IBM Security QRadar Incident Forensics
Version 7.3.0

Benutzerhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen unter „Bemerkungen" auf Seite 45 lesen.

Produktinformation

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.3.0 und nachfolgende Releases, bis es durch eine aktualisierte Version dieses Dokuments ersetzt wird.

Inhaltsverzeichnis

Einführung in IBM Security QRadar Incident Forensics

Dieses Handbuch enthält Informationen zur Untersuchung von Sicherheitsverstößen mithilfe von IBM® Security QRadar Incident Forensics.

Zielgruppe

Prüfer extrahieren Informationen aus dem Netzverkehr und den Dokumenten im Repository 'Forensics'. Diese Informationen werden bei der Untersuchung von Sicherheitsverstößen verwendet.

Technische Dokumentation

Wenn Sie im Web nach der Produktdokumentation zu IBM Security QRadar einschließlich der gesamten übersetzten Dokumentation suchen möchten, rufen Sie das IBM Knowledge Center auf (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Informationen zum Zugriff auf weitere technische Dokumentationen in der QRadar-Produktbibliothek finden Sie unter Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Kontaktierung der Kundenunterstützung

Informationen zur Kontaktierung der Kundenunterstützung finden Sie im Dokument Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden gesetzlichen Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

Bitte beachten:

Bei der Nutzung dieses Programms muss ggf. eine Reihe von Gesetzen und Bestimmungen beachtet werden, einschließlich solcher, die sich auf den Datenschutz, die Datensicherheit, arbeitsrechtliche Angelegenheiten sowie die elektronische

Kommunikation und die Speicherung beziehen. IBM Security QRadar darf nur für rechtmäßige Zwecke und auf rechtmäßige Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer erklärt, dass er die Zustimmung, Berechtigungen oder Lizenzen einholt bzw. einholen wird, die für die rechtmäßige Verwendung von IBM Security QRadar erforderlich sind.

Hinweis

IBM Security QRadar Incident Forensics soll Unternehmen dabei helfen, ihre Sicherheitsumgebung und Sicherheitsdaten zu verbessern. Insbesondere soll IBM Security QRadar Incident Forensics Unternehmen dabei unterstützen, die Vorgänge bei Sicherheitsverstößen im Netz zu untersuchen und besser zu verstehen. Mit dem Tool können Unternehmen einen Index für erfasste Netzpaketdaten (PCAPs) erstellen und diese durchsuchen und es enthält eine Funktion, mit dem diese Daten im ursprünglichen Format wiederhergestellt werden können. Mit dieser Wiederherstellungsfunktion können Daten und Dateien einschließlich E-Mail-Nachrichten, Anhänge von Dateien und Bildern, VoIP-Anrufe und Websites wiederhergestellt werden. Weitere Informationen zu den Funktionen des Programms und der Vorgehensweise bei der Konfiguration der Funktionen finden Sie in den Handbüchern und in der weiteren Dokumentation, die dem Programm beigefügt wurde. Die Verwendung dieses Programms kann verschiedene Gesetze oder Regelungen einschließen. Diese können sich auf die Geheimhaltung, den Datenschutz, die Benutzung und elektronische Kommunikation sowie auf die Speicherung beziehen. IBM Security QRadar Incident Forensics darf nur für gesetzlich zulässige Zwecke und in einer gesetzmäßigen Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden, und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer versichert, dass er alle Zustimmungen, Genehmigungen oder Lizenzen einholen wird oder eingeholt hat, die für eine rechtmäßige Nutzung von IBM Security QRadar Incident Forensics erforderlich sind.

Kapitel 1. Neuerungen für Benutzer in QRadar Incident Forensics V7.3.0

In IBM Security QRadar Incident Forensics V7.3.0 ist jetzt eine Packet Capture-Einheitenauswahl (PCAP) für Benutzer verfügbar, die eine Wiederherstellung ausführen.

PCAP-Einheitenauswahl für eine QRadar Incident Forensics-Wiederherstellung verfügbar

Wenn Sie bei der Ausführung einer QRadar Incident Forensics-Wiederherstellung nur den Datenverkehr aus den PCAP-Einheiten in Ihrer Implementierung sehen möchten, wählen Sie eine Einheit unter **Custom Capture Device** (Angepasste Aufzeichnungseinheit) aus.

 Weitere Informationen zur PCAP-Einheitenauswahl...

Kapitel 2. Sicherheitsuntersuchungen

Mit IBM Security QRadar Incident Forensics können Sie neu entstehende Bedrohungen erkennen, die zugrunde liegende Ursache ermitteln und Wiederholungen verhindern. Mithilfe von Forensiktools können Sie schnell analysieren, von wem die Bedrohung ausgegangen ist, wie er vorgegangen ist und welche Ziele angegriffen wurden.

Als Forensikprüfer können Sie die Aktionen von Cyberkriminellen Schritt für Schritt zurückverfolgen und die von einem Sicherheitsverstoß betroffenen Netzdaten in ihrer ursprünglichen Form wiederherstellen.

Sobald Ihr Unternehmen auf eine Bedrohung, ein potenzielles Sicherheitsrisiko oder einen Compliance-Verstoß aufmerksam wird, legen Sie Ziele zur Bewertung des Umfangs fest, ermitteln die betroffenen Entitäten und finden die Motivation heraus.

Sie können die Tools von IBM Security QRadar Incident Forensics in bestimmten Szenarios bei unterschiedlichen Untersuchungen einsetzen, z. B. in den Bereichen Netzsicherheit, Insideranalyse, Betrug und Missbrauch sowie Sammeln von Beweisen.

1. Stellen Sie Netzsitzungen zu und von einer IP-Adresse wieder her.
2. Sie können aus Vorfällen, die erstellt werden, Attributkategorien abfragen, um Beweise zu sammeln.

   Wenn eine Wiederherstellung stattfindet, wird ein Vorfall erstellt.
3. Verwenden Sie Suchfilter, um nur die Informationen abzurufen, die Sie interessieren.
4. Wählen Sie abhängig vom Typ der Untersuchung das Forensiktool aus, das Ihnen die benötigten Beweise liefert.

Verdächtige Inhalte

Über die Suchfunktion können Sie nach kontextbezogenen Elementen oder IDs suchen, die Ihnen über den Angreifer oder Vorfall bekannt sind. Wenn Sie das Schlüsselwort in der Suche verwenden, werden verdächtige Inhalte zurückgegeben. Einige der verdächtigen Inhalte können für die Untersuchung relevant sein.

Pivotieren von Daten

Durch das Pivotieren von Daten wird erreicht, dass die Inhalte eines Suchergebnisses als Hot Links dargestellt werden. Wenn Sie beispielsweise nach `"Tom"` suchen, kann das Ergebnis die von Tom geschriebenen E-Mails, seine Chats und weitere Kontextinformationen enthalten. Wenn Sie nun auf eine E-Mail klicken, um sie anzuzeigen, werden alle Assets oder Entitäten (z. B. Anhänge oder von Tom verwendete Computer-IDs) als Links dargestellt. Mithilfe dieser Links kann ein Prüfer seine Untersuchung schneller durchführen.

Digitale Spur

Nutzen Sie digitale Spuren, um die gewonnenen Daten zu durchsuchen und die Beziehungen zwischen Entitäten wie IP-Adressen, Namen und MAC-Adressen abhängig von ihrer Häufigkeit zuzuordnen. Sie können ein Ergebnis oder mehrere Er-

gebnisse auswählen, um die Häufigkeit und Richtung der Beziehungen anzuzeigen.

Surveyor

Mit dem Tool Surveyor können Sie Aktivitäten auf einer Zeitachse betrachten, um eine Attacke zurückzuverfolgen. Surveyor stellt die Sitzung wieder her und sortiert die Dokumente in zeitlicher Reihenfolge.

Inhaltsfilterung

Inhaltsfilter ermöglichen die Suche nach einer Untergruppe von Inhaltskategorien wie WebMail und Pornografie, um das Datenrauschen oder irrelevante Inhalte bei der Suche auszuschließen.

Untersuchungen zur Netzsicherheit

Sie können QRadar Incident Forensics verwenden, um zerstörerische Aktivitäten, die sich gegen kritische Assets richten, zu erkennen und zu untersuchen. Mithilfe der integrierten Forensiktools können Sie einen Netzsicherheitsverstoß korrigieren und verhindern, dass er sich wiederholt.

Verwenden Sie die Untersuchungswerkzeuge von QRadar Incident Forensics, um herauszufinden, wie das Ereignis zustande kam, und um seine Auswirkung auf ein Minimum zu reduzieren, und tun Sie alles, was möglich ist, um weitere Verstöße zu verhindern.

Patient Null: Quelle einer Attacke ermitteln

In diesem Szenario wird ein Unternehmen über einen verdächtigen Sicherheitsverstoß informiert. Es versucht, den Ausgangspunkt der Attacke zu finden, um die Quelle zu isolieren. Das Unternehmen muss die kompromittierten Entitäten in einen isolierten Bereich verlagern (Quarantäne), um eine Ausbreitung der Attacke auf andere Teile des Unternehmens zu verhindern.

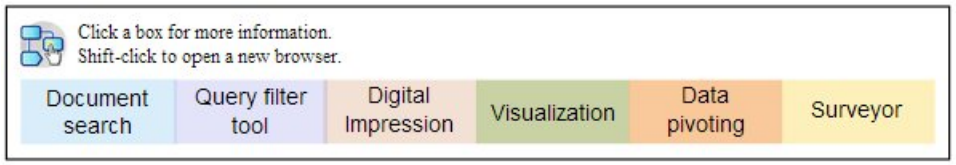
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Bestimmung des Typs der Attacke
- Ermittlung des ursprünglichen Eingangspunkts der Bedrohung
- Beschaffung von Details zu den zerstörerischen Nutzdaten
- Ermittlung, wie die zerstörerischen Nutzdaten hinter dem Eingangspunkt verbreitet wurden

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach symptomatischen Attributen in Verbindung mit zerstörerischen Nutzdaten zu suchen.
2. Verwenden Sie Inhaltskategorien, um Inhalte herauszufiltern, die für die Untersuchung nicht relevant sind.
3. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
4. Nutzen Sie digitale Spuren und Visualisierungen, um erweiterte Beziehungen der zerstörerischen Nutzdaten, des Täters oder des Ziels zu untersuchen.
5. Arbeiten Sie mit dem Pivotieren von Daten und folgen Sie den Datenverknüpfungen, um Patient Null zu ermitteln.
6. Betrachten Sie mithilfe von Surveyor die Aktivitäten auf einer Zeitachse, um eine Attacke zurückverfolgen zu können.

Kompromittierte Systeme

In diesem Szenario wird ein Unternehmen darüber informiert, dass ein oder mehrere seiner Systeme durch eine professionelle Cyberangriffstechnik wie Wasserloch-Attacke, Phishing, Brute-Force-Attacke oder SQL-Injection kompromittiert wurden.

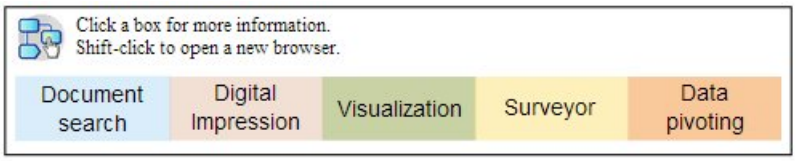
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Feststellung der Ausdehnung der Kompromittierung innerhalb des Unternehmens
- Ermittlung des Typs des operationellen Risikos der Kompromittierung für jedes einzelne System
- Aufdeckung aller peripheren Aktionen, die bei der ursprünglichen Attacke ausgeführt wurden, um Bereinigungsaktivitäten zu umgehen und eine Erkennung zu vermeiden

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach zerstörerischen Nutzdaten oder einem kompromittierten Asset zu suchen.
2. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
3. Nutzen Sie digitale Spuren und Visualisierungen, um Entitätsbeziehungen zu untersuchen, die das Ergebnis kompromittierter Systeme sind.
4. Betrachten Sie mithilfe von Surveyor die Aktivitäten auf einer Zeitachse, um eine Attacke zurückverfolgen zu können.
5. Spüren Sie mithilfe der freien Suche, durch Pivotieren von Daten und anhand verdächtiger Inhalte Inkonsistenzen oder verdächtige Interaktionen über Datenkategorien hinweg auf.

Daten sind an nicht berechtigte Entitäten abgeflossen

In diesem Szenario wird ein Unternehmen darüber informiert, dass vertrauliche Daten an nicht berechtigte Entitäten innerhalb des Unternehmens oder an externe Parteien abgeflossen sind.

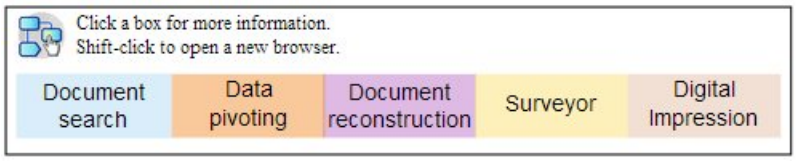
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Bestimmung der Art und der Menge der abgeflossenen Daten
- Feststellung der eingesetzten Verfahren
- Ermittlung des Täters
- Ermittlung der Quelle des Lecks

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach IDs von abgeflossenen Daten zu suchen.
2. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
3. Prüfen Sie den vollen Umfang abgeflossener oder abfließender Daten anhand einer Überprüfung der Datenwiederherstellung.
4. Nutzen Sie digitale Spuren und Visualisierungen, um alle involvierten Entitätsbeziehungen zu untersuchen.
5. Betrachten Sie mithilfe von Surveyor die Aktivitäten auf einer Zeitachse, um eine Attacke zurückverfolgen zu können.
6. Verwenden Sie die freie Suche, um die Motivation für das Datenleck zu erkennen.
7. Versuchen Sie durch das Pivotieren von Daten Verknüpfungen mit weiteren Daten zu finden, die möglicherweise abgeflossen sind.

Untersuchungen zur Insideranalyse

Mithilfe von QRadar Incident Forensics können Sie betrügerische Absprachen, Sabotage und den Missbrauch von Zugriffsberechtigungen erkennen. Sie können den Täter, Kollaborateure, komprimierte Systeme und Dokumentdatenverluste ermitteln.

Missbrauch von Zugriffsberechtigungen

In diesem Szenario wird ein Unternehmen darüber informiert, dass einer oder mehrere seiner Mitarbeiter Berechtigungsnachweise missbrauchen oder als Proxy für den Zugriff auf sensible Systeme und Daten für nicht autorisierte Aktivitäten dienen.

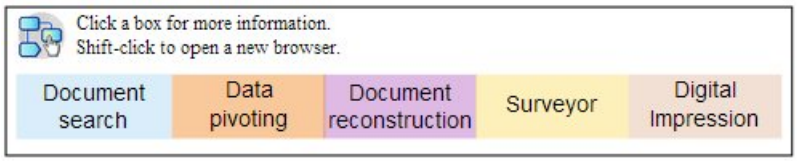
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Ermittlung der Identität des Benutzers
- Feststellung, wer oder was die Identität für nicht autorisierte Aktivitäten einsetzt
- Klärung des Ziels des Missbrauchs von Zugriffsberechtigungen
- Bewertung, ob die Entität weitere Identitäten besitzt, die ebenfalls missbraucht werden könnten

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach Identitäten zu suchen, die auf sensible Systeme oder Daten zugreifen.
2. Stellen Sie fest, welche dieser Zugriffsversuche verdächtig sind, indem Sie mithilfe der freien Suche, durch das Pivotieren von Daten und durch Inhaltsfilterung nach verdächtigen Inhalten suchen.
3. Zeigen Sie die Datenwiederherstellung für die Inhalte an, auf die zugegriffen wird.
4. Verfolgen Sie Zugriffsmuster zurück und bewerten Sie die Häufigkeit in Surveyor.
5. Nutzen Sie digitale Spuren, um die von einer einzelnen Entität verwendeten Aliasnamen aufzudecken.

Betrügerische Absprachen

In diesem Szenario wird ein Unternehmen darüber informiert, dass einer oder mehrere der Stakeholder in betrügerischer Absprache untereinander oder mit externen Parteien handeln, um sich an Aktivitäten zu beteiligen, die für das Unternehmen schädlich sind.

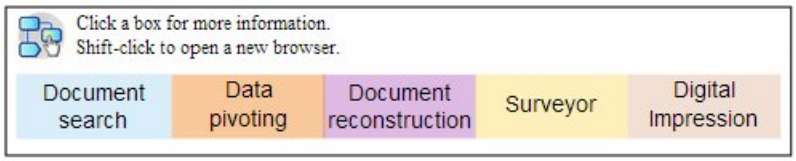
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Ermittlung der in betrügerischer Absprache handelnden Entitäten
- Feststellung der Art und Muster der Interaktionen zwischen den Kollaborateuren
- Aufdeckung der Inhalte, die dem Schema unterliegen
- Feststellung der Dauer des Schemas, um das Ausmaß des Risikos zu erkennen

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach IDs von involvierten Entitäten zu suchen.
2. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
3. Nutzen Sie digitale Spuren, Visualisierungen und Inhaltsfilter, um Beziehungen zu erkennen, die möglicherweise verdächtig sind.
4. Verfolgen Sie mithilfe von Surveyor die Aktivitäten von involvierten Entitäten zurück, um Informationen über die Inhalte der Interaktionen zu erhalten.
5. Ermitteln Sie die Motivation für die betrügerischen Absprachen, indem Sie wiederhergestellte Dokumente überprüfen.
6. Finden Sie mithilfe der freien Suche und durch Pivotieren von Daten heraus, wann die betrügerischen Aktivitäten begonnen haben.

Sabotage

In diesem Szenario wird ein Unternehmen darüber informiert, dass einer oder mehrere der Stakeholder versuchen, den Geschäftsbetrieb zu unterbrechen. Der Stakeholder wird möglicherweise als Proxy genutzt.

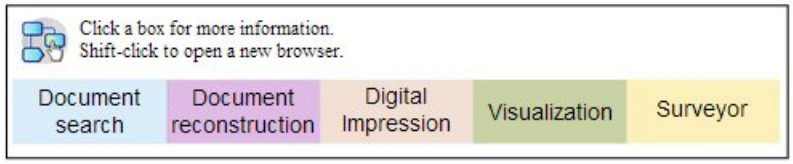
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Ermittlung des Saboteurs
- Feststellung der vom Saboteur eingesetzten Verfahren
- Bewertung der Auswirkung und des Umfangs der Unterbrechung
- Ermittlung der vom Saboteur ausgenutzten Schwachstellen

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach Symptomen der Sabotage zu suchen.
2. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
3. Nutzen Sie visuelle Navigation, digitale Spuren und Inhaltsfilter, um die Symptome zu untersuchen und IDs des Saboteurs zu erkennen.
4. Verfolgen Sie mithilfe von Surveyor die Aktivitäten des Saboteurs zurück.
5. Verwenden Sie die Datenwiederherstellung, um Rollen und Motivation des Saboteurs zu erkennen.
6. Verwenden Sie die Datenwiederherstellung, um die vom Saboteur genutzten Inhalte zu überprüfen.

7. Ermitteln Sie mithilfe der freien Suche, von Surveyor und anhand verdächtiger Inhalte die kompromittierten Systeme und Prozeduren, die die Sabotage ermöglichten.

Untersuchungen zu Betrug und Missbrauch

Verwenden Sie QRadar Incident Forensics, um nicht autorisierte Transaktionen, nicht genehmigte Zuteilungen von Ressourcen, Protokollabweichungen und Umgehungen gesetzlicher Kontrollen ausfindig zu machen.

Nicht autorisierte Transaktionen

In diesem Szenario wird ein Unternehmen darüber informiert, dass nicht autorisierte Transaktionen zu negativen finanziellen Auswirkungen auf Geschäftsoperationen führen.

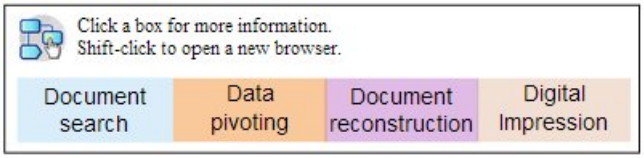
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Lokalisierung der nicht autorisierten Transaktionen
- Ermittlung der Entitäten, die in die nicht autorisierten Transaktionen involviert und dafür verantwortlich sind
- Feststellung der Häufigkeit und der Trends der nicht autorisierten Transaktionen
- Bewertung des Umfangs des Risikos durch die nicht autorisierten Transaktionen

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach inkonsistenten oder verdächtigen Transaktionen zu suchen.
2. Suchen Sie mithilfe der freien Suche und durch das Pivotieren von Daten nach Wiederholungen solcher Transaktionen.
3. Nutzen Sie das Pivotieren von Daten und digitale Spuren, um die Entitäten zu erkennen, die mit den verdächtigen Transaktionen in Verbindung stehen.
4. Decken Sie durch die Überprüfung wiederhergestellter Dokumente die Inhalte der Transaktionen auf, um den quantitativen Wert zu ermitteln.

Nicht genehmigte Zuteilung von Ressourcen

In diesem Szenario hegt ein Unternehmen den Verdacht, dass nicht genehmigte Zuteilungen von Ressourcen zu negativen finanziellen Auswirkungen auf Geschäftsoperationen führen.

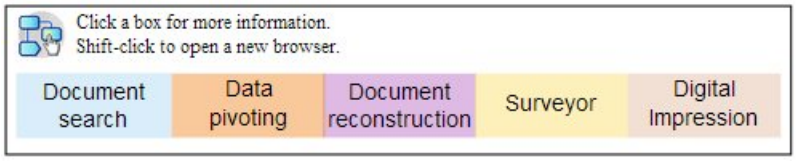
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Lokalisierung der fehlerhaften Zuteilung von Ressourcen
- Ermittlung der Entitäten, die in die fehlerhafte Zuteilung von Ressourcen involviert und dafür verantwortlich sind
- Ermittlung der Motivation für die fehlerhafte Zuteilung von Ressourcen
- Bewertung der Größe und des Umfangs der fehlerhaft zugeteilten Ressourcen

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach Kommunikationsvorgängen zu suchen, die mit zugeteilten Ressourcen in Verbindung stehen.
2. Nutzen Sie die freie Suche, das Pivotieren von Daten und digitale Spuren, um IDs von Entitäten zu finden, die nicht genehmigte Zuteilungen von Ressourcen vornehmen.
3. Verarbeiten Sie die Inhalte der involvierten Interaktionen, um die Motivation zu bewerten, indem Sie wiederhergestellte Dokumente überprüfen und Visualisierungen nutzen.
4. Verfolgen Sie mithilfe von Surveyor Zuordnungsaktivitäten zurück, um die Größe der fehlerhaft zugeteilten Ressourcen festzustellen.

Protokollabweichungen und Umgehung gesetzlicher Kontrollen

In diesem Szenario wird ein Unternehmen darüber informiert, dass Geschäftsprozesse, IT-Protokolle und gesetzliche Kontrollen umgangen wurden, was zu negativen finanziellen Auswirkungen führen kann.

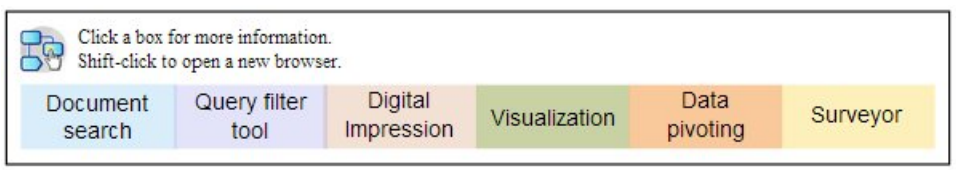
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Bewertung der umgangenen Protokolle oder gesetzlichen Kontrollen
- Ermittlung der Entitäten, die ein solches Verhalten zeigten
- Ermittlung der Motivation dieser Entitäten
- Bewertung der allgemeinen Verbreitung dieses Fehlverhaltens

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach Geschäftsprozessen zu suchen, die durch Protokolle oder Kontrollen reguliert werden.
2. Erstellen Sie mithilfe der freien Suche, durch das Pivotieren von Daten und anhand der Datenwiederherstellung Querverweise auf Dokumentationen, die Erläuterungen der Protokolle und gesetzlichen Kontrollen enthalten.
3. Verwenden Sie Inhaltsfilter und die freie Suche, um bestimmte Instanzen zu erkennen, von denen Protokolle/Kontrollen umgangen wurden.
4. Nutzen Sie digitale Spuren, Visualisierungen und Inhaltsfilter, um die zugehörigen Entitäts-IDs zu finden.
5. Verfolgen Sie mithilfe von Surveyor Entitätsaktivitäten zurück, um die mögliche Motivation zu finden.

Untersuchungen zur Sammlung von Beweisen

Verwenden Sie QRadar Incident Forensics, um das Risiko von Schwachstellen im Unternehmen zu bewerten, die Zuverlässigkeit der Erkennung von Bedrohungen oder Tätern zu quantifizieren und Sicherheitsverfahren zu optimieren.

Zuverlässigkeit bei der Erkennung von Bedrohungen

In diesem Szenario wird ein Unternehmen über eine bestimmte Bedrohung, ein Exploit oder eine Schwachstelle informiert. Um Korrekturmaßnahmen zu rechtfertigen, die sonst normalen Geschäftsoperationen möglicherweise zuvorkommen, soll für jedes zugehörige Risiko ein Konfidenzintervall quantifiziert werden.

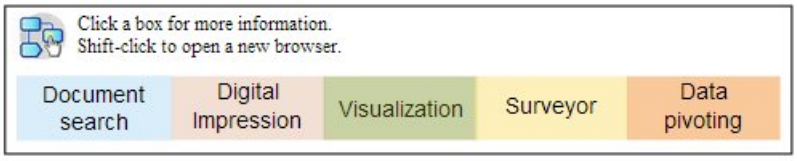
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Prüfung der Anfälligkeit für das Sicherheitsrisiko
- Feststellung, ob es einen Beweis für das Sicherheitsrisiko gibt
- Bewertung der Flexibilität und finanziellen Auswirkung des Sicherheitsrisikos
- Ermittlung der Art des Sicherheitsrisikos

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Suchen Sie mithilfe der freien Suche, anhand verdächtiger Inhalte und durch das Pivotieren von Daten nach der Bedrohung, dem Exploit oder der Schwachstelle, indem Sie Entitäten, die potenzielle Ziele darstellen, als Ausgangspunkte wählen.
2. Verwenden Sie die freie Suche und das Pivotieren von Daten, um Vorkommnisse zu kompilieren.
3. Verwenden Sie die freie Suche und Querverweisdokumente, die Verweise auf die Auswirkung bereitstellen.

4. Nutzen Sie digitale Spuren und Visualisierungen, um die betroffenen Entitäten zu ermitteln.
5. Analysieren Sie mithilfe von Surveyor die Aktivitäten, die mit der Bedrohung oder dem Täter in Verbindung stehen.

Sicherheitsverfahren optimieren

Die Erkennung neuer und riskanter Verhaltensweisen veranlasst ein Unternehmen, die Wirksamkeit bestehender Sicherheitsverfahren zu bewerten. In diesem Szenario möchte ein Unternehmen die Effektivität seiner Sicherheitsregeln in Bezug auf die vorhandenen Risiken quantifizieren.

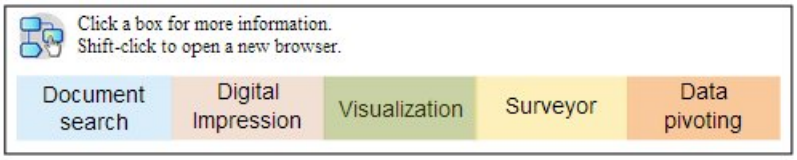
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Erkennung neuer oder riskanter Verhaltensweisen
- Bewertung der Effektivität bestehender Sicherheitsregeln
- Erkennung der durch dynamische Operationen entstehenden Sicherheitslücken
- Bewertung der Effektivität vorgeschlagener Sicherheitsverfahren

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach neuen oder riskanten Verhaltensweisen, z. B. nach mobilen Benutzern und cloudbasierten Services, zu suchen, indem Sie domänen- und unternehmensbezogenes Wissen nutzen.
2. Untersuchen Sie verdächtige Inhalte und erstellen Sie mithilfe von Surveyor Querverweise zwischen diesen Verhaltensweisen und bestehenden Sicherheitsregeln und -verfahren.
3. Analysieren Sie mithilfe von freier Suche, Surveyor, Inhaltswiederherstellung und Visualisierung die Falsch-Positiv-Rate bei Alarmen aufgrund von Sicherheitsregeln.
4. Verwenden Sie freie Suche, Surveyor, Inhaltswiederherstellung, Visualisierung und das Pivotieren von Daten, um Falsch-Negativ-Fälle aufzuspüren, die von bestehenden Sicherheitsregeln und -verfahren nicht erkannt werden.

Risikobewertungen

In diesem Szenario wird ein Unternehmen in einem Sicherheitsbulletin, das bestimmte Schwachstellen, Exploits oder zerstörerische Verhaltensweisen beschreibt, zu einer Risikobewertung aufgefordert. Durch die Risikobewertung wird festgestellt, ob das Unternehmen anfällig oder bereits kompromittiert ist.

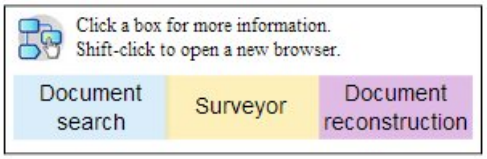
Ziele

Um das Problem in einer solchen Untersuchung zu beheben, setzt sich das Unternehmen folgende Ziele:

- Bewertung des Vorhandenseins ermittelter Schwachstellen im Unternehmen
- Erkennung der zerstörerischen Anwesenheit externer Parteien
- Beschaffung von Beweisen für eine Kompromittierung
- Ermittlung, ob das Unternehmen Opfer eines Exploits ist
- Ermittlung der Identität des Benutzers

Untersuchung

Nutzen Sie für Ihre Untersuchung die Tools auf der Registerkarte **Forensics** (Forensik).



1. Verwenden Sie die freie Suche, um nach Eigenschaften von Schwachstellen, Exploits oder sonstigen zerstörerischen Verhaltensweisen zu suchen, die im Sicherheitsbulletin angegeben sind.
2. Verwenden Sie die freie Suche, um Querverweise auf Forschungs- oder sonstige Daten zum Ableiten von Indikatoren zu erstellen.
3. Untersuchen Sie mithilfe von Surveyor Interaktionen, von denen ermittelte Schwachstellen möglicherweise ausgenutzt wurden.
4. Untersuchen Sie verdächtige Inhalte, die vom Produkt markiert wurden.
5. Überprüfen Sie Inhalte, die potenziell riskanten Interaktionen unterliegen, anhand der Datenwiederherstellung.
6. Verfolgen Sie mithilfe von Surveyor die Aktivitäten von potenziell riskanten Entitäten zurück.

Kapitel 3. Schnelleinstieg in Forensikuntersuchungen

In IBM Security QRadar Incident Forensics können Sie mit Ihren Forensikuntersuchungen sofort beginnen. Dazu navigieren Sie im Menü **Quick Start** (Schnelleinstieg) einfach zu den gewünschten Daten im Repository 'Forensics', die Sie über dieses Menü selbstverständlich auch filtern können. Dieses Launchpad enthält vordefinierte Übersichtsabfragen, mit denen Sie eine Suche starten oder die Beziehungen einer Entität abrufen können.

Folgen Sie zum schnellen Einstieg folgenden Anleitungen:

1. Starten Sie über die Registerkarte **Offenses** (Angriffe) eine forensische Wiederherstellung bzw. Suche nach einem Angriff.
   - Wenn Sie mit der rechten Maustaste auf einen Angriff oder eine IP-Adresse klicken und eine forensische Wiederherstellung ausführen, ruft die Forensik die rohen Erfassungsdaten für die angegebenen Zeiträume von der Erfassungseinheit ab, extrahiert Dokumente und erstellt sie neu und fügt dann die Ergebnisse zum Forensikrepository hinzu.
   - Wenn Sie mit der rechten Maustaste auf einen Angriff oder eine IP-Adresse klicken und danach eine forensische Suche ausführen, wird das Repository 'Forensics' entsprechend gefiltert und nach der IP-Adresse durchsucht. Die Ergebnisse werden in diesem Fall im Hauptraster auf der Registerkarte **Forensics** (Forensik) angezeigt. Sie können die Suche durch Abfragen präzisieren.

   Wenn QRadar Incident Forensics eine Suchanforderung erhält, verarbeitet es die Paketaufzeichnungsdaten und konvertiert sie in das Format zurück, das an den vorgesehenen Empfänger gesendet wurde. Microsoft Word-Dokumente beispielsweise werden als Word-Dateien wiederhergestellt. Voice-over-IP-Telefonanrufe werden als Audiodateien wiederhergestellt. Die wiederhergestellten Dateien werden anhand ihrer Metadaten und ihres Dateiinhalts indiziert, damit sie durchsucht werden können.
2. Klicken Sie auf der Registerkarte **Forensics** (Forensik) auf **Quick Start** (Schnelleinstieg).

   Nach einer Wiederherstellung oder Suche können Sie, statt freie Suchen durchzuführen oder eigene Abfragen zu erstellen, ihre Untersuchungen mit den vordefinierten Abfragen des Menüs **Quick Start** (Schnelleinstieg) der Registerkarte **Forensics** (Forensik) ganz schnell starten. Sie können sich zum Beispiel die Kategorie **Suspect Content** (Verdächtiger Inhalt) ansehen und eine der darin enthaltenen Abfragen, zum Beispiel **entity alert** (Entitätswarnung) ausführen. *Verdächtiger Inhalt* wird anhand eines vordefinierten Regelsatzes zu Inhalten erkannt, die auf verdächtige Aktivitäten hinweisen. Eine *Entitätswarnung* kennzeichnet eine möglicherweise zerstörerische Entität, die an der Verletzung einer Sicherheitsrichtlinie beteiligt ist.

   Durch die Inhaltskategorisierungs- und Filterfunktionen kann die Menge der zurückgegebenen Daten reduziert werden.
3. Wählen Sie im **Grid** (Raster) die Dokumente aus, die Sie näher untersuchen möchten.

   QRadar Incident Forensics gibt mit Prioritäten versehene Suchergebnisse zurück. Wie bei der Priorisierung von Sites in Internetsuchen werden die häufigsten Vorkommnisse am Anfang der Liste angezeigt.

Sie können mit dem Pivotieren (Untersuchen) der Daten beginnen, indem Sie auf die Links klicken oder die mit den Dokumenten verbundenen Metadaten durchsuchen. Die Datenpivotierungsfunktionen bieten verschiedene Suchansichten und Datenübersichten.

4. Zur Untersuchung der Beziehungen zwischen den Aktionen und Sicherheitsvorfällen wählen Sie in der Dokumentansicht einen Link aus und klicken Sie mit der rechten Maustaste auf **Get relations for** (Beziehungen abrufen für).

   Nachdem Sie die Attribute untersucht haben, können Sie die abgefragten Informationen durch Verbinden der Entitäten filtern.

5. Klicken Sie auf **Digital Impressions** (Digitale Spuren), um der Identität zu folgen und einen kompilierten Satz an Zuordnungen zu erhalten.

   Bei einer digitalen Spur handelt es sich um einen Metadatenindex, der dabei helfen kann, mutmaßliche Angreifer oder verdächtige Insider durch die Spuren, die ein böswilliger Benutzer nach sich zieht, zu identifizieren. Zur Erstellung solcher Beziehungen verwendet QRadar Incident Forensics Daten aus Netzquellen wie IP-Adressen, MAC-Adressen, TCP-Ports und TCP-Protokolle. Es findet auch Informationen wie Chat-IDs und es kann Informationen wie die Autorendaten aus Textverarbeitungs- oder Tabellenkalkulationsprogrammen lesen. Eine digitale Spur kann Beziehungen aufdecken, indem sie die Identität einer Entität mit identifizierenden Daten anderer Benutzer oder Entitäten verbindet.

Suchvorgänge und Lesezeichen in QRadar Incident Forensics

Prüfer können mit IBM Security QRadar Incident Forensics relevante Daten aus dem Netzverkehr und aus Dokumenten extrahieren.

Datensätze suchen und markieren

Um intuitive Forensikaktivitäten zu ermöglichen, ruft QRadar Incident Forensics Paketdaten ab und nimmt weitere Inhalte auf. Diese Technologie stellt eine durch Suchvorgänge gesteuerte Datenexploration, Sitzungswiederherstellung und Forensikintelligenz bereit, um Untersuchungen von Sicherheitsverstößen zu unterstützen.

Prüfer führen bei ihren Untersuchungen zunächst allgemeine Aktionen durch und nehmen dann eine Feinabstimmung der Untersuchungsergebnisse vor, um zu einem relevanten Endergebnis zu gelangen. Ein einfacher, allgemeiner Ansatz besteht darin, zuerst viele Datensätze zu suchen und zu markieren. Anschließend werden die markierten Datensätze genauer geprüft, um eine endgültige Gruppe von Datensätzen zu erstellen. Dabei wird bestimmt, welches Material relevant ist, und es werden durch differenzierte Abfragen Elemente ein- oder ausgeschlossen. Anhand des so gewonnenen Materials wird eine Hypothese überprüft.

Wenn sich neue Anhaltspunkte ergeben, kann diesen mithilfe anderer Methoden nachgegangen werden. Mit Visualisierungs- und Analysetools können die Ergebnisse manuell und automatisch auf ihre Relevanz überprüft werden. Zudem lassen sich durch variierende Abfragen unterschiedliche Aspekte desselben Problems betrachten.

Markierte Datensätze verarbeiten

Wenn Sie Ergebnisse finden, die für Ihre Untersuchung von Bedeutung sind, können Sie die Ergebnisse markieren, um später eine gründlichere Prüfung vorzunehmen und eine endgültige Entscheidung zu treffen. Setzen Sie mehr Lesezeichen, als Sie glauben, dass Sie benötigen werden. Setzen Sie im Zweifelsfall ein Lesezeichen.

Sie können nicht relevantes Material löschen und sich auf die Ergebnisse konzentrieren, von denen Sie denken, dass sie relevant sind.

Nachdem Sie für eine Gruppe von Ergebnissen, die Sie als relevant betrachten, Lesezeichen gesetzt haben, können Sie Ihre Überprüfung optimieren.

1. Untersuchen Sie jedes markierte Dokument mithilfe der Visualisierungs- und Analysetools.
2. Hängen Sie Fallhinweise an die Dokumente an und treffen Sie zu jedem Dokument eine endgültige Entscheidung bezüglich seiner Relevanz für den Fall.
3. Wenn ein Datensatz nicht relevant ist, entfernen Sie die Markierung.

   An diesem Punkt im Untersuchungsprozess haben Sie das relevante Material im Repository ermittelt und verfügen jetzt über eine Gruppe relevanter markierter Datensätze.
4. Drucken, exportieren oder verarbeiten Sie die relevanten Datensätze.

Suchen und Untersuchen von Dokumenten

Prüfer suchen Dokumente, die für einen Anhaltspunkt oder eine Hypothese bezüglich des Auftretens eines Sicherheitsverstoßes relevant sind.

Suchvorgänge

Statt die Massen an Dokumenten manuell zu durchstöbern, von denen sich die meisten nicht auf den Fall beziehen, verwenden Prüfer das Repository 'Forensic' zum Extrahieren der Dokumente, die die interessanten Merkmale erfüllen. Beispielsweise betrifft ein Dokument, das innerhalb eines bestimmten Zeitraums auftrat, ein Thema, das von Interesse ist, oder es handelt sich um ein Dokument, das von einem verdächtigen Angreifer gesendet oder empfangen wurde.

Suchvorgänge können spezifisch sein. "Suche die genaue Zeichenfolge “Mission Alpha”" ist zum Beispiel eine spezifische Suche. Alternativ können Suchvorgänge aber auch allgemein gehalten sein. "Suche alle Versicherungsnummern im gesamten Repository" ist zum Beispiel eine allgemeine Suche.

Suchvorgänge können einfach sein und nur auf einer einzigen Bedingung basieren. Komplexe Suchergebnisse müssen mehrere Bedingungen erfüllen. Die Suche nach allen E-Mails zwischen zwei verdächtigen Angreifern zu einem Thema unter Ausschluss aller E-Mails mit Anhängen ist zum Beispiel eine komplexe Suche. Eine Suche hat den Zweck, die Datensätze schnell und präzise auf ein einfach zu verwaltendes Arbeitsset zu reduzieren. Je kleiner die vom Prüfer zu untersuchende Gruppe von Dokumenten, desto höher die Wahrscheinlichkeit, dass die Dokumente für den Fall relevant sind.

Forensikwiederherstellung

Zum Abrufen der unaufbereiteten Paketaufzeichnungsdaten von Paketaufzeichnungseinheiten führen Sie über eine(n) oder mehrere IP-Adressen oder Ports einen Forensikwiederherstellungsjob aus.

Wiederherstellung über eine IP-Adresse oder einen Port ausführen

Führen Sie zum Abrufen der unaufbereiteten Aufzeichnungsdaten von einer Aufzeichnungseinheit eine Forensikwiederherstellung aus. Eine Wiederherstellung können Sie auch über mehrere IP-Adressen oder Ports ausführen. Wenn Sie keine IP-

Adresse und keinen Port angeben, wird der gesamte TCP- und UDP-Datenverkehr wiederhergestellt. Bei Angabe mehrerer IP-Adressen oder Ports müssen Sie diese durch ein Komma trennen.

Zur Ausführung einer Forensikwiederherstellung klicken Sie in QRadar mit der rechten Maustaste auf eine IP-Adresse oder einen Port oder Sie klicken auf das Symbol **Wiederherstellung ausführen**  auf der Registerkarte **Forensics** (Forensik).

Einschränkung: Sie können etwa sieben IPv4-Adressen und sieben Ports bzw. maximal 255 Zeichen eingeben. Die Felder **IP Address** und **Port** bilden gemeinsam mit anderen Ausdrücken eine Filterzeichenfolge. Diese Zeichenfolge darf nicht länger als 255 Zeichen sein.

Wiederherstellung wiederholen

Führen Sie im Ergebnisraster auf der Registerkarte **Forensics** (Forensik) die Option 'Re-run recovery' (Wiederherstellung wiederholen) aus, um eine zuvor erstellte Wiederherstellung zu wiederholen. Beispielsweise können Sie eine Forensikwiederherstellung wiederholen, wenn eine Ausführung unvollständige Daten zurückgibt. Sie können dann zum Beispiel andere IP-Adressen eingeben oder den Zeitrahmen gegenüber dem vorherigen Job ändern.

Zur erneuten Ausführung des zuvor ausgeführten Forensikwiederherstellungsjobs klicken Sie auf **Re-run this forensics recovery** (Forensikwiederherstellung wiederholen). Bei der Wiederholung eines Wiederherstellungsjobs enthält die Seite **Forensics Recovery** (Forensikwiederherstellung) die bei der letzten Wiederherstellung verwendeten Werte. Sie können die gleiche Wiederherstellung erneut ausführen oder die automatisch generierten Werte ändern.

Ein Wiederherstellungsjob kann nur nach Abschluss des Jobs wiederholt werden bzw., wenn der Status des Jobs 'Completed' (Abgeschlossen), 'Canceled' (Abgebrochen) oder 'Failed'(Fehlgeschlagen) lautet.

Forensic-Fälle

Bei Fällen handelt es sich um logische Container für Ihre Gruppe importierter Dokument- und Paketaufzeichnungsdateien.

Fälle können von Administratoren oder Prüfern erstellt werden, die über die Berechtigung zum Erstellen von Fällen verfügen. Administratoren können Fälle erstellen und Prüfern zuordnen. Prüfer können einen neuen Fall erstellen, wenn Sie Paketaufzeichnungsdaten von einer IP-Adresse in IBM Security QRadar abrufen.

Zugehörige Tasks:

„PCAP-Dateien und Dokumente von externen Systemen in Forensikfälle hochladen” auf Seite 19
Sie können externe Daten in bestimmte Fälle hochladen.

Datensammlungen

In Datensammlungen werden zusammengehörige Daten aus einer bestimmten Quelle (z. B. einer Datendatei für die Paketaufzeichnung (PCAP), einer PDF-Datei oder einem Netzdatenstrom) gruppiert.

Mithilfe von Datensammlungen werden Gruppen zusammengehöriger Daten ermittelt und verwaltet. Nach Abschluss Ihrer Untersuchung können Sie die Gruppendaten in der Datensammlung schnell löschen.

Datensammlungen werden von Administratoren oder Prüfern erstellt. Administratoren erstellen Datensammlungen, um Daten manuell in IBM Security QRadar Incident Forensics zu laden. Administratoren können außerdem Datensammlungen zu Fällen hinzufügen. Prüfer können eine neue Datensammlung erstellen, wenn Sie die Abfrage von Paketaufzeichnungsdaten aus einer IP-Adresse in IBM Security QRadar starten.

Beachten Sie die folgenden Regeln für Datensammlungen und Namen von Datensammlungen:

- Namen von Datensammlungen müssen eindeutig sein.
- Fälle enthalten eine oder mehrere Datensammlungen.
- Datensammlungen können mehreren Fällen hinzugefügt werden.
- Suchergebnisse geben doppelte Daten zurück, wenn ein Prüfer zwei Fälle mit der gleichen Datensammlung besitzt.
- Falls der Name einer Datensammlung beim Hochladen einer neuen Datendatei zur Paketaufzeichnung nicht eindeutig ist, wird die ursprüngliche Datensammlung vor dem Hochladen der neuen Datendatei zur Paketaufzeichnung gelöscht.

PCAP-Dateien und Dokumente von externen Systemen in Forensikfälle hochladen

Sie können externe Daten in bestimmte Fälle hochladen.

Vorbereitende Schritte

Ein Administrator muss sichere FTP-Berechtigungen für den Benutzer aktivieren, der externe Dateien hochladen möchte.

Informationen zu diesem Vorgang

IBM Security QRadar Incident Forensics kann Daten aus allen zugänglichen Verzeichnissen im Netz importieren. Die Daten können verschiedene Formate aufweisen, einschließlich folgender Formate:

- Dateien aus externen Quellen im PCAP-Standardformat
- Dokumente wie Textdateien, PDF-Dateien, Tabellenkalkulationen und Präsentationen
- Bilddateien
- Streaming-Daten aus Anwendungen
- Streaming-Daten aus externen PCAP-Quellen

Es können mehrere Dateien in einen Fall hochgeladen werden.

Einschränkung: Der Fallname muss eindeutig sein. Es kann kein Fall mit dem Namen eines bereits vorhandenen Falls erstellt werden.

Vorgehensweise

1. Gehen Sie im FTP-Client wie folgt vor:
   a. Stellen Sie sicher, dass Transport Layer Security (TLS) als Protokoll ausgewählt ist.

b. Fügen Sie die IP-Adresse des QRadar Incident Forensics-Hosts hinzu.
c. Führen Sie eine Anmeldung mit dem Benutzernamen und dem Kennwort durch, die für QRadar Incident Forensics eingerichtet wurden.

2. Stellen Sie eine Verbindung mit dem QRadar Incident Forensics-Server her und erstellen Sie ein neues Verzeichnis.
3. Erstellen Sie für die FTP-Übertragung und Speicherung von PCAP-Dateien unter dem für den Fall erstellen Verzeichnis ein Verzeichnis mit dem Namen `singles` und ziehen Sie die PCAP-Dateien in dieses Verzeichnis.
4. Erstellen Sie für die FTP-Übertragung und Speicherung aller anderen Dateien unter dem für den Fall erstellen Verzeichnis ein Verzeichnis mit dem Namen `import` und ziehen Sie die Dateien in dieses Verzeichnis.
5. Geben Sie folgenden Befehl ein, um den FTP-Server erneut zu starten:

   ```
   etc/init.d/vsftpd restart
   ```

6. Geben Sie folgenden Befehl ein, um einen Neustart des Servers durchzuführen, bei dem die Dateien aus dem Upload-Bereich in das QRadar Incident Forensics-Verzeichnis verschoben werden:

Ergebnisse

Sie können Ihren Fall in einem der Tools auf der Registerkarte **Forensics** (Forensik) anzeigen.

Abfragen im Repository 'Forensics'

Prüfer können die Kenndaten der Dokumente angeben, die Sie aus der Forensics-Datenbank abrufen möchten. Mit mehreren Abfragen wird eine Gruppe von Dokumenten zur Untersuchung gesucht.

Die Verwendung mehrerer Abfragen und die manuelle Prüfung einer kleinen Gruppe von Dokumenten ist leistungsfähiger als die Sichtung des gesamten Repositorys. Konzepte nachfolgender Abfragen und eingegrenzter Abfragen entstehen oft während der Überprüfung eines nicht relevanten Dokuments.

Die Zunahme der Menge und die Spezifität von Abfragebegriffen führen zu Ergebnismengen mit einer höheren Relevanz. Ihr Ziel ist es, möglichst viele bekannte Informationen zu den Ergebnissen zu definieren, die Sie erhalten möchten, und möglichst sehr spezifisch zu sein. In den Suchkriterien können beliebig viele Abfragebegriffe eingeben werden. Sie trennen Begriffe durch ein Leerzeichen oder mit einem booleschen Operator. Begriffe, die nur mit einem Leerzeichen voneinander getrennt werden, schließen einen booleschen Operator für das logische OR ein. Die Verwendung eines OR-Operators bedeutet, dass alle Ergebnisse für die Suchbegriffe gleichermaßen erwünscht sind. Ergebnisse, die die meisten Suchbegriffe erfüllen, werden an den Anfang der Liste gestellt, um die Stärke der Übereinstimmung mit den Abfragebegriffen anzuzeigen.

Ein einzelnes Suchkriterium wird auch als Abfragebegriff bezeichnet. Suchvorgänge enthalten normalerweise mehrere Abfragebegriffe. Die Gruppe der Abfragebegriffe für eine einzelne Suche wird auch als Abfragezeichenfolge bezeichnet. Die Fähigkeit zum Formulieren geeigneter Abfragen erfordert eine gewisse Übung, aber es ist nicht schwer. Dazu werden nur einige Abfragebegriffe benötigt und Sie müssen lernen, wie die Begriffe in Kombinationen erstellt und ausgeschlossen werden, um das gewünschte Resultat zu erzielen. Da Abfragezeichenfolgen in QRadar Incident Forensics gespeichert werden, können Sie Ihre Suchvorgänge laufend optimieren, während Sie mehr über die Daten erfahren.

Zugehörige Tasks:

„Beziehungen und Zuordnungen darstellen" auf Seite 32

Im Fenster **Visualize** (Visualisieren) können Sie die Beziehungen zwischen Attributen in wiederhergestellten Dokumenten anzeigen. Sie können beispielsweise die E-Mail-Adressen überprüfen, die mit einer bestimmten E-Mail-Adresse kommuniziert haben.

Unformatierte Abfragebegriffe

Prüfer suchen exakte Übereinstimmungen von Zeichenfolgen, indem Sie die Abfragebegriffe auf der Registerkarte **Forensics** direkt in das Feld mit den Suchbedingungen eingeben. Sie können einzelne oder mehrere Wörter abfragen.

In der folgenden Tabelle wird der Suchtyp für Abfragen beschrieben, der verwendet werden kann.

Tabelle 1. Typen von freien Abfragen

Typ der Suchabfrage	Beschreibung	Beispiel
Abfrage eines einzelnen Worts	Es wird nach einem Begriff in den Dokumenten gesucht.	Welpen
Einzelne Abfrage mit Platzhalterzeichen	Es wird nach einer Übereinstimmung mit einem oder mehreren Zeichen in der Mitte oder am Ende eines Abfragebegriffs gesucht. **Einschränkung:** Platzhalterzeichen können nicht als erstes Zeichen in einem Suchvorgang verwendet werden.	te?t test* te*t
Abfrage mehrerer Wörter	Gibt an, dass Suchergebnisse in der Reihenfolge der Relevanz eines Abfragebegriffs zurückgegeben werden. Dokumente, die beide Abfragebegriffe enthalten, werden zuerst aufgeführt, gefolgt von Dokumenten, die nur einen der Abfragebegriffe enthalten. Dokumente mit nur einem Abfragebegriff werden gemäß der Häufigkeit eingeordnet, mit der der einzelne Abfragebegriff auftritt.	Welpen befreien
Abfrage mehrerer Wörter mit Anführungszeichen	Es wird nach einer Übereinstimmung mit der exakten Zeichenfolge gesucht. Dokumente, die beide Wörter enthalten, jedoch nicht in dieser Reihenfolge und Position, werden nicht als Ergebnisse zurückgegeben. Durch die Anführungszeichen werden diese zwei Wörter also zu einer einzigen Zeichenfolge bzw. zu einem einzigen Abfragebegriff. Die Suchmaschine betrachtet sie nicht mehr als zwei separate Wörter.	"Welpen befreien"
Abfrage mehrerer Wörter, bei der der Operator AND verwendet wird	Gibt an, dass beide Abfragebegriffe im Dokument vorhanden sein müssen, damit es zu einer Übereinstimmung kommt. Die Reihenfolge der Abfragebegriffe spielt dabei keine Rolle und sie müssen nicht nahe beieinander liegen.	befreien AND Welpen

Metadatentags

Allgemeine Entitäten werden mit Tags versehen, damit Prüfer die exakten Ergebnisse aus relevanten Dokumenten schnell abrufen können.

Viele Metadatenfelder werden möglicherweise im Incident Forensic-Index verwendet, abhängig vom Typ der Sitzung, des Dokuments oder des Protokolls.

Der Tagname für Metadaten muss bei der Angabe exakt und im Repository 'Forensic' vorhanden sein.

In der folgenden Tabelle werden Suchtypen für Metadatentags aufgeführt.

Tabelle 2. Suchvorgänge mit Metadatentags

Suchtyp des Metadatentags	**Format**	**Beispiel**
Standard	`Metadatentag<Wert>`	`Anwendungsprotokoll:http`
Platzhalter	`Metadatentag:*`	`Kreditkartennummer:*`
Bereich	`Metadatentag:[<Anfangswert> TO <Endwert>`	`Dauer:[30 TO 56]`

Zugehörige Konzepte:

„Dokumentanmerkungen" auf Seite 25
Prüfer markieren Dokumente und fügen Dokumenten Anmerkungen hinzu, um Ideen und Begründungen zu Dokumenten zu protokollieren.

Boolesche Kombinationen

Mehrere Abfragebegriffe können mithilfe einfacher boolescher Operatoren aneinandergereiht werden, um besonders gezielte Abfragezeichenfolgen zu erstellen. Wenn diese Abfragezeichenfolgen entsprechend gebildet werden, können Ergebnisse zurückgegeben werden, die exakt mit der Suche eines Prüfers übereinstimmen.

Die grundlegenden booleschen Operatoren sind AND, OR, NOT und (). Der Operator AND gibt an, dass es für beide Abfragebegriffe eine Übereinstimmung im Dokument geben muss. Der Operator OR gibt an, dass einer der Abfragebegriffe in einem Dokument gesucht werden soll. Mit dem Operator NOT werden Ergebnisse vermieden oder entfernt, die mit den Abfragebegriffen übereinstimmen, die ausgeschlossen werden sollen. Der Operator () gruppiert Abfragebegriffe und Werte, um Funktionen für eine Gruppe anzuwenden, mehrere Werte für eine einzelne Funktion anzuwenden oder für die Übersichtlichkeit der Syntax.

Boolesche Operatoren müssen großgeschrieben werden.

In der folgenden Tabelle werden die booleschen Operatoren und ein Beispiel für eine Abfragezeichenfolge gezeigt.

Tabelle 3. Boolesche Operatoren für Abfragezeichenfolgen

Boolescher Operator	Beispiel für eine Abfragezeichenfolge	Erläuterung des Beispiels
AND	`TcpPort:80 AND Protocol:http`	Es werden zwei Abfragebegriffe verwendet, um den gesamten standardmäßigen Webdatenverkehr zu finden. Wenn der Web-Test an Port 8080 auftritt, besteht keine Übereinstimmung, da keiner der Abfragebegriffe den Wert 'true' hat.
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	Mit drei Abfragebegriffen werden die Ergebnisse auf Ergebnisse aus den Dokumentdatensammlungen 'Yahoo', 'CNN' und 'MSN' im Repository 'Forensics' beschränkt.
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	Es wird nach Datenverkehr mit einer Portnutzung gesucht, die vom Standard abweicht. Mit dem ersten Abfragebegriff wird der standardmäßige HTTP-Datenverkehr gesucht und mit dem zweiten Abfragebegriff der Datenverkehr ausgeschlossen, der akzeptierte HTTP-Ports verwendet.

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		In diesen Abfragen werden Klammern erfolgreich dazu verwendet, komplexe Ziele zu erreichen. Ohne Klammern sind diese Abfragen länger und die Formulierung sowie die Fehlerbehebung ist komplexer.

Tool für das Abfrageerstellungsprogramm

Mit dem Tool für das Abfrageerstellungsprogramm können Suchvorgänge erstellt oder gespeicherte Suchvorgänge verwaltet werden.

Mit dem Tool für das Abfrageerstellungsprogramm werden Prüfer grafisch durch den Prozess zum Erstellen leistungsfähiger Suchvorgänge geleitet, in denen kategorisierte Listen von Abfragebegriffen mit Beispielen verwendet werden.

Tabelle 4. Parameter zum Tool für das Abfrageerstellungsprogramm

Parameter	Beschreibung
Kategorie auswählen	Filtert die Liste der Metadatentags, die in der Liste **Feld auswählen** verfügbar sind.
Feld auswählen	Die Metadatentags, mit denen die Informationen im Repository 'Forensics' gekennzeichnet werden.
Query Example (Abfragebeispiel)	Führt die Abfrage aus, die sich im Feld **Query Input** (Abfrageeingabe) befindet, und dokumentiert die Anzahl der Ergebnisse.
Neu	Ersetzt eine vorhandene Abfrage durch die neue Abfrage, wenn Sie auf **Insert Query** (Abfrage eingeben) klicken.

Tabelle 4. Parameter zum Tool für das Abfrageerstellungsprogramm (Forts.)

Parameter	Beschreibung
AND	Kombiniert eine neue Abfrage mit der vorhandenen Abfrage, wenn Sie auf **Insert Query** (Abfrage eingeben) klicken. Die Dokumente müssen mit beiden Abfragebegriffen übereinstimmen.
OR	Kombiniert die neue Abfrage mit der vorhandenen Abfrage, wenn Sie auf **Insert Query** (Abfrage eingeben) klicken. Dokument müssen mit einem der Begriffe übereinstimmen.

Prüfer können Suchvorgänge in Ordnern auf dem Dateisystem speichern und verwalten, um die gemeinsame Nutzung zwischen Prüfern zu ermöglichen. Für Referenzen, die Verwaltung und zum besseren Verständnis verwenden Prüfer Beschreibungen oder Namen für gespeicherte Abfragen.

Über die Funktion **Use Query** (Abfrage verwenden) auf der Registerkarte **Abfrage** kann eine gespeicherte Abfrage zur Ausführung an das Feld **Search Criteria Input** (Eingabe der Suchkriterien) gesendet werden.

Prüfer suchen über die Liste der vorherigen Abfragen zuvor ausgeführte Abfragen und können diese erneut ausführen, indem Sie die Abfrage auswählen, die ausgeführt werden soll, und anschließend auf **Insert Query** (Abfrage eingeben) klicken.

Tool für Abfragefilter

Das Tool für Abfragefilter stellt mit den aktiven Daten visuelle Hinweise zur Erstellung permanenter Filter bereit.

Der Abfragefilter ist ein permanenter Hintergrundfilter, der die aktive Dokumentgruppe, die von der Abfragezeichenfolge abgefragt wird, verkleinert. Mithilfe eines Filters können Sie die verfügbare Dokumentgruppe verkleinern, ohne die Abfragezeichenfolge durch statische Abfragebegriffe überladen zu müssen. Dadurch erhalten Sie eine bessere Kontrolle über die Abfragezeichenfolge.

Der Abfragefilter ist aufgrund der Listen mit fallabhängigen Filtertypen, der dynamischen Aktualisierung und der Ergebniszusammenfassung in Echtzeit ein guter Ausgangspunkt für eine Untersuchung. Die Filtertyplisten werden mit allen Werten gefüllt, die in den für Sie verfügbaren Fällen gefunden werden. Sie erhalten einen schnellen Überblick über die Daten in den Fällen, deren Eigner Sie sind. Beim Auswählen oder Löschen von Elementen in der Filtertypliste wird die Ergebniszusammenfassung automatisch aktualisiert. Sie können sofort sehen, wie der Filter wirkt und wie groß eine Dokumentgruppe nach Anwendung des Filters noch ist.

Der Standardabfragefilter sollte nicht für Abfragen optimiert werden, die Sie wiederverwenden möchten. Erstellen Sie für Abfragen, die Sie speichern möchten, einen neuen Abfragefilter. Wenn Sie den Standardabfragefilter geändert haben, setzen Sie ihn nach Abschluss der Filterung zurück, um einen irrtümlichen Ausschluss von Dokumenten bei künftigen Suchabfragen zu vermeiden.

Ergebnisse für aktive Filter

Prüfer können im Abschnitt mit der Zusammenfassung der Ergebnisse im Tool für den Abfragefilter die Ergebnisse aus aktiven Filtern anzeigen.

Beim Ändern des Filters wird die Zusammenfassung aktualisiert und zeigt die Gesamtzahl der Dokumente und die Anzahl der verfügbaren Dokumente an. Bei der Gesamtzahl der Dokumente handelt es sich um die Anzahl der Dokumente, die vor dem Anwenden des Filters für den Prüfer verfügbar sind. Bei der Anzahl der verfügbaren Dokumente handelt es sich um die Dokumente, die nach dem Anwenden des Filters verfügbar sind. Prüfer können mit diesen Dokumentanzahl die Effektivität Ihrer Filter beurteilen und diese beim Erstellen entsprechend anpassen.

Suchfilter für das Tool des Abfragefilters

Prüfer filtern die Daten für Ihre zugeordneten Fälle. Die Daten werden nach Filtertyp (z. B. IP-Adresse oder MAC-Adresse) in Gruppen aufgeteilt.

Mit der Funktion zum Umschalten der logischen Aktion kann der Prüfer die in der Liste ausgewählten Elemente einschließen oder ausschließen.

Jede Gruppe von Suchfiltern enthält eine Funktion zum Umschalten der logischen Aktion, die so festgelegt werden kann, dass die in der Liste ausgewählten Elemente ein- oder ausgeschlossen werden. Wenn das Einschließen festgelegt ist, werden die Elemente in der Liste mit einer logischen AND-Verknüpfung verbunden, d. h., jedes verfügbare Dokument enthält alle ausgewählten Elemente. Wenn der Ausschluss festgelegt ist, wird ein logisches OR-Zeichen verwendet, d. h., keines der verfügbaren Dokumente enthält eines der ausgewählten Elemente.

Prüfer können in der Gruppe **UserQuery** eigene Abfragezeichenfolgen formulieren, die dem Filter hinzugefügt werden sollen.

Anzahl der von einer Suche zurückgegebenen Dokumente begrenzen

Ihren IBM Security QRadar Incident Forensics-Abfragen können Sie Filter hinzufügen, um die Anzahl bzw. den Typ der auf der Suchergebnisseite zurückgegebenen Dokumente zu begrenzen.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Forensics** (Forensik) auf das Symbol **Query Filters** (Abfragefilter).

   Die Daten werden nach Filtertyp in Gruppen eingeteilt.
2. Geben Sie im Fenster **Search Filters** (Suchfilter) für jeden Filtertyp mit **Include** (Einschließen) bzw. **Exclude** (Ausschließen) an, ob die Dokumente im Suchergebnis enthalten oder ausgeschlossen sein sollen.
3. So finden Sie ein Element in einer Filtergruppe:
   a. Erweitern Sie in der Spalte **Filter Type** (Filtertyp) eine Filtergruppe.
   b. Wählen Sie im Fenster **Search** (Suchen) die Suchkriterien aus und klicken Sie auf **Find** (Suchen).

      Wenn Sie in der Filtergruppe **Webcategory** einen Datensatz suchen, werden alle übereinstimmenden Kategoriefelder angezeigt. Suchen Sie beispielsweise nach **Webcategory equal chat**, werden **Chat** und alle zugehörigen Kategorien wie **Instant Messaging**, **Webmail/Unified Messaging**, **Search Engines/Web catalogs/Portals** und **Cloud** angezeigt.

Dokumentanmerkungen

Prüfer markieren Dokumente und fügen Dokumenten Anmerkungen hinzu, um Ideen und Begründungen zu Dokumenten zu protokollieren.

Dokumente können in der Hauptanzeige mit den Ergebnissen sowie im Surveyor-Tool im chronologischen Gitter, das die Reihenfolge der während einer Interaktion ausgetauschten Dokumente anzeigt, markiert werden. Da Abfragen und Untersuchungen unter Umständen sehr komplex sein können, markieren Prüfer alle Einträge, einschließlich der Dokumente mit geringerer Bedeutung. Dank der Markierungen müssen komplexe Abfragen und Aspekte der Untersuchung nicht erneut erstellt werden. Es können Anmerkungen erstellt werden, nachdem ein Eintrag markiert wurde.

Während einer Untersuchung kann es vorkommen, dass Sie zwei oder mehr Pfaden folgen möchten. Mithilfe der Browserfunktion können Sie die Registerkarte, auf der Sie sich gerade befinden, kopieren. Dies erleichtert es Ihnen, zu dieser Position zurückzukehren und den weiteren Pfaden zu folgen, ohne sich daran erinnern zu müssen, wie Sie zum Verzweigungspunkt gelangen. Sie können die aktuelle Registerkarte je nach Bedarf beliebig oft kopieren. Folgen Sie jedem unterschiedlichen Pfad auf einer anderen Registerkarte und setzen Sie dabei Lesezeichen für die entsprechenden Dokumente. Sie können einen Hinweis hinzufügen, mit dem der Pfad gekennzeichnet wird, der zu dem jeweils markierten Dokument führte.

Hinweise sind eine Möglichkeit, die während einer Untersuchung angestellten Überlegungen aufzuzeichnen. Hinweise können nur von einem Administrator entfernt werden. Hinweise werden mit der Benutzer-ID des Prüfer sowie mit der Zeitmarke der Eingabe gekennzeichnet. Beim Exportieren von Dokumenten werden Hinweise mit dem wiederhergestellten Dokument und den zugehörigen Attributen ausgegeben.

Zugehörige Konzepte:

„Metadatentags” auf Seite 22
Allgemeine Entitäten werden mit Tags versehen, damit Prüfer die exakten Ergebnisse aus relevanten Dokumenten schnell abrufen können.

Kapitel 4. Untersuchungstools

Prüfer können mit den Tools 'Surveyor', 'Digital Impressions', 'Export' und 'Visualize' Daten auf unterschiedliche Weise verwalten.

Die Suchergebnisseite ist die Standardseite auf der Registerkarte **Forensics**. Die Suchergebnisse sind auf der Registerkarte **Grid** verfügbar. Prüfer können mit den Suchergebnissen auf der Registerkarte 'Grid' Dokumente schnell suchen und darauf zugreifen. Auf der Registerkarte **Grid** (Gitter) können sie die Ergebnisse mithilfe der Tools 'Surveyor', 'Digital Impressions', 'Export' und 'Visualize' weiter untersuchen.

Zeilenindikator

Der Zeilenindikator stellt für jedes Dokument, das in einer Ergebnismenge zurückgegeben wird, eine eindeutige ID bereit. Verwenden Sie den Zeilenindikator, um ein Dokument und alle erforderlichen zugehörigen Dokumente an das Visualisierungstool 'Reconstructed View' (Wiederhergestellte Ansicht) zu senden.

Zeilensortierung

Sie können die im Gitter angezeigten Zeilen sortieren. Da die Gesamtzahl der Ergebnisse die Anzahl der im Gitter angezeigten Ergebnisse übersteigen kann, kann nicht die gesamte Ergebnismenge sortiert werden.

Indikator für angezeigte Dokumente

Der Indikator für angezeigte Dokumente ist ein kleiner roter oder grüner Kreis, der angibt, ob ein Prüfer ein Dokument angezeigt hat.

Dokumentauswahl

Prüfer wählen mit dem Selektor für angezeigte Dokumente die Anzahl der Dokumente aus, die im Gitter mit den Ergebnissen angezeigt werden. Sie können mit SELECT ALL Dokumente an eine nachfolgende Funktion senden und Sie können viele Dokumente zur Verarbeitung oder Visualisierung senden. Wenn Sie Dokumente mit dem Selektor für angezeigte Dokumente auswählen, werden nicht nur die im Gitter vorhandenen Dokumente, sondern alle Dokumente ausgewählt.

Visualisierung von Netzen und Dokumenten

Prüfer können mit dem Visualisierungstool Muster erkennen, ermitteln, wo der meiste Datenaustausch im Netz und Dokumentengpass während eines angegebenen Zeitraums stattfindet und verdächtige Inhalte anzeigen. Prüfer können beispielsweise Muster im Datenaustausch im Netz visualisieren, z. B. Server, auf die nach den Geschäftszeiten eines Unternehmens zugegriffen wird.

Das VGrid-Tool ist in Zeitblöcke unterteilt. Verdächtige Inhalte wie Datenaustausch im Netz oder Dokumente werden durch ein rotes Rechteck im Gitter dargestellt. Ein grünes Rechteck zeigt reguläre Inhalte an. Ein Block in leuchtenden Farben gibt stärkeren Datenverkehr an. Je stärker die Sättigung der Farbe ist, desto größer ist die Menge des Datenverkehrs. Die Helligkeit eines Zeitblocks ist relativ zu den ak-

tuell im VGrid-Tool angezeigten Daten. Beispiel: Ein Zeitblock in leuchtenden Farben wird dunkler, wenn verschiedene Zeitblöcke mit weiteren Daten geladen werden.

Prüfer können die Typen des Netzverkehrs sowie die Anzahl der Dokumente für jeden Zeitblock mit Inhalten anzeigen.

Netzverkehr und Dokumente in einem Zeitblock untersuchen

Prüfer möchten möglicherweise einzelne Dokumente überprüfen, Websites durchsuchen oder E-Mails innerhalb eines bestimmten Zeitblocks senden.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Forensics** die Registerkarte **VGrid** aus.
2. Verwenden Sie eine der folgenden Optionen, um Inhalte in einem Zeitblock zu überprüfen:
   - Um die Typen des Netzverkehrs und die Anzahl der Dokumente anzuzeigen bewegen Sie den Mauszeiger über den Zeitblock.
   - Wenn Sie Inhalte im Zeitblock durchsuchen möchten, wählen Sie einen oder mehrere Zeitblöcke aus. Klicken Sie mit der rechten Maustaste und wählen Sie **Search selected time blocks** (Ausgewählte Zeitblöcke durchsuchen) aus.
   - Zur Anzeige der Folge der Ereignisse wählen Sie den Zeitblock und anschließend **Surveyor** aus.
   - Zur Darstellung des Inhalts wählen Sie einen Zeitblock und anschließend **Visualize** (Visualisieren) aus.

Surveyor-Tool

Mit dem Surveyor-Tool kann eine Folge von Ereignissen in einem Sicherheitsverstoß beim Auftreten dargestellt werden.

Mit diesem Tool können Prüfer feststellen, was verdächtige Angreifer angezeigt haben, sowie deren Aktionen. Das Surveyor-Tool stellt die chronologische Folge der Aktivitäten in einem Sicherheitsverstoß in einer filmähnlichen Visualisierungskomponente dar. Da das Surveyor-Tool einen Zeitraum darstellt, werden bei Auswahl eines einzelnen Dokuments in der Ergebnisanzeige nur wenige Informationen wiedergegeben. Wenn zu wenig Dokumente ausgewählt wurden, erweitern Sie auf der Registerkarte **Attributes** den Zeitradius um die ausgewählten Dokumente. Erweitern Sie die Zeit, indem Sie auf den Link **Show Context** (Kontext anzeigen) klicken.

Auf der Registerkarte **Attributes** (Attribute) werden Zertifikatsinformationen und Metadaten angezeigt. Sie können mit der rechten Maustaste auf eine IP-Adresse oder einen Port klicken, um nach Ereignissen, Datenflüssen und Assets zu filtern, bzw. auf eine MAC-Adresse, um nach Ereignissen und Assets zu filtern.

Sie können Ihre Abfragen nach Fallzeit, Protokoll und IP-Adresse filtern.

Auf der Registerkarte **List** (Liste) wird eine chronologische Liste der gesendeten und empfangenen Dokumente angezeigt.

Grüne ID-Nummern für Dokumente zeigen an, dass ein Dokument von einem Prüfer geprüft wurde, während Dokumente mit roten ID-Nummern nicht geprüft wurden.

Wiederhergestellte Dokumentansicht

Auf der Registerkarte **Ansicht** wird eine wiederhergestellte Ansicht des Dokuments angezeigt, das auf der linken Seite des Bildschirms in der Ansicht 'Liste' ausgewählt wird.

Durch diese leistungsfähige Kombination der Reihenfolgeplanung auf der linken und der Wiederherstellung auf der rechten Seite können Sie anzeigen, was verdächtige Angreifer gesehen und im Netz vorgenommen haben. Neben den sichtbaren Dokumenten, die im Netz kursierten, zeigt Surveyor auch die Handshakes, die zwischen Computern im Hintergrund ablaufen, sowie den Austausch von Zertifikaten an.

Zugehörige Tasks:

Kapitel 5, „Netzverkehr für eine IP-Adresse überprüfen", auf Seite 41
Für die Anzeige der relevanten Inhalte des Datenaustauschs, der während eines Sicherheitsverstoßes auftrat, können Sie Netzverkehr, der einer IP-Adresse zugeordnet ist, wiederherstellen. Sie können auch vorhandene Fälle, die einen Bezug zu einer IP-Adresse haben, durchsuchen.

Extrahierte Dokumentinhalte

Auf der Registerkarte **Text** werden Inhalte gezeigt, die aus dem Dokument extrahiert wurden. Der Dokumentinhalt ist nicht formatiert.

Dieser Text stammt aus der Indexierungskomponente der Suchmaschine.

Export von Dokumenten in QRadar Incident Forensics

In IBM Security QRadar Incident Forensics enthalten alle exportierten Dokumente, mit Ausnahme von PCAP-Dokumenten, das wiederhergestellte Dokument, den unformatierten Text des Dokuments, Attribute und an das Dokument angehängte Anmerkungen.

Beim Export von PCAP-Dokumenten findet keine Wiederherstellung statt. Wenn Sie beispielsweise eine Webseite exportieren, wird alles heruntergeladen, was der Browser während der Hauptverbindung heruntergeladen hat. In der Regel ist dies der größte Teil des Textinhalts. Die meisten heutigen Browser verwenden jedoch zur Übertragung weiterer Elemente, die nicht unmittelbar Bestandteil des Exports sind, mehrere Verbindungen. Und dieser PCAP-Inhalt wird beim Export nicht unmittelbar wiederhergestellt.

Ein ähnliches Beispiel sind komplexe Protokolle wie FTP oder VOIP, bei denen es einen Hauptbefehl und eine Steuerverbindung sowie eine separate Datenverbindung gibt. Wenn Sie die PCAP-Dateien eines VOIP-Aufrufs oder FTP-Downloads exportieren, werden die Daten nicht wiederhergestellt und Sie erhalten möglicherweise unerwartete Ergebnisse.

Dokumente als PCAP-Dateien exportieren

Dokumente können Sie aus verschiedenen IBM Security QRadar Incident Forensics- und IBM Security QRadar Packet Capture-Anwendungen als PCAP-Dateien exportieren.

Einschränkung: Der in das PCAP-Format exportierte Inhalt wird nicht wiederhergestellt.

Vorgehensweise

1. Zur Auswahl der zu exportierenden Dokumente aktivieren Sie im Wiederherstellungsraster auf der Registerkarte **Forensics** (Forensik) die Kontrollkästchen der betreffenden Dokumente und klicken Sie dann auf **Export** (Exportieren).

   Auf einmal können Sie maximal 25 Dokumente in das PCAP-Format exportieren.
2. Klicken Sie in der Liste **Select Export Type** (Exporttyp auswählen) auf **PCAP**.
3. Nachdem alle Dokumente für einen QRadar Incident Forensics-Host exportiert sind, können Sie auf **Download** klicken.
4. Bei einem Exportfehler für ein Dokument können Sie einen erneuten Versuch starten, indem Sie auf die Nachricht **FAIL** zu diesem Dokument klicken.

Ergebnisse

Wenn Sie eine einzelne PCAP-Datei exportieren, wird die Datei sofort heruntergeladen. Wenn Sie mehrere PCAP-Dateien exportieren, werden diese Dateien in einer ZIP-Datei komprimiert und diese Datei wird heruntergeladen.

Mit jedem Dokument wird die IP-Adresse des QRadar Incident Forensics-Hosts sowie die IP-Adresse der QRadar Packet Capture-Einheit gespeichert, von der das Dokument stammt. Wenn Sie den betreffenden QRadar Incident Forensics-Host entfernen oder eine QRadar Packet Capture verschieben, lässt sich der Export vermutlich nicht mehr durchführen.

Digitale Spur

Bei einer *digitalen Spur* handelt es sich um eine kompilierte Gruppe von Zuordnungen und Beziehungen, die zur Ermittlung einer Identität beitragen können. Mithilfe einer digitalen Spur werden Beziehungen im Netz wiederhergestellt, um die Identität einer angreifenden Entität, ihre Kommunikationsweise und Kommunikationspartner aufzudecken.

Mithilfe von digitalen Spuren können folgende wichtige Fragen schnell beantwortet werden:

- Welche Informationen gibt es zu diesem verdächtigen Angreifer, Computer oder zu dieser verdächtigen IP-Adresse?
- Mit wem hat dieser verdächtige Angreifer kommuniziert?
- Wer befindet sich in deren Netz aus Kontakten?
- Versucht der verdächtige Angreifer, seine Identität zu verbergen?

Online-IDs

Mit Online-IDs wie beispielsweise E-Mail-Adressen, Skype-Adressen, MAC-Adressen, Chat-IDs, Social Media-IDs oder Twitter-IDs werden Entitäten oder Personen ermittelt. Bekannte Entitäten oder Personen, die im Netzverkehr und in Dokumenten gefunden werden, werden automatisch mit Tags versehen.

IBM Security QRadar Incident Forensics stellt eine Beziehung zwischen gekennzeichneten IDs her, die miteinander kommunizieren, um eine digitale Spur zu erstellen.

Die Beziehungen von Datensammlungen in den Berichten zu einer digitalen Spur stellen eine fortlaufend erfasste elektronische Präsenz dar, die einem Angreifer zugeordnet ist, bzw. eine netzbezogene Entität oder ein beliebiger Metadatenbegriff

zu einer digitalen Spur. Prüfer können auf die mit Tags versehene ID einer beliebigen digitalen Spur klicken, die einem Dokument zugeordnet ist. Der daraufhin erstellte Bericht zur digitalen Spur wird in tabellarischer Form aufgeführt und ist nach ID-Typ organisiert.

Informationen zu Beziehungen abrufen

In einem Bericht zu einer digitalen Spur werden die Interaktionen zwischen einer *zentralen ID* und allen anderen IDs gezeigt. Bei einer *zentralen ID* handelt es sich um die ID, die in einem Sicherheitsverstoß von vorrangigem Interesse ist.

Die in vielen Kategorien am häufigsten vorkommende ID ist normalerweise die Identität der zentralen ID im betreffenden ID-Typ oder in der betreffenden ID-Kategorie. Wenn es sich bei der ID beispielsweise um eine MAC-Adresse handelt, gehört die E-Mail-Adresse mit den meisten Interaktionen wahrscheinlich zum verdächtigen Angreifer, dem der Computer gehört. Wenn IP-Adressen allerdings dynamisch zugeordnet werden, müssen Sie außerdem die IP-Adressen überprüfen, die während eines Zeitraums zugeordnet wurden.

Die Korrelationen zwischen anderen Kategorien und der zentralen ID sind normalerweise weniger stark. Bevor Sie auf Grundlage digitaler Spuren Maßnahmen ergreifen, sollten Sie die Daten anhand unabhängiger Quellen überprüfen. Verwenden Sie digitale Spuren, um den Radius einer Untersuchung auf weitere verdächtige Angreifer und Entitäten auszuweiten.

Beziehungen zum Aufzeichnen von Identitätsprotokollen überprüfen

Das Tool 'Digital Impression' stellt Beziehungen im Netz wieder her, damit Sie eine angreifende Entität und weitere Entitäten, mit denen diese kommuniziert, ermitteln können.

Das Tool 'Digital Impressions' zeigt die Häufigkeitsverteilung von korrelierten Ereignissen an. Es zeigt die Beziehungen zwischen Entitäten und erfasst die Anzahl der Beziehungen. Je höher die Anzahl, desto stärker die Beziehung. Wenn Sie beispielsweise die Beziehungen zwischen einer E-Mail-Adresse und anderen Entitäten anzeigen, können Sie sehen, wer mit wem kommuniziert. Sie können die der E-Mail-Adresse zugehörigen IP-Adressen, die von dem verdächtigen Element besuchten IP-Adressen und die anderen der E-Mail-Adresse zugeordneten Namen anzeigen.

In verteilten Implementierungen können Sie Beziehungen für einen Knoten in Ihrem Unternehmen anzeigen.

Vorgehensweise

1. Wählen Sie aus der Liste der Dokumente im Wiederherstellungsgitter ein Ergebnis aus und klicken Sie auf die Registerkarte **Digital Impression** (Digitale Spur).
2. Wählen Sie aus der Liste ein Element aus, das Sie untersuchen möchten.

   Der Bericht zur digitalen Spur wird standardmäßig in tabellarischer Form aufgeführt und ist nach ID-Typ organisiert. Es werden alle IDs angezeigt, die mit der zentralen ID interagieren. Die interagierenden IDs werden nach ID-Typ organisiert und sind nach der Häufigkeit der Interaktion sortiert.
3. Wenn eine ID für Sie von Interesse ist, wählen Sie diese aus.

Bei IDs handelt es sich um Hyperlinks und Sie können diese als zentrale ID eines anderen Berichts verwenden. Es wird eine weitere Registerkarte erstellt und die neue zentrale ID wird angezeigt. Sie können erkennen, mit wem ein angegebener verdächtiger Angreifer interagiert und mit wem die Interaktionen des verdächtigen Angreifers interagieren. Sie können den Radius einer Untersuchung auf weitere verdächtige Angreifer und Entitäten erweitern, mit denen diese interagieren.

4. Wenn Sie einen anderen Host anzeigen möchten, wählen Sie in der Liste **Select Remote Host** (Fernen Host auswählen) die entsprechende IP-Adresse aus.

   In verteilten Installationen können Sie den QRadar Incident Forensics-Host auswählen und anschließend die digitale Spur anzeigen. Die Standardansicht ist der primäre Host, aber Sie können jeden beliebigen sekundären Host auswählen, der QRadar Incident Forensics zugeordnet ist.
5. Wenn Sie eine Darstellung der Zuordnungen und Beziehungen für die Interaktionen der zentralen ID mit anderen IDs anzeigen möchten, klicken Sie auf die Registerkarte **Visualize Data** (Daten darstellen).

Visualisierungstool

Sie können Zuordnungen und Beziehungen in mehreren Attributen und Datenkategorien visuell untersuchen.

Im Fenster **Visualize** (Visualisieren) können Sie ein relationales Abbild der Metadaten für ein oder zwei Dokumente oder für eine große Auswahl an Dokumenten anzeigen. Bei der Verwendung einer großen Auswahl von Dokumenten erhält der Prüfer eine umfassende Ansicht der Beziehungen zwischen den Metadaten und deren relative Häufigkeit. Prüfer können diesen Pfaden anschließend folgen, um einen Sicherheitsverstoß weiter zu untersuchen.

Die Darstellung der ausgewählten Dokumente kann mit einer unterschiedlichen Relation einfach erneut erstellt werden, indem eine oder beide Beziehungen geändert werden.

Die Darstellung zeigt jede Beziehung innerhalb der ausgewählten Dokumente sowie die Häufigkeit der Beziehung auf. Jeder Knoten stellt einen eindeutigen Teil der Metadaten dar, auf die sich die ausgewählten Dokumente beziehen. Die Größe stellt die relative Häufigkeit im Vergleich mit anderen Knoten dar. Verknüpfungen zeigen die Verbindungen, die zwischen eindeutigen Teilen der Metadaten gefunden werden, sowie die Häufigkeit über die Größe. Prüfer können mit diesen Knoten mögliche Zugänge für eine weitere Untersuchung ermitteln.

Beziehungen und Zuordnungen darstellen

Im Fenster **Visualize** (Visualisieren) können Sie die Beziehungen zwischen Attributen in wiederhergestellten Dokumenten anzeigen. Sie können beispielsweise die E-Mail-Adressen überprüfen, die mit einer bestimmten E-Mail-Adresse kommuniziert haben.

Vorgehensweise

1. Aktivieren Sie im Gitter zur Wiederherstellung die Kontrollkästchen für die Dokumente, die Sie untersuchen möchten, und klicken Sie auf **Visualize** (Visualisieren).
2. Wählen Sie das Layout, die Anzahl der anzuzeigenden Dokumente und die Beziehungen zwischen Attributen aus, die Sie anzeigen möchten, und klicken Sie anschließend auf 'Refresh' (Aktualisieren).

3. Verwenden Sie die Zoomsteuerung, um weniger oder mehr Details der Abbildung anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten, um eine neue Suche auszuführen oder den aktiven Filter zu ändern.

   Sie können diese Metadaten aus dem Kontextmenü zurückholen, um eine neue Suche auszuführen. Sie können auch den aktiven Filter ändern, um Metadaten ein- oder auszuschließen.

   Einschränkung: In einem einzigen **Visualize**-Fenster können bis zu 9999 Dokumente gleichzeitig angezeigt werden.

Artefaktanalyse für verdächtige oder schädliche Inhalte

Als Sicherheitsanalyst können Sie nach unentdeckt gebliebenen Bedrohungen suchen, indem Sie wiederhergestellte Artefakte wie Dateien und Bilder analysieren. Um Verbindungen zwischen Kollaborateuren und Artefakten zu erkennen, können Sie auch die Links zu und von diesen Dateien und Bildern untersuchen.

Beispiel - Suche nach der Quelle einer Attacke (Patient Null) mithilfe der Artefaktanalyse

John ist Sicherheitsanalyst bei Replay Industries. Mehrere Systeme wurden infiziert, obwohl alle Sicherheitsmaßnahmen aktiviert sind. Nachdem John die betroffenen Systeme identifiziert und unter Quarantäne gestellt hat, muss er herausfinden, wie die Systeme infiziert wurden und ob andere Assets auf ähnliche Weise kompromittiert sind.

Paketwiederherstellung von einer IP-Adresse

Ausgehend von den IP-Adressen und dem vermutlich betroffenen Zeitraum kann John mithilfe von QRadar Incident Forensics die relevanten Paketdaten wiederherstellen.

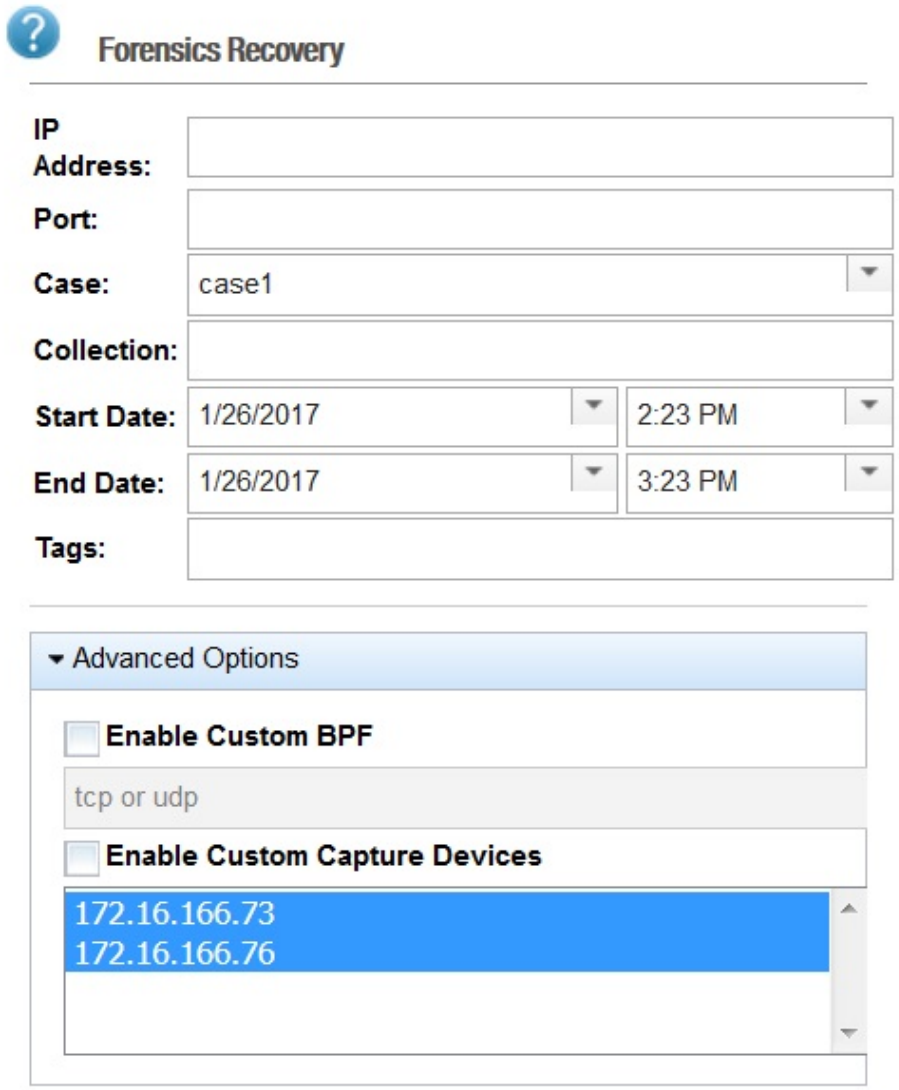


Abbildung 1. Wiederherstellung von einer IP-Adresse

Dateianalyse

Auf der Suche nach ausführbaren Inhalten setzt John zunächst die in QRadar Incident Forensics enthaltenen Dateianalysefunktionen ein. Er erhält eine Liste mit allen Dateien und ihren Entropiebewertungen sowie Angaben dazu, wie oft sie gesendet wurden und ob sie eingebettete Dateien oder Scripts enthalten. John fällt sofort eine Bilddatei auf, die QRadar Incident Forensics sowohl als Datei mit verdächtigem Inhalt als auch als Datei mit einem eingebetteten Skript markiert hat.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

Abbildung 2. Dateianalyseattribute

Die *Dateientropiebewertung*, die die Zufälligkeit von Daten misst und dazu dient, verschlüsselte Malware zu finden, sowie die Entropieverteilung zeigen deutlich,

dass ein Teil der Datei nicht das ist, was er sein sollte. Weitere Analysen bestätigen, dass die Datei eine neue Form von Malware enthält, die durch bestehende Sicherheitsmaßnahmen nicht entdeckt wurde und für die infizierten Systeme verantwortlich ist.

Im folgenden Diagramm dient die Entropie als Indikator der Variabilität von Bits pro Byte. Da jedes Zeichen in einer Dateneinheit aus 1 Byte besteht, gibt der Entropiewert die Variation der Zeichen und die Komprimierbarkeit der Dateneinheit an. Variationen bei den Entropiewerten in der Datei können darauf hinweisen, dass in Dateien verdächtige Inhalte versteckt sind. Beispielsweise können die hohen Entropiewerte ein Hinweis darauf sein, dass die Daten verschlüsselt und komprimiert gespeichert wurden, und die niedrigen Werte können ein Hinweis darauf sein, dass die Nutzdaten zur Laufzeit in verschiedenen Abschnitten verschlüsselt und gespeichert wurden.

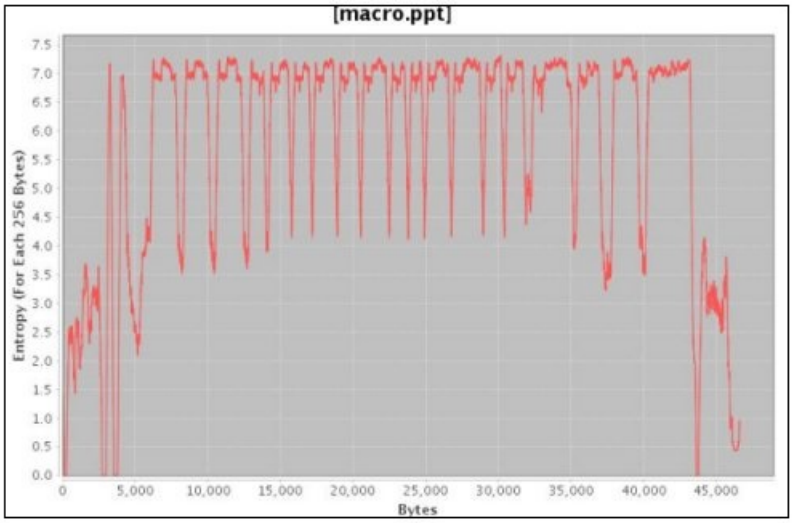


Abbildung 3. Beispiel einer Dateientropiegrafik, die eingebettete Scripts zeigt

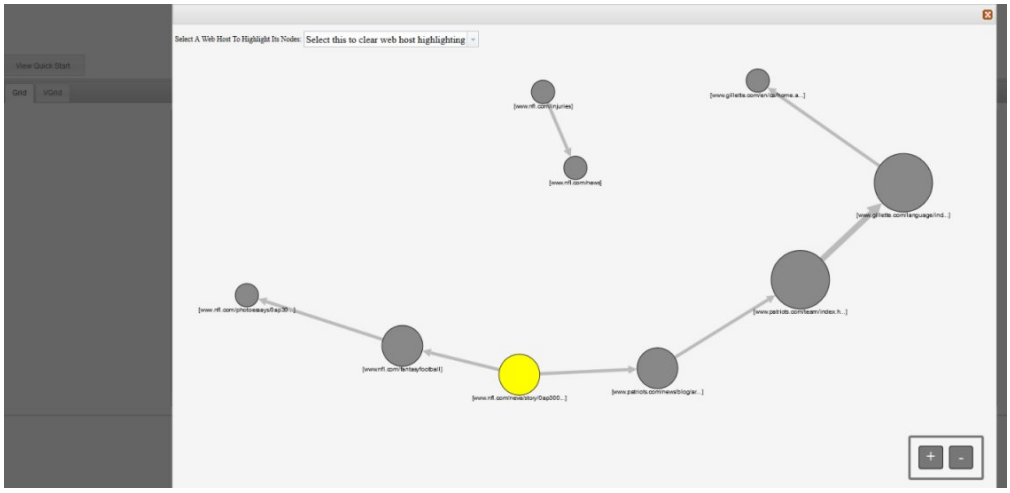
John muss jetzt ermitteln, woher die Datei kam und wer sonst sie noch haben könnte. Er findet mithilfe von QRadar Incident Forensics schnell den Web-Server, von dem die infizierte Bilddatei stammt. Die fragliche Webseite wird häufig besucht, weil sie die neuesten Nachrichten über die beliebtesten Fußballvereine verbreitet, und sie ist kompromittiert. Obwohl sich auf der Website viele Bilder befinden, war es nur dieses eine Bild, das John zuvor mithilfe der Dateianalyse gefunden hat, das die eingebettete Malware enthielt.

Linkanalyse zur Visualisierung der Websitekommunikation

Um zu ermitteln, welche anderen Systeme möglicherweise betroffen sind, nutzt John die Linkanalyse, um schnell alle Websites, die angezeigt wurden, zu visualisieren. Trotz des umfangreichen Datenverkehrs auf den Websites der Unternehmen, mit denen Replay Geschäfte macht, ist gegebenenfalls eine kleine Untermenge von Zugriffen auf den infizierten Web-Host deutlich erkennbar. John analysiert diese Links, um zu sehen, über welche anderen Server in seinem Netz auf den betreffenden Web-Host zugegriffen wurde.

Bei dieser Untersuchung nutzt John die Knoten in der Grafik, die für Webseiten stehen, und die Pfeile zwischen den Knoten, die die Beziehungen oder Transaktionen zwischen den Webseiten darstellen, um schnell Datenverkehrsmuster zu be-

werten und zu sehen, wie Dokumente traversiert wurden. Je größer der Knoten, desto mehr Links enthält der Pfad des Dokuments, und je größer der Linkpfeil, desto öfter wurde der Link benutzt.



Da es sich um eine beliebte Website für Fußballnachrichten handelte, war es keine Überraschung, dass mehrere andere Server mit dem Web-Host kommuniziert hatten und deshalb potenziell betroffen waren.

Bildanalyse

Um die Server einzugrenzen, die die schädliche Bilddatei heruntergeladen haben, wechselt John zur Bildanalyse und sieht sofort alle Bilddateien, die gesendet oder empfangen wurden.

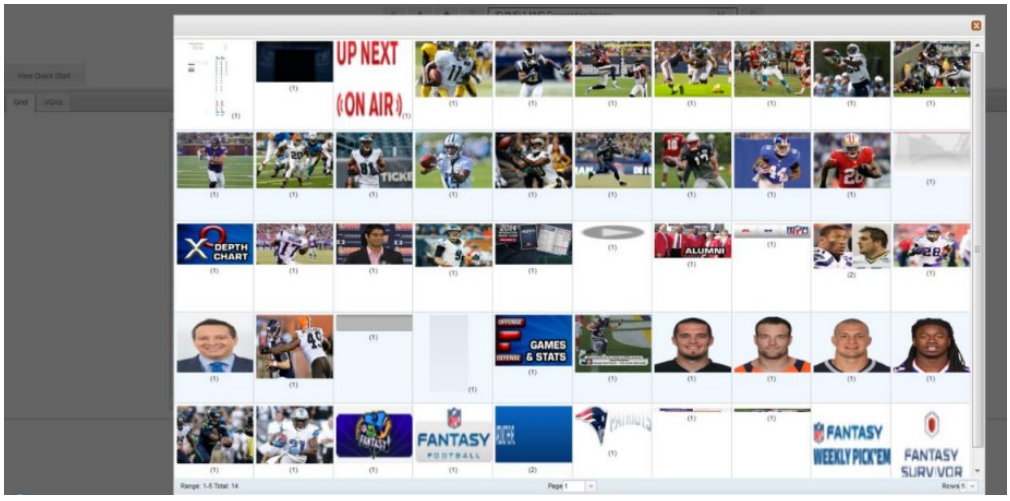


Abbildung 4. Beispiel für die Analyse und Verteilung von Bildern

John findet schnell heraus, dass alle infizierten Server sowie zwei Server, die er nicht in Verdacht hatte, auf die kompromittierte Bilddatei zugegriffen haben.

John stellt auch fest, dass mehrere der anderen Server, die auf dieselbe Website zugegriffen haben, die infizierte Datei nicht heruntergeladen haben. Er hat jetzt die Informationen, die er benötigt, um die beiden zusätzlichen Server unter Quarantäne zu stellen und einen neuen Datei-Hash für die infizierte Datei zu erstellen, den

Replay Industries hochladen und mit anderen in IBM X-Force Exchange teilen kann.

Dateien auf eingebetteten Inhalt und schädliche Aktivität analysieren

Um Dateien auf versteckte Bedrohungen zu untersuchen, können Sie Dateientropiewerte überprüfen, eingebettete Dateien und Scripts zur weiteren Analyse herunterladen und das Dokument und seine Attribute anzeigen.

Da Eindringlinge den Inhalt von binären Dateien innerhalb von Containerdateien verschleiern können, lässt sich mithilfe der Dateianalyse in IBM Security QRadar Incident Forensics prüfen, ob Dateien eingebettete Scripts oder sonstige binäre Inhalte aufweisen.

Dateientropie misst die Zufälligkeit von Daten in einer Datei und hilft dabei zu ermitteln, ob eine Datei versteckte Daten oder verdächtige Scripts enthält. Die Zufälligkeitsskala reicht von 0, nicht zufällig, bis 8, völlig zufällig, z. B. für eine verschlüsselte Datei. Je stärker eine Einheit komprimiert werden kann, desto niedriger der Entropiewert; je schlechter eine Einheit komprimiert werden kann, desto höher der Entropiewert.

Im folgenden Diagramm dient die Entropie als Indikator der Variabilität von Bits pro Byte. Da jedes Zeichen in einer Dateneinheit aus 1 Byte besteht, gibt der Entropiewert die Variation der Zeichen und die Komprimierbarkeit der Dateneinheit an. Variationen in den Entropiewerten in der Datei können darauf hinweisen, dass in Dateien verdächtige Inhalte versteckt sind. Beispielsweise können die hohen Entropiewerte ein Hinweis darauf sein, dass die Daten verschlüsselt und komprimiert gespeichert wurden, und die niedrigen Werte können ein Hinweis darauf sein, dass die Nutzdaten zur Laufzeit in verschiedenen Abschnitten verschlüsselt und gespeichert wurden.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Forensics** (Forensik) eine oder mehrere wiederhergestellte Dateien in der Ansicht **Grid** (Raster) aus.
2. Klicken Sie im Menü für Untersuchungswerkzeuge am Anfang des Rasters auf **File Analysis** (Dateianalyse).

   In den Ergebnissen enthält jede Zeile des Rasters Analysedaten für ein Dokument, z. B. Dateiname, Beschreibung, ob verdächtiger Inhalt erkannt wurde und Entropiewerte.
3. Wenn Sie Dateien nach einem bestimmten Attribut, z. B. Entropie, sortieren möchten, klicken Sie auf die entsprechende Spaltenüberschrift.
4. Klicken Sie in der Dateiliste mit der rechten Maustaste auf eine Datei, um sie näher zu untersuchen.
   - Klicken Sie auf **Display Document** (Dokument anzeigen), um das Dokument und seine Attribute zu überprüfen.
   - Klicken Sie auf **Display Entropy** (Entropie anzeigen), um eine Entropiegrafik zu überprüfen und um zu prüfen, ob eine eingebettete Datei oder ein eingebettetes Script möglicherweise Malware enthält.

     Entropiewerte können einen Hinweis darauf geben, ob die Datei möglicherweise schädlichen Inhalt enthält. Zum Beispiel sind ASCII-Textdateien normalerweise hoch komprimierbar und haben deshalb niedrige Entropiewerte.

Verschlüsselte Daten sind in der Regel nicht komprimiert und haben normalerweise einen hohen Entropiewert. Malware wird oft sowohl in Dateien als auch in Bildern gepackt und versteckt.

- Klicken Sie zum Herunterladen von eingebetteten Dateien auf **Extract Embedded Files** (Eingebettete Dateien extrahieren) und wählen Sie die gewünschten Dateien aus.

  Diese Option ist nur für Dokumente mit eingebetteten Dateien oder Scripts verfügbar. Dateien werden an die in Ihrem Web-Browser eingestellte Speicherposition für Downloads heruntergeladen. Öffnen Sie potenziell schädliche Scripts nicht in einer ungeschützten Umgebung.

Bilder auf versteckte Bedrohungen oder verdächtige Aktivität analysieren

Angezeigte Bilder werden nach Größe und Relevanz mit einer Häufigkeitszahl in Klammern sortiert. Diese Analyse kann hilfreich sein, wenn ein Mitarbeiter Unternehmensressourcen nutzt, um unzweckmäßige, eingeschränkte oder verbotene Bilder zu betrachten. Dabei kann es sich zum Beispiel um Bilder von Flugzeugen, bestimmten Gebäuden oder Orten handeln, die Ziele für Sicherheitsverstöße sein können.

Mit der Bildanalyse können Sie die wichtigsten Bilder aus einem oder mehreren Dokumenten in einer oder mehreren Paketaufzeichnungsdateien in einer einzigen Anzeige betrachten, statt jedes Dokument einzeln öffnen und die Bilder anzeigen zu müssen.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Forensics** (Forensik) ein oder mehrere Dokumente, in deren Beschreibung ein Bild enthalten ist, in der Ansicht **Grid** (Raster) aus.
2. Klicken Sie im Menü für Untersuchungswerkzeuge am Anfang des Rasters auf **Image Analysis** (Bildanalyse).

   In den Ergebnissen werden Piktogrammversionen aller Bilder, die in den Dokumenten enthalten sind, nach Relevanz angezeigt. Die Zahl in Klammern neben dem Bild gibt die Anzahl der Instanzen des Bildes im Dokument an. Wenn Sie den Cursor auf ein Piktogramm setzen, wird das Bild vergrößert.
3. Klicken Sie mit der rechten Maustaste auf ein Bild, um es weiter zu untersuchen.
   - Klicken Sie auf **Display Document** (Dokument anzeigen), um das Bild und seine Attribute zu überprüfen.
   - Klicken Sie auf **Display Entropy** (Entropie anzeigen), um eine Entropiegrafik zu überprüfen und um zu prüfen, ob das Bild möglicherweise Malware enthält.

     Entropiewerte können einen Hinweis darauf geben, ob die Datei möglicherweise schädlichen Inhalt enthält. Zum Beispiel sind Bitmapbilddateien und ASCII-Textdateien normalerweise hoch komprimierbar und haben deshalb niedrige Entropiewerte. Verschlüsselte Daten sind in der Regel nicht komprimiert und haben normalerweise einen hohen Entropiewert. Malware wird oft sowohl in Dateien als auch in Bildern gepackt und versteckt.

Links für Verbindungen und Beziehungen analysieren

In der Linkanalyse zeigen die Links die Gemeinsamkeit zwischen den aufgerufenen Websites an. Bei Untersuchungen von Sicherheitsvorfällen können Sie schnell erkennen, wo es Überschneidungen gibt und wie Personen kommunizieren.

Wenn Sie beispielsweise glauben, dass Tätergruppen zusammenarbeiten, aber nicht wissen wie, können Sie Dokumente von mehreren Benutzern überprüfen und mithilfe der Linkanalyse gemeinsame Webseiten anzeigen. Anschließend können Sie bestimmte Websites untersuchen.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Forensics** (Forensik) eine oder mehrere Webseiten in der Ansicht **Grid** (Raster) aus.
2. Klicken Sie im Menü für Untersuchungswerkzeuge am Anfang des Rasters auf **Link Analysis**.

   Wenn es eine Beziehung zwischen Websites gibt, zeigt eine Cytoscape-Grafik die Webseiten als Kreise (Knoten) sowie Links zu und von den Webseiten als Pfeile an. Je größer der Knoten, desto mehr Links enthält der Pfad des Dokuments, und je größer der Linkpfeil, desto öfter wurde der Link benutzt. Ausgewählte Knoten werden gelb dargestellt.
3. Wenn Sie die Kommunikation von einem bestimmten Web-Host untersuchen möchten, wählen Sie den Web-Host in der Liste **Select Web Host** (Web-Host auswählen) aus.

   Die Knoten, die für die Webseiten von dem ausgewählten Web-Host stehen, werden als dunkelgraue Kreise hervorgehoben.
4. Über die Steuerelemente für Vergrößern (+) und Verkleinern (-) können Sie die Kreise (Knoten) und Pfeile vergrößern oder verkleinern.

   Sie können auch das Mausrad auf- oder abwärts drehen, um die Knoten und Pfeile zu vergrößern oder zu verkleinern.
5. Durch Anklicken und Ziehen können Sie einen oder mehrere Knoten verschieben.

   Sie können die gesamte Grafik verschieben, indem Sie irgendwo auf den Hintergrund klicken und sie dann durch Halten und Ziehen verschieben.

Wiederherstellung von der Seite Attributes eines Dokuments ausführen

Auf der Registerkarte **Attributes** (Attribute) eines Dokuments können Sie eine Wiederherstellung für eine IP-Adresse oder einen Port ausführen.

Vorgehensweise

1. Führen Sie auf der Seite **Search** (Suche) der Registerkarte **Forensics** (Forensik) eine Suche aus.
2. Klicken Sie in der Liste der zurückgegebenen Dokumente auf ein Dokument, um es zu öffnen.
3. Klicken Sie auf die Registerkarte **Attributes** (Attribute).
4. Klicken Sie auf eine IP-Adresse oder einen Port.
5. Klicken Sie im Menü auf **Run Recovery for** (Wiederherstellung ausführen für).

Kapitel 5. Netzverkehr für eine IP-Adresse überprüfen

Für die Anzeige der relevanten Inhalte des Datenaustauschs, der während eines Sicherheitsverstoßes auftrat, können Sie Netzverkehr, der einer IP-Adresse zugeordnet ist, wiederherstellen. Sie können auch vorhandene Fälle, die einen Bezug zu einer IP-Adresse haben, durchsuchen.

Wenn der Netzverkehr aus einer IP-Adresse wiederhergestellt wird, wird ein Vorfall erstellt. Die Prüfer können eine Folge von Ereignissen aus dem Sicherheitsverstoß visualisieren oder die Dokumente im Vorfall anzeigen.

In IBM Security QRadar Incident Forensics wird ein Index aller verfügbaren Netzdaten, Dateidaten, Metadaten und Zeichen erstellt, die sich in jeder wiederhergestellten Datei befinden.

In verteilten Implementierungen erfassen mehrere Aufzeichnungseinheiten und QRadar Incident Forensics-Hosts Daten und verarbeiten diese. Sie können die zusammengefassten Ergebnisse der Wiederherstellung eines Vorfalls oder Ergebnisse nach Host und Aufzeichnungseinheit anzeigen.

Vorgehensweise

1. Wenn Sie einen Fall erstellen und Daten von der Paketaufzeichnungseinheit abrufen möchten, klicken Sie in QRadar mit der rechten Maustaste auf eine IP-Adresse und wählen Sie **Run Forensics Recovery** (Forensikwiederherstellung ausführen) aus, oder klicken Sie auf das Symbol für die Forensikwiederherstellung  .
   a. Stellen Sie die Parameter der Forensikwiederherstellung ein. Orientieren Sie sich dabei an den folgenden Informationen:

Tabelle 5. Parameter für die Forensikwiederherstellung

Parameter	Beschreibung
IP-Adresse	Bei Eingabe mehrerer IP-Adressen müssen Sie diese durch Kommas trennen. Fehlt die Angabe von IP-Adresse oder Port, wird der Standard TCP- oder UDP-Port verwendet.
Port	Bei Eingabe mehrerer Ports müssen Sie diese durch Kommas trennen.
Fall	Der Fallname muss eindeutig sein.
Datensammlung	Wiederhergestellte Daten werden in einer Datensammlung gruppiert und dem Fall zugeordnet. Der Name der Datensammlung muss eindeutig sein. Wenn der Name der Datensammlung im Fall vorhanden ist, wird die ursprüngliche Datensammlung gelöscht.
Tags	Optional. Zum schnellen Abrufen exakter Ergebnismengen aus relevanten Dokumenten. Bei Eingabe mehrerer Tags müssen Sie diese durch Kommas trennen. Zulässig sind nur alphanumerische Zeichen, keine Sonderzeichen.

Tabelle 5. Parameter für die Forensikwiederherstellung (Forts.)

Parameter	Beschreibung
Enable Custom BPF (Berkeley Packet Filter) (Angepassten BPF (Berkeley Packet Filter) aktivieren)	Nur verfügbar für Administratoren. Wenn Sie das Kontrollkästchen auswählen, wird ein BPF-Eingabefeld aktiviert, in dem Sie eine IP-Adresse und einen Port angeben können.
Enable Custom Capture Devices (Angepasste Aufzeichnungseinheiten aktivieren)	Nur verfügbar für Administratoren. Wenn Sie das Kontrollkästchen auswählen, wird die Liste der PCAP-Einheiten in Ihrer Implementierung generiert. Wählen Sie eine oder mehrere Einheiten aus, damit nur der Datenverkehr aus diesen Einheiten angezeigt wird.

b. Klicken Sie auf **OK** und anschließend auf die Registerkarte **Forensics**.

   Fehlerbehebung: Wenn die Nachricht angezeigt wird, dass Sie nicht zur Wiederherstellung der Daten berechtigt sind, müssen Sie sicherstellen, dass Ihr Sicherheitsprofil Zugriff auf die IP-Adresse hat. Diese Nachricht kann in einigen Fällen angezeigt werden, wenn Sie im Feld **Tags** das Zeichen # angegeben haben.

c. Klicken Sie auf das Symbol für Vorfälle  , um Ihre Vorfälle anzuzeigen. Beim Navigieren durch die Hierarchie können Sie die Inhalte erweitern und wieder schließen.

d. Zum Anzeigen der Dokumente im Vorfall klicken Sie auf **Jump to search page results** (Zu Ergebnissen der Suchseite wechseln).

e. Zum Visualisieren einer Folge von Ereignissen für den Vorfall klicken Sie auf **Jump to surveyor page results** (Zu den Ergebnissen der Surveyor-Seite wechseln).

f. Zum Entfernen oder Abbrechen eines bestimmten Vorfalls klicken Sie auf **Delete or cancel this incident** (Vorfall löschen oder abbrechen).

g. Zur erneuten Ausführung des zuvor ausgeführten Forensikwiederherstellungsjobs klicken Sie auf **Re-run this forensics recovery** (Forensikwiederherstellung wiederholen). Beispielsweise können Sie eine Forensikwiederherstellung wiederholen, wenn eine Ausführung unvollständige Daten zurückgibt. Sie können dann zum Beispiel andere IP-Adressen eingeben oder den Zeitrahmen gegenüber dem vorherigen Job ändern.

2. Wenn Sie in QRadar vorhandene Fälle durchsuchen möchten, klicken Sie mit der rechten Maustaste auf eine IP-Adresse und wählen Sie dann **Run Forensics Search** (Forensiksuche ausführen) aus.
   a. Klicken Sie auf der Registerkarte **Forensics** auf das Symbol für Vorfälle.
   b. Um eine Anhäufung der Aktivitäten zu untersuchen, die einem Vorfall zugeordnet sind, heben Sie einen Fall hervor, indem Sie den Mauszeiger darüber bewegen, und klicken anschließend auf das Suchsymbol.
   c. Um Aktivitäten nach QRadar Incident Forensics-Host und Aufzeichnungseinheit in verteilten Implementierungen zu untersuchen, erweitern Sie den Eintrag **Case** (Fall) und anschließend den Eintrag **Collection** (Datensammlung).
   d. Zur Anzeige einer chronologischen Liste der Interaktionen in einem Vorfall heben Sie die Datensammlung hervor, indem Sie die Maustaste darüber bewegen, und klicken Sie anschließend auf das Surveyor-Symbol.

Zugehörige Konzepte:

„Wiederhergestellte Dokumentansicht" auf Seite 29
Auf der Registerkarte **Ansicht** wird eine wiederhergestellte Ansicht des Dokuments angezeigt, das auf der linken Seite des Bildschirms in der Ansicht 'Liste' ausgewählt wird.

Benutzerdefinierter BPF-Filter

Wenn Sie bei der Ausführung einer Forensikwiederherstellung nur bestimmte Datenverkehrstypen anzeigen möchten, können Sie einen benutzerdefinierten BPF-Filter (BPF) verwenden.

Wenn Sie das betreffende Kontrollkästchen auf der Registerkarte **Forensics Recovery** (Forensikwiederherstellung) auswählen, wird ein BPF-Eingabefeld aktiviert, in dem Sie einen BPF-Filter für die Filterung des Netzverkehrs angeben können.

Zur Angabe von BPF-Filtern verwenden Sie die BPF-Syntax. Ein Ausdruck in dieser Syntax besteht aus einem oder mehreren Primitives (Basiselementen). Primitives sind Verweise auf ein oder mehrere Felder in einem Netzprotokollheader. 'host', 'port' und 'tcp port' sind beispielsweise Primitives. Mittels der Operatoren AND, OR und NOT können Sie daraus komplexe Filterausdrücke erstellen.

Hier einige Filterbeispiele:

```
host 10.0.0.1
port 80
tcp port 80 and host 10.0.0.1
host 10.0.0.1 or host 10.0.0.2 or port 80 or port 443
```

Für die Erstellung eines benutzerdefinierten BPF-Filters benötigen Sie die Berechtigungen einer Administratorrolle. Benutzer ohne die Berechtigungen eines Administrators haben lediglich Lesezugriff auf das Textfeld des BPF-Filters. Benutzer mit Administratorberechtigungen können BPF-Ausdrücke auch eingeben.

Einschränkung: Bei der Forensikwiederherstellung wird die bereitgestellte BPF-Eingabe berücksichtigt. Falls die Ergebnisse einer Wiederherstellung nicht Ihren Erwartungen entsprechen, überprüfen Sie nicht nur die Wiederherstellungseinstellungen, sondern auch die BPF-Einstellungen.

Auch wenn vom BPF-Filter nicht verwendet, enthält das BPF-Feld immer den Inhalt des Felds **IP Address** (IP-Adresse) bzw.**Port**. Fehlt die Angabe von IP-Adresse oder Port, so verwendet der benutzerdefinierte BPF-Filter den Standard-TCP- oder UDP-Port.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Défense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter als IBM werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation

North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die Leistungsdaten und Kundenbeispiele dienen allein der Veranschaulichung. Die tatsächliche Leistung ist von der jeweiligen Konfiguration und den Betriebsbedingungen abhängig.

Alle Informationen zu Produkten anderer Anbieter als IBM stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit den Namen real existierender Einzelpersonen oder Unternehmen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Nutzungsbedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Rechte

Abgesehen von den hier gewährten Rechten werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

IBM Online-Datenschutzerklärung

IBM Software-Produkte, einschließlich "Software as a Service"-Lösungen (Softwareangebote) verwenden möglicherweise Cookies oder andere Technologien, um Nutzungsinformationen zum Produkt zu erfassen, die Erfahrung der Endbenutzer zu verbessern, Interaktionen mit dem Endbenutzer zu optimieren usw. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nach implementierten Konfigurationen verwendet dieses Softwareangebot auch Sitzungscookies, die zum Zwecke der Sitzungsverwaltung und Authentifizierung die Sitzungs-IDs der Benutzer aufzeichnen. Diese Cookies können inaktiviert werden. Dadurch wird aber zugleich die durch die Cookies bereitgestellte Funktionalität inaktiviert.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der "IBM Online-Datenschutzerklärung, Schwerpunkte" unter http://www.ibm.com/privacy, in der "IBM Online-Datenschutzerklärung" unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" sowie im "IBM Software Products and Software-as-a Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Glossar

Dieses Glossar enthält Begriffe und Definitionen für die IBM Security QRadar Incident Forensics-Software und -Produkte.

In diesem Glossar werden folgende Querverweise verwendet:

- *Siehe* verweist von einem nicht bevorzugten Begriff auf den bevorzugten Begriff oder von einer Abkürzung auf den ausgeschriebenen Begriff.
- *Siehe auch* verweist auf einen verwandten oder entgegengesetzten Begriff.

Weitere Begriffe und Definitionen finden Sie auf der IBM Terminology-Website (wird in einem neuen Fenster geöffnet).

„A" „B" „D" „E" auf Seite 50 „F" auf Seite 50 „H" auf Seite 50 „I" auf Seite 50 „K" auf Seite 50 „M" auf Seite 50 „P" auf Seite 50 „S" auf Seite 50 „U" auf Seite 51 „V" auf Seite 51 „W" auf Seite 51 „Z" auf Seite 51

A

Angreifer
Ein Benutzer (Mensch oder Computerprogramm), der versucht, einem Informationssystem Schaden zuzufügen oder auf nicht für den allgemeinen Zugang vorgesehene Informationen zuzugreifen. Siehe auch Attacke.

Angriff
Eine aufgrund einer überwachten Bedingung gesendete Nachricht oder ein aus dem gleichen Grund generiertes Ereignis. Ein Angriff liefert beispielsweise Informationen darüber, ob gegen eine Richtlinie verstoßen wurde oder ob das Netz angegriffen wird.

Anomalie
Eine Abweichung vom erwarteten Verhalten des Netzes.

Attacke
Jeder Versuch eines Unbefugten, den Betrieb eines Softwareprogramms oder vernetzten Systems zu beeinträchtigen. Siehe auch Angreifer.

Audit-Trail
Digitale Spuren, die in einen Fall involvierte Personen mit Personen außerhalb des Falls verbinden.

Aufzeichnungseinheit
Siehe Paketaufzeichnungseinheit.

B

Beziehung digitaler Spuren
Eine Beziehung zwischen mit Tags versehenen IDs in Bezug auf einen Fall.

Boolescher Operator
Eine integrierte Funktion, die bei der Auswertung von Operationsgruppen eine logische Operation vom Typ AND, OR oder NOT angibt. Boolesche Operatoren sind die Zeichen &&, || und !.

D

Datenflussaufzeichnung
Eine Aufzeichnung des Dialogs zwischen zwei Hosts.

Datensammlung
Eine bestimmte benannte Gruppe von Daten, die einem Fall zugeordnet sind. Dies kann beispielsweise eine geordnete Gruppe von erfassten Netzpaketen sein.

Datenverkehr
In der Datenübertragung die Datenmenge, die ab einem bestimmten Punkt in einem Pfad übertragen wird.

Decapping
Der Prozess, bei dem Paketaufzeichnungsdaten dekompiliert werden, damit alle erfassten Daten zu einem Ergebnisbericht verarbeitet werden.

Dialog
Ein forensisch wiederhergestellter Datenfluss zwischen zwei oder mehreren Endpunkten in einem Netz. Dies kann zum Beispiel ein Dialog in einem sozialen Netzwerk sein.

Digitale Spur
Ein Bericht, der aus mit Tags versehenen

IDs besteht, die innerhalb eines einzelnen Falls in Verbindung zueinander stehen.

Domänenprüfer
Ein spezialisiertes Prüfprogramm, das dazu entwickelt wurde, forensische Daten von bestimmten Domänen-Websites, z. B. Facebook oder Gmail, zu zerlegen und zu extrahieren.

E

Erfasster Netzverkehr
Aufgezeichneter Netzverkehr, der durch den forensischen Decapping-Prozess verarbeitet wurde.

F

Fall Die in einer Datenbank enthaltenen Informationen, die eine bestimmte Untersuchung betreffen.

Forensischer Prüfer
Der Benutzer, der relevante Daten aus dem Netzverkehr und aus Dokumenten in das Forensikrepository extrahiert.

H

Hauptlink
Ein Webschnittstellenelement, das die Position des Benutzers innerhalb einer Site anzeigt. Dabei handelt es sich normalerweise um eine Folge von Hyperlinks am oberen oder unteren Rand der Seite. Die Links geben angezeigte Seiten an und ermöglichen es dem Benutzer, zurück zum Ausgangspunkt zu navigieren.

Hypothese
Eine angenommene Erklärung für einen Vorfall, die auf den verfügbaren in einem Fall gesammelten Beweisen basiert. Eine Hypothese muss überprüfbar und falsifizierbar sein.

I

Identität
Eine Sammlung von Attributen aus einer Datenquelle, die eine Person, ein Unternehmen, einen Bereich oder ein Element darstellen.

K

Kategorie
Eine Gruppe von Elementen, die gemäß einer bestimmten Beschreibung oder Klassifizierung gruppiert wurden. Kategorien können unterschiedliche Informationsebenen innerhalb einer Dimension sein.

Kontinuierlich erfasste elektronische Anwesenheit Die Onlineidentität eines Angreifers in Form einer Sammlung von digitalen Spuren, die verlinkt sind.

M

Metadaten
Daten, die die Merkmale von Daten beschreiben; beschreibende Daten.

P

Paketaufzeichnungseinheit
Eine eigenständige Einheit, die Verkehrsdaten abfängt und protokolliert.

Paketaufzeichnungsinformationen
Die Verkehrsdateninformationen, die von einer Aufzeichnungseinheit erfasst werden.

Protokollprüfer
Ein spezialisiertes Prüfprogramm, das dazu entwickelt wurde, forensische Daten aus Netzprotokollen wie HTTP oder FTP zu extrahieren.

S

Schwachstelle
Ein Sicherheitsrisiko in einer Betriebssystem-, Systemsoftware- oder Anwendungssoftwarekomponente.

Sicherheitsverstoß
Ein Ereignis, bei dem der normale Netzbetrieb gestört, beeinträchtigt oder angegriffen wird.

Surveyor
Ein Tool, das die chronologische Folge von Aktivitäten in einem Sicherheitsverstoß in einer Visualisierungskomponente anzeigt.

U

Übergeordneter Datenfluss
Ein einzelner Datenfluss, der aus mehreren Datenflüssen mit ähnlichen Eigenschaften besteht, um die Verarbeitungskapazität durch eine Verringerung der Speicherbeschränkungen zu erhöhen.

V

Verschlüsselung
In der IT-Sicherheit der Prozess zur Umwandlung von Daten in ein nicht verständliches Format, sodass die ursprünglichen Daten entweder gar nicht oder nur mithilfe eines Entschlüsselungsprozesses erhalten werden können.

Vorfall
Siehe Sicherheitsverstoß.

W

Wiederherstellungsjob
Ein Prozess, der abgefragte Aufzeichnungsdaten wiederherstellt und zur Erfassung an die Decapper-Einheit weiterleitet.

Z

Zentrale ID
Das Kategorieelement, mit dem alle anderen IDs interagiert haben. Die zentrale ID ist das zentrale Element in einer Untersuchung.

Zuordnung relationaler Metadaten
Eine Zuordnung, die zusammengehörige Metadaten aus Falldokumenten anzeigt.

Index