSM(이벤트 ID: File Transfer, FTP Opened, FTP Action Allowed, TFTP Session Opened)

Verdasys Digital Guardian(이벤트 ID: Network Transfer Upload, Network Transfer Download)

WatchGuard Fireware OS(이벤트 ID: 2AFF0004, 1CFF0019)

UBA : Suspicious Access Followed by Data Exfiltration

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Access Followed by Data Exfiltration

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

데이터 유출 시도가 수행된 비정상적, 제한된 또는 금지된 위치에서의 액세스를 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Data Exfiltration
- UBA : User Access from Restricted Location
- UBA : User Access from Prohibited Location
- UBA : User Geography, Access from Unusual Locations

필수 구성

다음 룰을 사용으로 설정하십시오.

- UBA : User Access from Restricted Location
- UBA : User Access from Prohibited Location
- UBA : User Geography, Access from Unusual Locations

데이터 소스

Cisco Stealthwatch(이벤트 ID: 45)

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

Skyhigh Networks Cloud Security Platform(이벤트 ID: 10003, 10004)

UBA : User Volume Activity Anomaly - Traffic to External Domains(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다.

- UBA : User Volume Activity Anomaly - Traffic to External Domains
- UBA : User Volume Activity Anomaly - Traffic to External Domains Found

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

UBA : User Volume Activity Anomaly - Traffic to External Domains은 Anomaly Detection Engine을 사용하여 사용자의 트래픽 사용량을 모니터하고 트래픽의 비정상 볼륨에 대한 경보를 전송하는 동일한 개별 ADE 룰(UBA : User Volume of Activity Anomaly - Traffic)을 지원하는 CRE 룰입니다.

UBA : User Volume Activity Anomaly - Traffic to External Domains Found는 Anomaly Detection Engine을 사용하여 아웃바운드 트래픽 사용량을 모니터하고 비정상 시도 수에 대한 경보를 전송하는 동일한 개별 ADE 룰(UBA : User Volume Activity Anomaly - Traffic to External Domains)을 지원하는 CRE 룰입니다.

데이터 소스

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

---

지역

UBA : Anomalous Account Created From New Location

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Anomalous Account Created From New Location

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

새 위치에서 비정상 계정 작성 활동을 발견합니다.

지원 룰

- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created
- BB:UBA : Common Event Filters
- UBA : User Geography Change

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : User Geography Change"

데이터 소스

AhnLab Policy Center APC(이벤트 ID: Administrator Account Add:Succeeded, ADD_ADMIN_ACCOUNT_SUCCESS)

Application Security DbProtect(이벤트 ID: Database user created, Login created - standard, Login added - Windows, Database role - created)

Aruba Mobility Controller(이벤트 ID: authmgr_user_add)

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

Box(이벤트 ID: NEW_USER)

Brocade FabricOS(이벤트 ID: SEC-1180,SEC-3025, SEC-1182)

CA ACF2(이벤트 ID: ACF2-L)

Check Point(이벤트 ID: User Added, device_added)

Cilasoft QJRN/400(이벤트 ID: C20010, C20011)

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

Cisco Firewall Services Module(FWSM)(이벤트 ID: 502101, 504001)

Cisco IOS(이벤트 ID: %APF-6-USER_NAME_CREATED)

Cisco Identity Services Engine(이벤트 ID: 86006)

Cisco NAC Appliance(이벤트 ID: CCA-1500)

Cisco PIX Firewall(이벤트 ID: %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(이벤트 ID: 502101)

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

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

CloudPassage Halo(이벤트 ID: Halo user added, Halo user re-added, Local account created(linux 에만 해당))

CorreLog Agent for IBM zOS(이벤트 ID: RACF ADDUSER: No Violations)

Cyber-Ark Vault(이벤트 ID: 180, 2)

EMC VMWare(이벤트 ID: AccountCreatedEvent)

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

Extreme Matrix K/N/S Series Switch(이벤트 ID: created with, User Created Event)

Extreme NAC(이벤트 ID: Added registered user, Add Registered User)

Flow Classification Engine(이벤트 ID: 3031, 3041)

Forcepoint Sidewinder(이벤트 ID: passport addition)

Fortinet FortiGate Security Gateway(이벤트 ID: add, auth-logon)

Foundry Fastiron(이벤트 ID: SNMP_USER_ADDED)

HBGary Active Defense(이벤트 ID: CreateUser)

HP Network Automation(이벤트 ID: User Added)

IBM AIX Audit(이벤트 ID: USER_Create SUCCEEDED)

IBM AIX Server(이벤트 ID: USER_Create)

IBM DB2(이벤트 ID: ADD_USER SUCCESS)

IBM IMS(이벤트 ID: USER CREATED)

IBM QRadar Packet Capture(이벤트 ID: UserAdded)

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

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

IBM Security Directory Server(이벤트 ID: SDS Audit)

IBM Security Identity Governance(이벤트 ID: 49, 70004, 42)

IBM Security Identity Manager(이벤트 ID: Add Success, Add SUBMITTED, Add SUCCESS)

IBM SmartCloud Orchestrator(이벤트 ID: user)

IBM Tivoli Access Manager for e-business(이벤트 ID: 13402 - Succeeded, 13401 - Succeeded, 13402 Command Succeeded, 13401 Command Succeeded)

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

Imperva SecureSphere(이벤트 ID: NEW_USERS_ACCOUNT, SOX_NEW_USERS, SOX - New users, New Users Account)

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

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

Linux OS(이벤트 ID: ADD_USER)

McAfee Application/Change Control(이벤트 ID: USER_ACCOUNT_CREATED)

McAfee ePolicy Orchestrator(이벤트 ID: 20792)

Microsoft ISA(이벤트 ID: user added)

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

Microsoft SharePoint(이벤트 ID: 37)

Microsoft Windows Security Event Log(이벤트 ID: 624, 645, 1318, 4720, 4741)

NCC Group DDos Secure(이벤트 ID: 1003)

Netskope Active(이벤트 ID: Create Admin, Created new admin)

Novell eDirectory(이벤트 ID: CREATE_ACCOUNT)

OS Services Qidmap(이벤트 ID: User Account Added)

OSSEC(이벤트 ID: 5902, 18110)

Okta(이벤트 ID: 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(이벤트 ID: add user)

Oracle Enterprise Manager(이벤트 ID: User Create(successful), Computer Create(successful))

Oracle RDBMS Audit Record(이벤트 ID: 51:1, 51:0, CREATE USER-Standard:1, CREATE USER-Standard:0)

Oracle RDBMS OS Audit Record(이벤트 ID: 51)

Pirean Access: One(이벤트 ID: IsimUserRegistration;*;1)

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

RSA Authentication Manager(이벤트 ID: Added user, unknown, REMOTE_PRINCIPAL_CREATE, CREATE_PRINCIPAL, CREATE_AM_PRINCIPAL)

SIM Audit(이벤트 ID: Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT(이벤트 ID: Active DirectorycomputerObject AddedTrueFalse, Console ? user/group added, Console user/group added, Active DirectoryuserObject AddedTrueFalse, Console - user/group added)

SafeNet DataSecure/KeySecure(이벤트 ID: Added user)

Salesforce Security Auditing(이벤트 ID: Created new Customer User, Created new user)

Skyhigh Networks Cloud Security Platform(이벤트 ID: 10016)

Solaris BSM(이벤트 ID: create user)

SonicWALL SonicOS(이벤트 ID: 558)

Symantec Encryption Management Server(이벤트 ID: ADMIN_IMPORTED_USER)

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

Trend Micro Deep Discovery Email Inspector(이벤트 ID: SYSTEM_EVENT_ACCOUNT_CREATED)

Trend Micro Deep Security(이벤트 ID: 650)

Universal DSM(이벤트 ID: Computer Account Added, User Account Added)

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

Vormetric Data Security(이벤트 ID: DAO0089I)

iT-CUBE agileSI(이벤트 ID: U0, AU7)

UBA : Anomalous Cloud Account Created From New Location

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Anomalous Cloud Account Created From New Location

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

새 위치에서 클라우드 계정 작성 활동을 발견합니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created
- UBA : User Geography Change

필수 구성

다음 룰을 사용으로 설정하십시오. "UBA : User Geography Change"

데이터 소스

Amazon AWS CloudTrail(이벤트 ID: CreateUser)

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

UBA : User Access from Multiple Locations

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access from Multiple Locations

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

다중 위치 또는 소스에서 같은 사용자 계정을 동시에 사용하고 있음을 표시합니다. 일치 및 지속 시간 매개변수를 조정하여 반응성을 조정하십시오.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access from Prohibited Location

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access from Prohibited Location

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

"UBA : Allowed Location List"에 없는 위치에서의 사용자 액세스를 발견합니다.

지원 룰:

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
-

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Allowed Location List

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Access from Restricted Location

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access from Restricted Location

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

"UBA : Restricted Location List"에 있는 위치에서의 사용자 액세스를 발견합니다. "지리적 위치"의 국가를 "UBA : Restricted Location List"에 추가할 수 있습니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
-

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Restricted Location List

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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 : User Geography Change

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Geography Change

기본적으로 사용 가능

True

senseVaule 기본값

5

설명

일치는 사용자가 사용자의 최근 원격 로그인한 국가와 다른 국가에서 원격으로 로그인했음을 표시합니다. 이 룰은 특히 룰 일치가 근접하게 시간 내에 발생한 경우 계정 손상을 표시할 수도 있습니다.

지원 룰

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- UBA : User Geography Map

필수 구성

다음 룰을 사용으로 설정하십시오. UBA : User Geography Map

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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

지원 룰

User Geography Map

이 룰은 필수 데이터로 연관된 참조 세트를 업데이트합니다.

UBA : User Geography, Access from Unusual Locations

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Geography, Access from Unusual Locations

기본적으로 사용 가능

True

senseVaule 기본값

15

설명

빌딩 블록 룰 "UBA : BB : Unusual Source Locations"에 의해 정의된 대로 사용자가 사용자의 네트워크에 일반적이지 않은 국가에서 인증할 수 있었음을 표시합니다.

지원 룰

- BB:UBA : Unusual Source Locations
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

데이터 소스

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 운영 체제(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 및 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(사용 안함), 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

네트워크 트래픽 및 공격

UBA : D/DoS Attack Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : D/DoS Attack Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

사용자에 의한 네트워크 서비스 거부(DoS) 공격을 발견합니다.

참고: 이 룰을 사용하려면 먼저 다음 단계를 완료하십시오.

1. **관리** 탭에서 **UBA 설정**을 클릭하십시오.
2. 자산 테이블에서 사용자 이름을 검색하려면 **이벤트 또는 플로우 데이터에 대한 사용자 이름이 사용 불가능한 경우 자산에서 사용자 이름 검색** 선택란을 선택하십시오. UBA 앱은 이벤트에 사용자가 나열되지 않은 경우 IP 주소에 대한 사용자를 검색하기 위해 자산을 사용합니다.
3. 이 이벤트 룰을 사용하려면 "Snort Open Source IDS" 로그 소스가 작동해야 합니다.

지원 룰

- BB:UBA : Common Log Source Filters
- BB:CategoryDefinition: DDoS Attack Events
- BB:CategoryDefinition: Network DoS Attack
- BB:CategoryDefinition: Service DoS

데이터 소스

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 및 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 : Honeytoken Activity

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Honeytoken Activity

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Honeytoken 계정을 사용하여 활동을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Honeytoken Accounts

다음 로그 소스 그룹에 적절한 로그 소스를 추가하십시오. UBA : Systems with Honeytoken Accounts

데이터 소스

모든 로그 소스가 UBA : Systems with Honeytoken Accounts 로그 소스 그룹에 추가되었습니다.

UBA : Network Traffic : Capture, Monitoring and Analysis Program Usage

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Network Traffic : Capture, Monitoring and Analysis Program Usage

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

프로세스가 작성되었으며 그 프로세스 이름이 참조 세트 "UBA : Network Capture, Monitoring and Analysis Program Filenames"에 나열된 2진 이름 중 하나와 일치함을 표시합니다. 이 참조 세트는 소프트웨어를 캡처하는 네트워크 패킷의 2진 이름을 나열합니다. 참조 세트는 일부 공통 네트워크 프로토콜 분석 소프트웨어 파일 이름의 이름으로 사전에 채워집니다.

모니터링을 위한 프로그램 추가 또는 제거에 대한 자세한 정보는 네트워크 모니터링 도구 관리를 참조하십시오.

지원 룰

BB:UBA : Common Event Filters

필수 구성

다음 참조 세트에 적절한 값을 추가하십시오. UBA : Network Capture, Monitoring and Analysis Program Filenames

데이터 소스

Microsoft Windows Security Event Log

UBA : User Behavior, Session Anomaly by Destination(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다.

UBA : User Behavior, Session Anomaly by Destination

UBA : User Behavior, Session Anomaly by Destination Found

참고: ADE 룰을 사용하면 UBA 앱과 QRadar 시스템의 성능에 영향을 미칠 수 있습니다.

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

UBA : User Behavior, Session Anomaly by Destination 사용자가 과거에 액세스했던 것과 현저하게 다른 대상 IP 주소에 액세스하고 있음을 표시합니다. 이벤트가 손상을 표시하는 것일 필요는 없습니다. 작동에서의 변경은 사용자의 작업 책임 또는 작업 습관에서 중요한 변경을 나타낼 수 있습니다.

UBA : User Behavior, Session Anomaly by Destination Found 사용자가 과거에 액세스했던 것과 현저하게 다른 대상 IP 주소에 액세스하고 있음을 표시하는 동일한 개별 ADE 룰 UBA : User Behavior, Session Anomaly by Destination을 지원하는 CRE 룰입니다. 이벤트가 손상을 표시하는 것일 필요는 없습니다. 작동에서의 변경은 사용자의 작업 책임 또는 작업 습관에서 중요한 변경을 나타낼 수 있습니다.

데이터 소스

지원되는 모든 로그 소스.

UBA : User Event Frequency Anomaly Categories(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 기계 학습 분석: 카테고리별 활동(Activity by Category)으로 대체되었습니다. 추가 정보는 211 페이지의 『카테고리별 활동 분석 구성』의 내용을 참조하십시오.

UBA : User Event Frequency Anomaly Categories(ADE 룰)

UBA : User Event Frequency Anomaly - Categories Found

참고: ADE 룰을 사용하면 UBA 앱과 QRadar 시스템의 성능에 영향을 미칠 수 있습니다.

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

UBA : User Event Frequency Anomaly Categories Anomaly Detection Engine을 사용하여 사용자의 이벤트에 대한 카테고리 분배를 모니터합니다. 비정상적 빈도 변경에 대해 경고합니다.

UBA : User Event Frequency Anomaly - Categories Found Anomaly Detection Engine을 사용하여 사용자의 이벤트에 대한 카테고리 분배를 모니터하는 동일한 개별 ADE 룰 UBA : User Event

Frequency Anomaly - Categories를 지원하는 CRE 룰입니다. 비정상적인 빈도 변경에 대한 경보를 전송합니다.

데이터 소스

지원되는 모든 로그 소스.

UBA : User Volume Activity Anomaly - Traffic to Internal Domains(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다.

- UBA : User Volume Activity Anomaly - Traffic to Internal Domains
- UBA : User Volume Activity Anomaly - Traffic to Internal Domains Found

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

이 룰은 Anomaly Detection Engine을 사용하여 사용자의 트래픽 사용량을 모니터하고 트래픽의 비정상 볼륨에 대한 경보를 전송하는 동일한 개별 룰(UBA : User Volume of Activity Anomaly - Traffic to Internal Domains)을 지원하는 CRE 룰입니다.

데이터 소스

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

---

QRadar DNS Analyzer

자세한 정보는 IBM QRadar DNS Analyzer를 참조하십시오.

UBA : Potential Access to Blacklist Domain

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Potential Access to Blacklist Domain

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

사용자가 블랙리스트 도메인에 잠재적으로 액세스했음을 표시하는 이벤트를 발견합니다. IBM QRadar DNS Analyzer 앱이 필요합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar DNS Analyzer 앱을 설치해야 합니다. 자세한 정보는 IBM QRadar DNS Analyzer를 참조하십시오.

데이터 소스

IBM QRadar DNS Analyzer

UBA : Potential Access to DGA Domain

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Potential Access to DGA Domain

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

사용자가 DGA(Domain Generated by Algorithm) 도메인에 잠재적으로 액세스했음을 표시하는 이벤트를 발견합니다. IBM QRadar DNS Analyzer 앱이 필요합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar DNS Analyzer 앱을 설치해야 합니다. 자세한 정보는 IBM QRadar DNS Analyzer를 참조하십시오.

데이터 소스

IBM QRadar DNS Analyzer

UBA : Potential Access to Squatting Domain

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Potential Access to Squatting Domain

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

사용자가 스쿼팅 도메인에 잠재적으로 액세스했음을 표시하는 이벤트를 발견합니다. IBM QRadar DNS Analyzer 앱이 필요합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar DNS Analyzer 앱을 설치해야 합니다. 자세한 정보는 IBM QRadar DNS Analyzer를 참조하십시오.

데이터 소스

IBM QRadar DNS Analyzer

UBA : Potential Access to Tunneling Domain

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Potential Access to Tunneling Domain

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

사용자가 잠재적으로 터널링 도메인에 액세스했음을 표시하는 이벤트를 발견합니다. IBM DNS Analyzer 앱이 필요합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar DNS Analyzer 앱을 설치해야 합니다. 자세한 정보는 IBM QRadar DNS Analyzer를 참조하십시오.

데이터 소스

IBM QRadar DNS Analyzer

QNI(QRadar Network Insights)

QRadar V7.2.8에서 QNI 룰 설치에 대한 자세한 정보는 QRadar Network Insights Content v7.2.8을 참조하십시오.

QRadar V7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

UBA : QNI - Access to Improperly Secured Service - Certificate Expired

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Access to Improperly Secured Service - Certificate Expired

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

QNI(QRadar Network Insights)가 만료된 인증서를 사용하는 SSL/TLS 세션을 발견했습니다. 서버 및 클라이언트가 SSL(Secure Sockets Layer) 또는 TLS(Transport Layer Security)를 사용하여 통신을 확립할 때 인증서를 사용합니다. 인증서는 인증서의 유효한 상태가 유지되는 기간을 나타내는 만료 날짜를 포함하여 발행됩니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를

참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

QNI(QRadar Network Insights)가 올바르지 않은 인증서를 사용하는 SSL/TLS 세션을 발견했습니다. 서버 및 클라이언트가 SSL(Secure Sockets Layer)을 사용하여 통신을 확립할 때 X.509 인증서를 사용합니다. 인증서는 인증서가 유효하게 되는 가장 빠른 날짜를 표시하는 이후(Not Before) 날짜를 포함하여 발행됩니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

QNI(QRadar Network Insights)가 2048 미만의 하위 공개 키 비트 수가 있는 인증서를 사용하는 SSL/TLS 세션을 발견했습니다. 약한 공개 키 인증서(1024비트 미만의)를 제공하는 서버는 보안 위험을 나타낼 수 있습니다. NIST 서적 800-57에 따라 2011년에 시작된 최소 권장 RSA 키는 2048비트입니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

QNI(QRadar Network Insights)가 자체 서명된 인증서를 사용하는 SSL/TLS 세션을 발견했습니다. 공용 또는 프로덕션 서버 애플리케이션의 자체 서명된 인증서는 원격 공격자가 중간자 공격을 시작하도록 허용할 수 있습니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Confidential Content Being Transferred to Foreign Geography

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Confidential Content Being Transferred to Foreign Geography

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

액세스가 제한된 국가 및 지역으로 기밀 컨텐츠가 전송되고 있음을 발견합니다. 이러한 국가 및 지역은 다음 빌딩 블록에 정의되어 있음을 참고하십시오. "Countries/Regions with Restricted Access". 이 룰을 사용하기 전에 사용자의 유스 케이스에 따라 빌딩 블록이 설정되어 있는지 확인하십시오.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Observed File Hash Associated with Malware Threat

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Observed File Hash Associated with Malware Threat

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

이 룰은 플로우 컨텐츠가 Threat Intelligence 데이터 피드에 포함된 알려진 불량 파일 해시와 일치하는 파일 해시를 포함할 때 트리거됩니다. 네트워크에서 누군가 악성코드를 전송했음을 나타냅니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Observed File Hash Seen Across Multiple Hosts

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Observed File Hash Seen Across Multiple Hosts

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

이 룰은 악성코드와 연관된 동일한 파일 해시가 여러 대상으로 전송되는 것으로 표시될 때 트리거됩니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

이 룰은 존재하지 않는 수신자 주소로 발송되어 거부된 이메일 이벤트가 시스템에 표시될 때 트리거됩니다. 이는 스팸 또는 피싱 시도를 나타낼 수 있습니다. 조직과 관련된 QID를 포함하도록 BB:CategoryDefinition: Rejected Email Recipient 빌딩 블록을 구성하십시오. 모니터링하기에 적절한 다음 QID로 미리 채워집니다. Microsoft Exchange; Linux OS [running sendmail]; Solaris Operating System Sendmail Logs 및 Barracuda Spam and Virus Firewall.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers

기본적으로 사용 가능

False

senseVaule 기본값

5

설명

이 룰은 다중 송신 서버가 일정 기간에 스팸 또는 피싱을 나타낼 수 있는 동일한 이메일 제목을 발송할 때 트리거됩니다.

필수 구성

이 QNI 룰을 사용으로 설정하기 전에 QRadar Network Insights Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. QRadar 7.2.8은 QRadar Network Insights Content v7.2.8를 참조하십시오. QRadar 7.3.0 이상은 QRadar Network Insights Content v7.3.0+를 참조하십시오.

데이터 소스

QNI(QRadar Network Insights)

탐색

자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of DHCP Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of DHCP Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

DHCP 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Database Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Database Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

데이터베이스 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of DNS Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of DNS Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

DNS 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of FTP Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of FTP Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

FTP 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Game Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of Game Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

게임 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Generic ICMP Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Generic ICMP Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

ICMP 프로토콜을 사용하는 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Generic TCP Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Generic TCP Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

공통 TCP 포트를 사용하는 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Generic UDP Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of Generic UDP Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

공통 UDP 포트를 사용하는 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of IRC Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of IRC Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

IRC 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of LDAP Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of LDAP Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

LDAP 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Mail Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Mail Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

메일 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Messaging Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of Messaging Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

메시징 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of P2P Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of P2P Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

P2P 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Proxy Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Proxy Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

프록시 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of RPC Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of RPC Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

RPC 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of SNMP Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of SNMP Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

SNMP 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of SSH Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Unusual Scanning of SSH Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

SSH 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Web Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Web Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

웹 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

UBA : Unusual Scanning of Windows Servers Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스케이스를 지원합니다.

UBA : Unusual Scanning of Windows Servers Detected

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

Windows 서버에 대한 네트워크의 비정상적 스캐닝을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM Security Reconnaissance Content 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM Security Reconnaissance Content를 참조하십시오.

시스템 모니터링(Sysmon)

자세한 정보는 IBM QRadar Content Extension for Sysmon을 참조하십시오.

UBA : Common Exploit Tools Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Common Exploit Tools Detected

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

keylogger 및 PsExec과 같이 일반적으로 사용되는 악용 도구의 사용을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Common Exploit Tools Detected(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Common Exploit Tools Detected

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

keylogger 및 PsExec과 같이 일반적으로 사용되는 악용 도구의 사용을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Malicious Process Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Malicious Process Detected

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 호스트에서 악의적인 동작을 표시하는 프로세스를 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Network Share Accessed

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Network Share Accessed

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

네트워크 공유를 포함한 의심스러운 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Sysmon 룰

UBA : Process Creating Suspicious Remote Threads Detected(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Process Creating Suspicious Remote Threads Detected(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

원격 시스템에서 의심스럽게 스레드를 작성하고 있는 프로세스를 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Activities on Compromised Hosts

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Activities on Compromised Hosts

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

손상된 호스트에서 수행되는 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Activities on Compromised Hosts(Assets)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Activities on Compromised Hosts(Assets)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

손상된 호스트에서 수행되는 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Administrative Activities Detected

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Administrative Activities Detected

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

드물게 수행된 의심스러워 보이는 관리 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Command Prompt Activity

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Command Prompt Activity

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

명령 프롬프트 스크립트에 대한 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Entries in System Registry(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Entries in System Registry(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 레지스트리 수정 또는 업데이트가 포함된 의심스러운 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Image Load Detected(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Image Load Detected(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

중요한 위치에 업로드된 의심스러운 이미지를 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Pipe Activities(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Pipe Activities(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 호스트에서 프로세스 파이프가 포함된 의심스러운 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious PowerShell Activity

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious PowerShell Activity

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Microsoft PowerShell 스크립트에 대한 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious PowerShell Activity(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious PowerShell Activity(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Microsoft PowerShell 스크립트에 대한 활동을 발견합니다. 이 룰에서는 "이벤트 또는 플로우 데이터에 사용자 이름을 사용할 수 없는 경우 자산에서 사용자 이름 검색" 기능이 사용 가능해야 합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Scheduled Task Activities

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Scheduled Task Activities

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 호스트에서 스케줄된 태스크의 의심스러운 작성을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Service Activities

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Service Activities

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 컴퓨터에서 의심스러운 서비스 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : Suspicious Service Activities(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Suspicious Service Activities(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

Windows 컴퓨터에서 의심스러운 서비스 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

UBA : User Access Control Bypass Detected(Asset)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Access Control Bypass Detected(Asset)

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

UAC(User Access Control) 우회를 표시하는 프로세스 활동을 발견합니다.

필수 구성

이 룰을 사용으로 설정하기 전에 IBM QRadar Content Extension for Sysmon 팩을 설치하고 해당 룰 컨텐츠를 사용으로 설정해야 합니다. 자세한 정보는 IBM QRadar Content Extension for Sysmon 을 참조하십시오.

데이터 소스

Microsoft Windows Security Event Logs

위협 인텔리전스

UBA : Abnormal visits to Risky Resources(ADE 룰)

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다.

- UBA : Abnormal visits to Risky Resources
- UBA : Abnormal visits to Risky Resources Found

참고: ADE 룰을 사용하면 UBA 앱과 QRadar 시스템의 성능에 영향을 미칠 수 있습니다.

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

UBA : Abnormal visits to Risky Resources 이 룰은 Anomaly Detection Engine을 사용하여 사용자가 위험한 자원(예: 의심스러운 URL, 익명 서비스 및 악성코드 호스트)에 액세스하는 횟수를 모니터하고 방문 수가 비정상적으로 변경되는 경우 경보를 전송합니다.

UBA : Abnormal visits to Risky Resources Found Anomaly Detection Engine을 사용하여 사용자가 위험한 자원(예: 의심스러운 URL, 익명 서비스 및 악성코드 호스트)에 액세스하는 횟수를 모니터하고 방문 수가 비정상적으로 변경되는 경우 경보를 전송하는 동일한 개별 ADE 룰 UBA : Abnormal visits to Risky Resources를 지원하는 CRE 룰입니다.

데이터 소스

지원되는 모든 로그 소스.

UBA : Detect IOCs For Locky

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Detect IOCs For Locky

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

X-Force 캠페인 피드에서 채워진 URL 또는 IP를 사용하여 IOC(Indicators of Compromise) for Locky를 표시하는 사용자 컴퓨터를 발견합니다.

지원 룰

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect Locky Using IP
- BB:UBA : Detect Locky Using URL

필수 구성

- 다음 참조 세트에 적절한 값을 추가하십시오. UBA : IOCs-Locky IP 및 UBA : IOCs-Locky URL
- **관리 설정** > **UBA 설정**에서 "자산에서 사용자 검색"을 사용으로 설정하십시오.

데이터 소스

지원되는 모든 로그 소스.

UBA : Detect IOCs for WannaCry

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : Detect IOCs For WannaCry

기본적으로 사용 가능

False

senseVaule 기본값

10

설명

X-Force 캠페인 피드에서 채워진 URL, IP 또는 해시를 사용하여 IOC(Indicators of Compromise) for WannaCry를 표시하는 사용자 컴퓨터를 발견합니다.

지원 룰

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect WannaCry Using Hashes
- BB:UBA : Detect WannaCry Using IP
- BB:UBA : Detect WannaCry Using URL

필수 구성:

- 다음 참조 세트에 적절한 값을 추가하십시오. UBA : Malware Activity WannaCry - Hash, UBA : Malware Activity WannaCry - IP 및 UBA : Malware Activity WannaCry - URL
- **관리 설정** > **UBA 설정**에서 "자산에서 사용자 검색"을 사용으로 설정하십시오.

데이터 소스

지원되는 모든 로그 소스.

UBA : ShellBags Modified By Ransomware

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : ShellBags Modified By Ransomware

기본적으로 사용 가능

True

senseVaule 기본값

10

설명

일반적인 악성 코드 또는 랜섬웨어 동작을 표시하는 ShellBag 레지스트리 수정을 발견합니다.

지원 룰

BB:UBA : Common Event Filters

데이터 소스

Microsoft Windows Security Event Logs (이벤트 ID: 4657)

UBA : User Accessing Risky Resources

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

참고: 이 룰은 더 이상 지원되지 않습니다.

V2.3.0부터 UBA : User Accessing Risky Resources는 기본적으로 사용 안함으로 설정됩니다. 이제 룰은 다음 유형별로 나열되며 기본적으로 사용으로 설정됩니다.

- UBA : User Accessing Risky IP, Anonymization
- UBA : User Accessing Risky IP, Botnet
- UBA : User Accessing Risky IP, Dynamic
- UBA : User Accessing Risky IP, Malware
- UBA : User Accessing Risky IP, Spam

기본적으로 사용 가능

False

senseVaule 기본값

15

설명

부적절하거나 위험하게 여겨지거나 감염의 조짐을 표시하는 외부 자원에 사용자가 액세스했음을 표시합니다.

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Risky IP, Anonymization

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Risky IP, Anonymization(이전에는 X-Force Risky IP, Anonymization이라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자 또는 호스트가 외부 익명화 서비스에 연결하는 경우를 발견합니다.

지원 룰

- X-Force Risky IP, Anonymization
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky IP, Anonymization

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Risky IP, Botnet

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Risky IP, Botnet(이전에는 X-Force Risky IP, Botnet라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자 또는 호스트가 봇네트 명령 및 제어 서버에 연결하는 경우를 발견합니다.

지원 룰

- X-Force Risky IP, Botnet
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky IP, Botnet

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Risky IP, Dynamic

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Risky IP, Dynamic(이전에는 X-Force Risky IP, Dynamic이라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자 또는 호스트가 동적으로 지정된 IP 주소에 연결하는 경우를 발견합니다.

지원 룰

- X-Force Risky IP, Dynamic
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky IP, Dynamic

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Risky IP, Malware

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Risky IP, Malware(이전에는 X-Force Risky IP, Malware라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자 또는 호스트가 악성코드 호스트에 연결하는 경우를 발견합니다.

지원 룰

- X-Force Risky IP, Malware
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky IP, Malware

데이터 소스

지원되는 모든 로그 소스.

UBA : User Accessing Risky IP, Spam

QRadar User Behavior Analytics(UBA) 앱은 특정한 작동 비정상에 대한 룰을 기반으로 하는 유스 케이스를 지원합니다.

UBA : User Accessing Risky IP, Spam(이전에는 X-Force Risky IP, Spam이라고 함)

기본적으로 사용 가능

True

설명

이 룰은 로컬 사용자 또는 호스트가 스팸 전송 호스트에 연결하는 경우를 발견합니다.

지원 룰

- X-Force Risky IP, Spam
- BB:UBA : Common Event Filters

필수 구성

- **관리 설정** > **시스템 설정**에서 "X-Force Threat Intelligence 피드 사용"을 예(Yes)로 설정하십시오.
- 다음 룰을 사용으로 설정하십시오. X-Force Risky IP, Spam.

데이터 소스

지원되는 모든 로그 소스.

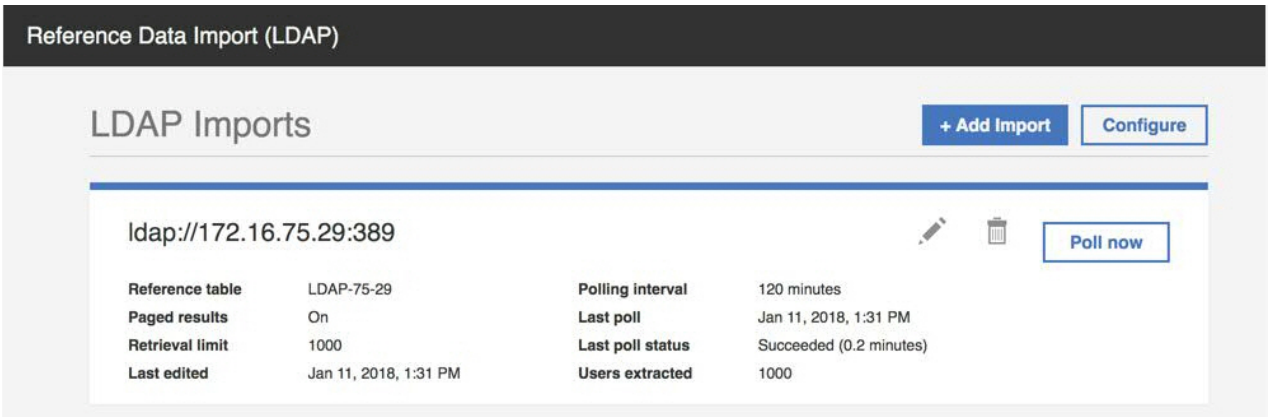
8 참조 데이터 가져오기 - LDAP 앱

참조 데이터 가져오기 - LDAP 앱을 사용하여 여러 LDAP 소스의 컨텍스트 ID 정보를 QRadar Console에 수집합니다.

경고: 참조 데이터 가져오기 - LDAP 앱은 QRadar on Cloud에서 지원되지 않습니다.

IBM® QRadar® User Behavior Analytics(UBA) 앱을 설치할 때 참조 데이터 가져오기 LDAP 앱도 설치됩니다. LDAP 앱을 사용하여 LDAP/AD 서버 또는 CSV 파일에서 QRadar 참조 테이블로 사용자 데이터를 가져올 수 있습니다. 그런 다음 참조 테이블은 UBA 앱에 의해 사용되거나, QRadar 검색 또는 룰에 사용될 수 있습니다.

참고: 참조 데이터 가져오기 - LDAP 앱을 사용하려면 QRadar V7.2.8 이상이 필요합니다.



QRadar에서 LDAP 데이터 사용

참조 테이블이 업데이트될 때마다 `ReferenceDataUpdated` 이벤트가 트리거됩니다. 참조 테이블에서 LDAP 데이터에 대한 TTL(Time-To-Live) 값을 설정할 수 있습니다. TTL 기간이 초과되면 `ReferenceDataExpiry` 이벤트가 트리거됩니다. 이러한 이벤트에 응답하는 룰을 작성하거나 QRadar **로그 보기** 탭에서 이러한 이벤트의 페이로드를 조회하는 검색을 작성할 수 있습니다.

참조 데이터 가져오기 - LDAP 앱에 액세스

관리 설정에서 **참조 데이터 가져오기 LDAP** 아이콘을 클릭하여 QRadar 참조 데이터 가져오기 - LDAP 앱에 액세스하십시오.

QRadar의 참조 데이터 콜렉션에 대한 자세한 정보는 *IBM QRadar SIEM* 관리 안내서를 참조하십시오.

LDAP 앱에 지원되는 브라우저

IBM Security QRadar 제품의 기능이 올바르게 작동하려면 지원되는 웹 브라우저를 사용해야 합니다.

다음 표에는 지원되는 웹 브라우저 버전이 나열되어 있습니다.

표 *1. QRadar* 참조 데이터 가져오기 *LDAP* 앱에 지원되는 웹 브라우저

웹 브라우저	지원되는 버전
Mozilla Firefox	45.2 확장 지원 릴리스
Google Chrome	최신

CSV 파일에서 사용자 데이터 가져오기

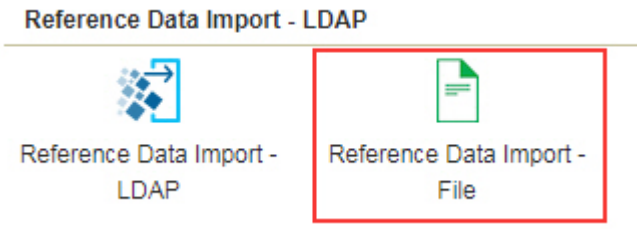
참조 데이터 가져오기를 사용하여 사용자 데이터가 포함된 CSV 파일을 업로드할 수 있음 - LDAP 앱

이 태스크 정보

사용자 데이터가 표준 CSV 형식으로 있는 경우 데이터를 CSV 파일에서 UBA 앱으로 가져올 수 있습니다.

프로시저

1. IBM QRadar V7.3.1 이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. QRadar 7.3.1이상 버전에서는 **앱** > **참조 데이터 가져오기 - LDAP** > **참조 데이터 가져오기 - 파일**을 클릭하십시오.



3. 참조 데이터 가져오기(파일) 창에서 **구성**을 클릭하여 권한 서비스 토큰을 작성하십시오.
4. 참조 데이터 가져오기(파일) 창에서 **가져오기**를 클릭하십시오.
5. 사용자 데이터 추가 화면에서 사용자 데이터가 포함된 CSV 파일을 찾으십시오.

참고:

파일은 5MB 이하여야 하고, 파일에는 컬럼 이름이 있는 헤더 행이 포함되고, 고유 데이터가 포함된 하나 이상의 컬럼이 있어야 합니다.

6. **다음**을 클릭하고 기존 참조 테이블이 있는 데이터를 병합하거나 참조 테이블을 작성할지 선택하십시오.
   - 기존 참조 테이블에 병합하려면 **다음**을 클릭하고 기존 참조 테이블을 선택하십시오.
   - 참조 테이블을 선택하려면 **다음**을 클릭하고 참조 테이블을 작성하십시오.
7. **다음**을 클릭하십시오.
8. 속성 맵핑 화면에서 속성 이름 및 참조 테이블에 대한 키를 설정하고 **가져오기**를 클릭하십시오.

권한 서비스 토큰 작성

참조 테이블에 데이터를 추가하도록 LDAP 서버를 구성하려면 먼저 권한 서비스 토큰을 작성해야 합니다.

시작하기 전에

주의: QRadar on Cloud 관리자는 제한된 관리자 기능으로 인해 QRadar 앱에 대한 권한 서비스 토큰을 작성할 수 없습니다. QRadar on Cloud 고객인 경우, 고객 지원에 문의하여 권한 서비스 토큰을 작성하십시오.

이 태스크 정보

참고: 권한 서비스 토큰을 제출한 후에는 권한 있는 새 서비스 토큰이 적용되도록 변경사항을 배치해야 합니다.

IBM QRadar에서는 참조 데이터 가져오기 - LDAP 앱이 작성하는 API 호출을 인증하기 위해 사용자가 인증 토큰을 사용해야 합니다. **관리** 설정의 권한 서비스 관리 창을 사용하여 권한 서비스 토큰을 작성합니다.

프로시저

1. 참조 데이터 가져오기 - LDAP 앱 창에서 **구성**을 클릭하십시오.
2. 권한 서비스 토큰 구성 대화 상자에서 **권한 서비스 관리**를 클릭하십시오.
3. 권한 서비스 관리 창에서 **권한 서비스 추가**를 클릭하십시오.
4. 다음 필드에서 관련 정보를 추가하고 **서비스 작성**을 클릭하십시오.
   a. **서비스 이름** 필드에 이 권한 서비스의 이름을 입력하십시오. 이름은 최대 255자까지 가능합니다.
   b. **사용자 역할** 목록에서 **관리**를 선택하십시오.
   c. **보안 프로파일** 목록에서 이 권한 서비스에 지정할 보안 프로파일을 선택하십시오. 보안 프로파일은 이 서비스가 QRadar 사용자 인터페이스에 액세스할 수 있는 네트워크 및 로그 소스를 판별합니다.
   d. **만료 날짜** 목록에서 이 서비스가 만료될 날짜를 입력하거나 선택하십시오. 만료 날짜가 필요하지 않은 경우 **만료되지 않음**을 선택하십시오.

5. 작성한 서비스가 포함된 행을 클릭하고, 메뉴 표시줄의 **선택한 토큰** 필드에서 토큰 문자열을 선택하여 복사한 후 권한 서비스 관리 창을 닫으십시오.
6. 권한 서비스 토큰 구성 대화 상자에서 토큰 문자열을 **토큰** 필드에 붙여넣고 **확인**을 클릭하십시오.
7. 새 권한 서비스 토큰이 적용되도록 변경사항을 배치하십시오.

다음에 수행할 작업

『LDAP 구성 추가』

개인용 루트 인증 기관(CA) 추가

LDAP 앱에서 사용하기 위해 IBM QRadar에 개인용 루트 인증 기관(CA) 번들을 업로드할 수 있습니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **참조 데이터 가져오기 LDAP** 아이콘을 클릭하십시오.
3. 참조 데이터 가져오기 LDAP 앱 기본 창에서 **구성**을 클릭하십시오.
4. **파일 선택**을 클릭한 후 **업로드**를 클릭하십시오. `.pem` 파일 유형만 지원됩니다.
5. **확인**을 클릭하십시오.

LDAP 구성 추가

사용자 데이터를 맵의 참조 맵에 삽입하는 데 사용하는 LDAP 서버 정보를 추가하십시오.

시작하기 전에

LDAP 구성을 추가하려면 먼저 참조 데이터 가져오기 - LDAP 앱에 인증 토큰을 작성하여 추가해야 합니다.

프로시저

1. 참조 데이터 가져오기 - LDAP 앱 창에서 **가져오기 추가**를 클릭하십시오.
2. **LDAP 구성** 탭에서 다음 정보를 입력하십시오.
   a. **LDAP URL** 필드에 `ldap://` 또는 `ldaps://`(TLS의 경우)로 시작하는 URL을 입력하십시오.
   b. **기본 DN** 필드에 서버가 사용자를 검색해야 하는 LDAP 디렉토리 트리의 지점을 입력하십시오.

예를 들어, LDAP 서버가 도메인 example.com에 있는 경우 dc=example,dc=com을 사용할 수 있습니다.

c. 참조 테이블로 가져온 데이터를 정렬하려면 사용하려는 속성을 **필터** 필드에 입력하십시오. 예를 들어, 다음과 같습니다.

```
cn=*; uid=*; sn=*
```

Active Directory로 작업하는 기본값은 다음과 같습니다. (&(sAMAccountName=*)(samAccountType=805306368)).

d. **속성 목록** 필드에 참조 테이블로 가져오려는 속성을 입력하십시오.

Active Directory로 작업하는 기본값은 다음과 같습니다.
userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title.

e. **사용자 이름** 필드에 LDAP 서버를 인증하는 데 사용되는 사용자 이름을 입력하십시오.

f. **비밀번호** 필드에 LDAP 서버의 비밀번호를 입력하십시오.

3. 진행하기 전에 **연결 테스트**를 클릭하여 IBM QRadar가 LDAP 서버에 연결할 수 있는지 확인하십시오.

연결 시도가 성공적이면 LDAP 서버의 정보가 **LDAP 구성** 탭에 표시됩니다.

4. **다음**을 클릭하십시오.

다음에 수행할 작업

『속성 선택』.

관련 태스크:

194 페이지의 『개인용 루트 인증 기관(CA) 추가』
LDAP 앱에서 사용하기 위해 IBM QRadar에 개인용 루트 인증 기관(CA) 번들을 업로드할 수 있습니다.

193 페이지의 『권한 서비스 토큰 작성』
참조 테이블에 데이터를 추가하도록 LDAP 서버를 구성하려면 먼저 권한 서비스 토큰을 작성해야 합니다.

196 페이지의 『LDAP 속성 맵핑 추가』
별명을 추가하거나 참조 테이블에 대한 키를 설정할 수 있습니다.

속성 선택

LDAP 서버에서 추출할 속성을 선택합니다.

프로시저

1. **속성** 선택 탭에서 특정 속성을 검색하고 LDAP 서버에서 추출하려는 속성을 선택하십시오.
2. **다음**을 클릭하십시오.

다음에 수행할 작업

LDAP 속성 맵핑 추가

LDAP 속성 맵핑 추가

별명을 추가하거나 참조 테이블에 대한 키를 설정할 수 있습니다.

이 태스크 정보

여러 소스의 LDAP 데이터를 동일한 참조 테이블에 병합하려는 경우 서로 다른 소스에서 동일한 이름을 가진 LDAP 속성을 구별하기 위해 사용자 정의 별명을 사용할 수 있습니다.

프로시저

1. **속성 맵핑** 탭에서 참조 테이블에 대한 키를 설정하십시오.

   팁: 추가를 클릭하고 두 개의 속성을 결합하여 새 LDAP 속성 필드를 작성할 수 있습니다. 다음과 같은 구문을 작성할 수 있습니다. 예: `"Last: {ln}, First: {fn}"`.
2. **다음**을 클릭하십시오.

다음에 수행할 작업

LDAP 데이터를 저장하기 위한 참조 데이터 테이블 구성

관련 태스크:

『참조 데이터 구성 추가』
참조 구성 탭을 사용하여 LDAP 데이터를 저장하기 위한 참조 데이터 테이블을 설정합니다.

199 페이지의 『LDAP 데이터 업데이트에 응답하는 룰 작성』
QRadar에서 참조 테이블에 LDAP 서버의 데이터를 저장하도록 IBM QRadar 참조 데이터 가져오기 - LDAP 앱을 구성한 후에 이 데이터를 사용하여 이벤트 룰을 작성할 수 있습니다.

참조 데이터 구성 추가

참조 구성 탭을 사용하여 LDAP 데이터를 저장하기 위한 참조 데이터 테이블을 설정합니다.

시작하기 전에

LDAP 서버 정보를 구성한 후 앱에 전달되는 LDAP 데이터를 저장하기 위한 참조 테이블을 설정해야 합니다. 그런 다음 저장된 데이터를 사용하여 QRadar에 룰을 구축하거나 검색 및 보고서를 작성할 수 있습니다.

프로시저

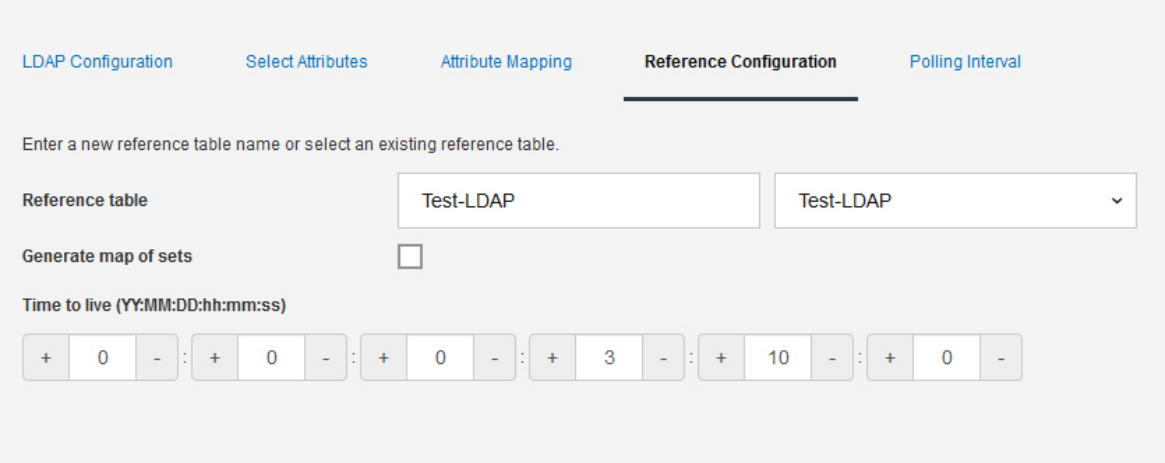
1. **참조 구성** 탭을 사용하여 새 참조 테이블을 입력하거나 LDAP 데이터를 추가하려는 기존 참조 테이블을 지정하십시오.

a. **참조 데이터** 필드에 참조 데이터 콜렉션의 이름을 입력하거나 목록에서 기존 참조 데이터 콜렉션을 선택하십시오.

b. 기본적으로 **세트의 맵 생성** 선택란은 사용 안함으로 설정됩니다. 이 선택란을 사용으로 설정하면 데이터를 참조 세트 형식으로 전송하여 QRadar 검색을 개선하며 성능에 영향을 미칠 수 있습니다.

c. 데이터를 참조 테이블에 지속시키려는 기간을 정의하려면 **TTL(Time to live)** 필드를 사용하십시오. 기본적으로 사용자가 추가하는 데이터는 만료되지 않습니다. TTL 기간이 초과되면 `ReferenceDataExpiry` 이벤트가 트리거됩니다.

   참고: 맵의 기존 참조 맵에 데이터를 추가하면 앱은 원래 TTL 매개변수를 사용합니다. 이러한 매개변수는 **참조 구성** 탭에서 대체될 수 없습니다.



2. **다음**을 클릭하십시오.

다음에 수행할 작업

폴링 간격을 설정하십시오.

관련 태스크:

『폴링 구성』

폴링 간격 탭을 사용하여 앱이 새 정보에 대해 LDAP 서버를 폴링하는 간격을 구성하십시오.

폴링 구성

폴링 간격 탭을 사용하여 앱이 새 정보에 대해 LDAP 서버를 폴링하는 간격을 구성하십시오.

시작하기 전에

LDAP 서버 정보 및 참조 데이터 콜렉션을 구성한 후 앱이 LDAP 서버에서 데이터를 내려받을 빈도를 구성합니다.

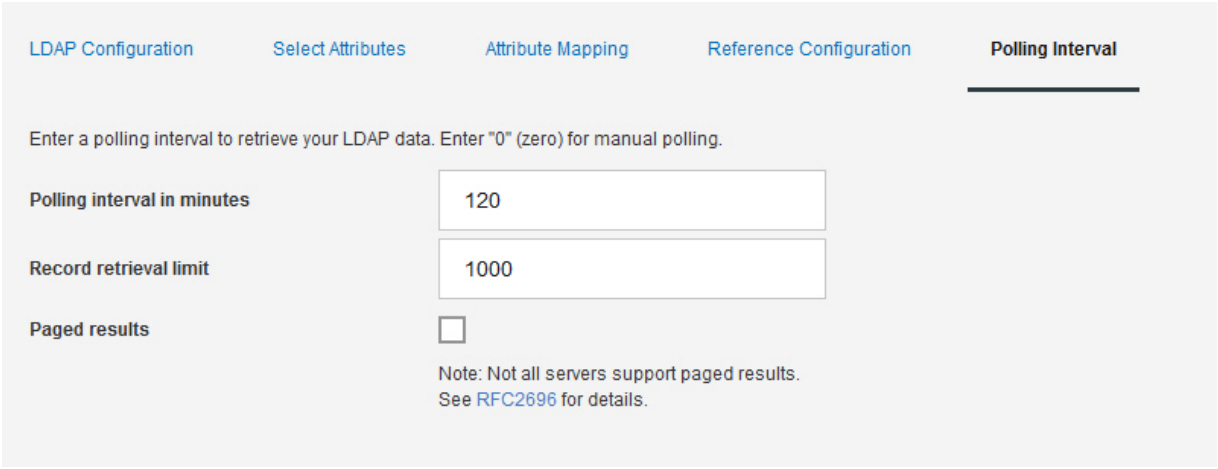
프로시저

1. **폴링 간격(분)** 필드를 사용하여 데이터에 대해 앱이 LDAP 서버를 폴링할 간격(분)을 정의하십시오.

   허용 가능한 최소 폴링 간격 값은 120입니다.
2. **레코드 검색 한계** 필드에 폴링이 리턴할 레코드 수의 값을 입력하십시오.

   기본적으로 100,000개의 레코드가 리턴됩니다. 리턴 가능한 최대 레코드 수는 200,000입니다.
3. 각 폴링에 대해 LDAP 서버가 리턴하는 레코드 수가 제한되지 않도록 **페이징된 결과** 선택란은 기본적으로 선택됩니다.

   참고: 페이징된 결과가 모든 LDAP 서버에서 지원되지는 않습니다.
4. **저장**을 클릭하십시오.



결과

구성한 간격으로 사용자가 선택한 참조 데이터 콜렉션에 LDAP 서버의 데이터가 추가됩니다. IBM QRadar 콘솔에서 API 페이지를 사용하여 데이터가 참조 데이터 콜렉션에 추가되었는지 확인할 수 있습니다.

관련 태스크:

『데이터가 참조 데이터 콜렉션에 추가되었는지 확인』

IBM QRadar API 문서 페이지를 사용하여 사용자가 작성한 참조 데이터 콜렉션에 데이터가 추가되었는지 여부를 테스트할 수 있습니다.

데이터가 참조 데이터 콜렉션에 추가되었는지 확인

IBM QRadar API 문서 페이지를 사용하여 사용자가 작성한 참조 데이터 콜렉션에 데이터가 추가되었는지 여부를 테스트할 수 있습니다.

이 태스크 정보

QRadar 콘솔의 API 문서 페이지에는 참조 데이터 가져오기 - LDAP 앱에서 작성한 참조 테이블에 저장된 데이터가 표시될 수 있습니다. API 문서 페이지를 사용하여 LDAP 정보가 앱에 의해 업데이트되었는지 확인할 수 있습니다.

프로시저

1. QRadar API 문서 페이지에 로그인하십시오.

   `https://<Console_IP>/api_doc`
2. 탐색 트리에서 최신 API를 여십시오.
3. **/reference_data** > **/table** > **/name** > **GET**으로 이동하십시오.
4. **이름** 매개변수의 **값** 필드에 LDAP 정보를 저장하기 위해 작성한 참조 데이터 콜렉션의 이름을 입력하고 **체험해 보기**를 클릭하십시오.

   앱에서 추가한 데이터가 **응답 본문** 필드에 리턴됩니다.

LDAP 데이터 업데이트에 응답하는 룰 작성

QRadar에서 참조 테이블에 LDAP 서버의 데이터를 저장하도록 IBM QRadar 참조 데이터 가져오기 - LDAP 앱을 구성한 후에 이 데이터를 사용하여 이벤트 룰을 작성할 수 있습니다.

이 태스크 정보

LDAP 서버를 폴링하고 데이터가 참조 테이블에 추가되면 `ReferenceDataUpdated` 이벤트가 트리거됩니다. **참조 구성** 탭에서 구성한 TTL(Time-To-Live) 기간이 초과되면 `ReferenceDataExpiry` 이벤트가 트리거됩니다. `ReferenceDataUpdated` 또는 `ReferenceDataExpiry` 이벤트 페이로드 내에서 컨텐츠에 응답하는 룰을 작성할 수 있습니다.

참조 데이터 콜렉션에서 앱에 의해 저장된 LDAP 데이터는 QRadar **룰 마법사**를 사용하여 구성할 수 있는 룰에 사용할 수 있습니다. **룰 마법사**는 **오펜스**, **로그 보기** 또는 **네트워크 활동** 탭에서 액세스할 수 있습니다.

프로시저

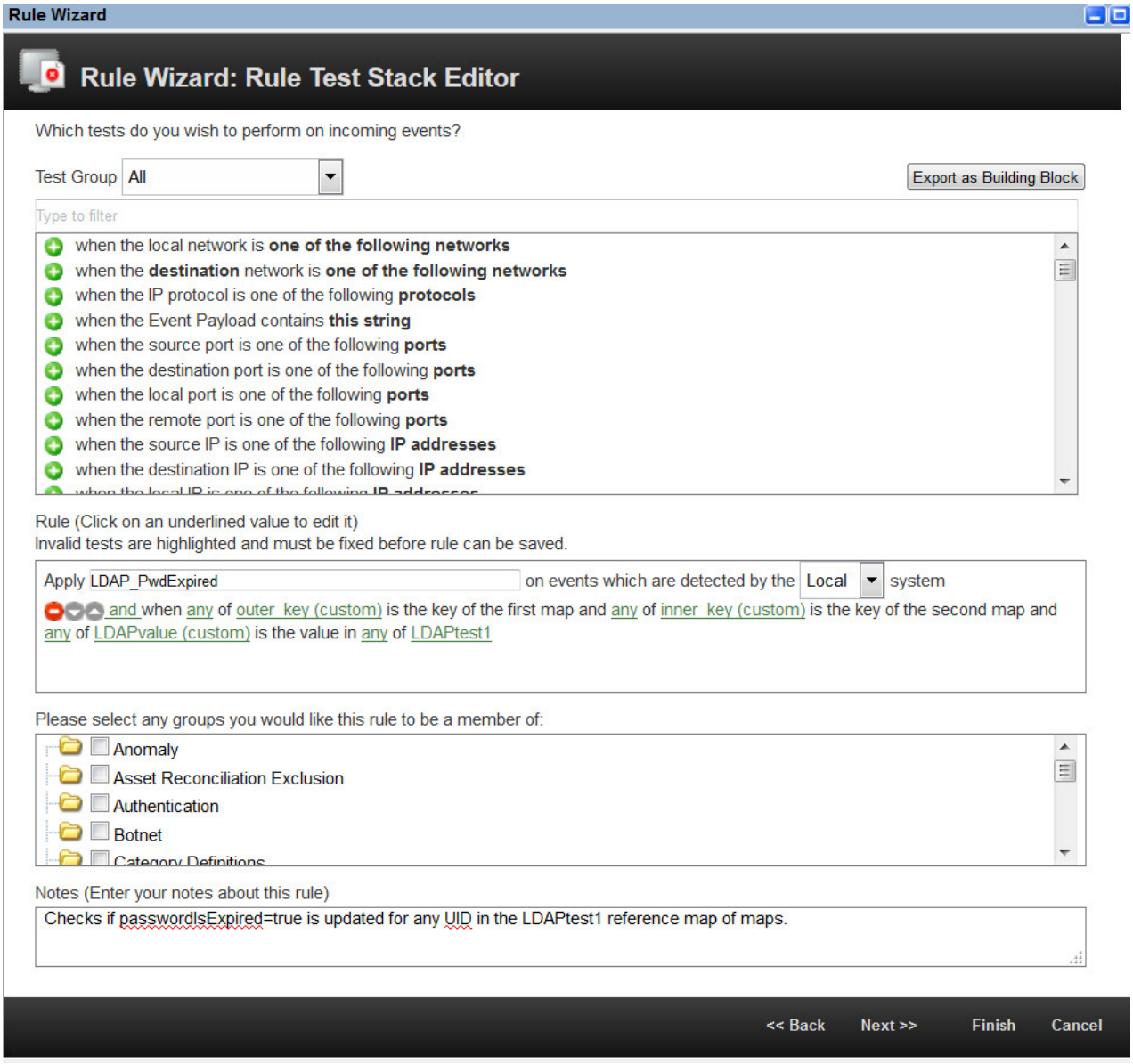
1. **로그 보기** > **룰** > **조치** > **새 이벤트 룰**을 클릭하십시오.
2. **룰 마법사** 소개 페이지에서 **다음**을 클릭하십시오.
3. **이벤트** 단일 선택 단추가 선택되었는지 확인하고 **다음**을 클릭하십시오.
4. 제공된 필드에 룰의 이름을 입력하십시오.
5. **테스트 그룹** 목록에서 테스트를 선택하고 사용하려는 테스트 옆의 + 아이콘을 클릭하십시오.

   사용자가 선택하는 룰 테스트는 LDAP 데이터를 보유하는 참조 데이터 콜렉션에서 검색하려는 정보에 따라 다릅니다.

맵의 다음 참조 맵 이벤트 특성 테스트는 참조 데이터 가져오기 - LDAP 앱 참조 테이블이 업데이트될 때 트리거되는 이벤트를 테스트하도록 설계되었습니다.

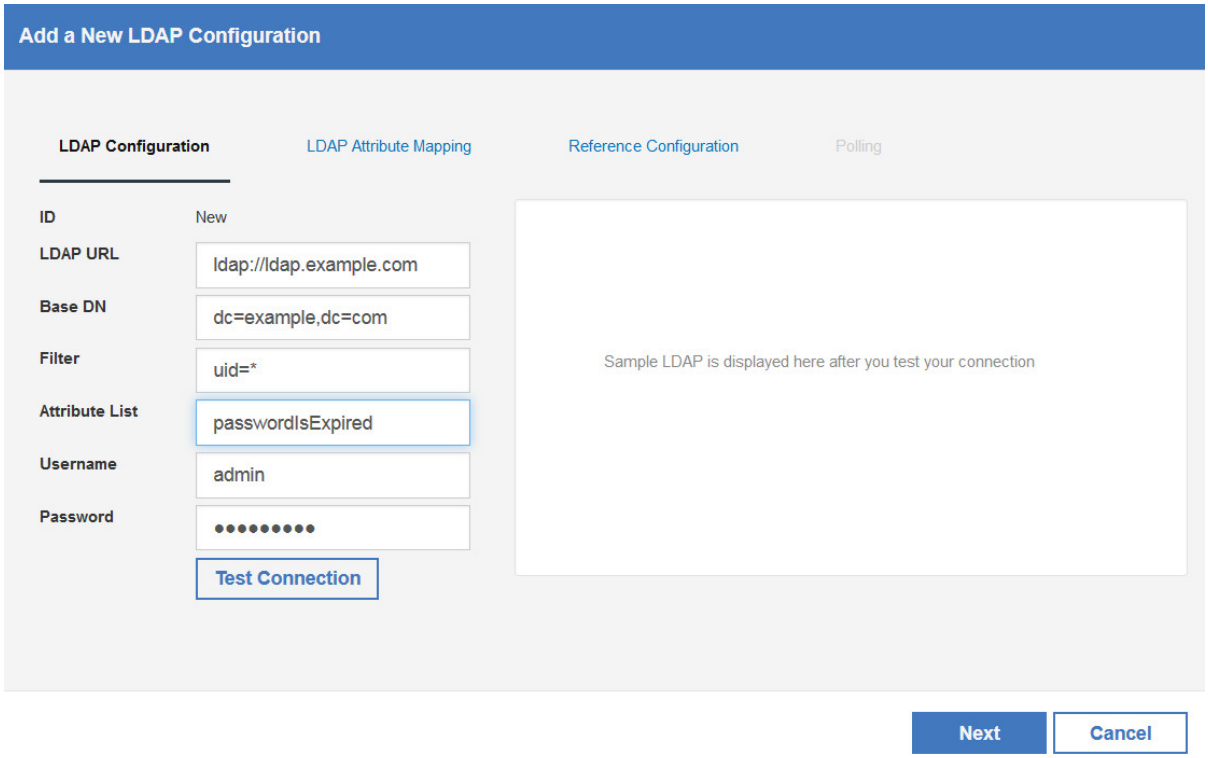
```
when any of these event properties is the key of the first map
 and any of these event properties is the key of the second map
 and any of these event properties is the value
 in any of these reference map of maps.
```

이 룰은 LDAP 속성 **PasswordIsExpired**가 **LDAPtest1** 참조 데이터 콜렉션의 UID에 대해 `true`로 업데이트되는 경우 `ReferenceDataExpiry` 이벤트 페이로드를 테스트하도록 구성됩니다.



이 이벤트 특성 테스트를 사용하려면 **외부 키**(첫 번째 맵의 키), **내부 키**(두 번째 맵의 키) 및 **값** 필드에 대한 사용자 정의 이벤트 특성을 작성해야 합니다. 다음 예제에서는 참조 데이터 가져오기 - LDAP 앱이 `example.com`의 LDAP 서버에서 비밀번호가 만료된 사용자에 대한 정보를 가져오

도록 구성되었습니다.



외부 키

이 특성에는 앱 LDAP 구성 탭의 **기본 DN** 및 **필터** 필드에서 지정된 LDAP 필드에 입력된 데이터가 포함되어 있습니다. 사용자 정의 이벤트 특성의 regex는 다음과 유사할 수 있습니다.

```
(uid=(.*?),dc=example,dc=com)
```

내부 키

이 특성에는 앱 LDAP 구성 탭에서 **속성** 필드에 지정된 LDAP 필드에 입력된 데이터가 포함되어 있습니다. 이 필드에서 속성 별명을 사용할 수 있습니다. 사용자 정의 이벤트 특성의 regex는 다음과 유사할 수 있습니다.

```
(passwordIsExpired)
```

값 필드

이 특성에는 각 사용자에 대한 **passwordIsExpired** LDAP 속성에 대해 검색된 데이터가 포함되어 있습니다. 사용자 정의 이벤트 특성의 regex는 다음과 유사할 수 있습니다.

```
(\['true'\])
```

사용자 정의 이벤트 특성에 대한 자세한 정보는 *IBM QRadar SIEM* 사용자 안내서의 내용을 참조하십시오.

6. **다음**을 클릭하십시오.

7. 룰에 적용하려는 룰 조치, 룰 응답 및 룰 리미터를 선택하고 **완료**를 클릭하십시오.

   사용자 정의 이벤트 룰에 대한 자세한 정보는 *IBM QRadar SIEM* 사용자 안내서의 내용을 참조하십시오.

결과

다음 번에 LDAP 서버를 폴링하고 사용자가 작성한 참조 데이터 콜렉션이 업데이트되면 사용자 룰이 트리거됩니다.

관련 태스크:

196 페이지의 『LDAP 속성 맵핑 추가』
별명을 추가하거나 참조 테이블에 대한 키를 설정할 수 있습니다.

196 페이지의 『참조 데이터 구성 추가』
참조 구성 탭을 사용하여 LDAP 데이터를 저장하기 위한 참조 데이터 테이블을 설정합니다.

9 Machine Learning Analytics 앱

Machine Learning Analytics(ML) 앱은 기계 학습 분석에 대한 유스 케이스를 추가하여 QRadar User Behavior Analytics(UBA) 앱 및 QRadar 시스템의 기능을 확장합니다. Machine Learning Analytics 유스 케이스를 사용하면 예측 모델링을 통해 사용자 행위패턴에 대한 추가적인 통찰을 얻을 수 있습니다. ML 앱을 통해 네트워크에 있는 사용자의 예상 행위패턴을 파악할 수 있습니다.

주의: UBA 앱 및 ML 앱을 설치하기 전에 IBM QRadar V7.2.8 이상을 설치해야 합니다.

중요사항:

- 처음에 UBA 앱을 구성하고 하루 뒤에 Machine Learning Analytics 설정을 사용으로 설정하는 것이 좋습니다. 이 대기 기간을 통해 사용자를 위한 위험 프로파일을 작성할 수 있는 충분한 시간이 UBA 앱에 제공됩니다.
- 모델은 7일마다 업데이트됩니다. 이는 Machine Learning Analytics 앱에서 최근의 위험한 사용자를 모니터하기 위한 것입니다.
- QRadar Console은 앱에서 사용할 수 있는 메모리의 양을 제한합니다. ML 애플리케이션 설치 크기 옵션은 QRadar에서 현재 애플리케이션용으로 보유하고 있는 메모리 양을 기반으로 합니다.
  - ML 애플리케이션을 설치하는 데 필요한 최소 사용 가능한 메모리는 QRadar Console에서는 2GB이고 애플리케이션 노드에서는 5GB입니다.
  - ML 앱에서 모니터하는 사용자 수는 ML 앱 설치 크기와 특정 Machine Learning 분석에 따라 달라집니다. 모든 Machine Learning 분석에 의해 모니터되는 최대 사용자 수는 Machine Learning 설치 크기의 GB당 500명의 사용자입니다. 예를 들어, 2GB는 최대 1000명의 사용자가 될 수 있고 50GB는 최대 25000명의 사용자가 될 수 있습니다.
- 사용 가능한 메모리의 부족으로 인해 설치가 실패할 수 있습니다. 이 상황은 다른 애플리케이션이 설치되어서 애플리케이션에 사용 가능한 메모리 크기가 줄어든 경우에 발생할 수 있습니다.

Machine Learning Analytics의 알려진 문제점

Machine Learning Analytics 앱에는 설치 필수 정보 및 알려진 문제점이 있습니다.

Machine Learning Analytics 앱에는 다음과 같은 알려진 문제점이 있습니다.

- Machine Learning 앱에서 Machine Learning 상태 섹션에 경고 메시지를 표시할 수 있습니다. 추가 정보는 234 페이지의 『대시보드에서 Machine Learning 앱 상태가 경고를 표시함』의 내용을 참조하십시오.
- 사용 가능한 메모리의 부족으로 인해 설치가 실패할 수 있습니다. 이 상황은 여러 개의 다른 앱이 이미 설치되어 있고 ML 앱이 사용할 수 있는 메모리가 10GB 미만으로 남아 있는 경우에 128GB

콘솔에서 발생할 수 있습니다. 설치에 실패하면 오류 메시지 "실패"가 표시됩니다. 이 상황을 해결하려면 나머지 앱의 일부를 설치 제거한 후 다시 시도하십시오.

Machine Learning Analytics 앱 설치의 전제조건

Machine Learning Analytics 앱을 설치하기 전에 요구사항을 충족하는지 확인하십시오.

Machine Learning Analytics 앱을 설치하려면 먼저 다음 시스템 요구사항을 충족하고 User Behavior Analytics(UBA) 앱을 전체 설치 및 구성해야 합니다.

구성요소	최소 요구사항
시스템 메모리	• 콘솔: 64GB • 앱 노드: 5GB
IBM QRadar 버전	V7.2.8 이상
Sense DSM	DSM RPM 파일을 설치하십시오.
UBA 앱	• UBA V3.1.0 앱을 설치하십시오. • UBA 설정을 구성하십시오. • **사용자 분석** 탭을 클릭하고 UBA 대시보드가 사용자 데이터를 포함하고 있는지 확인하십시오.

수동으로 IBM Sense DSM 설치

UBA 앱 및 Machine Learning Analytics 앱은 다음 IBM Sense DSM 파일을 사용하여 QRadar에 사용자 위험성 점수 및 오펜스를 추가합니다.

- V7.2.8의 경우: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
- QRadar V7.3.1 이상의 경우: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`

제한사항: DSM(Device Support Module) 설치 제거는 QRadar에서 지원되지 않습니다.

1. DSM RPM 파일을 QRadar Console에 복사하십시오.
2. SSH를 사용하여 root 사용자로 QRadar 호스트에 로그인하십시오.
3. 다운로드한 파일이 있는 디렉토리로 이동하십시오.
4. 다음 명령을 입력하십시오.

   ```
   rpm -Uvh <rpm_filename>
   ```

5. **관리** 설정에서 **고급** > **전체 구성 배치**를 클릭하십시오.

참고: UBA 앱 설치 및 구성에 대한 지시사항은 IBM Knowledge Center에 있습니다.

관련 태스크:

19 페이지의 『User Behavior Analytics 앱 설치』
IBM QRadar 확장 관리 도구를 사용하여 QRadar Console에 직접 앱 아카이브를 업로드하고 설치합니다.

30 페이지의 『UBA 설정 구성』
IBM QRadar User Behavior Analytics(UBA) 앱에서 정보를 보려면 UBA 애플리케이션 설정을 구성해야 합니다.

Machine Learning Analytics 앱 설치

확장 관리자에서 UBA 앱을 설치한 후에 Machine Learning Analytics 앱을 설치하십시오.

시작하기 전에

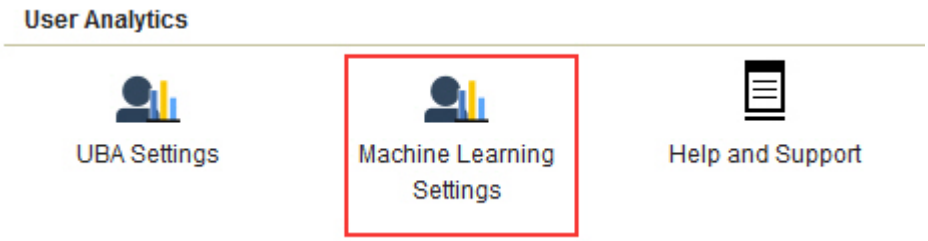
Machine Learning Analytics 앱 설치를 위한 전제조건을 모두 완료했는지 확인하십시오.

이 태스크 정보

User Behavior Analytics(UBA) 앱 V2.1.0 이상을 설치한 후에 Machine Learning 설정 페이지에서 Machine Learning Analytics 앱을 설치할 수 있습니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.



3. Machine Learning 설정 페이지에서 **ML 앱 설치**를 클릭하십시오.
4. 프롬프트에서 **예**를 클릭하여 앱을 설치하십시오. ML 앱을 설치하는 데 몇 분이 걸립니다.

다음에 수행할 작업

설치가 완료되면 ML 유스 케이스를 사용으로 설정한 후 **구성 저장**을 클릭할 수 있습니다.

Machine Learning Analytics 앱 업그레이드

Machine Learning 설정 페이지에서 Machine Learning Analytics 앱을 업그레이드하십시오.

시작하기 전에

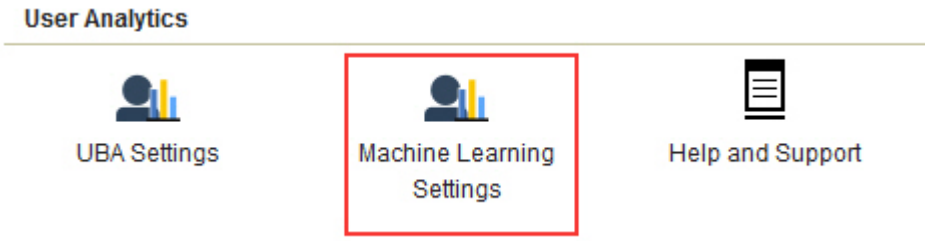
ML V2.2.0이 포함된 UBA부터 업그레이드 프로시저가 없습니다. Machine Learning 앱은 UBA 앱을 통해 자동 업그레이드됩니다. User Behavior Analytics(UBA) 앱을 설치하거나 업그레이드한 후에 Machine Learning 설정 페이지에서 기존 Machine Learning Analytics 앱을 업그레이드할 수 있습니다.

주의: Machine Learning Analytics(ML) 앱 V2.0.0이 설치되어 있고 UBA 앱을 최신 버전으로 업그레이드하는 경우, QRadar 확장 관리자에서 Machine Learning Analytics 앱을 설치 제거하지 마십시오. 확장 관리자에서 Machine Learning Analytics 앱을 설치 제거하려고 하면 ML 앱 설치에서 문제가 발생할 수 있습니다.

참고: Machine Learning Analytics 앱 V2.1.0 이하에서 업그레이드하는 경우 각 사용자 분석의 **감지 이벤트의 위험한 값**이 현재 Machine Learning 기본값으로 업데이트됩니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.



3. Machine Learning 설정 페이지에서 **ML 앱 업그레이드**를 클릭하십시오.
4. 프롬프트에서 **예**를 클릭하십시오. ML 앱을 업그레이드하는 데 몇 분이 걸립니다.
5. 업그레이드가 완료되면 모델 빌드가 다시 시작됩니다.

다음에 수행할 작업

Machine Learning 설정이 올바르게 구성되었는지 검증하십시오. 설정을 변경하는 경우 **구성 저장**을 확인하십시오.

Machine Learning Analytics 설정 구성

Machine Learning Analytics 앱에서 정보를 보려면 Machine Learning Analytics 애플리케이션 설정을 구성해야 합니다.

총 활동 분석 구성

총 활동 기계 학습 분석을 구성하여 UBA 대시보드에 하루동안 사용자의 실제 및 예상(학습된) 활동량을 표시할 수 있습니다.

이 태스크 정보

경고: 설정을 구성하거나 수정한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

중요사항: V2.2.0부터 **감지 이벤트의 위험 값**에 대한 기본값이 변경되었습니다. 새 기본값이 이전 기본값보다 많이 작기 때문에 새 기본값이 기존 기본값이나 이전에 수정한 값을 겹쳐씁니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 **총 활동**을 클릭하십시오.
4. **사용**  을 클릭해서 총 활동 분석을 켜십시오.

   중요사항: 분석에서 모델을 생성하려면 7일 동안 데이터가 사용 가능해야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 총 활동 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 총 활동 그래프를 표시하지 않으려면 전환을 클릭하십시오.

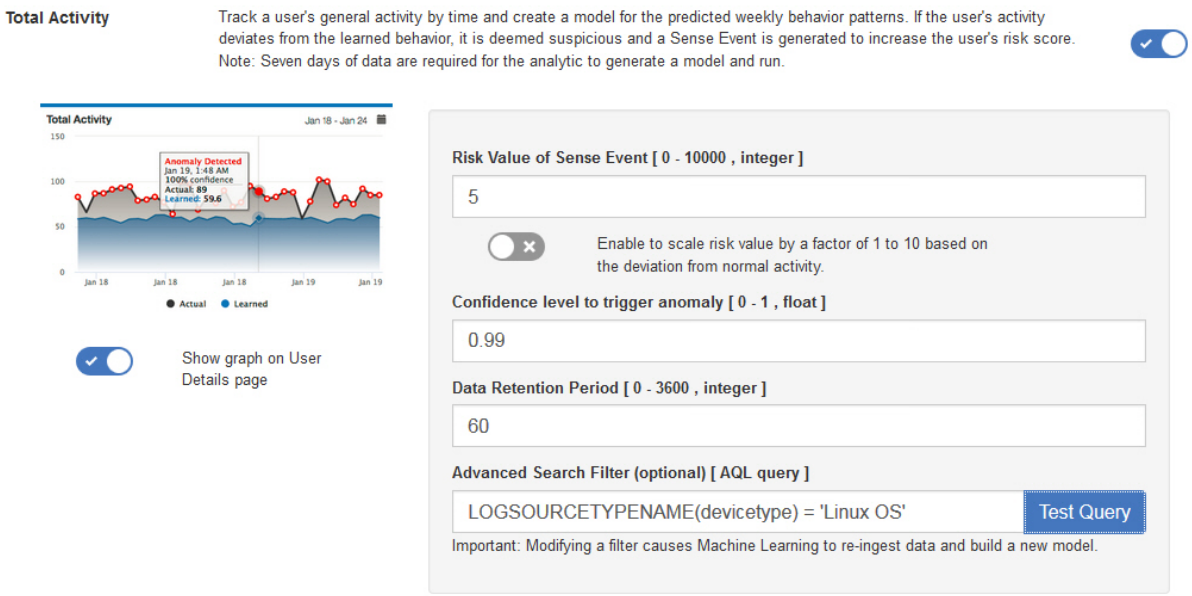
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

    - `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)`

    자세한 정보는 Ariel Query Language를 참조하십시오.
11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

비정상 아웃바운드 전송 시도 분석 구성

비정상 아웃바운드 전송 시도 기계 학습 분석을 구성하여 UBA 대시보드에 각 사용자에 대한 아웃바운드 전송 사용량을 표시할 수 있습니다.

이 태스크 정보

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

비정상 아웃바운드 전송 시도 기계 학습 분석은 V2.8.0 이상에서 사용 가능합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.

3. Machine Learning 설정 페이지에서 **비정상 아웃바운드 전송 시도**를 클릭하십시오.
4. **사용**  을 클릭해서 비정상 아웃바운드 전송 시도 분석을 켜십시오.

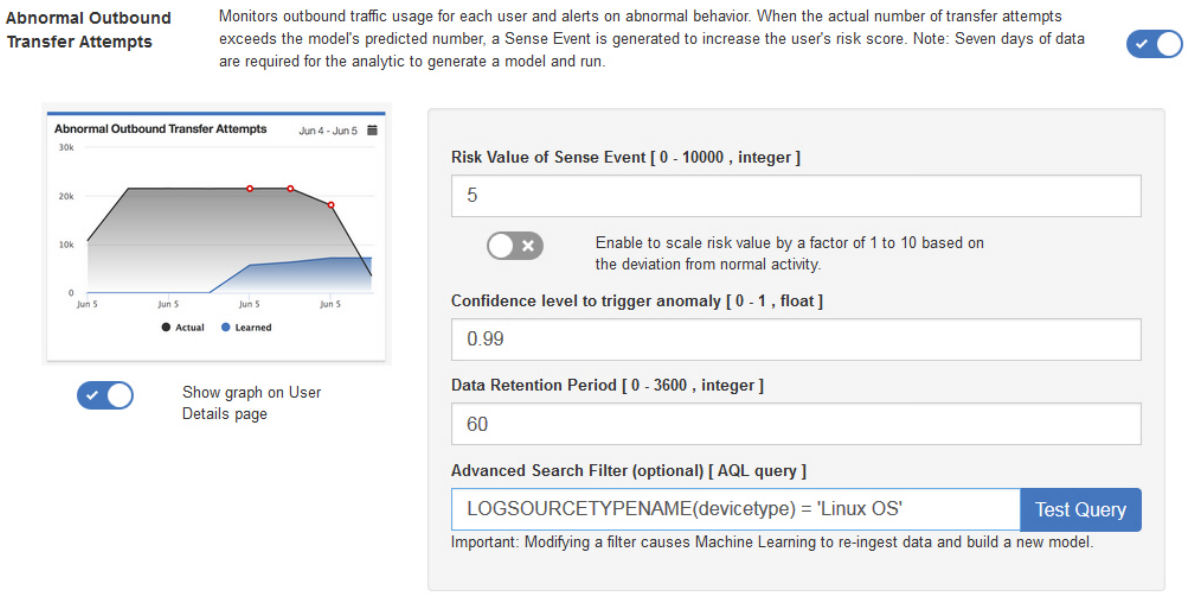
   중요사항: 시스템에서 UBA 컨텐츠를 사용으로 설정한 후 7일 간의 데이터가 있어야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 기본적으로 꺼져 있습니다. 비정상 아웃바운드 전송 시도 그래프를 사용자 세부사항 페이지에 표시하려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

    - `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)`

    자세한 정보는 Ariel Query Language를 참조하십시오.
11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

카테고리별 활동 분석 구성

카테고리별 활동 기계 학습 분석을 구성하여 UBA 대시보드에 상위 레벨 카테고리별 실제 및 예상되는 사용자 활동의 작동 패턴을 표시할 수 있습니다.

이 태스크 정보

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

중요사항: V2.2.0부터 **감지 이벤트의 위험 값**에 대한 기본값이 변경되었습니다. 새 기본값이 이전 기본값보다 많이 작기 때문에 새 기본값이 기존 기본값이나 이전에 수정한 값을 겹쳐씁니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.

- QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.

3. Machine Learning 설정 페이지에서 **카테고리별 활동**을 클릭하십시오.
4. **사용**  을 클릭하여 카테고리별 활동 분석을 켜고 사용자 세부사항 페이지에 카테고리별 활동 그래프를 표시하십시오.

   중요사항: 분석에서 초기 모델을 생성하려면 7일 간의 데이터가 사용 가능해야 합니다. 이 QRadar 시스템에 대해 7일 미만의 사용자 데이터가 있는 경우 7일 간의 사용자 데이터가 누적된 후에 초기 모델이 생성됩니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 카테고리별 활동 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 카테고리별 활동 그래프를 표시하지 않으려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 1입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **추적할 카테고리** 섹션에서 기본적으로 상위 레벨 이벤트 카테고리가 사용으로 설정됩니다. 카테고리 모니터링을 사용 안함으로 설정하려면 카테고리를 클릭하십시오. 카테고리에 대한 자세한 정보는 IBM Knowledge Center의 상위 레벨 카테고리 주제를 참조하십시오.
10. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
11. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

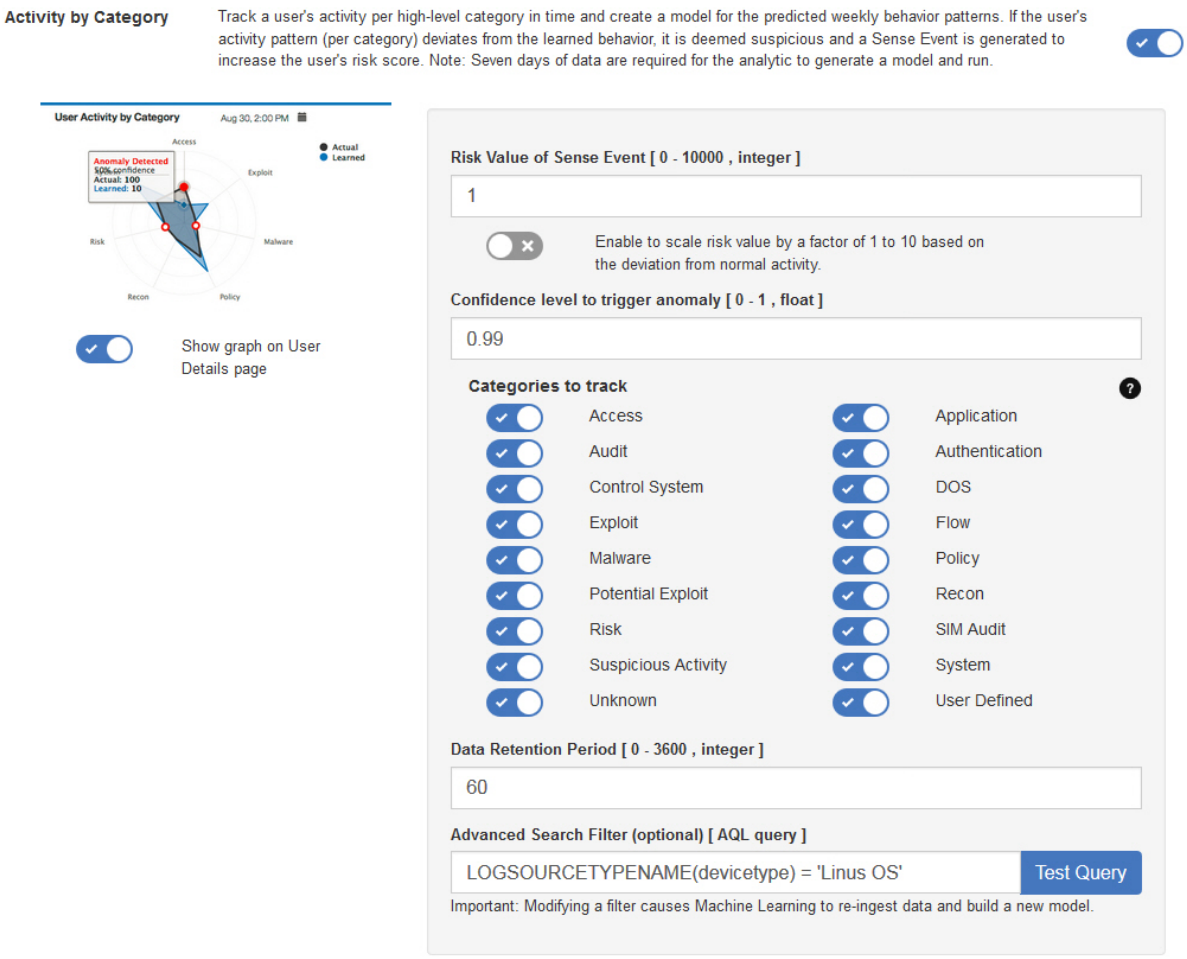
    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

    - `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)**

자세한 정보는 Ariel Query Language를 참조하십시오.

12. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

위험 관리 태세 분석 구성

위험 관리 태세 기계 학습 분석을 구성하여 UBA 대시보드에 사용자 위험성 점수 편차를 표시할 수 있습니다.

이 태스크 정보

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

중요사항: V2.2.0부터 **감지 이벤트의 위험 값**에 대한 기본값이 변경되었습니다. 새 기본값이 이전 기본값보다 많이 작기 때문에 새 기본값이 기존 기본값이나 이전에 수정한 값을 겹쳐씁니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 **위험 관리 태세**를 클릭하십시오.
4. **사용**  을 클릭해서 위험 관리 태세 분석을 켜십시오.

   중요사항: 분석에서 모델을 생성하려면 7일 동안 데이터가 사용 가능해야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 위험 관리 태세 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 위험 관리 태세 그래프를 표시하지 않으려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

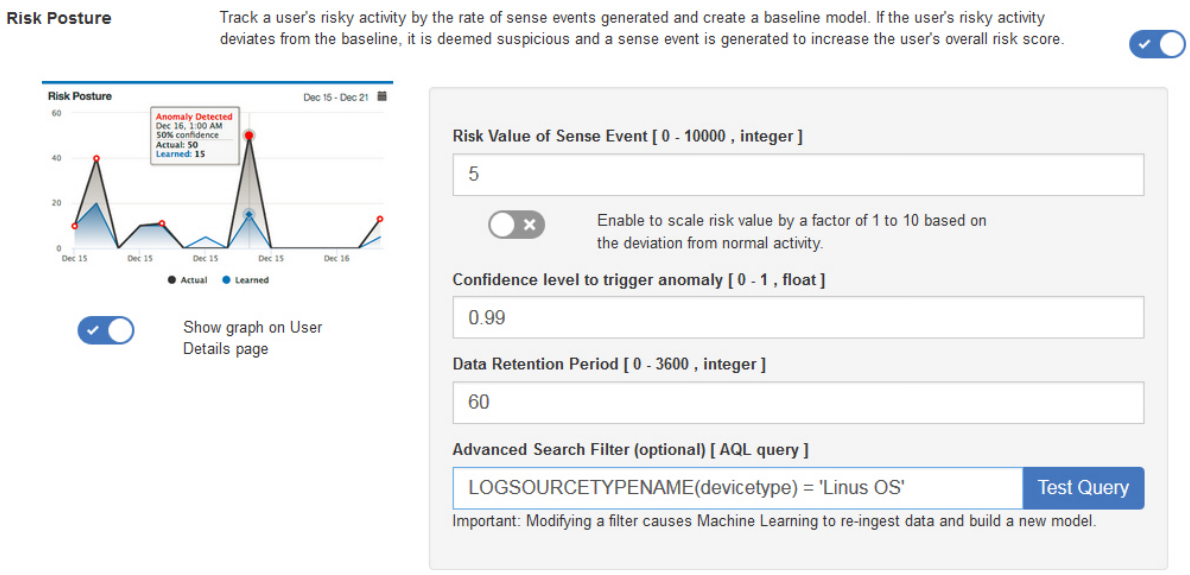
    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

- **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)**

자세한 정보는 Ariel Query Language를 참조하십시오.

11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

외부 도메인에 대한 비정상 데이터 볼륨 분석 구성

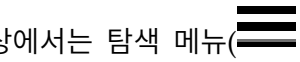
외부 도메인에 대한 비정상 데이터 볼륨 기계 학습 분석을 구성하여 UBA 대시보드에 각 사용자에 대한 실제 및 예상(학습된) 로컬 대 원격 업로드 볼륨을 표시할 수 있습니다.

이 태스크 정보

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

외부 도메인에 대한 비정상 데이터 볼륨 기계 학습 분석은 V3.0.0 이상에서 사용 가능합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴()를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 **외부 도메인에 대한 비정상 데이터 볼륨**을 클릭하십시오.
4. **사용**()을 클릭하여 외부 도메인에 대한 비정상 데이터 볼륨 분석을 켜십시오.

   중요사항: 시스템에서 UBA 컨텐츠를 사용으로 설정한 후 7일 간의 데이터가 있어야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 기본적으로 꺼져 있습니다. 사용자 세부사항 페이지에 외부 도메인에 대한 비정상 데이터 볼륨 그래프를 표시하려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 1입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

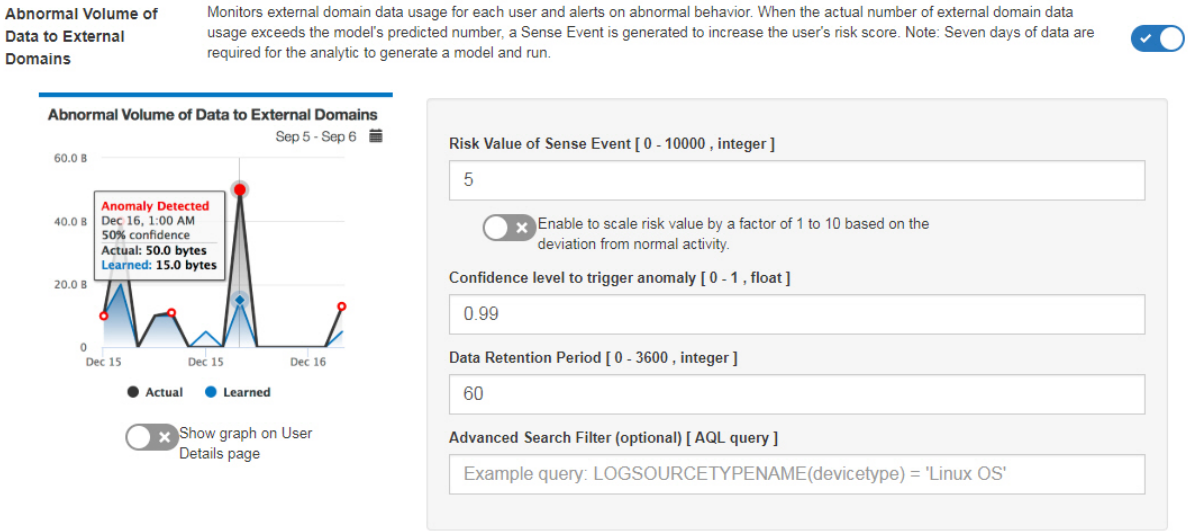
    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

- `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)`

자세한 정보는 Ariel Query Language를 참조하십시오.

11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

활동 분포 분석 구성

활동 분포 기계 학습 분석을 구성하여 UBA 대시보드에 기계 학습에서 모니터하는 모든 사용자에 대한 동적 작동 클러스터를 표시할 수 있습니다.

이 태스크 정보

활동 분포 기계 학습 분석은 V2.2.0 이상에서 사용 가능합니다.

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.

- IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.

2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 **활동 분포**를 클릭하십시오.
4. **사용**  을 클릭하여 활동 분포 분석을 켜고 사용자 세부사항 페이지에 활동 분포 그래프를 표시하십시오.

   중요사항: 분석에서 모델을 생성하려면 7일 동안 데이터가 사용 가능해야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 활동 분포 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 활동 분포 그래프를 표시하지 않으려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

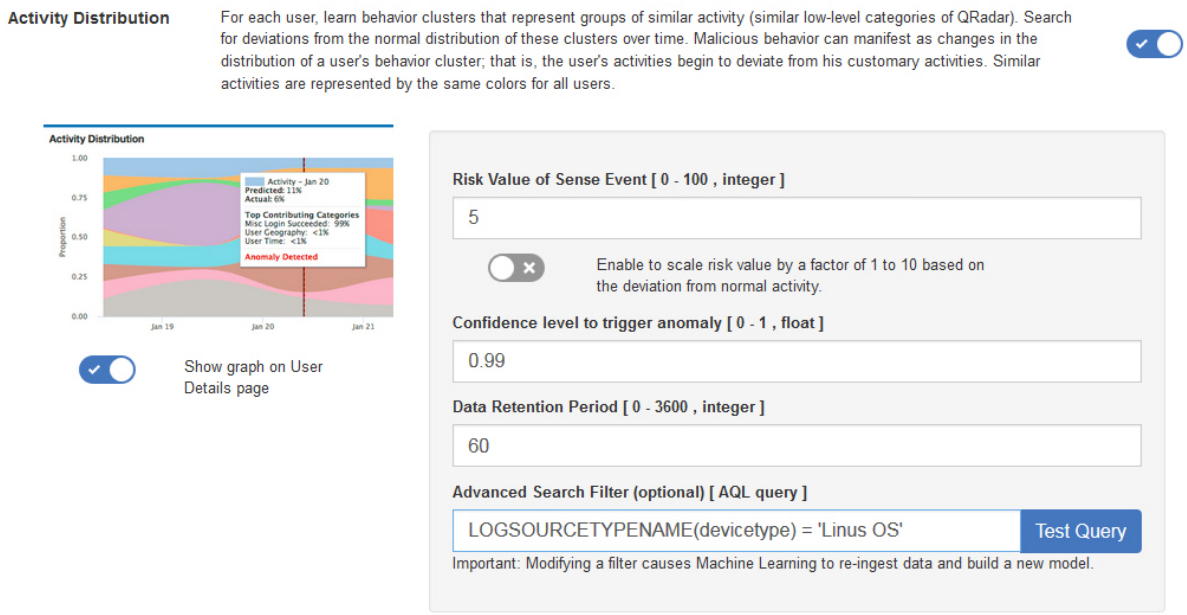
    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

    - `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)**

자세한 정보는 Ariel Query Language를 참조하십시오.

11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

정의된 피어 그룹 분석 구성

정의된 피어 그룹 기계 학습 분석을 구성하여 UBA 대시보드에 사용자의 이벤트 활동이 정의된 피어 그룹의 이벤트 활동에서 벗어난 정도를 표시할 수 있습니다.

시작하기 전에

- 정의된 피어 그룹 분석을 사용하려면 참조 테이블에 올바른 사용자 그룹을 배치한 다음, 참조 테이블을 사용하도록 **UBA 설정** > **속성 표시** > **사용자 정의 그룹**을 구성해야 합니다. 추가 정보는 230 페이지의 『정의된 피어 그룹 분석을 위한 사용자 그룹』의 내용을 참조하십시오.
- 분석에서 모델을 생성하려면 7일 간의 이벤트 데이터가 사용 가능해야 합니다.

이 태스크 정보

정의된 피어 그룹 기계 학습 분석은 V2.6.0 이상에서 사용 가능합니다.

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 정의된 피어 그룹을 클릭하십시오.
4. **사용**  을 클릭해서 정의된 피어 그룹 분석을 켜십시오.

   중요사항: 분석에서 모델을 생성하려면 7일 동안 데이터가 사용 가능해야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 정의된 피어 그룹 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 정의된 피어 그룹 그래프를 표시하지 않으려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. **그룹 기준** 필드에서 정의된 피어 그룹 분석에서 사용할 그룹을 선택하십시오.
11. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을

줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

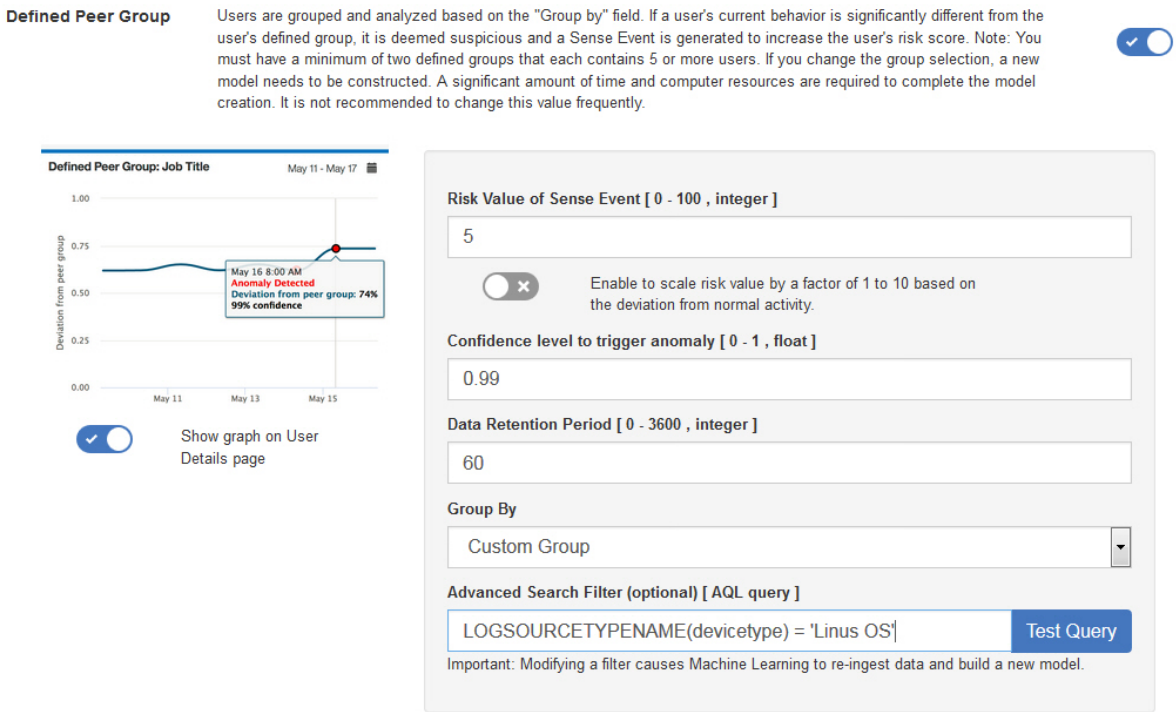
중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

- `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)`

자세한 정보는 Ariel Query Language를 참조하십시오.

12. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

학습된 피어 그룹 분석 구성

학습된 피어 그룹 기계 학습 분석을 구성하여 사용자의 이벤트 활동이 UBA 대시보드에 사용자가 속한 것으로 예상했던 유추된 피어 그룹에서 벗어난 정도를 표시할 수 있습니다.

시작하기 전에

- 학습된 피어 그룹 분석을 사용으로 설정하려면 앱 노드를 설치해야 합니다. 추가 정보는 https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_adm_appnode_intro.html의 내용을 참조하십시오.
- 학습된 피어 그룹 분석에서 모델을 생성하려면 7일 간의 이벤트 데이터가 사용 가능해야 합니다.

이 태스크 정보

학습된 피어 그룹 기계 학습 분석은 V2.2.0 이상에서 사용 가능합니다.

경고: 설정을 구성한 후에 데이터를 수집하고 초기 모델을 빌드하고 사용자에 대한 초기 결과를 보려면 최소 1시간이 걸립니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴( )를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
3. Machine Learning 설정 페이지에서 학습된 피어 그룹을 클릭하십시오.
4. **사용**  을 클릭해서 학습된 피어 그룹 분석을 켜십시오.

   중요사항: 분석에서 모델을 생성하려면 7일 동안 데이터가 사용 가능해야 합니다.
5. **사용자 세부사항 페이지에 그래프 표시** 전환은 사용자 세부사항 페이지에 학습된 피어 그룹 그래프를 표시하도록 기본적으로 사용으로 설정됩니다. 사용자 세부사항 페이지에 학습된 피어 그룹 그래프를 표시하지 않으려면 전환을 클릭하십시오.
6. **감지 이벤트의 위험 값** 필드에 감지 이벤트가 트리거되는 경우 사용자의 위험성 점수를 늘릴 크기를 입력하십시오. 기본값은 5입니다.

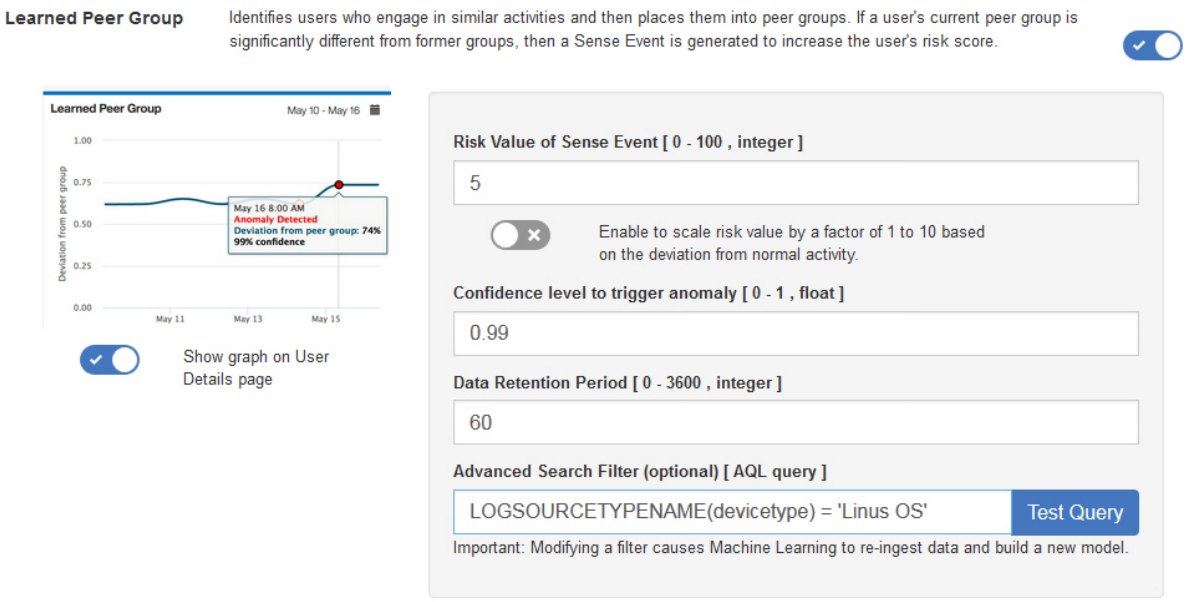
7. 위험 값의 크기를 조정하려면 전환을 사용으로 설정하십시오. 사용으로 설정되면 기본 위험 값에 인수(1 - 10 범위)가 곱해집니다. 이 인수는 단순히 사용자가 예상 작동에서 벗어난 사실이 아니라 사용자가 예상 작동에서 벗어난 정도에 의해 판별됩니다.
8. **비정상 트리거 신뢰구간** 필드에 기계 학습 알고리즘이 비정상 이벤트를 트리거하기 전에 신뢰해야 하는 백분율을 입력하십시오. 기본값은 0.99입니다.
9. **데이터 보존 기간** 필드에 모델 데이터를 저장하려는 일 수를 설정하십시오. 기본값은 60입니다. 데이터의 자동 제거를 사용 안함으로 설정하려는 경우 값을 0(영)으로 설정하십시오.
10. 옵션: **고급 검색 필터** 필드에서 AQL 필터를 추가하여 QRadar에서 분석 조회에 사용하는 데이터를 좁힐 수 있습니다. AQL 조회를 사용하여 필터링하면 분석 대상인 사용자 수나 분석 유형을 줄일 수 있습니다. 구성을 저장하기 전에 **조회 테스트**를 클릭하여 QRadar에서 전체 AQL 조회를 실행하면 조회를 검토하고 결과를 확인할 수 있습니다.

    중요사항: AQL 필터를 수정하면 분석의 기존 모델은 올바르지 않은 모델로 표시되고 다시 빌드됩니다. 다시 빌드하는 데 걸리는 시간은 수정된 필터에 의해 리턴되는 데이터 양에 따라 다릅니다.

    특정 로그 소스, 네트워크 이름 또는 특정 사용자가 포함된 참조 세트를 필터링할 수 있습니다. 다음 예제를 참조하십시오.

    - `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)`

    자세한 정보는 Ariel Query Language를 참조하십시오.
11. **구성 저장**을 클릭하십시오.



결과

앱이 데이터를 수집하고 초기 모델을 빌드하는 데 최소 1시간이 걸릴 수 있습니다.

Machine Learning Analytics가 있는 UBA 대시보드

Machine Learning Analytics가 있는 IBM QRadar User Behavior Analytics(UBA) 앱에는 선택된 사용자의 Machine Learning Analytics 상태 및 추가 세부사항이 포함되어 있습니다.

대시보드

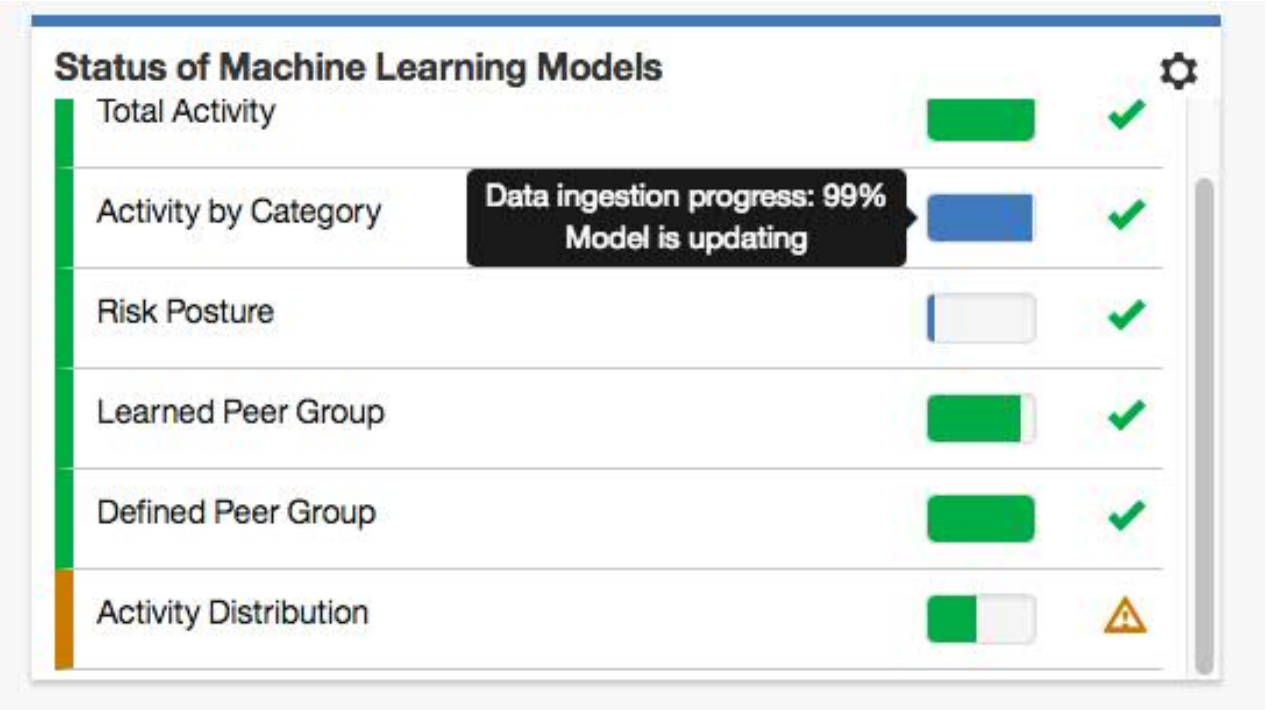
Machine Learning Analytics를 사용으로 설정한 후 **사용자 분석** 탭을 클릭하여 대시보드를 여십시오.

Machine Learning 모델의 상태 섹션은 사용으로 설정한 각 분석에 대한 모델 수집 및 모델 빌드 진행상태를 표시합니다. 7일마다 모델이 업데이트됩니다.

- 파란색 진행 표시줄은 분석에서 데이터를 수집 중임을 표시합니다.
- 녹색 진행 표시줄은 분석에서 모델을 빌드 중임을 표시합니다.
- 녹색 체크 표시는 분석이 사용됨을 표시합니다.
- 노란색 경고 아이콘은 모델 빌드 단계에서 문제가 발생했음을 표시합니다. 234 페이지의 『대시보드에서 Machine Learning 앱 상태가 경고를 표시함』의 내용을 참조하십시오.

ML 설정 아이콘( )을 클릭하여 Machine Learning Analytics 페이지를 열고 Machine Learning Analytics 유스 케이스의 구성을 편집하십시오.

참고: 구성이 저장된 후에 이를 편집하는 경우 새 모델이 빌드되고 수집 및 모델 빌드 대기 시간이 재설정됩니다.

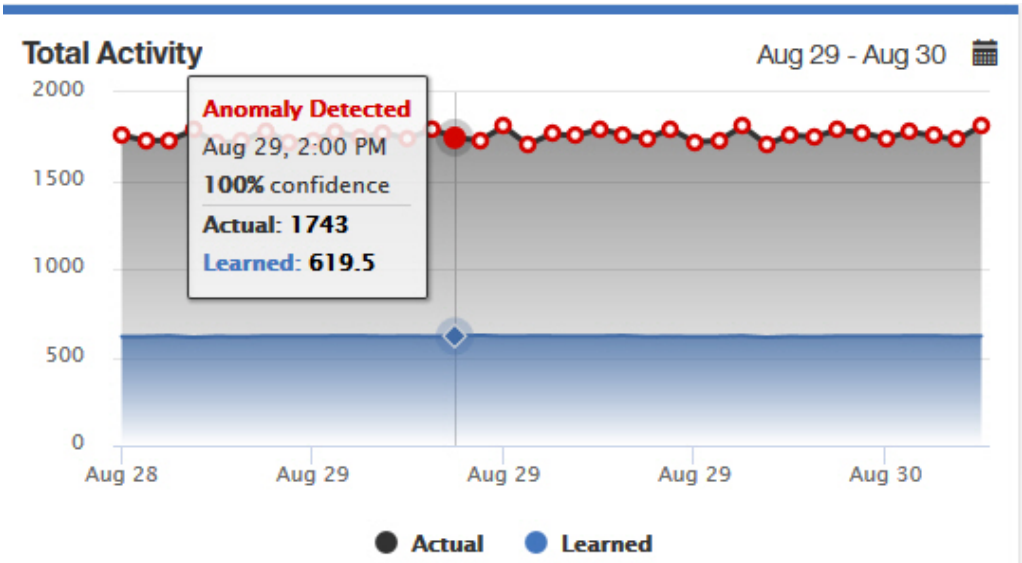
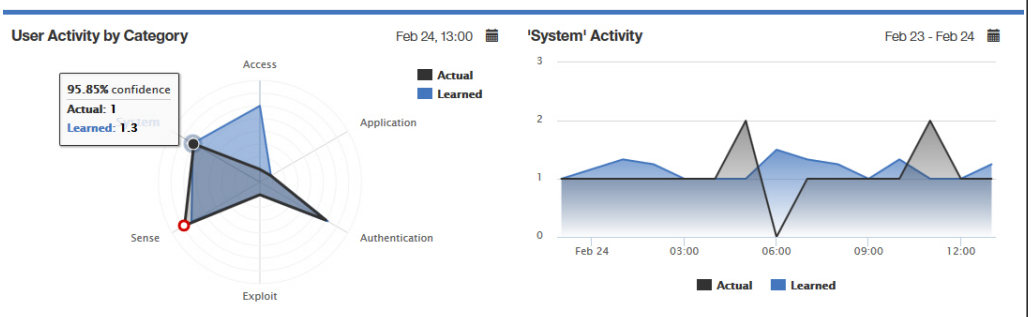


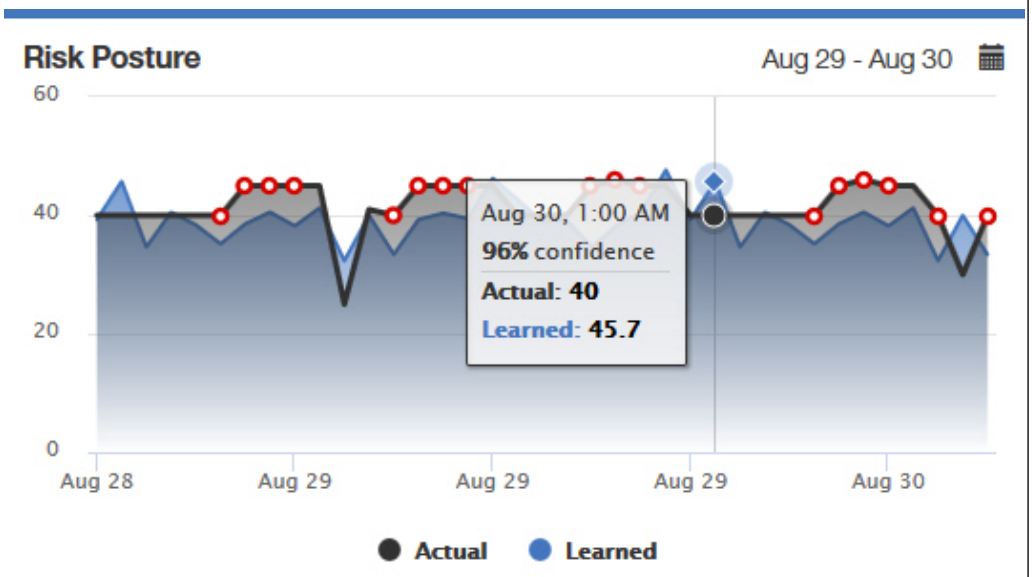
사용자 세부사항 페이지

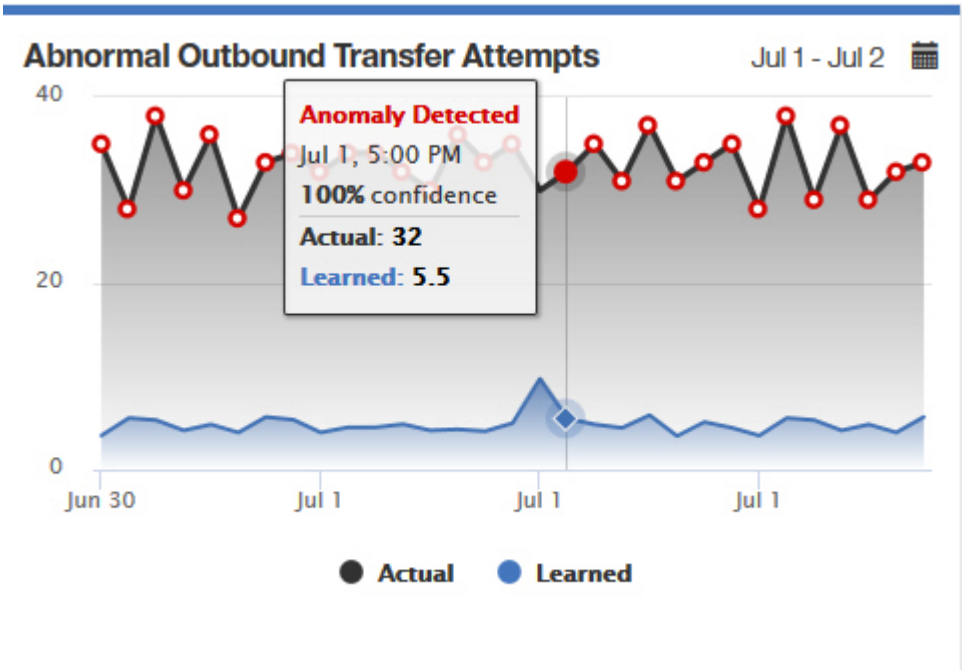
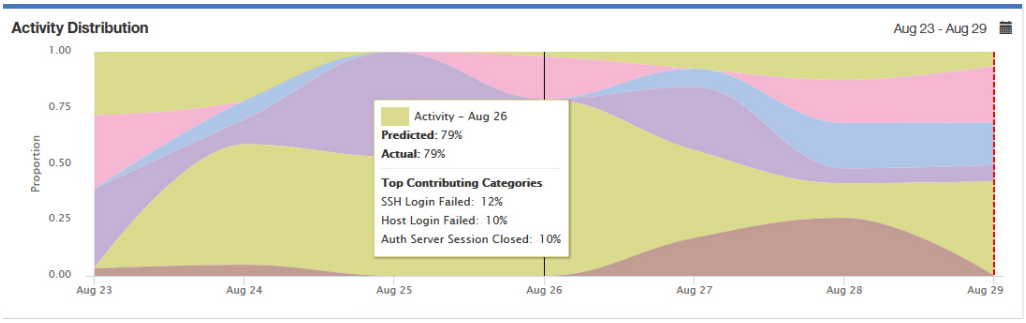
앱의 어디서든 사용자 이름을 클릭하여 선택한 사용자에 대한 세부사항을 볼 수 있습니다.

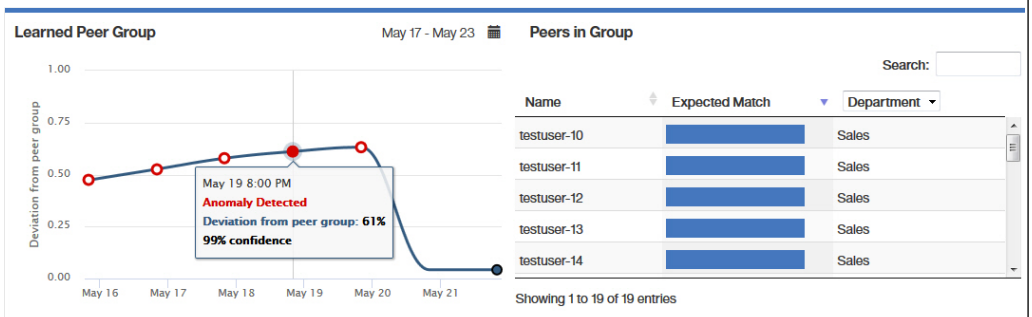
V2.5.0부터는 이벤트 뷰어 분할창에서 사용자 활동에 대한 자세한 정보를 볼 수 있습니다. 이벤트 뷰어 분할창은 선택한 활동 또는 시점에 대한 정보를 표시합니다. 이벤트 뷰어 분할창에서 이벤트를 클릭하면 syslog 이벤트 및 페이로드 정보와 같은 세부사항이 표시됩니다. 이벤트 뷰어 분할창은 사용자 세부사항 페이지의 모든 원 및 선 그래프에 사용할 수 있습니다.

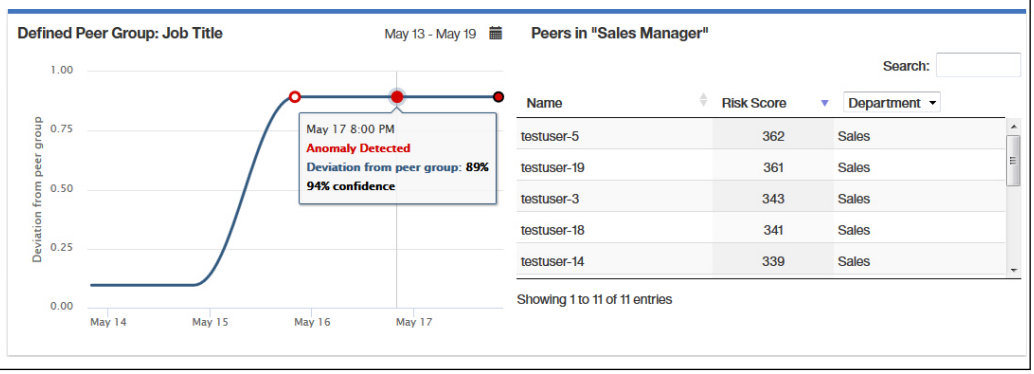
다음 표는 사용자 세부사항 페이지에서 사용 가능한 Machine Learning Analytics 그래프에 대해 설명합니다.

총 활동	하루동안 사용자의 실제 및 예상(학습된) 활동량을 표시합니다. 실제 값은 선택된 기간 동안 해당 사용자에 대한 이벤트 수입니다. 예상 값은 선택된 기간 동안 해당 사용자에 대한 예측된 이벤트 수입니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다. 총 활동 그래프에서 다음을 수행할 수 있습니다. • 데이터 노드를 클릭하여 비정상을 구성하는 이벤트의 조회 목록을 가져옵니다. • **캘린더** 아이콘을 클릭하여 사용자 정의 날짜 범위를 지정합니다. 
카테고리별 사용자 활동	상위 레벨 카테고리별로 실제 및 예상되는 사용자 활동의 작동 패턴을 표시합니다. 실제 값은 선택된 기간 동안 해당 사용자에 대한 상위 레벨 카테고리당 이벤트 수입니다. 예상 값은 선택된 기간 동안 해당 사용자에 대한 상위 레벨 카테고리당 예측된 이벤트 수입니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다. 카테고리별 사용자 활동 그래프에서 다음을 수행할 수 있습니다. • **캘린더** 아이콘을 클릭하여 시간 및 날짜를 지정하십시오. • 카테고리를 클릭하여 선택된 카테고리의 타임라인 그래프를 여십시오. 선택된 카테고리의 타임라인 그래프에서 다음을 수행할 수 있습니다. • 데이터 노드를 클릭하여 해당 항목을 표시하는 이벤트의 조회 목록을 가져옵니다. • **캘린더** 아이콘을 클릭하여 사용자 정의 날짜 범위를 지정합니다. 

위험 관리 태세	사용자의 위험성 점수가 예상 위험성 점수 패턴에서 벗어나는지 여부를 표시합니다. 실제 값은 선택된 기간 동안 해당 사용자에 대한 감지 이벤트의 감지 값 합계입니다. 예상 값은 선택된 기간 동안 해당 사용자에 대한 감지 이벤트의 예측된 감지 값의 합계입니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다. 위험 관리 태세 그래프에서 다음을 수행할 수 있습니다. • 노드를 클릭하여 이벤트의 조회 목록을 가져옵니다. • **캘린더** 아이콘을 클릭하여 사용자 정의 날짜 범위를 지정합니다. 

비정상 아웃바운드 전송 시도	사용자의 아웃바운드 트래픽 사용량이 예상되는 작동에서 벗어났는지 여부를 표시합니다. 실제 값은 선택된 기간 동안 해당 사용자에 대한 전송 시도 수입니다. 학습된 값은 모델에서 예측한 전송 시도 수입니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다. 비정상 아웃바운드 전송 시도 그래프에서 다음을 수행할 수 있습니다. • 노드를 클릭하여 이벤트의 조회 목록을 가져옵니다. • **캘린더** 아이콘을 클릭하여 사용자 정의 날짜 범위를 지정합니다. 
활동 분포(V2.2.0 이상)	기계 학습에서 모니터하는 모든 사용자에 대한 동적 작동 클러스터를 표시합니다. 클러스터는 기계 학습에서 모니터하는 모든 사용자에 대한 하위 레벨 활동 카테고리별로 유추됩니다. 실제 값은 해당 클러스터에 대한 백분율 일치입니다. 예상 값은 해당 클러스터에 대해 예측된 백분율 일치입니다. 그래프의 각 색상은 기계 학습에서 모니터하는 모든 사용자에 대해 고유한 동적 작동 클러스터를 표시합니다. 특정 그룹을 나타내는 데 사용되는 색상은 모든 사용자에게 동일합니다. 빨간색 세로선은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다. 활동 분포 그래프에서 다음을 수행할 수 있습니다. • 각 클러스터 위로 마우스를 이동하여 실제 및 예측된 활동 백분위수 및 상위 3개의 기여 하위 레벨 카테고리를 봅니다. • **캘린더** 아이콘을 클릭하여 날짜 범위를 지정합니다. 

학습된 피어 그룹 (V2.2.0 이상)	사용자가 속한 것으로 예상했던 유추된 피어 그룹에서 벗어난 정도를 표시합니다. 학습된 피어 그룹은 사용자에 대한 하위 레벨 활동 카테고리별로 유추됩니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다.**피어 그룹에서의 편차**는 사용자가 유추한 피어 그룹에서 벗어난 백분율을 나타냅니다. **신뢰도**는 모델 빌드의 기반이 된 히스토리 데이터의 컨텍스트에서 편차의 백분위수입니다. 편차 및 신뢰도 모두 임계값을 초과하면 경보가 트리거됩니다. 학습된 피어 그룹 그래프에서 다음을 수행할 수 있습니다. • 데이터 점을 클릭하여 그룹의 피어 테이블을 봅니다. • **캘린더** 아이콘을 클릭하여 날짜 범위를 지정합니다. 그룹의 피어 테이블은 예상된 사용자 및 실제로 그룹에 있는 모든 사용자를 보여줍니다. 다음을 수행할 수 있습니다. • 사용자 이름을 클릭하여 사용자 세부사항 페이지를 엽니다. • **예상 일치**는 분석에서 해당 사용자가 그룹에 있음을 신뢰하는 정도를 표시합니다. • 드롭 다운 목록을 클릭하여 표시할 사용자 속성을 선택합니다. • 사용자 이름을 필터링할 검색을 수행합니다. 

정의된 피어 그룹 (V2.6.0 이상)	사용자의 이벤트 활동이 정의된 피어 그룹의 이벤트 활동에서 벗어난 정도를 표시합니다. 분석에서는 사용자 이벤트의 하위 레벨 활동 카테고리를 사용하여 정의된 피어 그룹의 사용자 편차를 판별합니다. 빨간색 원은 기계 학습에서 비정상 항목을 발견했으며 감지 이벤트가 생성되었음을 표시합니다.**피어 그룹에서의 편차**는 사용자가 정의한 피어 그룹에서 벗어난 백분율을 나타냅니다. **신뢰도**는 모델 빌드의 기반이 된 히스토리 데이터의 컨텍스트에서 편차의 백분위수입니다. 편차 및 신뢰도 모두 임계값을 초과하면 경보가 트리거됩니다. 정의된 피어 그룹 분석을 보려면 사용자 그룹을 정의해야 합니다. 추가 정보는 『정의된 피어 그룹 분석을 위한 사용자 그룹』의 내용을 참조하십시오. 정의된 피어 그룹 그래프에서 다음을 수행할 수 있습니다. • 데이터 점을 클릭하여 "정의된 피어 그룹"의 피어 테이블을 봅니다. • **캘린더** 아이콘을 클릭하여 날짜 범위를 지정합니다. "정의된 피어 그룹"의 피어 테이블은 현재 사용자 그룹에서 가장 위험한 사용자를 표시합니다. 다음을 수행할 수 있습니다. • 사용자 이름을 클릭하여 사용자 세부사항 페이지를 엽니다. • 드롭 다운 목록을 클릭하여 표시할 사용자 속성을 선택합니다. • 사용자 이름을 필터링할 검색을 수행합니다. 

정의된 피어 그룹 분석을 위한 사용자 그룹

UBA가 그룹별 선택 중 하나를 사용하여 최소 다섯 명의 사용자가 있는 둘 이상의 그룹이 포함된 참조 테이블을 사용하도록 구성된 경우 Machine Learning 앱에서 정의된 피어 그룹 분석을 사용할 수 있습니다.

참고: V2.6.0 이상에서 UBA의 사용자 그룹을 추출하고 정의된 피어 그룹 분석을 사용할 수 있습니다.

그룹 선택사항은 **직위**, **부서** 또는 UBA 설정 페이지의 속성 표시 아래 **사용자 정의 그룹** 필드에 정의한 사용자 정의 특성입니다. UBA가 각각 다섯 명 이상의 사용자가 있는 셋 이상의 개별 그룹을 발견하면 정의된 피어 그룹 분석을 사용할 수 있습니다. 올바른 사용자 그룹을 가지려면 사용자 특성(직위, 부서 또는 다른 LDAP 속성 그룹)을 참조 테이블로 추출할 수 있도록 참조 데이터 가져오기 LDAP 앱을 구성할 수 있습니다. 그런 다음 작성한 참조 테이블을 사용하도록 UBA를 구성할 수 있습니다.

정의된 피어 그룹 분석에서는 최대 20개의 그룹을 모니터할 수 있습니다. 구성된 **그룹 기준** 필드에서 최대 20개의 그룹이 선택됩니다. 모니터할 사용자의 수는 각 그룹에서 Machine Learning 설치 크기에 대해 모니터되는 사용자 한계를 지키도록 조금씩 줄입니다.

알아두기: 참조 테이블 가져오기에는 UBA 설정 페이지에 구성된 대로 2시간의 최소 반복 스케줄이 있습니다. 가져오기를 실행하도록 스케줄한 경우 새 사용자 그룹 속성을 모두 가져옵니다.

Machine Learning Analytics 앱 설치 제거

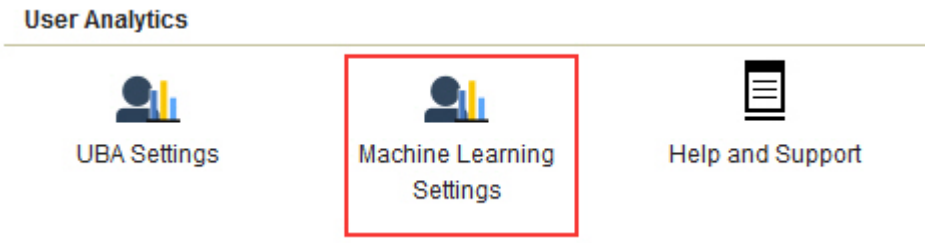
Machine Learning 설정 페이지에서 Machine Learning Analytics 앱을 설치 제거하십시오.

이 태스크 정보

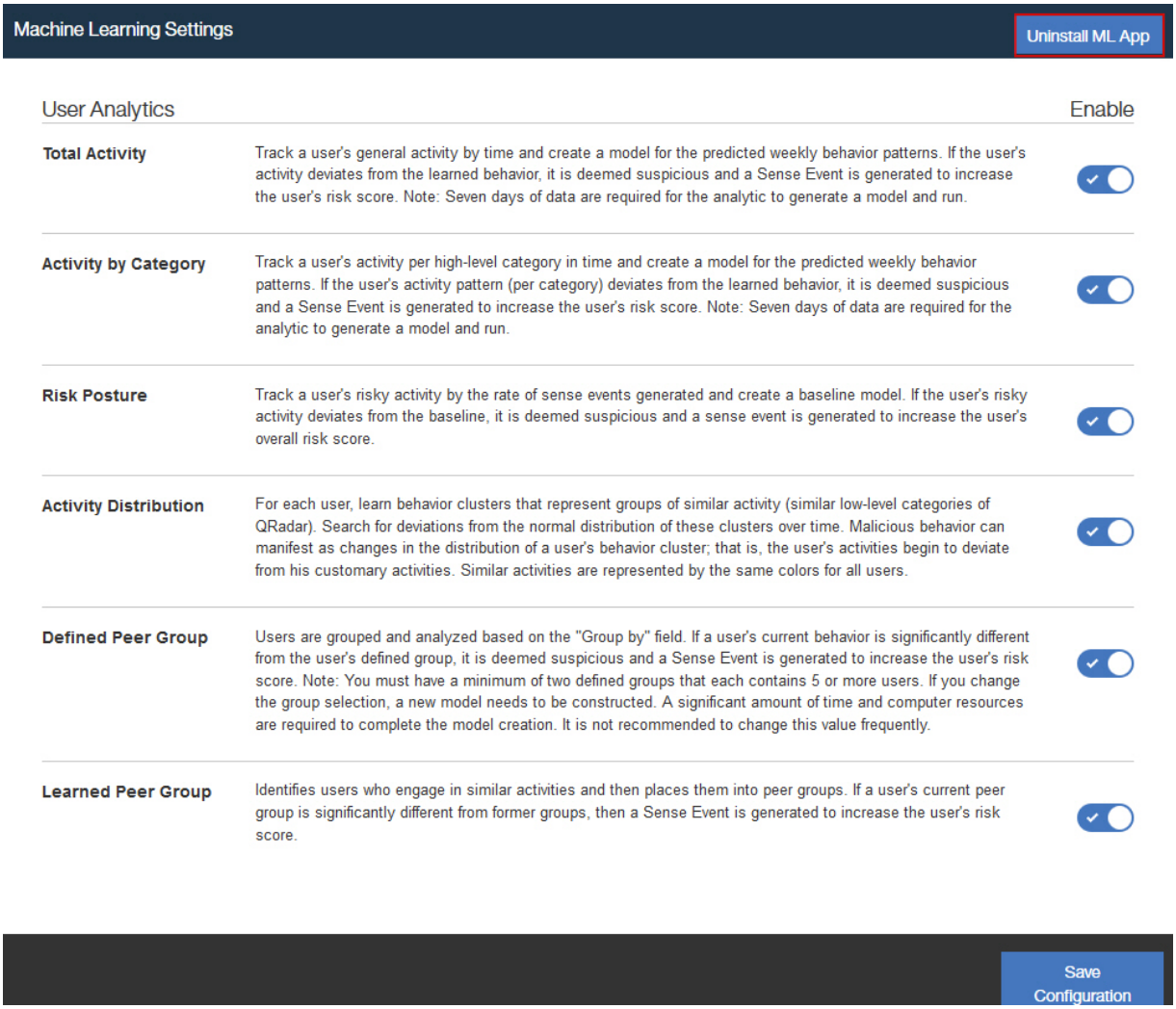
UBA 앱을 설치 제거하기 전에 ML 앱을 설치 제거하기 위한 다음 프로시저를 완료해야 합니다. UBA를 설치 제거하기 전에 ML 앱을 설치 제거하지 않은 경우에는 대화식 API 문서 인터페이스에서 ML 앱을 제거해야 합니다.

프로시저

1. **관리** 설정을 여십시오.
   - IBM QRadar V7.3.0 이하에서는 **관리** 탭을 클릭하십시오.
   - IBM QRadar V7.3.1이상에서는 탐색 메뉴(☰)를 클릭한 후 **관리**를 클릭하여 관리 탭을 여십시오.
2. **Machine Learning 설정** 아이콘을 클릭하십시오.
   - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.
   - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **Machine Learning 설정**을 클릭하십시오.



3. Machine Learning 설정 화면에서 **ML 앱 설치 제거**를 클릭하십시오.



4. 설치 제거 프롬프트에서 **예**를 클릭하십시오.

다음에 수행할 작업

QRadar Console에 다시 로그인하기 전에 브라우저 캐시를 지워야 합니다.

10 문제점 해결 및 지원

IBM 제품에 대한 문제점을 구분하고 해결하기 위해 문제점 해결 및 지원 정보를 사용할 수 있습니다.

User Behavior Analytics 앱 및 Machine Learning Analytics 앱에 관한 공통 지원 질문에 대한 응답은 https://developer.ibm.com/answers/topics/uba/의 내용을 참조하십시오.

UBA에 대한 도움말 및 지원 페이지

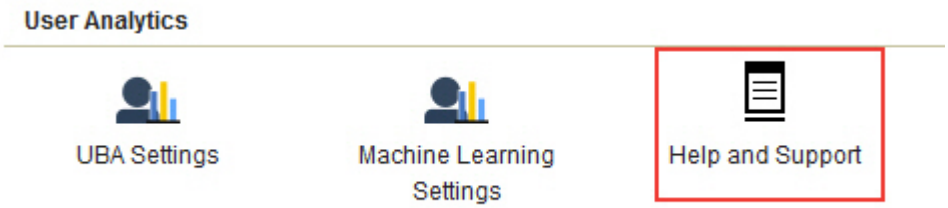
UBA 앱(V2.5.0)에는 UBA 앱, LDAP 앱 및 Machine Learning Analytics 앱 사용을 위한 도움말 및 지원 섹션이 있습니다.

UBA의 도움말 및 지원 페이지 액세스

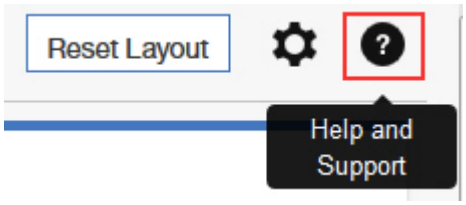
도움말 및 지원 페이지에서는 문서, 문제점 해결 및 지원, 비디오 학습서, 로그 파일 및 관리 기능에 대한 링크를 제공합니다. 도움말 및 지원 페이지에서 로그 파일을 보고 관리 기능을 완료하려면 QRadar® 관리자 권한이 있어야 합니다.

UBA 앱을 설치하면 다음 위치에서 도움말 및 지원 페이지에 액세스할 수 있습니다.

- **관리** 설정에서 다음을 수행하십시오.
  - QRadar V7.3.0 또는 이전 버전에서는 **플러그인** > **사용자 분석** > **도움말 및 지원**을 클릭하십시오.
  - QRadar 7.3.1 이상 버전에서는 **앱** > **사용자 분석** > **도움말 및 지원**을 클릭하십시오.



- **사용자 분석** 탭에서 **도움말 및 지원** 아이콘을 클릭하십시오.



관리 기능

로그 파일을 보고 관리 기능을 완료하려면 QRadar® 관리자 권한이 있어야 합니다.

관리 기능에는 다음 조치를 완료하는 기능이 포함되어 있습니다.

- **UBA 데이터 지우기**를 클릭하면 모든 UBA 사용자 데이터를 제거하지만 현재 UBA 구성 설정은 모두 그대로 유지합니다. UBA 데이터를 지우면 UBA 앱이 **UBA 설정**이 설치되고 구성된 것처럼 작동합니다. Machine Learning 앱이 설치된 경우에는 **UBA 데이터 지우기** 단추를 사용하여 ML 앱을 재설정할 수도 있습니다.
- Machine Learning 앱이 설치되어 있고 모든 Machine Learning 설정을 재설정하고 사용으로 설정된 모든 분석을 사용 안함으로 설정하려면 **ML 설정 재설정**을 클릭하십시오.

서비스 요청

서비스 요청은 PMR(Problem Management Record)이라고도 합니다.

IBM Software Technical Support에 진단 정보를 제출하는 방법에는 여러 가지가 있습니다. 서비스 요청을 열거나 기술 지원과 정보를 교환하려면 IBM Software Support Exchanging information with Technical Support 페이지(http://www.ibm.com/software/support/exchangeinfo.html)를 참조하십시오. 서비스 요청(PMR) 도구(http://www.ibm.com/support/entry/portal/Open_service_request)를 사용하여 서비스 요청을 직접 제출할 수도 있습니다.

대시보드에서 Machine Learning 앱 상태가 경고를 표시함

UBA 대시보드에서 Machine Learning 모델의 상태가 경고 메시지를 표시하는 경우 프로시저를 검토하여 문제를 해결하십시오.

Machine Learning 모델 상태에서 분석에 대해 **모델을 빌드하지 못함**이 표시되면 문제를 해결하기 위해 다음을 수행하십시오.

- ML 앱에 대한 오류 로그를 참조하십시오.
- Machine Learning 앱을 실행 중인 시스템에서 디스크 공간을 확인하십시오.
- UBA 앱에 이벤트가 있는 사용자가 있는지 확인하십시오.
- IBM 고객 지원 부서에 문의하십시오.

관련 개념:

236 페이지의 『UBA 및 Machine Learning 로그 추출』
UBA 및 Machine Learning 로그 파일을 사용하여 문제를 해결할 수 있습니다.

Machine Learning 앱 상태에서 데이터 수집에 대한 진행상태를 표시하지 않음

UBA 대시보드에서 Machine Learning 모델의 상태가 데이터 수집 단계 중에 중지된 것으로 표시하는 경우 프로시저를 검토하여 문제를 해결하십시오.

Machine Learning 모델의 상태가 분석에 대해 데이터 수집에 대한 진행상태를 표시하지 않는 경우 문제를 해결하기 위해 다음을 수행하십시오.

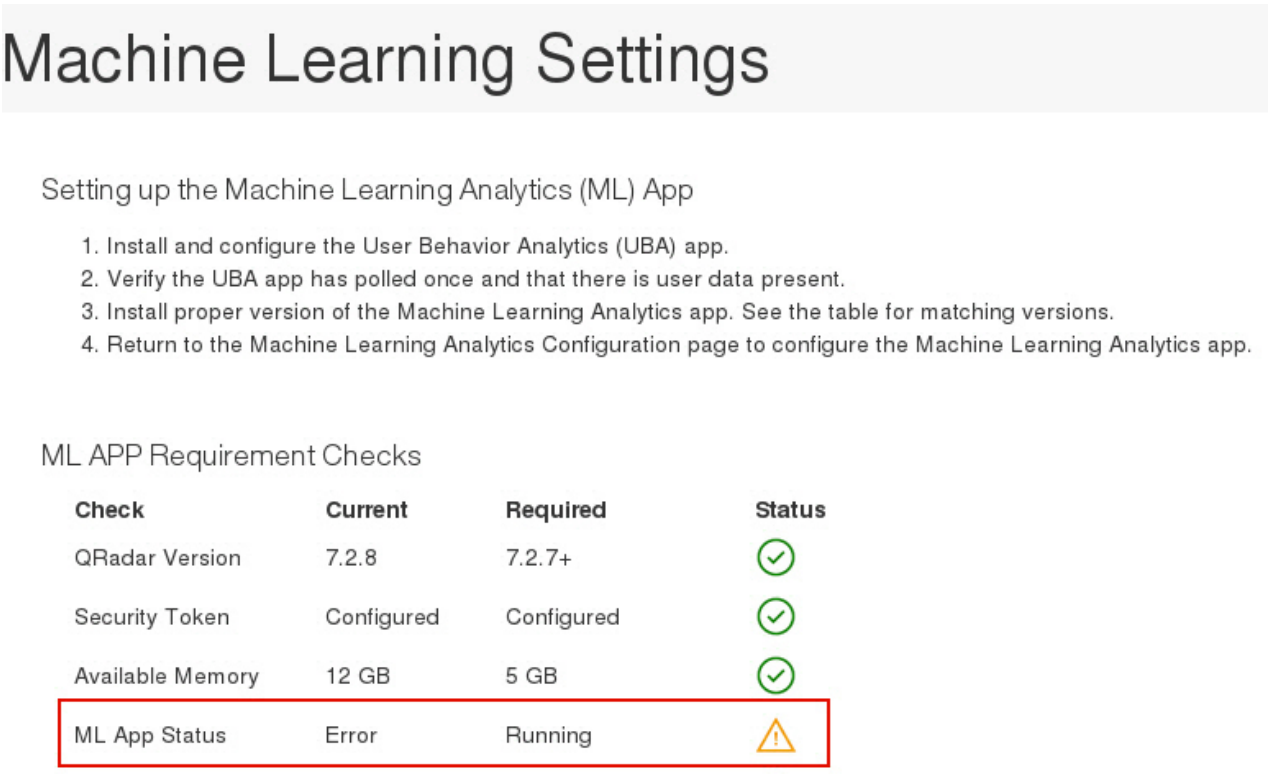
- Ariel Server Service를 다시 시작하십시오.
- Machine Learning 앱을 실행 중인 시스템에서 디스크 공간을 확인하십시오.
- **UBAController** 프로세스가 실행 중인지 확인하려면 ML 컨테이너 내부를 검사하십시오.
- IBM 고객 지원 부서에 문의하십시오.

ML 앱 상태가 오류 상태임

Machine Learning Analytics(ML) 앱이 설치에 실패하고 Machine Learning 설정이 오류 상태를 표시하는 경우, **cURL** 명령행 도구 및 API 문서 설정을 사용하여 ML 앱을 설치 제거할 수 있습니다.

프로시저

Machine Learning 설정 페이지의 ML 앱 상태에서 오류를 표시하는 경우 실패한 앱을 설치 제거하는 프로시저를 완료하십시오.



참고: 올바른 인증 토큰이 있어야 합니다. QRadar Console의 관리 설정에 있는 권한 서비스 섹션에서 구성된 인증 토큰의 목록을 볼 수 있습니다.

1. SSH를 사용하여 QRadar Console에 로그인하십시오.
2. 다음 명령을 실행하십시오.

   # psql -U qradar -c 'select id,name,status from installed_application'

   출력 예제:

```
 id  |  name  |  status
-----+--------------------------------+---------
1356 | User Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. 명령 출력에서 Machine Learning Analytics의 *id* 값을 찾아 기록하십시오.
4. *<valid token>* 대신 올바른 인증 토큰을 사용하고 *<id>* 대신 기록된 ID 값을 사용해서 다음 명령을 실행하여 실패한 Machine Learning 앱을 설치 제거하십시오. **# curl -X DELETE -k -H 'SEC:<valid token>' https://127.0.0.1/api/gui_app_framework/applications/<id>**

Machine Learning 앱 제거

gui_app_framework API를 사용하여 Machine Learning 앱을 제거하려면 다음 단계를 완료하십시오.

1. QRadar Console을 열고 다음 위치에서 API 문서 페이지를 탐색하십시오.
   https://*<host_address_port>*/api_doc
2. 가장 높은 API 버전 번호의 폴더를 여십시오(번호는 QRadar 버전에 따라 다름(예: QR 7.2.8의 경우 7.0)).
3. `/gui_app_framework` 폴더를 연 다음 `/applications`를 선택하십시오.
4. 이때 사용자는 **GET API**에 있어야 합니다. **"체험해 보기"** 단추를 클릭하여 설치된 애플리케이션 목록을 가져오십시오.
5. 4단계의 결과에서 `Machine Learning Analytics`를 검색하고 `application_id` 속성 값을 가져오십시오.
6. API 문서(3단계와 동일한 위치)에서 `/applications` 메뉴를 펼치고 `/application_id` API를 선택한 후 **삭제** 탭을 클릭하십시오.
7. 5단계의 애플리케이션 ID 값을 입력한 다음 **"체험해 보기"** 단추를 클릭하여 애플리케이션을 제거하십시오.
8. API에서 애플리케이션이 제거되었음을 나타내는 HTTP 204 상태 코드를 리턴해야 합니다.

UBA 및 Machine Learning 로그 추출

UBA 및 Machine Learning 로그 파일을 사용하여 문제를 해결할 수 있습니다.

앱 로그 파일 다운로드

233 페이지의 『UBA에 대한 도움말 및 지원 페이지』에서 UBA 앱 및 Machine Learning 앱의 로그 파일을 쉽게 다운로드할 수 있습니다.

UBA 앱 로그 파일

docker 컨테이너에서 UBA 앱 로그 파일을 수동으로 추출하려면 다음 단계를 따르십시오.

1. UBA를 실행 중인 QRadar 호스트에서 앱의 모든 로그 파일을 포함하는 zip 파일을 작성하기에 충분한 공간이 있는 디렉토리로 이동하십시오.
2. 다음 명령을 실행하십시오.

   find /store/docker/v* -name uba.db
3. `uba.db` 앞에 있는 디렉토리 경로를 복사하십시오.

   예를 들어, 디렉토리 경로는 다음과 같습니다.
   /store/docker/volumes/qapp-1001/uba.db
   여기에서 다음을 복사하십시오.
   /store/docker/volumes/qapp-1001/
4. 1단계의 디렉토리 경로를 대체하는 다음 명령을 실행하십시오.

   zip -qr uba_logs.zip <your_path_here>log*

   예를 들어, 다음과 같습니다. **zip -qr uba_logs.zip /store/docker/volumes/qapp-1001/log***

Machine Learning 앱 로그 파일

docker 컨테이너에서 Machine Learning 앱 로그 파일을 수동으로 추출하려면 다음 단계를 따르십시오.

1. UBA를 실행 중인 QRadar 호스트에서 앱의 모든 로그 파일을 포함하는 zip 파일을 작성하기에 충분한 공간이 있는 디렉토리로 이동하십시오.
2. 다음 명령을 실행하십시오.

   find /store/docker/v* -name itproot
3. `itproot` 앞에 있는 디렉토리 경로를 복사하십시오.

   예를 들어, 디렉토리 경로는 다음과 같습니다.
   /store/docker/volumes/qapp-1003/itproot
   여기에서 다음을 복사하십시오.
   /store/docker/volumes/qapp-1003/
4. 1단계의 디렉토리 경로를 대체하는 다음 명령을 실행하십시오.

   zip -qr ml_logs.zip <your_path_here>log*

예를 들어, 다음과 같습니다. **zip -qr ml_logs.zip /store/docker/volumes/qapp-1003/log***

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

2바이트 문자 세트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

인용된 성능 데이터와 고객 예제는 예시 용도로만 제공됩니다. 실제 성능 결과는 특정 구성과 운영 조건에 따라 다를 수 있습니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

상표

IBM, IBM 로고 및 ibm.com®은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Adobe, Adobe 로고, PostScript 및 PostScript 로고는 미국 또는 기타 국가에서 사용되는 Adobe Systems Incorporated의 등록상표 또는 상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

Java™ 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

제품 문서의 이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용성

본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 개인적, 비상업적 용도로 복제할 수 있습니다. 귀하는 IBM의 명시적 동의 없이 본 발행물 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 귀하 기업집단 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하는 귀하의 기업집단 외에서는 IBM의 명시적 동의 없이 이 책의 2차적 저작물을 만들거나 이 책 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

권한

본 허가에서 명시적으로 부여된 경우를 제외하고, 이 책이나 이 책에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대한 어떠한 허가나 라이센스 또는 권한도 명시적 또는 묵시적으로 부여되지 않습니다.

IBM은 이 책의 사용이 IBM의 이익을 해친다고 판단하거나 위에서 언급된 지시사항이 준수되지 않는다고 판단하는 경우 언제든지 부여한 허가를 철회할 수 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하는 경우에만 본 정보를 다운로드, 송신 또는 재송신할 수 있습니다.

IBM은 이 책의 내용과 관련하여 아무런 보장을 하지 않습니다. 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 현 상태대로 제공합니다.

IBM 온라인 개인정보처리방침

SaaS(Software as a Service) 솔루션을 포함한 IBM 소프트웨어 제품(이하 "소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 일반 사용자의 사용 경험을 개선하거나 일반 사용자와의 상호 작용을 조정하거나 그 외의 용도로 쿠키나 기타 다른 기술을 사용할 수 있습니다. 많은 경우에 있어서, 소프트웨어 오퍼링은 개인 식별 정보를 수집하지 않습니다. IBM의 일부 소프트웨어 오퍼링은 귀하가 개인 식별 정보를 수집하도록 도울 수 있습니다. 본 소프트웨어 오퍼링이 쿠키를 사용하여 개인 식별 정보를 수집할 경우, 본 오퍼링의 쿠키 사용에 대한 특정 정보가 다음에 규정되어 있습니다.

본 소프트웨어 오퍼링은 배치된 구성에 따라 세션 관리 및 인증의 용도로 각 사용자의 세션 ID를 수집하는 세션 쿠키를 사용할 수 있습니다. 쿠키를 사용하지 못하도록 할 수 있지만 이 경우 쿠키를 통해 사용 가능한 기능도 제거됩니다.

본 소프트웨어 오퍼링에 배치된 구성이 쿠키 및 기타 기술을 통해 최종 사용자의 개인 식별 정보 수집 기능을 고객인 귀하에게 제공하는 경우, 귀하는 통지와 동의를 위한 요건을 포함하여 이러한 정보 수집과 관련된 법률 자문을 스스로 구해야 합니다.

이러한 목적의 쿠키를 포함한 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인정보처리방침(http://www.ibm.com/privacy/kr/ko/), IBM 온라인 개인정보처리방침(http://www.ibm.com/privacy/details/kr/ko/) "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a-Service) 개인정보처리방침"(http://www.ibm.com/software/info/product-privacy) 부분을 참조하십시오.

일반 개인정보 보호법률(General Data Protection Regulation)

고객은 유럽 연합 일반 개인정보 보호법률(General Data Protection Regulation)을 포함한 다양한 법령과 규정을 준수해야 할 책임이 있습니다. 고객은 고객의 비즈니스에 영향을 줄 수 있는 관련 법령 및 규정에 대한 확인과 해석, 그러한 법령 및 규정의 준수를 위해 필요한 고객의 모든 조치와 관련하여 적절한 법률 자문을 받아야 할 단독 책임이 있습니다. 여기에서 설명하는 제품, 서비스 및 기타 기능은 일부 고객의 상황에는 해당되지 않을 수 있으며 그 가용성이 제한될 수 있습니다. IBM은 법률, 회계 또는 감사와 관련한 조언을 제공하지 않으며 서비스 또는 제품이 고객의 법률 또는 규정 준수를 보장한다는 어떠한 표현이나 보증도 하지 않습니다.

IBM의 GDPR 준비 과정 및 GDPR 기능과 오퍼링에 대한 자세한 정보는 다음 정보를 참조하십시오. https://ibm.com/gdpr.