Konfigurieren der Integration von sicheren Malwareanalysen (ehemals Threat Grid) mit Umbrella

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Secure Malware Analytics (ehemals Threat Grid) in Umbrella integriert wird.

Integration von Cisco Secure Malware Analytics (Threat Grid) für Cisco Umbrella - Überblick

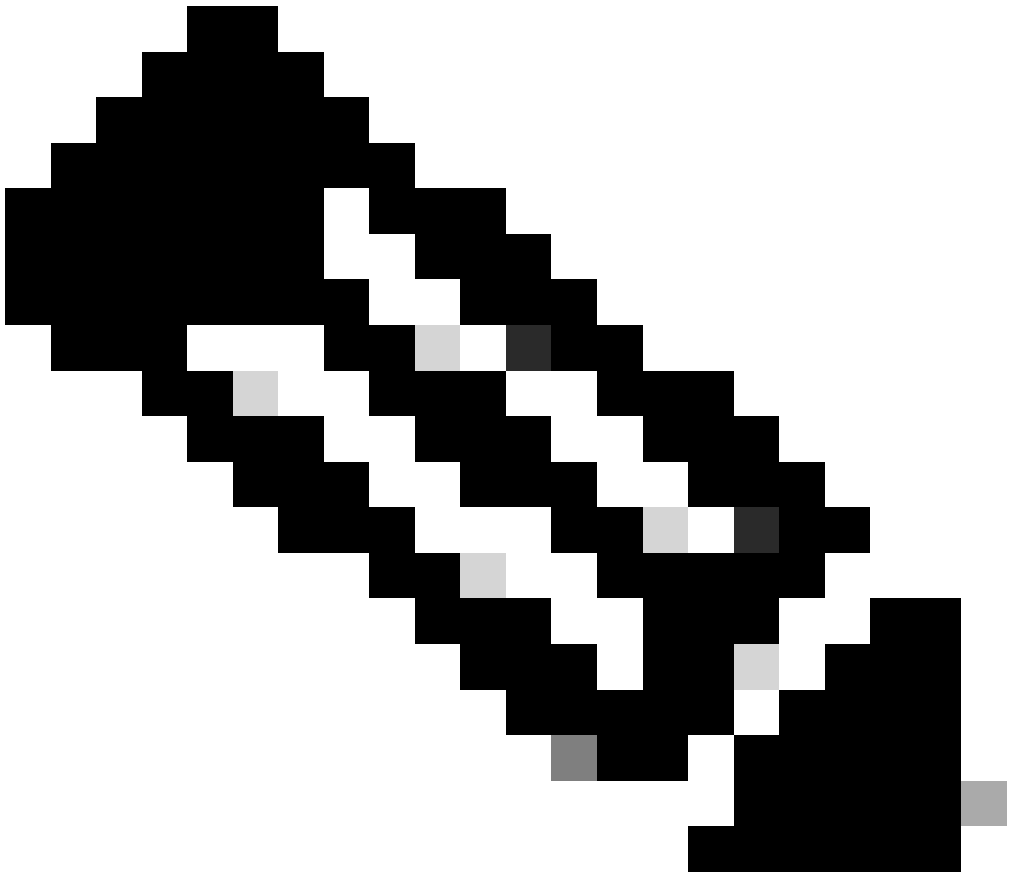
Durch die Integration von Cisco Secure Malware Analytics (ehemals Threat Grid) und Cisco Umbrella können Sicherheitsteams nun ihre Transparenz verbessern und den Schutz vor modernen Bedrohungen für mobile Laptops, Tablets oder Telefone durchsetzen. Gleichzeitig erhalten sie eine weitere Durchsetzungsebene für ein verteiltes Unternehmensnetzwerk.

In diesem Leitfaden wird erläutert, wie Cisco Secure Malware Analytics (Threat Grid) für die

Kommunikation mit Cisco Umbrella konfiguriert wird, damit die von Cisco Secure Malware Analytics (Threat Grid) generierte Threat Intelligence automatisch in Richtlinien integriert werden kann, die Clients unter Ihrem Cisco Umbrella schützen.

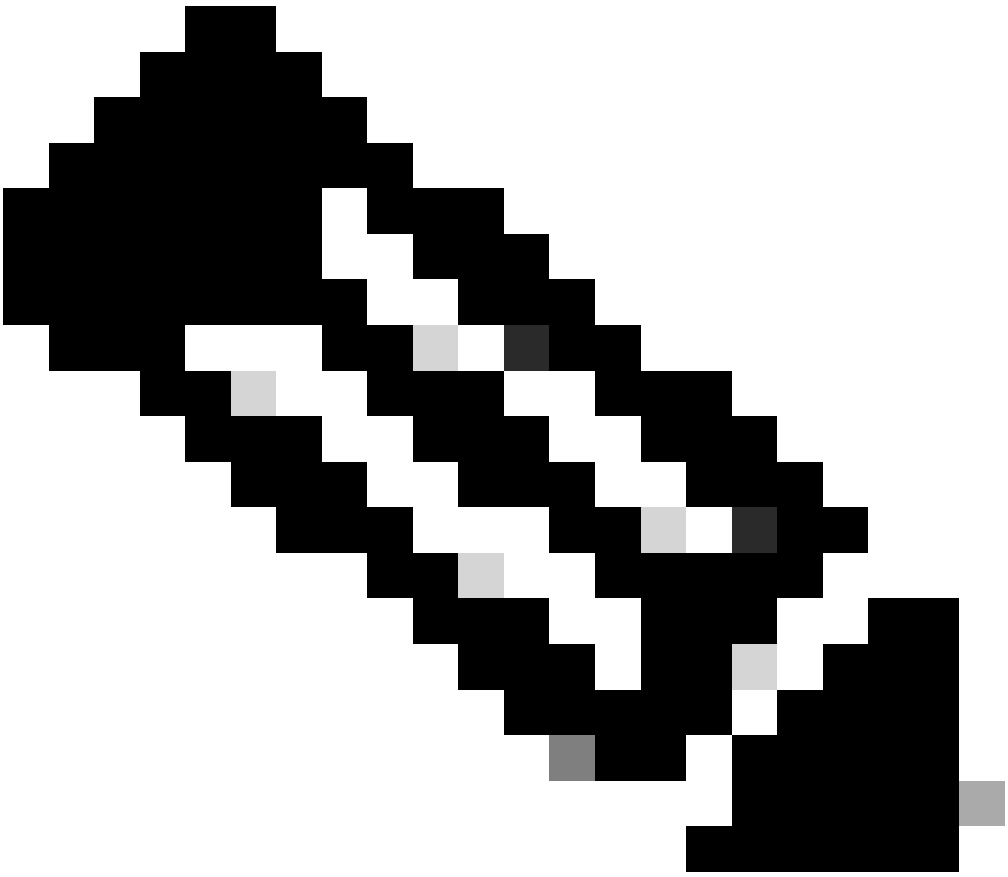
Voraussetzungen

- Ein funktionsfähiges Cisco Secure Malware Analytics (Threat Grid)-Dashboard mit Zugriff auf den API-Schlüssel Ihres Kontos.



> Anmerkung: Cisco Secure Malware Analytics (Threat Grid)-Appliances und -Endgeräte werden derzeit nicht unterstützt.

- Administratorrechte für das Cisco Umbrella Dashboard
- Im Cisco Umbrella Dashboard muss die Integration von Cisco Secure Malware Analytics (Threat Grid) aktiviert sein.



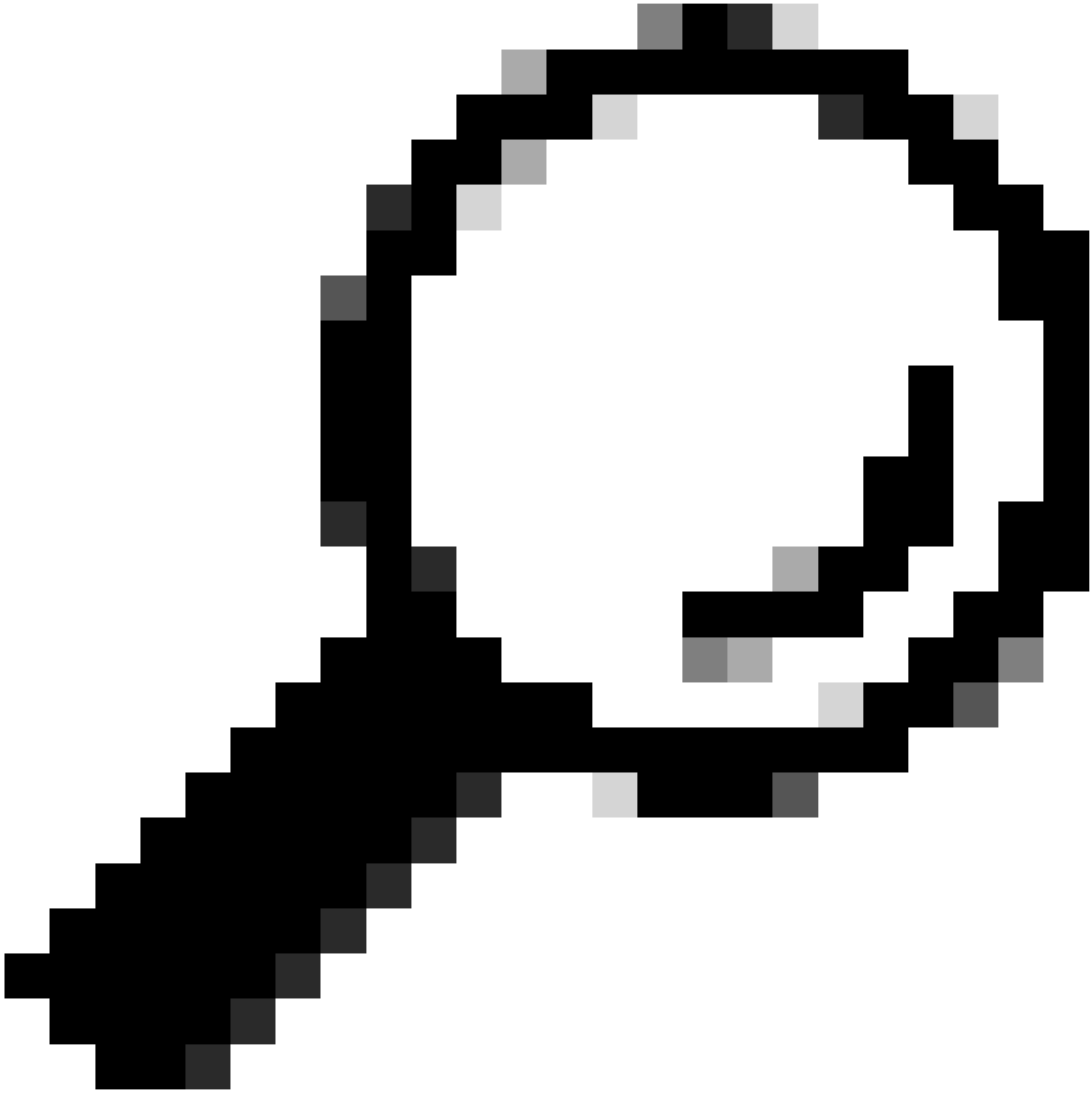
Anmerkung: Die Integration von Cisco Secure Malware Analytics (Threat Grid) ist nur in Cisco Umbrella-Paketen wie DNS Essentials, DNS Advantage, SIG Essentials oder SIG Advantage enthalten. Wenn Sie kein Cisco Umbrella-Paket haben und diese Integration wünschen, wenden Sie sich an Ihren Cisco Umbrella Account Manager. Wenn Sie über ein Cisco Umbrella-Paket verfügen, Cisco Secure Malware Analytics (Threat Grid) jedoch nicht als Integrationslösung für Ihr Dashboard betrachten, wenden Sie sich an den Cisco Umbrella Support.

Wie funktioniert diese Integration?

Cisco Umbrella greift auf die API von Cisco Secure Malware Analytics (Threat Grid) zu und ruft Listen von Domänen ab, die aus der Analyse schädlicher Stichproben generiert werden. Cisco Umbrella importiert diese Liste dann über die Cisco Umbrella Enforcement API. Dieser Ansatz unterscheidet sich von anderen Integrationen dadurch, dass Cisco Umbrella die Bedrohungsinformationen durch API-Abfragen an die Cisco Secure Malware Analytics (Threat Grid)-API bezieht, anstatt Vorfälle von anderen Systemen zu akzeptieren, die Bedrohungsinformationen in den Cisco Umbrella-Service übertragen.

Cisco Umbrella validiert die Bedrohung, um sicherzustellen, dass sie Ihrer Richtlinie hinzugefügt werden kann. Wenn sich bestätigt, dass die Informationen von Cisco Secure Malware Analytics (Threat Grid) eine Bedrohung darstellen oder keine zweifelsfrei funktionierende Domäne sind, wird die Domänenadresse der Zielliste von Cisco Secure Malware Analytics (Threat Grid) als Teil einer Sicherheitseinstellung hinzugefügt, die auf eine beliebige Cisco Umbrella-Richtlinie angewendet werden kann. Diese Richtlinie wird sofort auf alle Anfragen angewendet, die von Geräten mithilfe von Richtlinien gestellt werden, die die Cisco Secure Malware Analytics (Threat Grid)-Integration nutzen.

Cisco Umbrella bezieht zwei separate Feeds von Cisco Secure Malware Analytics (Threat Grid): einen öffentlichen (globalen) Feed und einen nur für einen Kunden bestimmten (privaten) Feed.



Tipp: Während Cisco Umbrella sich bemüht, bekanntermaßen sichere Domains (z. B. Google und Salesforce) zu validieren und zuzulassen, empfehlen wir, Domains, die

---

niemals blockiert werden sollen, der globalen Zulassungsliste oder anderen Ziellisten gemäß Ihrer Richtlinie hinzuzufügen, um unerwünschte Unterbrechungen zu vermeiden.

Beispiele:

- Die Startseite für Ihre Organisation.
- Domänen, die von Ihnen bereitgestellte Dienste darstellen und sowohl interne als auch externe Datensätze enthalten können. Beispiel: "mail.myservicedomain.com" und "portal.myotherservicedomain.com".
- Weniger bekannte Cloud-Anwendungen, von denen Sie in hohem Maße abhängig sind, werden von Cisco Umbrella möglicherweise nicht erkannt oder in ihre automatische Domänenvalidierung einbezogen. Beispiel: "localcloudservice.com".

Diese Domänen müssen der globalen Zulassungsliste hinzugefügt werden, die unter Richtlinien > Ziellisten in Cisco Umbrella zu finden ist.

Konfigurieren des Cisco Umbrella Dashboards zum Abrufen von Informationen von Cisco Secure Malware Analytics (Threat Grid)

Der erste Schritt besteht darin, den API-Schlüssel in Ihrem Cisco Secure Malware Analytics (Threat Grid) Dashboard zu finden oder zu generieren:

1. Melden Sie sich bei Ihrem Cisco Secure Malware Analytics (Threat Grid) Dashboard an, und wählen Sie Ihre Kontodetails aus.
2. Unter Ihren Kontodetails ist möglicherweise bereits ein API-Schlüssel sichtbar, wenn Sie diesen bereits erstellt haben. Andernfalls wählen Sie "Neuen API-Schlüssel generieren".

   Der API-Schlüssel wird dann unter Benutzerdetails > API-Schlüssel angezeigt.

Fügen Sie anschließend dem Cisco Umbrella Dashboard den API-Schlüssel hinzu, mit dem Daten aus Cisco Secure Malware Analytics (Threat Grid) abgerufen werden können:

1. Melden Sie sich als Administrator bei Ihrem Cisco Umbrella Dashboard an.
2. , navigieren Sie zu Policies > Policy Components > Integrations, und wählen Sie "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) in der Tabelle aus, um sie zu erweitern.
3. Wählen Sie Aktivieren, fügen Sie den API-Schlüssel in das Feld API-Schlüssel ein, und wählen Sie dann Speichern.

Wenn Sie an diesem Punkt einen Fehler erhalten, liegt wahrscheinlich ein Problem mit dem API-Schlüssel oder der Kommunikation zwischen den Services vor. Überprüfen Sie Ihren API-Schlüssel, und versuchen Sie es erneut. Sollte dieser weiterhin fehlschlagen, wenden Sie sich an den Cisco Umbrella Support.

Wenn Sie eine Erfolgsmeldung erhalten, bedeutet dies, dass der Cisco Umbrella Service den API-Schlüssel verwenden konnte, um eine erste Verbindung zur API von Cisco Secure Malware Analytics (Threat Grid) herzustellen. Der Cisco Umbrella Service nutzt ein Abfrageintervall von

fünf Minuten, um Daten von Cisco Secure Malware Analytics (Threat Grid) abzurufen.

Selbst nach Ablauf des Fünf-Minuten-Intervalls werden möglicherweise keine Informationen angezeigt, wenn keine gültigen Daten oder gültigen Bedrohungsereignisse verfügbar sind, die vom Cisco Umbrella Dashboard abgerufen werden können. Wenn die Integration zum ersten Mal aktiviert wird, beginnt sie damit, für den globalen und den rein organischen Feed jeweils fünf Minuten zurückzugehen. Beim ersten Abrufen von Daten erfolgt das Intervall im nächsten Fünfminütebereich, sodass die Daten möglicherweise nicht sofort angezeigt werden.

Wenn der API-Schlüssel auf Seite von Cisco Secure Malware Analytics (Threat Grid) deaktiviert oder entfernt würde, wäre die Integration deaktiviert. Um die Integration wiederherzustellen, muss ein neuer API-Schlüssel im Cisco Umbrella Dashboard bereitgestellt werden. Bei einer Zeitüberschreitung oder einem internen Dienstfehler zwischen Cisco Umbrella und Cisco Secure Malware Analytics (Threat Grid) wird eine andere Ausnahme ausgelöst, und die Integration wird nicht deaktiviert. Stattdessen werden wie unter normalen Bedingungen weiterhin alle fünf Minuten Verbindungen versucht.

Technische Details

Die genauen API-Abfragen, die zum Abrufen von Informationen aus Cisco Secure Malware Analytics (Threat Grid) verwendet werden, sind unten aufgeführt. Beachten Sie, dass nur Ereignisse mit einem Schweregrad größer als 90, einer Zuverlässigkeit größer als 90 und des Typs Domains gesammelt werden. Die Zeit in diesem Beispiel ist ein Fünf-Minuten-Bereich, der für die nächste Abfrage inkrementiert wird. Der in Cisco Umbrella bereitgestellte `api_key` wird anstelle der <`key`> Variablen verwendet:

- Öffentlich (globaler Feed):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Nur Kunde (privater Feed):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

Oder:

- Öffentlich (globaler Feed):

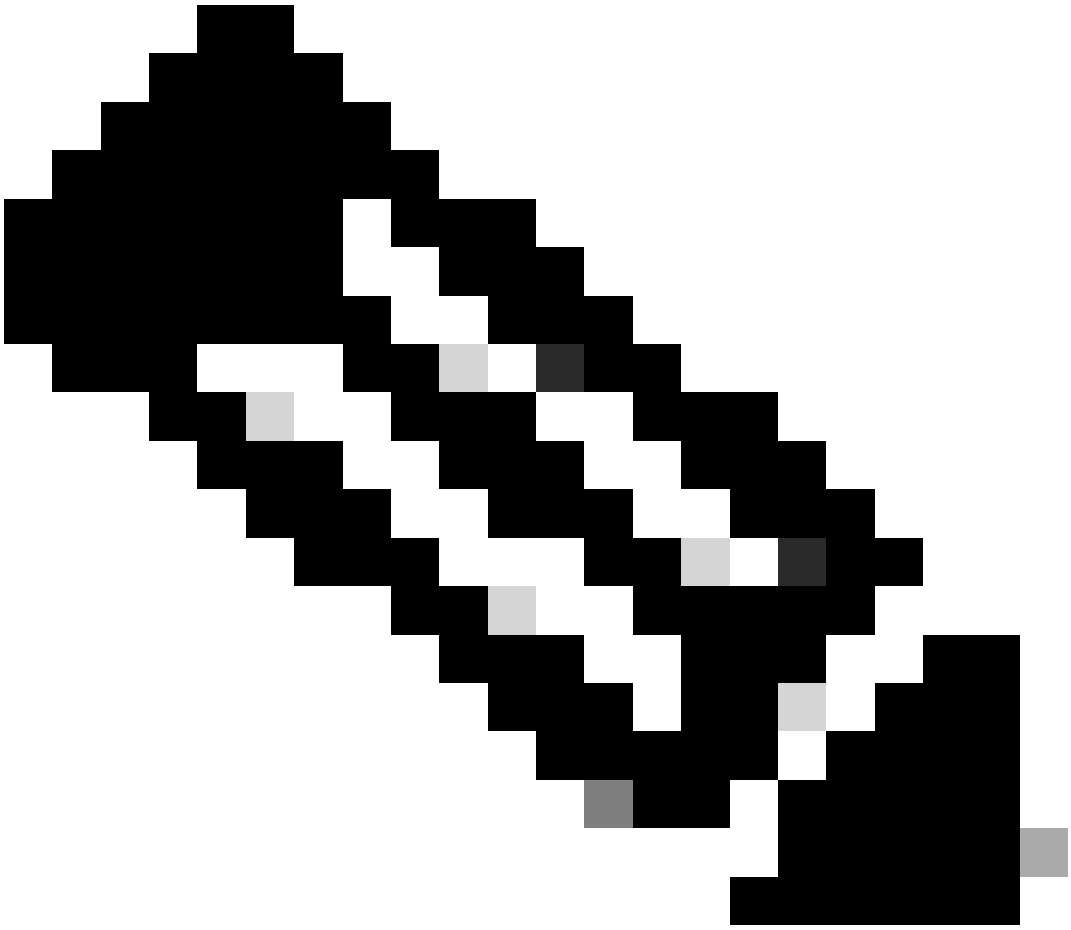
```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Nur Kunde (privater Feed):

hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=

Beobachtung von Ereignissen, die zu Cisco Secure Malware Analytics (Threat Grid) hinzugefügt wurden, im Audit-Modus

Im Laufe der Zeit beginnen die Ereignisse von Cisco Secure Malware Analytics (Threat Grid) mit dem Ausfüllen einer Liste spezifischer Ziele, die auf Richtlinien als Kategorie von Cisco Secure Malware Analytics (Threat Grid) angewendet werden können. Standardmäßig befinden sich die Zielliste und die Sicherheitskategorie im "Überwachungsmodus". Sie werden nicht auf Richtlinien angewendet und führen daher nicht zur Blockierung von Anforderungen. Sie können jedoch sehen, welche Anforderungen mit der Sicherheitskategorie von Cisco AMP Threat Grid verknüpft sind (und möglicherweise blockiert wurden).



Anmerkung: Der "Überwachungsmodus" kann je nach Bereitstellungsprofil und Netzwerkkonfiguration so lange wie nötig oder sogar auf unbestimmte Zeit aktiviert

---

werden.

Zielliste überprüfen

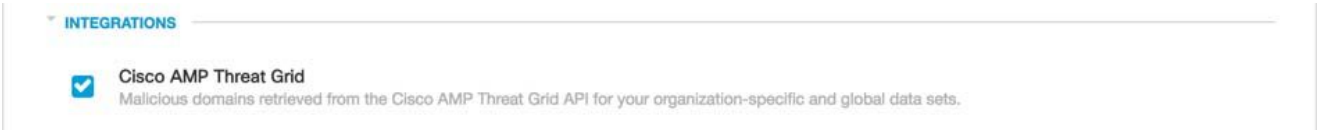
Sie können die Liste der Cisco Secure Malware Analytics (Threat Grid)-Ziele jederzeit einsehen.

1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Integrationen.
2. Erweitern Sie in der Tabelle "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)), und wählen Sie "Domains anzeigen" aus.

Sicherheitseinstellungen für eine Richtlinie überprüfen

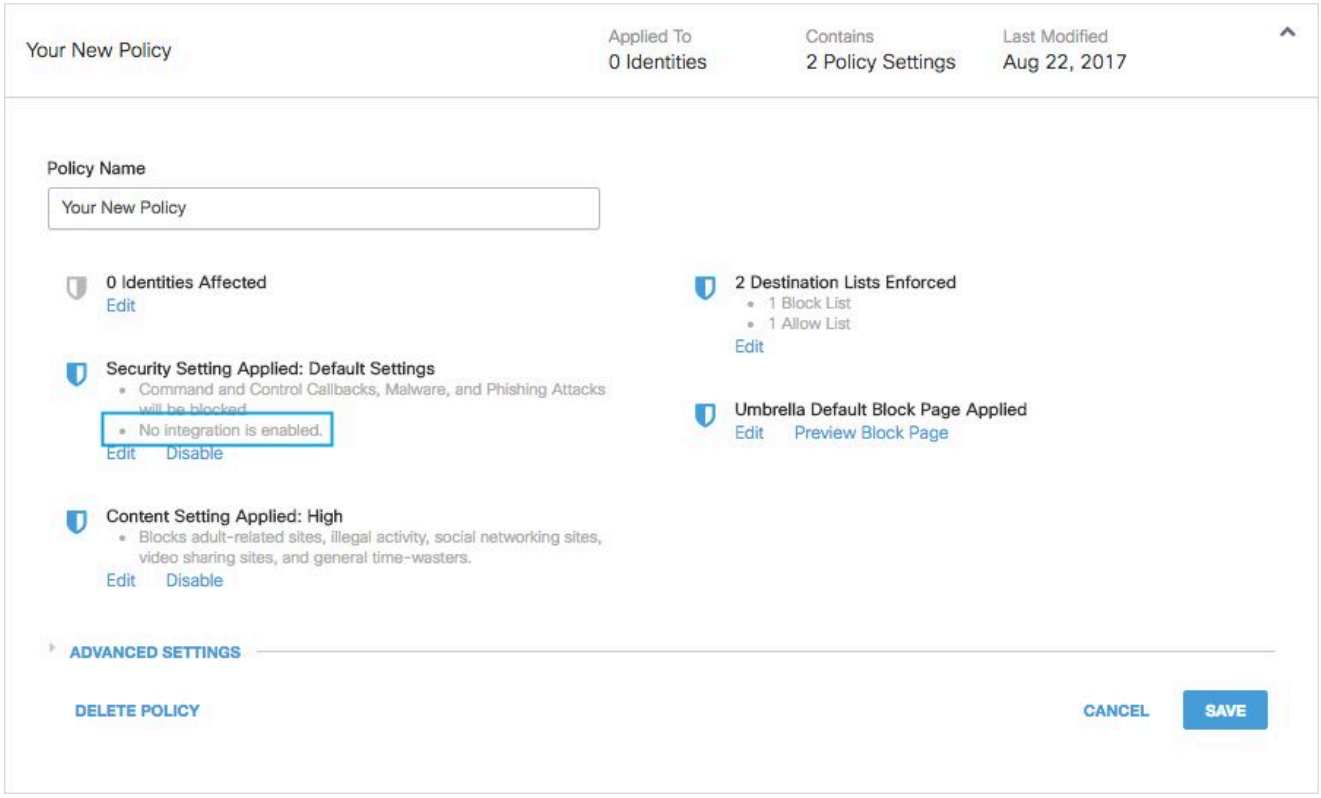
Sie können die Sicherheitseinstellungen, die für eine Richtlinie aktiviert werden können, jederzeit in Cisco Umbrella überprüfen:

1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Sicherheitseinstellungen.
2. Klicken Sie auf eine Sicherheitseinstellung in der Tabelle, um sie zu erweitern.
3. Scrollen Sie zum Abschnitt Integrationen, und erweitern Sie diesen Abschnitt, um die Integration von Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen für die Cisco AMP Threat Grid-Integration (Cisco Secure Malware Analytics (Threat Grid)), und wählen Sie dann Speichern.

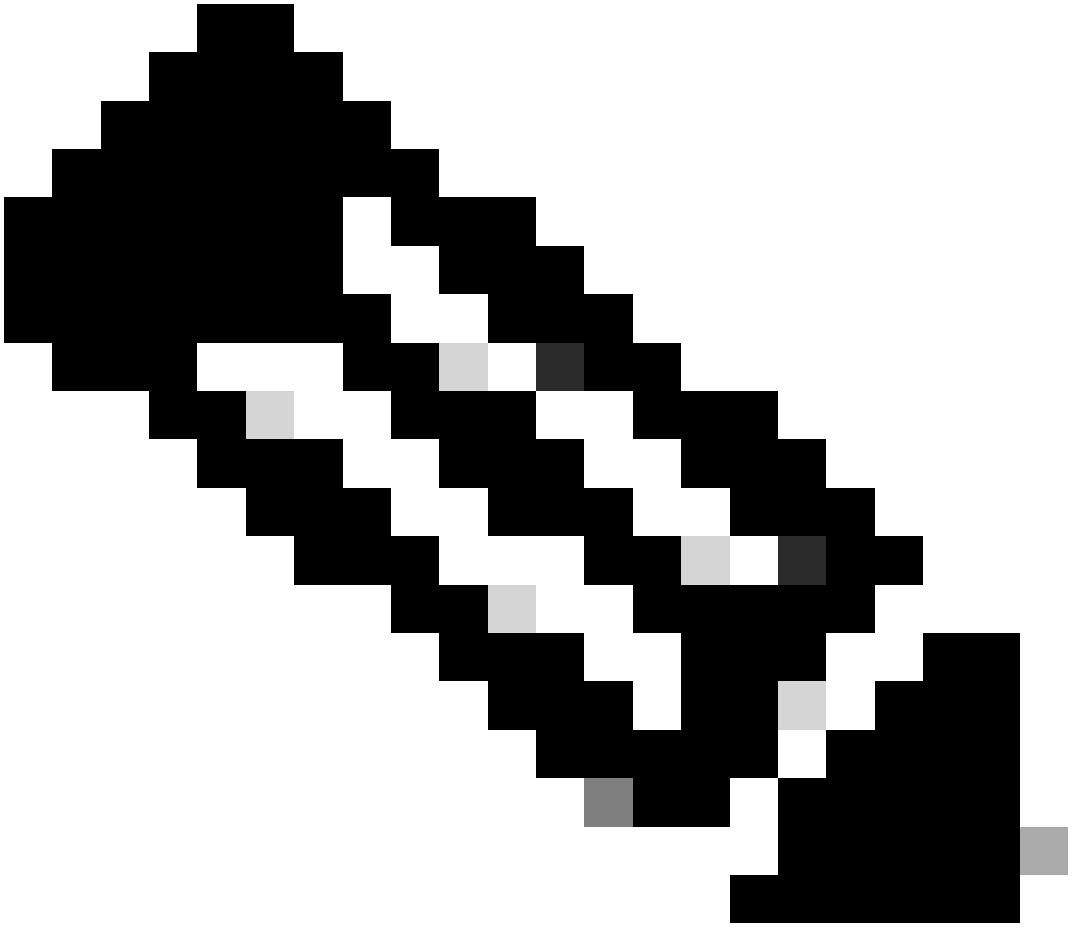


115014151543

Sie können die Integrationsinformationen auch auf der Seite Zusammenfassung der Sicherheitseinstellungen überprüfen.



20993269073556



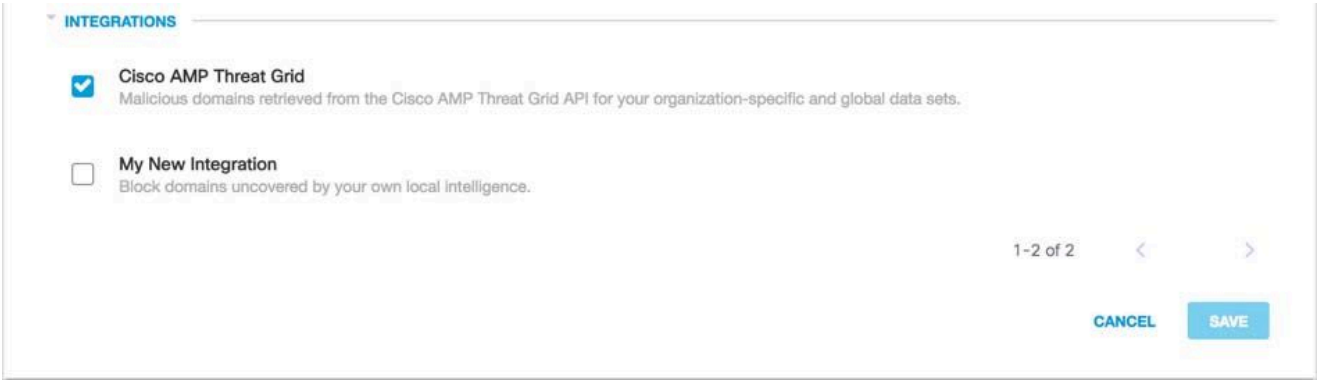
Anmerkung: Die Übernahme der Einstellungen kann bis zu fünf Minuten dauern. Wenn keine neuen Ereignisse in das Cisco Secure Malware Analytics (Threat Grid)-System eingespeist werden, werden der Integration möglicherweise keine neuen Domänen hinzugefügt.

Anwendung der Sicherheitseinstellung von Cisco Secure Malware Analytics (Threat Grid) im "Blockmodus" auf eine Richtlinie für verwaltete Clients

Wenn Sie diese Domänen für Clients blockiert haben, die von Cisco Umbrella verwaltet werden, ändern Sie die Sicherheitseinstellung in einer vorhandenen Richtlinie, oder erstellen Sie eine neue Richtlinie, die über Ihrer Standardrichtlinie liegt, um sicherzustellen, dass sie zuerst durchgesetzt wird.

1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Sicherheitseinstellungen.

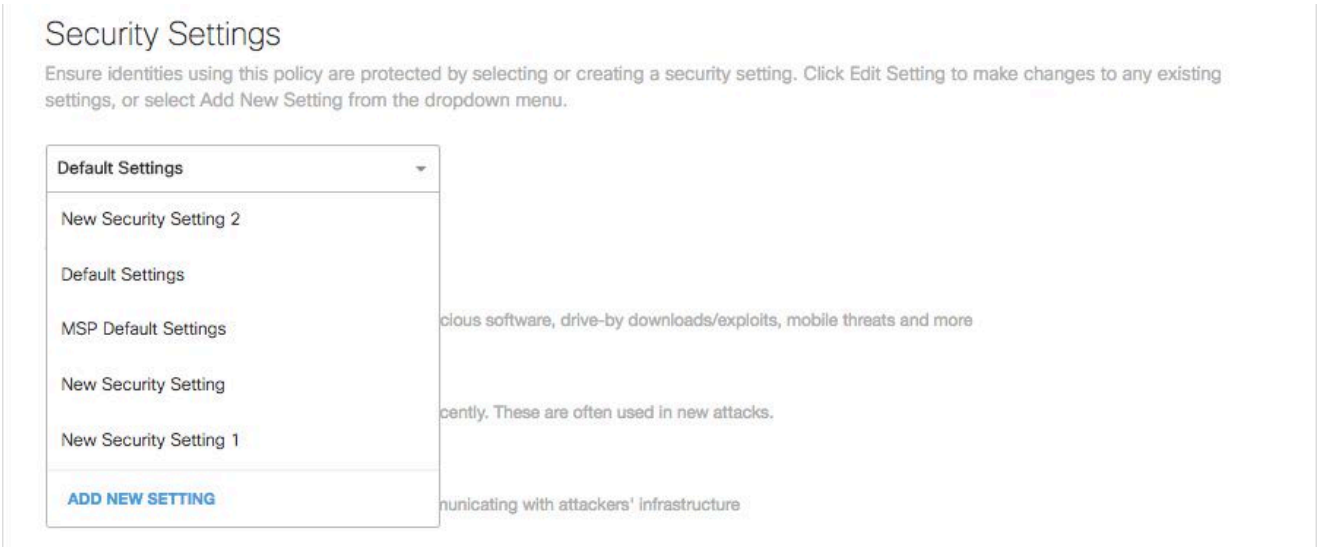
2. Überprüfen Sie unter Integrationen, ob das Kontrollkästchen "Cisco AMP Threat Grid" aktiviert ist. Andernfalls aktivieren Sie das Kontrollkästchen, und wählen Sie Speichern aus.



115013987086

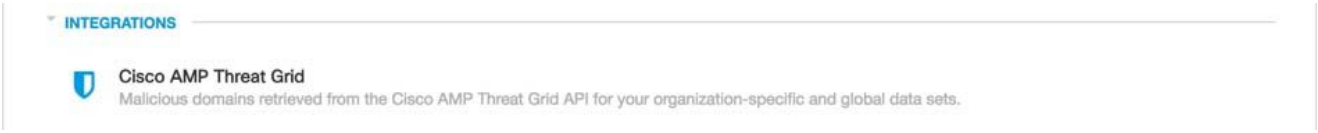
Fügen Sie anschließend im Cisco Umbrella Policy-Assistenten eine Sicherheitseinstellung zu der Richtlinie hinzu, die Sie bearbeiten:

1. Navigieren Sie zu Richtlinien > Verwaltung > Alle Richtlinien.
2. Erweitern Sie eine Richtlinie, und wählen Sie unter Sicherheitseinstellung angewendet die Option Bearbeiten aus.
3. Wählen Sie im Pulldown-Menü Security Settings (Sicherheitseinstellungen) eine Sicherheitseinstellung aus, die auch die Einstellung "Cisco AMP Threat Grid" (Cisco AMP Threat Grid) enthält.



20993282642708

Das Schildsymbol unter Integrationen wird auf blau aktualisiert.



4. Wählen Sie Festlegen und Zurücksenden.

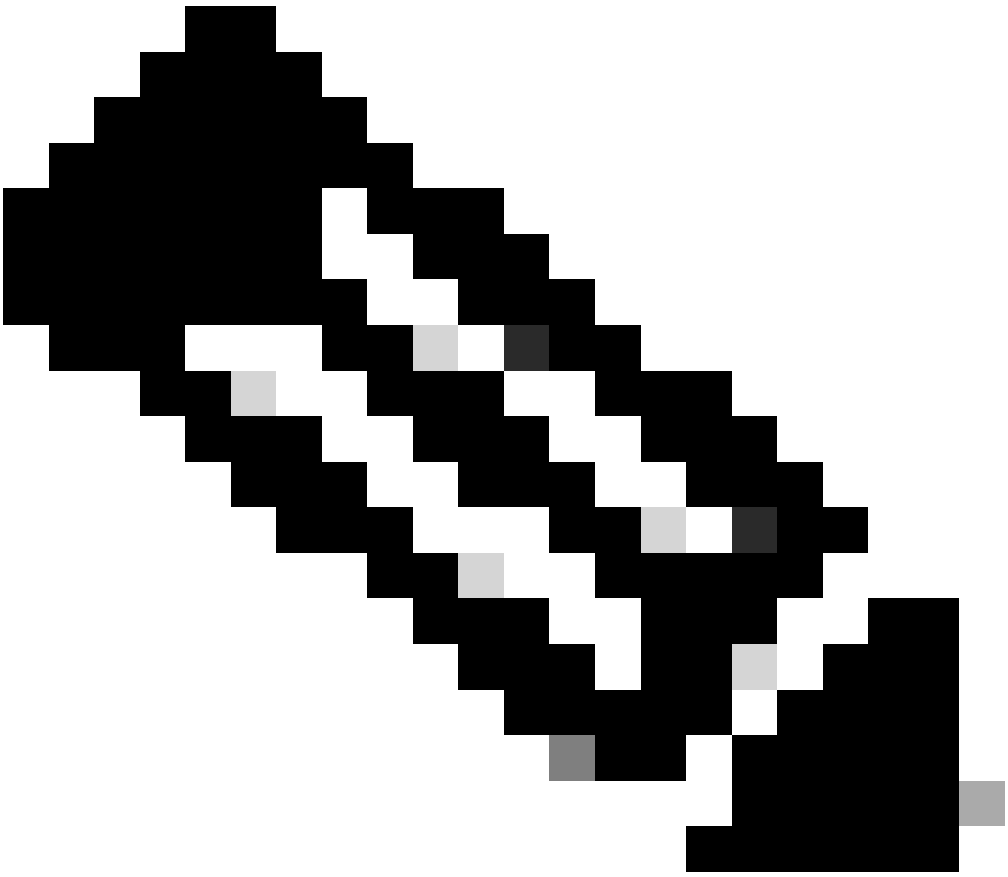
   Domänen von Cisco Secure Malware Analytics (Threat Grid), die in den Sicherheitseinstellungen für Cisco Secure Malware Analytics (Threat Grid) enthalten sind, werden für diese Identitäten mithilfe der Richtlinie blockiert.

Berichterstattung innerhalb von Cisco Umbrella für Cisco Secure Malware Analytics-Ereignisse

Berichte zu Cisco Secure Malware Analytics (Threat Grid)-Sicherheitsereignissen

Die Zielliste von Cisco Secure Malware Analytics (Threat Grid) ist eine der Listen mit Sicherheitskategorien, über die Sie Berichte erstellen können. Die meisten oder alle Berichte verwenden die Sicherheitskategorien als Filter. So können Sie beispielsweise Sicherheitskategorien filtern, um nur Aktivitäten im Zusammenhang mit Cisco Secure Malware Analytics (Threat Grid) anzuzeigen.

1. Navigieren Sie zu Reporting > Core Reports > Activity Search, und wählen Sie unter Security Categories "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) aus, um den Bericht zu filtern und nur die Sicherheitskategorie für Cisco Secure Malware Analytics (Threat Grid) anzuzeigen.



Anmerkung: Wenn die Cisco AMP Threat Grid-Integration deaktiviert ist, wird sie nicht im Filter "Sicherheitskategorien" angezeigt.

115014210123

2. Wählen Sie Anwenden aus.

Berichte über das Hinzufügen von Domänen zur Zielliste von Cisco Secure Malware Analytics (Threat Grid)

Das Cisco Umbrella Admin Audit-Protokoll enthält Ereignisse aus dem Cisco Secure Malware Analytics (Threat Grid) Dashboard, wenn Domänen zur Zielliste hinzugefügt werden. Ein Benutzer mit dem Namen "Cisco AMP Threat Grid Domain List", der ebenfalls mit dem Cisco Logo versehen ist, generiert die Ereignisse. Zu diesen Ereignissen gehören die hinzugefügte Domäne und der Zeitpunkt, zu dem sie hinzugefügt wurde.

Wenn Sie den Eintrag "Admin Audit Log" (Admin-Audit-Protokoll) auswählen, werden darin Details angezeigt, einschließlich der spezifischen Domäne, die hinzugefügt wurde.

Sie können Filter anwenden, um nur Cisco Secure Malware Analytics (Threat Grid)-Änderungen einzubeziehen, indem Sie einen Filter auf den Benutzer "Cisco AMP Threat Grid Domain List"

anwenden.

Umgang mit unerwünschten Erkennungen oder Fehlalarmen

Zwei Arten von Cisco Secure Malware Analytics (Threat Grid)-Erkennungen und zwei Auflösungen

Derzeit gibt es zwei Arten von Cisco Secure Malware Analytics (Threat Grid)Blöcken: Eine mit einer möglichen Auflösung und eine zweite mit einer aktuellen Auflösung zu einer unerwünschten Erkennung.

1. Global Threat Grid-Eintrag (öffentlich): Zu diesem Zeitpunkt besteht die einzige Möglichkeit, die Domäne zuzulassen, darin, sie Ihrer Zulassungsliste hinzuzufügen.
2. Nur Kunden-Feed (privat): Kann mit einem Eintrag in der Zulassungsliste oder einem Löschvorgang in der Integrationsliste von AMP Threat Grid adressiert werden.

Zulassungslisten

Es ist zwar unwahrscheinlich, aber es ist möglich, dass Domänen, die automatisch durch die Integration von Cisco Secure Malware Analytics (Threat Grid) hinzugefügt werden, möglicherweise eine unerwünschte Erkennung auslösen, die Ihre Benutzer am Zugriff auf bestimmte Websites hindert. In einer solchen Situation wird empfohlen, die Domäne(n) einer Zulassungsliste hinzuzufügen (Richtlinien > Ziellisten), die Vorrang vor allen anderen Typen von Sperrlisten hat, einschließlich der Sicherheitseinstellungen.

Es gibt zwei Gründe, warum dieser Ansatz bevorzugt wird. Wenn das Dashboard von Cisco Secure Malware Analytics (Threat Grid) die Domäne nach dem Entfernen erneut hinzufügen sollte, schützt die Zulassungsliste vor weiteren Problemen. Zweitens zeigt die Zulassungsliste einen Verlaufsdatensatz problematischer Domänen an, die für forensische oder Auditberichte verwendet werden können.

Standardmäßig gibt es eine globale Zulassungsliste, die auf alle Richtlinien angewendet wird. Durch Hinzufügen einer Domäne zur globalen Zulassungsliste wird die Domäne in allen Richtlinien zugelassen.

Wenn die Sicherheitseinstellung von Cisco Secure Malware Analytics (Threat Grid) im Blockmodus nur auf eine Teilmenge Ihrer verwalteten Cisco Umbrella-Identitäten angewendet wird (z. B. nur auf Roaming-Computer und mobile Geräte), können Sie eine spezifische Zulassungsliste für diese Identitäten oder Richtlinien erstellen.

So erstellen Sie eine Zulassungsliste:

1. Navigieren Sie zu Policies > Policy Components > Destination Lists, und wählen Sie 

25463394696852

("Hinzufügen").
2. Wählen Sie Zulassen aus, und fügen Sie Ihre Domäne zur Liste hinzu.
3. Wählen Sie Speichern aus.

Nachdem die Liste gespeichert wurde, können Sie sie einer vorhandenen Richtlinie hinzufügen, die die Clients abdeckt, die von der unerwünschten Sperre betroffen sind.

Löschen von Domänen aus der Zielliste von Cisco Secure Malware Analytics (Threat Grid)

Neben jedem Domänennamen in der Liste von Cisco Secure Malware Analytics (Threat Grid) befindet sich ein Symbol ("Löschen"). Durch das Löschen von Domänen können Sie die Cisco Secure Malware Analytics (Threat Grid)-Zielliste bereinigen, wenn eine unerwünschte Erkennung auftritt.

Der Löschvorgang ist nicht dauerhaft, wenn das Cisco Secure Malware Analytics (Threat Grid)-Dashboard die Domäne erneut an Cisco Umbrella senden würde.

1. Navigieren Sie zu Policies > Policy Components > Integrations (Richtlinien > Richtlinienkomponenten > Integrationen), und wählen Sie "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) aus, um das Fenster zu erweitern.
2. Wählen Sie Siehe Domänen aus.
3. Suchen Sie nach dem Domänennamen, den Sie löschen möchten.
4. Wählen Sie das Symbol ("Löschen") aus.
5. Wählen Sie Schließen aus.
6. Wählen Sie Speichern aus.

Im Fall einer unerwünschten Erkennung oder eines Fehlalarms empfehlen wir, sofort eine Zulassungsliste in Cisco Umbrella zu erstellen und den Fehlalarmen im Cisco Secure Malware Analytics (Threat Grid) Dashboard zu beheben. Später können Sie die Domäne aus der Zielliste von Cisco Secure Malware Analytics (Threat Grid) entfernen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.