RSA NETWITNESS® SUITE

Konfigurationsleitfaden Malware Analysis

für Version 11.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2018

Inhalt

Funktionsweise von Malware Analysis

NetWitness Suite Malware Analysis ist eine automatisierte Verarbeitungssoftware zur Analyse von Schadsoftware, die bestimmte Typen von Dateiobjekten analysiert (z. B. Windows PE, PDF und MS Office), um die potenzielle Schädlichkeit einer Datei zu bewerten.

Malware Analysis erkennt Indikatoren für infizierte Dateien mit vier verschiedenen Analysemethoden:

- Netzwerksitzungsanalyse (Netzwerk)
- Statische Dateianalyse (Statisch)
- Dynamische Dateianalyse (Sandbox)
- Sicherheitscommunityanalyse (Community)

Jede dieser vier Analysemethoden ist so konzipiert, dass sie inhärente Schwachstellen der jeweils anderen ausgleicht. Die dynamische Dateianalyse erkennt zum Beispiel Zero-Day-Angriffe, die in der Phase der Sicherheitscommunityanalyse nicht erkannt werden. Indem bei der Schadsoftwareanalyse mehrere Methoden eingesetzt werden, werden nicht so viele falsche negative Ergebnisse erzeugt.

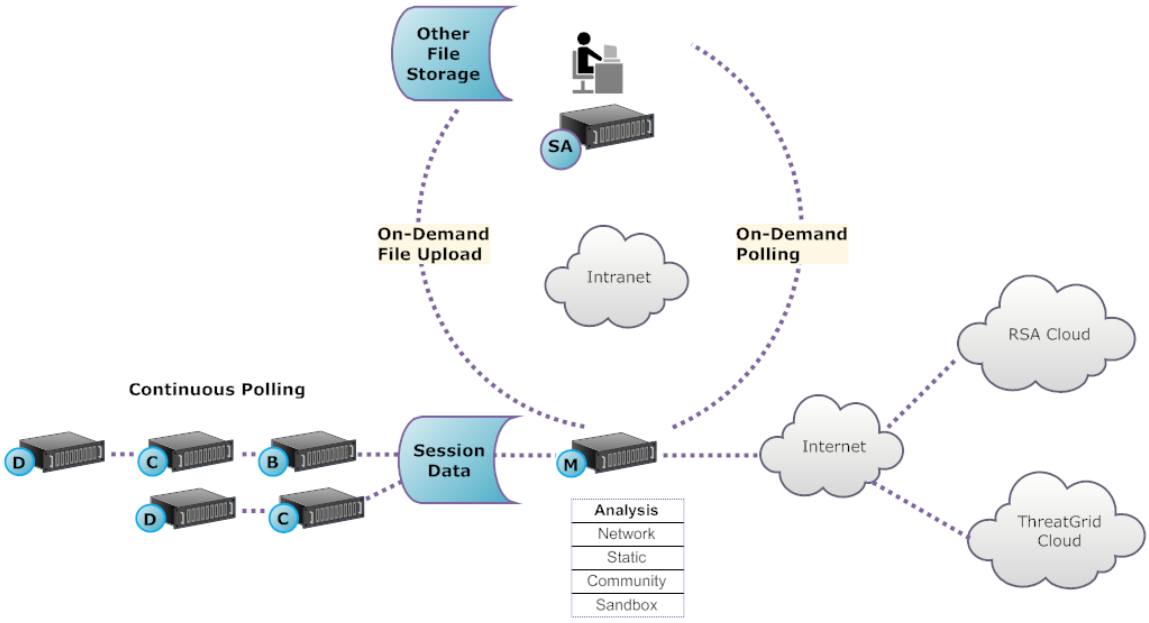
Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis auch in YARA geschriebene Indikatoren für eine Infizierung. YARA ist eine Regelsprache, die es Schadsoftwareforschern ermöglicht, Schadsoftwaremuster zu identifizieren und zu klassifizieren. Dies ermöglicht es IOC-Autoren, Erkennungsfunktionen zu RSA Malware Analysis hinzuzufügen, indem sie YARA-Regeln erstellen und in RSA Live veröffentlichen. Diese YARA-basierten IOCs in RSA Live werden automatisch heruntergeladen und in dem abonnierten Host aktiviert, um die bestehenden Analysen, die in jeder Datei durchgeführt werden, zu ergänzen.

Malware Analysis bietet auch Funktionen, die Warnmeldungen für das Incident-Management unterstützen.

Funktionsübersicht

In dieser Abbildung ist die funktionelle Beziehung zwischen den Core-Services (Decoder, Concentrator und Broker), dem Malware Analysis-Service und dem NetWitness-Server dargestellt.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



Der Malware Analysis-Service analysiert Dateiobjekte mit einer beliebigen Kombination der folgenden Methoden:

- **Kontinuierliche automatische Abfrage eines Concentrator oder Broker**, um Sitzungen zu extrahieren, die von einem Parser als potenziell mit Schadsoftware infiziert eingestuft werden
- **Abfrage eines Concentrator oder Broker nach Bedarf**, um Sitzungen zu extrahieren, die von einem Schadsoftwareanalysten als potenziell mit Schadsoftware infiziert eingestuft werden
- **Hochladen von Dateien nach Bedarf** aus einem vom Benutzer definierten Ordner

Wenn der automatische Abruf eines Concentrator oder Broker aktiviert ist, extrahiert und priorisiert der Malware Analysis-Service fortlaufend ausführbaren Inhalt, PDF-Dokumente und Microsoft Office-Dokumente in Ihrem Netzwerk, die direkt von den erfassten Daten stammen und vom Core-Service analysiert werden. Da der Malware Analysis-Service eine Verbindung mit einem Concentrator oder Broker herstellt, um nur solche ausführbaren Dateien zu extrahieren, die als mögliche Schadsoftware markiert sind, ist der Prozess schnell und effizient. Dieser Prozess ist kontinuierlich und erfordert keine Überwachung.

Bei der bedarfsweisen Abfrage eines Concentrator oder Broker verwendet der Schadsoftwareanalyst Security Analytics Investigation, um sich die erfassten Daten genauer anzusehen und die zu analysierenden Sitzungen auszuwählen. Der Malware Analysis-Service nutzt diese Informationen, um den Concentrator oder Broker automatisch abzufragen und die angegebenen Sitzungen zur Analyse herunterzuladen.

Beim Hochladen von Dateien bei Bedarf kann der Analyst Dateien prüfen, die außerhalb der Core-Infrastruktur erfasst wurden. Die Schadsoftware wählt einen Ordnerspeicherort aus und identifiziert eine oder mehrere Dateien, die hochgeladen und von Malware Analysis analysiert werden sollen. Diese Dateien werden mithilfe derselben Methodik analysiert wie Dateien, die automatisch aus Netzwerksitzungen extrahiert werden.

Analysemethode

Für die Netzwerkanalyse sucht der Malware Analysis-Service ähnlich einem Analysten nach Merkmalen, die dem Anschein nach von der Norm abweichen. Durch die Untersuchung von Hunderten bis Tausenden von Merkmalen und eine Kombination der Ergebnisse in einem Bewertungssystem mit entsprechenden Gewichtungen werden harmlose Sitzungen, die zufälligerweise einige anormale Merkmale aufweisen, ignoriert, während die potenziell bedrohlichen Sitzungen hervorgehoben werden. Ein Benutzer kann die Muster erlernen, die auf eine anormale Aktivität in den Sitzungen hinweisen und einer weiteren Untersuchung bedürfen; diese Muster werden auch als Indikatoren für eine Infizierung bezeichnet.

Der Malware Analysis-Service kann statische Analysen von verdächtigen Objekten durchführen, die er im Netzwerk findet, und ermitteln, ob diese Objekte schädlichen Code enthalten. Bei der Communityanalyse wird neue im Netzwerk entdeckte Schadsoftware in die RSA-Cloud übertragen, um sie anhand der RSA-Daten zur Schadsoftwareanalyse und der Feeds vom SANS Internet Storm Center, von SRI International, vom US-Finanzministerium und von VeriSign zu prüfen. Für Sandbox-Analysen können die Services auch Daten mittels Push an die wichtigen SIEM-Hosts (Security, Information and Event Management) übertragen (die ThreatGrid-Cloud).

Malware Analysis verfügt über eine einzigartige Methode für die Analyse, bei der mit führenden Unternehmen und Experten der Branche zusammengearbeitet wird, die mit ihren Technologien das Bewertungssystem von Malware Analysis ideal ergänzen.

NetWitness-Server Zugreifen auf den Malware Analysis-Service

Der NetWitness-Server wird so konfiguriert, dass er eine Verbindung mit dem Malware Analysis-Service herstellen und markierte Daten für eine tiefer gehende Analyse in Investigation importieren kann. Der Zugriff erfolgt auf Basis auf drei Abonnementebenen.

- Kostenloses Abonnement: Alle NetWitness Suite-Kunden verfügen über ein kostenloses Abonnement, das sie über einen Schlüssel für eine kostenlose Testversion der ThreatGrid-Analyse nutzen können. Die Rate des Malware Analysis-Services ist auf 100 Dateistichproben pro Tag begrenzt. Die Anzahl der Stichproben (aus den oben beschriebenen Dateigruppen), die für die Sandbox-Analyse an die ThreatGrid-Cloud übertragen werden kann, ist hierbei auf 5 pro Tag begrenzt. Wenn eine Netzwerksitzung 100 Dateien aufweist, würde das Limit nach Verarbeitung dieser einen Netzwerksitzung bereits

erreicht sein. Wenn 100 Dateien manuell hochgeladen werden, würde das Limit ebenfalls erreicht sein.

- Standardabonnement: Die Anzahl der Übertragungen an den Malware Analysis-Service ist unbegrenzt. Die Anzahl an Stichproben, die zur Sandbox-Analyse an die ThreatGrid Cloud übermittelt werden, beläuft sich auf 1.000 pro Tag.
- Enterprise-Abonnement: Die Anzahl der Übertragungen an den Malware Analysis-Service ist unbegrenzt. Die Anzahl an Stichproben, die an die ThreatGrid Cloud zur Sandbox-Analyse übermittelt wurden, beläuft sich auf 5.000 pro Tag.

Bewertungsmethode:

Standardmäßig werden die Indikatoren für eine Infizierung (Indicators of Compromise, IOC) anhand von Branchen-Best-Practices gewichtet. Während der Analyse führen die ausgelösten IOCs dazu, dass die Bewertung ansteigt oder reduziert wird. Dies gibt die Wahrscheinlichkeit an, ob die Stichprobe schädlich ist. Die Gewichtung der IOCs ist in NetWitness Suite einsehbar, sodass der Schadsoftwareanalyst selbst entscheiden kann, ob die zugeordnete Bewertung ignoriert werden soll oder ob ein IOC komplett aus der Bewertung herausgenommen werden soll. Der Analyst hat die Flexibilität, entweder die standardmäßige Gewichtung zu verwenden oder die Gewichtung vollständig an bestimmte Anforderungen anzupassen.

YARA-basierte IOCs werden mit den integrierten IOCs in jeder integrierten Kategorie verschachtelt und lassen sich nicht von den systemeigenen IOCs unterscheiden. Bei der Anzeige von IOCs in der Servicekonfigurationsansicht können Administratoren YARA in der Auswahlliste „Modul“ auswählen, um eine Liste der YARA-Regeln einzusehen.

Nachdem eine Sitzung in NetWitness Suite importiert wurde, stehen alle Anzeige- und Analysefunktionen in Investigation zur Verfügung, um die Indikatoren für eine Infizierung genauer zu analysieren. Bei der Anzeige in Investigation werden YARA-IOCs von den integrierten IOCs durch das Tag `Yara rule.` unterschieden.

Bereitstellung

Der Malware Analysis-Service wird als separater RSA Malware Analysis-Host bereitgestellt. Der dedizierte Malware Analysis-Host verfügt über einen integrierten Broker, der eine Verbindung mit der Core-Infrastruktur herstellt (entweder ein anderer Broker oder ein Concentrator). Vor dieser Verbindung müssen den Decoders, die mit den Concentrators und Brokers verbunden sind, von denen der Malware Analysis-Service Daten abruft, eine Reihe von Parsern und Feeds hinzugefügt werden. Auf diese Weise können verdächtige Datendateien zur Extraktion markiert werden. Der Inhalt dieser Dateien ist mit dem Tag `malware analysis` gekennzeichnet und steht über das RSA Live-Contentmanagementsystem zur Verfügung.

Bewertungsmodule

RSA NetWitness Suite Malware Analysis analysiert und wertet Sitzungen und die integrierten Dateien in diesen Sitzungen anhand von vier Kategorien aus: Netzwerk, Statische Analyse, Community und Sandbox. Jede Kategorie umfasst viele einzelne Regeln und Prüfungen, die verwendet werden, um eine Punktzahl zwischen 1 und 100 zu berechnen. Je höher die Punktzahl, desto wahrscheinlicher enthält die Sitzung Schadsoftware und desto eher wird sich eine detaillierte Folgeermittlung lohnen.

Malware Analysis kann Untersuchungen des Verlaufs von Ereignissen vereinfachen, die zu einem Netzwerkalarm oder Incident führen. Wenn Sie wissen, dass eine bestimmte Art von Aktivität in Ihrem Netzwerk stattfindet, können Sie nur die in Frage kommenden Berichte auswählen, um den Content von Datensammlungen zu überprüfen. Sie können auch das Verhalten für jede Auswertungskategorie basierend auf der Auswertungskategorie oder dem Dateityp (Windows PE, PDF und Microsoft Office) ändern.

Sobald Sie sich mit Datennavigationsmethoden vertraut gemacht haben, können Sie die Daten vollständiger untersuchen, indem Sie Folgendes tun:

- Suchen nach bestimmten Arten von Informationen
- Überprüfen bestimmten Contents im Detail.

Kategorieauswertungen für Netzwerk, Statische Analyse, Community und Sandbox werden unabhängig voneinander verwaltet und berichtet. Wenn Ereignisse basierend auf den unabhängigen Auswertungen angezeigt werden, geht aus dem Analyseabschnitt hervor, sobald eine Kategorie Schadsoftware entdeckt.

Netzwerk

Die erste Kategorie überprüft jede Core-Netzwerksitzung, um zu ermitteln, ob die Bereitstellung der Schadsoftwarekandidaten verdächtig war. Beispielsweise gilt eine gutartige Software, die von einer bekannten sicheren Website mithilfe geeigneter Ports und Protokolle heruntergeladen wird, als weniger verdächtig als eine als gefährlich bekannte Software von einer als zweifelhaft bekannten Downloadsite. Die Beispielfaktoren, die bei der Auswertung dieses Kriterienkatalogs verwendet werden, können Sitzungen enthalten, die:

- Bedrohungsfeedinformationen enthalten
- Sich mit wohlbekannten gefährlichen Websites verbinden
- Sich mit Domains/Ländern mit hohem Risiko verbinden (z. B. einer .cc-Domain)
- Wohlbekannte Protokolle auf nicht standardmäßigen Ports verwenden
- Getarntes JavaScript verwenden

Statische Analyse

Die zweite Kategorie analysiert jede Datei in der Sitzung auf Anzeichen einer Tarnung, um die Wahrscheinlichkeit vorherzusagen, dass sich die Datei schädlich verhalten wird, sobald sie ausgeführt wird. Beispielsweise wird eine Software, die sich mit Netzwerkbibliotheken verbindet, wahrscheinlicher verdächtige Netzwerkaktivitäten durchführen. Zu den Beispielfaktoren, die bei der Auswertung dieses Kriterienkatalogs verwendet werden, können die Folgenden gehören:

- Dateien, die als XOR-kodiert erkannt wurden
- Dateien, die als eingebettet innerhalb nicht ausführbarer Formate erkannt wurden (z. B. eine PE-Datei, die in einem GIF-Format eingebettet ist)
- Dateien, die sich mit riskanteren Importbibliotheken verbinden
- Dateien, die in hohem Maße vom PE-Format abweichen

Community

Die dritte Kategorie wertet die Sitzung und die Dateien basierend auf dem kollektives Wissen der Sicherheits-Community aus. So werden z. B. Dateien, deren Fingerabdruck/Hash angesehenen Virenschutzanbietern (AV) bereits als positiv oder negativ bekannt ist, entsprechend klassifiziert. Eine Datei wird auch aufgrund des Wissens, dass sie von einer Website stammt, die von der Sicherheits-Community als positiv oder negativ bekannt ist, klassifiziert.

Die Auswertung durch die Community zeigt auch an, ob der AV in Ihrem Netzwerk die Dateien als schädlich markiert hat. Es zeigt nicht an, ob das vorhandene AV-Produkt Maßnahmen ergriffen hat, um Ihr System zu schützen.

Sandbox

Die vierte Kategorie untersucht das Verhalten der Software, indem sie in einer Sandbox-Umgebung tatsächlich ausgeführt wird. Durch Ausführung der Software, um ihr Verhalten zu beobachten, kann durch die Erkennung wohlbekannter schädlicher Aktivitäten eine Punktzahl berechnet werden. Beispielsweise erhielte eine Software, die sich bei jedem Neustart automatisch startet und IRC-Verbindungen herstellt, eine höhere Punktzahl als eine Datei, die kein als schädlich bekanntes Verhalten zeigt.

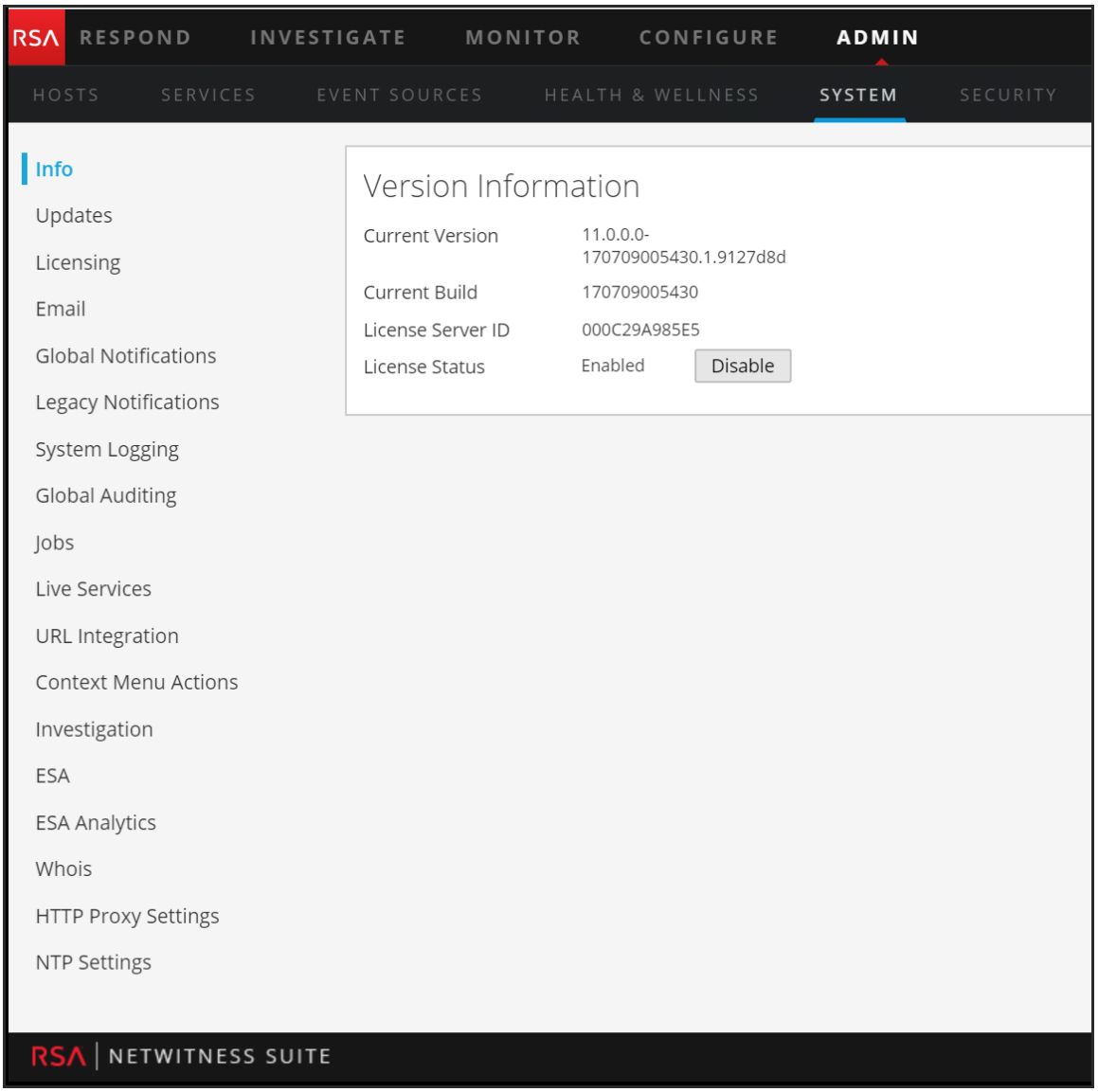
Rollen und Berechtigungen für Analysten

In diesem Thema werden die Benutzerrollen und Berechtigungen erläutert, die für einen Benutzer zum Durchführen einer Schadsoftwareanalyse in NetWitness Suite erforderlich sind. Wenn Sie eine Analyseaufgabe nicht durchführen oder eine Ansicht nicht sehen können, muss der Administrator unter Umständen die für Sie konfigurierten Rollen und Berechtigungen anpassen.

Erforderliche Rollen und Berechtigungen

RSA NetWitness Suite managt die Sicherheit durch Gewähren des Zugriffs auf Ansichten und Funktionen mithilfe von Systemberechtigungen und Berechtigungen für individuelle Services.

Auf der Systemebene in der Ansicht „Administration > System“ muss dem Benutzer eine Systemrolle zugewiesen werden, die Zugriff auf bestimmte Ansichten und Funktionen gewährt.



Der standardmäßigen Rolle `Malware_Analysts` in NetWitness Suite 11.0 werden alle unten aufgeführten Berechtigungen zugewiesen. Falls erforderlich, kann ein Administrator eine benutzerdefinierte Rolle mit mehreren der folgenden Berechtigungen erstellen:

- Auf Investigation-Modul zugreifen (erforderlich)
- Investigation – Navigieren durch Ereignisse
- Investigation – Navigieren durch Werte
- Auf Incident-Modul zugreifen
- Incidents anzeigen und managen
- Anzeigen von Schadsoftwareereignissen (zum Anzeigen von Ereignissen)

- Dateidownload (zum Herunterladen von Dateien aus dem Malware Analysis-Service)
- Initiieren eines Schadsoftwarescans (zum Initiieren eines einmaligen Servicescans oder eines einmaligen Dateiuploads)
- Dashlet-Berechtigungen aus praktischen Gründen: Dashlet – Untersuchen der Top-Werte, Dashlet – Untersuchen der Servicelisten, Dashlet – Untersuchen der Jobs, Dashlet – Untersuchen der Verknüpfung.

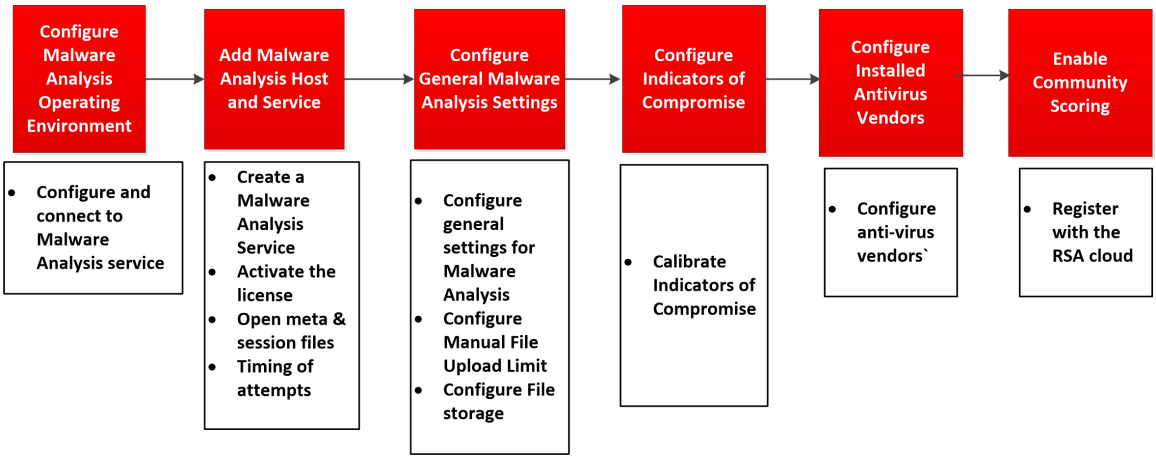
Ein Anwendungsbeispiel für die Erstellung einer benutzerdefinierten Rolle ist die Rolle eines Assistenten des Schadsoftwareanalysten mit eingeschränkten Berechtigungen, die nicht die Berechtigungen zum Herunterladen von Dateien umfassen.

Für bestimmte Services muss ein Schadsoftwareanalyst der Gruppe **Analysten** oder einer anderen Gruppe angehören, die die zwei Standardberechtigungen der Gruppe „Analysten“ aufweist: **sdk.meta** und **sdk.content**. Benutzer mit diesen Berechtigungen können zum Zwecke der Analyse für den Service bestimmte Anwendungen verwenden, Abfragen ausführen und Inhalte anzeigen.

Konfiguration von Malware Analysis

Malware Analysis kann als Service auf einem Decoder oder als Service auf einer dedizierten Appliance ausgeführt werden. In diesem Handbuch werden Anweisungen zur Einrichtung der Betriebsumgebung und der anschließenden Konfiguration des Malware Analysis-Services bereitgestellt. Sobald diese Konfiguration abgeschlossen ist, können Analysten eine Schadsoftwareanalyse durchführen.

Dies sind die erforderlichen Schritte zur Konfiguration von Malware Analysis sowie zur Änderung der Konfiguration. Führen Sie die in diesem Abschnitt aufgezeigten Schritte in vorgegebener Reihenfolge aus.



Checkliste der grundlegenden Konfiguration

In der folgenden Checkliste sind die Aufgaben enthalten, die zur Konfiguration von Malware Analysis erforderlich sind, das in Übereinstimmung mit dem *Leitfaden für die ersten Schritte mit Hosts und Services* zu NetWitness Suite hinzugefügt wurde.

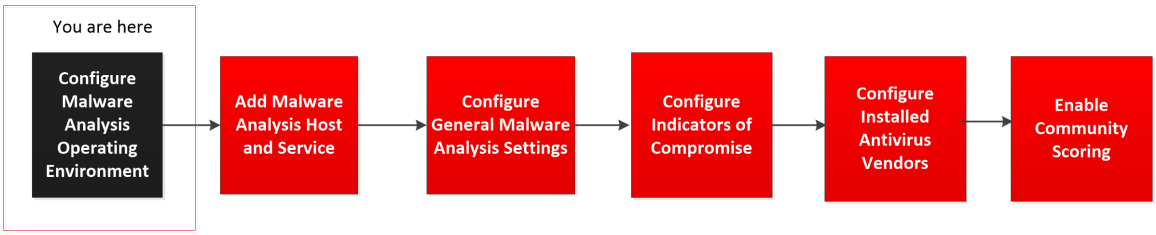
Schritt	Allgemeine Aufgaben
Schritt 1: Konfigurieren der Malware Analysis-Betriebsumgebung	Konfigurieren der Malware Analysis-Betriebsumgebung In diesem Thema werden die Verfahren zum Konfigurieren der Betriebsumgebung für die Verbindung mit einem Malware Analysis-Service beschrieben.

Schritt	Allgemeine Aufgaben
Schritt 2: Hinzufügen eines Malware Analysis-Hosts und -Services	Hinzufügen eines Malware Analysis-Hosts und -Services **Hinweis:** Um diesen Schritt abzuschließen, müssen Sie den NetWitness Suite-Lizenzserver so eingerichtet haben, wie es im Handbuch zur Lizenzierung beschrieben ist. Erstellen Sie in NetWitness Suite einen Malware Analysis-Service und aktivieren Sie die Lizenz. Der Standard REST-Port ist 60007. Auf Standorten, an denen die kostenlose Version von Malware Analysis verwendet wird, muss die Service-IP-Adresse als localhost oder loopback installiert werden.
Schritt 3: Konfigurieren der allgemeinen Malware Analysis-Einstellungen	Konfigurieren der allgemeinen Malware Analysis-Einstellungen • Aktivieren Sie kontinuierliches Abfragen. • Konfigurieren Sie ein Limit für Dateien, die manuell hochgeladen werden können. • Konfigurieren Sie das Dateienspeicher-Repository und die Datenbank. • Kalibrieren Sie die Bewertungsmodule Statisch, Netzwerk, Community und Sandbox.
Schritt 4: Konfigurieren der Indikatoren für eine Infizierung	Konfigurieren der Indikatoren für eine Infizierung Kalibrieren Sie die Indikatoren für eine Infizierung, die für jedes Bewertungsmodul (Statisch, Netzwerk, Community, Sandbox) und für YARA-basierende IOCs angewendet werden.
Schritt 5: Konfigurieren installierter Virenschutzanbieter	Konfigurieren installierter Virenschutzanbieter
Schritt 6: Aktivieren der Community-Bewertung	Aktivieren der Communityanalyse Registrieren Sie sich in der RSA-Cloud und testen Sie Verbindungen, um Communitybewertungen zu aktivieren.

Schritt	Allgemeine Aufgaben
Schritt 7: Konfigurieren des Auditing auf dem Malware Analysis-Host	(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host Konfigurieren Sie Schwellenwerte für das Auditing und aktivieren Sie Syslog, SNMP und Dateiauditing.
Schritt 8: Konfigurieren eines Hash-Filters	(Optional) Konfigurieren eines Hash-Filters Konfigurieren Sie Hash-Filter zur Feinabstimmung der Malware Analysis-Ereignisanalye basierend auf bekannten sauberen oder fehlerhaften Datei-Hashs.
Schritt 9: Konfigurieren der Malware Analysis-Proxyeinstellungen	(Optional) Konfigurieren der Malware Analysis-Proxyeinstellungen Konfigurieren Sie Malware Analysis für die Kommunikation mit RSA Cloud über einen Webproxy statt direkt zu kommunizieren.
Schritt 10: Registrieren für einen ThreatGrid-API-Schlüssel.	(Optional) Registrieren für einen ThreatGrid-API-Schlüssel

Konfigurieren der Malware Analysis-Betriebsumgebung

Sie können die NetWitness Suite-Betriebsumgebung zur Verbindungsherstellung mit einem NetWitness Suite Malware Analysis-Service konfigurieren.



Malware Analysis fungiert als Service auf einer dedizierten Malware Analysis-Appliance. Wenn Ihr Standort eine dedizierte Appliance verwendet, führen Sie einen der folgenden Schritte aus:

- Wenn Ihr Standort eine neue dedizierte NetWitness Suite Malware Analysis-Appliance hinzufügt, installieren Sie die physische Appliance in Ihrem Netzwerk und konfigurieren Sie

die Betriebsumgebung.

- Wenn an Ihrem Standort eine dedizierte Spectrum-Appliance auf eine dedizierte NetWitness Suite Malware Analysis-Appliance aktualisiert werden soll, müssen Sie die Spectrum-Appliance per Image als Malware Analysis-Appliance erstellen.

Malware Analysis ist bei der Ausführung abhängig von der Core-Infrastruktur. Um eine erfolgreiche Datenanalyse durch Malware Analysis zu gewährleisten, müssen Sie die folgenden Schritte ausführen.

1. Konfigurieren Sie den integrierten Broker in der Malware Analysis-Appliance für die Verbindung mit einem anderen Broker oder Concentrator in der vorhandenen Core-Infrastruktur.

   Hinweis: Wenn keine Core-Infrastruktur vorhanden ist, können nur manuell hochgeladene Dateien analysiert werden.

2. Verwenden Sie NetWitness Suite Live, um alle Live-Ressourcen mit dem Tag `malware analysis` zu finden, und stellen Sie diese Ressourcen für jeden Decoder-Service bereit, der Datenverkehr zur Analyse durch Malware Analysis erfasst. NetWitness Suite verwendet diese proprietären Parser und Feeds, um Ereignisse zu finden, die höchstwahrscheinlich Schadsoftware enthalten.
3. Konfigurieren Sie Kommunikationsports. Malware Analysis erfordert mehrere verschiedene geöffnete Kommunikationsports, einschließlich TCP/443 für HTTPS. Diese werden im unten stehenden Abschnitt Netzwerkverbindungen beschrieben.
4. Konfigurieren Sie die NextGen-Quelle, mit der Malware Analysis verbunden werden soll. Dies ist der Broker oder Concentrator.
   Malware Analysis ist jetzt bereit für die Analyse des Netzwerkdatenverkehrs.

Netzwerkverbindungen

Eingehende und ausgehende Netzwerkverbindungen müssen so konfiguriert werden, dass die Malware Analysis-Appliance ohne Probleme mit Services, RSA-Quellen für Softwareupdates und anderen wichtigen Informationen kommunizieren kann.

Ihre Netzwerkfirewall muss so konfiguriert sein, dass Malware Analysis Zugriff auf das Internet hat. Falls notwendig können Proxyserver verwendet werden, um diese Verbindungen leichter herzustellen.

Eingehende Verbindungen

TCP/22 – Secure Shell-Zugriff auf den Malware Analysis-Server zur Überprüfung von Protokolldateien und für Troubleshooting. Der Zugriff kann auf IP-Adressen begrenzt werden, die Malware Analysis managen.

- TCP/443 – HTTPS-webbasierte Verbindung für den Zugriff auf die Malware Analysis-Benutzeroberfläche.
- TCP/50008 – JMX-Port für Performance-Troubleshooting unter Verwendung einer Anwendung wie zum Beispiel JVisualVM. Dies ist optional und der Zugriff kann auf IP-Adressen begrenzt werden, die Malware Analysis managen.

Ausgehende Verbindungen

- TCP/443 – HTTPS-Verbindungen zu SSL-basierten Webservern. Manche Funktionen ermöglichen es, dass Malware Analysis Dateien oder Dokumente zur Analyse an Server sendet. Hierfür werden sichere Verbindungen benötigt. Die Verwendung eines Webproxyservers wird unterstützt.
- (TCP/443 – SSL-Verbindung zwischen Malware Analysis und der RSA-Cloud. Die Verwendung eines SOCKS-Proxyservers wird unterstützt. Veränderungen der Kundeninfrastruktur sind gegebenenfalls erforderlich, um zu gewährleisten, dass 443 für cloud.netwitness.com geöffnet ist.)
- TCP/50103 – REST API-Port für die Kommunikation mit einem Broker (NetWitness Suite 10.3.x und älter).
- TCP/50105 – REST API-Port für die Kommunikation mit einem Concentrator (NetWitness Suite 10.3.x und älter).
- TCP/50003, TCP/56003 – Ports für die Kommunikation mit einem Broker (NetWitness Suite 10.4 und höher).
- TCP/50005, TCP/56005 – Ports für die Kommunikation mit einem Concentrator (NetWitness Suite 10.4 und höher).
- ICMP – JMS-Verbindung zwischen NetWitness Suite und dem Malware Analysis-Service zur Verifizierung der Gültigkeit des eingegebenen Hostnamens und der IP-Adresse für eine erfolgreiche Testverbindung.

Hinzufügen eines Malware Analysis-Hosts und -Services

Sie können NetWitness Suite einen Malware Analysis-Host und -Service hinzufügen. Ihre NetWitness Suite-Umgebung legt fest, wie Sie einen Host hinzufügen. Grundlegende Anweisungen für das Hinzufügen eines Hosts finden Sie unter „Hinzufügen oder Aktualisieren eines Hosts“ im „Leitfaden für die ersten Schritte mit Hosts und Services“. Wenden Sie das Verfahren in diesem Abschnitt nur an, wenn Sie einen Malware Analysis-Host manuell hinzufügen müssen.

Hinweis: Um diesen Schritt abzuschließen, müssen Sie den NetWitness Suite-Lizenzserver so eingerichtet haben, wie es im Handbuch zur Lizenzierung beschrieben ist.

- Fügen Sie einen Malware Analysis-Host hinzu, wenn eine physische oder virtuelle Malware Analysis-Appliance vorhanden ist.

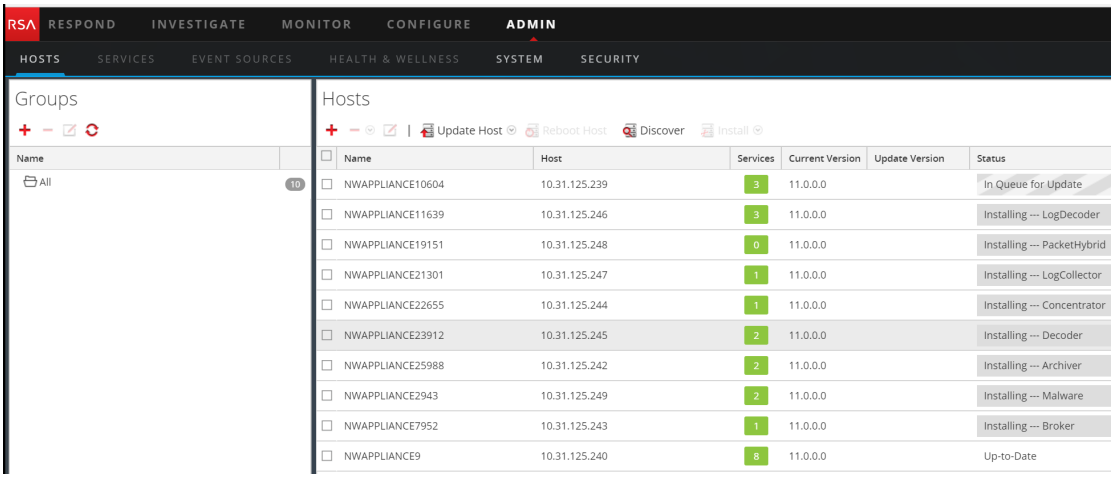
Voraussetzung

Um einen Host und einen Service in NetWitness Suite hinzuzufügen, muss die Einrichtung der Vorgänge abgeschlossen sein und es muss eine Instanz von NetWitness Suite installiert sein und laufen.

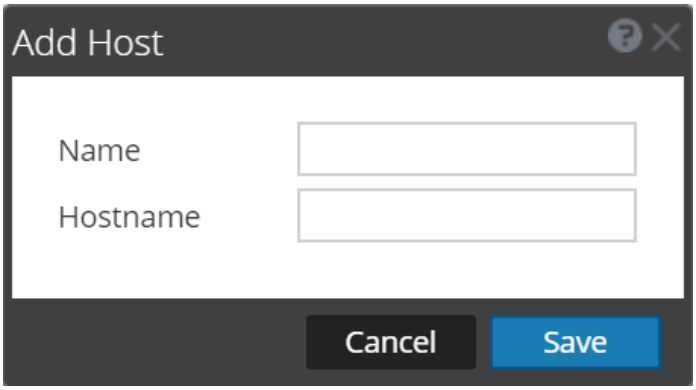
Verfahren

So fügen Sie NetWitness Suite manuell einen Malware Analysis-Host hinzu:

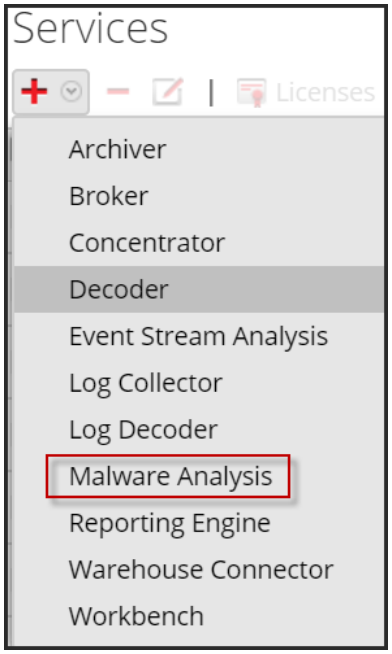
1. Melden Sie sich bei NetWitness Suite an.
2. Wählen Sie im Hauptmenü **Administration > Hosts** aus. Die Ansicht „Administration“ > „Hosts“ wird angezeigt.



3. Klicken Sie in der Symbolleiste des Bereichs „Hosts“ auf  .
   Das Dialogfeld „Host hinzufügen“ wird angezeigt.



4. Geben Sie im Feld **Name** einen Namen für den Malware Analysis-Host ein. Geben Sie in das Feld **Hostname** den Hostnamen, die virtuelle IP-Adresse oder die IP-Adresse in Malware Analysis ein. Klicken Sie auf **Speichern**.
5. Wählen Sie in der Symbolleiste die Option **Services** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Services** auf  und wählen Sie in der daraufhin angezeigten Drop-down-Liste mit verfügbaren Services **Malware Analysis** aus.

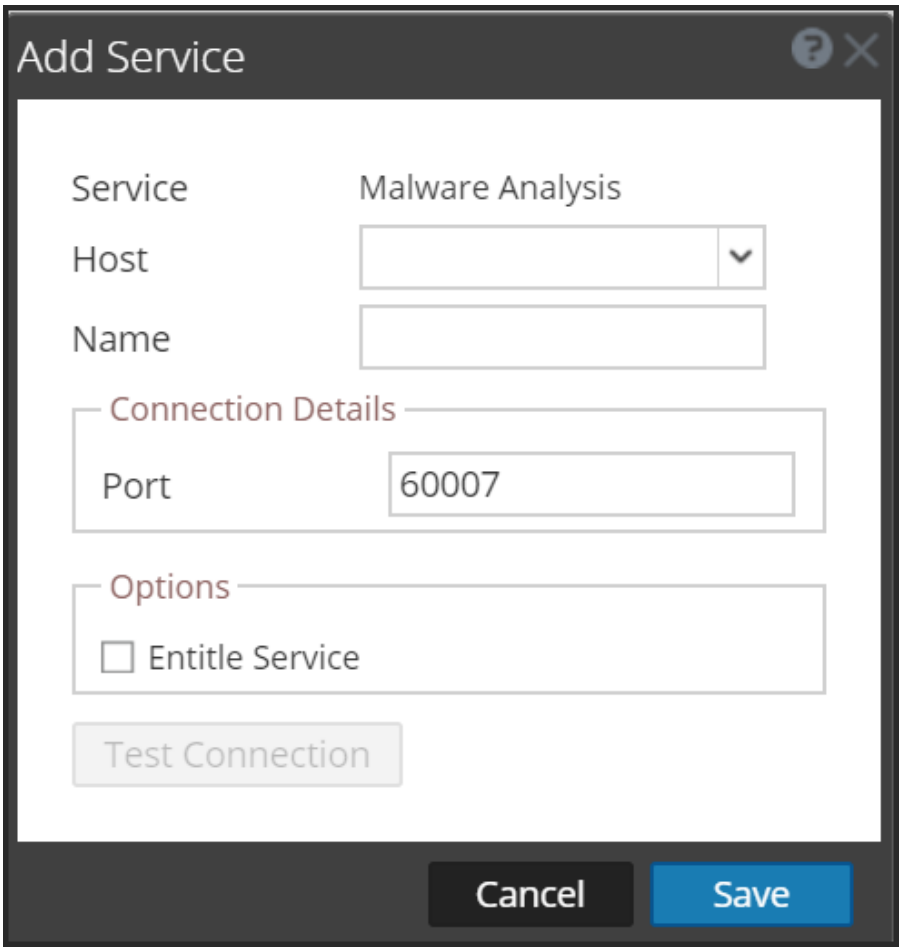


   Das Dialogfeld Service hinzufügen wird mit dem Servicetyp Malware Analysis angezeigt.
7. Geben Sie die folgenden Informationen ein:
   Geben Sie im Feld **Name** einen Namen für den Malware Analysis-Service ein.
   Geben Sie in das Feld **Host** den Hostnamen, die virtuelle IP-Adresse oder die IP-Adresse in

Malware Analysis ein.

Geben Sie in das Feld **Port 60007** ein.

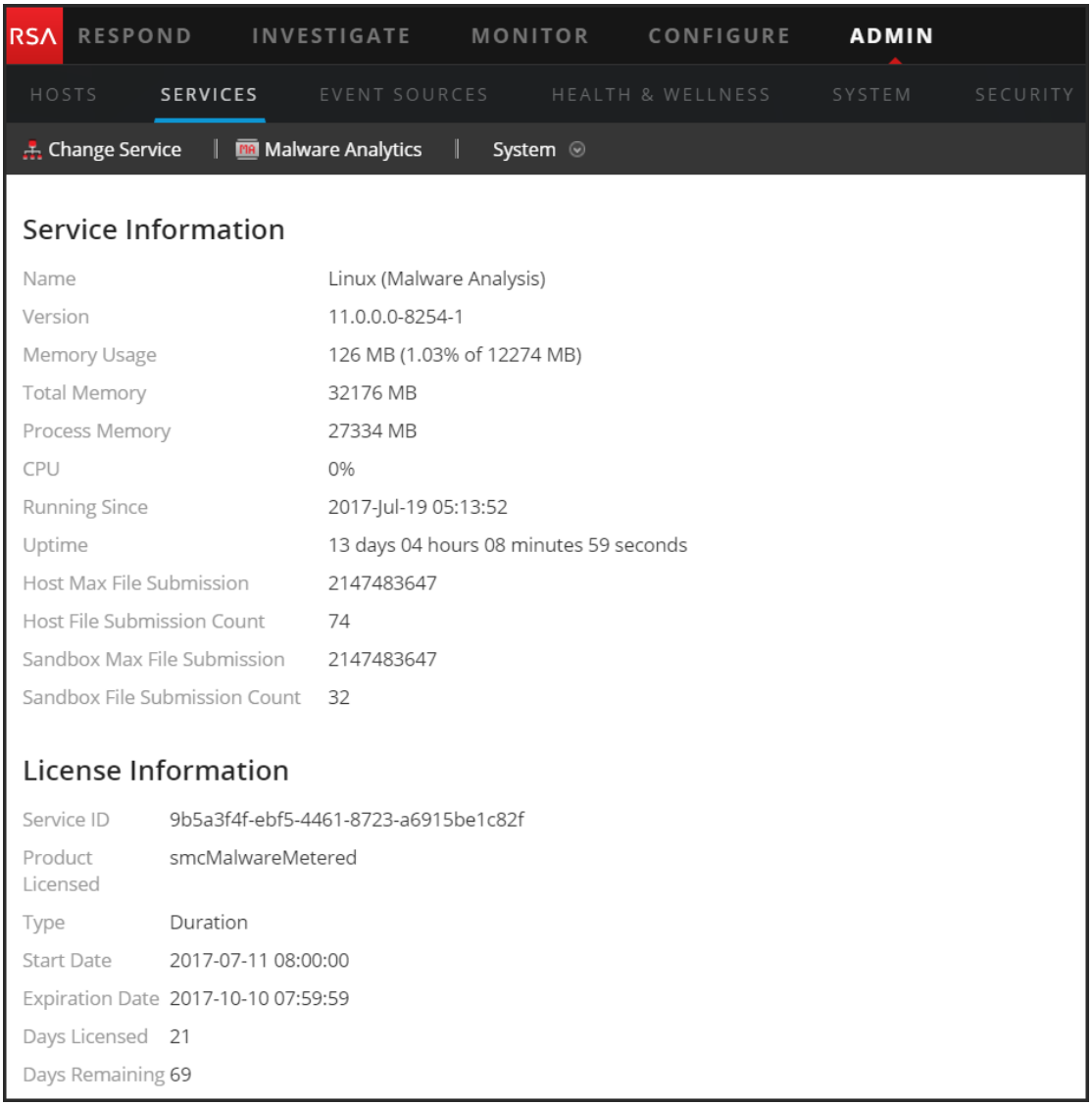
(Optional) Wählen Sie unter **Optionen** die Option **Service berechtigen** aus.



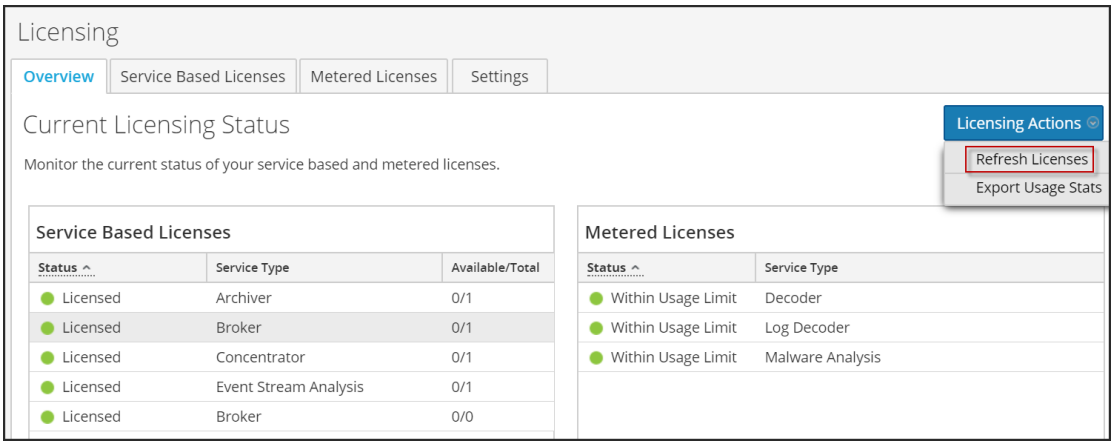
8. Klicken Sie auf **Verbindung testen**.

   Während der Service hinzugefügt wird, sendet NetWitness Suite ICMP-Pakete an den Service, um zu überprüfen, ob der Hostname und die IP-Adresse, die eingegeben wurden, für eine erfolgreiche Testverbindung gültig sind. Das Ergebnis des Tests wird im Dialogfeld Service hinzufügen angezeigt. Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Serviceinformationen und versuchen Sie es erneut.

9. Wenn das Ergebnis erfolgreich ist, klicken Sie auf **Speichern**. Das Dialogfeld „Service hinzufügen“ wird geschlossen und der Malware Analysis-Service steht NetWitness Suite zur Verfügung. (Optional) Überprüfen Sie den Status des Malware Analysis-Service. Wählen Sie in der Ansicht „Administration“ > „Services“ den Malware Analysis-Service und anschließend **Ansicht > System** aus. Es folgt ein Beispiel der verfügbaren Informationen für einen Malware Analysis-Service.

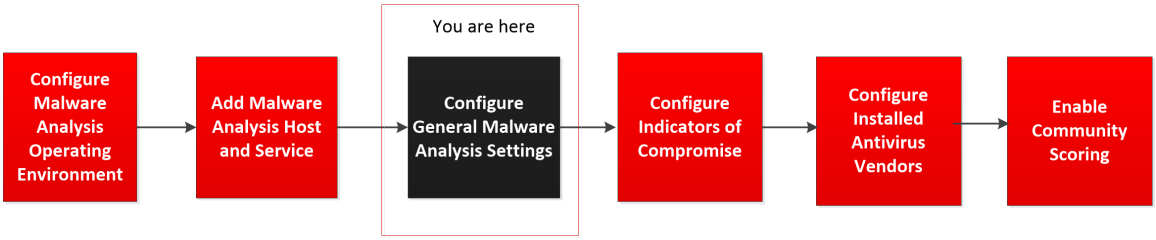


Wenn der Service nicht lizenziert ist, navigieren Sie zu „Administration“ > „System“ > Bereich „Lizenzierung“ und wählen Sie im Menü **Lizenzierungsaktionen** die Option **Lizenzen aktualisieren** aus.



Konfigurieren der allgemeinen Malware Analysis-Einstellungen

Sie können verschiedene Grundeinstellungen konfigurieren, die erforderlich sind, um die Verarbeitung von Sitzungen, den manuellen Dateiupload und die verschiedenen Bewertungsmodule, die Malware Analysis zum Analysieren von Daten nutzt, zu aktivieren und zu kalibrieren.



Sie können außerdem die Dateifreigabe im Daten-Repository einrichten. Malware Analysis verfügt über drei Modi zum Verarbeiten von Sitzungen und Dateien. Jede Kombination dieser drei Modi kann zum Initiieren von Analysen in Malware Analysis verwendet werden. Die Modi sind folgende:

- **Kontinuierliche Abfrage des Core-Service:** Sie können eine kontinuierliche Abfrage des Core-Service aktivieren und konfigurieren. Ist dies aktiviert und konfiguriert, fragt Malware Analysis den Core-Service kontinuierlich auf für die Analyse gekennzeichnete Sitzungen ab. Standardmäßig ist die kontinuierliche Abfrage deaktiviert. Während der kontinuierlichen Abfrage können Sie die Prävention vor Denial of Service (DOS)-Angriffen aktivieren. Sie können die Verbindung zum Malware Analysis-Service, der kontinuierlich abgefragt wird, mithilfe einer Option auf der Registerkarte „Integration“ testen.

Hinweis: Wenn Sie in Malware Analysis 10.3.5 und früher einen Core-Service als Service für kontinuierliche Abfrage hinzufügen, verwenden Sie den REST-Port. Fügen Sie zum Beispiel einen Concentrator zu Malware Analysis 10.3.5 über den REST-Port (50105) anstatt über den nativen NexGen-Port (50005) hinzu.

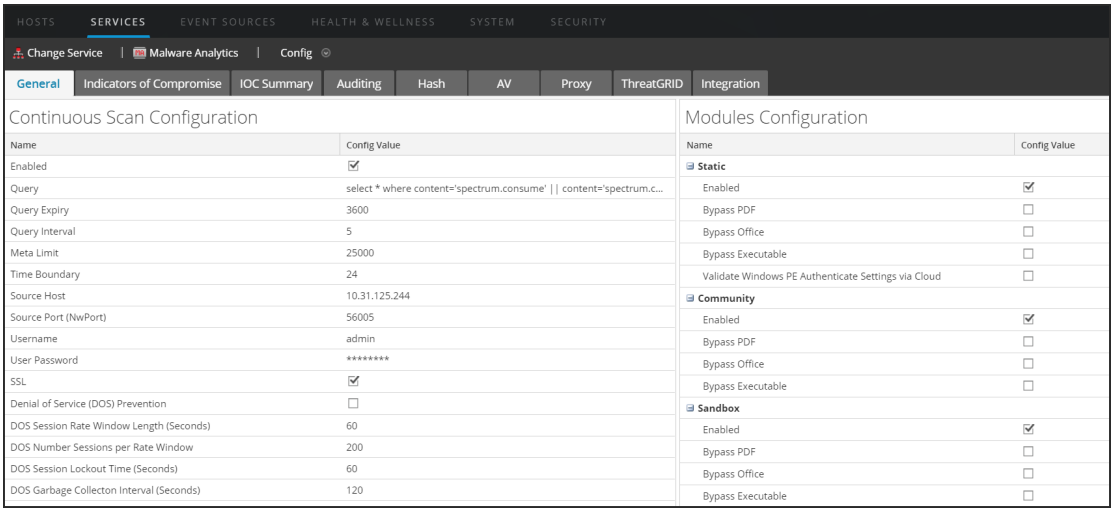
- **Analyse des Core-Service nach Bedarf:** Sie können Sitzungen basierend auf Ermittlungen analysieren, die direkt in NetWitness Suite initiiert wurden. Diese Methode ermöglicht eine manuell gesteuerte Verarbeitung von Core-Sitzungen sowie eine stärkere Kontrolle der Verarbeitung von Dateien in diesen Sitzungen (z. B. durch Senden an eine Sandbox zur Verarbeitung). Bei Dokumenttypen können die Standardeinschränkungen umgangen werden, indem sie unabhängig von der konfigurierten Einstellung immer zur Verarbeitung an die Community oder eine Sandbox gesendet werden.
- **Manueller Dateiupload:** Sie können eine oder mehrere zu analysierende Dateien manuell hochladen, indem Sie zu einem sichtbaren Ordner auf Ihrem Computer navigieren und die hochzuladenden Dateien auswählen. Die maximale Größe für die hochgeladenen Dateien ist konfigurierbar.

Anzeigen der Basiseinstellungen

So zeigen Sie die Basiseinstellungen an:

1. Wählen Sie im **Hauptmenü** die Optionen **Administration > Services** aus.
2. Wählen Sie im Raster **Services** einen Malware Analysis-Service aus und klicken Sie auf  **> Ansicht > Konfiguration**.

   Die Servicekonfiguration für den Service wird angezeigt und die Registerkarte **Allgemein** geöffnet.



Konfigurieren der kontinuierlichen Abfrage

Die Übertragungsrate von Malware Analysis ist beschränkt, sodass maximal 1.000 Dateien pro Tag zur Sandbox-Bearbeitung an die ThreatGrid-Cloud gesendet werden können. Um die Nutzung der Sandbox zu optimieren, können Sie in der Malware Analysis-Konfiguration angeben, welche Verarbeitungsmethode Malware Analysis verwenden soll. Sie können die kontinuierliche Abfrage aktivieren oder deaktivieren.

Ein wichtiger Faktor bei der Konfiguration der kontinuierlichen Abfrage sind die Parameter zur Denial of Service(DOS)-Verhinderung. Diese Funktion ist standardmäßig deaktiviert, da Sie die Einstellungen für Ihre Umgebung vor dem Aktivieren der Funktion sorgfältig prüfen sollten.

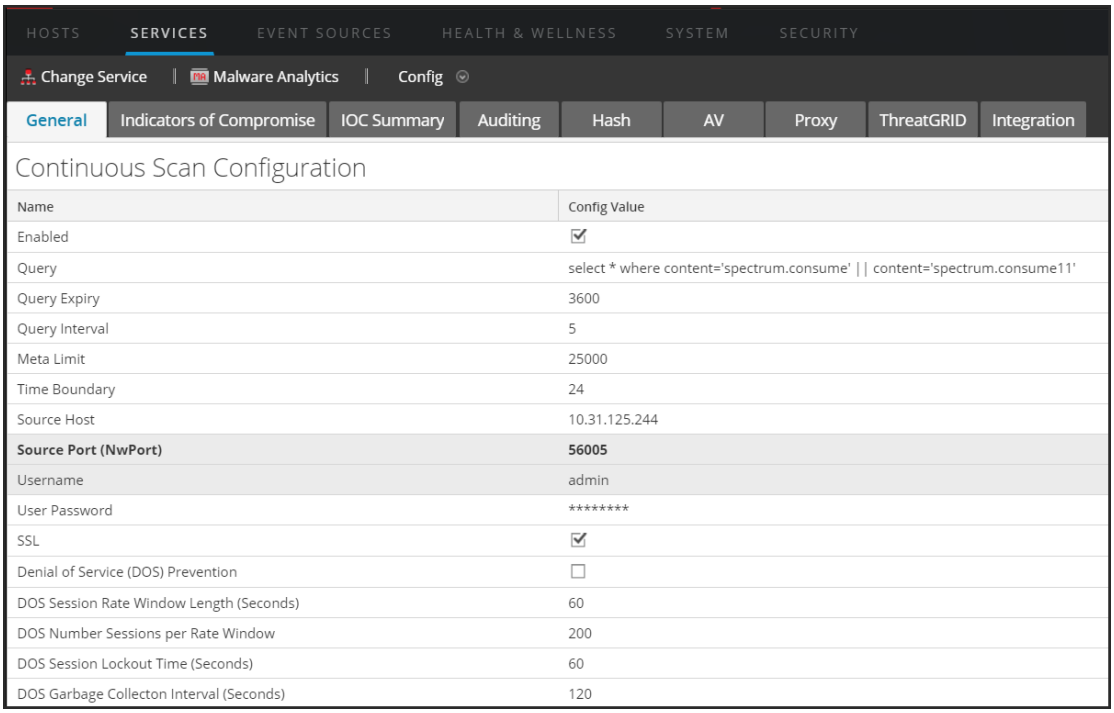
Wenn die DOS-Verhinderung deaktiviert ist, analysiert Malware Analysis die in der Warteschlange befindlichen Sitzungen in First-In-First-Out-Reihenfolge. Ein DOS-Angriff kann die Warteschlange jedoch schnell füllen, sodass Malware Analysis mit dem Verarbeiten dieser Sitzungen beschäftigt ist, während in einer späteren Sitzung ein Schadsoftwareangriff stattfindet. Die spätere Sitzung mit dem eigentlichen Angriff erreicht möglicherweise nicht den Anfang der Warteschlange und wird erst nach Beginn des Angriffs analysiert.

Wenn die DOS-Verhinderung aktiviert ist, stuft Malware Analysis zu viele Sitzungen von einer einzigen IP-Adresse als DOS-Angriff ein. Wenn eine IP-Adresse die Anzahl von Sitzungen pro Ratenfenster überschreitet, beginnt Malware Analysis, die Sitzungen von dieser Adresse zu ignorieren, bis die Sitzungssperrzeit erreicht ist. Dann setzt Malware Analysis die Analyse der Sitzungen von dieser IP-Adresse fort. Die ignorierten Sitzungen von dieser IP-Adresse werden überhaupt nicht analysiert, sodass ein Schadsoftwareangriff während der Sitzungssperrzeit unbemerkt eindringen kann.

Gemäß der Einstellung „DOS-Intervall für automatische Speicherbereinigung“ leert Malware Analysis den In-Memory-Arbeitsspeicher einer IP-Quelle nach einer angegebenen Anzahl von Sekunden. IP-Adressen mit geringer Aktivität während dieses Intervalls werden aus dem Speicher gelöscht. Wenn eine IP-Adresse in Intervallen aktiv ist, die das Intervall in „DOS-Intervall für automatische Speicherbereinigung“ überschreiten, erkennt Malware Analysis sie unter Umständen nicht als DOS-Angriff.

Um Malware Analysis für die kontinuierliche Abfrage zu konfigurieren, gehen Sie im Abschnitt „Konfiguration des kontinuierlichen Scannens“ wie folgt vor:

1. Klicken Sie unter **Admin** auf **Services**.
2. Sie können die kontinuierliche Abfrage auf der Registerkarte **Allgemein** unter **Konfiguration des kontinuierlichen Scannens** konfigurieren.



3. Klicken Sie zum Aktivieren der kontinuierlichen Abfrage auf **Aktiviert**.
4. (Optional) Wenn Sie die Standardwerte für die Abfrage ändern möchten, geben Sie neue Werte für **Ablaufzeit der Abfrage**, **Abfrageintervall**, **Metadatenbegrenzung** und **Zeitgrenze** ein.
5. Geben Sie zur Konfiguration der Malware Analysis-Appliance, die von Malware Analysis abgefragt wird, um Daten für die Analyse abzurufen, **Quellhost** und **Quellport (NwPort)** an.
6. (Optional) Wenn Sie die standardmäßigen Anmeldeinformationen für die Malware Analysis-Appliance ändern möchten, geben Sie den **Benutzernamen** und das **Benutzerpasswort** an.
7. Wenn Sie für die Kommunikation zwischen der Malware Analysis-Appliance und dem Core-Service **SSL** nutzen möchten, müssen Sie die Option SSL aktivieren.
8. (Optional) Wenn Sie die Denial of Service(DOS)-Verhinderung konfigurieren möchten, gehen Sie wie folgt vor:
   a. Aktivieren Sie den Parameter **Denial of Service (DOS)-Verhinderung**.
   b. Richten Sie die Sitzungsbeschränkungen für die DOS-Verhinderung ein:
      - Geben Sie die Anzahl der Sekunden für das Zeitfenster an, während dem Malware Analysis Sitzungen für eine einzelne IP-Adresse zählt (**DOS - Fensterlängen-Sitzungsrate**). Das Fenster wird als Ratenfenster bezeichnet und ein Zähler wird

festgelegt, wenn die erste Sitzung von dieser IP-Quelle empfangen wird. Der Standardwert ist 60 Sekunden.

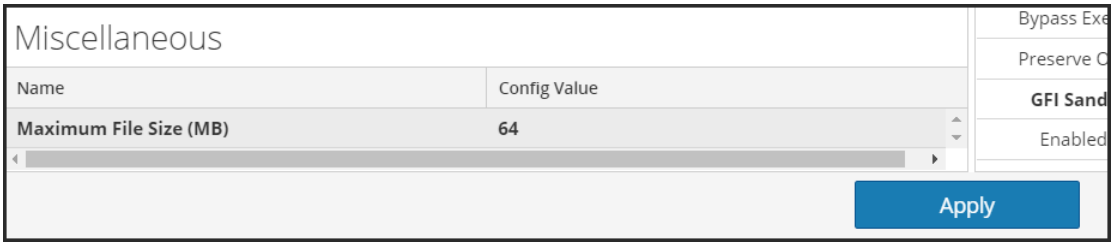
- Geben Sie unter **DOS - Anzahl von Sitzungen pro Ratenfenster** die Anzahl von Sitzungen ein, die pro Ratenfenster zulässig sein soll. Der Standardwert ist 200 Sitzungen. Wenn die Anzahl der Sitzungen innerhalb des Ratenfensters erreicht wurde, beginnt Malware Analysis, Sitzungen von dieser IP-Adresse zu ignorieren, und die ignorierten Sitzungen von dieser IP-Adresse werden nicht analysiert. Malware Analysis ignoriert Sitzungen so lange, bis die Sperrzeit erreicht ist.
- Geben Sie die Dauer der Sperrzeit (während der Sitzungen von der IP-Adresse ignoriert und nicht analysiert werden) unter **DOS - Sitzungssperrzeit (Sekunden)** an. Der Standardwert ist 60 Sekunden. Wenn die Sperrdauer verstrichen ist, setzt Malware Analysis die Analyse der Sitzungen von dieser IP-Adresse fort.
- Geben Sie unter **DOS–Intervall für automatische Speicherbereinigung (Sekunden)** das Inaktivitätsintervall für IP-Adressen an, nach dessen Ablauf NetWitness Suite das In-Memory-Objekt für die IP-Quelle entfernt. Der Standardwert ist 120 Sekunden.

9. Klicken Sie auf **Apply**, um die Änderungen anzuwenden.
   Die Änderungen werden sofort wirksam, sobald Malware Analysis neue Pakete empfängt.
10. Testen Sie die Verbindung des Malware Analysis-Service zum Core-Service, der auf der Registerkarte **Integration** ausgewählt wurde, indem Sie im Abschnitt **Verbindungstest für kontinuierliches Scannen** auf die Schaltfläche **Verbindung testen** klicken.

Konfigurieren von Einstellungen für den manuellen Dateiupload

So konfigurieren Sie die maximale Dateigröße für den manuellen Dateiupload:

1. Geben Sie unter „Verschiedenes“ die maximale Dateigröße (in MB) für Dateien ein, die für einen Malware Analysis-Scanvorgang manuell hochgeladen werden.



2. Klicken Sie auf **Anwenden**.
   Die Änderungen werden sofort wirksam.

Konfigurieren des Daten-Repository

Malware Analysis kann eine begrenzte Anzahl von Dateien auf der Appliance speichern. Die Daten-Repository-Konfiguration sieht eine Dateisystem-Aufbewahrungsfrist von 60 Tagen vor. Mit dieser Einstellung wird festgelegt, wie lange Dateien in der Malware Analysis-Appliance aufbewahrt werden. Wenn alte Dateien gelöscht werden, können sie nicht wiederhergestellt werden. Jeden Tag löscht Malware Analysis Dateien, bei denen die Dateisystem-Aufbewahrungsfrist überschritten wurde, um sicherzustellen, dass kein Speicherplatz unnötig belegt wird.

Die Dateisystem-Aufbewahrungsfrist ist die einzige Einstellung, durch die das Löschen von Dateien gesteuert wird. Dateien werden nicht basierend auf der Menge von belegtem Speicherplatz gelöscht. Muss die Einstellung aus diesem Grund angepasst werden, kann der Administrator die Aufbewahrungsfrist so einstellen, dass sie ungefähr der prognostizierten Speicherbelegung entspricht.

Die sichtbaren Daten-Repository-Parameter in der NetWitness Suite-Benutzeroberfläche sind folgende:

- Das Repository-Verzeichnis ist **/var/lib/netwitness/malware-analytics-server/spectrum**. Ändern Sie diesen Wert nicht.
- Das Dateifreigabeprotokoll zum Kopieren von Dateien des Malware Analysis-Services.
- Die Dateiaufbewahrungsfrist in Tagen.

Gehen Sie zum Konfigurieren der Dateifreigabe im Abschnitt „Daten-Repository“ wie folgt vor:

1. Klicken Sie auf „Dateifreigabeprotokoll“, um FTP oder SAMBA auszuwählen.
2. Wählen Sie die Anzahl von Tagen aus, über die Dateien im Repository aufbewahrt werden sollen.
3. Klicken Sie auf **Anwenden**.

Die Änderungen werden sofort wirksam.

Kalibrieren von Bewertungsmodulen

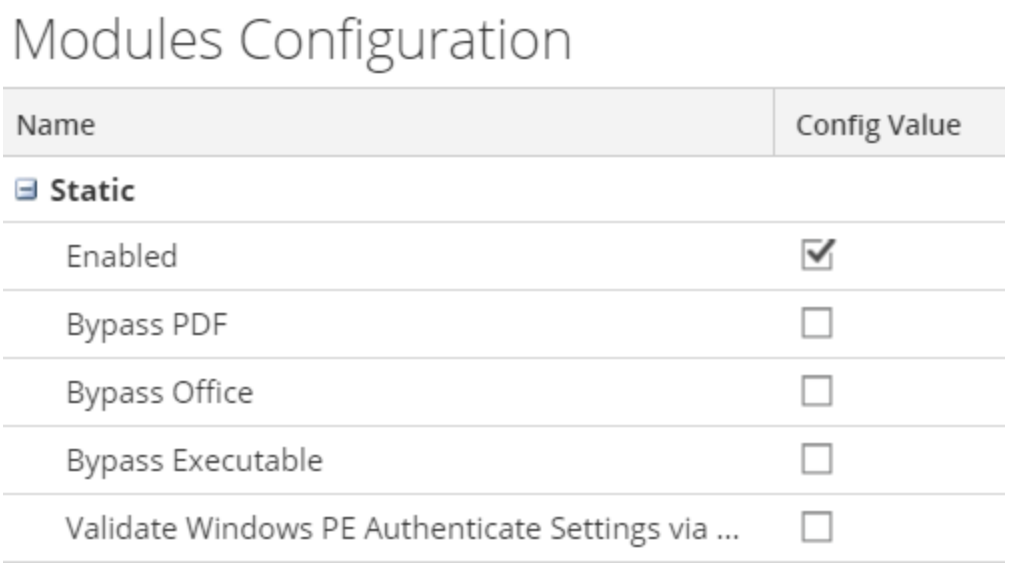
Im Abschnitt „Modulkonfiguration“ finden Sie Informationen dazu, wie Sie diese Komponenten von Malware Analysis konfigurieren, um Folgendes zu bewerkstelligen:

- Vollständige Deaktivierung von Bewertungsmodulen (Statisch, Community und Sandbox). Vor dem Deaktivieren oder Aktivieren eines Bewertungsmoduls sollten Sie sicherstellen, dass Sie die Funktionsweise dieses Bewertungsmoduls kennen.
- Malware Analysis markiert Sitzungen mit Microsoft Office-, Windows PE- und PDF-Dateien zur Verarbeitung durch den Malware Analysis-Service. Sie können Malware Analysis aber

so konfigurieren, dass Windows PE-, Microsoft Office- und PDF-Dokumente ignoriert werden. Eine bessere Option ist jedoch, in den Core-Einstellungen festzulegen, dass diese Dateien ignoriert werden sollen, sodass sie nicht für die Malware Analysis-Verarbeitung markiert werden.

Eine Beispielanwendung für die Kalibrierung von Bewertungsmodulen ist folgende: Zum Einrichten von Regelgruppen oder Analysieren der Systemperformance können Sie verschiedene Szenarien testen, in denen Microsoft Office- und Windows PE-Dokumente analysiert werden, PDF-Dokumente jedoch nicht. Sie können diese Szenarien mit jedem der drei Bewertungsmodule testen. Wenn Sie eine messbare Verbesserung bei der Systemperformance sehen, können Sie diese Kenntnisse auf einen größeren Maßstab übertragen.

Konfigurieren der statischen Analysebewertung



Zum Konfigurieren der statischen Analysebewertung gehen Sie im Abschnitt **Modulkonfiguration** wie folgt vor:

1. Standardmäßig ist das Modul Statisch aktiviert. Zum Aktivieren oder Deaktivieren der statischen Analyse klicken Sie auf das Kontrollkästchen **Aktiviert**.
2. Um die Verarbeitung von PDF-, Microsoft Office- und Windows PE-Dateien in einer Sitzung zu konfigurieren, aktivieren Sie bei Bedarf eines oder mehrere der Kontrollkästchen **PDF umgehen**, **Office umgehen**, **Ausführbare Datei umgehen**.
3. Um Ihre Einstellungen für die Authenticode-Validierung digital signierter Windows PE-Dateien zu konfigurieren, klicken Sie in das Kontrollkästchen **Windows PE-Authentifizierungseinstellungen über die Cloud überprüfen**. Wenn digital signierte Windows PE-Dateien nicht zur Validierung an die RSA-Cloud übermittelt werden sollen,

deaktivieren Sie das Kontrollkästchen.
Ist es deaktiviert, werden ALLE statischen Analysen lokal durchgeführt (die Authenticode-Validierung wird übersprungen). Unabhängig von dieser Einstellung unterliegen PDF- und MS Office-Dokumente keiner Authenticode-Validierung und werden während der statischen Analyse niemals über das Netzwerk übertragen.

4. Klicken Sie auf **Anwenden**. Die Änderungen werden sofort wirksam, sobald Malware Analysis neue Pakete empfängt.

Konfigurieren der Communityanalysebewertung

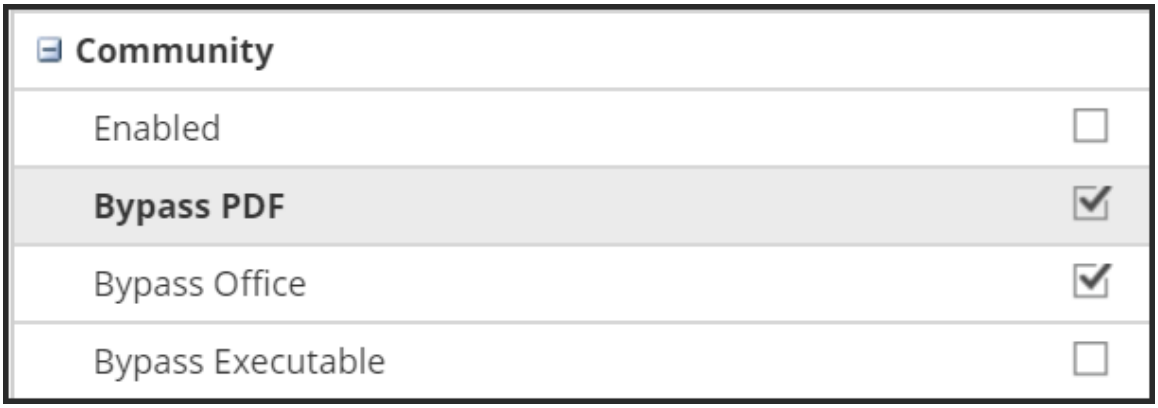
Wenn das Communitymodul aktiviert ist, analysiert die Sicherheitscommunity alle Dokumente, die nicht aus der Verarbeitung ausgeschlossen wurden. Dies geschieht durch Senden der Netzwerksitzungs- und Dateiattribute an die RSA-Cloud. Die RSA-Cloud nimmt dann unter Umständen eine externe Verbindung zu Partnern der Sicherheitscommunity auf, um die Informationen zu verarbeiten.

Dateiinhalte werden niemals zur Analyse an die Community gesendet. Stattdessen wird der MD5/SHA-1-Hash der Datei gesendet, um eine Viruserkennung und Blacklisting vorzunehmen. In ähnlicher Weise werden im Rahmen dieses Prozesses Metadaten der Sitzung gesammelt und analysiert. Metaelemente wie URLs und Domainnamen werden untersucht und an die RSA-Cloud übertragen, um bekanntermaßen schadhafte URLs/Domains zu ermitteln.

Sie können die Communityanalyse aktivieren und die zu verarbeitenden Dokumenttypen einschränken. Es werden keine Dateiinhalte (mit Ausnahme eines Hash-Werts) außerhalb des Netzwerks versendet.

Hinweis: Um Zugriff auf die RSA-Cloud zu erhalten, in der die Verarbeitung durchgeführt wird, müssen Sie Ihren Malware Analysis-Service beim RSA Customer Service registrieren. Es gibt zwei Methoden: Registrieren Sie den Service mithilfe der Optionen auf der Registerkarte „Integration“ oder wenden Sie sich an RSA Customer Care.

Zum Konfigurieren der Communityanalysebewertung gehen Sie im Abschnitt Modulkonfiguration wie folgt vor:



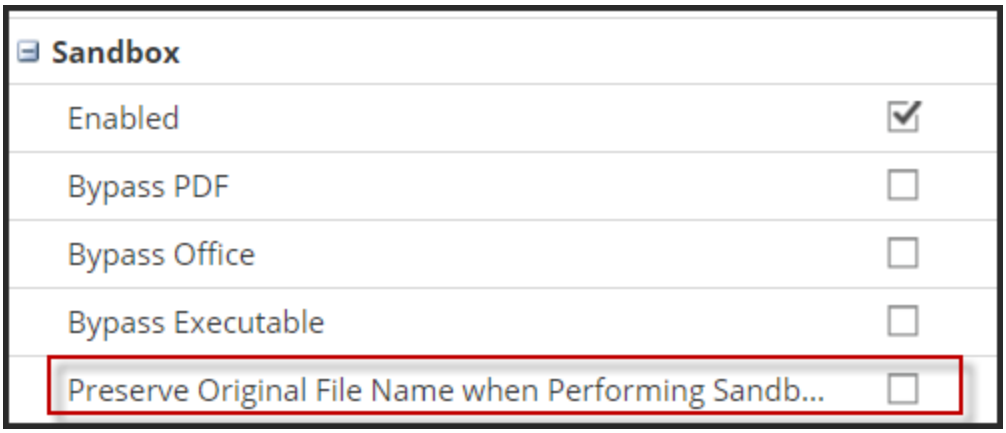
1. Zum Aktivieren oder Deaktivieren der Communityanalyse klicken Sie auf das Kontrollkästchen **Aktiviert**. Der Standardwert ist **Deaktiviert**.
2. Um die Verarbeitung von PDF-, Microsoft Office- und Windows PE-Dateien in einer Sitzung zu konfigurieren, aktivieren Sie die Kontrollkästchen **PDF umgehen**, **Office umgehen, Ausführbare Datei umgehen**.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern und sofort anzuwenden, wenn Malware Analysis neue Pakete empfängt.

Konfigurieren der Sandbox-Analysebewertung

Das Sandbox-Modul ist standardmäßig deaktiviert und MS Office- sowie PDF-Dateien werden nicht verarbeitet. Diese restriktive Einstellung soll verhindern, dass potenziell vertrauliche Informationen ohne ausdrückliches Einverständnis des Benutzers außerhalb des Netzwerks übertragen werden. Wurde ein Dokumenttyp nicht von der Verarbeitung ausgeschlossen, wird die gesamte Datei (nicht nur der Hash-Wert) an den Sandbox-Zielserver gesendet.

Außerdem können Sie angeben, dass der ursprüngliche Dateiname bei der Sandbox-Analyse beibehalten werden soll.

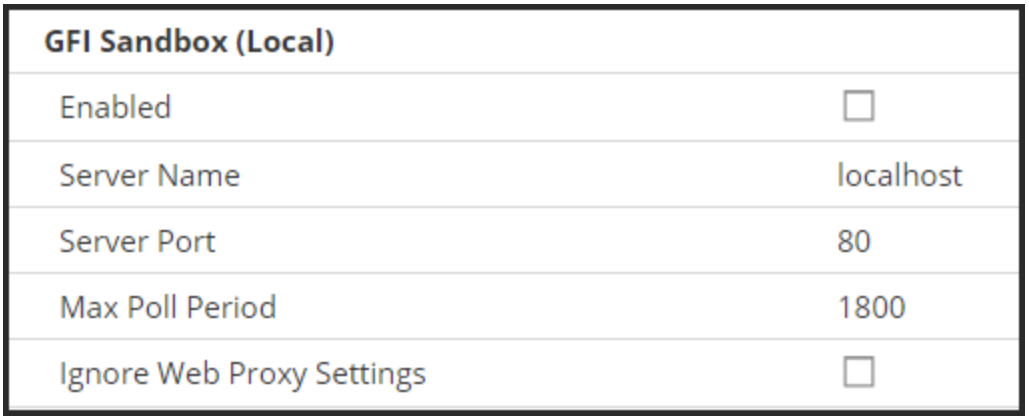
Hinweis: Wenn Sie den Parameter **Ursprünglichen Dateinamen beim Ausführen der Sandbox-Analyse beibehalten** nicht aktivieren, weist NetWitness Suite der Datei einen Hash-Wert zu.



Wenn Sie das Sandbox-Modul aktivieren, müssen Sie angeben, ob die Sandbox-Verarbeitung über eine lokale GFI-Sandbox, eine lokale ThreatGrid-Sandbox oder eine Cloudversion der ThreatGrid-Sandbox durchgeführt werden soll. Die Cloudversion der ThreatGrid-Sandbox wird direkt von ThreatGrid bereitgestellt und erfordert einen Aktivierungsschlüssel, der von ThreatGrid angefordert werden kann und auf der Registerkarte „ThreatGRID“ konfiguriert werden muss.

Einstellungen für eine GFI-Sandbox

Um eine lokal installierte GFI-Sandbox zu verwenden, müssen Sie GFI aktivieren und den Servernamen und Serverport des GFI-Sandboxservers angeben. Mit den Angaben unter „Max. Polling-Dauer“ und „Polling-Intervall“ wird angegeben, wie lange die Verarbeitungszeit für eine übermittelte Stichprobe sein darf und wie oft der Status geprüft werden soll (in Sekunden). Über die Option „Webproxyeinstellungen ignorieren“ können Sie angeben, dass Malware Analysis beim Herstellen einer Verbindung keinen Webproxy verwenden soll. Wenn kein Webproxy in Malware Analysis konfiguriert wurde, wird die Einstellung ignoriert.



Einstellungen für eine ThreatGrid-Sandbox

Hinweis: Bevor die ThreatGrid-Bewertung aktiviert werden kann, muss ein von ThreatGrid bereitgestellter Serviceschlüssel konfiguriert werden, sodass ThreatGrid von dieser Site übermittelte Stichproben als legitim einstuft. Nutzen Sie NetWitness Suite, um einen ThreatGrid-API-Schlüssel abzurufen, und aktivieren und konfigurieren Sie dann eine lokal installierte ThreatGrid-Sandbox oder die ThreatGrid-Cloud-Sandbox. Weitere Informationen finden Sie unter: Registrieren für einen ThreatGrid-API-Schlüssel.

Über die Einstellung „Webproxyeinstellungen ignorieren“ können Sie angeben, dass Malware Analysis beim Herstellen einer Verbindung keinen Webproxy verwenden soll. Wenn kein Webproxy in Malware Analysis konfiguriert wurde, wird die Einstellung ignoriert.

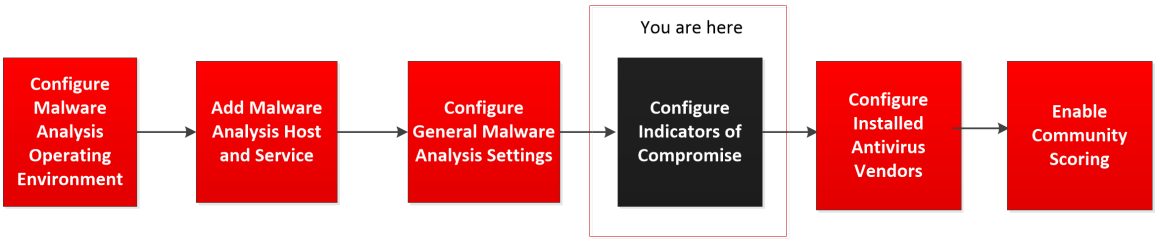
Gehen Sie zum Konfigurieren der Sandbox-Bewertung im Abschnitt „Modulkonfiguration“ wie folgt vor:

1. Klicken Sie zum Aktivieren oder Deaktivieren der Sandbox-Analyse auf das Kontrollkästchen **Aktiviert**. Der Standardwert ist **Deaktiviert**.
2. Um die Verarbeitung von PDF-, Microsoft Office- und Windows PE-Dateien in einer Sitzung zu konfigurieren, aktivieren Sie bei Bedarf die Kontrollkästchen **PDF umgehen**, **Office umgehen, Ausführbare Datei umgehen**.

3. Konfigurieren Sie den aktiven Sandbox-Anbieter. Sie haben drei Möglichkeiten:
   a. Wenn Sie eine lokal installierte Instanz der GFI-Sandbox verwenden möchten, geben Sie den Servernamen und Serverport des GFI-Sandbox-Servers ein, legen Sie „Max. Polling-Dauer“ und „Polling-Intervall“ fest und aktivieren Sie optional das Kontrollkästchen „Webproxyeinstellungen ignorieren“.
   b. Wenn Sie eine lokal installierte Instanz von ThreatGrid verwenden möchten, aktivieren Sie die ThreatGrid-Bewertung, geben Sie den ThreatGrid-Serviceschlüssel an und aktivieren Sie optional das Kontrollkästchen „Webproxyeinstellungen ignorieren“.
   c. Um die ThreatGrid-Cloud verwenden zu können, benötigen Sie zunächst einen ThreatGrid-API-Schlüssel. Aktivieren Sie dann die ThreatGrid-Bewertung, geben Sie den ThreatGrid-Serviceschlüssel an, geben Sie die URL für den ThreatGrid-Server ein (https://panacea.threatgrid.com) und aktivieren Sie optional das Kontrollkästchen „Webproxyeinstellungen ignorieren“.
4. Klicken Sie auf **Anwenden**.
   Die Änderungen werden sofort wirksam.

Konfigurieren der Indikatoren für eine Infizierung

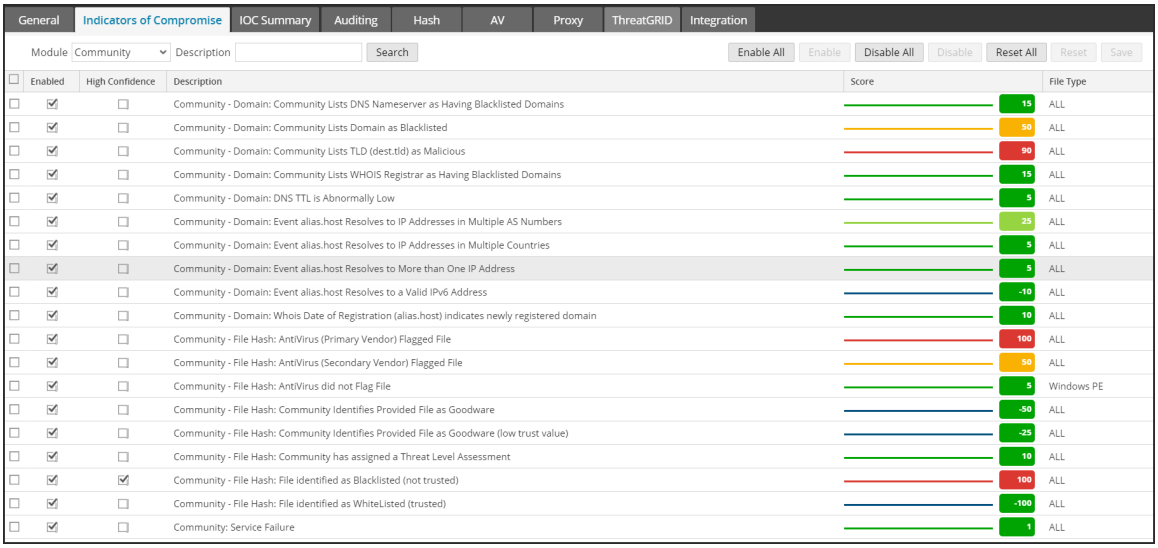
Die Indikatoren für eine Infizierung (Indicators of Compromise – IOC) für die Bewertungsmodule von Malware Analysis werden konfiguriert, weil jedes Malware Analysis-Bewertungsmodul – Netzwerk, Statisch, Community, Sandbox und YARA – eine Standardeinstellung für die IOCs hat, die zur Auswertung der Dateien und Sitzungen verwendet wird, um den Wahrscheinlichkeitsgrad einer Infizierung mit Schadsoftware zu bewerten.



Auf jeden IOC wird eine Bewertungsskala von -100 (gut) bis 100 (schlecht) angewendet. Wenn ein IOC ausgelöst wird, wird die angewendete Bewertungsskala in die Gesamtbewertung der analysierten Datei oder Sitzung miteinberechnet. Die einzelnen Bewertungsgewichtungen aller passenden IOCs werden aggregiert und ergeben die Endbewertung jeder Sitzung oder Datei. Die aggregierte Bewertung wird angepasst, um sicherzustellen, dass sie innerhalb der zulässigen Bewertungsskala (-100 bis 100) liegt.

Hinweis: Die gewichtete Bewertung, die einem IOC zugewiesen wurde, ist nicht zwingend der eindeutige Bewertungswert, der aggregiert wird (es handelt sich nicht um eine simple Addition von Bewertungen für die einzelnen IOCs, die ausgelöst wurden). Stattdessen ist die Bewertung eines IOCs eine Gewichtung oder ein Anzeichen der Wichtigkeit, die bei der Berechnung einer allgemeinen Bewertung berücksichtigt werden.

Die Konfigurationseinstellungen der Indikatoren für eine Infizierung (IOC) für Malware Analysis finden Sie in der Ansicht „Servicekonfiguration“ auf der Registerkarte „Indikatoren für eine Infizierung“. Es folgt ein Beispiel für eine Registerkarte.



Verwendung von **Community – Datei-Hash: Bei einem IOC von AntiVirus (Primärer Anbieter) als schädlich markierter Datei** kann die IOC-Punktezahl beispielsweise auf 100 eingestellt werden. Malware Analysis schwächt diesen Wert jedoch auf Grundlage des Prozentsatzes des primären AV-Anbieters ab, welcher der Schädlichkeit der Probe zustimmt. Je näher die Anbieter, die zustimmen, dass die Probe schädlich ist, bei der 100 %-Marke liegen, desto höher ist der Wert der 100 Punkte, die für die Aggregation einer Bewertung verwendet werden. Nähert sich der Prozentsatz dem Nullwert, fällt die Proportion der 100 Punkte in der aggregierten Bewertung ab.

IOCs verwenden die nativ in Malware Analysis implementierte Logik. Sie können die Logik nicht anpassen. Stattdessen können Sie nur IOCs anpassen, sodass deren Auswirkung auf die Bewertung steigt oder sinkt, um eine Konfidenzeinstellung anzugeben oder die IOC an- oder auszuschalten. Das typische Szenario ist das Tuning einer limitierten Einstellung von IOC-Punkten in der Bewertungsgewichtung für IOCs nach unten, welche die Endbewertung vergrößern und falsch positive Analyseergebnisse erzeugen. Eine extreme Version des Tunings wäre IOCs zu deaktivieren, wenn diese ständig zu falsch-positiven Ergebnissen beitragen. Außerdem können Sie alle IOCs deaktivieren und wählen, einige wenige aktiv zu lassen. Es können zum Beispiel alle IOCs mit Ausnahme einiger weniger ausgewählten IOCs, die AntiVirus-Treffer erkennen, deaktiviert werden. Durch die Verwendung von Malware Analysis in dieser sehr eingeschränkten Konfiguration können Sie Ergebnisse in Malware Analysis verringern, sodass nur bekannte AV-Treffer Ergebnisse erzeugen.

Sie können diese Funktionen auf verschiedene Arten konfigurieren:

- Deaktivieren Sie IOCs, sodass diese nicht als Teil des Bewertungsmoduls, zu dem sie zugeteilt wurden, berechnet werden.
- Passen Sie die Bewertungsgewichtung für einen IOC an, sodass seine Auswirkung auf die aggregierte Bewertung vergrößert oder verkleinert wird.
- Markieren Sie IOCs, von denen Sie glauben, sie seien starke Indikatoren für Schadsoftware, und versehen Sie Sitzungen, die diese IOCs in den Malware Analysis-Ergebnissen ausgelöst haben, mit einem Flag für hohe Vertrauenswürdigkeit (HC).
- Passen Sie die Bewertung und Einstellungen zur Vertrauenswürdigkeit einzig und allein dem Dateityp an, der analysiert wird. Jeder IOC wurde ein Dateityp vorab zugeteilt, auf den sie angewendet wird. Mögliche Werte sind **ALLE**, **PDF**, **MS Office** und **Windows PE**. Der IOC, auf den die meisten Dateitypen zutreffen, wird während der dateibasierten Analyse verwendet. Wird zum Beispiel eine PDF analysiert, wird eher ein IOC mit einem Dateitypen mit dem Wert **PDF** gewählt als derselbe IOC mit einem Dateityp mit dem Wert **ALL**. Wenn es keinen dateitypenspezifischen Treffer gibt, wird der IOC mit dem Dateitypen mit dem Wert **ALL** gewählt.
- Suchen Sie nach Regeln, die im Raster angezeigt werden, basierend auf einem Treffer der Regelbeschreibung.

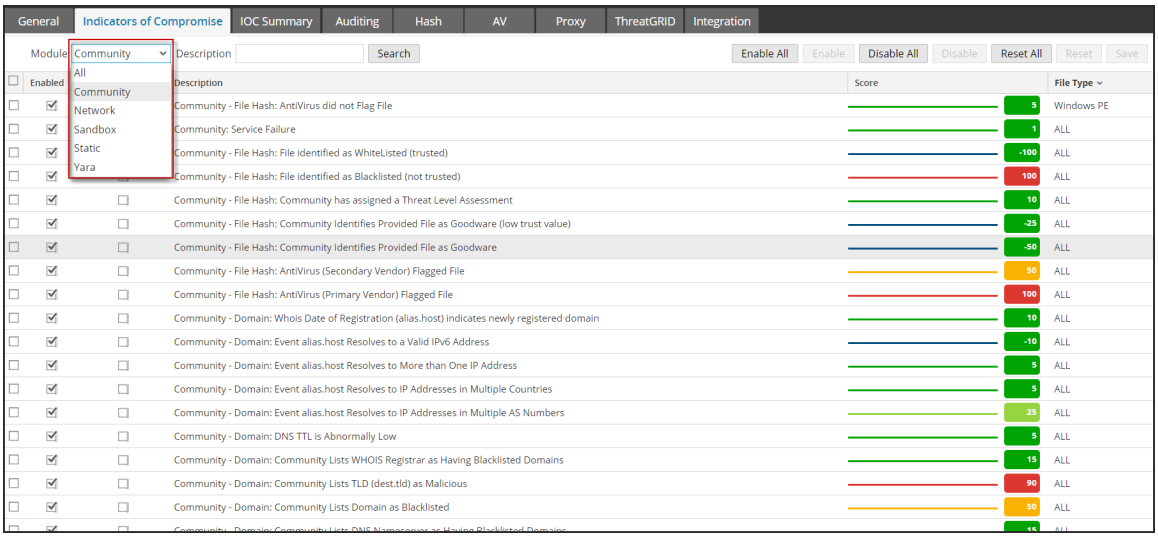
Filtern der angezeigten IOCs nach Modul

Sie können die angezeigten IOCs nach dem Bewertungsmodul nach einem der vier integrierten Modulen oder YARA filtern. YARA-basierte IOCs überlappen mit den ursprünglichen IOCs mit jeder Kategorie. Obwohl YARA-IOCs in den anderen Ansichten nicht als solche identifiziert werden, können Sie YARA aus der Auswahlliste Modul auswählen, um eine Liste der YARA-Regeln anzusehen.

So sehen Sie IOCs für ein oder vier Bewertungsmodule oder für YARA an:

1. Wählen Sie im **Hauptmenü** die Optionen **Admin > Services aus.**
2. Wählen Sie einen Malware Analysis Service aus.
3. Wählen Sie in der Zeile  **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Indikatoren für eine Infizierung**.
5. Wählen Sie in der Auswahlliste **Modul** Alle, NextGen, Statisch, Community, Sandbox, oder Yara aus.

   Die konfigurierten Regeln und Einstellungen für das Modul werden angezeigt.



Filtern der angezeigten Module, damit nur veränderte Module angezeigt werden

Die Registerkarte **Indikatoren für eine Infizierung** identifiziert lokal veränderte IOCs visuell. Wenn zum Beispiel ein IOC verändert wurde, wurde die Bewertungsgewichtung verändert und der Name wird rot angezeigt. Er enthält einen Indikator für Veränderung im Anhang an den IOC-Namen. Der Indikator für Veränderung ist ++ und kann als Filtermechanismus beim Suchen nach IOCs verwendet werden.
So beschränken Sie die Ansicht auf lokal veränderte IOCs:

1. Geben Sie im Feld **Beschreibung** ++ ein.
2. Klicken Sie auf **Suchen**.

   Die Ansicht wird gefiltert, sodass nur veränderte IOCs angezeigt werden.

Aktivieren und Deaktivieren von IOCs für ein Bewertungsmodul

Wenn ein IOC deaktiviert wird, hat er keine Auswirkungen mehr auf die aggregierte Bewertung des dazugehörigen Bewertungsmoduls. Wenn ein IOC mehrere Instanzen (die sich nur durch den Dateitypen unterscheiden) hat, hat das Deaktivieren eines dateitypspezifischeren IOC die Verwendung einer dateitypagnostischeren Version der IOC-Bewertung zur Folge.
Wenn zum Beispiel derselbe IOC als Dateityp **ALL** und als Dateityp **Windows PE** existiert, hat das Deaktivieren der Instanz **Windows PE** des IOC zur Folge, dass bei der Bewertung die Version **ALL** verwendet wird. Um den IOC für **Windows PE** völlig zu deaktivieren, während er für andere Dateitypen aktiv bleibt, stellen Sie die Bewertungsgewichtung der Instanz **Windows PE** des IOC auf einen Wert von null, wie unten beschrieben. Dadurch bleibt der IOC für Windows-PE-Dateien aktiv (obwohl er eine Gewichtung von null hat und nicht in den Analyseergebnissen angezeigt wird) und hat keine Auswirkungen auf andere Dateitypen. Die verbleibenden Dateitypen verwenden weiterhin die Instanz **ALL** des IOC.

So aktivieren oder deaktivieren Sie einen IOC, sodass er im Bewertungsmodul nicht mehr berücksichtigt wird:

1. Wählen Sie im **Hauptmenü** die Optionen **Admin > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und in der Zeile  > **Ansicht > Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Indikatoren für eine Infizierung**.
4. Wählen Sie in der Auswahlliste **Modul** ein Bewertungsmodul aus: Alle, Community, Netzwerk, Sandbox, Statisch, oder Yara.
   Die konfigurierten Regeln und Einstellungen für das Modul werden angezeigt.
5. Führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie in der Spalte neben der Regel, die Sie aktivieren möchten, auf das Kontrollkästchen **Aktivieren**.
   b. Wählen Sie eine oder mehrere Regeln aus und klicken Sie in der Symbolleiste auf **Aktivieren** oder **Deaktivieren**.
   c. Um bei allen auf der Seite angezeigten Regeln zwischen Aktivieren und Deaktivieren umschalten zu können, klicken Sie im Spaltentitel auf das Kontrollkästchen **Aktiviert**.
   d. Um alle Regeln für ein Bewertungsmodul zu aktivieren oder deaktivieren, klicken Sie in der Symbolleiste auf **Alle aktivieren** oder **Alle deaktivieren** .
6. Um die Änderungen an der Seite zu speichern, klicken Sie in der Symbolleiste auf **Speichern**.

> **Hinweis:** Regeln, die Einstellungen geändert haben, werden mit einer roten Ecke gekennzeichnet. Wenn Sie vor dem Speichern zu einer anderen Regelseite navigieren, gehen alle Änderungen an dieser Seite verloren.

Anpassung der Bewertungsgewichtung für IOCs

Die Anpassung der Bewertungsgewichtung für IOCs verstärkt oder verringert die allgemeinen Auswirkungen einer IOC auf die aggregierte Bewertung des Moduls, in welchem sie konfiguriert ist. Um den allgemeinen Einfluss von IOCs zu vergrößern oder verkleinern, verkleinern Sie den aktuellen Wert auf eine neue Einstellung.

- Werte zwischen -100 und -1 deuten darauf hin, dass die analysierte Sitzung oder Datei wahrscheinlich keine Schadsoftware ist (bei -100 ist die Wahrscheinlichkeit am geringsten, dass es sich um eine Schadsoftware handelt).
- Werte zwischen 1 und 100 deuten darauf hin, dass die analysierte Sitzung oder Datei wahrscheinlich eine Schadsoftware ist (bei 100 ist die Wahrscheinlichkeit am höchsten, dass es sich um eine Schadsoftware handelt).

- Bei einer Einstellung des Wertes auf Null bleibt der IOC aktiv, hat aber keinen Einfluss mehr auf die aggregierte Bewertung und wird nicht mehr in den Analyseergebnissen angezeigt. Die Einstellung des Wertes auf null stellt eine Methode dar, um eine dateitypenspezifische Instanz eines IOC zu deaktivieren, während die ursprüngliche dateitypagnostische Instanz für die Bewertung der verbleibenden Dateitypen intakt bleibt.

So passen Sie die Bewertungsgewichtung an:

1. Wählen Sie im **Hauptmenü** die Optionen **Admin > Services** aus.
2. Wählen Sie einen Malware Analysis Service aus.
3. Wählen Sie in der **Symbolleiste** die Optionen **Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Indikatoren für eine Infizierung**.
5. Wählen Sie in der Auswahlliste **Modul** ein Bewertungsmodul aus: Alle, Netzwerk, Statisch, Community, Sandbox oder Yara.
   Die konfigurierten Regeln und Einstellungen für das Modul werden angezeigt.
6. Führen Sie einen der folgenden Schritte aus:
   a. Verschieben Sie den Regler nach links oder rechts um die Bewertungsgewichtung zu vergrößern oder verkleinern.
   b. Klicken Sie direkt auf die angezeigte Bewertungsgewichtung und geben Sie eine neue Bewertungsgewichtung ein.
7. Um die Änderungen an der Seite zu speichern, klicken Sie in der Symbolleiste auf **Speichern**.

   Hinweis: Regeln, die Einstellungen geändert haben, werden mit einer roten Ecke gekennzeichnet. Wenn Sie vor dem Speichern zu einer anderen Regelseite navigieren, gehen alle Änderungen an dieser Seite verloren.

Einstellen der Kennzeichnung Hohe Wahrscheinlichkeit für IOCs

Die Einstellung Hohe Vertrauenswürdigkeit wird als Kennzeichnungsmethode für spezifische IOCs mit Indikatoren von hoher Vertrauenswürdigkeit, dass eine Schadsoftware vorhanden ist, verwendet. Zum Beispiel **Community - Datei-Hash: Der IOC Von AntiVirus (Primärer Anbieter) als schädlich markierte Datei** weist eine geringe Wahrscheinlichkeit für ein falsch-positives Ergebnis und gleichzeitig eine hohe Wahrscheinlichkeit für eine akkurate Messung von

vorhandener Schadsoftware auf. Durch die Kennzeichnung dieser (und anderer) IOCs als hoch vertrauenswürdig können Sie einen Filter in den Malware Analysis-Ergebnissen verwenden, sodass nur die Sitzungen angezeigt werden, die eine oder mehrere vertrauenswürdige Regeln beinhalten. Dadurch wird die Ansicht auf eine kleinere Teilmenge jener Ergebnisse beschränkt, deren Genauigkeit ein höherer Grad an Vertrauenswürdigkeit zugeteilt wird. Eine nicht auf hochvertrauenswürdige IOCs beschränkte Ansicht der Ergebnisse ermöglicht Ihnen weiterhin eine Ansicht der weniger eindeutigen Ergebnisse. Dies sorgt für Ergebnisse, bei denen die Wahrscheinlichkeit, dass sie falsch-positiv sind, geringer ist. Die Wahl, Ergebnisse nach dem Konfidenzlevel zu filtern oder nicht, ist ein gültiges Fallbeispiel in dem NetWitness Suite-Workflow.

So stellen Sie die Kennzeichnung Hohe Wahrscheinlichkeit ein:

1. Wählen Sie auf der Registerkarte **Indikatoren für eine Infizierung** ein Bewertungsmodul aus der Auswahlliste **Modul** aus: Alle, Netzwerk, Statisch, Community, Sandbox oder Yara. Die konfigurierten Regeln und Einstellungen für das Modul werden angezeigt.
2. Klicken Sie in der Spalte neben der Regel, die Sie mit der Kennzeichnung „Wahrscheinliches“ oder „Nichtwahrscheinliches“ Indikatoren für eine Schadsoftware markieren möchten, in einer Sitzung auf das Kontrollkästchen **Hohe Wahrscheinlichkeit**.
3. Um die Änderungen an der Seite zu speichern, klicken Sie in der Symbolleiste auf **Speichern**.

> **Hinweis:** Regeln, die Einstellungen geändert haben, werden mit einer roten Ecke gekennzeichnet. Wenn Sie vor dem Speichern zu einer anderen Regelseite navigieren, gehen alle Änderungen an dieser Seite verloren.

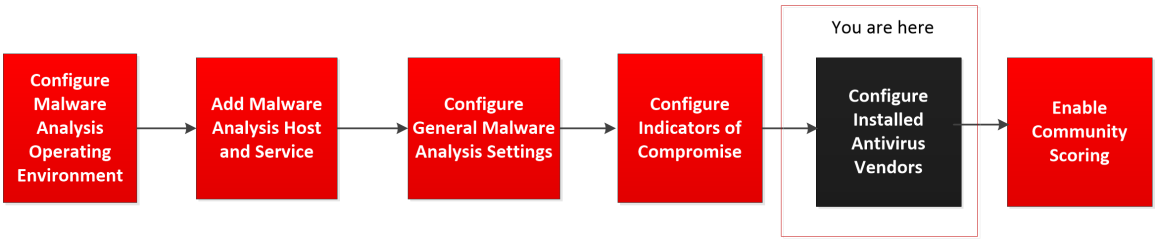
Zurücksetzen von IOCs auf die Standardeinstellungen

1. Wählen Sie auf der Registerkarte **Indikatoren für eine Infizierung** ein Bewertungsmodul aus der Auswahlliste Modul aus: Alle, Netzwerk, Statisch, Community, Sandbox oder Yara. Die konfigurierten Regeln und Einstellungen für das Modul werden angezeigt.
2. Wenn Sie alle Regeln auf der aktuellen Seite auf deren Standardeinstellungen zurücksetzen möchten, klicken Sie in der Symbolleiste auf **Zurücksetzen**.
3. Wenn Sie alle Regeln des gewählten Bewertungsmoduls auf ihre Standardeinstellungen zurücksetzen möchten, klicken Sie in der Symbolleiste auf **Alle zurücksetzen**.
4. Um die Änderungen an der Seite zu speichern, klicken Sie in der Symbolleiste auf **Speichern**.

Konfigurieren installierter Virenschutzanbieter

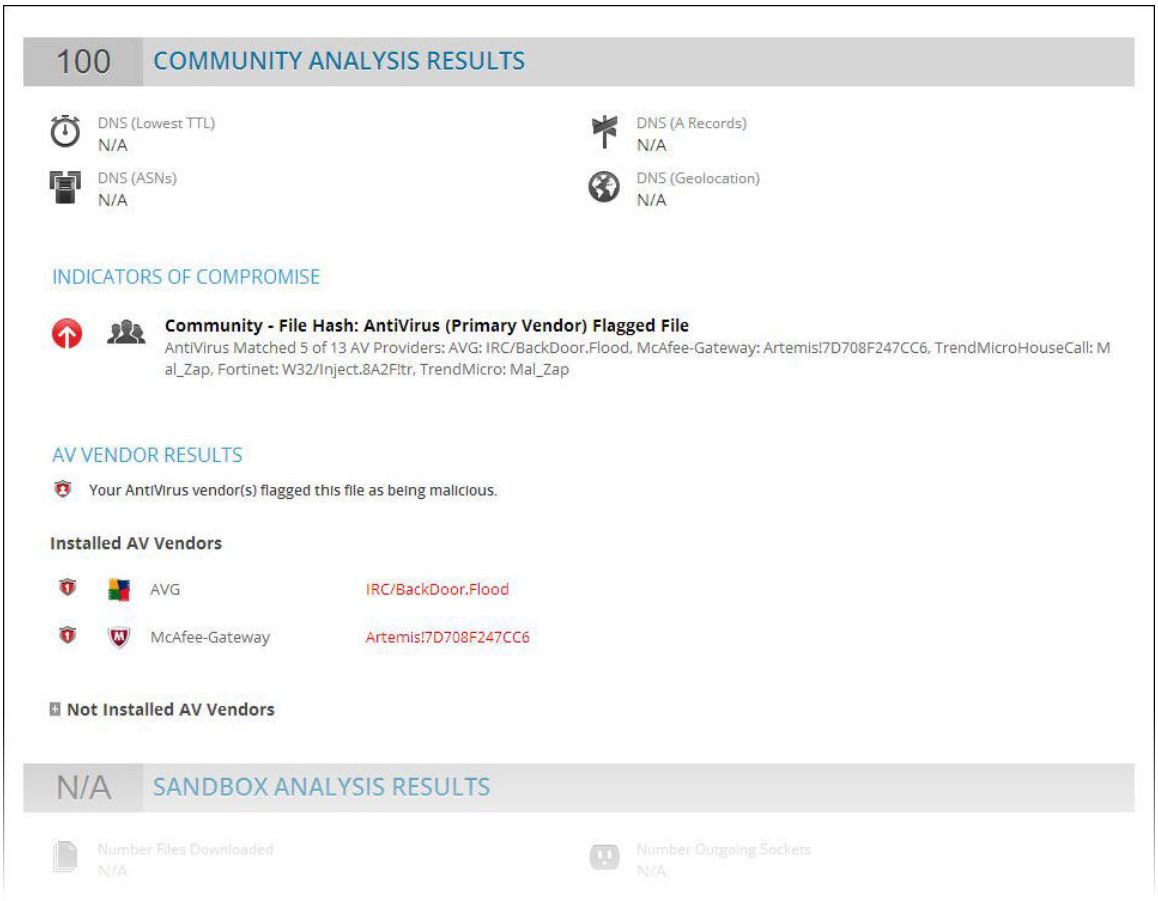
Sie können Dateianalyseergebnisse von Ihren installierten Virenschutzanbietern mit Communityergebnissen aus der Malware Analysis-Wissensdatenbank vergleichen. Während eine Datei durch Communityanalyse analysiert wird, prüft Malware Analysis eine Antivirus-Wissensdatenbank, um festzustellen, ob die Stichprobe bereits als schädlich bekannt ist. Wenn die Datei als schädlich bekannt ist, markiert NetWitness Suite die Datei, um anzuzeigen, ob ein primärer oder ein sekundärer Virenschutzanbieter die Stichprobe identifiziert hat. NetWitness Suite stuft Anbieter als primär oder sekundär ein, um den Reputationsgrad anzuzeigen, den die Anbieter in der Branche haben, und bei den Infizierungsindikatoren wird diese Reputation berücksichtigt. So hat zum Beispiel eine Erkennung nur von sekundären Virenschutzanbietern möglicherweise geringeres Gewicht als die Erkennung von primären Anbietern.

Hinweis: Wenn Sie Virenschutzsoftware in Ihrem Netzwerk installieren, wird dringend empfohlen, dass Sie mindestens einen Anbieter von der NetWitness Suite-Liste mit primären Anbietern auswählen.



Sie können die in Ihrem Netzwerk installierten Virenschutzanbieter gegenüber NetWitness Suite kenntlich machen. NetWitness Suite vergleicht die Virenschutzergebnisse während der Communityanalyse mit den Ergebnissen der installierten Anbieter, die in der Registerkarte „Virenschutz“ ausgewählt sind. Wenn eine Übereinstimmung erkannt wird, wird die analysierte Datei markiert, um anzuzeigen, dass Ihre lokal installierte primäre oder sekundäre Virenschutzsoftware die Stichprobe erkannt hat.

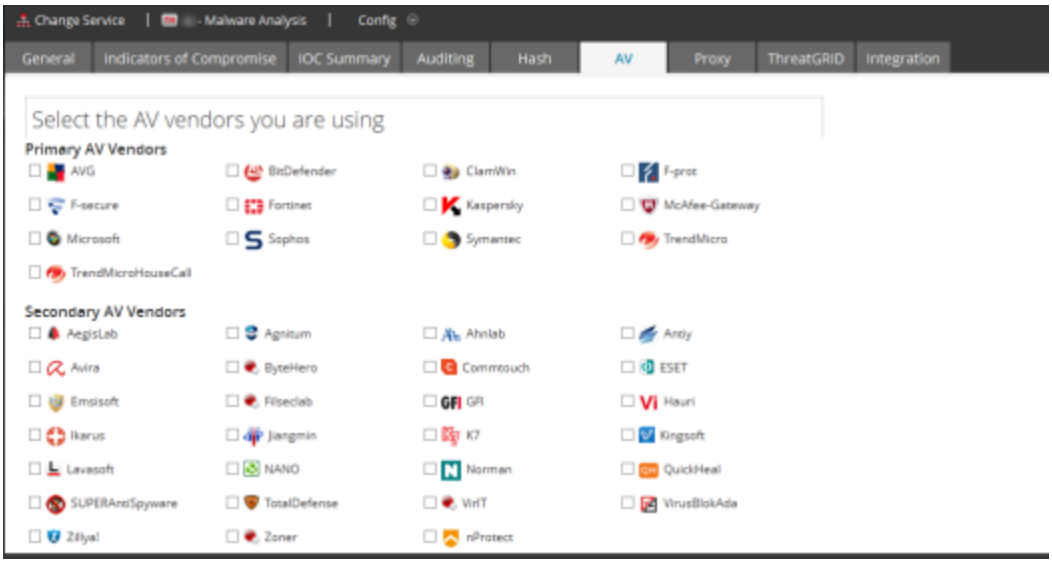
Das Beispiel unten zeigt die Ergebnisse der Communityanalyse für eine Datei mit einer Punktzahl von 100. Unter **Indikatoren für eine Infizierung** können Sie sehen, dass die Datei durch die aufgelisteten Virenschutzanbieter in der Community markiert wurde. Unter **AV-Anbieterergebnisse** zeigt NetWitness Suite an, ob die in Ihrer Umgebung installierten Virenschutzanbieter die Datei als schädlich markiert haben. Wenn Ihre installierten Virenschutzanbieter den Virus erkannt haben, wird der Name der Schadsoftware angezeigt. Wenn Ihre installierten Virenschutzanbieter den Virus nicht erkannt haben, wird **--Nicht erkannt--** neben dem Namen des Virenschutzanbieters angezeigt. Unter **Nicht installierte Anbieter** können Sie auf + klicken, um den Abschnitt einzublenden und um zu sehen, ob andere Anbieter, die nicht in Ihrem System installiert sind, den Virus erkannt haben.



Identifizieren installierter Virenschutzsoftware

So identifizieren Sie in Ihrem Netzwerk installierte Virenschutzsoftware:

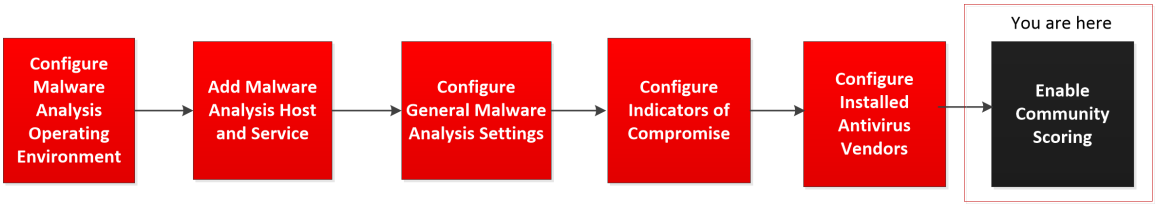
1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und in der Zeile > **Ansicht** > **Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Virenschutz** aus.



4. Aktivieren Sie das Kontrollkästchen neben jedem Virenschutzanbieter (primäre und andere), die in Ihrem Netzwerk installiert sind.
5. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.
   Die Communityanalyseergebnisse zeigen an, ob Ihre Software ein Ereignis markiert hat.
6. (Optional) Wenn Sie die Liste der installierten AV-Software auf den Standardwert (keine) zurücksetzen möchten, klicken Sie auf **Zurücksetzen**.
   Alle ausgewählten Elemente werden entfernt.
7. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.

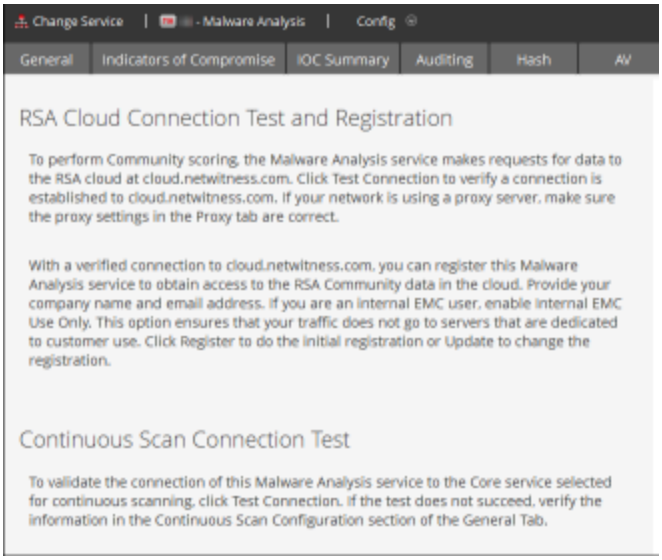
Aktivieren der Communityanalyse

Ein Administrator kann die Communityanalyse aktivieren. Bei der Communityanalyse wird neue im Netzwerk entdeckte Schadsoftware in die RSA-Cloud übertragen, um sie anhand der RSA-Daten zur Schadsoftwareanalyse und der Feeds vom SANS Internet Storm Center, von SRI International, vom US-Finanzministerium und von VeriSign zu prüfen. Um die Communityanalyse zu aktivieren, müssen Sie sich bei der RSA-Cloud registrieren, die Verbindung zur Cloud testen und dann die Verbindung zwischen der RSA-Cloud und dem konfigurierten Service für kontinuierliches Scannen testen.



Eine vollständige Beschreibung der Analysemethoden finden Sie unter Funktionsweise von Malware Analysis.

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann in der Zeile > **Ansicht** > **Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Integration** aus.



4. Blättern Sie nach unten zu „Verbindungstest für kontinuierliches Scannen“ und klicken Sie auf **RSA-Cloud-Verbindungstest und -Registrierung**.

   NetWitness Suite testet die Kommunikation mit der Website unter `https://cloud.netwitness.com`. Wenn Ihr Unternehmen einen Proxy für ausgehenden Datenverkehr verwendet wird, prüfen Sie die Proxyeinstellungen. Eine gültige Verbindung ist erforderlich, um sich beim RSA Community Service zu registrieren.

5. Geben Sie Ihren Unternehmensnamen und eine E-Mail-Kontaktadresse ein. Klicken Sie auf **Register**.

   Wenn alle Pflichtfelder ausgefüllt sind, ist Ihre Registrierung abgeschlossen. Die Bezeichnung auf der Schaltfläche für die Registrierung wird in „Aktualisieren“ geändert.

6. Klicken Sie auf **Verbindungstest für kontinuierliches Scannen**, um zu überprüfen, ob der Malware Analysis-Service eine Verbindung zum ausgewählten Core-Service für kontinuierliches Scannen herstellen kann.

   NetWitness Suite initiiert eine Überprüfung basierend auf den Angaben unter „Quellhost“, „Quellport“, „Benutzername“ und „Benutzerpasswort“ in der Registerkarte „Allgemein“. Wenn der Test erfolgreich ausgeführt wird, können Analysten die Communitybewertungen in Malware Analysis sehen.

(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host

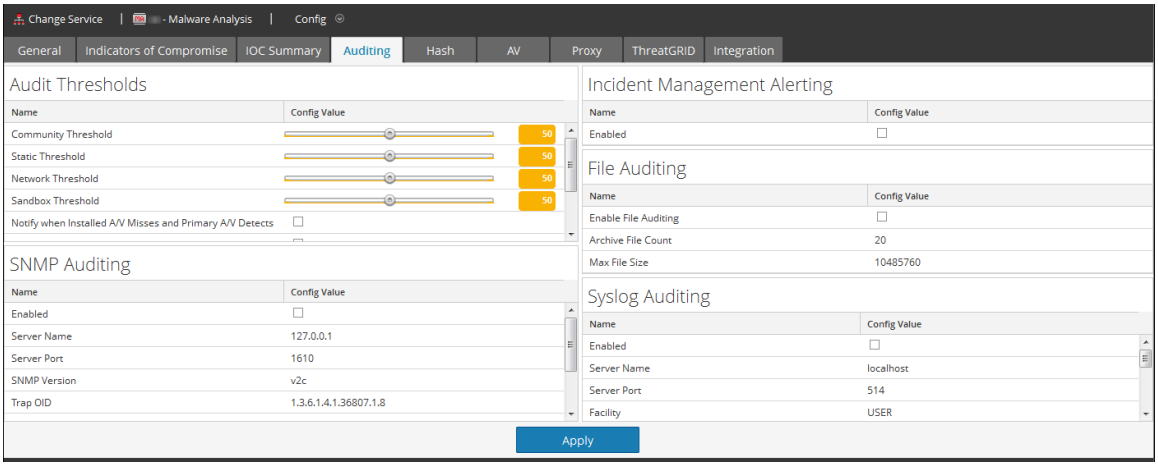
In diesem Thema werden die konfigurierbaren Funktionen des Auditing-Protokolls von Malware Analysis eingeführt und Verfahren zur Konfiguration der Funktionen erläutert. Malware Analysis kann basierend auf konfigurierten Bewertungsmodulschwellenwerten Auditingwarnmeldungen erzeugen. Wenn die Analysebewertung für eine Datei in einer Analysesitzung den oder die konfigurierten Schwellenwerte erreicht oder überschreitet, wird eine Auditing-Warnmeldung erzeugt. Durch diese Schwellenwerte können Sitzungen und Dateien, deren Bewertung hoch genug ist, um auf mögliche Schadsoftware hinzuweisen, automatisch eine Warnmeldung erzeugen.

Warnmeldungen können so konfiguriert werden, dass sie als SNMP-, Syslog- oder Datei-Einträge formatiert werden. Durch die Unterstützung verschiedener Auditformate können externe Systeme Auditing-Ereignisse in einer Form erhalten, in der sie die unterstützten Formate analysieren können.

Neben Auditing-Analysesitzungen lösen auch die folgenden Ereignisse eine Audit-Warnmeldung aus:

- Erfolgreiche und fehlgeschlagene Benutzeranmeldungen
- Änderungen an den Systemkonfigurationseinstellungen
- Serverneustart
- Upgrade und Installation von Serverversionen

Die Konfigurationseinstellungen für das Auditing für Malware Analysis befinden sich in der Ansicht „Service-Konfiguration“ in der Registerkarte „Auditing“.



Konfigurieren des Auditing-Schwellenwerts

Der alleinige Zweck der Schwellenwerte besteht in der Angabe von Kriterien, die erreicht werden müssen, bevor eine Warnmeldung für eine analysierte Sitzung/Datei erzeugt wird. Wenn Auditing aktiviert ist, wird jede bewertete Datei/Sitzung untersucht, um festzustellen, ob die Bewertung in einem Bewertungsmodul den konfigurierte Auditing-Schwellenwert erreicht oder überschreitet. Wenn das der Fall ist, wird eine Warnmeldung im konfigurierten Audit-Warnmeldungsformat erzeugt (z. B. SNMP, Syslog oder Datei). Wenn Sie z B. SNMP konfigurieren und den Communityschwellenwert auf 90 setzen, erzeugen alle Sitzungen/Dateien, die im Communitybewertungsmodul mit 90 oder höher bewertet werden, ein SNMP-Trap. Wenn alle Schwellenwerte auf 90 eingestellt werden, wird erst dann eine Warnmeldung erzeugt, wenn eine Sitzung/Datei in den Netzwerk-, Community- und Sandbox-Bewertungsmodulen sowie im statischen Bewertungsmodul 90 oder höher erreicht.

So konfigurieren Sie den Auditing-Schwellenwert:

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und anschließend  **> Ansicht > Konfiguration** aus.
3. Klicken Sie in der Ansicht **Service-Konfiguration** auf die Registerkarte **Auditing**.
4. Im Abschnitt **Auditing-Schwellenwerte**:
   a. Stellen Sie **Communityschwellenwert**, **Statischer Schwellenwert**, **Netzwerkschwellenwert** und **Sandbox-Schwellenwert** ein, indem Sie für jedes Bewertungsmodul einen der folgenden Schritte ausführen:
      - Klicken Sie im Schieberegler auf den Griff und ziehen Sie ihn in eine der beiden Richtungen.
      - Geben Sie im Feld Wert eine Zahl zwischen 0 und 100 ein.
   b. (Optional für 10.3 SP2) Wählen Sie einen oder mehrere Auslöser aus, um eine Nachricht aufzuzeichnen und durch alle aktivierten Auditing-Methoden zuzustellen.
   c. Klicken Sie auf **Anwenden**.
      - Die Schwellenwerteinstellung tritt sofort für alle aktivierten Auditing-Methoden in Kraft: SNMP, Datei und Syslog.
      - Die aufgezeichneten Nachrichten werden über alle aktivierten Auditing-Methoden gesendet: SNMP, Datei und Syslog.

Konfigurieren von Warnmeldungen für Incident Management

Bei Aktivierung kann Incident Management Warnmeldungen in Malware Analysis überwachen und in den Incident Management-Workflow einspeisen.

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis Service und anschließend **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Auditing** aus.
4. Aktivieren Sie im Abschnitt **Incident-Management Alerting** das Kontrollkästchen „Aktiviert“ und klicken Sie auf „Anwenden“.
   Alerting tritt sofort in Kraft.

Konfigurieren des SNMP-Auditing

SNMP (Simple Network Management Protocol) ist ein Internetstandardprotokoll zum Managen von Services in IP-Netzwerken. Wenn das SNMP-Auditing aktiviert ist, kann Malware Analysis ein Auditereignis als SNMP-Trap an einen konfigurierten SNMP-Trap-Host senden. Neben Bewertung und Ereignis-ID umfasst die Warnmeldung alle Sitzungsmetadaten sowie erzeugte Metadaten. Dies ist für Benutzer hilfreich, die Ereignisdaten in Drittanbietersysteme eingeben möchten.

So konfigurieren Sie SNMP-Auditing:

1. Wählen Sie im Hauptmenü die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Auditing** aus.
4. Klicken Sie im Abschnitt **SNMP-Auditing** auf das Kontrollkästchen, um SNMP-Auditing zu aktivieren.
5. Konfigurieren Sie den SNMP-Servernamen und Port.
6. Konfigurieren Sie die SNMP-Version und die Trap-OID zum Senden von Traps.
7. Konfigurieren Sie die Malware Analysis-Community und die Parameter für erneute Versuche und Timeout beim Senden von Traps.
8. Klicken Sie auf **Anwenden**.
   Die SNMP-Auditing-Einstellungen treten sofort in Kraft.

Konfigurieren von Dateiaudit-Einstellungen

Wenn das Dateiauditing aktiviert ist, wird die Auditprotokolldatei im Stammverzeichnis von Malware Analysis hinterlegt. Der Standardspeicherort für die folgenden Protokolldateien lautet:

`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`.

Wenn ein Protokoll die maximale Dateigröße erreicht, wird es archiviert und ein neues Protokoll wird erstellt. Sowohl die Größe als auch die Anzahl dieser Auditprotokolle sind konfigurierbar.

Achtung: Vermeiden Sie es, die maximale Dateigröße und die Archivdateianzahl zu hoch einzustellen, da dadurch der verfügbare Festplattenspeicher auf der Malware Analysis-Appliance beeinträchtigt werden kann.

So konfigurieren Sie die Dateiaudit-Einstellungen:

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und anschließend  **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Auditing** aus.
4. Klicken Sie im Abschnitt **Dateiaudit** auf das Kontrollkästchen, um Dateiaudit zu aktivieren.
5. (Optional) Legen Sie die Anzahl Archivdateien und die maximale Dateigröße fest.
6. Klicken Sie auf **Anwenden**.
   Die Dateiaudit-Einstellungen treten sofort in Kraft.

Konfigurieren von Syslog-Auditing-Einstellungen

Wenn diese Funktion aktiviert ist, wird das Auditing von Syslog über das Syslog-Protokoll RFC 5424 bereitgestellt. Gemäß Vorschriften wie SOX, PCI DSS, HIPAA und vielen anderen müssen Unternehmen umfassende Sicherheitsmaßnahmen implementieren. Dies umfasst häufig das Sammeln und Analysieren von Protokollen aus vielen unterschiedlichen Quellen. Da es für Syslog zahlreiche systemeigene und Open-Source-Tools für das Reporting und Analysen gibt, hat sich Syslog als effektives Format zur Konsolidierung von Protokollen erwiesen.

Neben Bewertung und Ereignis-ID umfasst das Syslog alle Sitzungsmetadaten sowie erzeugte Metadaten. Dies ist für Benutzer hilfreich, die Ereignisdaten in Drittanbietersysteme eingeben möchten.

So konfigurieren Sie die Syslog-Auditing-Einstellungen:

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und anschließend  **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **Auditing** aus.
4. Klicken Sie im Abschnitt **Syslog-Auditing** auf das Kontrollkästchen, um Syslog-Auditing zu aktivieren.
5. Konfigurieren Sie den Host, auf dem der Syslog-Zielprozess ausgeführt wird, und den Port auf dem Host, den der Syslog-Prozess abhört.

6. Konfigurieren Sie Einrichtung, Codierung, Format, maximale Länge und Zeitstempel für die ausgehenden Syslog-Nachrichten.

   Hinweis: (Optional) Konfigurieren Sie die Identitätszeichenfolge, die am Anfang der Syslog-Warnmeldungen eingefügt werden soll.
   Zusätzliche Erwägungen zum CEF-Format finden Sie unter Erstellen angepasster Warnmeldungen im CEF-Format.

7. Klicken Sie auf **Anwenden**.

   Die Syslog-Auditing-Einstellungen treten sofort in Kraft.

(Optional) Konfigurieren eines Hash-Filters

In diesem Thema wird erklärt, wie Hash-Filter zum Markieren von sauberen oder fehlerhaften Dateien in Malware Analysis verwendet werden können. Das Verfahren des Hash-Filterns ermöglicht es Ihnen, ein Verzeichnis mit sauberen und fehlerhaften Datei-Hashes zu führen. Auf der Registerkarte „Hash“ können Sie die Malware Analysis-Ereignisanalyse basierend auf Datei-Hashes anpassen. Wird ein Datei-Hash als sauber markiert, analysiert Malware Analysis diesen beim nächsten Mal nicht mehr. Wird ein Datei-Hash als fehlerhaft markiert, erhöht Malware Analysis den Communitywert der Datei automatisch um eine hohe Anzahl von Punkten. Malware Analysis analysiert diese Datei weiterhin, um zu überprüfen, ob neue Informationen zur Verfügung gestellt werden.

Hinweis: Enthält ein Ereignis eine einzelne Datei und wird der Hash dieser Datei als sauber markiert, filtert Malware Analysis das gesamte Ereignis und Sie können es nicht in den Malware Analysis-Ergebnissen sehen.

Um Hash-Filter der Hash-Liste hinzuzufügen, können Sie eine der folgenden manuellen Methoden anwenden:

1. Hinzufügen mithilfe des Kontextmenüs in der Ereignisdetailansicht: Wenn Sie mit der rechten Maustaste auf eine Datei klicken, wird ein Kontextmenü geöffnet und Sie können den Hash der ausgewählten Datei als sauber (Normal) oder als fehlerhaft (Schädlich) markieren.
2. Symbolleiste der Registerkarte „Hash“: Klicken Sie in der Registerkarte „Hash“ auf „Hinzufügen“, um einen Datei-Hash und die Dateigröße hinzuzufügen und optional den Hash als vertrauenswürdig zu markieren.

Es gibt zudem eine automatisierte Methode, um Malware Analysis Hash-Filter hinzuzufügen. Sie können eine Hash-Liste als Ganzes aus dem überwachten Ordner importieren. Hashes, die durch den überwachten Ordner importiert wurden, erscheinen nicht in der Hash-Liste. Kopieren Sie mit diesem Massenimport und dem überwachten Verzeichnis (/var/netwitness/malware-analytics-server/spectrum/hashWatch), das auf dem Malware Analysis-Server eingerichtet wurde, eine Hash-Liste in den überwachten Ordner, sodass diese Liste automatisch in das System importiert wird. Hashes, die mithilfe des Massenimports importiert wurden, überschreiben Hashes, die zuvor durch den überwachten Ordner importiert wurden.

Anzeigen der Hash-Liste

So zeigen Sie die Hash-Liste an:

1. Wählen Sie im **Hauptmenü** die Optionen **ADMIN > Services** aus.
2. Wählen Sie in der Ansicht „Services“ einen Malware Analysis-Service und dann die Optionen  **>Ansicht > Konfiguration** aus.
3. Wählen Sie die Registerkarte **Hash** aus.

   Die Hash-Liste wird in der Registerkarte „Hash“ angezeigt. Es werden nur Datei-Hashes angezeigt, die durch eine der gezeigten Methoden hinzugefügt wurden.

Hinzufügen eines Datei-Hashs zum Hash-Filter

So fügen Sie dem Hash-Filter einen Datei-Hash hinzu:

1. Klicken Sie in der Registerkarte **Hash** auf **Hinzufügen**.

   Das Dialogfeld Hash hinzufügen wird angezeigt.
2. Ist der Hash vertrauenswürdig, wählen Sie **Vertrauenswürdig**.
3. Geben Sie den MD5-Hash und die Dateigröße in Bytes an.
4. Klicken Sie auf **Speichern**.

   Der Datei-Hash wird den Hashes hinzugefügt und für das Hash-Filtern in Malware Analysis verwendet.

Markieren eines Hashs als vertrauenswürdig oder nicht vertrauenswürdig

So markieren Sie einen Hash als vertrauenswürdig oder nicht vertrauenswürdig:

1. Klicken Sie in der Registerkarte **Hash** auf die Reihe **Vertrauenswürdig** für diesen Hash, um zwischen dem Status Vertrauenswürdig und Nicht Vertrauenswürdig umzuschalten.
2. Klicken Sie in der Symbolleiste auf **Bearbeitung speichern**.

Löschen eines Hashs aus dem Hash-Filter

So löschen Sie einen Hash aus dem Hash-Filter:

1. Wählen Sie in der Registerkarte **Hash** einen oder mehrere Hashs aus, die Sie von dem Hash-Filter entfernen möchten.
2. Klicken Sie in der Symbolleiste auf **Löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt und bietet die Möglichkeit zum Abbruch des Vorgangs.
3. Klicken Sie zum Bestätigen des Löschvorgangs auf **Ja**.

   Der Datei-Hash wird aus dem Raster gelöscht und nicht mehr für das Hash-Filtern in Malware Analysis verwendet.

Nach einem Datei-Hash suchen

Auf der Registerkarte „Hash“ können Sie nach einem Datei-Hash suchen, der im Raster angezeigt wird. Geben Sie im MD5-Feld den Datei-Hash ein, den Sie suchen, und klicken Sie auf **Suchen**. Eine Liste mit Dateien, die diesen Hash enthalten, wird im Raster angezeigt.

Importieren einer Hash-Liste mithilfe des überwachten Ordners

Um eine Hash-Liste aus dem beobachteten Verzeichnis zu importieren, muss die Hash-Liste in dem angegebenen Format sein und auf md5 sortiert werden. Sie können eine Datei mit dem unten beschriebenen Format in einen Ordner (/var/netwitness/malware-analytics-server/spectrum/hashWatch) der Malware Analysis-Appliance einfügen. Diese wird dann automatisch in die lokale Hash-Datenbank importiert. Dies ist die einzige Möglichkeit, Datei-Hashes in zu importieren. Ein weiteres Anwendungsbeispiel sieht vor, dass ein Systemadministrator das überwachte Verzeichnis einem Prozess aussetzt, der eine Datei in dieses Verzeichnis schiebt. Dieses Verfahren ist eine Art Massenimport für die Verwaltung einer großen Menge an Hash-Importen.

Dies ist eine Datei im CSV-Format ohne Leerzeichen zwischen den Daten in jeder Zeile. Es wird angenommen, dass es von den Daten in der Hash-Liste keine Duplikate gibt. Duplikate werden während der Verarbeitung ignoriert. Tauchen Duplikat-Hashes auf, zeigt die Protokolldatei folgende Meldung mit der Anzahl an Duplikat-Hashes in der Datei an:

2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing - /var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /var/lib/rsa>malware/hashWatch/test.csv

Unten stehend finden Sie ein Beispiel einer Hash-Liste im Standard-Dateiformat.

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

Eine NetWitness Suite-Konfigurationsdatei (**/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml**) bestimmt das Format und die Optionen des Importprozesses der Hash-Liste. Unten stehend finden Sie eine Liste der Konfigurationsdatei.

```
<config>
 <enabled>true</enabled>
 <distributedCacheEnabled>true</distributedCacheEnabled>

<watchDirectory>/
/var/lib/rsamalware/hashWatch</watchDirectory>

<processedDirectory>/
var/lib/rsamalware/hashWatch/processed</processedDirectory>
```

```
<erroredDirectory>/
var/lib/rsamalware/hashWatch/error</erroredDirectory>
 <md5Col>0</md5Col>
 <fileSizeCol>-1</fileSizeCol>
 <isTrustedCol>1</isTrustedCol>
 <isTrust>false</isTrust>
 <ignoreFirstLine>false</ignoreFirstLine>
 <frequencyInMinutes>1</frequencyInMinutes>
 <isGzipCompressed>false</isGzipCompressed>
 </config>
```

Liniendiagramm	Beschreibung
<md5Col>0</md5Col>	Die Position des MD5-Hashes in jedem Eintrag. Die Standardposition ist **0** oder die erste Position.
<fileSizeCol>1</fileSizeCol>	Die Position der Hash-Größe in jedem Eintrag. Die Standardposition ist **1** oder die zweite Position. Ist die Hash-Größe nicht in der CSV-Datei enthalten, muss der Wert **-1** betragen.
<isTrustedCol>2</isTrustedCol>	Die Position der Reihe Vertrauenswürdig in jedem Eintrag. Die Standardposition ist **2**. Ist der Parameter Vertrauenswürdig nicht in der CSV-Datei enthalten, muss der Wert **-1** betragen.
<isTrust>false</isTrust>	Die Standard-Annahme für den Parameter **Vertrauenswürdig** in jedem Eintrag ist **false**.
<ignoreFirstLine>false</ignoreFirstLine>	Vorhandensein eines Headers im Hash Der Standardwert ist **false**. Besitzt der Hash einen Header, muss der Wert auf **true** gesetzt werden.
<frequencyInMinutes>1</frequencyInMinutes>	Intervall zwischen den Überprüfungen durch NetWitness Suite im überwachten Verzeichnis Der Standardwert beträgt **1** Minute.
<isGzipCompressed>false</isGzipCompressed>	Der Hash wird mit Gzip komprimiert. Der Standardwert ist **false**. Wenn der Hash mit Gzip komprimiert wird, muss der Wert auf **true** gesetzt werden.

Wurde die Hash-Liste importiert, enthält das Systemprotokoll Einträge wie diesen:

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processed -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

Taucht beim Laden der Datei ein Problem auf, enthält das Systemprotokoll Einträge wie diesen:

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 ... Verbose log
 2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Error Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

So importieren Sie mithilfe der Methode des beobachteten Ordners eine Hash-Liste:

1. Kopieren Sie die Hash-Listen, die Sie importieren möchten, in das Verzeichnis **/var/netwitness/malware-analytics-sever/spectrum/hashWatch**.
   Malware Analysis beobachtet diesen Ordner automatisch und verarbeitet die hier gespeicherten Dateien.
   Malware Analysis fügt diesem Hash-Filter jeden in der Hash-Liste gefundenen Hash hinzu.
   Wenn Verarbeitungsfehler auftreten, werden diese im Verzeichnis **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error** protokolliert. Die verarbeiteten Dateien werden im Verzeichnis **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed** katalogisiert. Die verarbeiteten Dateien werden nicht aus dem Verzeichnis „hashWatch“ entfernt.
2. Nachdem die Masse der Hashes importiert wurde, kann der Systemadministrator mithilfe eines Cron-Jobs alte verarbeitete Dateien bereinigen.

(Optional) Konfigurieren der Malware Analysis-Proxyeinstellungen

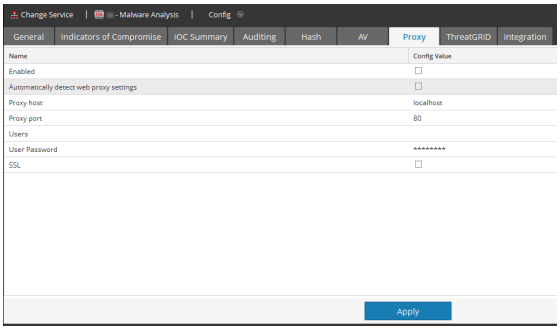
In diesem Thema wird die Konfiguration eines Webproxys für die Kommunikation mit dem RSA-Cloud-Service und dem lokalen ThreatGrid- oder GFI-Service beschrieben. Mit den Einstellungen in der Ansicht „Service-Konfiguration“ in der Registerkarte „Proxy“ wird die Kommunikation durch den Webproxy eingerichtet, den Malware Analysis für die Kommunikation mit der RSA-Cloud zur Community- und Sandbox-Analyse verwenden kann. Nach Konfiguration des Proxys:

- Malware Analysis kommuniziert durch den Webproxy mit der RSA-Cloud für die Communityanalyse.
- Malware Analysis kommuniziert durch den Webproxy mit dem konfigurierten ThreatGrid- oder GFI-Sandbox-Service. Die Verwendung eines Webproxys kann sich negativ auf die Performance auswirken. Die Abschnitte ThreatGrid- und GFI-Konfiguration in der Registerkarte Allgemein bieten eine Option zum Ausblenden des Webproxys und zur direkten Kommunikation mit der Sandbox. So kann die Performance verbessert werden.

Konfigurieren des Webproxys

So konfigurieren Sie den Webproxy für Malware Analysis:

1. Navigieren Sie zur Ansicht **ADMIN > Services**.
2. Wählen Sie einen Malware Analysis-Service und  **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Services konfigurieren** die Registerkarte **Proxy** aus.



4. Um den Proxy zu aktivieren, setzten Sie einen Haken im Kontrollkästchen **Aktivieren**.
5. (Optional) Aktivieren Sie das Kontrollkästchen, um automatisch Proxyeinstellungen für den NetWitness-Server zu finden.

   Die Felder „Proxyhost“ und „Proxyport“ werden automatisch gefüllt.
6. Möchten Sie einen anderen Proxy verwenden, geben Sie den **Proxyhost** und **Proxyport** ein.

7. Geben Sie den Benutzernamen und das Passwort ein, dass Sie zur Anmeldung im Proxyhost verwendet haben.
8. (Optional) Wählen Sie **SSL**, wenn der Proxyhost über SSL kommuniziert.
9. Klicken Sie auf **Anwenden**.

   Die Einstellungen wurden gespeichert und umgehend übernommen.

Hinweis: Malware Analysis unterstützt keine NTML-Webproxy-Authentifizierung.

(Optional) Registrieren für einen ThreatGrid-API-Schlüssel

In diesem Thema wird das Verfahren zum Abrufen eines Schlüssels für eine ThreatGrid-API-Testversion beschrieben, der in der ThreatGrid-Cloud-Sandbox verwendet werden soll. Bevor ThreatGrid als Sandbox-Service im Sandbox-Modul aktiviert werden kann, muss ein von ThreatGrid bereitgestellter Serviceschlüssel so konfiguriert werden, dass ThreatGrid erkennen kann, dass Muster, die von dieser Site übermittelt werden, legitim sind.

Wenn Sie keinen von ThreatGrid bereitgestellten Serviceschlüssel haben, können Sie mithilfe dieser Registerkarte einen Schlüssel erhalten. Der Schlüssel wird versuchsweise bereitgestellt.

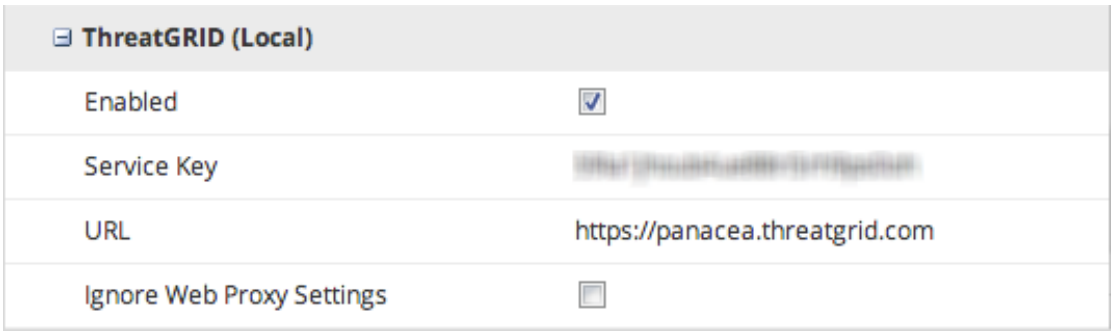
Wenn Sie Ihre Benutzerinformationen eingeben und auf **Registrieren** klicken, wird ein Schlüssel auf dieser Registerkarte angezeigt und automatisch zur ThreatGrid-Konfiguration in der Registerkarte **Allgemein** hinzugefügt. Nach einigen Minuten erhalten Sie eine E-Mail-Nachricht vom ThreatGrid mit einem Link zu ihrer Seite, auf der Sie sich anmelden können. Nachdem Sie die Lizenzbedingungen auf der ThreatGrid-Seite akzeptiert haben, können Sie die Dateien zur Analyse übermitteln. ThreatGrid erkennt Dateien, die von Malware Analysis für die Sandbox-Analyse übertragen werden.

So rufen Sie einen Schlüssel für eine ThreatGrid-API-Testversion ab:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Services**.
2. Wählen Sie einen Malware Analysis-Service und dann  **> Ansicht > Konfiguration** aus.
3. Wählen Sie in der Ansicht **Service-Konfiguration** die Registerkarte **ThreatGrid** aus.
4. Geben Sie Ihren vollständigen Namen, Ihren Beruf, den Namen des Unternehmens und Ihre E-Mail-Adresse ein.
5. Erstellen Sie im Feld Benutzer-ID und Passwort eine Benutzer-ID und ein Passwort, mit denen Sie sich bei ThreatGrid anmelden.
6. Klicken Sie auf **Register**.

Ihre Registrierung wird an ThreatGrid gesendet und unter der Schaltfläche Registrieren wird ein Schlüssel eingeblendet. Der Schlüssel wird automatisch in der Registerkarte **Allgemein** ausgefüllt.

7. Wählen Sie die Registerkarte **Allgemein**, um zu überprüfen, ob die ThreatGRID-Konfiguration nun den API-Schlüssel enthält.



8. Wenn Sie eine E-Mail-Nachricht von ThreatGrid mit einem Link zur Anmeldung erhalten, melden Sie sich an und akzeptieren Sie die Bedingungen der Lizenzvereinbarung.

   Ihre Testversion von ThreatGrid wird wirksam. Malware Analysis kann fünf Dateien pro Tag für die Sandbox-Analyse an die ThreatGrid-Cloud senden.

Zusätzliche Verfahren zur Konfiguration von Malware Analysis

In diesem Thema werden Verfahren behandelt, mit denen ein Administrator ein Ziel erreichen kann, das nicht zur grundlegenden Einrichtung von Malware Analysis gehört. Nach der Konfiguration von Malware Analysis können Administratoren den Service noch feiner anpassen und erweiterte Anpassungen implementieren. Ein Beispiel wäre die Implementierung von benutzerdefiniertem YARA-Inhalt.

Erstellen angepasster Warnmeldungen im CEF-Format

Dieses Thema enthält Anweisungen zur Erstellung von Warnmeldungen im CEF (Common Event Format)-Format, um sie an einen Service zu senden, der Ereignisse als CEF aufnimmt. Dies ist eine fortgeschrittene Konfigurationsaufgabe, die ausreichende Kenntnisse zur manuellen Bearbeitung der Konfigurationsdatei erfordert: `/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`. Bevor Sie die Datei bearbeiten, müssen Sie den Malware Analysis-Service im Betriebssystem beenden. Die CEF-Warnmeldung wird aktiv, wenn Sie den Malware Analysis-Service neu starten.

Die CEF-Vorlage

Um Ereignisse an einen Service zu senden, der sie als CEF aufnimmt, lässt NetWitness Suite eine Konfigurationsdatei, die als CEF-Vorlage dient, über die Ereignisse laufen, bevor sie an eine Korrelationstechnologie übergeben werden. Sie können an der Konfigurationsdatei, die die Reihenfolge und Zuordnung von Syslog-Feldern in jeder Warnmeldung angegeben, Einstellungen vornehmen.

Das folgende Beispiel einer Syslog-Meldung zeigt die CEF-Felder im Erweiterungsabschnitt der Warnmeldung an (nach dem letzten '|' in der Warnmeldung). Jedes Feld kann so konfiguriert werden, dass die Reihenfolge angezeigt wird (beschrieben im Beispielabschnitt unten). Felder können über eine Konfigurationseinstellung vollständig aus der Warnmeldung ausgeschlossen werden.

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0
nextgen=25.0 community=100.0 sandbox=25.0 file.name=myFile.exe
file.size=1234556 file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563
event.type=MANUAL_UPLOAD event.id=0 country.dst.code=--
country.dst=Unavailable ip.src=0:0:0:0:0:0:0:1
ip.dst=0:0:0:0:0:0:0:1 event.uuid=f7a6155a-31de-4fa6-ba16-
41fb9a8e5f26 ...
```

Verstehen eines Syslog-Auditing-Dateieintrags

Die Beschreibung der Dateistruktur basiert auf dem folgenden Beispiel.

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125

CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected
suspicious
 network event ID 857 session ID 73|2|

static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307

com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2
referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/
risk.info=http client server version mismatch
```

Erste Zeile

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

Protokollinformationen	Beschreibung
Feb 6 10:02:28	Der Zeitstempel für den Eintrag.
10.10.10.125	Die Quell-IP-Adresse des Ereignisses.

Protokollinformationen	Beschreibung
SpectrumServer125	Der Quellhostname des Ereignisses.

Audit Common Event Format (CEF) Header

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
network event ID 857 session ID 73|2|
```

Der Audit-CEF-Header ist eine durch Pipe-Zeichen getrennte Liste der folgenden Felder:

Protokollinformationen	Beschreibung
0	Die Version für das ArcSight CEF-Format wird für Audit-Syslog verwendet.
NetWitness	Der Service, der die Syslog-Nachricht erstellt hat.
Spectrum	Malware Analysis ist das Protokollmodul für das Ereignis.
1.2.1.130	Version von Malware Analysis
Ereignis-ID 857	Eindeutige Netzwerkereignis-ID für dieses Ereignis
Sitzungs-ID 73	Eindeutige Sitzungs-ID von Core für die Sitzung, die dieses Ereignis enthielt.
2	Schweregrad – eine Zahl zwischen 1 und 6, die den Schweregrad der Meldung angibt. • 1 = INFORMATION_LEVEL • 2 = WARNING_LEVEL • 3 = ERROR_LEVEL • 4 = SUCCESS_LEVEL • 5 = FAILURE_LEVEL • 6 = AUDIT_FAILURE_LEVEL

Audit-CEF-Erweiterung

```
static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc  file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
```

```
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-
fc12-149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server
version mismatch
```

Analysewerte

Der erste Eintrag in der Audit-CEF-Erweiterung liefert die vier Malware Analysis-Werte für das Ereignis: Statisch, Netzwerk, Community und Sandbox.

Protokollinformationen	Beispielwert
static	100.0
Netzwerk	29.0
community	8,0 Ein Wert von 0,0 kann ein Communitywert für das Ereignis sein oder bedeuten, dass kein Communityservice aktiviert wurde.
Sandbox	N/R N/R bedeutet, dass keine Ausführung stattgefunden hat (Not Run). Dies weist darauf hin, dass die GFI-Sandbox nicht aktiviert wurde.

Dateiinformationen

Die nächsten drei Einträge stellen Dateiinformationen bereit: Dateiname, Größe und Hash.

Protokollinformationen	Beispielwert
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0

Protokollinformationen	Beispielwert
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

Von NextGen abgerufene Ereignismetadaten

Die Aufzeichnung wird mit Core-Metadaten für dieses Ereignis fortgesetzt. Die Metadaten in der Meldung hängen vom Ereignis ab. Die Datenmenge in der Meldung ist gemäß den Syslog-Einstellungen auf die maximal zulässige Länge (in Byte) begrenzt. Der Standardwert ist 1024.

Protokollinformationen	Beispielwert
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149
Client	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Private
time	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
Aktion	get
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	RTF
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6

Protokollinformationen	Beispielwert
tcp.flags	27
ip.src	10.25.50.61
tcp.dstport	80
threat.category	SPectrum
eth.dst	00:0C:29:F8:50:2D
Dauer	0
alert.id	nw32535
sessionid	73
medium	1
Größe	117864
Inhalt	spectrum.consume11
extension	doc
directory	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
service	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
server	Apache/2.2.13 (Fedora)
Streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	http client server version mismatch

Bearbeiten Sie die Konfigurationsdatei.

1. Beenden Sie den Malware Analysis-Service.
2. Bearbeiten Sie die Konfigurationsdatei, wie im Beispiel beschrieben.
3. Starten Sie den Malware Analysis-Service.
   Der Malware Analysis-Service beginnt damit, Warnmeldungen mithilfe der Konfigurationsdatei zu verarbeiten und CEF-Warnmeldungen an designierte Services zu senden.

Beispiel

Die Konfigurationsdatei kann verwendet werden, um vorzugeben, welche Felder in der resultierenden Warnmeldung angezeigt werden, welche Bezeichnung jedes Feld erhalten soll, und in welcher Reihenfolge die Datenfelder angezeigt werden. Die Konfigurationsdatei besteht aus einem oder mehreren `MalwareCefExtension`-XML-Blöcken, wie im Beispiel unten gezeigt. Die Reihenfolge dieser Blöcke in der Konfigurationsdatei impliziert die Reihenfolge der Datenfelder in der CEF-Warnmeldung.

Um Beispiel unten würde die CEF-Warnmeldung zwei Datenfelder beinhalten, `ip.src` gefolgt von `ip.dst`. Mit `customKey` wird die Bezeichnung des Datenfelds in der Warnmeldung angezeigt. Dies erlaubt es dem Benutzer, eine angepasste Bezeichnung zu wählen, damit das Format der Warnmeldung besser mit den Erwartungen der Empfänger der Warnmeldung übereinstimmt. Mit anderen Worten, das Format kann so eingestellt werden, dass unerwünschte Änderungen an einem bestehenden Warnmeldungsparser verhindert werden. Schließlich legt die Einstellung `isDisplay` fest, ob das Feld in der Warnmeldungsausgabe enthalten sein wird. So kann der Benutzer Datenfelder abschalten, ohne den Block `MalwareCefExtension` physisch von der Konfiguration löschen zu müssen.

```
 <config>
 <malwareExtensionList>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.src</customKey>
   <malwareKey>ip.src</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.dst</customKey>
   <malwareKey>ip.dst</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
 </malwareExtensionList>
```

```
</config>
```

Am Ende der Konfigurationsdatei sind drei zusätzliche Einstellungen, mit denen das Format der Warnmeldung noch feiner eingestellt werden kann. Sie lauten wie folgt:

Einstellung	Beschreibung
`includesUnknownMeta`	Diese Einstellung, die die Werte „wahr“ oder „falsch“ annehmen kann, zeigt an, ob unbekannte Datenelemente in der resultierenden Warnmeldung enthalten sein können. Alle beliebigen NextGen-Sitzungsdaten können in einer CEF-Warnmeldung enthalten sein. Da zusätzliche Sitzungsmetadaten über die Erstellung neuer NextGen-Parser eingeführt werden können, können auch Metadaten gefunden werden, die in der Standardkonfiguration nicht enthalten sind. Sie können `includesUnknownMeta` auf „wahr“ einstellen, um die unbekannten Metadaten in der Warnmeldung einzuschließen, und sie mithilfe des NextGen-Metaschlüsselnamens bezeichnen. Um einen angepassten Schlüssel für die nicht bekannten Metadaten zu erzwingen, müssen Sie diese Datei bearbeiten und eine neue `MalwareCefExtension` zum Wörterbuch hinzufügen. Wenn Sie unbekannte Metadaten aus der Warnmeldung auslassen möchten, stellen Sie `includesUnknownMeta` auf „falsch“ ein.
`displayNulls`	Diese Einstellung, die die Werte „wahr“ oder „falsch“ annehmen kann, zeigt an, ob auf Null gesetzte Werte in der Warnmeldung enthalten sein können. Wenn `displayNulls` auf „falsch“ eingestellt ist, werden die Felder mit dem Wert Null ausgelassen, auch wenn ihre Eigenschaft `MalwareCefExtension isDisplay` aktiviert ist. Dies erlaubt dynamisches Formatieren von Warnmeldungen, um Nullfelder auszuschließen.

Einstellung	Beschreibung
`valueIfNull`	Diese Einstellung, die die Werte „wahr“ oder „falsch“ annehmen kann, erlaubt Ihnen, einen Platzhalter für die Zeichenfolge anzugeben (standardmäßig `n/a`), der als Wert für alle Felder mit dem Wert Null verwendet wird. Wenn `displayNulls` auf „wahr“ eingestellt ist, werden Felder mit Nullwerten in den Warnmeldungen eingeschlossen. Ihr Wert wird auf den in `valueIfNull` angegebenen Wert festgelegt.

Folgendes repräsentiert die Standard-CEF-Konfigurationsdatei. Die Standard Konfigurationsdatei enthält alle Standard-NextGen-Sitzungsmetadaten.

```
<config>
  <malwareExtensionList>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>static</customKey>
   <malwareKey>static</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>nextgen</customKey>
   <malwareKey>nextgen</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>community</customKey>
   <malwareKey>community</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>sandbox</customKey>
   <malwareKey>sandbox</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>file.name</customKey>
<malwareKey>file.name</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.size</customKey>
<malwareKey>file.size</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>
<malwareKey>country.dst.code</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcpport</customKey>
<malwareKey>tcp.srcpport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
<malwareKey>agency.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
```

```
<malwareKey>threat.category</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>lifetime</customKey>
<malwareKey>lifetime</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
<malwareKey>latdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>size</customKey>
<malwareKey>size</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>
<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
```

```
<isDisplay>false</isDisplay>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filename</customKey>
<malwareKey>filename</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
<malwareKey>streams</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referer</customKey>
<malwareKey>referer</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>
<malwareKey>risk.warning</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>attachment</customKey>
<malwareKey>attachment</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrar</customKey>
<malwareKey>whois.registrar</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrant</customKey>
<malwareKey>whois.registrant</malwareKey>
<isDisplay>false</isDisplay>
```

```
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.date.creation</customKey>
    <malwareKey>whois.date.creation</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.server</customKey>
    <malwareKey>whois.server</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
  </malwareExtensionList>
  <includesUnknownMeta>false</includesUnknownMeta>
  <displayNulls>false</displayNulls>
  <valueIfNull>n/a</valueIfNull>
</config>
```

Aktivieren von angepassten YARA-Inhalten

In diesem Thema erhalten Sie Anweisungen zum Aktivieren von angepassten YARA-Inhalten auf dem NetWitness Suite-Host, auf dem der Malware Analysis-Service installiert ist. Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis auch in YARA geschriebene Indikatoren für eine Infizierung. YARA ist eine Regelsprache, die es Schadsoftware-Forschern erlaubt, Muster von Schadsoftware zu identifizieren und zu klassifizieren. RSA stellt integrierte YARA-basierte IOCs (Indicators of Compromise) in RSA Live zur Verfügung; diese werden automatisch heruntergeladen und auf abonnierten Appliances aktiviert.

Kunden mit fortgeschrittenen Fähigkeiten und Kenntnissen können die Erkennungsfunktionen von RSA Malware Analysis erweitern, indem sie YARA-Regeln erstellen und sie in RSA Live veröffentlichen, oder YARA-Regeln in einen beobachteten Ordner stellen, zur Verarbeitung durch die Appliance. Dieser Abschnitt enthält Anweisungen für den Administrator, der Appliances konfiguriert, um die Erstellung von angepassten YARA-Inhalten zu aktivieren.

Voraussetzungen

Hierbei handelt es sich um eine erweiterte Konfigurationsaufgabe, die ausreichende Berechtigungen und Kenntnisse erfordert, um zur Erstellung von YARA eine GNU Compiler Collection (GCC) und C++ Python-Entwicklungsbibliothek einzurichten. Außerdem müssen Sie mit der Standard-YARA-Dokumentaktion sehr vertraut sein. Die folgenden Komponenten sind erforderlich:

- die Perl-Compatible Regular Expression (PCRE)-Bibliothek: pcre-8.33.tar.bz2
- die Yara 1.7 (Rev:167) eigenständige YARA-Befehlszeile: yara-1.7.tar
- die YARA-Erweiterung für Python: yara-python-1.7.tar.gz
- YARA-Regeldokumentation: YARA-Benutzerhandbuch 1.6.pdf

Die Komponenten stehen hier zum Download zur Verfügung: https://code.google.com/p/yara-project/downloads/list

Hinweis: Zum Zeitpunkt der Erstellung dieses Dokuments war YARA 2.0 bereits verfügbar, wurde aber noch nicht von Malware Analysis 10.5 unterstützt.

Installieren von Bibliotheken und Anwendungen, die zum Erstellen von YARA auf einer CentOs-basierten Appliance erforderlich sind

Als Voraussetzung zum Erstellen von YARA auf einem Host, auf dem CentOS ausgeführt wird, müssen Sie `make`, die GNU Compiler Collection und die C++ `Python`-Entwicklungsbibliothek auf der Appliance installieren. So installieren Sie die Anwendungen und Bibliotheken, die zum Erstellen von YARA erforderlich sind:

1. Um sicherzustellen, dass der Ordner „/etc/yum.repos.d“ nur die Standard-YUM-Repo-Dateien und keine anderen Repo-Dateien enthält, geben Sie den folgenden Befehl ein:

   `ls -al /etc/yum.repos.d`

   Die Ergebnisse sollten ähnlich wie folgende aussehen:

   ```
   -rw-r-r-. 1 root root 1926 Jun 26  2012 CentOS-Base.repo
   -rw-r-r-. 1 root root  637 Jun 26  2012 CentOS-Debuginfo.repo
   -rw-r-r-. 1 root root  626 Jun 26  2012 CentOS-Media.repo
   -rw-r-r-. 1 root root 2593 Jun 26  2012 CentOS-Vault.repo
   ```

2. Geben Sie zum Installieren von `make` auf der Appliance die folgenden Befehle ein:

   a. **`yum search make`**

      Die folgende Meldung wird zurückgegeben: `make.x86_64 : A GNU tool which simplifies the build process for user`

   b. **`yum install make.x86_64`**

3. Geben Sie zum Installieren und Testen von GCC auf der Appliance die folgenden Befehle ein:

   a. **yum search gcc**
      Daraufhin werden die folgenden Meldungen angezeigt:
      ```
      gcc-c+.x86_64 : C+ support for GCC
       gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)
      ```

   b. Geben Sie die folgenden Befehle ein:
      ```
      yum install gcc.x86_64
       yum install gcc-c++.x86_64
      ```

   c. Zum Testen der GCC-Befehle geben Sie die folgenden Befehle ein:
      ```
      gcc -v
       cc -v
      ```

4. Zum Installieren der C++ Python-Entwicklungsbibliothek auf der Appliance geben Sie die folgenden Befehle ein:

   a. **yum search python dev**
      Die folgende Meldung wird zurückgegeben:
      ```
      python-devel.x86_64 : The libraries and header files needed for
      Python development
      ```

   b. **yum install python-devel.x86_64**

Einrichten von Yara

So erstellen Sie eine GCC- und C++ Python-Entwicklungsbibliothek auf dem NetWitness Suite-Host, auf dem Malware Analysis ausgeführt wird, um dort YARA zu erstellen:

1. Führen Sie einen der folgenden Schritte aus:

   a. Wenn auf dem Host, auf dem Sie die Installation durchführen, Mac OS ausgeführt wird, installieren Sie xCode für Mac OS.

   b. Wenn auf dem Host, auf dem Sie die Installation durchführen, CentOS ausgeführt wird, installieren Sie make, GCC- und C++ Python-Entwicklungsbibliothek mithilfe der YUM-Befehlszeile.

2. Öffnen Sie zum Installieren der PCRE-Bibliothek auf dem Host ein Terminalfenster und geben Sie die folgenden Befehle ein:
   ```
   tar -xvf pcre-8.33.tar.bz2
    cd pcre-8.33
    ./configure
   ```

```
make
sudo make install
```

3. Zum Installieren der eigenständigen YARA-Befehlszeile geben Sie die folgenden Befehle ein:

```
tar -xvf yara-1.7.tar
cd yara-1.7
./configure
make
sudo make install
```

4. So testen Sie die eigenständige YARA-Befehlszeile:
   a. Geben Sie den folgenden Befehl ein:

```
yara
```

   b. Wenn der Befehl erfolgreich ausgeführt wird, fahren Sie fort mit Schritt 7. Wenn der Befehl fehlschlägt und den Fehler `yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory` zurückgibt, geben Sie den folgenden Befehl ein, um die Datei `/etc/ld.so.conf` oder die Umgebungsvariable `LD_LIBRARY_PATH` zu prüfen.

```
ldconfig -v
```

5. Zum Installieren der YARA-Erweiterung für Python geben Sie die folgenden Befehle ein:

```
tar -xvf yara-python-1.7.tar.gz
cd yara-python-1.7
python setup.py build
sudo python setup.py install
```

6. So testen Sie die YARA-Erweiterung:
   a. Geben Sie den folgenden Befehl ein: **`python`**
   b. Geben Sie an der Python-Eingabeaufforderung (>>>) die folgenden Befehle ein:

```
import yara
exit()
```

Nach dem Abschluss dieser Konfiguration können Analysten angepasste YARA-IOCs zur Verarbeitung auf einem Malware Analysis-Host erstellen, wie unter „Implementieren von angepassten YARA-Inhalten“ im *Leitfaden zu Investigation und Malware Analysis* beschrieben.

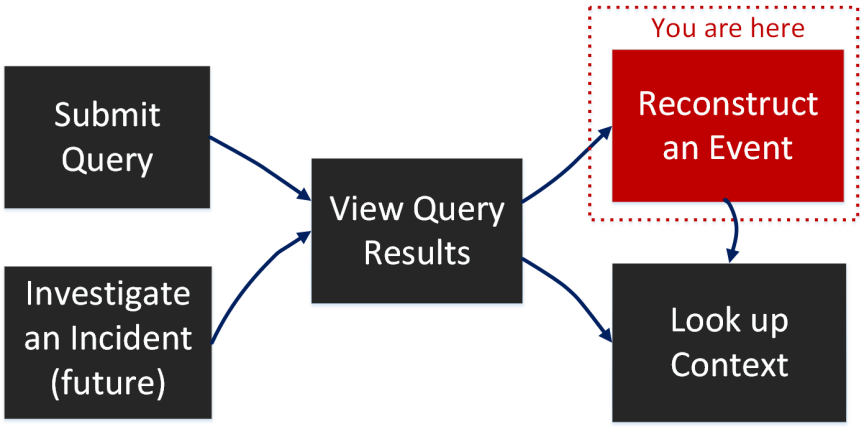
Ressourcen für Malware Analysis

- Ansicht „Services > Konfiguration“ – Registerkarte „Auditing“
- Ansicht „Service-Konfiguration“ – Registerkarte „AV“
- Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“
- Ansicht „Service-Konfiguration“ – Registerkarte „Hash“
- Ansicht „Service-Konfiguration“ – Registerkarte „Indikatoren für eine Infizierung“
- Ansicht „Service-Konfiguration“ – Registerkarte „Integration“
- Ansicht „Service-Konfiguration“ – Registerkarte „IOC-Zusammenfassung“
- Ansicht „Service-Konfiguration“ – Registerkarte „Proxy“
- Ansicht „Service-Konfiguration“ – Registerkarte „ThreatGRID“

Ansicht „Services > Konfiguration“ – Registerkarte „Auditing“

Im Bereich Ansicht „Ereignisse“ und Neue Ansicht „Ereignisse“ – Ereignisrekonstruktion (**Untersuchen > Bereich „Ereignisse“ > Klicken auf ein Ereignis)** können Sie auf sichere Weise eine Rekonstruktion eines Ereignisses aus der Ansicht „Navigieren“ oder dem Bereich „Ereignisse“ anzeigen, über das Sie mehr erfahren möchten.

Workflow



Was möchten Sie tun?

Benutzerrolle	Aufgabe	Dokumentation
Threat Hunter	Abfrage senden	Durchführen einer Ermittlung
Threat Hunter	Abfrageergebnisse anzeigen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Ereignis rekonstruieren*	Rekonstruieren eines Ereignisses
Threat Hunter	Dateien aus einem Ereignis exportieren	Rekonstruieren eines Ereignisses
Threat Hunter	Zusätzlichen Kontext für ein Ereignis suchen	Nachschlagen kontextbezogener Informationen

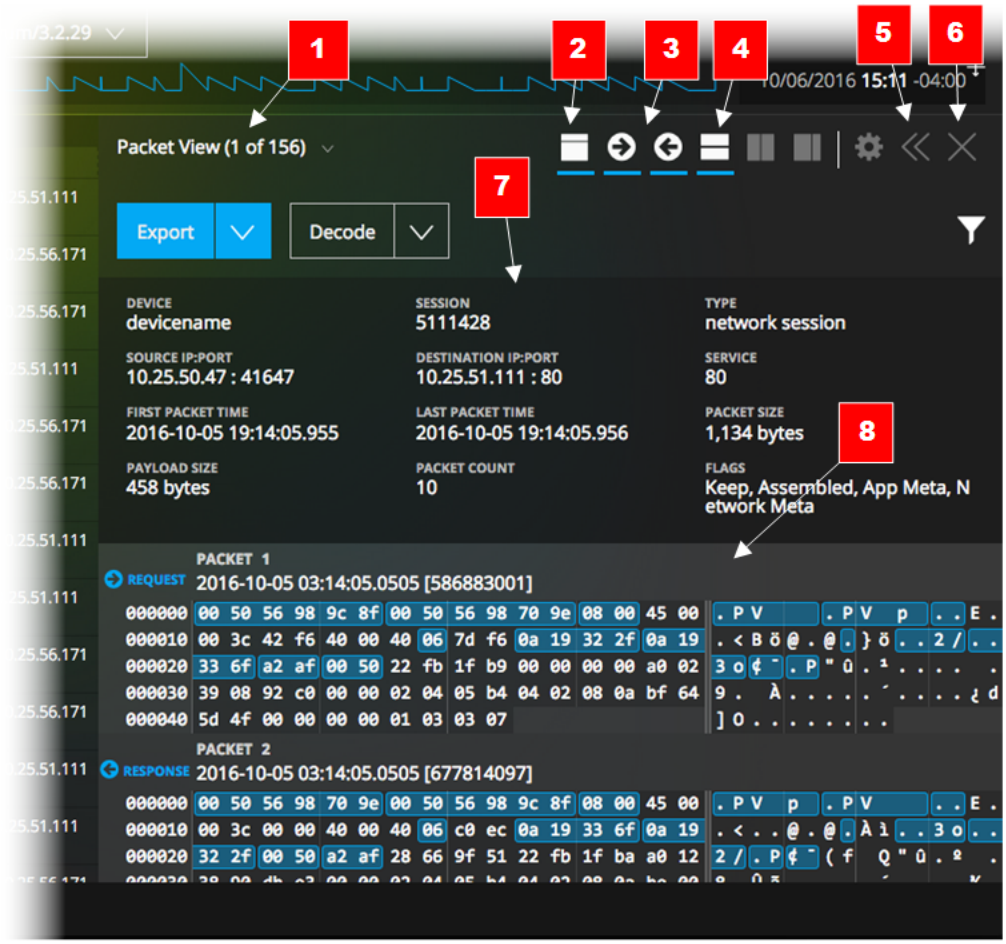
Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Durchführen einer Ermittlung
- Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
- Ansicht „Navigieren“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“

Überblick

Der Bereich „Untersuchen > Rekonstruktion“ zeigt eine Rekonstruktion eines einzelnen Ereignisses in der Paketansicht, Dateiansicht und Textansicht an. Wenn Sie im Bereich „Ereignisse“ auf ein Ereignis klicken, wird im angrenzenden Bereich „Rekonstruktion“ die Paketrekonstruktion des Ereignisses angezeigt. Sie können mit den Optionen in der Symbolleiste „Ereignisrekonstruktion“ den Typ und die Richtung der Rekonstruktion (Anforderung oder Antwort) ändern, die Bereichsüberschrift verbergen oder anzeigen und den Bereich „Ereignisrekonstruktion“ einblenden, verkleinern und schließen. Je nach ausgewähltem Rekonstruktionstyp und dem Inhalt der Nutzlast stehen zusätzliche Optionen zur Verfügung. Sie können z. B. die Nutzlast nur in der Textansicht anzeigen, Dateien in der Dateiansicht herunterladen und PCAP-Dateien in der Paketansicht herunterladen.

Im Folgenden finden Sie ein Beispiel für eine Paketrekonstruktion.



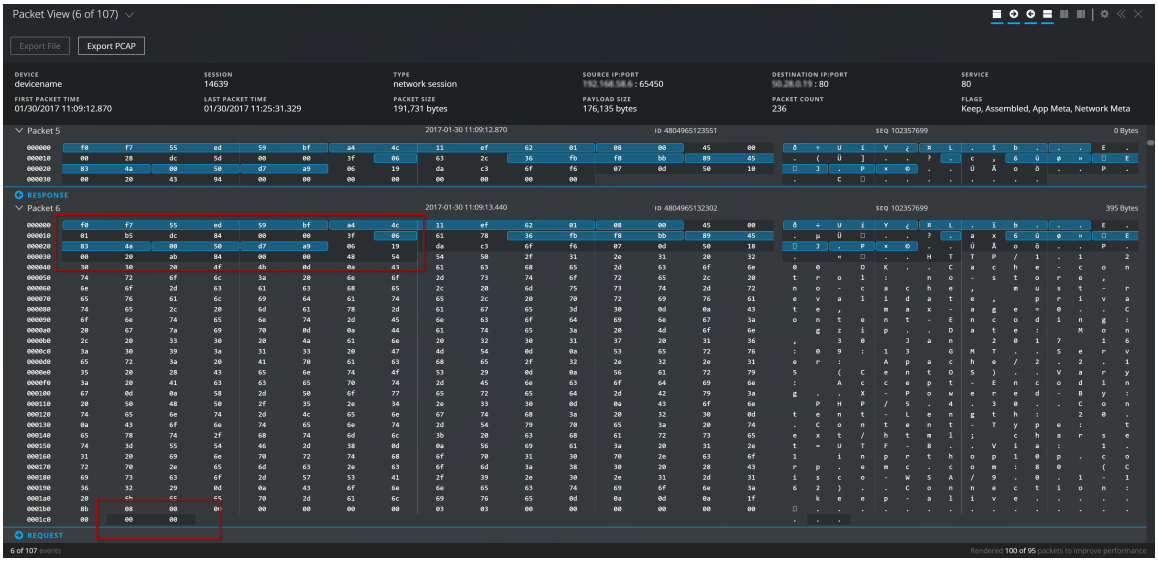
1	Registerkarten oder Drop-down-Menü, um den Rekonstruktionstyp auszuwählen: Paketansicht, Dateiansicht, Textansicht. Der aktuell ausgewählte Typ wird in der Bezeichnung angezeigt.
2	Klicken Sie, um die Bereichsüberschrift ein- oder auszublenden.
3	Klicken Sie auf diese Symbole, um die Anforderung, Antwort oder beides einzublenden.
4	Klicken Sie auf dieses Symbol, um den Bereich „Ereignis-Metadaten“ ein- oder auszublenden, der eine detaillierte Auflistung der dem Ereignis zugeordneten Metadaten enthält.
5	Eine Option zum horizontalen Erweitern oder Verkleinern des Bereichs „Rekonstruktion“ in der Ansicht „Navigieren“
6	Eine Option zum Schließen des Bereichs „Rekonstruktion“
7	In der Kopfzeile werden zusammenfassende Informationen für das zu rekonstruierende Ereignis angezeigt.

8 Listet jedes Paket im Ereignis auf. Für jedes Paket werden die Paketnummer, die Richtung (Anfrage oder Antwort) und der Paketinhalt links im Binärformat, in der Mitte im hexadezimalen Format und rechts im Textformat angezeigt.

Details der Paketrekonstruktion

In der Paketrekonstruktion werden unter „Untersuchen“ die Paketnummer, die Richtung des Pakets (Anforderung oder Antwort), die Startzeit des Pakets und der Inhalt des Pakets angezeigt.

Alle Pakete beginnen mit einer Kopfzeile und einige Pakete weisen eine Fußzeile auf. In der Paketansicht haben die Kopfzeile und Fußzeile einen dunkleren Hintergrund, damit sie von der Nutzlast des Pakets zu unterscheiden sind. Der dunklere Hintergrund für die Kopf- und Fußzeile wird im hexadezimalen und im Textformat angezeigt.



Der Inhalt des Pakets wird im hexadezimalen und im Textformat angezeigt. Die Metadaten sind in Blau hervorgehoben. Wenn Sie den Mauszeiger über die Metadaten bewegen, werden der Metaschlüssel und der Metawert als Kurzinfo angezeigt.

Zusätzliche Optionen in der Paketansicht beinhalten die Möglichkeit, die PCAP-Datei für das Ereignis herunterzuladen und nur Nutzlast anzuzeigen. Wenn nur Nutzlast angezeigt wird, können Sie mit der Option „Byte schattieren“ Muster in den Daten unterscheiden.

Details der Textrekonstruktion

In der Textrekonstruktion werden Netzwerkereignisse und Protokollereignisse unterschiedlich dargestellt. Für Netzwerkereignisse stellt „Untersuchen“ die Richtung des Pakets (Anforderung oder Antwort) und die Inhalte jedes Pakets im Textformat bereit.

Für Protokollereignisse (Filter „Medium = Protokoll“) gibt es keine Anforderung oder Antwort; in der Textrekonstruktion wird nur das Rohdatenprotokoll angezeigt.

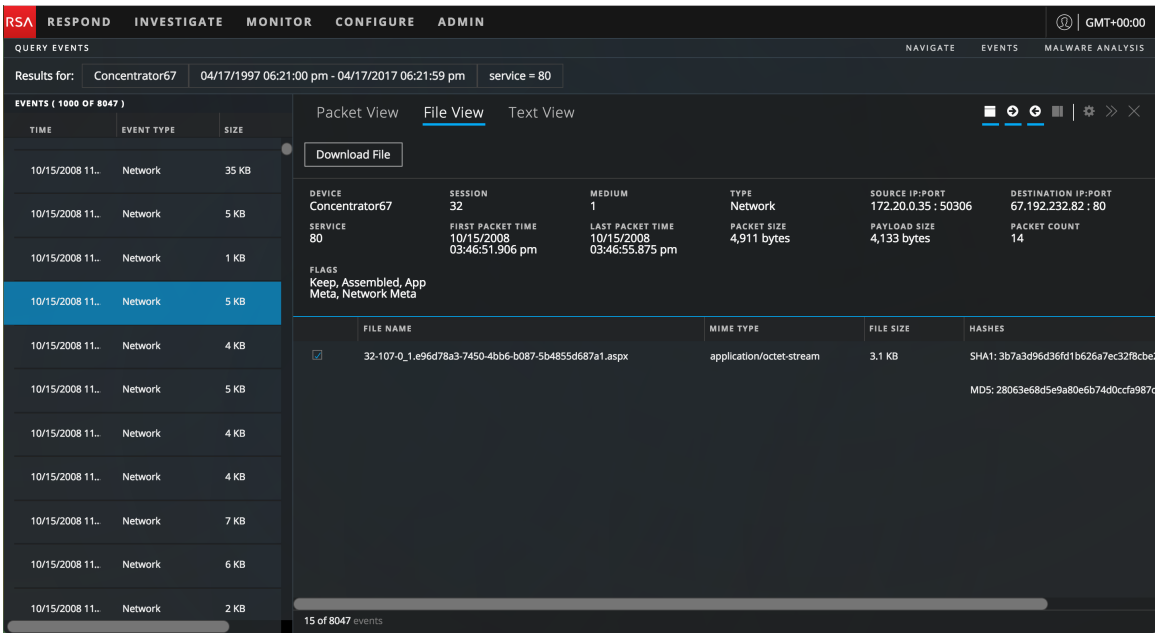
Eine Teilmenge der Rekonstruktionsoptionen ist in der Textansicht verfügbar. Sie können Folgendes tun:

- Die Kopfzeile aus- und einblenden.
- Für Netzwerkereignisse die Anzeige nur von Anforderungen oder nur von Antworten oder von beiden auswählen.
- Für Netzwerkereignisse die Sitzung als PCAP-Datei exportieren.
- Für Protokollereignisse das Rohdatenprotokoll exportieren.
- Zwischen einer komprimierten und dekomprimierten Ansicht der Nutzlast wechseln. Wenn die Sitzung dekomprimiert wird, werden die komprimierten Teile des Textes lesbar.
- Text für die Decodierung und Codierung auswählen.

Hinweis: Diese Funktion ist für die Dateiansicht, andere als http-Netzwerksitzungen und Protokolldaten nicht verfügbar.

Details der Dateirekonstruktion

In der Dateirekonstruktion zeigt Ermittlung eine Liste der Dateien an, die mit dem ausgewählten Netzwerkereignis verknüpft sind.



Sie können eine Datei, mehrere Dateien oder alle Dateien für den Export in Ihr lokales Dateisystem auswählen. Wenn Dateien ausgewählt sind, wird die Schaltfläche „Dateien exportieren“ aktiviert, auf der die Anzahl der ausgewählten Dateien angezeigt wird. Durch Klicken auf die Schaltfläche werden die ausgewählten Dateien als ZIP-Archiv exportiert. Damit wird sichergestellt, dass potenziell schädliche Dateien nicht von der Standardanwendung geöffnet und ausgeführt werden. Das exportierte Archiv wird nach der folgenden Konvention benannt:

`<service-ID or host name>_SID<nnnnnnnn>_FC<n>.zip`

Hierbei gilt:

- `<service-ID or host name>` ist der Name des Services (z. B. Concentrator oder Broker), in dem die Sitzung gespeichert wurde.
- `SID<nnnnnnnn>` ist die Sitzungs-ID-Nummer.
- `FC<nnnnnnnn>` ist die Dateianzahl oder die Anzahl der Dateien im Archiv.

NetWitness Suite exportiert das Archiv mit Passwortschutz, um zu verhindern, dass es beim Herunterladen automatisch entpackt wird. Geben Sie zum Öffnen eines Archivs das folgende Passwort ein: **netwitness**.

Achtung: Beim Entpacken und Öffnen von Dateien, die mit einer Standardanwendung verknüpft sind, ist Vorsicht geboten; beispielsweise könnte eine Excel-Tabelle automatisch in Excel geöffnet werden, bevor Sie überprüfen konnten, ob sie sicher ist.

Detaillierte Beschreibung

Funktion	Beschreibung
Menü „Rekonstruktionstyp“	In diesem Menü können Sie den Typ der Rekonstruktion auswählen: **Paket** oder **Datei**. Wenn Sie eine Rekonstruktion zum ersten Mal öffnen, wählt NetWitness Suite standardmäßig die beste Rekonstruktion aus.
Downloadoptionen	Optionen zum Exportieren eines Protokolls, einer PCAP-Datei oder von Dateien zur genaueren Analyse und zum Teilen mit anderen.

Funktion	Beschreibung
	Steuert die Anzeige einer Kopfzeile über der Paketliste; Sie können auf dieses Symbol klicken, um die Kopfzeile aus- oder einzublenden. Durch Ausblenden der Kopfzeile steht mehr Platz für die Paketliste zur Verfügung und der erforderliche Bildlauf zur Anzeige weiterer Pakete wird reduziert. Die Kopfzeile enthält Informationen über das rekonstruierte Ereignis: Name des Services, der das Paket erfasst hat, Sitzungs- oder Ereignisnummer, Typ des Ereignisses (Netzwerk), Quell-IP:Port, Ziel-IP:Port, Servicetyp, erste Paketzeit im Ereignis, letzte Paketzeit im Ereignis, Ereignisgröße, Größe der Nutzlast in Byte, Paketanzahl sowie die Flags des Ereignisses (beibehalten, zusammengestellt, App-Metadaten, Netzwerkmetadaten).
	Zwei Steuerelemente aktivieren und deaktivieren die Anzeige von Anforderung und Antwort (siehe Rekonstruieren eines Ereignisses).
	Zeigt die Metadetails für das Ereignis in einem anderen Bereich an.
	(Zukünftig) Menü „Einstellungen“.
	Dimensionierung der Steuerelemente für den Bereich „Rekonstruktion“ (siehe Rekonstruieren eines Ereignisses).
	Schließt den Bereich „Rekonstruktion“. In der Ansicht wird jetzt nur der Bereich „Ereignisse“ angezeigt.

Ansicht „Service-Konfiguration“ – Registerkarte „AV“

In diesem Thema werden Merkmale und Funktionen der Registerkarte „AV“ in der Ansicht „Service-Konfiguration“ für einen Malware Analysis-Service beschrieben. Auf der Registerkarte „AV“ werden die Anbieter der Virensoftware angezeigt, deren Software Sie in Ihrem Netzwerk verwenden. NetWitness Suite kann die Ergebnisse dieser Anbieter in die detaillierte Ergebnisansicht eines Ereignisses einbeziehen, das mithilfe von Malware Analysis analysiert wurde.

Dies ist ein Beispiel für die Registerkarte „AV“.

Funktionen

In der Registerkarte AV werden die Virenschutzanbieter aufgeführt, deren Software möglicherweise in Ihrem Netzwerk installiert ist. Für Anbieter stehen zwei Kategorien zur Verfügung: Primäre: die vertrauenswürdigsten Anbieter, und Sekundäre: die weniger bekannten Anbieter. Jeder Anbietername ist mit einem Kontrollkästchen und einem Symbol versehen. Wenn Sie ein Kontrollkästchen neben einem Anbieternamen aktivieren, bedeutet das, dass die Virenschutzsoftware dieses Anbieters in Ihrer Umgebung installiert ist.

In dieser Tabelle werden die Optionen in der Registerkarte „AV“ beschrieben.

Funktion	Beschreibung
Kontrollkästchen Anbieter	Wählen Sie einen oder mehrere Virenschutzanbieter aus der vorgegebenen Liste aus, um die in der lokalen Organisation installierten Produkte anzugeben.
Anwenden	Speichert die in der Registerkarte AV vorgenommenen Änderungen.
Zurücksetzen	Setzt die Liste AV auf den Standardstatus zurück, in dem kein Anbieter ausgewählt ist.

Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“

Dieses Thema bietet eine Einführung in die Konfigurationseinstellungen in der Ansicht „Service-Konfiguration“ > Registerkarte „Allgemein“ für Malware Analysis, die für den Malware Analysis-Service spezifische Parameter enthält. In dieser Registerkarte können Sie Folgendes konfigurieren:

- Verarbeitungsparameter für datenerfassende Core-Services.
- Das Repository, das für erfasste Daten verwendet wird.
- Die Bewertungsmodule Statisch, Community und Sandbox, die zur Datenanalyse verwendet werden.

Die folgende Aufgabe bietet ausführliche Verfahren: Konfigurieren der allgemeinen Malware Analysis-Einstellungen.

Dies ist ein Beispiel für die Registerkarte „Allgemein“.

Diese Registerkarte ist in vier Abschnitte aufgeteilt: „Konfiguration des kontinuierlichen Scannens“, „Repository-Konfiguration“, „Verschiedenes“ und „Modulkonfiguration“.

Abschnitt „Konfiguration des kontinuierlichen Scannens“

Diese Tabelle zeigt die Funktionen des Abschnitts „Konfiguration des kontinuierlichen Scannens“.

Parameter	Beschreibung
Aktiviert	Vollständiges Aktivieren oder Deaktivieren der kontinuierlichen Abfrage des Core-Services. Standardmäßig ist dies **deaktiviert**.

Parameter	Beschreibung
Abfrage	Während der Decoder den Netzwerkdatenverkehr analysiert, wird ein Metafeld mit der Bezeichnung „content“ und dem Wert **spectrum.consume** in Sitzungen erstellt, die wahrscheinlich Schadsoftware enthalten. Standardmäßig führt Malware Analysis nur Analysen von Ereignissen durch, die diesen Metawert aufweisen. Durch Änderung der Abfrage kann Malware Analysis so konfiguriert werden, dass verschiedene Arten von Ereignissen analysiert werden. Wird der Geltungsbereich der Abfrage zu umfassend gewählt, könnte Malware Analysis zu viele Ereignisse analysieren, was zu Verzögerungen oder schlechten Ergebnissen führen kann. Die Standardabfrage entspricht **select * where content='spectrum.consume'**
Ablaufzeit der Abfrage	Wenn Malware Analysis den Core-Service nach Metadaten abfragt, werden die Ergebnisse innerhalb weniger Sekunden ermittelt. Taucht ein Problem auf, z. B. mit der Netzwerkverbindung, beendet Malware Analysis die Abfrage nach dieser konfigurierten Zeitspanne. Der Standardwert entspricht **3.600 Sekunden**.
Abfrageintervall	Zeitintervall (in Minuten), in dem Metadaten und Dateien neuer Sitzungen abgefragt werden.
Metadatenbegrenzung	Jedes Mal, wenn Malware Analysis den Core-Service abfragt, werden Metadaten bis zu dieser Metadatenbegrenzung abgerufen. Diese Einstellung kann in Verbindung mit dem Abfrageintervall die Performance von Malware Analysis in der Core-Infrastruktur verbessern. Der Standardwert ist **25.000**.

Parameter	Beschreibung
Zeitgrenze	Malware Analysis analysiert Sitzungen, die nach dieser Zeitgrenze stattgefunden haben. Diese Einstellung ist bei der Installation einer neuen Malware Analysis-Appliance enorm wichtig, da diese bestimmt, wie weit die zu analysierenden Sitzungen in der Vergangenheit liegen dürfen. Liegt die Grenze zu viele Stunden in der Vergangenheit, könnte dies dazu führen, dass Malware Analysis zu viele zurückliegende Ereignisse analysiert. Dies führt zu einer großen Verzögerung und es dauert sehr lange, bis Sie den aktuell ablaufenden Datenverkehr betrachten können. Die Standardeinstellung entspricht **24 Stunden**.
Quellhost	Hostname der Malware Analysis-Appliance. Dies ist die IP-Adresse oder der Hostname des Services, dessen Daten von Malware Analysis zur Analyse abgefragt werden. Verwenden Sie localhost nicht als Quellhost. Je nach Modell der Appliance und der Konfiguration der NetWitness Suite-Infrastruktur kann dieser Quellhost variieren.
Quellport	Malware Analysis kommuniziert mit der NetWitness Suite-Infrastruktur über den REST-Service, der diesen Port überwacht. Die Portnummer ist für die Art von Core-Service, der als Quellhost verwendet wird, spezifisch. Dies entspricht den ausgehenden Verbindungen Ihres Core-Services.
Benutzername	Benutzername Der Standardwert ist **admin**. Malware Analysis muss sich bei jeder Datenabfrage beim Quellhost authentifizieren. In den meisten Fällen entspricht das von Malware Analysis verwendete Konto dem, das für den Zugriff auf den Core-Service durch NetWitness Suite verwendet wird. Es wird jedoch empfohlen, ein neues, für Malware Analysis dediziertes Konto für den Core-Service zu erstellen.
Benutzerpasswort	Benutzerpasswort. Der Standardwert ist **netwitness**.

Parameter	Beschreibung
SSL	Verwenden Sie SSL bei der Kommunikation mit Core. Aktivieren Sie diese Option, wenn Malware Analysis eine SSL-Verbindung für die Kommunikation mit einem Core-Service verwendet. Standardmäßig ist die Einstellung deaktiviert.
Denial of Service (DOS)-Verhinderung	Die Denial of Service (DOS)-Verhinderung ist eine Schutzfunktion gegen Schadsoftware, die vorsätzlich große Mengen an Netzwerkverbindungen zwischen zwei Endpunkten mit Windows PE-Inhalt generiert. Durch das Generieren einer großen Menge an Verbindungen wird der Datenverkehr künstlich in die Höhe getrieben. Sicherheitsdienste, die das Netzwerk überwachen, müssen diese Menge an Datenverkehr lesen und analysieren, was zu einer Dienstverweigerung (Denial of Service) führt. Diese Funktion hilft dabei, diese Sitzungen zu identifizieren, sodass die laufende Analyse diese nicht berücksichtigt. Standardmäßig ist die Einstellung deaktiviert.

Parameter	Beschreibung
DOS - Fensterlängen-Sitzungsrate (Sekunden)	Malware Analysis verwendet diesen Parameter zusammen mit den Parametern **DOS – Anzahl von Sitzungen pro Ratenfenster** und **DOS – Sitzungssperrzeit (Sekunden)**, um einen Denial-of-Service-Angriff zu identifizieren und festzulegen, wie lange Sitzungen mit einer bestimmten IP-Adresse ignoriert werden. Um einen Denial-of-Service-Angriff zu identifizieren, überwacht Malware Analysis die Anzahl an Sitzungen, die während eines bestimmten Zeitraums von einer IP-Adresse erstellt werden. Unter **DOS - Fensterlängen-Sitzungsrate (Sekunden)** wird dieser Zeitrahmen definiert. Wenn die Anzahl der Sitzungen den Wert der Einstellung **DOS – Anzahl von Sitzungen pro Ratenfenster** innerhalb der in **DOS – Fensterlängen-Sitzungsrate (Sekunden)** definierten Anzahl von Sekunden überschreitet, identifiziert Malware Analysis die Aktivität als einen Denial-of-Service-Versuch. In diesem Fall wird der von dieser IP-Adresse ausgehende Datenverkehr für die unter **DOS – Sitzungssperrzeit (Sekunden)** angegebene Dauer ignoriert. Der Standardwert ist **60** Sekunden.

Parameter	Beschreibung
DOS - Anzahl von Sitzungen pro Ratenfenster	Malware Analysis verwendet diesen Parameter zusammen mit den Parametern **DOS – Fensterlängen-Sitzungsrate (Sekunden)** und **DOS – Sitzungssperrzeit (Sekunden)**, um einen Denial-of-Service-Angriff zu identifizieren und festzulegen, wie lange Sitzungen mit dieser IP-Adresse ignoriert werden. Um einen Denial-of-Service-Angriff zu identifizieren, überwacht Malware Analysis die Anzahl an Sitzungen, die während eines bestimmten Zeitraums von einer IP-Quelle erstellt werden. Unter **DOS - Fensterlängen-Sitzungsrate (Sekunden)** wird dieser Zeitrahmen definiert. Wenn die Anzahl der Sitzungen den Wert der Einstellung **DOS – Anzahl von Sitzungen pro Ratenfenster** innerhalb der in **DOS – Fensterlängen-Sitzungsrate (Sekunden)** definierten Anzahl von Sekunden überschreitet, identifiziert Malware Analysis die Aktivität als einen Denial-of-Service-Versuch. In diesem Fall wird der Datenverkehr für die unter **DOS – Sitzungssperrzeit (Sekunden)** angegebene Dauer ignoriert. Der Standardwert ist **200** Sitzungen.

Parameter	Beschreibung
DOS - Sitzungssperrzeit (Sekunden)	Malware Analysis verwendet diesen Parameter zusammen mit den Parametern **DOS – Fensterlängen-Sitzungsrate (Sekunden)** und **DOS – Anzahl von Sitzungen pro Ratenfenster**, um einen Denial-of-Service-Angriff zu identifizieren und festzulegen, wie lange dieser Angriff ignoriert wird. Um einen Denial-of-Service-Angriff zu identifizieren, überwacht Malware Analysis die Anzahl an Sitzungen, die während eines bestimmten Zeitraums von einer IP-Adresse erstellt werden. Unter **DOS - Fensterlängen-Sitzungsrate (Sekunden)** wird dieser Zeitrahmen definiert. Wenn die Anzahl der Sitzungen den Wert der Einstellung **DOS – Anzahl von Sitzungen pro Ratenfenster** innerhalb der in **DOS – Fensterlängen-Sitzungsrate (Sekunden)** definierten Anzahl von Sekunden überschreitet, identifiziert Malware Analysis die Aktivität als einen Denial-of-Service-Versuch. In diesem Fall wird der Datenverkehr für die unter **DOS – Sitzungssperrzeit (Sekunden)** angegebene Dauer ignoriert. Der Standardwert ist **60** Sekunden.
DOS–Intervall für automatische Speicherbereinigung (Sekunden)	Führt die automatische Speicherbereinigung in der internen Speicherstruktur zur Nachverfolgung von Denial-of-Service-Versuchen durch. Ist die Speichernutzung ungewöhnlich hoch, können Sie das eingestellte Intervall verkleinern, sodass ungenutzter Speicherplatz häufiger freigegeben wird. Ist die CPU-Nutzung ungewöhnlich hoch, können Sie diese Einstellungen erhöhen, um den Verarbeitungsoverhead (auf Kosten der Speichernutzung) zu eliminieren. Der Standardwert ist **120** Sekunden.

Abschnitt „Repository-Konfiguration“

Malware Analysis speichert alle analysierten Dateien für die zukünftige Verwendung. Auf diese Dateien kann durch eines der Dateifreigabeprotokolle zugegriffen werden oder Sie können diese mithilfe der Benutzeroberfläche herunterladen.

In der Tabelle sind die Funktionen des Abschnitts „Repository-Konfiguration“ beschrieben.

Parameter	Beschreibung
Verzeichnispfad	Alle Dateien werden im folgenden Verzeichnis auf der Malware Analysis-Appliance gespeichert: **/var/lib/netwitness/spectrum**
Dateifreigabeprotokoll	Mögliche Werte für das Dateiabfrageprotokoll können sein: FTP, SAMBA oder Keines. Sie können den FTP-Zugriff und die SAMBA-Dateiabfrage aktivieren, um Benutzern den Zugriff auf die gespeicherten Dateien in Malware Analysis von einem Remotestandort aus zu ermöglichen. Für den Zugriff auf diese Dateien sind keine Anmeldeinformationen notwendig. Für den FTP-Zugriff wird der Port TCP/21 benötigt. Das Standardprotokoll zur Dateiabfrage ist **Keines**.
Aufbewahrung (in Tagen)	Malware Analysis bewahrt Dateien, die im Repository gespeichert sind, die angegebene Anzahl von Tagen auf. Sie können die Anzahl der Tage, die die Dateien vor dem Löschen aufbewahrt werden, definieren. Der Standardwert entspricht **60** Tagen.

Konfigurationsabschnitt „Verschiedenes“ (10.3 SP2 und höher)

In der Tabelle sind die Funktionen des Konfigurationsabschnitts „Verschiedenes“ beschrieben.

Parameter	Beschreibung
Maximale Dateigröße	Begrenzt die Größe jeder einzelnen Datei, nach der Sie manuell suchen können. Dieser Parameter bezieht sich auf die Funktion, die unter „Dateien hochladen für Schadsoftwarescans“ im „Leitfaden Investigation und Malware Analysis“ beschrieben ist. Der Standardwert ist **64 MB**. Wurde die maximale Dateigröße überschritten, hindert Sie daran, die Datei zu scannen.

Abschnitt Modulkonfiguration

Der Abschnitt „Modulkonfiguration“ ermöglicht die Konfiguration der Bewertungskategorien Statisch, Community und Sandbox.

Konfiguration Statische Analyse

Das statische Modul ist die einzige Bewertungskategorie, die standardmäßig aktiviert ist. In dieser Tabelle sind die Parameter für die Konfiguration der statischen Analyse beschrieben.

Funktion	Beschreibung
Aktiviert	Zum vollständigen Deaktivieren oder Aktivieren der statischen Analyse. Standardmäßig ist dies **aktiviert**.
PDF umgehen	Zum Deaktivieren der Analyse von PDF-Dokumenten. Standardmäßig ist dies deaktiviert. Alle PDF-Dateien werden einer statischen Analyse unterzogen.
Office umgehen	Zum Deaktivieren der Analyse von Office-Dokumenten. Standardmäßig ist dies deaktiviert. Alle MS-Office-Dateien werden einer statischen Analyse unterzogen.
Ausführbare Datei umgehen	Zum Deaktivieren der Analyse von Windows PE-Dokumenten. Standardmäßig ist dies deaktiviert. Alle Windows PE-Dateien werden einer statischen Analyse unterzogen.

Funktion	Beschreibung
Windows PE-Authentifizierungseinstellungen über die Cloud überprüfen	Legen Sie fest, ob Windows PE-Dateien an die RSA Netwitness-Cloud zur Authenticode-Validierung gesendet werden. Standardmäßig ist die Einstellung aktiviert. • Bei Aktivierung werden alle Windows PE-Dateien, die digital signiert werden, über das (gesamte) Netzwerk an die RSA Netwitness-Cloud zur Validierung gesendet. Sollen Windows PE-Dateien das Nutzernetzwerk nicht verlassen, müssen Sie diese Option deaktivieren. • Ist diese Option nicht aktiviert, wird die statische Analyse lokal durchgeführt (Authenticode-Validierung wird übersprungen). Unabhängig von dieser Einstellung sind PDF- und MS Office-Dokumente nicht von der Authenticode-Validierung betroffen und werden während der statischen Analyse nicht über das Netzwerk gesendet.

Konfiguration der Communityanalyse

Das Communitymodul ist standardmäßig deaktiviert und die Optionen sind aktiviert, um zu verhindern, dass PDF- und MS Office-Dokumente verarbeitet werden. Die Einstellungen sollen so restriktiv wie möglich gewählt werden, sodass keine sensiblen Dokumente das Netzwerk ohne Zustimmungen durch den Nutzer verlassen. In dieser Tabelle sind die Parameter zur Konfiguration der Communityanalyse beschrieben.

Funktion	Beschreibung
Aktiviert	Zum vollständigen Deaktivieren oder Aktivieren der statischen Analyse. Standardmäßig ist dies **deaktiviert**.
PDF umgehen	Zum Deaktivieren der Analyse von PDF-Dokumenten. Standardmäßig ist dies aktiviert und PDF-Dateien werden nicht verarbeitet.
Office umgehen	Zum Deaktivieren der Analyse von Office-Dokumenten. Standardmäßig ist dies aktiviert und Microsoft Office-Dokumente werden nicht verarbeitet.

Funktion	Beschreibung
Ausführbare Datei umgehen	Zum Deaktivieren der Analyse von Windows PE-Dokumenten. Standardmäßig ist dies aktiviert und Windows PE-Dokumente werden nicht verarbeitet.

Konfiguration Sandbox-Analyse

Das Sandbox-Modul ist standardmäßig deaktiviert und MS Office- sowie PDF-Dateien werden nicht verarbeitet. Die Einstellungen sollen so restriktiv wie möglich gewählt werden, sodass der Nutzer ganz gezielt auswählen muss, ob potenziell vertrauliche Informationen übermittelt und außerhalb des Netzwerkes verarbeitet werden. Wird der Dokumenttyp dennoch verarbeitet, wird die Datei als Ganzes (nicht nur ein Hash oder Dateiinhalte) an den Ziel-Sandbox-Server gesendet.

In dieser Tabelle sind die Parameter zur Konfiguration der Sandbox-Analyse beschrieben.

Funktion	Beschreibung
Aktiviert	Zum vollständigen Deaktivieren oder Aktivieren der Sandbox-Analyse. Standardmäßig ist dies **deaktiviert**.
PDF umgehen	Zum Deaktivieren der Analyse von PDF-Dokumenten. Standardmäßig ist dies aktiviert und PDF-Dateien werden nicht verarbeitet. Ist dies nicht ausgewählt, werden alle PDF-Dateien in ihrer Gesamtheit zur Analyse an die Sandbox gesendet.
Office umgehen	Zum Deaktivieren der Analyse von Office-Dokumenten. Standardmäßig ist dies aktiviert und Microsoft Office-Dokumente werden nicht verarbeitet. Ist dies nicht ausgewählt, werden alle MS Office-Dateien als Ganzes zur Analyse an die Sandbox gesendet.
Ausführbare Datei umgehen	Zum Deaktivieren der Analyse von Windows PE-Dokumenten. Standardmäßig ist dies aktiviert und Windows PE-Dokumente werden nicht verarbeitet. Ist diese Option nicht ausgewählt, werden alle Windows PE-Dateien als Ganzes zur Analyse an die Sandbox gesendet.

Funktion	Beschreibung
Ursprünglichen Dateinamen beim Ausführen der Sandbox-Analyse beibehalten	Aktivieren Sie in 10.3 SP2 und späteren Versionen die Funktion zum Hashen von Dateinamen, wenn diese an eine lokale Sandbox gesendet werden. Standardmäßig ist die Einstellung deaktiviert. **Hinweis:** Wenn Sie diesen Parameter nicht aktivieren, weist NetWitness Suite der Datei einen Hash-Wert zu.

Einstellungen für eine GFI-Sandbox

Im Abschnitt „GFI-Sandbox“ können Sie die Sandbox-Verarbeitung durch GFI aktivieren und die lokal installierte GFI-Sandbox konfigurieren. In dieser Tabelle werden die Parameter zur Konfiguration der GFI-Sandbox beschrieben.

Funktion	Beschreibung
Aktiviert	Ist diese Option aktiviert, wird die Sandbox-Verarbeitung durch eine lokale Kopie von GFI durchgeführt. Standardmäßig ist die Einstellung **deaktiviert**. Wenn Sie GFI aktivieren, müssen Sie die restlichen Parameter konfigurieren.
Servername	Der Servername der GFI-Sandbox. Kein Standardwert.
Serverport	Der Serverport der GFI-Sandbox. Der Standardwert beträgt **80**.
Max. Polling-Dauer	Bestimmt die Verarbeitungsdauer einer übermittelten Probe. Der Standardwert beträgt **600 Sekunden**.
Webproxyeinstellungen ignorieren	Weist Malware Analysis an, beim Herstellen dieser Verbindung den Webproxy zu umgehen, sofern dieser konfiguriert ist. Wenn kein Webproxy in Malware Analysis konfiguriert wurde, wird die Einstellung ignoriert.

Einstellungen für eine ThreatGrid-Sandbox

Im Bereich „ThreatGrid-Sandbox“ können Sie die Sandbox-Verarbeitung durch ThreatGrid aktivieren und wählen, ob für die Sandbox-Analyse ein lokal installierter ThreatGrid oder eine ThreatGrid-Cloud verwendet wird.

- Wenn Sie eine lokale Kopie von ThreatGrid besitzen, konfigurieren Sie die Sandbox-Verarbeitung für diese lokale Kopie.
- Wurde keine lokale Instanz von ThreatGrid erworben oder installiert, konfigurieren Sie die ThreatGrid-Cloud.

In dieser Tabelle werden die Parameter zur Konfiguration der ThreatGrid-Sandbox beschrieben.

Hinweis: Bevor Sie diesen Service aktivieren, müssen Sie einen von ThreatGrid bereitgestellten Serviceschlüssel konfigurieren. Der Dienstschlüssel ermöglicht es ThreatGrid zu erkennen, dass die von diesem Standort eingereichten Stichproben unbedenklich sind.

Funktion	Beschreibung
Aktiviert	Ist diese Option aktiviert, führt entweder eine lokale Kopie von ThreatGrid oder die ThreatGrid-Cloud diese Sandbox Verarbeitung aus. Der Standardwert ist **deaktiviert**.
Serviceschlüssel	Bevor Sie das Sandbox-Modul aktivieren, müssen Sie einen von ThreatGrid bereitgestellten Serviceschlüssel konfigurieren. Der Dienstschlüssel ermöglicht es ThreatGrid zu erkennen, dass die von diesem Standort eingereichten Stichproben unbedenklich sind.
URL	Die vom ThreatGrid-Server verwendete URL (wenn Sie keinen lokal installierten ThreatGrid verwenden). Die ThreatGrid-Cloud finden Sie unter https://panacea.threatgrid.com.
Webproxyeinstellungen ignorieren	Weist Malware Analysis an, beim Herstellen dieser Verbindung den Webproxy zu umgehen, sofern dieser konfiguriert ist. Wenn kein Webproxy in Malware Analysis konfiguriert wurde, wird die Einstellung ignoriert.

Ansicht „Service-Konfiguration“ – Registerkarte „Hash“

Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „Hash“ der Ansicht „Service-Konfiguration“ für Malware Analysis.

Auf dieser Registerkarte können Sie die Hash-Filterung in Malware Analysis verwalten. Zunächst ist das Hash-Raster leer. Im Raster werden die Filter aufgeführt, die Malware Analysis hinzugefügt wurden. In dieser Ansicht können Sie einen Hash-Filter hinzufügen, löschen, als vertrauenswürdig oder nicht vertrauenswürdig markieren und Änderungen speichern.

Dies ist ein Beispiel für die Registerkarte „Hash“.

Dies ist ein Beispiel für das Dialogfeld Hash hinzufügen.

Funktionen

Die Registerkarte **Hash** umfasst eine Symbolleiste und ein auslagerungsfähiges Hash-Raster.

In dieser Tabelle wird die Symbolleiste auf der Registerkarte „Hash“ beschrieben.

Funktion	Beschreibung
MD5-Suche	Geben Sie einen MD5-Hash ein, für den Sie Ergebnisse im Raster suchen möchten. Bei der Suchfunktion wird zwischen Groß- und Kleinschreibung unterschieden.
Hinzufügen	Zeigt das Dialogfeld Hash hinzufügen an, in dem Sie dem Hash-Raster einen neuen Hash hinzufügen können, angeben können, ob der Hash vertrauenswürdig ist, und die Hash-Dateigröße angeben können.
Bearbeitung speichern	Speichert alle hinzugefügten oder bearbeiteten Hashes im Hash-Raster.
Delete	Löscht ausgewählte Hashes aus dem Raster.

In dieser Tabelle werden die Spalten des Hash-Rasters beschrieben.

Funktion	Beschreibung
Ausgewähltes Kontrollkästchen	Klicken Sie zum Auswählen einer Zeile. Klicken Sie in die Spaltenüberschrift, um einen Header auszuwählen.
Vertrauenswürdig	Markiert einen Hash als vertrauenswürdig oder nicht vertrauenswürdig.
MD5	Identifiziert den MD5-Hash.
Dateigröße	Identifiziert die Hash-Dateigröße in Kilobyte.

Ansicht „Service-Konfiguration“ – Registerkarte „Indikatoren für eine Infizierung“

Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „Indikatoren für eine Infizierung“ der Servicekonfigurationsansicht, die für den Malware Analysis-Service gilt. Diese Registerkarte bietet die Möglichkeit, zu konfigurieren, wie jedes der vier Bewertungsmodule die verfügbaren Regeln zur Bewertung von Daten verwendet.

Dies ist ein Beispiel für die Registerkarte Indikatoren für eine Infizierung.

Funktionen

Die Registerkarte Indikatoren für eine Infizierung besteht aus einer Symbolleiste und einem auslagerbaren Raster.

In dieser Tabelle werden die Funktionen des Rasters beschrieben.

Funktion	Beschreibung
Modulauswahlliste	Wählt das Bewertungsmodul aus, für das Sie die Indikatoren für eine Infizierung anzeigen möchten: Alle, Netzwerk, Statisch, Community, Sandbox oder Yara.
Feld „Suche“	Geben Sie in das Beschreibungsfeld Text ein, nach dem Sie suchen möchten.
Option „Suche“	Filtert das Raster so, dass nur Beschreibungen angezeigt werden, die den Beschreibungssuchbegriffen entsprechen.
Alle aktivieren	Klicken Sie hierauf, um alle Regeln für das Bewertungsmodul zu aktivieren, statt alle Regeln auf der Seite über das Kontrollkästchen zu aktivieren.
Aktivieren	Klicken Sie hierauf, um die ausgewählten Regeln zu aktivieren.
Alle deaktivieren	Klicken Sie hierauf, um alle Regeln für das Bewertungsmodul zu deaktivieren, statt alle Regeln auf der Seite über das Kontrollkästchen zu deaktivieren.

Funktion	Beschreibung
Deaktivieren	Klicken Sie hierauf, um die ausgewählten Regeln zu deaktivieren.
Alle zurücksetzen	Klicken Sie hierauf, um alle Zeilen auf der Seite auf ihre Standardwerte zurückzusetzen.
Zurücksetzen	Klicken Sie hierauf, um die ausgewählten Zeilen auf ihre Standardwerte zurückzusetzen.
Speichern	Klicken Sie hierauf, um an dieser Seite vorgenommene Änderungen zu speichern. Wenn Sie die Seite verlassen, ohne sie zu speichern, gehen die Änderungen verloren. Die Beschreibung jeder Zeile mit nicht gespeicherten Änderungen hat eine rote Ecke.

In dieser Tabelle werden die Funktionen der Symbolleiste beschrieben.

Spalte	Beschreibung
Kontrollkästchen „Auswahl“	Kontrollkästchen zur Auswahl einzelner Zeilen oder aller Zeilen auf der Seite.
Kontrollkästchen „Aktiviert“	Wenn die Indikatoren für eine Infizierung aktiviert sind, verwendet Malware Analysis die Regel für die Bewertung von Sitzungsdaten.
Kontrollkästchen „Hohe Wahrscheinlichkeit“	Im aktivierten Zustand behandelt Malware Analysis die Regel als eine, die das Vorhandensein von Schadsoftware sehr wahrscheinlich anzeigen wird, und ein Ereignis, das diese Regel auslöst, wird im Ergebnisraster markiert.
Beschreibung	Beschreibt die Indikatoren für eine Infizierung.
Bewertung	Gibt den Wert an, den Sie für jedes Ereignis, das die Regel auslöst, für den Gesamtwert berücksichtigen möchten. Der Standardwert wird angezeigt und Sie können den Wert erhöhen oder senken, indem Sie den Schieberegler bewegen oder eine Zahl in das Wertfeld eingeben.
Dateityp	Zeigt die Dateitypen an, für die die Regel gilt. Mögliche Werte sind **ALLE**, **PDF**, **MS Office** und **Windows PE**.

Ansicht „Service-Konfiguration“ – Registerkarte „Integration“

Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „Integration“ in der Ansicht „Administration > Service-Konfiguration“ für Malware Analysis. Diese Registerkarte bietet eine Möglichkeit, durch Registrierung des Malware Analysis-Services Verbindungen zu testen und Communitybewertungen zu aktivieren. Ein Administrator kann die Verbindung zu cloud.netwitness.com und zu einem Core-Service testen, der für kontinuierliches Scannen konfiguriert wurde.

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Integration“.

Funktionen

Diese Registerkarte ist in zwei Abschnitte aufgeteilt: RSA-Cloud-Verbindungstest und -Registrierung und Verbindungstest für kontinuierliches Scannen. In der folgenden Tabelle sind die Funktionen beschrieben.

Funktion	Beschreibung
Schaltfläche „RSA-Cloud-Verbindungstest und -Registrierung“	Durch Klicken auf diese Schaltfläche können Sie testen, ob eine aktive Verbindung zu cloud.netwitness.com besteht. NetWitness Suite testet Kommunikationen mit der Website und prüft Proxyeinstellungen. Eine gültige Verbindung ist erforderlich, um sich beim RSA Community Service zu registrieren.
Unternehmensname	Dies ist der Name Ihrer Firma. Dies ist ein Pflichtfeld.
E-Mail-Adresse des Kontakts	Dies ist die E-Mail-Adresse des Kontakts. Dies ist ein Pflichtfeld.
Kontrollkästchen „Nur für EMC-interne Verwendung?“	Hierbei handelt es sich um ein optionales Feld. EMC Kunden, Vertriebsmitarbeiter, oder Benutzer der Demo sollten diese Option aktivieren, um dafür zu sorgen, dass ihre Anforderungen keine Bandbreite auf dem Produktionsserver verwenden. Wenn das Kästchen aktiviert ist, wird die folgende Warnmeldung angezeigt: `Checking this box may cause a less robust performance because the production server isn't being used.`

Funktion	Beschreibung
Schaltfläche Registrieren	Das Klicken auf die Schaltfläche „Registrieren“ schließt die Registrierung ab, wenn alle Pflichtfelder ausgefüllt sind. Die Schaltfläche „Registrieren“ wird zur Schaltfläche „Aktualisieren“, nachdem die Registrierung abgeschlossen ist.
Schaltfläche „Update“	Die Schaltfläche „Aktualisieren“ wird angezeigt, nachdem die Registrierung abgeschlossen ist.
Schaltfläche „Verbindungstest für kontinuierliches Scannen“	Durch Klicken auf diese Schaltfläche wird die Prüfung initiiert, ob der Malware Analysis-Service sich mit dem Core-Service verbinden kann, der für kontinuierliches Scannen ausgewählt wurde (Quellhost, Quellport, Benutzername und Benutzerpasswort wie auf der Registerkarte „Allgemein“ angegeben).

Ansicht „Service-Konfiguration“ – Registerkarte „IOC-Zusammenfassung“

In diesem Thema erhalten Sie eine Einführung zu den Funktionen auf der Registerkarte „IOC-Zusammenfassung“ in der Ansicht „Service-Konfiguration“. Auf dieser Registerkarte können Sie für jeden IOC zusammenfassende Informationen anzeigen. Ein Raster für jedes Bewertungsmodul listet die konfigurierten IOCs jeweils zusammen mit den Statistiken für den IOC für einen bestimmten Zeitbereich auf. Hierzu gehören die folgenden Statistiken:

- die Anzahl an Ereignissen für eine Netzwerksitzung oder die Anzahl an im IOC gekennzeichneten Dateien für ein statisches Ereignis bzw. ein Community- oder Sandbox-Ereignis
- die aktuelle für den IOC konfigurierte Bewertung auf der Registerkarte Indikatoren für eine Infizierung
- die von den einzelnen Bewertungsmodulen zurückgegebenen Bewertungen

Wenn Sie ein Ereignis auswählen, können Sie entweder die Ansicht Schadsoftwareereignisse oder die Ansicht Schadsoftwaredateien für den IOC anzeigen. Sie können den ausgewählten IOC auch auf der Registerkarte „Indikatoren für eine Infizierung“ öffnen, um die aktuelle Bewertung zu bearbeiten.

Dies ist ein Beispiel der Registerkarte „IOC-Zusammenfassung“ für das Netzwerk-Bewertungsmodul.

Funktionen

Die IOC-Zusammenfassung enthält vier Registerkarten – eine pro Bewertungsmodul: Netzwerk, Statisch, Community und Sandbox. Alle Registerkarten besitzen dasselbe Format und dieselben Informationen sowie eine Symbolleiste und ein auslagerbares Raster.

In der folgenden Tabelle werden die Funktionen der einzelnen Registerkarten beschrieben.

Funktion	Beschreibung
Zeitbereich	Wählt den Zeitbereich für die IOC-Zusammenfassung aus. Die möglichen Werte sind: „Letzte 5 Minuten„, „Letzte 15 Minuten“, „Letzte 30 Minuten“, „Letzte Stunde“, „Letzte 3 Stunden“, „Letzte 6 Stunden“, „Letzte 12 Stunden“, „Letzte 24 Stunden“, „Letzte 2 Tage“, „Letzte 5 Tage“, „Morgen“, „Vormittag“, „Nachmittag“, „Abend“, „Den ganzen Tag“, „Gestern“, „Diese Woche“, „Letzte Woche“ oder „Benutzerdefiniert“.
Spalte Beschreibung	Führt die Beschreibungen für die IOCs auf.
Spalte Anzahl	Führt die Anzahl der Vorkommen von IOCs auf. Auf der Registerkarte Netzwerk ist dies die Anzahl an Ereignissen, in denen ein IOC gefunden wurde. Auf den anderen Registerkarten stellt der Wert unter Anzahl die Anzahl an Dateien dar, in denen ein IOC gefunden wurde.
Spalte Aktuelle Bewertung	Führt die aktuelle Bewertung für die IOCs laut der Konfiguration auf der Registerkarte Indikatoren für eine Infizierung auf.
Spalten Statisch, Netzwerk, Community und Sandbox	Führt die Bewertungen auf, die die einzelnen Bewertungsmodule den IOCs zugewiesen haben.
Drop-down-Menü „Aktionen“	Das Drop-down-Menü „Aktionen“ enthält zwei Optionen: „Ereignisse/Dateien anzeigen“ und „Bearbeiten“. Über die Option „Ereignisse anzeigen“ wird der IOC in der Ansicht „Ermittlungsereignisse“ bzw. „Dateien“ geöffnet. Sie können diese Ansicht auch aufrufen, indem Sie auf den IOC doppelklicken. Über die Option Bearbeiten wird der IOC auf der Registerkarte Indikatoren für eine Infizierung geöffnet, damit die aktuelle Bewertung bearbeitet werden kann.

Ansicht „Service-Konfiguration“ – Registerkarte „Proxy“

In diesem Thema werden die Parameter beschrieben, die auf der Registerkarte „Proxy“ in der Ansicht „Service-Konfiguration“ für einen Malware Analysis-Service konfiguriert werden können. Auf dieser Registerkarte wird die Malware Analysis-Kommunikation mit der RSA-Cloud für die Communityanalyse und mit dem Sandbox-Service für die Sandbox-Analyse über einen Webproxy konfiguriert, um Anonymität zu gewährleisten. Wenn Sie einen lokalen Sandbox-Service verwenden, ist die Kommunikation über einen Webproxy nicht erforderlich und kann die Performance beeinträchtigen. Beim Konfigurieren des Sandbox-Moduls auf der Registerkarte **Allgemein** können Sie festlegen, dass der konfigurierte Webproxy umgangen werden soll.

Dies ist ein Beispiel für die Registerkarte „Proxy“.

Funktionen

In dieser Tabelle werden die Funktionen auf der Registerkarte „Proxy“ beschrieben.

Funktion	Beschreibung
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um die Kommunikation mit der RSA-Cloud für die Communityanalyse und mit dem Sandbox-Service für die Sandbox-Analyse über einen Webproxy durchzuführen, um Anonymität zu gewährleisten.
Webproxyeinstellungen automatisch erkennen	Aktivieren Sie dieses Kontrollkästchen, um die in den Systemeinstellungen konfigurierten Einstellungen zu verwenden.
Proxyhost	Geben Sie den Hostnamen für den Proxyhost ein.
Proxyport	Geben Sie den Port für die Kommunikation mit dem Proxyhost ein.
Benutzer	Geben Sie den zum Anmelden beim Proxyhost verwendeten Benutzernamen ein.
Benutzerpasswort	Geben Sie das Benutzerpasswort für die Anmeldung beim Proxyhost ein.
SSL	(Optional) Aktivieren Sie das Kontrollkästchen, um die Kommunikation über SSL zu aktivieren.

Funktion	Beschreibung
Schaltfläche Anwenden	Klicken Sie auf die Schaltfläche **Anwenden**, um die gewählten Einstellungen zu übernehmen.

Ansicht „Service-Konfiguration“ – Registerkarte „ThreatGRID“

In diesem Thema werden die Parameter erläutert, die zum Abrufen eines ThreatGRID-API-Testschlüssels für die ThreatGrid-Cloud-Sandbox auf der Malware Analysis-Registerkarte **ThreatGRID** erforderlich sind. Bevor ThreatGrid als Sandbox-Service im Sandbox-Modul aktiviert werden kann, muss ein von ThreatGrid bereitgestellter Serviceschlüssel so konfiguriert werden, dass ThreatGrid erkennen kann, dass Muster, die von dieser Site übermittelt werden, legitim sind.

Wenn Sie keinen von ThreatGrid bereitgestellten Serviceschlüssel haben, können Sie mithilfe dieser Registerkarte einen Schlüssel erhalten. Der Schlüssel wird versuchsweise bereitgestellt.

Dies ist ein Beispiel für die Registerkarte „ThreatGRID“.

Funktionen

In dieser Tabelle werden die Funktionen der Registerkarte **ThreatGRID** beschrieben.

Funktion	Beschreibung
Vor- und Nachname	Ihr Vor- und Nachname.
Titel	Ihre Position.
Name der Organisation	Der Name Ihres Unternehmens.
E-Mail	Ihre E-Mail-Adresse.
Benutzer-ID	Ihre Benutzer-ID für den Zugriff auf ThreatGrid.
Password	Ihr Passwort für den Zugriff auf ThreatGrid.
Schaltfläche Registrieren	Klicken Sie auf **Registrieren** um die Anforderung abzusenden.