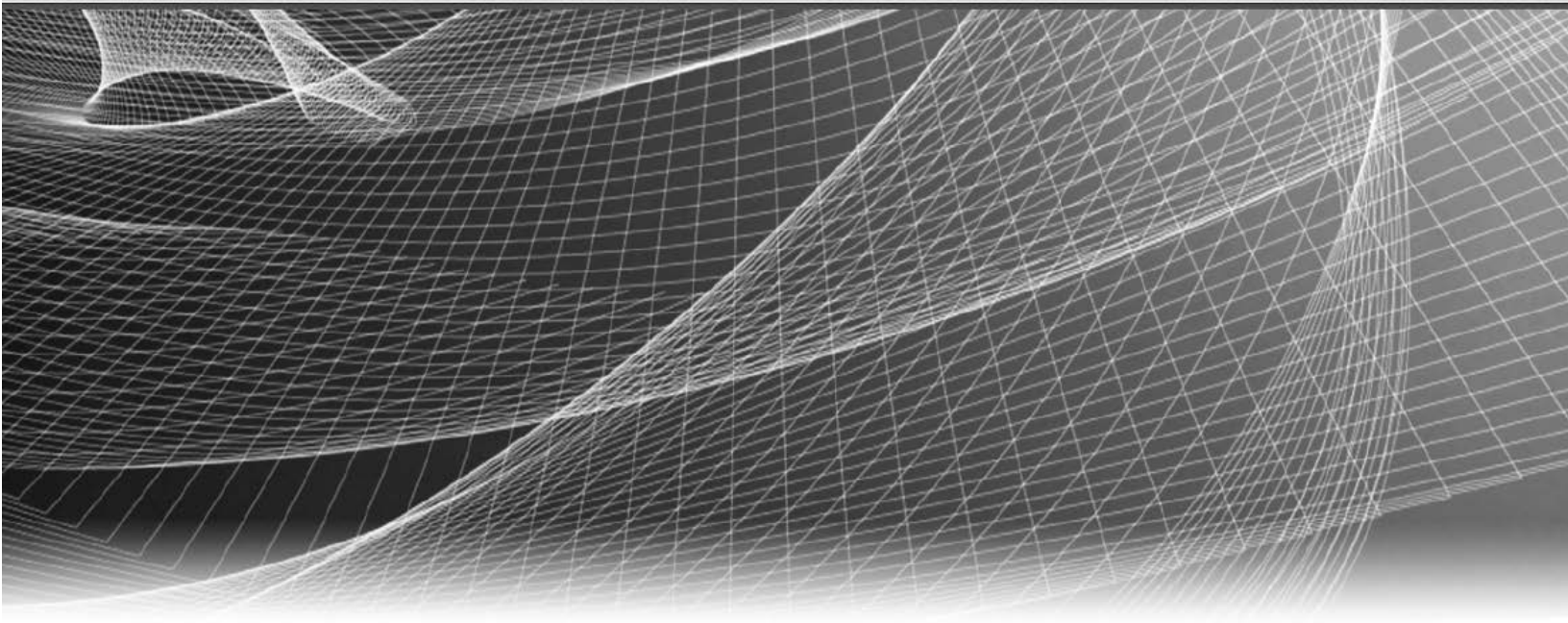


RSA Security Analytics

Konfigurationsleitfaden Malware Analysis für Version 10.6

für Version 10.6

RSA

EMC²

Marken

Lizenzvereinbarung

Drittanbieterlizenzen

Hinweis zu Verschlüsselungstechnologien

Verteilung

Inhalt

Funktionsweise von Malware Analysis 1

Funktionsübersicht 1

Analysemethode 3

Security Analytics-Serverzugriff auf den Malware Analysis-Service 3

Bewertungsmethode: 4

Bereitstellung 4

Bewertungsmodule 6

Netzwerk 6

Statische Analyse 7

Community 7

Sandbox 7

Rollen und Berechtigungen für Analysten 8

Erforderliche Rollen und Berechtigungen 8

Basiseinrichtung 11

Konfigurieren der Malware Analysis-Betriebsumgebung 13

Netzwerkverbindungen 14

Hinzufügen eines Malware Analysis-Hosts und -Services 15

Voraussetzung 15

Verfahren 15

Konfigurieren der allgemeinen Malware Analysis-Einstellungen 18

Anzeigen der Basiseinstellungen 19

Konfigurieren der kontinuierlichen Abfrage 19

Konfigurieren von Einstellungen für den manuellen Dateiupload 22

Konfigurieren des Daten-Repository 22

Kalibrieren von Bewertungsmodulen 23

Konfigurieren der statischen Analysebewertung 24

Konfigurieren der Communityanalysebewertung 24

Konfigurieren der Sandbox-Analysebewertung 25

Konfigurieren der Indikatoren für eine Infizierung 28

Filtern der angezeigten IOCs nach Modul 30

Filtern der angezeigten Module, damit nur veränderte Module angezeigt werden 31

Aktivieren und Deaktivieren von IOCs für ein Bewertungsmodul 32
Anpassung der Bewertungsgewichtung für IOCs 33
Einstellen der Kennzeichnung Hohe Wahrscheinlichkeit für IOCs 34
Zurücksetzen von IOCs auf die Standardeinstellungen 34
Konfigurieren installierter Virenschutzanbieter 35
Identifizieren installierter Virenschutzsoftware 36
Aktivieren der Communityanalyse 37
(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host 39
Konfigurieren des Auditing-Schwellenwerts 40
Konfigurieren von Warnmeldungen für Incident Management 40
Konfigurieren des SNMP-Auditing 41
Konfigurieren von Dateiaudit-Einstellungen 41
Konfigurieren von Syslog-Auditing-Einstellungen 42
(Optional) Konfigurieren eines Hash-Filters 43
Anzeigen der Hash-Liste 44
Hinzufügen eines Datei-Hashs zum Hash-Filter 44
Markieren eines Hashs als vertrauenswürdig oder nicht vertrauenswürdig 45
Löschen eines Hashs aus dem Hash-Filter 45
Nach einem Datei-Hash suchen 46
Importieren einer Hash-Liste mithilfe des überwachten Ordners 46
(Optional) Konfigurieren der Malware Analysis-Proxyeinstellungen 51
Konfigurieren des Webproxys 51
(Optional) Registrieren für einen ThreatGrid-API-Schlüssel 52

Zusätzliche Verfahren 54

Erstellen angepasster Warnmeldungen im CEF-Format 54
Die CEF-Vorlage 54
Verstehen eines Syslog-Auditing-Dateieintrags 55
Bearbeiten Sie die Konfigurationsdatei. 60
Beispiel 60
Aktivieren von angepassten YARA-Inhalten 74
Voraussetzungen 75
Installieren von Bibliotheken und Anwendungen, die zum Erstellen von YARA auf einer CentOs-basierten Appliance erforderlich sind 75
Einrichten von Yara 76

Ressourcen für Malware Analysis 78

Ansicht „Service-Konfiguration“ – Registerkarte „Auditing“ 79

Funktionen 80

Ansicht „Service-Konfiguration“ – Registerkarte „AV“ 86

Funktionen 86

Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“ 88

Funktionen 88

Konfiguration Statische Analyse 97

Konfiguration der Communityanalyse 99

Konfiguration Sandbox-Analyse 100

Einstellungen für eine GFI-Sandbox 101

Einstellungen für eine ThreatGrid-Sandbox 102

Ansicht „Service-Konfiguration“ – Registerkarte „Hash“ 104

Funktionen 104

Ansicht „Service-Konfiguration“ – Registerkarte „Indikatoren für eine Infizierung“ 106

Funktionen 106

Ansicht „Service-Konfiguration“ – Registerkarte „Integration“ 109

Funktionen 109

Ansicht „Service-Konfiguration“ – Registerkarte „IOC-Zusammenfassung“ 111

Funktionen 112

Ansicht „Service-Konfiguration“ – Registerkarte „Proxy“ 114

Funktionen 114

Ansicht „Service-Konfiguration“ – Registerkarte „ThreatGRID“ 116

Funktionen 116

Funktionsweise von Malware Analysis

Security Analytics 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. Mit Malware Analysis kann der Schadsoftwareanalyst unter den zahlreichen erfassten Dateien die Dateien priorisieren, von denen potenziell die größte Gefahr ausgeht.

Security Analytics 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.

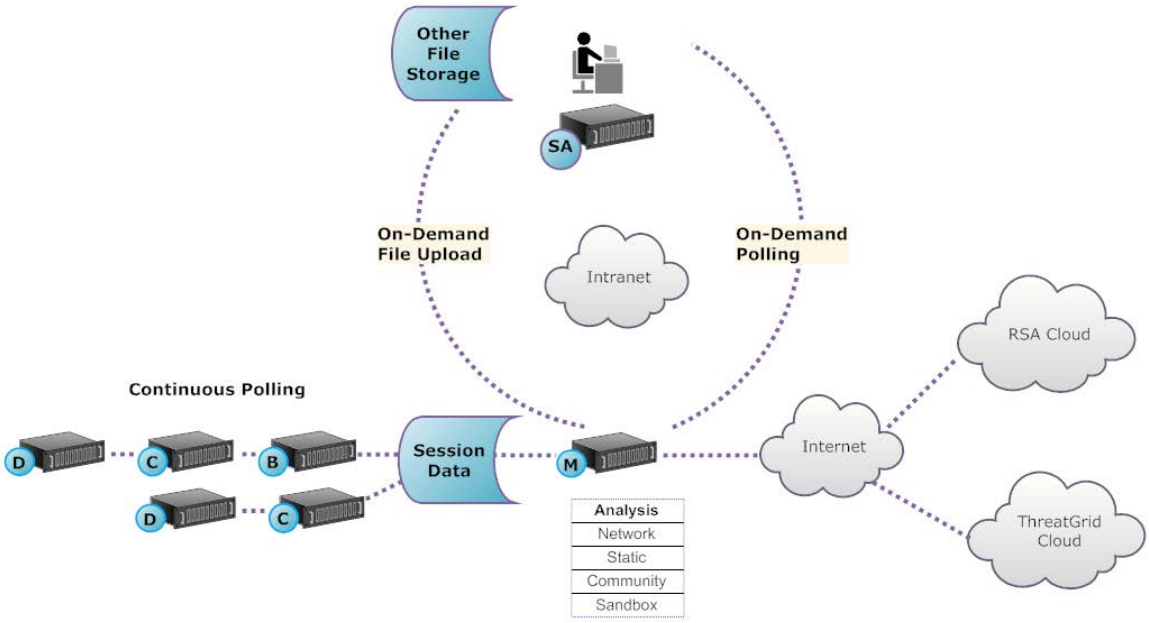
Neben den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis ab Security Analytics 10.3 die Indikatoren für infizierte Dateien, die in YARA geschrieben wurden. YARA ist eine Regelsprache, die es Schadsoftwareforschern ermöglicht, Schadsoftwaremuster zu identifizieren und zu klassifizieren. 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.

Ab Security Analytics 10.4 bietet Malware Analysis Funktionen, die Warnmeldungen für Incident Management unterstützen.

Funktionsübersicht

In dieser Abbildung ist die funktionelle Beziehung zwischen den Security Analytics Core-Services (Decoder, Concentrator und Broker), dem Security Analytics Malware Analysis-Service und dem Security Analytics-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 Security Analytics 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 Abfrage eines Concentrator oder Broker nach Bedarf 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. Der Schadsoftwareanalyst verwendet Security Analytics, um einen Ordnerspeicherort auszuwählen und ein oder mehrere Dateien zu identifizieren, die hochgeladen und von Security Analytics 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).

Security Analytics 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 Security Analytics Malware Analysis ideal ergänzen.

Security Analytics-Serverzugriff auf den Malware Analysis-Service

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

- Kostenloses Abonnement: Alle Security Analytics-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. Auf jeden IOC wird eine Bewertungsskala von -100 (gut) bis +100 (schlecht) angewendet. 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 Security Analytics 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 Security Analytics importiert wurde, stehen alle Anzeige- und Analysefunktionen in Security Analytics 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 Security Analytics Malware Analysis-Service wird als paralleler Service auf einem Security Analytics-Server oder mit einem dedizierten RSA Malware Analysis-Host bereitgestellt.

Der dedizierte Malware Analysis-Host verfügt über einen integrierten Broker, der eine Verbindung mit der Security Analytics 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 Security Analytics Malware Analysis analysiert und wertet Sitzungen und die integrierten Dateien in diesen Sitzungen aus, indem vier Kategorien ausgewertet werden: 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.

Security Analytics Malware Analysis kann Ermittlungen 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 Security Analytics Core-Kernnetzwerksitzung, 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 Security Analytics 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 Security Analytics 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 Security Analytics 10.5 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.

Hinweis: Beim Upgrade von Security Analytics 10.4 auf Security Analytics 10.5 wird die standardmäßige Rolle `MalwareAnalysts` von Security Analytics 10.4 ohne Änderungen an den zugewiesenen Berechtigungen in `Malware_Analysts` umbenannt.
Beim Durchführen eines Upgrades von Security Analytics 10.3 und früher enthält die Rolle `Malware Analyst` einen Teil dieser Berechtigungen. Die Standardrolle `Malware Analyst` wird in `MalwareAnalysts` umbenannt, sofern sie vorhanden ist, und die neuen Berechtigungen werden hinzugefügt. Wenn die Rolle `Malware Analyst` nicht vorhanden ist, wird die neue Rolle `MalwareAnalysts` erstellt.

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.

Basiseinrichtung

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

Schritt	Allgemeine Aufgaben	Abgeschlossen
1	Konfigurieren der Malware Analysis-Betriebsumgebung Wenn Ihr Standort eine dedizierte Appliance verwendet, führen Sie einen der folgenden Schritte aus: • Wenn Ihr Standort eine neue dedizierte Security Analytics Malware Analysis-Appliance hinzufügt, installieren Sie die physische Security Analytics Malware Analysis-Appliance in Ihrem Netzwerk und konfigurieren Sie die Betriebsumgebung. • Wenn an Ihrem Standort eine dedizierte Spectrum-Appliance auf eine dedizierte Security Analytics Malware Analysis-Appliance aktualisiert werden soll, müssen Sie die Spectrum-Appliance per Image neu mit Security Analytics Malware Analysis erstellen.	
2	Hinzufügen eines Malware Analysis-Hosts und -Services **Hinweis:** Um diesen Schritt abzuschließen, müssen Sie den Security Analytics-Lizenzserver so eingerichtet haben, wie es im Leitfaden zur Security Analytics-Lizenzierung beschrieben ist. Erstellen Sie in Security Analytics einen Malware Analysis-Service und aktivieren Sie die Lizenz. Der Standard REST-Port ist 60007. Auf Standorten, an denen die kostenlose Version von Security Analytics Malware Analysis verwendet wird, muss die Service-IP-Adresse als localhost oder loopback installiert werden.	

Schritt	Allgemeine Aufgaben	Abgeschlossen
3	Konfigurieren der allgemeinen Malware Analysis-Einstellungen Konfigurieren Sie die allgemeinen Einstellungen für Security Analytics Malware Analysis. • 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.	
4	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.	
5	Konfigurieren installierter Virenschutzanbieter Konfigurieren Sie die Antivirus-Anbieter, die Sie installiert haben.	
6	Aktivieren der Communityanalyse Registrieren Sie sich in der RSA-Cloud und testen Sie Verbindungen, um Communitybewertungen zu aktivieren.	
7	(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host Konfigurieren Sie Schwellenwerte für das Auditing und aktivieren Sie Syslog, SNMP und Dateiauditing.	
8	(Optional) Konfigurieren eines Hash-Filters Konfigurieren Sie Hash-Filter zur Feinabstimmung der Security Analytics Malware Analysis-Ereignisanalye basierend auf bekannten sauberen oder fehlerhaften Datei-Hashs.	

Schritt	Allgemeine Aufgaben	Abgeschlossen
9	(Optional) Konfigurieren der Malware Analysis-Proxyeinstellungen Konfigurieren Sie Malware Analysis für die Kommunikation mit RSA Cloud über einen Webproxy statt direkt zu kommunizieren.	
10	(Optional) Registrieren für einen ThreatGrid-API-Schlüssel Registrieren Sie sich für einen ThreatGrid-API-Schlüssel.	

Konfigurieren der Malware Analysis-Betriebsumgebung

In diesem Thema werden die Verfahren zum Konfigurieren der Security Analytics-Betriebsumgebung für die Verbindung mit einem Security Analytics Malware Analysis-Service beschrieben. Security Analytics Malware Analysis kann als paralleler Service auf einem Security Analytics-Server oder als Service auf einer dedizierten Malware Analysis-Appliance ausgeführt werden. Wenn Ihr Standort eine dedizierte Appliance verwendet, führen Sie einen der folgenden Schritte aus:

- Wenn Ihr Standort eine neue dedizierte Security Analytics Malware Analysis-Appliance hinzufügt, installieren Sie die physische Security Analytics Malware Analysis-Appliance in Ihrem Netzwerk und konfigurieren Sie die Betriebsumgebung.
- Wenn an Ihrem Standort eine dedizierte Spectrum-Appliance auf eine dedizierte Security Analytics Malware Analysis-Appliance aktualisiert werden soll, müssen Sie die Spectrum-Appliance per Image neu als Security Analytics Malware Analysis-Appliance erstellen.

Security Analytics Malware Analysis ist bei der Ausführung abhängig von der Core-Infrastruktur. Um eine erfolgreiche Datenanalyse durch Security Analytics 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 Security Analytics Core-Infrastruktur.

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

2. Verwenden Sie Security Analytics Live, um alle Live-Ressourcen mit dem Tag malware analysis zu suchen, und stellen Sie diese Ressourcen für jeden Decoder-Service bereit, der Datenverkehr für die Analyse durch Security Analytics Malware Analysis erfasst. Security

Analytics verwendet dieses Reihe an Parsern und Feeds, um Ereignisse zu finden, die höchstwahrscheinlich Schadsoftware enthalten.

3. Konfigurieren Sie Kommunikationsports. Security Analytics Malware Analysis erfordert eine Reihe an verschiedenen geöffneten Kommunikationsports, einschließlich TCP/443 für HTTPS. Diese werden im unten stehenden Abschnitt Netzwerkverbindungen beschrieben.
4. Konfigurieren Sie die NextGen-Quelle, mit der Security Analytics Malware Analysis verbunden werden soll. Dies ist der Broker oder Concentrator.
   Security Analytics Malware Analysis ist jetzt bereit für die Analyse des Netzwerk-Datenverkehrs.

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 Security Analytics Malware Analysis-Server zur Überprüfung von Protokolldateien und für Troubleshooting. Der Zugriff kann auf IP-Adressen begrenzt werden, die Security Analytics Malware Analysis verwalten.

- TCP/443 – HTTPS-webbasierte Verbindung für den Zugriff auf die Security Analytics 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 Security Analytics Malware Analysis verwalten.

Ausgehende Verbindungen

- TCP/443 – HTTPS-Verbindungen zu SSL-basierten Webservern. Manche Funktionen ermöglichen es, dass Security Analytics 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 Security Analytics 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. (Security Analytics 10.3 und älter)
- TCP/50105 – REST API-Port für die Kommunikation mit einem Concentrator. (Security Analytics 10.3 und älter)
- TCP/50003 TCP/56003 – Ports für die Kommunikation mit einem Broker. (Security Analytics 10.4 und höher)
- TCP/50005 TCP/56005 – Ports für die Kommunikation mit einem Concentrator. (Security Analytics 10.4 und höher)
- ICMP – JMS-Verbindung zwischen Security Analytics 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

Dieses Thema enthält Anweisungen zum Hinzufügen eines Malware Analysis-Hosts und -Services zu Security Analytics. Ihre Security Analytics-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.

- Wenn sich Malware Analysis ebenfalls auf dem Security Analytics-Server befindet, ist der Security Analytics-Server bereits als Host hinzugefügt und Sie müssen dem Server nur den Malware Analysis-Service hinzufügen.
- Fügen Sie einen Malware Analysis-Host nur dann hinzu, wenn eine physische oder virtuelle Malware Analysis-Appliance vorhanden ist (der Malware Analysis-Service sich also nicht auf dem Security Analytics-Server befindet).

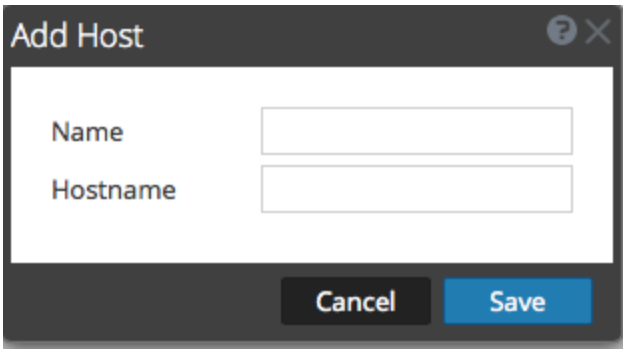
Voraussetzung

Um einen Host und einen Service in Security Analytics hinzuzufügen, muss die Einrichtung der Vorgänge abgeschlossen sein und es muss eine Instanz von Security Analytics installiert sein und ausgeführt werden.

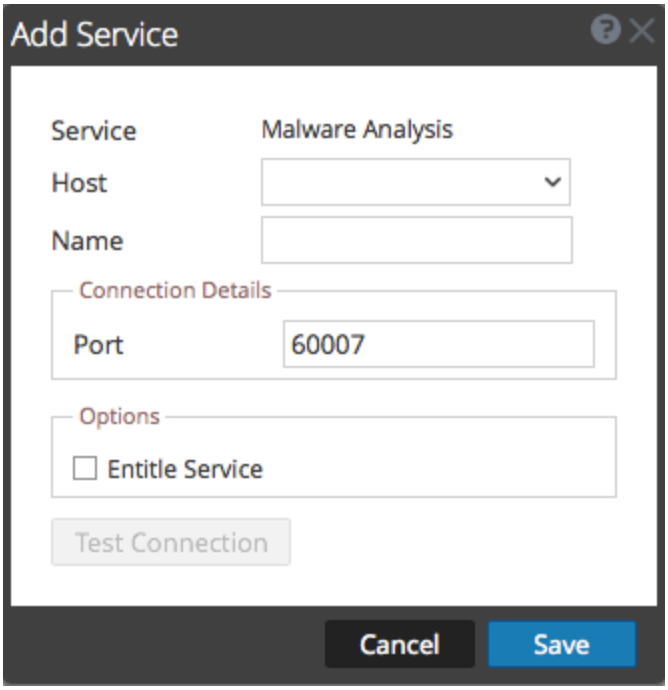
Verfahren

So fügen Sie einen Malware Analysis-Hosts manuell zu Security Analytics hinzu:

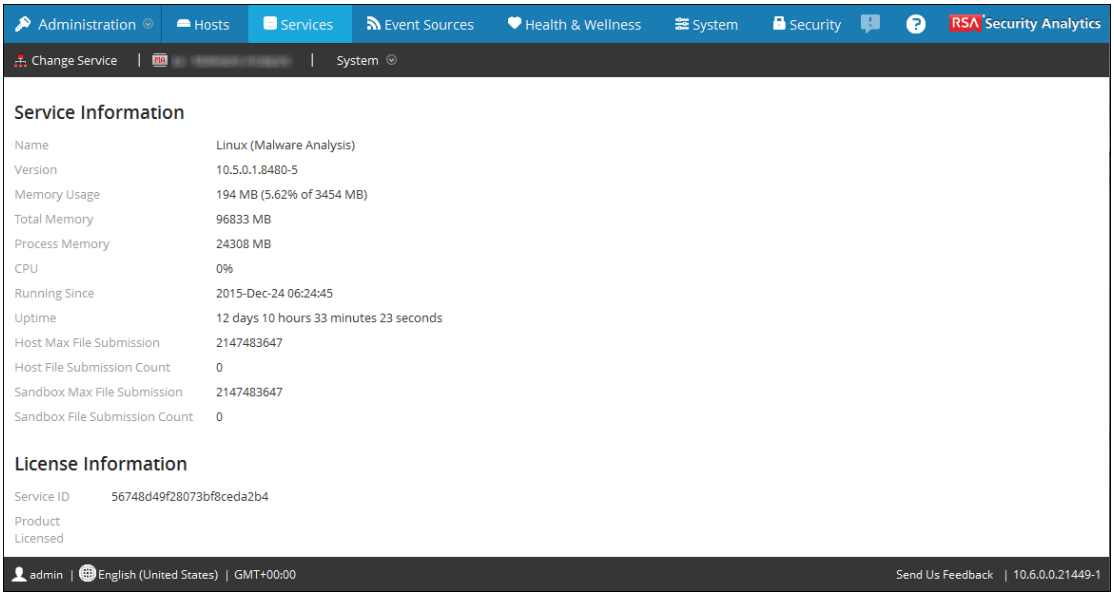
1. Melden Sie sich bei Security Analytics an.
2. Wählen Sie im Menü „Security Analytics“ die Optionen **Administration > Hosts** aus.
   Die Ansicht „Administration“ > „Hosts“ wird angezeigt.
3. Klicken Sie in der Symbolleiste des Bereichs „Hosts“ auf +.
   Das Dialogfeld Host hinzufügen wird angezeigt.



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 **Save**.
5. Wählen Sie im Menü „Security Analytics“ die Option **Services** aus.
6. Klicken Sie in der Symbolleiste des Bereichs **Services** auf + und in der daraufhin angezeigten Drop-down-Liste mit verfügbaren Services auf **Malware Analysis**.
   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 automatisch berechtigen** aus.
8. Klicken Sie auf **Verbindung testen**.
   Während der Service hinzugefügt wird, sendet Security Analytics 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 ist für Security Analytics verfügbar.
10. (Optional) Überprüfen Sie den Status des Malware Analysis-Service. Wählen Sie in der Ansicht „Administration“ > „Services“ den Malware Analysis-Service und dann > **Ansicht > System** aus. Es folgt ein Beispiel der verfügbaren Informationen für einen Malware Analysis-Service.



11. 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

In diesem Thema werden die grundlegenden Konfigurationseinstellungen für den Security Analytics Malware Analysis-Service vorgestellt. Verschiedene Grundeinstellungen sind erforderlich, um die Verarbeitung von Sitzungen, den manuellen Dateiupload und die verschiedenen Bewertungsmodule, die Security Analytics Malware Analysis zum Analysieren von Daten nutzt, zu aktivieren und zu kalibrieren. Sie können außerdem die Dateifreigabe im Daten-Repository einrichten.

Security Analytics 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 Security Analytics Core-Services**: Sie können eine kontinuierliche Abfrage des Security Analytics Core-Services aktivieren und konfigurieren. Ist dies aktiviert und konfiguriert, fragt Malware Analysis den Security Analytics 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.

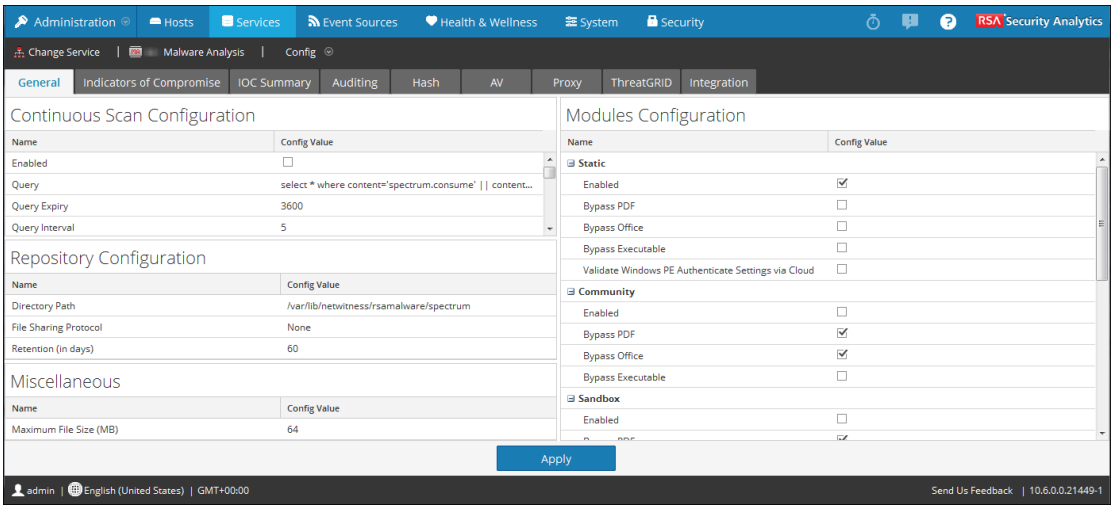
- **Analyse des Security Analytics Core-Services nach Bedarf:** Sie können Sitzungen basierend auf Ermittlungen analysieren, die direkt in Security Analytics initiiert wurden. Diese Methode ermöglicht eine manuell gesteuerte Verarbeitung von Security Analytics Core-Sitzungen sowie eine stärkere Kontrolle 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 Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie im Raster **Services** einen Malware Analysis-Service und die Optionen > **Ansicht > Konfiguration** aus.
   Die Ansicht „Service-Konfiguration“ für den Service wird mit geöffneter Registerkarte **Allgemein** angezeigt.



Konfigurieren der kontinuierlichen Abfrage

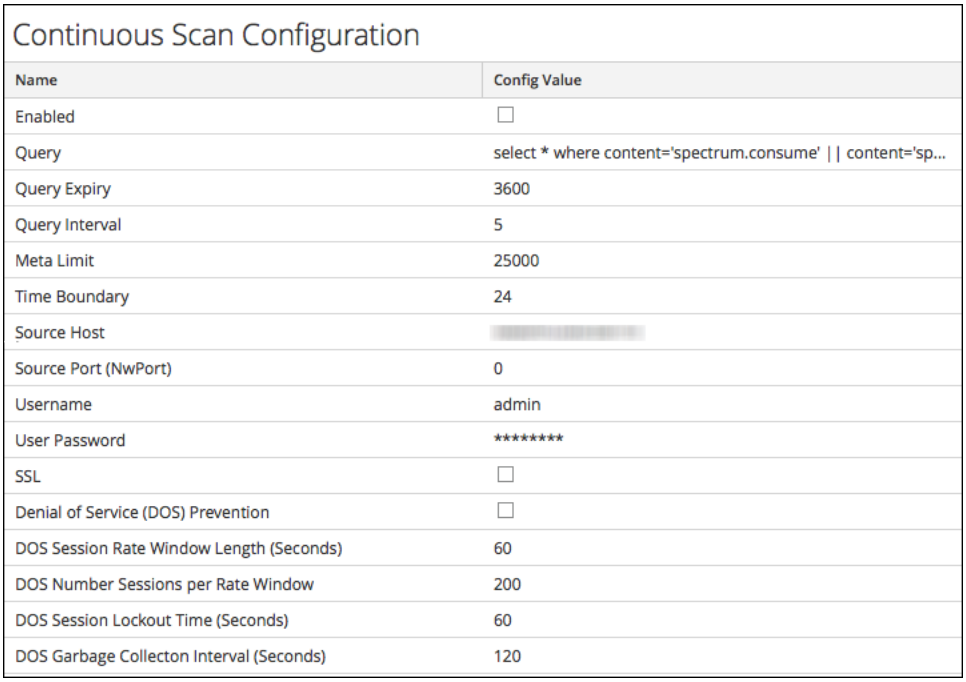
Die Übertragungsrate von Security Analytics Malware Analysis ist beschränkt, sodass maximal 1.000 Dateien pro Tag zur Sandbox-Bearbeitung an die ThreatGrid-Cloud gesendet werden können. Um Ihre Nutzung der Sandbox zu optimieren, können Sie in der Malware Analysis-Konfiguration angeben, welche Verarbeitungsmethode Security Analytics 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 Prävention von Denial of Service (DOS)-Angriffen. 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.



Continuous Scan Configuration

Name	Config Value
Enabled	☐
Query	select * where content='spectrum.consume' || content='sp...
Query Expiry	3600
Query Interval	5
Meta Limit	25000
Time Boundary	24
Source Host	
Source Port (NwPort)	0
Username	admin
User Password	********
SSL	☐
Denial of Service (DOS) Prevention	☐
DOS Session Rate Window Length (Seconds)	60
DOS Number Sessions per Rate Window	200
DOS Session Lockout Time (Seconds)	60
DOS Garbage Collecton Interval (Seconds)	120

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

1. Klicken Sie zum Aktivieren der kontinuierlichen Abfrage auf **Aktivieren**.

2. (Optional) Wenn Sie die Standardwerte für die Abfrage ändern möchten, geben Sie neue Werte für **Ablaufzeit der Abfrage**, **Abfrageintervall**, **Metadatenbegrenzung** und **Zeitgrenze** ein.
3. Zur Konfiguration der Malware Analysis-Appliance, die von Security Analytics Malware Analysis abgefragt wird, um Daten für die Analyse abzurufen, geben Sie **Quellhost** und **Quellport** an.
4. (Optional) Wenn Sie die standardmäßigen Anmeldeinformationen für die Malware Analysis-Appliance ändern möchten, geben Sie den **Benutzernamen** und das **Benutzerpasswort** an.
5. Wenn Sie für die Kommunikation zwischen der Malware Analysis-Appliance und dem Security Analytics Core-Service SSL nutzen möchten, müssen Sie die Option **SSL** aktivieren.
6. (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 Security Analytics das In-Memory-Objekt für die IP-Quelle entfernt. Der Standardwert ist 120 Sekunden.

7. Klicken Sie auf **Anwenden**.
   Die Änderungen werden sofort wirksam, sobald Security Analytics Malware Analysis neue Pakete empfängt.
8. Testen Sie die Verbindung des Malware Analysis-Services 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.

Miscellaneous

Name	Config Value
Maximum File Size (MB)	64

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

Konfigurieren des Daten-Repository

Security Analytics 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 Security Analytics 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.

Repository Configuration

Name	Config Value
Directory Path	/var/lib/netwitness/rsamalware/spectrum
File Sharing Protocol	None
Retention (in days)	60

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 Security Analytics-Benutzeroberfläche sind folgende:

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

Zum Konfigurieren der Dateifreigabe gehen Sie im Abschnitt „Daten-Repository“ wie folgt vor:

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

Die Änderungen werden sofort wirksam.

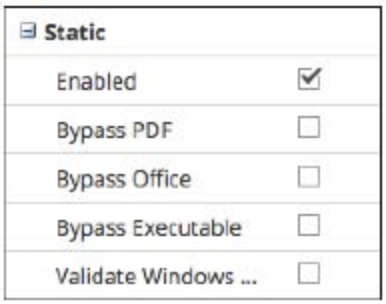
Kalibrieren von Bewertungsmodulen

Im Abschnitt „Modulkonfiguration“ können Sie Security Analytics Malware Analysis wie folgt konfigurieren:

- 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.
- Security Analytics 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. In diesem Fall ist es jedoch günstiger, in den Security Analytics Core-Einstellungen festzulegen, dass diese Dateien ignoriert werden sollen, sodass sie gar nicht erst zur Verarbeitung durch Security Analytics Malware Analysis 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

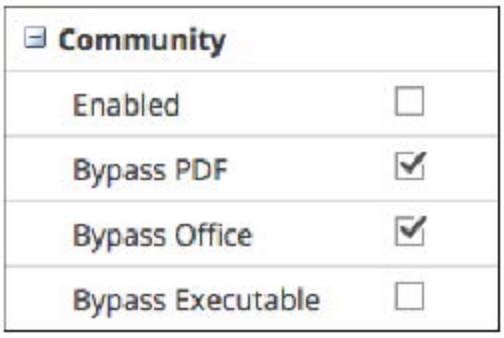


Zum Konfigurieren der statischen Analysebewertung gehen Sie im Abschnitt **Modulkonfiguration** wie folgt vor:

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 Security Analytics 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 ein 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 bei Bedarf die Kontrollkästchen **PDF umgehen**, **Office umgehen, Ausführbare Datei umgehen**.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern und sofort anzuwenden, wenn Security Analytics Malware Analysis neue Pakete empfängt.

Konfigurieren der Sandbox-Analysebewertung

Standardmäßig ist das Sandbox-Modul deaktiviert und MS Office- und 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.

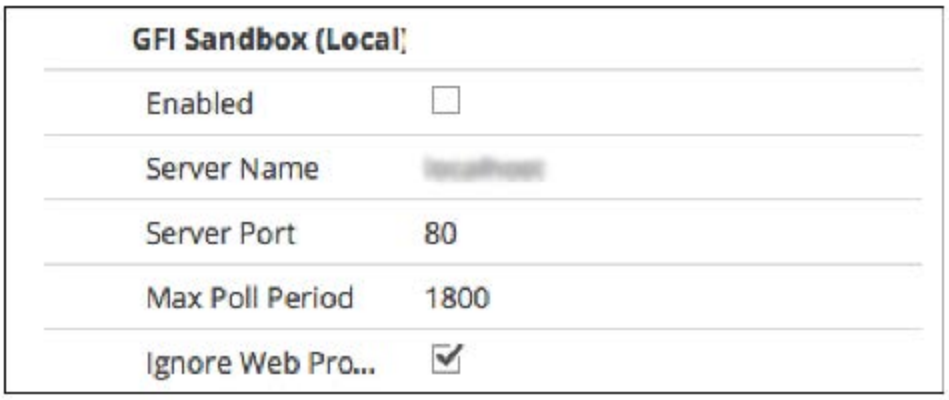
Außerdem können Sie angeben, dass der ursprüngliche Dateiname bei der Sandbox-Analyse beibehalten werden soll.

Hinweis: Wenn Sie den Parameter **Ursprünglichen Dateinamen beim Ausführen der Sandbox-Analyse beibehalten** nicht aktivieren, weist Security Analytics 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

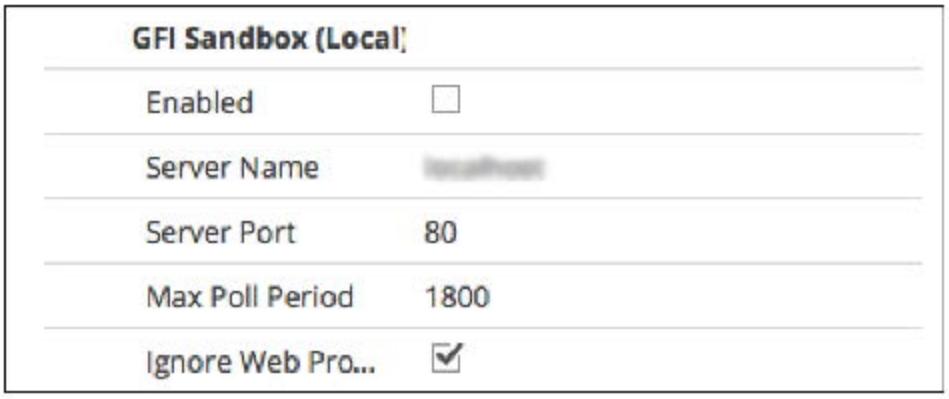
Um eine lokal installierte GFI-Sandbox zu verwenden, müssen Sie GFI aktivieren und den Servernamen und Serverport des GFI-Sandboxservers angeben. Mit den Angaben unter „Max. Polling-Dauer“ und „Polling-Intervall“ wird angegeben, wie lange die Verarbeitungszeit für eine übermittelte Stichprobe sein darf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



Zum Konfigurieren der Sandbox-Bewertung gehen Sie im Abschnitt „Modulkonfiguration“ wie folgt vor:

1. Zum Aktivieren oder Deaktivieren der Sandbox-Analyse klicken Sie auf das Kontrollkästchen **Aktiviert**. Der Standardwert ist **Deaktiviert**.

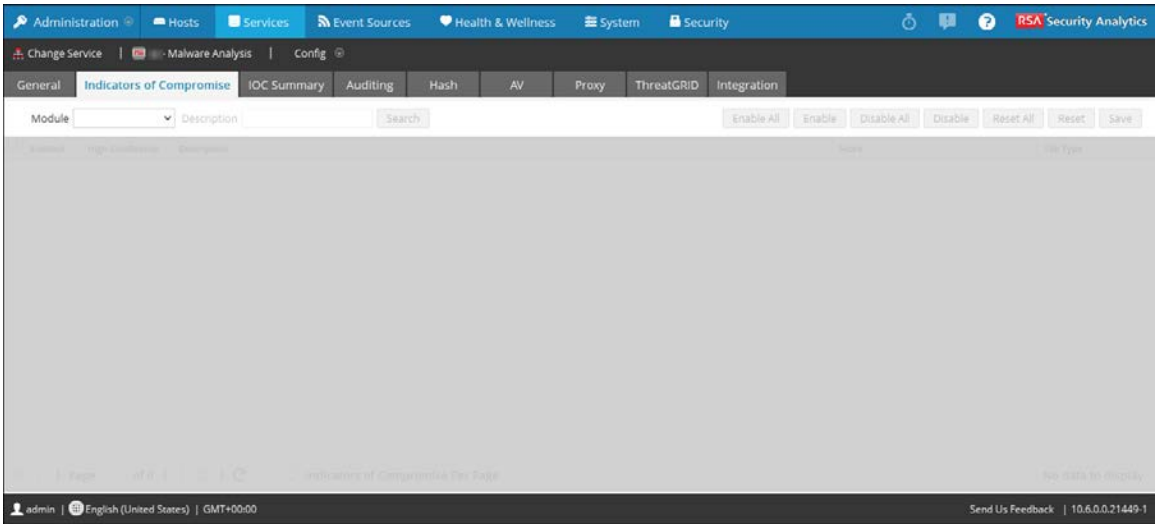
2. Um die Verarbeitung von PDF-, Microsoft Office- und Windows PE-Dateien in einer Sitzung zu konfigurieren, aktivieren Sie bei Bedarf die Kontrollkästchen **PDF umgehen**, **Office umgehen, Ausführbare Datei umgehen**.
3. Konfigurieren Sie den aktiven Sandbox-Anbieter. Sie haben drei Möglichkeiten:
   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

Dieses Thema ist eine Einführung in die Konfiguration der Indikatoren für eine Infizierung (IOC) der Security Analytics Malware Analysis-Bewertungsmodule. Jedes Security Analytics Malware Analysis-Bewertungsmodul – Netzwerk, Statisch, Community, Sandbox und YARA – hat eine Standardeinstellung für die IOCs (Indicators of Compromise, Indikatoren für eine Infizierung), welche 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 Security Analytics Malware Analysis finden Sie in der Ansicht „Service-Konfiguration“ > 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. Security Analytics Malware Analysis schwächt diesen Wert basierend auf dem Prozentsatz des primären AV-Anbieters ab, der 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 Security Analytics 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 Security Analytics Malware Analysis in dieser sehr eingeschränkten Konfiguration können Sie Ergebnisse in Security Analytics 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.

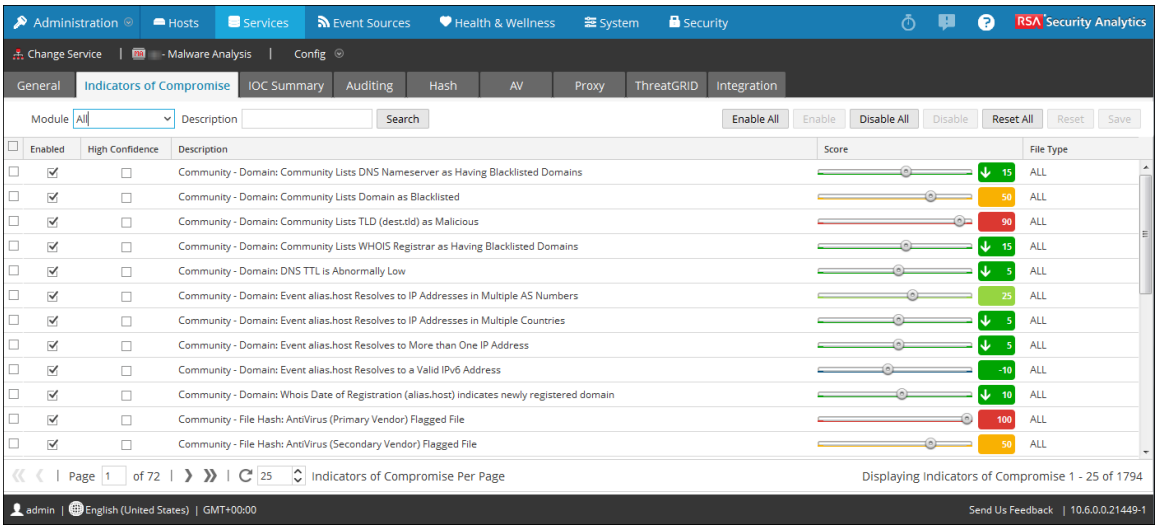
Filtern der angezeigten IOCs nach Modul

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 Menü **Security Analytics** die Optionen Administration **Services> aus.**
2. Wählen Sie einen Malware Analysis Service.
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 Menü **Security Analytics** die Optionen Administration **Services> aus.**
2. Wählen Sie einen Malware Analysis-Service und wählen Sie 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 Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis Service.
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. Beispiel: **Community – Datei-Hash: 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 hochvertrauenswürdig können Sie einen Filter in den Security Analytics 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 Security Analytics-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**.

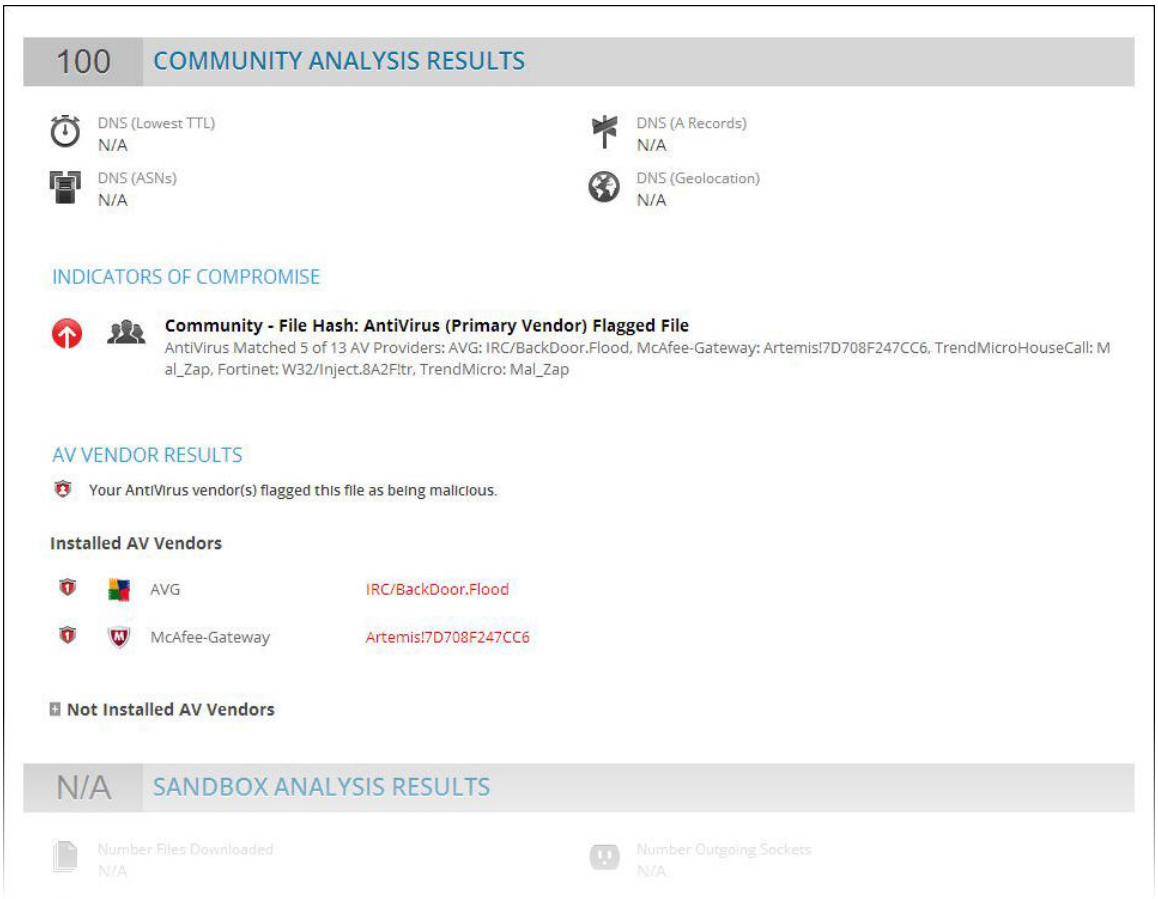
Konfigurieren installierter Virenschutzanbieter

Dieses Thema enthält eine Einführung in eine Funktion von Security Analytics Malware Analysis, die Dateianalyseergebnisse von Ihren installierten Anbietern von Virenschutz (AV) mit Community-Ergebnissen aus der Security Analytics Malware Analysis-Wissensdatenbank vergleicht. Darüber hinaus sind Anweisungen für die Konfiguration der Funktion enthalten. Security Analytics Malware Analysis überprüft eine Antivirus-Wissensdatenbank, um festzustellen, ob die Stichprobe bereits als schädlich bekannt ist. Wenn die Datei als schädlich bekannt ist, markiert Security Analytics die Datei, um anzuzeigen, ob ein primärer oder ein sekundärer Virenschutzanbieter die Stichprobe identifiziert hat. Security Analytics stuft Anbieter als primär oder sekundär ein, um den Reputationsgrad anzuzeigen, den die Anbieter in der Branche haben, und Indikatoren für eine Infizierung berücksichtigen die Reputation bei der Auswertung. 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 Security Analytics-Liste mit primären Anbietern auswählen.

Sie können die in Ihrem Netzwerk installierten Virenschutzanbieter Security Analytics gegenüber identifizieren. Security Analytics vergleicht die Virenschutzergebnisse während der Communityanalyse mit den Ergebnissen der installierten Anbieter, die auf der Registerkarte „AV“ 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 Security Analytics 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.

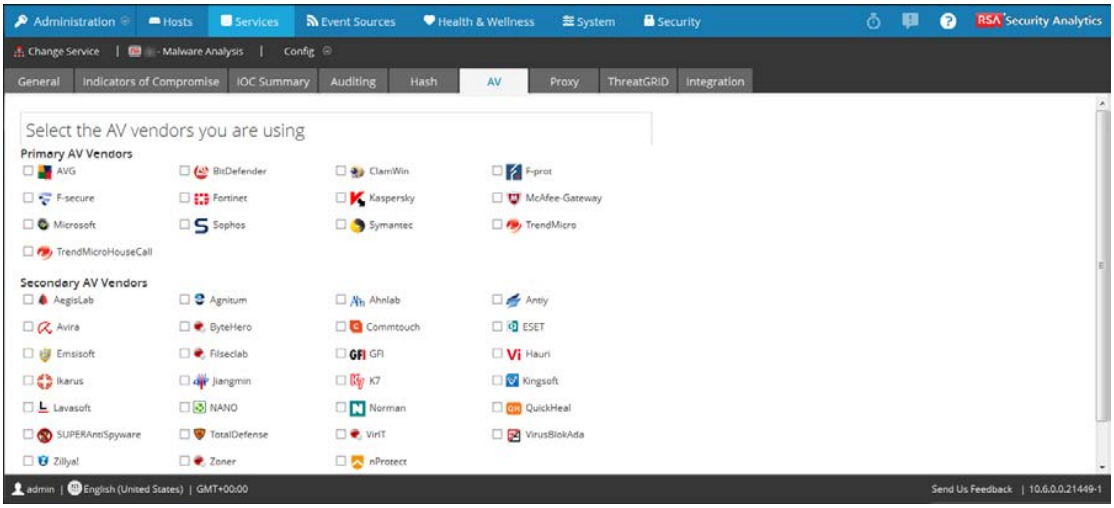


Identifizieren installierter Virenschutzsoftware

So identifizieren Sie in Ihrem Netzwerk installierte Virenschutzsoftware:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und wählen Sie 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 Community-Analyseergebnisse 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**.

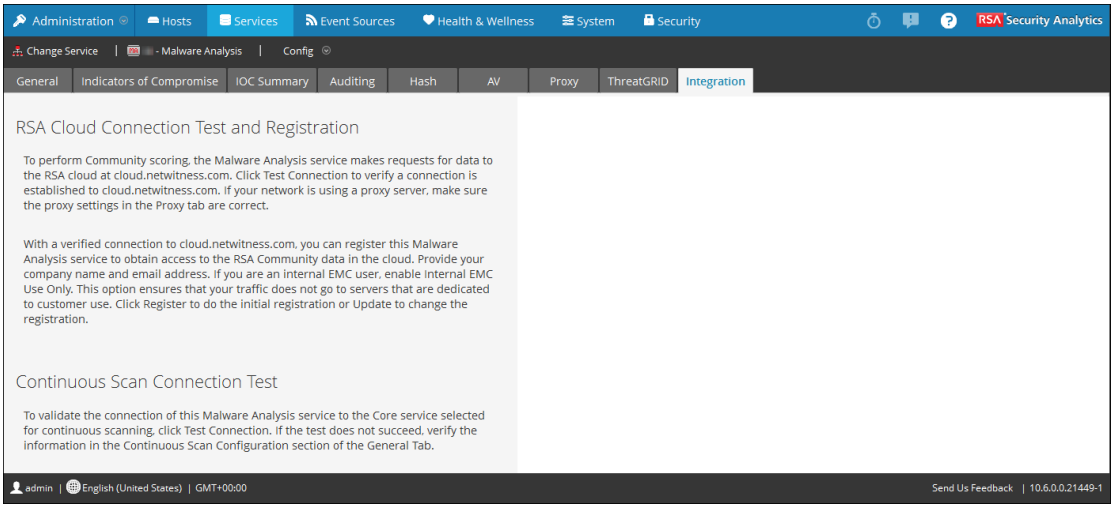
Aktivieren der Communityanalyse

Dieses Thema enthält Anweisungen für Administratoren zum aktivieren der Communityanalyse. Bei der Communityanalyse wird neue im Netzwerk entdeckte Schadsoftware in die RSA-Cloud übertragen, um sie anhand der Schadsoftware-Analysedaten von RSA 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 Menü **Security Analytics** die Optionen Administration **Services> aus.**
2. Wählen Sie einen Malware Analysis-Service und wählen Sie 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**.
   Security Analytics 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.
   Security Analytics initiiert eine Überprüfung basierend auf den Angaben unter „Quellhost“, „Quellport“, „Benutzername“ und „Benutzerpasswort“ auf der Registerkarte „Allgemein“. Wenn der Test erfolgreich ausgeführt wird, können Analysten die Community-Bewertungen in Malware Analysis sehen.

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

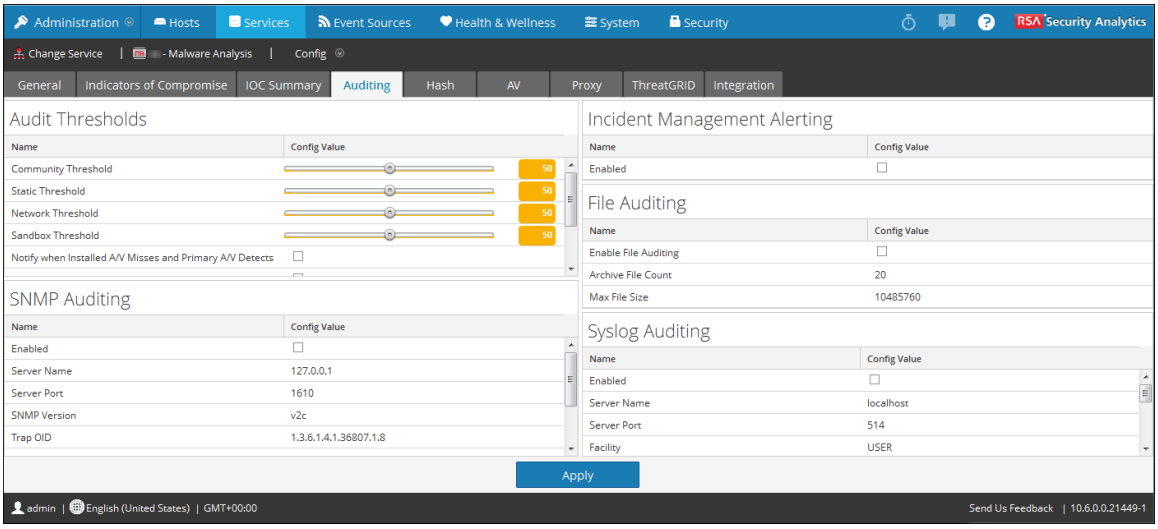
In diesem Thema werden die konfigurierbaren Funktionen des Auditing-Protokolls von Security Analytics Malware Analysis eingeführt und Verfahren zur Konfiguration der Funktionen erläutert. Security Analytics Malware Analysis kann basierend auf konfigurierten Bewertungsmodulschwellenwerten Auditingwarnmeldungen 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 Security Analytics Malware Analysis befinden sich unter Registerkarte „Auditing“ > Ansicht „Service-Konfiguration“.



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 Menü **Security Analytics** die Optionen Administration **Services> aus.**
2. Wählen Sie einen Malware Analysis-Service und dann **> 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 Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann > **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“ aus 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 Security Analytics 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 Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie eine Malware Analysis-Service und dann > **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 Security Analytics 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 Security Analytics Malware Analysis hinterlegt. Der Standardspeicherort für diese Protokolldatei ist `/var/lib/netwitness/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, die maximale Dateigröße und Archivdateianzahl zu hoch einzustellen, da dadurch der verfügbare Festplattenspeicher auf der Security Analytics Malware Analysis-Appliance beeinträchtigt werden kann.

So konfigurieren Sie die Dateiaudit-Einstellungen:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann  **> 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 Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann  **> 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.
   Für das CEF-Format finden Sie unter Erstellen angepasster Warnmeldungen im CEF-Format weitere Überlegungen.

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 Security Analytics 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 Security Analytics 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:

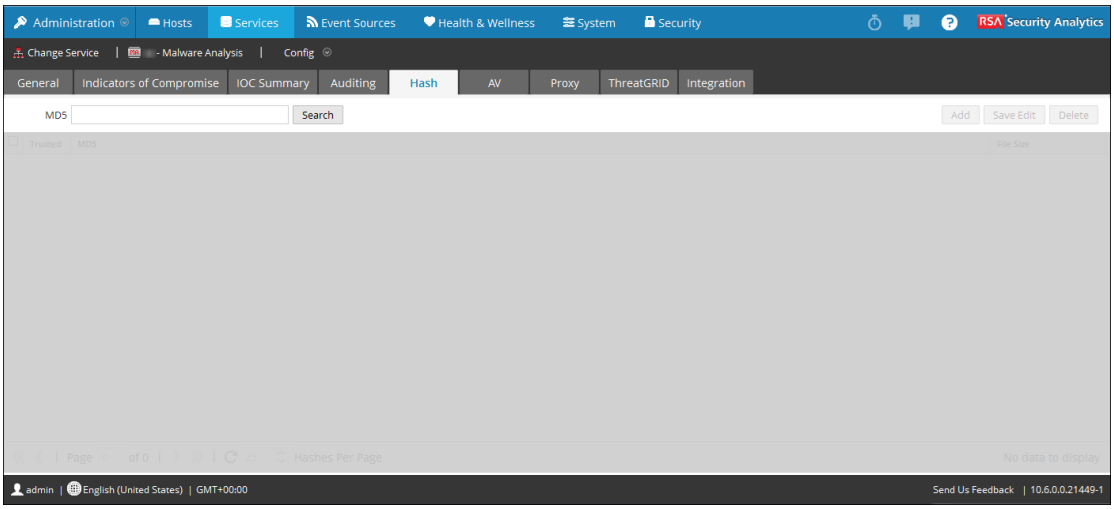
1. Hinzufügen mithilfe des Kontextmenüs in der Ereignisdetailansicht: Wenn Sie mit der rechten Maustaste auf eine Datei klicken, wird ein Kontextmenü geöffnet und Sie können den Hash der ausgewählten Datei als sauber (Normal) oder als fehlerhaft (Schädlich) markieren.
2. Symbolleiste der Registerkarte „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 Security Analytics Malware Analysis Hash-Filter hinzuzufügen, indem Sie 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/lib/rsamalware/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:

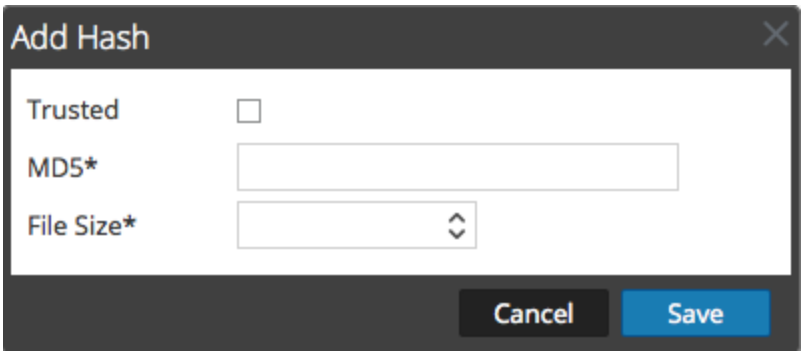
1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie in der Ansicht „Services“ einen Malware Analysis-Service und dann die Optionen  **> Ansicht > Konfiguration** aus.
3. Wählen Sie die Registerkarte **Hash** aus.
   Die Hash-Liste wird in der Registerkarte „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 **Save**
   Der Datei-Hash wird den Hashes hinzugefügt und für das Hash-Filtern in Security Analytics 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 länger für das Hash-Filtern in Security Analytics 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 Feld „MD5“ den Datei-Hash ein, den Sie suchen, und klicken Sie auf **Suchen**. Die 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/lib/rsamalware/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 Security Analytics 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.HashFi
leWatch - Processing -
/var/lib/rsamalware/hashWatch/test.csv
 2013-08-09 09:47:56,619 [jobExecutor-2
(HashFileWatch)] INFO
com.netwitness.malware.core.services.file.hash.Ha
shServiceImpl - Skipped 21 Duplicate Hashes
Already on File
 2013-08-09 09:48:06,638 [jobExecutor-2
(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFi
leWatch - Processed -
/var/lib/rsamalware/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 Security Analytics-Konfigurationsdatei (**/var/lib/rsamalware/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</distributedCacheEn
abled>

<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**.

Liniendiagramm	Beschreibung
<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 Security Analytics 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.HashFi
leWatch - 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.HashFi
leWatch - 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.HashFi
leWatch - 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.HashFi
leWatch - 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/lib/rsamalware/spectrum/hashWatch**.
   Security Analytics Malware Analysis beobachtet diesen Ordner automatisch und verarbeitet die hier gespeicherten Dateien.
   Security Analytics Malware Analysis fügt diesem Hash-Filter jeden in der Hash-Liste gefundenen Hash hinzu.
   Wenn Verarbeitungsfehler auftreten, werden diese in **/var/lib/rsamalware/spectrum/hashWatch/error** protokolliert.
   Verarbeitete Dateien werden in **/var/lib/rsamalware/spectrum/hashWatch/processed** katalogisiert.
   Verarbeitete Dateien werden aus dem Verzeichnis hashWatch nicht 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

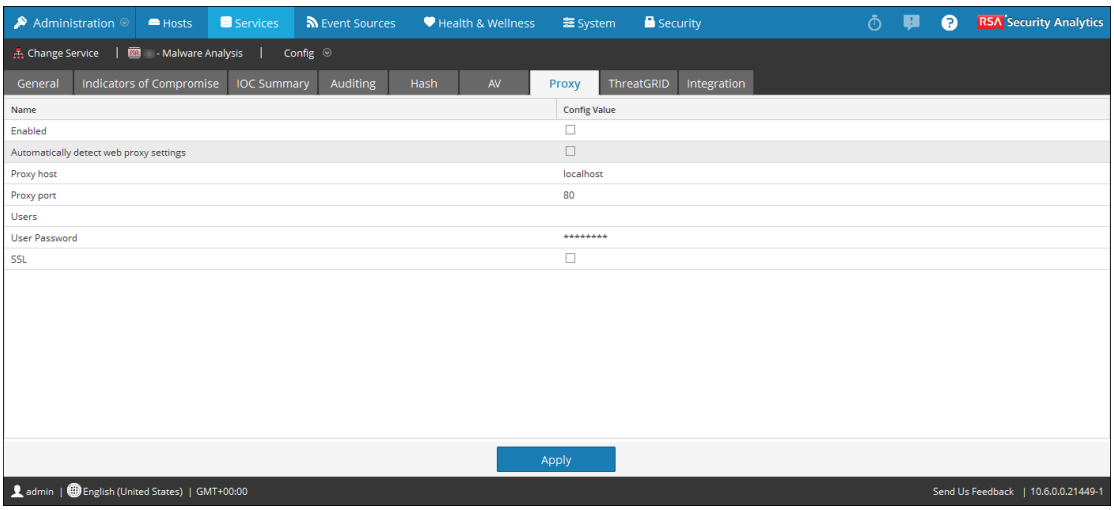
In diesem Thema wird die Konfiguration eines Webproxys für die Kommunikation mit dem RSA-Cloud-Service und dem lokalen ThreatGrid- oder GFI-Service beschrieben. Mit den Einstellungen in der Ansicht „Service-Konfiguration“ > Registerkarte „Proxy“ wird die Kommunikation durch den Webproxy eingerichtet, den Security Analytics 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 Security Analytics Malware Analysis:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann > **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) Um automatisch Proxyeinstellungen für den Security Analytics-Server zu erkennen, aktivieren Sie das Kontrollkästchen.
   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.

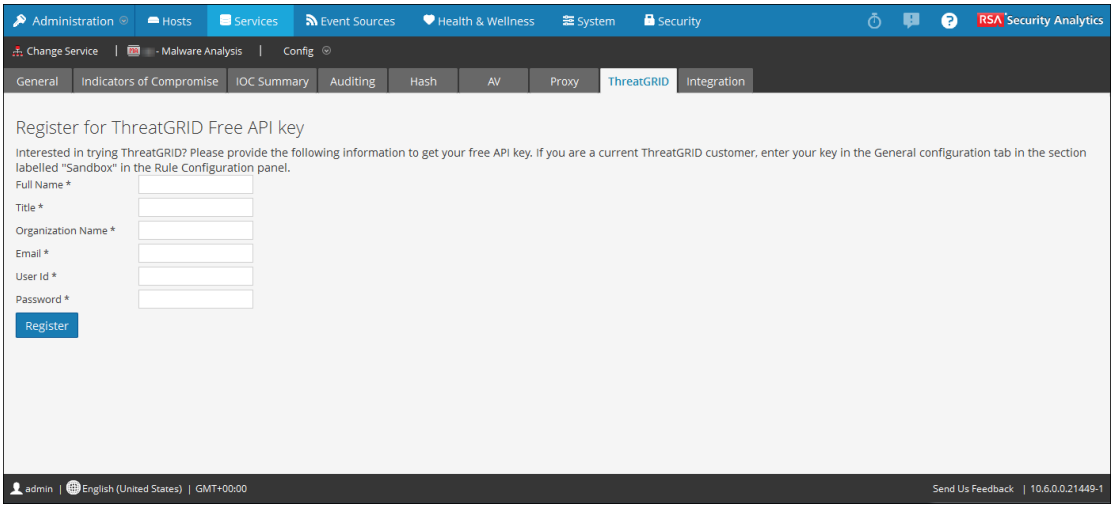
Wenn Sie keinen von ThreatGrid bereitgestellten Serviceschlüssel haben, können Sie mithilfe dieser Registerkarte einen Schlüssel erhalten. Der Schlüssel wird versuchsweise bereitgestellt.

Wenn Sie Ihre Benutzerinformationen eingeben und auf **Registrieren** klicken, wird ein Schlüssel auf dieser Registerkarte angezeigt und automatisch zur ThreatGrid-Konfiguration auf 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 Security Analytics Malware Analysis für die Sandbox-Analyse übertragen werden.

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

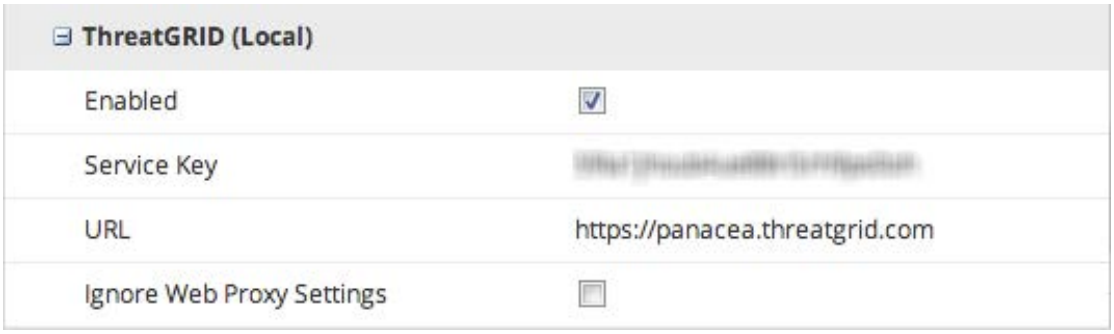
1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Malware Analysis-Service und dann **> Ansicht > Konfiguration** aus.

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. Security Analytics Malware Analysis kann fünf Dateien pro Tag für die Sandbox-Analyse an die ThreatGrid-Cloud senden.

Zusätzliche Verfahren

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
- Aktivieren von angepassten YARA-Inhalten

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/lib/rsamalware/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 Security Analytics 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.
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	Security Analytics Malware Analysis ist das Protokollmodul für das Ereignis.
1.2.1.130	Security Analytics Malware Analysis-Version.
Ereignis-ID 857	Eindeutige Netzwerkereignis-ID für dieses Ereignis
Sitzungs-ID 73	Eindeutige Sitzungs-ID von Security Analytics 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 Security Analytics Malware Analysis-Analysewerte 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

Protokollinformationen	Beispielwert
file.size	0
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

Von NextGen abgerufene Ereignismetadaten

Die Aufzeichnung wird mit Security Analytics 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

Protokollinformationen	Beispielwert
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
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/

Protokollinformationen	Beispielwert
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 unbekannten 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 Security Analytics-Host, auf dem der Malware Analysis-Service installiert ist. Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Security Analytics Malware Analysis YARA-basierte 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 Security Analytics 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 folder 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 Security Analytics-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 `/etc/ld.so.conf`-Datei oder die `LD_LIBRARY_PATH`-Umgebungsvariable 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 Investigation und Malware Analysis* beschrieben.

Ressourcen für Malware Analysis

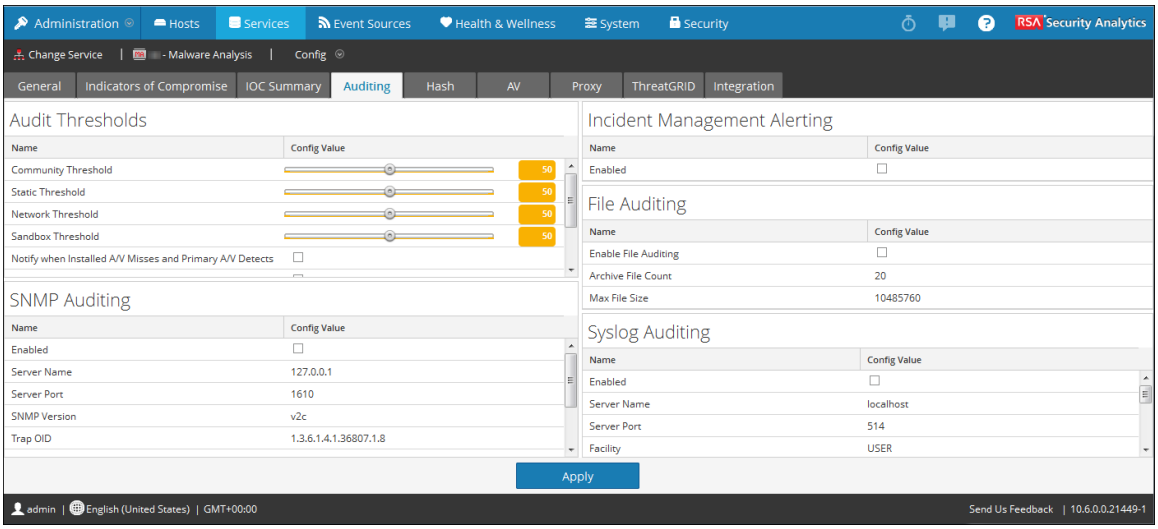
- Ansicht „Service-Konfiguration“ – Registerkarte „Auditing“
- Ansicht „Service-Konfiguration“ – Registerkarte „AV“
- Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“
- Ansicht „Service-Konfiguration“ – Registerkarte „Hash“
- Ansicht „Service-Konfiguration“ – Registerkarte „Indikatoren für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

Ansicht „Service-Konfiguration“ – Registerkarte „Auditing“

Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „Auditing“ in der Ansicht „Services“ > „Konfiguration“ für Security Analytics Malware Analysis. Mit der Registerkarte „Auditing“ in der Ansicht „Service-Konfiguration“ für Security Analytics Malware Analysis können Sie die Auditing-Funktion konfigurieren. Malware Analysis verfügt über ein automatisiertes Auditing-System, das Warnmeldungen versenden kann (syslog, snmp, Auditprotokolldateieinträge), wenn Malware Analysis konfigurierte Schwellenwerte des jeweiligen Bewertungsmoduls (Netzwerk, Static, Community, Sandbox) überschreitet. Security Analytics Malware Analysis kann automatisch Meldungen an jedes externe System senden, das die unterstützten Auditformate aufnehmen kann. Eine Warnmeldung wird für jede Datei in einer analysierten Sitzung erzeugt, die den konfigurierten Schwellenwert erreicht oder überschreitet.
Das Auditprotokoll ist eine Protokolldatei, die auf der Malware Analysis-Appliance für alle signifikanten Ereignisse oder Aktionen geführt wird. Die Auditprotokolle werden implementiert und über die Zeit archiviert, wenn sie größer werden, sodass ein Auditverlauf gepflegt wird. Sowohl die Größe als auch die Anzahl dieser Auditprotokolle sind konfigurierbar.
Einige Beispiele für Ereignisse, die protokolliert werden, sind:

- Erfolgreiche und fehlgeschlagene Benutzeranmeldungen
- Änderungen an den Systemkonfigurationseinstellungen
- Serverneustart
- Upgrade und Installation von Serverversionen
- Verdächtige Ereignisse, die die Auditschwellenwerte überschreiten

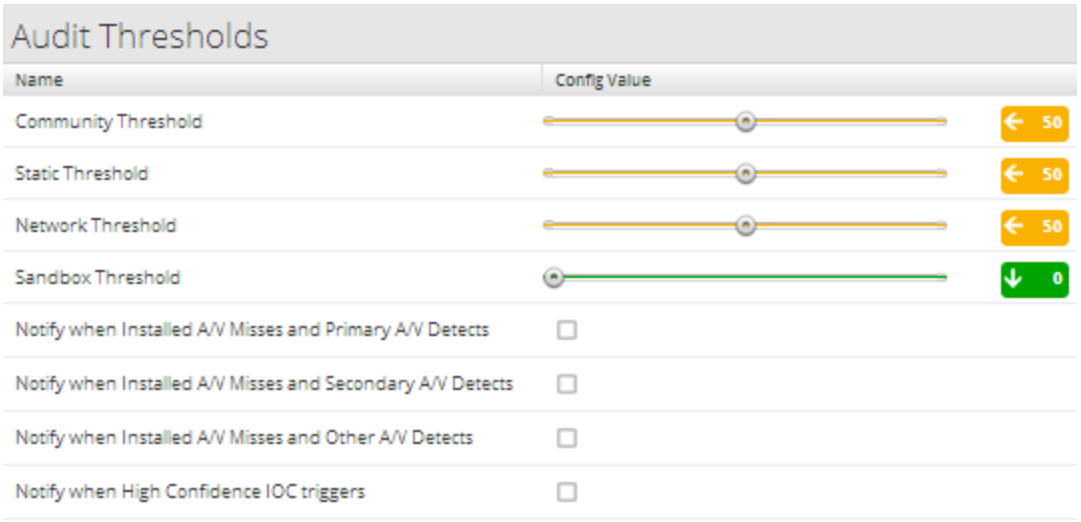
Security Analytics Malware Analysis kann Auditereignisse als SNMP-Trap an einen konfigurierten SNMP-Trap-Host senden und Protokolle im Syslog-Format konsolidieren. Detaillierte Verfahren finden Sie im folgenden Aufgabenthema: Konfigurieren des Auditing auf der Malware Analysis-Appliance



Funktionen

Die Registerkarte Auditing umfasst vier Abschnitte und eine Schaltfläche Anwenden, die dazu dient, Änderungen in dieser Registerkarte zu speichern und in Kraft treten zu lassen.

Auditschwellenwerte



In dieser Tabelle werden die Funktionen im Abschnitt Auditschwellenwerte beschrieben.

Name	Konfigurationswert

Name	Konfigurationswert
Schwellenwerte für **Community**, **Static**, **Netzwerk** und **Sandbox**	Malware Analysis-Bewertungsmodul-Schwellenwerte für die Aufnahme von Ereignisinformationen in einer Protokolldatei Security Analytics Malware Analysis nimmt die Ereignisinformationen in einer Protokolldatei auf, wenn das Ereignis hoch genug klassifiziert wurde, um alle Auditschwellenwerte zu erfüllen. Jede Auswertungskategorie, die die Analyse abgeschlossen hat (zum Beispiel rufen nicht alle Sitzungen die Sandbox-Analyse auf), wird mit dem konfigurierten Auditschwellenwert für diese Kategorie verglichen. Alle abgeschlossenen Kategorien müssen den Schwellenwert übertreffen, damit ein Auditereignis ausgelöst wird. Eine Ganzzahl zwischen 0 und 100 ist ein gültiger Wert. Wenn diese Schwellenwerte zu niedrig eingestellt werden, kann es zu einer sehr großen Anzahl von Auditereignissen und -benachrichtigungen kommen.
Benachrichtigen, wenn die installierte AV-Lösung einen Fehler übersieht und die primäre AV-Lösung diesen erkennt	Zeichnet eine Meldung in einer Protokolldatei auf, wenn die installierte Virenschutzsoftware einen Virus übersieht und die primäre Virenschutzsoftware diesen Virus erkennt. Die aufgezeichnete Nachricht wird über alle aktivierten Auditing-Methoden gesendet: SNMP, Datei und Syslog. Der Standardwert ist deaktiviert.
Benachrichtigen, wenn die installierte AV-Lösung einen Fehler übersieht und die sekundäre AV-Lösung diesen erkennt	Zeichnet eine Meldung in einer Protokolldatei auf, wenn die installierte Virenschutzsoftware einen Virus übersieht und die sekundäre Virenschutzsoftware diesen Virus erkennt. Die aufgezeichnete Nachricht wird über alle aktivierten Auditing-Methoden gesendet: SNMP, Datei und Syslog. Der Standardwert ist deaktiviert.

Name	Konfigurationswert
Benachrichtigen, wenn die installierte AV-Lösung einen Fehler übersieht und eine andere AV-Lösung diesen erkennt	Zeichnet eine Meldung in einer Protokolldatei auf, wenn die installierte Virenschutzsoftware einen Virus übersieht und die andere Virenschutzsoftware diesen Virus erkennt. Die aufgezeichnete Nachricht wird über alle aktivierten Auditing-Methoden gesendet: SNMP, Datei und Syslog. Der Standardwert ist deaktiviert.
Benachrichtigen, wenn ein Gefährdungsindikator mit hoher Wahrscheinlichkeit ausgelöst wird	Zeichnet diese Meldung in einer Protokolldatei auf, wenn ein Indikator für eine Infizierung mit hoher Wahrscheinlichkeit ausgelöst wird. Die aufgezeichnete Nachricht wird über alle aktivierten Auditing-Methoden gesendet: SNMP, Datei und Syslog. Der Standardwert ist deaktiviert.

SNMP-Auditing

SNMP (Simple Network Management Protocol) ist ein Internetstandardprotokoll zum Managen von Services in IP-Netzwerken. Wenn das SNMP-Auditing aktiviert ist, kann Security Analytics Malware Analysis ein Auditereignis als SNMP-Trap an einen konfigurierten SNMP-Trap-Host senden.

SNMP Auditing

Name	Config Value
Enabled	☐
Server Name	127.0.0.1
Server Port	1610
SNMP Version	2
Trap OID	1.3.6.1.4.1.36807.1.8
Community	public
Number Of Retries	2
Timeout	1500

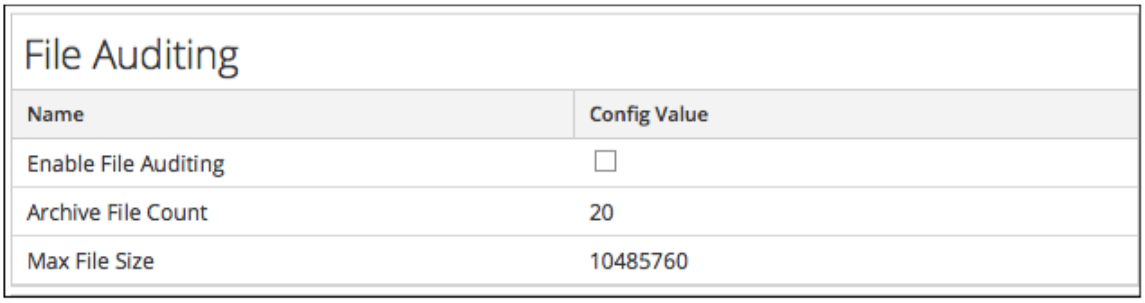
In dieser Tabelle werden die Funktionen im Abschnitt SNMP-Auditing beschrieben.

Name	Konfigurationswert
Aktiviert	Klicken Sie hier, um SNMP-Auditing zu aktivieren oder zu deaktivieren.
Servername	Der Host, auf dem der Ziel-SNMP-Server ausgeführt wird.
Serverport	Der verwendete Port, den der SNMP-Trap-Empfänger überwacht.
SNMP-Version	Die Version des SNMP-Protokolls, die beim Senden von Traps verwendet wird.
Trap-OID	Der Objektbezeichner, der identifiziert, welcher Typ von Trap gesendet wird.
Community	Die SNMP-Gruppe, zu der Security Analytics Malware Analysis gehört.
Anzahl erneuter Versuche	Die Anzahl erneuter Versuche, eine Trap zu senden.
Timeout	Die Timeout-Dauer, die auf Bestätigung gewartet wird.

Incident Management-Auditing

Der Abschnitt „Incident Management-Auditing“ enthält ein Kontrollkästchen, bei dessen Aktivierung Security Analytics Incident Management Warnmeldungen von Malware Analysis empfangen kann. Wenn Sie auf „Aktiviert“ klicken, wird das Syslog-Auditing aktiviert oder deaktiviert.

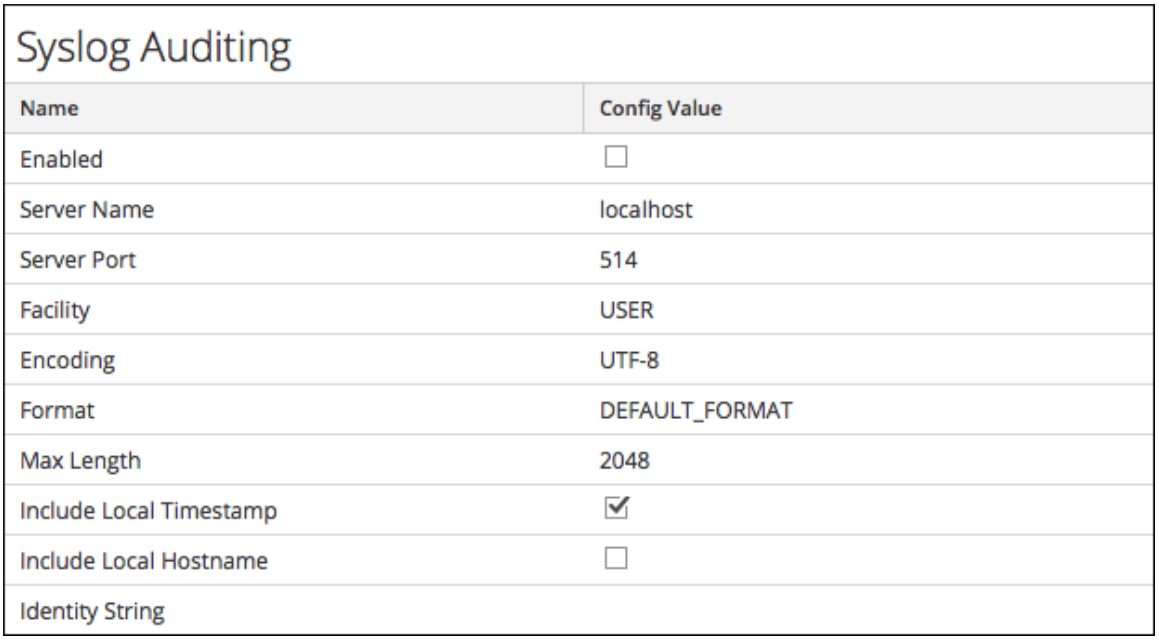
Dateiaudit



In dieser Tabelle werden die Funktionen im Abschnitt Dateiaudit beschrieben. Vermeiden Sie es, die maximale Dateigröße und die Archivdateianzahl zu hoch einzustellen, da dadurch der verfügbare Festplattenspeicher auf der Security Analytics Malware Analysis-Appliance beeinträchtigt werden kann.

Name	Konfigurationswert
Dateiaudit aktivieren	Klicken Sie hier, um Dateiaudit zu aktivieren oder zu deaktivieren.
Anzahl Archivdateien	Security Analytics Malware Analysis behält nur so viele Protokolldateien, wie in dieser Einstellung definiert sind. Wenn die maximale Anzahl erreicht ist, werden die ältesten Protokolldateien gelöscht und können nicht wiederhergestellt werden. Der Standardwert ist 20. Gültiger Wert: Ganze Zahl von 1 bis einschließlich 50
Max. Dateigröße	Die maximale Dateigröße für ein einzelnes Auditprotokoll, bevor es archiviert wird Der Standardwert ist 10485760 Byte.

Syslog-Auditing



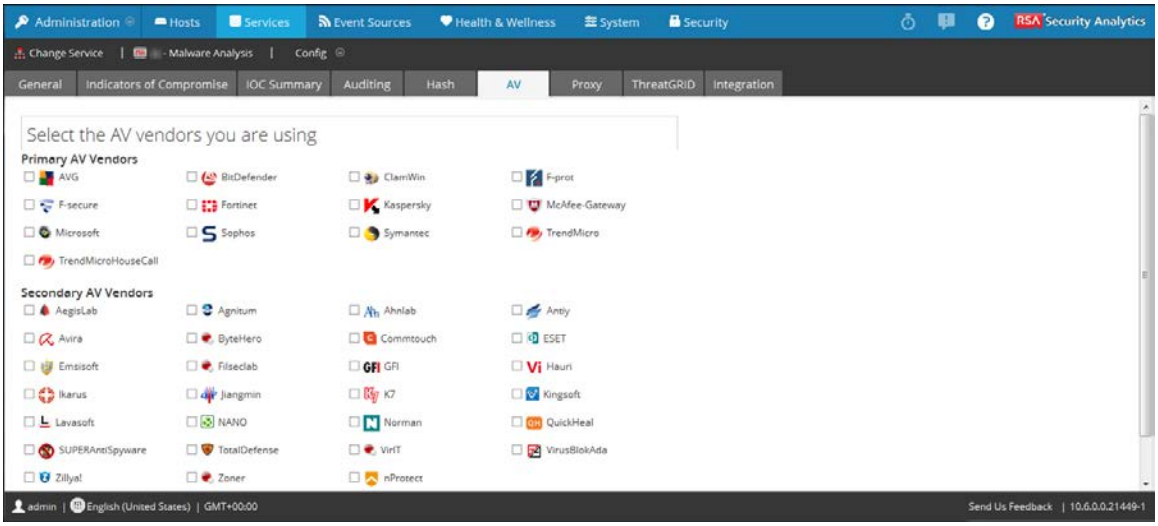
In dieser Tabelle werden die Funktionen im Abschnitt Auditschwellenwerte beschrieben.

Funktion	Beschreibung
Aktiviert	Klicken Sie hier, um Syslog-Auditing zu aktivieren oder zu deaktivieren.
Servername	Dies ist der Host, auf dem der Ziel-Syslog-Prozess ausgeführt wird.
Serverport	Dies ist der Port, den der Ziel-Syslog-Prozess überwacht.
Facility	Dies ist die designierte Syslog-Facility, die für alle ausgehenden Nachrichten verwendet wird. Mögliche Werte sind KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV und LOCAL1 bis LOCAL7.
Codierung	Dies ist die Codierung, die für Text in Syslog-Nachrichten zu verwenden ist; zum Beispiel UTF-8.
Format	Das ist das gewünschte Ausgabeformat. Die möglichen Werte sind: Standard, PCI-DSS oder SEC
Max. Länge	Dies ist die maximal zulässige Länge einer Syslog-Nachricht in Byte. Der Standardwert ist 1024. Nachrichten, die die maximale Länge überschreiten, werden gekürzt.
Lokalen Zeitstempel hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um den lokalen Zeitstempel in Nachrichten hinzuzufügen.
Lokalen Hostnamen hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um den lokalen Hostnamen hinzuzufügen.
Identitätszeichenfolge	Dies ist eine Identitätszeichenfolge, die jeder Syslog-Warnmeldung vorangestellt werden muss. Wenn die Zeichenfolge leer ist, wird den ausgehenden Syslog-Warnmeldungen keine Identitätszeichenfolge vorangestellt. Sie können damit die Quelle der Warnmeldung identifizieren. Benutzer stellen sie herkömmlicherweise auf den Namen des Programms ein, das die Meldungen an ein Syslog-Auditing übermittelt.

Ansicht „Service-Konfiguration“ – Registerkarte „AV“

Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „AV“ der Ansicht „Services“ > „Konfiguration“ für einen Security Analytics Malware Analysis-Service. Über die Registerkarte „AV“ kann der Anbieter der in Ihrem Netzwerk eingesetzten Virenschutzsoftware identifiziert werden. Security Analytics kann die Ergebnisse von diesen Anbietern in der detaillierten Ergebnisansicht eines Ereignisses einschließen, das mithilfe von Security Analytics 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.

Funktion	Beschreibung
Zurücksetzen	Setzt die Liste AV auf den Standardstatus zurück, in dem kein Anbieter ausgewählt ist.

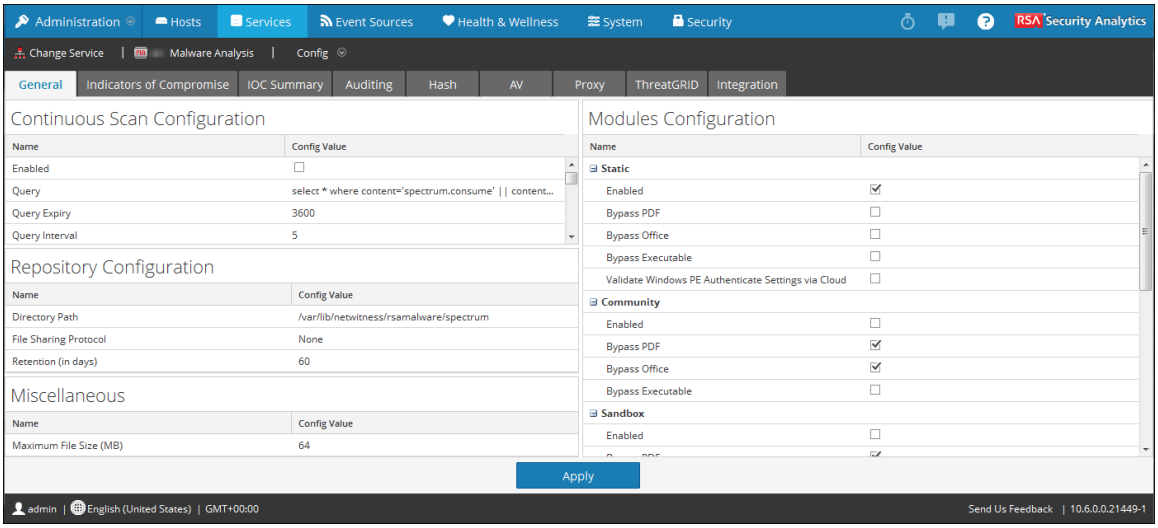
Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“

Dieses Thema bietet eine Einführung in die Konfigurationseinstellungen in der Ansicht „Service-Konfiguration“ > Registerkarte „Allgemein“ für Security Analytics 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.

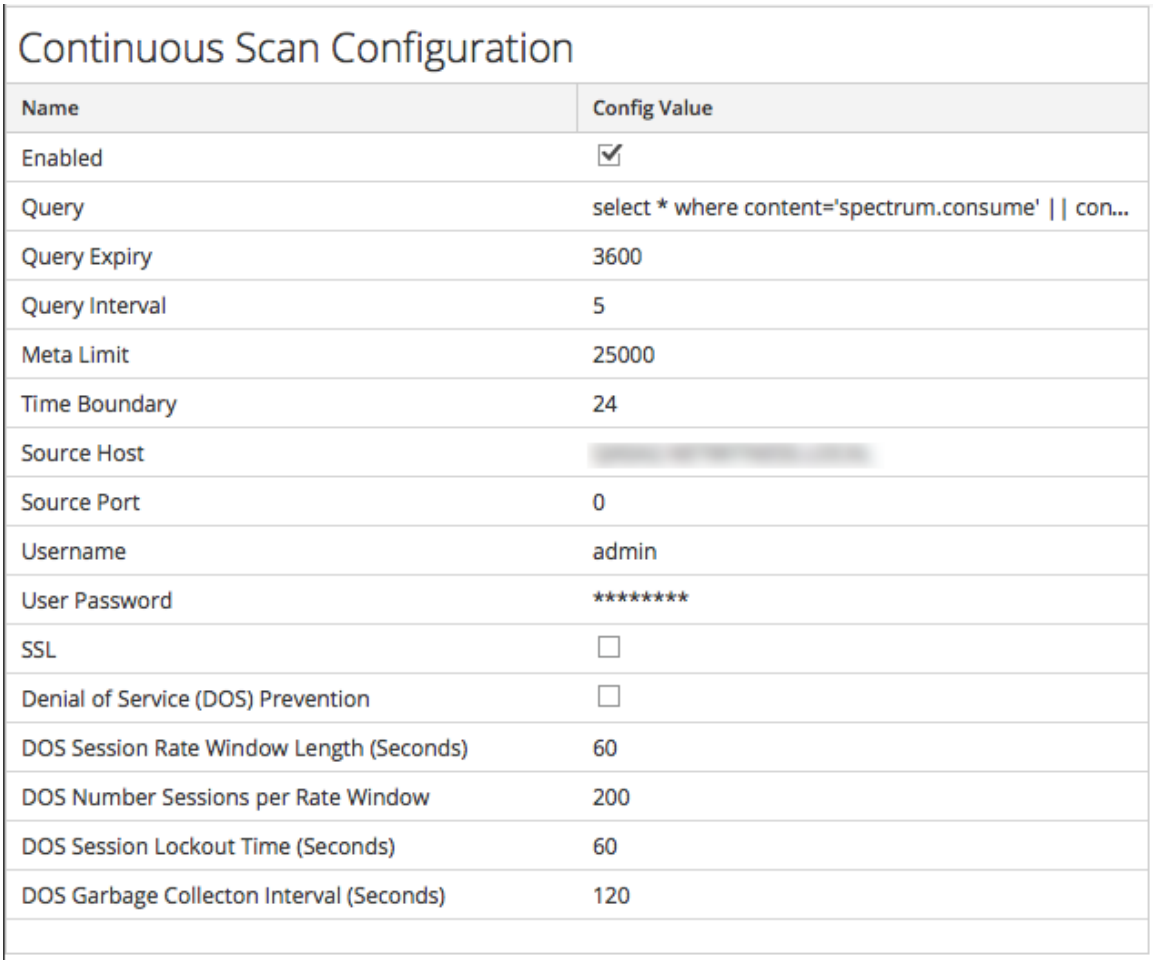
Dies ist ein Beispiel für die Registerkarte „Allgemein“.



Funktionen

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

Abschnitt „Konfiguration des kontinuierlichen Scannens“



Continuous Scan Configuration

Name	Config Value
Enabled	☑
Query	select * where content='spectrum.consume' || con...
Query Expiry	3600
Query Interval	5
Meta Limit	25000
Time Boundary	24
Source Host	[redacted]
Source Port	0
Username	admin
User Password	********
SSL	☐
Denial of Service (DOS) Prevention	☐
DOS Session Rate Window Length (Seconds)	60
DOS Number Sessions per Rate Window	200
DOS Session Lockout Time (Seconds)	60
DOS Garbage Collecton Interval (Seconds)	120

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

Parameter	Beschreibung
Aktiviert	Aktivieren oder Deaktivieren der kontinuierlichen Abfrage des Security Analytics 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 Security Analytics Malware Analysis nur Analysen von Ereignissen durch, die diesen bestimmten 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 Security Analytics Core-Service nach Metadaten abfragt, werden Ergebnisse innerhalb weniger Sekunden zurückgesendet. 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 Security Analytics Core-Service abfragt, werden Metadaten bis zu dieser Metadatenbegrenzung abgerufen. Unter Verwendung dieser Einstellung und in Verbindung mit dem Abfrageintervall kann die Performance von Malware Analysis in der Security Analytics Core-Infrastruktur verbessert werden. 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 Security Analytics Malware Analysis-Appliance. Dies ist die IP-Adresse oder der Hostname des Services, dessen Daten von Malware Analysis zur Analyse abgefragt werden. Verwenden Sie keinen lokalen Host als Quellhost. Je nach Modell der Appliance und der Konfiguration der Security Analytics-Infrastruktur kann dieser Quellhost variieren.
Quellport	Malware Analysis kommuniziert mit der Security Analytics-Infrastruktur unter Verwendung des REST-Services, der diesen Port überwacht. Die Portnummer ist spezifisch für die Art von Security Analytics Core-Service, der als Quellhost verwendet wird. Dies entspricht den ausgehenden Verbindungen Ihres Security Analytics 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 Security Analytics verwendet wird. Es wird jedoch empfohlen, ein neues, für Malware Analysis dediziertes Konto für den Security Analytics Core-Service zu erstellen.

Parameter	Beschreibung
Benutzerpasswort	Benutzerpasswort. Der Standardwert ist **netwitness**.
SSL	Verwenden Sie SSL für die Kommunikation mit Security Analytics 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 zu bestimmen, 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 Länge 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 zu bestimmen, 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 Länge 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 zu bestimmen, wie lange dieser Angriff außer Acht gelassen 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 Länge 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 deaktivieren, um den Verarbeitungsoverhead (auf Kosten der Speichernutzung) zu eliminieren. Der Standardwert ist **120** Sekunden.

Abschnitt „Repository-Konfiguration“

Security Analytics Malware Analysis speichert alle Dateien, die für zukünftige Verwendungen analysiert werden. 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 in der Security Analytics 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 Nutzern den Zugriff auf die gespeicherten Dateien in Security Analytics 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)	Security Analytics Malware Analysis bewahrt Dateien, die im Repository gespeichert sind, einige Tage 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)

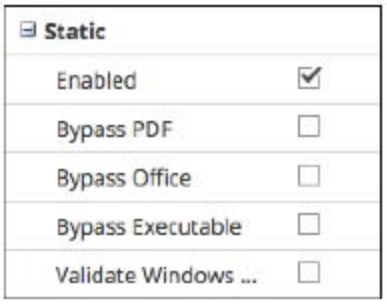
In der Tabelle sind die Funktionen des Konfigurationsabschnitt „Verschiedenes“ beschrieben.

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**. Wenn die maximale Dateigröße überschritten wird, hindert Sie Security Analytics daran, die Datei zu scannen.

Abschnitt „Modulkonfiguration“

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

Konfiguration Statische Analyse

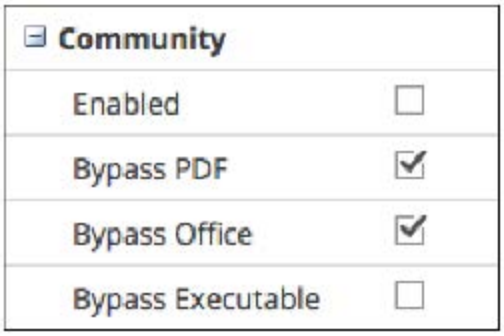


Das statische Modul ist die einzige Bewertungskategorie, die standardmäßig aktiviert ist. Diese Tabelle beschreibt die Parameter für die Konfiguration der statischen Analyse.

Funktion	Beschreibung
Aktiviert	Zum vollständigen Deaktivieren oder Aktivieren der statischen Analyse. Standardmäßig ist dies **aktiviert**.

Funktion	Beschreibung
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.
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. Diese Tabelle beschreibt die Parameter zur Konfiguration der Communityanalyse.

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.
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

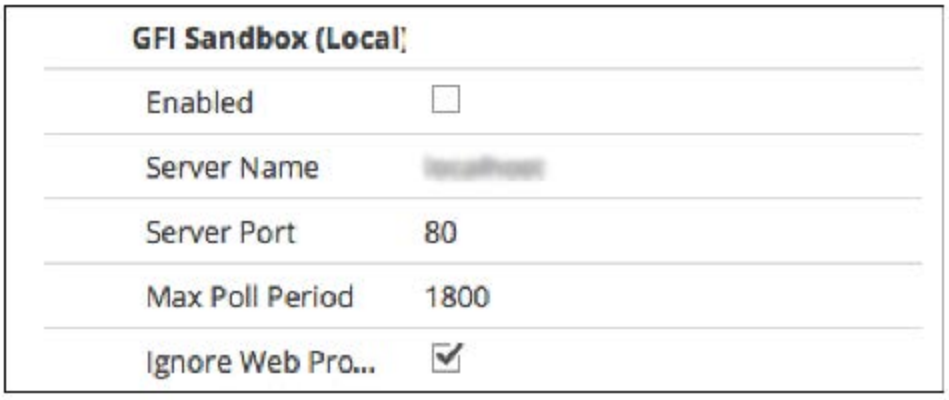
Das Sandbox-Modul ist standardmäßig deaktiviert und MS Office- sowie PDF-Dateien werden nicht verarbeitet. Die Einstellungen sollen so restriktiv wie möglich gewählt werden, sodass der Nutzer ganz gezielt auswählen muss, ob potenziell vertrauliche Informationen übermittelt und außerhalb des Netzwerkes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

Diese Tabelle beschreibt die Parameter zur Konfiguration der Sandbox-Analyse.

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.

Funktion	Beschreibung
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.
Ursprünglichen Dateinamen beim Ausführen der Sandbox-Analyse beibehalten	Aktivieren Sie bei 10.3 SP2 und späteren Versionen die Funktion zum Hashen von Dateinamen, wenn diese an eine lokale Sandbox gesendet werden. Diese Option ist standardmäßig deaktiviert. **Hinweis:** Wenn Sie diesen Parameter nicht aktivieren, weist Security Analytics 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.

Funktion	Beschreibung
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 Security Analytics Malware Analysis an, beim Herstellen dieser Verbindung den Webproxy zu umgehen, sofern einer konfiguriert ist. Wenn kein Webproxy in Security Analytics 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.

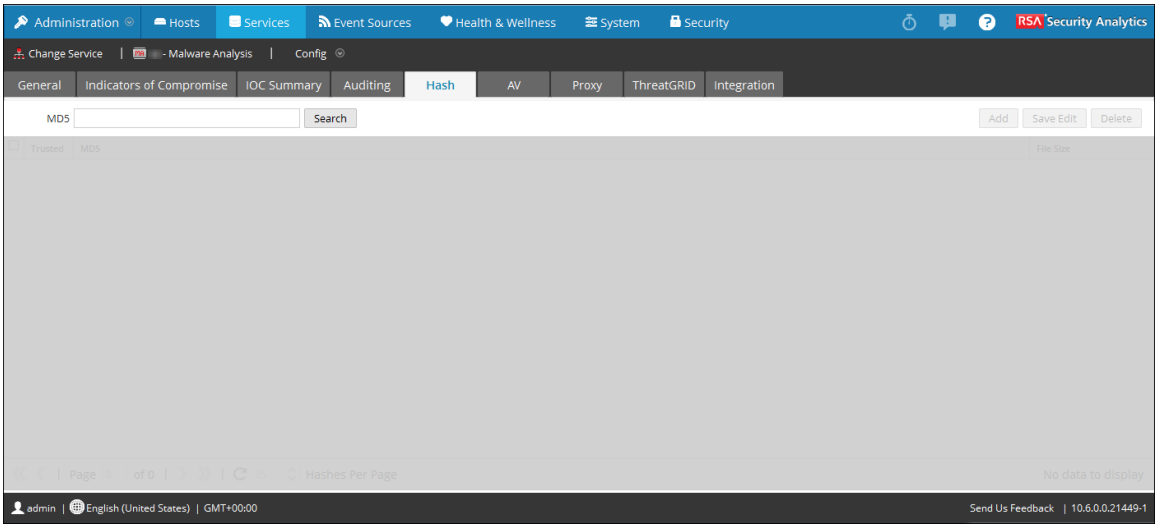
Funktion	Beschreibung
Aktiviert	Ist diese Option aktiviert, führt entweder eine lokale Kopie von ThreatGrid oder die ThreatGrid-Cloud diese Sandbox Verarbeitung aus. Standardmäßig ist die Einstellung **deaktiviert**.
Serviceschlüssel	Bevor Sie das Sandbox-Modul aktivieren, müssen Sie einen von ThreatGrid 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 Security Analytics Malware Analysis an, beim Herstellen dieser Verbindung den Webproxy zu umgehen, sofern einer konfiguriert ist. Wenn kein Webproxy in Security Analytics Malware Analysis konfiguriert wurde, wird die Einstellung ignoriert.

Ansicht „Service-Konfiguration“ – Registerkarte „Hash“

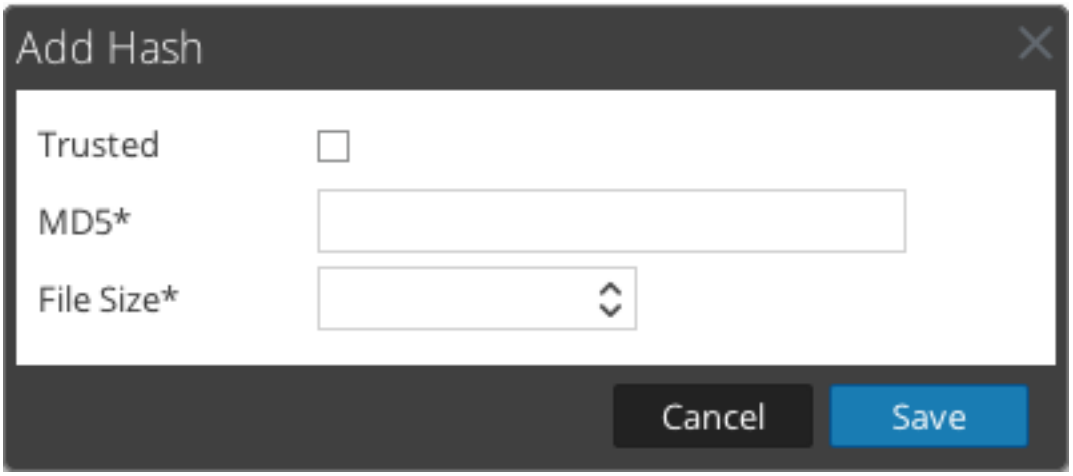
Dieses Thema bietet eine Einführung in die Funktionen der Registerkarte „Hash“ der Ansicht „Service-Konfiguration“ für Security Analytics Malware Analysis.

Auf dieser Registerkarte können Sie die Hash-Filterung in Security Analytics Malware Analysis managen. 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.

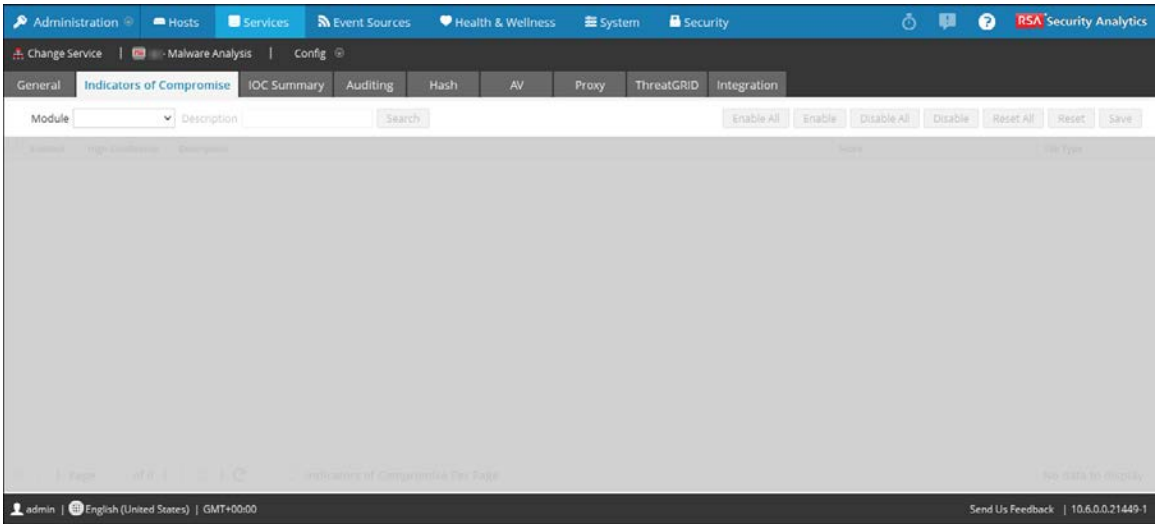
In dieser Tabelle werden die Spalten des Hash-Rasters beschrieben.

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.

Funktion	Beschreibung
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.
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.

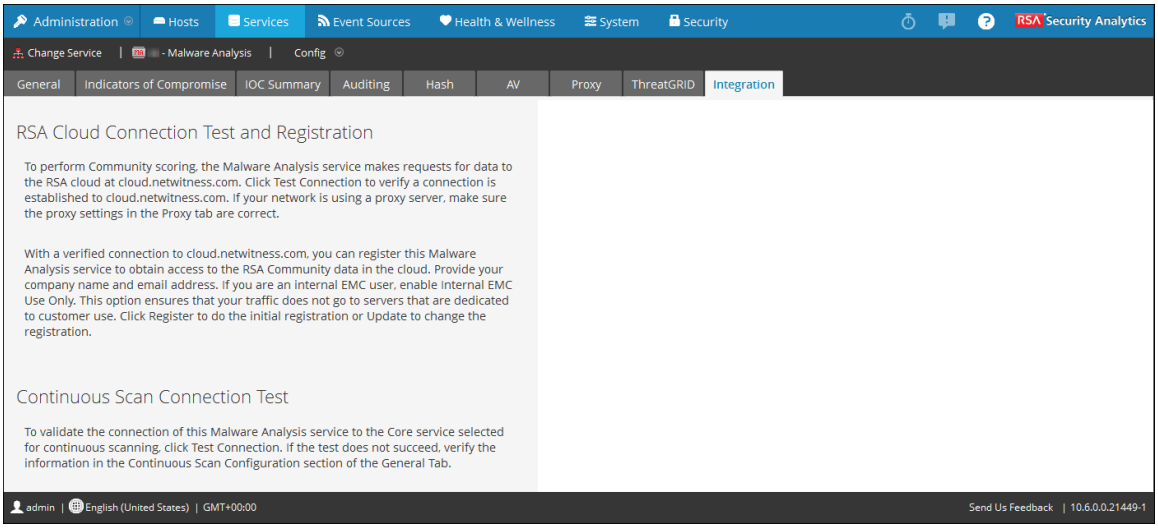
Spalte	Beschreibung
Kontrollkästchen „Auswahl“	Kontrollkästchen zur Auswahl einzelner Zeilen oder aller Zeilen auf der Seite.
Kontrollkästchen „Aktiviert“	Wenn die Indikatoren für eine Infizierung aktiviert sind, verwendet Security Analytics Malware Analysis die Regel für die Bewertung von Sitzungsdaten.

Spalte	Beschreibung
Kontrollkästchen Hohe Wahrscheinlichkeit	Im aktivierten Zustand behandelt Security Analytics 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 RSA Security Analytics 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
RSA-Cloud-Verbindungstest und -Registrierung Schaltfläche	Durch Klicken auf diese Schaltfläche können Sie testen, ob eine aktive Verbindung zu cloud.netwitness.com besteht. Security Analytics 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.

Funktion	Beschreibung
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.`
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.
Verbindungstest für kontinuierliches Scannen Schaltfläche Testen	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).

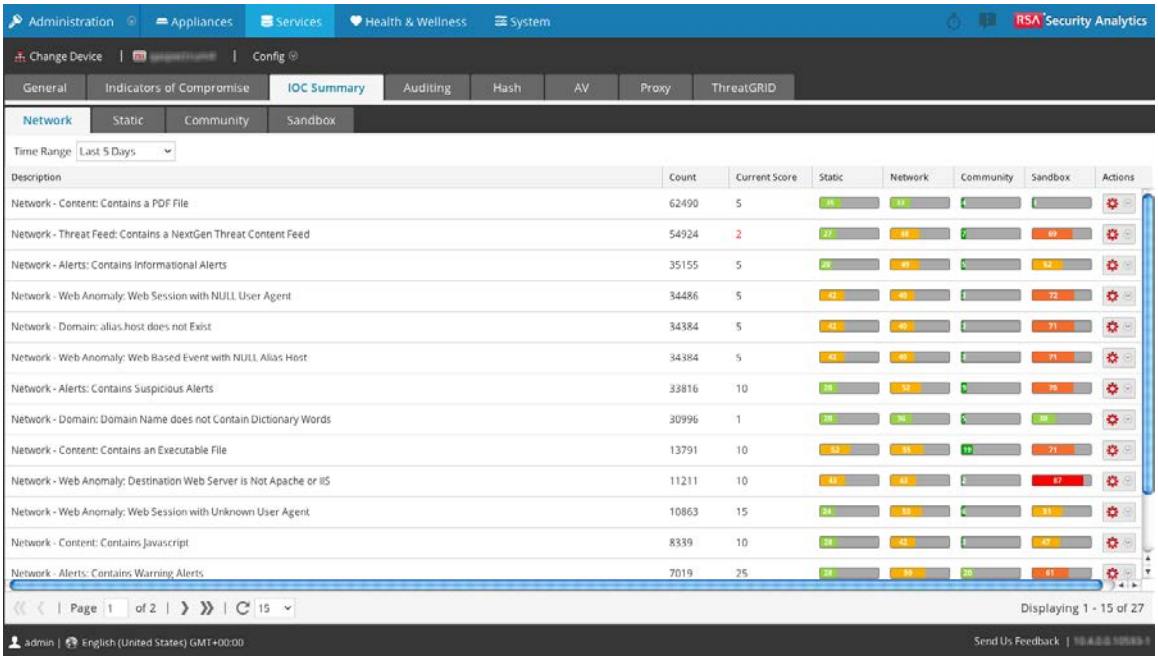
Ansicht „Service-Konfiguration“ – Registerkarte „IOC-Zusammenfassung“

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.

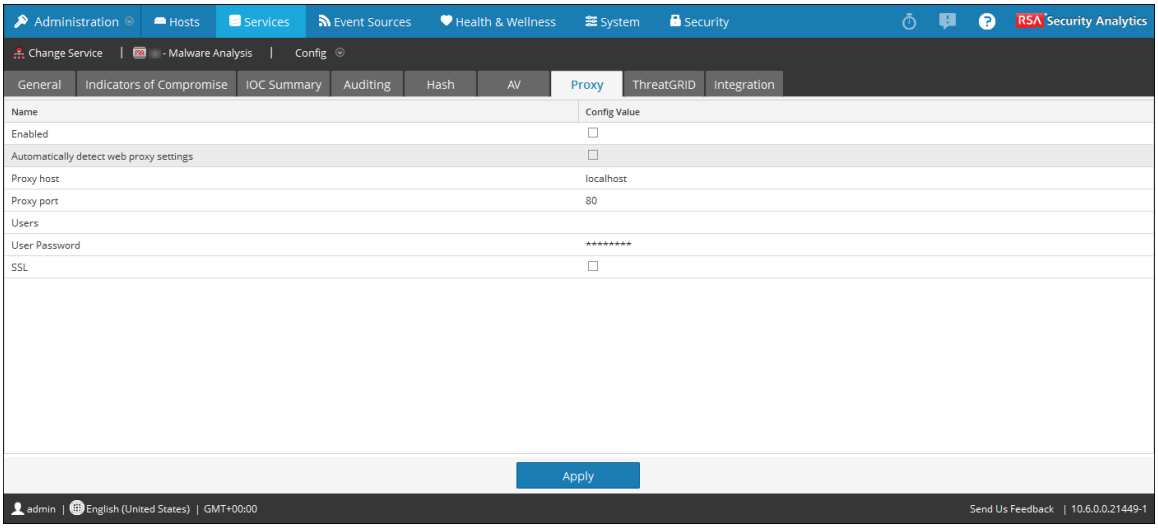
Funktion	Beschreibung
Zeitbereich	Wählt den Zeitbereich für die IOC-Zusammenfassung aus. Die möglichen Werte sind: Letzte 5 Minuten, Letzte 15 Minuten, Letzte 30 Minuten, Letzte Stunde, Letzte 3 Stunden, Letzte 6 Stunden, Letzte 12 Stunden, Letzte 24 Stunden, Letzte 2 Tage, Letzte 5 Tage, Morgen, Vormittag, 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.

Funktion	Beschreibung
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 Security Analytics Malware Analysis-Service konfiguriert werden können. Auf dieser Registerkarte wird die Security Analytics 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.

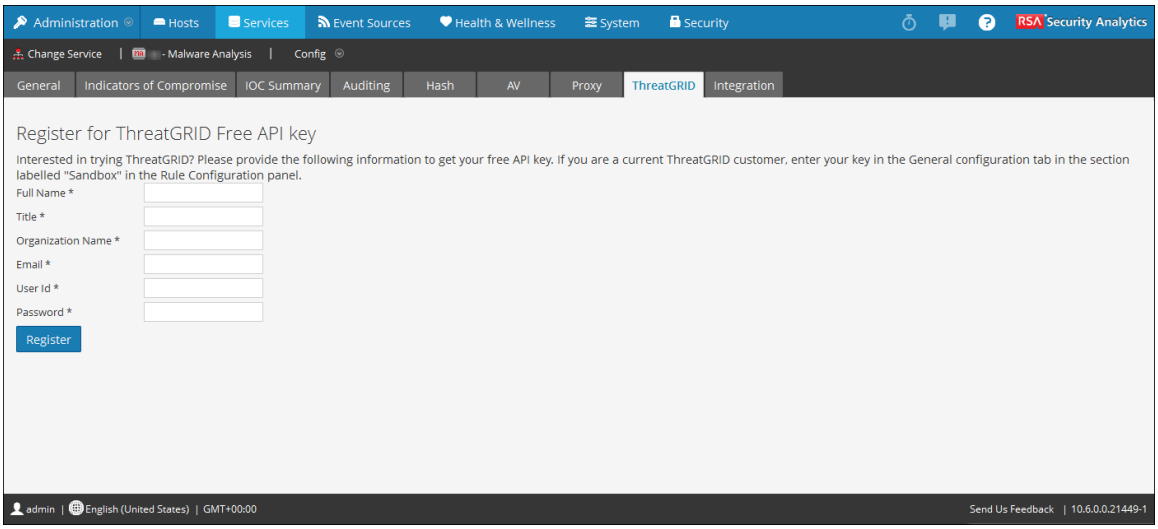
Funktion	Beschreibung
Webproxyeinstellungen automatisch erkennen	Aktivieren Sie dieses Kontrollkästchen, um die in den Systemeinstellungen konfigurierten Einstellungen zu verwenden.
Proxyhost	Geben Sie den Hostnamen für den Proxyhost ein.
Proxyport	Geben Sie den Port für die Kommunikation mit dem Proxyhost 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.
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 Security Analytics 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.
Title	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.

Funktion	Beschreibung
Password	Ihr Passwort für den Zugriff auf ThreatGrid.
Schaltfläche Registrieren	Klicken Sie auf **Registrieren** um die Anforderung abzusenden.