



Leitfaden zur automatisierten Bedrohungserkennung

für Version 11.0



Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Februar 2018

Inhalt

NetWitness Suite – Automatisierte Bedrohungserkennung	4
Automatisierte Bedrohungserkennung für verdächtige Domains	4
Workflow für Modul „Verdächtige Domains“	5
Automatisierte Bedrohungserkennung für verdächtige Domains für Pakete im Vergleich zu Webproxy-Protokollen	7
Konfigurieren der automatisierten Bedrohungserkennung für verdächtige Domains	8
Voraussetzungen	8
Konfigurieren der automatisierten Bedrohungserkennung für verdächtige Domains	9
Schritt 1: (Nur für Protokolle) Konfigurieren der Protokolleinstellungen	10
So erhalten Sie die aktuelle enVision-Konfigurationsdatei:	12
So überprüfen Sie, ob die enVision-Konfigurationsdatei korrekt aktualisiert wurde:	13
So überprüfen Sie, ob die Indizes für die Datei „index-concentrator.xml“ aktualisiert wurden:	13
Schritt 2: Erstellen Sie eine Domain-Whitelist (Optional)	14
Schritt 3: Konfigurieren des Whois-Abfrageservice	17
Schritt 4: Zuordnen von Datenquellen zu ESA Analytics-Modulen	17
Schritt 5: Überprüfen, ob die Regel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ aktiviert ist, und Überwachen der Regel	17
Schritt 6: Überprüfen, ob der Incident nach verdächtigem C&C gruppiert ist	18
Nächste Schritte	18
Troubleshooting für NetWitness Suite – Automatisierte Bedrohungserkennung	19
Mögliche Probleme	19

NetWitness Suite – Automatisierte Bedrohungserkennung

Die automatisierte Bedrohungserkennung von RSA NetWitness® Suite verwendet vorkonfigurierte ESA Analytics-Module, um bestimmte Arten von Bedrohungen zu identifizieren. Ein ESA Analytics-Modul ist eine Pipeline aus Aktivitätsobjekten, die ein Ereignis durch mathematische Berechnungen um zusätzliche Informationen ergänzen. ESA Analytics-Module befinden sich in den ESA Analytics-Services. Die ESA Analytics-Services verwenden abfragebasierte Aggregation (Query-Based Aggregation, QBA), um gefilterte Ereignisse für die Module von Concentrators zu erfassen. Nur die von einem Modul benötigten Daten werden zwischen dem Concentrator und dem ESA Analytics-System übertragen.

Es gibt zwei ESA-Services, die auf einem ESA-Host ausgeführt werden können:

- Event Stream Analysis (ESA-Korrelationsregeln)
- Event Stream Analytics Server (ESA Analytics)

Der erste Service ist der Event Stream Analysis-Service, der Warnmeldungen aus ESA-Regeln, auch bekannt als ESA-Korrelationsregeln, erstellt, die Sie manuell erstellen oder von Live herunterladen. Der zweite Service ist der ESA Analytics-Service, der für die automatisierte Bedrohungserkennung verwendet wird. Da der ESA Analytics-Service für die automatisierte Bedrohungserkennung vorkonfigurierte Module verwendet, müssen Sie keine Regeln erstellen oder herunterladen, um die automatisierte Bedrohungserkennung verwenden zu können.

Die automatisierte Bedrohungserkennung für NetWitness Suite verfügt derzeit über zwei Module „Verdächtige Domains“, Command and Control (C2) für Pakete und C2 für Protokolle.

Da jedes ESA Analytics-Modul unterschiedliche Datenanforderungen hat, achten Sie darauf, dass alle modulspezifischen Anforderungen erfüllt sind, bevor Sie ein Modul für die automatisierte Bedrohungserkennung bereitstellen.

Automatisierte Bedrohungserkennung für verdächtige Domains

Das Modul „Verdächtige Domains“ untersucht Ihren HTTP-Datenverkehr, um Domains zu erkennen, die wahrscheinlich Schadsoftware-Command-and-Control-Server sind und sich mit Ihrer Umgebung verbinden. Nachdem die automatisierte Bedrohungserkennung von NetWitness Suite für verdächtige Domains Ihren HTTP-Datenverkehr untersucht hat, erzeugt sie Bewertungen basierend auf verschiedenen Aspekten des Verhaltens Ihres Datenverkehrs (z. B. die Häufigkeit und Regelmäßigkeit, mit der eine bestimmte Domain kontaktiert wird). Wenn diese Bewertungen einen festgelegten Schwellenwert erreichen, wird eine ESA-Warnmeldung erzeugt. Diese ESA-Warnmeldung wird an der Ansicht „Reagieren“ weitergeleitet. Die Warnmeldung in der Ansicht „Reagieren“ wird mit Daten erweitert, die Ihnen helfen, die Bewertungen zu interpretieren, um festzustellen, welche Gegenmaßnahmen zu ergreifen sind.

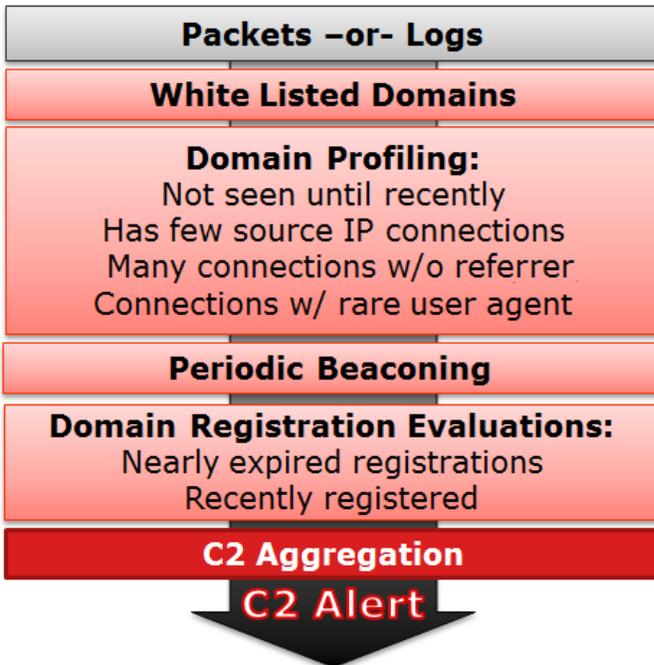
Die Module „Verdächtige Domains“ der automatisierten Bedrohungserkennung erlauben Bewertungen, um Command-and-Control-Kommunikation zu erkennen. Command-and-Control-Kommunikation erfolgt, wenn Schadsoftware ein System infiziert hat und Daten zurück zu einer Quelle sendet. Oft kann Command-and-Control-Schadsoftware über Beaconing-Verhalten erkannt werden. Beaconing tritt auf, wenn die Schadsoftware regelmäßig Kommunikation zurück an den Command-and-Control-Server sendet, um ihn zu informieren, dass eine Maschine infiziert wurde und dass die Schadsoftware auf weitere Anweisungen wartet. Die Fähigkeit, die Schadsoftware an diesem Punkt der Infizierung zu ergreifen, kann weiteren Schaden an der infizierten Maschine vermeiden und gilt als kritische Phase in der „Kill Chain“.

Die automatisierte Bedrohungserkennung von NetWitness Suite löst einige häufige Probleme, die bei der Suche nach Schadsoftware auftreten:

- **Fähigkeit zur Verwendung von Algorithmen anstatt Signaturen.** Da viele Ersteller von Schadsoftware inzwischen polymorphe oder verschlüsselte Codesegmente verwenden, für die nur sehr schwer eine Signatur erstellt werden kann, kann dieser Ansatz manchmal Schadsoftware nicht entdecken. Da die automatisierte Bedrohungserkennung von NetWitness Suite einen verhaltensbasierten Algorithmus verwendet, kann sie Schadsoftware schneller und effizienter erkennen.
- **Möglichkeit zur Automatisierung der Jagd.** Das manuelle Durchsuchen von Daten ist eine effektive, aber sehr zeitaufwändige Methode zum Auffinden von Schadsoftware. Die Automatisierung dieses Prozesses erlaubt es Analysten, ihre Zeit effizienter zu nutzen.
- **Fähigkeit, einen Angriff schnell zu entdecken.** Anstatt Daten in Batches zu sammeln und dann zu analysieren, analysiert die automatisierte Bedrohungserkennung Daten, während sie von NetWitness Suite aufgenommen werden, sodass die Angriffe nahezu in Echtzeit gefunden werden können.

Workflow für Modul „Verdächtige Domains“

Die automatisierte Bedrohungserkennung von NetWitness Suite funktioniert ähnlich wie ein Filtersystem. Sie überprüft, ob ein bestimmtes Verhalten auftritt (oder bestimmte Bedingungen bestehen), und wenn dieses Verhalten oder diese Bedingung auftritt, fährt es mit dem nächsten Schritt im Prozess fort. Damit wird das System effizienter und es bleiben Ressourcen frei, da Ereignisse, die als nicht bedrohlich eingestuft werden, nicht im Arbeitsspeicher gehalten werden. Das folgende Diagramm bietet eine vereinfachte Version des Workflows für das Modul „Verdächtige Domains“.



- 1.) **Pakete oder Protokolle werden zum ESA-Service geleitet.** Die HTTP-Pakete oder Protokolle werden vom Decoder oder Log Decoder analysiert und an den ESA-Host gesendet.
- 2.) **Die Whitelist wird geprüft.** Wenn Sie eine Whitelist über Context Hub erstellt haben, prüft der ESA-Service diese Liste, um Domains auszuschließen. Wenn eine Domain im Ereignis auf der Whitelist steht, wird das Ereignis ignoriert.
- 3.) **Das Profil der Domain wird geprüft.** Automatisierte Bedrohungserkennung prüft, ob die Domain neu in Erscheinung tritt (ca. drei Tage), über wenige Quell-IP-Verbindungen verfügt, viele Verbindungen ohne einen Referrer oder Verbindungen mit seltenen Benutzeragenten hat. Wenn eine oder mehrere dieser Bedingungen zutrifft, wird die Domain als nächstes auf regelmäßiges Beaconsing geprüft.
- 4.) **Die Domain wird auf regelmäßiges Beaconsing geprüft.** Beaconsing tritt auf, wenn die Schadsoftware regelmäßig Kommunikation zurück an den Command-and-Control-Server sendet, um ihn zu informieren, dass eine Maschine infiziert wurde und dass die Schadsoftware auf weitere Anweisungen wartet. Wenn die Website Beaconsing-Verhalten zeigt, werden die Registrierungsinformationen der Domain geprüft.
- 5.) **Registrierungsinformationen der Domain werden geprüft.** Der Whois-Service wird verwendet, um festzustellen, ob die Domain vor kurzem registriert wurde oder fast abgelaufen ist. Domains, die eine sehr kurze Lebensdauer haben, sind oft Kennzeichen für Schadsoftware.

6.) **Command and Control (C2) aggregiert Bewertungen.** Jeder der oben genannten Faktoren erzeugt eine separate Bewertung, die gewichtet wird, um verschiedene Niveaus der Wichtigkeit zu kennzeichnen. Die gewichteten Bewertungen bestimmen, ob eine Warnmeldung erzeugt werden soll. Wenn eine Warnmeldung generiert wird, werden die zusammengefassten Warnmeldungen in der Ansicht „Reagieren“ angezeigt und können dann von dort aus weiter untersucht werden. Sobald die Warnmeldungen in der Ansicht „Reagieren“ angezeigt werden, werden sie weiter unter dem zugehörigen Incident aggregiert. Dies erleichtert das Durchgehen großer Mengen von Warnmeldungen, die für einen Command-and-Control-Incident generiert werden können.

Analysten können die Warnmeldungen in der Ansicht „Reagieren“ anzeigen.

Automatisierte Bedrohungserkennung für verdächtige Domains für Pakete im Vergleich zu Webproxy-Protokollen

RSA NetWitness Suite bietet Ihnen die Möglichkeit, eine automatisierte Bedrohungserkennung für verdächtige Domains über Pakete oder Webproxy-Protokolle auszuführen. Während die Paketdaten direkt über das Internet in die NetWitness Suite-Installation gestreamt und direkt analysiert werden können, kann die Verwendung eines Webproxy in Ihrer Installation vorteilhaft sein, sofern dies möglich ist. Da einige Installationen Netzwerkadressübersetzung oder SSL-Verschlüsselung verwenden, kann die echte Quell-IP einer ausgehenden Verbindung maskiert sein, wenn Sie sie auf Paketebene beobachten. Durch die Verwendung eines Webproxys profitieren Sie von der Möglichkeit zum Beschleunigen und Entschlüsseln von SSL-Datenverkehr sowie der Möglichkeit, die tatsächlichen Quell-IP-Adressen des überwachten Datenverkehrs zu verfolgen.

Verdächtige Domains für Pakete (C2 für Pakete) und verdächtige Domains für Protokolle (C2 für Protokolle) sollten dieselben Ergebnisse liefern. Im Hinblick auf die Ergebnisse bietet keine der beiden Möglichkeiten einen echten Vorteil.

Konfigurieren der automatisierten Bedrohungserkennung für verdächtige Domains

Dieses Thema enthält Informationen für Administratoren und Analysten zur Konfiguration eines „Suspicious Domains“-Moduls für die automatisierte Bedrohungserkennung von NetWitness Suite. Mit der Funktion der automatisierten Bedrohungserkennung können Sie die Daten auf einem oder mehreren Concentrators analysieren, indem Sie vorkonfigurierte ESA Analytics-Module verwenden. Beispielsweise kann ein ESA Analytics-Service mithilfe eines „Suspicious Domains“-Moduls Ihren HTTP-Datenverkehr untersuchen, um die Wahrscheinlichkeit dafür zu ermitteln, dass böswillige Aktivitäten in Ihrer Umgebung stattfinden.

Es gibt zwei Arten von vorkonfigurierten „Suspicious Domains“-Modulen in NetWitness Suite: Befehl und Kontrolle (Command and Control, C2) für Pakete und C2 für Protokolle. Das Modul „Suspicious Domains“ definiert eine Untergruppe von Ereignissen sowie die bei Eintreten dieser Ereignisse ausgeführten Aktivitäten zur Identifikation verdächtiger C2-Domains.

Bevor Sie ein ESA Analytics-Modul für die automatisierte Bedrohungserkennung aktivieren, sollten Sie beachten, dass es viele potenzielle Installationskonfigurationen gibt, die auf dem ESA-Service installiert werden können, einschließlich: ESA Analytics, ESA Correlation Rules und Context Hub. Sie alle binden Ressourcen, daher ist es wichtig, vor dem Bereitstellen der automatisierten Bedrohungserkennung auf Ihrem ESA-Service die Dimensionierung zu berücksichtigen.

Voraussetzungen

- Wenn Sie Paketdaten verwenden, müssen Sie einen Decoder für HTTP-Paketdaten konfiguriert haben sowie einen Lua- oder Flex-HTTP-Parser.
- Wenn Sie Protokolldaten für den Webproxy verwenden, müssen Sie den entsprechenden Log Decoder mit dem richtigen Parser für den Webproxy konfiguriert haben.
- Wenn Sie Protokolldaten für den Webproxy verwenden, müssen Sie auf die aktuellen Protokollparser aktualisiert haben. Die folgenden Parser werden unterstützt: Blue Coat Cache Flow (Cacheflowelff), Cisco IronPort WSA (Ciscoportwsa) und Zscaler (Zscalernss).
- Wenn Sie Protokolldaten für den Webproxy verwenden, sollten Sie zum Erzielen der bestmöglichen Ergebnisse alle Ergebnisse auf die gleiche Weise konfigurieren (auf dieselbe Zeitzone festlegen, die gleiche Sammlungsmethode – syslog oder Stapel – verwenden und, wenn Sie Stapel verwenden, den gleichen Zeitplan für die Stapelverarbeitung nutzen).

- Eine Verbindung zwischen dem ESA-Host und dem Whois-Service (selber Speicherort wie RSA Live cms:netwitness.com:443) muss über Port 443 geöffnet werden. Überprüfen Sie mit Ihrem Systemadministrator, ob dieser Vorgang abgeschlossen ist.
- Fügen Sie eine Domain zur Whitelist hinzu, indem Sie den Context Hub-Service aktivieren.

Wichtig: Die automatisierte Bedrohungserkennung benötigt eine Anlaufphase, bei der der Bewertungsalgorithmus auf den Datenverkehr in Ihrem Netzwerk abgestimmt wird. Sie müssen die automatisierte Bedrohungserkennung so konfigurieren, dass die Anlaufphase auch während des normalen Datenverkehrs stattfinden kann. Beispielsweise ermöglicht das Starten der automatisierten Bedrohungserkennung an einem Dienstag um 8:00 Uhr in der Zeitzone, in dem sich der Großteil Ihrer Benutzer befindet, dass das Modul einen Tag mit normalem Datenverkehr analysieren kann.

Konfigurieren der automatisierten Bedrohungserkennung für verdächtige Domains

Dieses Verfahren enthält die Schritte zum Konfigurieren eines „Suspicious Domains“-Moduls für ESA Analytics für die automatisierte Bedrohungserkennung. ESA Analytics-Module wie „Suspicious Domains“ gelten als vorkonfiguriert, da Sie nicht manuell ESA-Regeln für sie erstellen müssen.

Die erforderlichen grundlegenden Schritte sind:

1. **Konfigurieren der Protokolleinstellungen (nur für Protokolle).** Bevor Sie die automatisierte Bedrohungserkennung für Protokolle verwenden können, müssen Sie verschiedene Einstellungen konfigurieren. Überspringen Sie diesen Schritt, wenn Sie vorhaben, die automatisierte Bedrohungserkennung für Pakete zu verwenden.
2. **Eine Whitelist (optional) mithilfe des Service „Context Hub“ erstellen.** Durch das Erstellen einer Whitelist können Sie sicherstellen, dass häufig verwendete Websites von der Bewertung durch die automatisierten Bedrohungserkennung ausgenommen sind.
3. **Konfigurieren des Whois-Abfrageservice.** Mit dem Service „Whois“ können Sie präzise Daten über Domains erhalten, mit denen Sie sich verbinden. Es ist wichtig, dass Sie den Whois-Abfrageservice konfigurieren, um eine effektive Bewertung zu ermöglichen. Stellen Sie sicher, dass der Whois-Service aus Ihrer Umgebung erreichbar ist.
4. **Ordnen Sie Datenquellen ESA Analytics-Modulen zu.** Sie legen fest, wie die automatisierte Bedrohungserkennung von NetWitness Suite Advanced Threats automatisch erkennen soll, indem Sie ein vorkonfiguriertes ESA Analytics-Modul mehreren Datenquellen, z. B. Concentrators, und einem ESA Analytics-Service zuordnen.

5. **Stellen Sie sicher, dass die C2-Incident-Regel aktiviert ist, und überwachen Sie sie auf Aktivität.** Nach der Zuordnung Ihres „Suspicious Domains“-Moduls muss etwas Zeit vergehen, bis der Bewertungsalgorithmus angelaufen ist. Stellen Sie nach der Anlaufphase sicher, dass die C2-Regel in den Incident-Regeln aktiviert ist, und überwachen Sie, ob die Regel ausgelöst wird.
6. **Stellen Sie sicher, dass die Incident-Regeln richtig konfiguriert sind.** Wenn Sie in der Ansicht „Reagieren“ Incidents anzeigen, ist es hilfreich, wenn die Incidents nach „Verdächtige C&C“ gruppiert sind.

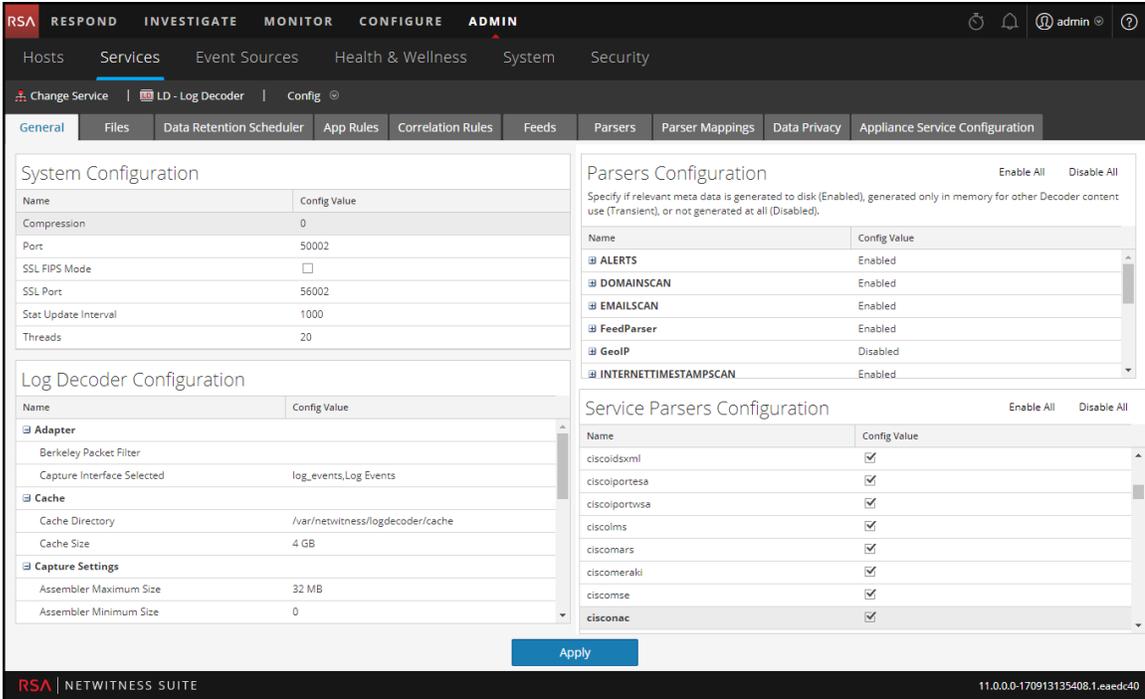
Schritt 1: (Nur für Protokolle) Konfigurieren der Protokolleinstellungen

Konfigurieren Sie die automatisierte Bedrohungserkennung für Protokolle, indem Sie einige zusätzliche Konfigurationsschritte ausführen:

- Stellen Sie sicher, dass die unterstützten Parser für Ihren Log Decoder aktiviert sind.
- Rufen Sie die aktuellen Versionen des entsprechenden Webproxy-Parser von RSA Live ab.
- Aktualisieren Sie die Zuordnung für die enVision-Konfigurationsdatei. Diese Datei ist erforderlich, um den Log Decoder zu aktualisieren, sodass er mit den neuen, über den Parser verfügbaren Metadaten arbeiten kann.
- Stellen Sie sicher, dass die Datei „table-map.xml“ korrekt aktualisiert wurde.
- Stellen Sie sicher, dass die Indizes korrekt aktualisiert wurden.

So überprüfen Sie, ob die Parser in Ihrem Log Decoder ausgeführt werden:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Log Decoder und anschließend  > **Ansicht > Konfiguration aus**. Im Abschnitt „Serviceparserkonfiguration“ wird eine Liste der aktivierten Parser angezeigt.
3. Stellen Sie sicher, dass der entsprechende Webproxy-Parser aktiviert ist.



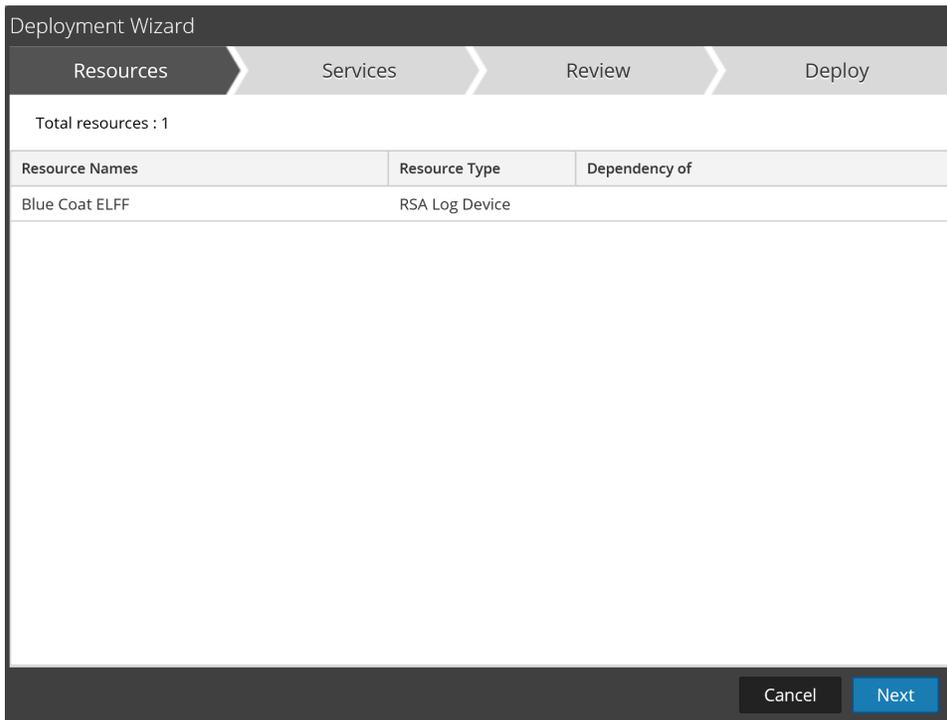
So erhalten Sie die aktuellen Parser von RSA Live:

1. Navigieren Sie zu **Konfigurieren > Live-Inhalte**.
2. Geben Sie einen Suchbegriff für einen der unterstützten Webproxy-Parser ein.
3. Wählen Sie den passenden Webproxy-Parser aus [zum Beispiel Blue Coat ELFF (cacheflowelf)].

Hinweis: Sie sollten die Protokollierung so konfiguriert haben, dass sie korrekt auf dem Webproxy-Parser ausgeführt wird.

4. Klicken Sie auf **Bereitstellen**.

Der Bereitstellungsassistent wird geöffnet.

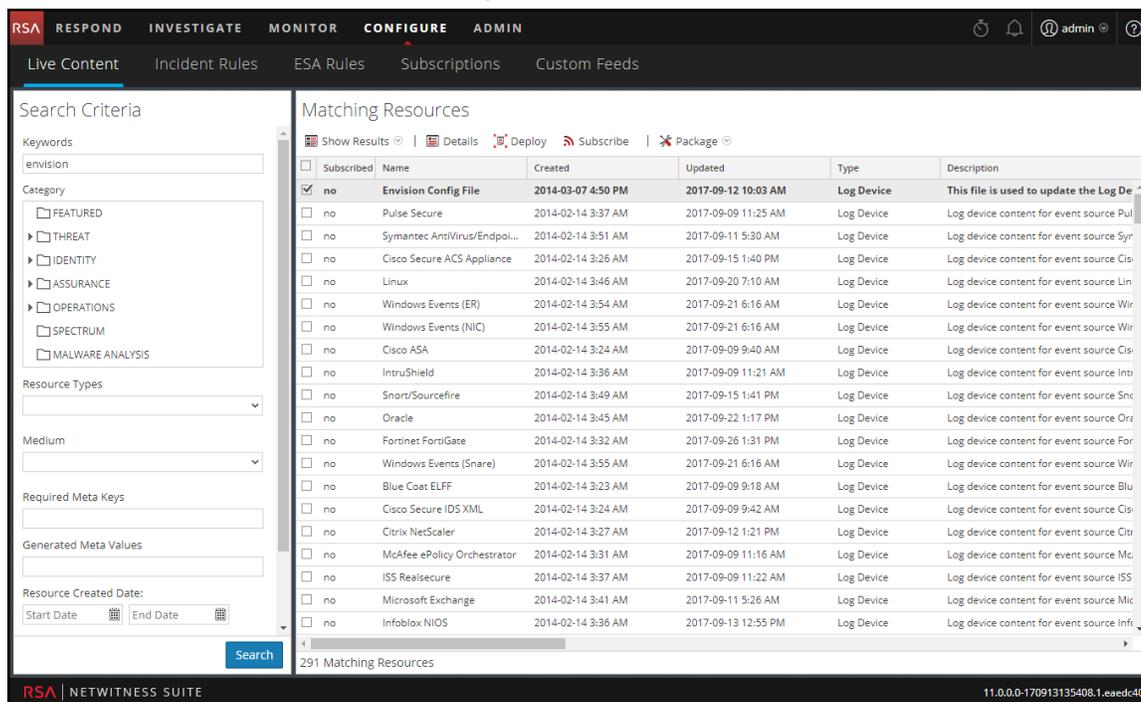


5. Wählen Sie unter **Services** den Log Decoder als Service aus.
6. Klicken Sie auf **Bereitstellen**, um den Parser auf Ihrem Log Decoder bereitzustellen.

So erhalten Sie die aktuelle enVision-Konfigurationsdatei:

1. Navigieren Sie zu **Konfigurieren > Live-Inhalte**.
2. Geben Sie **enVision** als Schlüsselwort für die Suche ein.

- Wählen Sie die aktuelle enVision-Konfigurationsdatei aus und klicken Sie auf **Bereitstellen**.



- Wählen Sie im Bereitstellungsassistenten unter **Services** Ihren Log Decoder aus.
- Klicken Sie auf **Bereitstellen**, um die enVision-Konfigurationsdatei auf dem Log Decoder bereitzustellen.

So überprüfen Sie, ob die enVision-Konfigurationsdatei korrekt aktualisiert wurde:

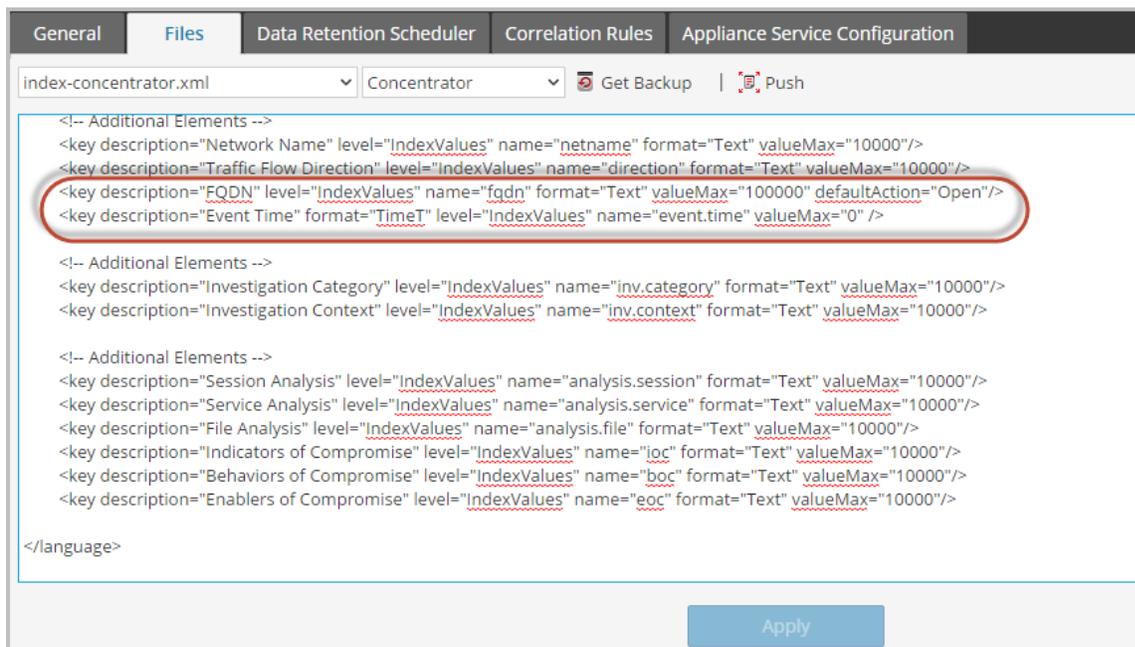
- Gehen Sie zu **ADMIN > Services**, wählen Sie einen Log Decoder aus und wählen Sie dann  > **Ansicht > Konfiguration > Dateien** aus.
Sie sehen die Datei **table-map.xml**. Diese Datei wird geändert, wenn Sie die enVision-Konfigurationsdatei aktualisieren.
- Suchen Sie nach *event.time*. Das Feld sollte nun *"event.time" Flags = "None"* enthalten. Das bedeutet, dass die „event.time“-Metadaten jetzt in der Zuordnung enthalten sind. Auf ähnliche Weise sollte der FQDN-Flag auf „None“ festgelegt werden.

So überprüfen Sie, ob die Indizes für die Datei „index-concentrator.xml“ aktualisiert wurden:

Sie müssen sicherstellen, dass die Datei **index-concentrator.xml** die „event.time“- und die FQDN-Metadaten enthält.

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie Ihren Concentrator aus und navigieren Sie dann dazu  > **Ansicht > Konfiguration**.
2. Suchen Sie auf der Registerkarte „Dateien“ nach der Datei **index-concentrator.xml**.
3. Stellen Sie sicher, dass der folgende Eintrag in der Datei „index-concentrator.xml“ vorhanden ist. Wenn dies nicht der Fall ist, müssen Sie sicherstellen, dass Ihr Concentrator auf die richtige Version aktualisiert wurde:

```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/><key description="Event Time" format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```



The screenshot shows the configuration interface for the file `index-concentrator.xml` in the `Concentrator` section. The XML content is displayed in a text area, and a red circle highlights the following entries:

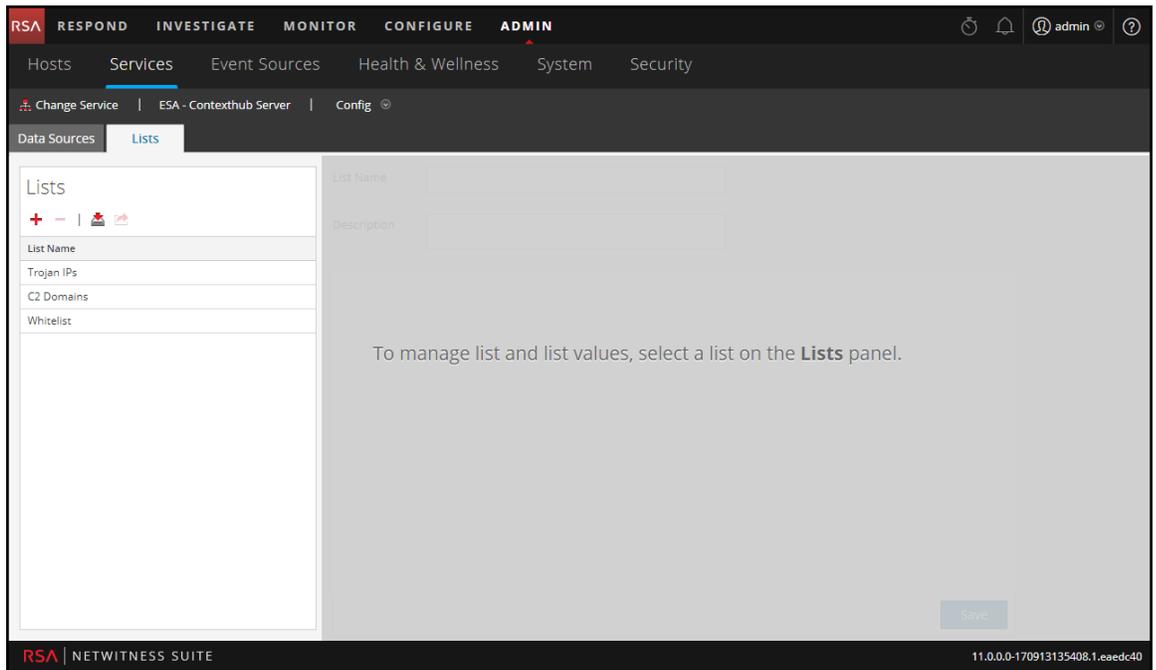
```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/>
<key description="Event Time" format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```

Schritt 2: Erstellen Sie eine Domain-Whitelist (Optional)

Dieses Verfahren wird bei der Arbeit mit der automatisierten Bedrohungserkennung verwendet, um sicherzustellen, dass bestimmte Domains keine Bedrohungsbewertung auslösen. Manchmal kann eine Domain, auf die Sie regelmäßig zugreifen, eine Bewertung durch die automatisierte Bedrohungserkennung auslösen. Beispielsweise könnte ein Wetterdienst ein ähnliches Beaconing-Verhalten zeigen wie eine Befehl-und-Kontrolle-Kommunikation und so eine nicht gerechtfertigte negative Bewertung auslösen. Eine solche Bewertung wird als falsch positiv bezeichnet. Sie können das Auslösen einer falsch positiven Bewertung verhindern, indem Sie die Domain einer Whitelist hinzufügen. Die meisten Domains müssen nicht einer Whitelist hinzugefügt werden, da die Lösung nur bei sehr verdächtigem Verhalten eine Warnmeldung ausgibt. Die Domains, die möglicherweise einer Whitelist hinzugefügt werden sollten, sind gültige automatisierte Services, mit denen sich nicht viele Hosts verbinden.

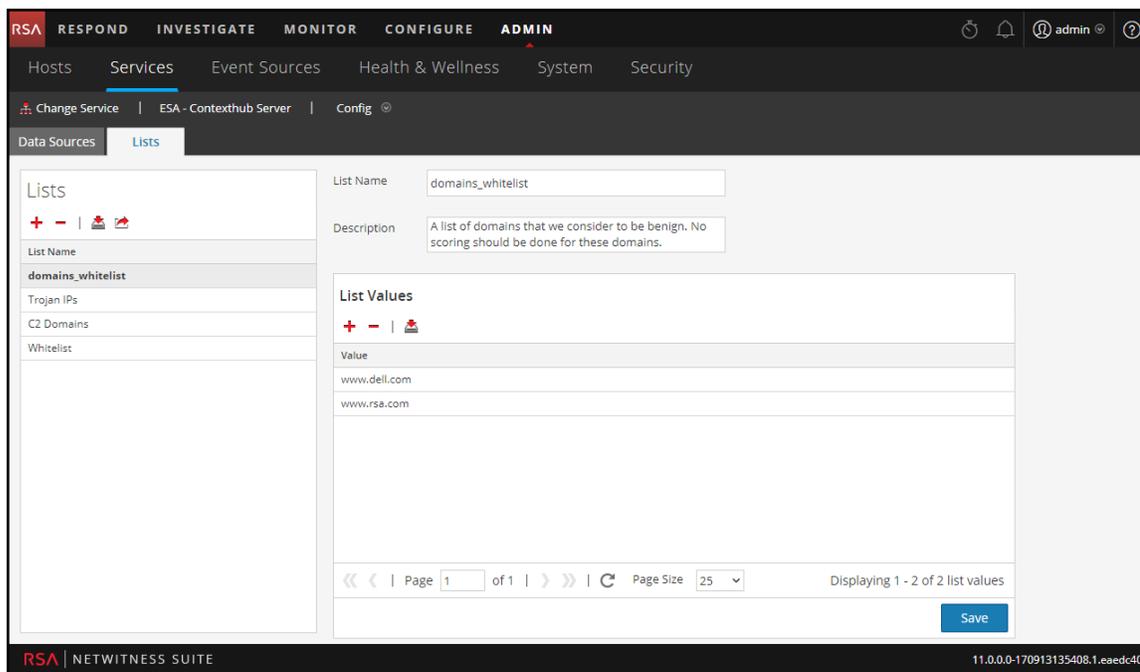
Hinweis: Bei Migrationen ab Version 10.6.x gilt: Wenn Ihre vorherige Whitelist für die automatisierte Bedrohungserkennung (Domains auf weißer Liste) auf der Registerkarte „Listen“ angezeigt wird, können Sie sie in **domains_whitelist** umbenennen, um sie für die „Suspicious Domains“-Module zu verwenden.

1. Erstellen Sie eine Whitelist für Domains in Context Hub mit dem Namen **domains_whitelist**:
 - a. Navigieren Sie zu **ADMIN > Services**, wählen Sie den Context Hub Server-Service aus und gehen Sie dann zu **Ansicht > Konfiguration > Registerkarte „Listen“**.
Auf der Registerkarte „Listen“ werden die aktuellen Listen in Context Hub angezeigt.



- b. Klicken Sie im Bereich „Listen“ auf **+**, um eine Liste hinzuzufügen. Geben Sie im Feld **Listenname domains_whitelist** ein. Sie müssen diesen Namen verwenden,

damit er vom Modul erkannt wird.



2. Fügen Sie der Liste manuell Domains hinzu oder importieren Sie eine CSV-Datei, die eine Liste von Domains enthält.

Sie können vollständige Domains eingeben oder einen Platzhalter verwenden, um alle Subdomains für eine bestimmte Domain einzuschließen. Beispielsweise können Sie „*.gov“ eingeben, um alle IP-Adressen von Regierungsbehörden einer Whitelist hinzuzufügen. Sie können jedoch keine anderen Regex-Funktionen wie [a-z]*.gov verwenden. Das liegt daran, dass *.gov eine vollständige Zeichenfolge wie z. B. www.irs.gov ersetzt.

- a. Klicken Sie zum manuellen Hinzufügen von Domains im Abschnitt **Listenwerte** auf , um Domains hinzuzufügen.
 - b. Wählen Sie die Domain aus und klicken Sie auf , um eine Domain zu entfernen.
 - c. Klicken Sie zum Importieren einer CSV-Datei im Abschnitt **Listenwerte** auf  und navigieren Sie im Dialogfeld **Listenwerte importieren** zur CSV-Datei. Wählen Sie eines der folgenden Trennzeichen aus: Komma, LF (Zeilenvorschub) und CR (Wagenrücklauf), je nachdem, wie Sie die Werte in Ihrer Datei getrennt haben. Klicken Sie auf **Hochladen**.
3. Klicken Sie auf **Speichern**.
- Die Whitelist **domains_whitelist** wird im Bereich „Listen“ angezeigt. Analysten können dieser Liste in der Ansicht „Reagieren“ und in anderen Bereichen von „Untersuchen“

Domains hinzufügen. Im *Context Hub-Konfigurationsleitfaden* finden Sie zusätzliche Informationen.

Schritt 3: Konfigurieren des Whois-Abfrageservice

Siehe „Konfigurieren des Whois-Abfrageservice“ im *ESA-Konfigurationsleitfaden*.

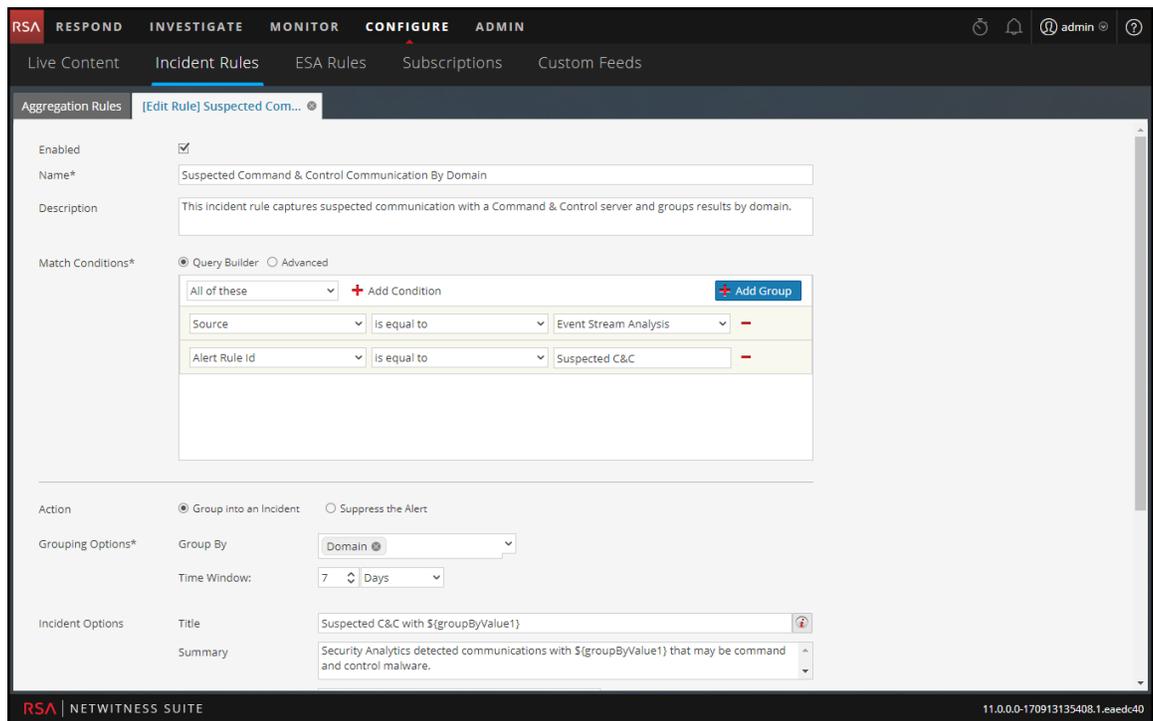
Schritt 4: Zuordnen von Datenquellen zu ESA Analytics-Modulen

Weitere Informationen finden Sie im Thema „Zuordnen von ESA-Datenquellen zu Analytics-Modulen“ im *ESA-Konfigurationsleitfaden*.

Schritt 5: Überprüfen, ob die Regel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ aktiviert ist, und Überwachen der Regel

Überprüfen Sie die Regel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ in den Incident-Regeln.

1. Navigieren Sie zu **Konfigurieren > Incident-Regeln > Aggregationsregeln**.
2. Wählen Sie die Regel **Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain** aus und doppelklicken Sie darauf, um sie zu öffnen.



3. Überprüfen Sie, ob **Aktiviert** ausgewählt ist.

Wenn sie aktiviert ist, zeigt die Regel eine grüne „Aktiviert“-Schaltfläche an.

Ergebnis

Nach der Bereitstellung der Zuordnung des „Suspicious Domains“-Moduls von ESA Analytics für die automatisierte Bedrohungserkennung beginnt ESA damit, den HTTP-Datenverkehr zu analysieren. Sie können in der Ansicht „Reagieren“ detaillierte Informationen für jeden Incident anzeigen.

Schritt 6: Überprüfen, ob der Incident nach verdächtigem C&C gruppiert ist

Sie können Incidents in der Ansicht „Reagieren“ korrekt gruppieren, indem Sie die Bedingung „Gruppieren nach“ auf „Domain“ festlegen.

1. Navigieren Sie zu **Konfigurieren > Incident-Regeln > Aggregationsregeln**.
2. Wählen Sie die Regel **Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain** aus und doppelklicken Sie darauf, um sie zu öffnen.
3. Überprüfen Sie, ob das Feld **Gruppieren nach** auf *Domain* festgelegt ist.

Dadurch werden Warnmeldungen aggregiert und es werden Incidents für „Verdächtige C&C“ erstellt.

Nächste Schritte

Überwachen Sie die Ansicht „Reagieren“, um festzustellen, ob die Regel ausgelöst wird. Im *NetWitness Respond-Benutzerhandbuch* finden Sie zusätzliche Informationen.

Troubleshooting für NetWitness Suite – Automatisierte Bedrohungserkennung

NetWitness Suite Die automatisierte Bedrohungserkennung ist eine Analyse-Engine, die Ihre HTTP-Daten untersucht. Sie verwendet auch andere Komponenten, wie etwa die Services „Whois“ und „Context Hub“, die Ihre Installation komplexer machen können. Dieses Thema enthält Vorschläge zum Auffinden von Problemen, wenn Ihre Bereitstellung der automatisierten Bedrohungserkennung nicht die Ergebnisse liefert, die Sie erwarten.

Mögliche Probleme

Problem	Mögliche Ursachen	Lösungen
Ich erhalte zu viele Warnmeldungen (falsch positive Ergebnisse).	Verschiedene	Eine mögliche Ursache ist, dass der Whois-Abfrageservice fehlgeschlagen oder nicht konfiguriert ist. Die Whois-Abfrage ist hilfreich bei der Ermittlung, ob eine URL gültig ist, und wenn die Verbindung fehlschlägt oder nicht ordnungsgemäß konfiguriert ist, kann es zu falsch positiven Ergebnissen kommen. Siehe „Konfigurieren des Whois-Abfrageservice“ im <i>ESA-Konfigurationsleitfaden</i> .
		Sie müssen eventuell URLs zur Whitelist hinzufügen. Manchmal löst das legitime Verhalten für eine URL eine Warnmeldung aus. Eine Möglichkeit, dies zu verhindern, besteht darin, die URL zur Whitelist hinzuzufügen. Siehe „Hinzufügen einer Entität zu einer Whitelist“ im <i>NetWitness Respond-Benutzerhandbuch</i> .

Problem	Mögliche Ursachen	Lösungen
Ich sehe keine Warnmeldungen.	Der ESA-Host erfordert eine „Aufwärmphase“, wenn Sie eine ESA Analytics-Modulzuordnung für die automatisierte Bedrohungserkennung bereitstellen.	Wenn Sie eine ESA Analytics-Modulzuordnung für die automatisierte Bedrohungserkennung bereitstellen, gibt es eine Aufwärmphase, während der keine Warnmeldungen angezeigt werden. Jeder Modultyp hat eine Standardaufwärmphase und Sie müssen warten, bis die Aufwärmphase abgeschlossen ist. Weitere Informationen finden Sie im Thema „Zuordnen von ESA-Datenquellen zu Analytics-Modulen“ im <i>ESA-Konfigurationsleitfaden</i> .
Ich sehe Performanceprobleme (es werden mehr Ressourcen verbraucht oder der Durchsatz geht zurück).	Verschiedene	Wenn Sie Performanceprobleme bei einem ESA-Host haben, der sowohl die automatisierte Bedrohungserkennung (ESA Analytics) als auch ESA-Regeln ausführt, befolgen Sie die Schritte zum Troubleshooting für Regeln. Diese Troubleshooting-Schritte finden Sie unter „Troubleshooting für ESA“ im <i>Handbuch Versenden von Warnmeldungen mit ESA</i> .