Integration von Cisco SecureX in Cisco Umbrella

Inhalt

Einleitung

In diesem Dokument wird der Prozess zur Konfiguration und Verifizierung der Umbrella-Integration mit SecureX über die drei verfügbaren APIs beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Umbrella
- Cisco Secure X
- Cisco Threat Response

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Umbrella-Konto mit DNS Advantage-Lizenz
- Sicheres X

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Um diese Integration mit all ihren Funktionen vollständig zu konfigurieren, benötigen Sie Zugriff auf diese 3 APIs

- Reporting-API (in allen Lizenzen enthalten)
- Durchsetzungs-API
- Analyse-API

Um die Umbrella-Integration zu konfigurieren, müssen Sie zuerst einige Informationen von Ihren Umbrella-Instanzen sammeln und dann das Formular Neues Umbrella-Modul hinzufügen ausfüllen.

Konfigurieren

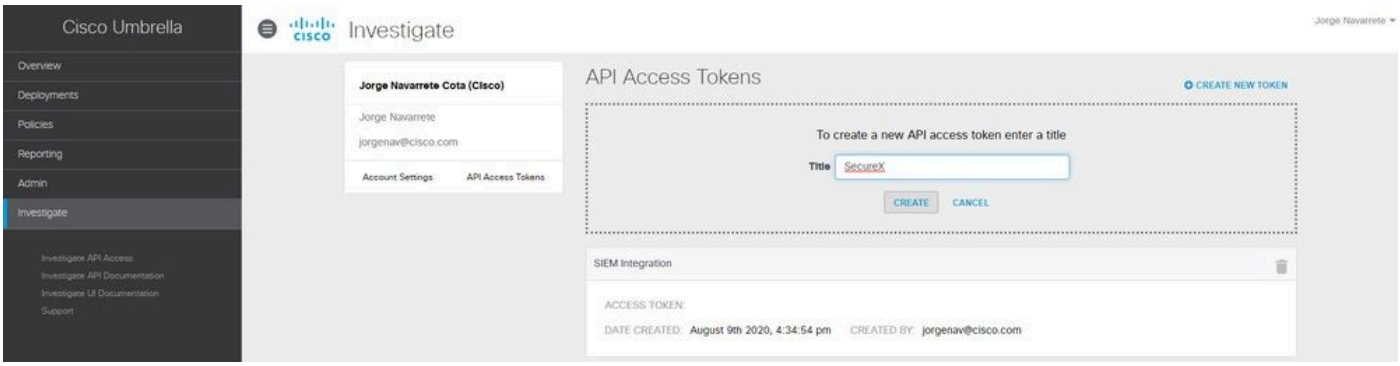
Modul erstellen

1. Melden Sie sich bei Ihrem Secure X-Konto an. Wenn Sie noch kein Konto haben, können Sie ein Konto mit Cisco Secure Sign-On erstellen.
2. Navigieren Sie zu Integrationen > Neues Modul hinzufügen. Scrollen Sie auf der Seite Verfügbare Integrationen nach unten zur Option Umbrella, und klicken Sie auf Neues Modul hinzufügen.

Führen Sie diese Schritte aus, um die erforderlichen Informationen von Ihrem Umbrella-Konto zu sammeln und im Formular Add New Umbrella Module (Neues Umbrella-Modul hinzufügen) einzureichen.

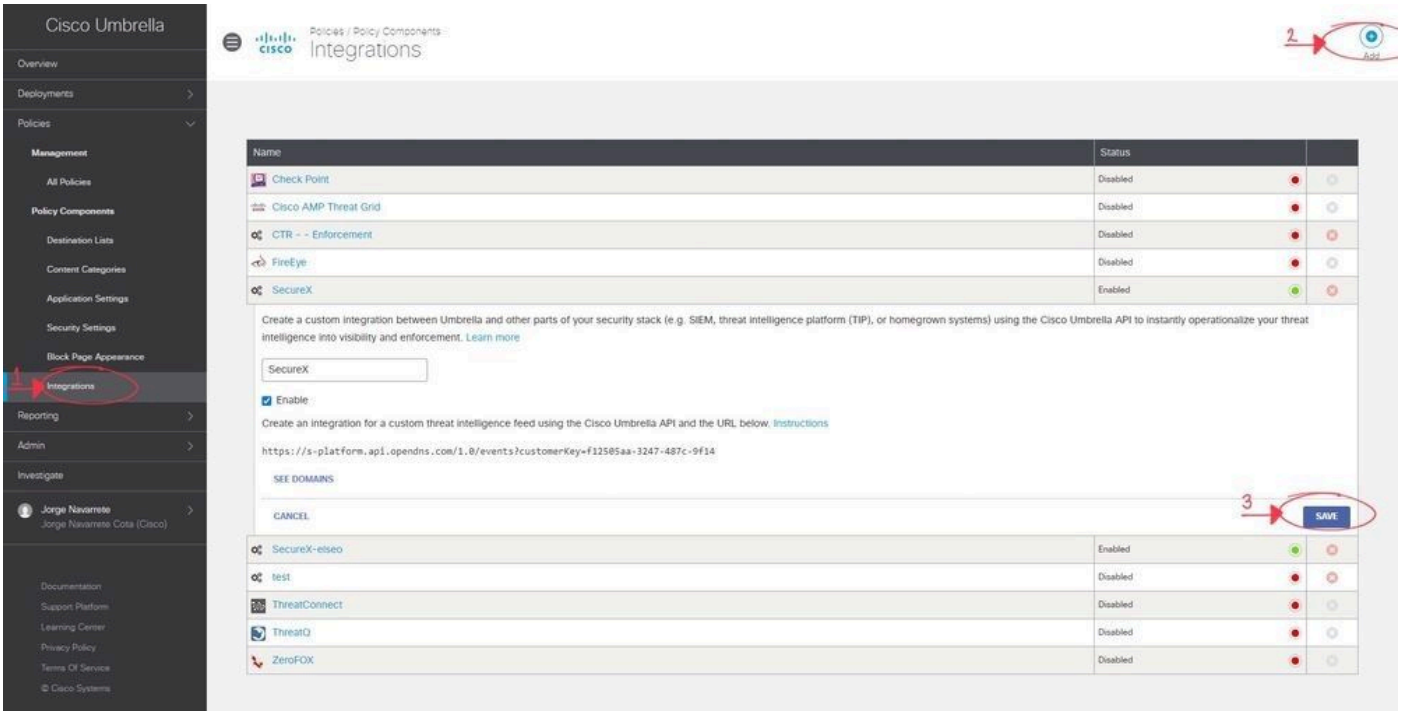
Analyse-API

1. Navigieren Sie in Umbrella zu Investigate > Investigate API Access, klicken Sie auf Create New Token (Neues Token erstellen), geben Sie einen Titel für das Token ein, und klicken Sie dann erneut auf Create New Token (Neues Token erstellen).
2. Kopieren Sie den Wert des Zugriffstokens in das Feld "API-Token" im Formular "Neues Umbrella-Modul hinzufügen".



Durchsetzungs-API

1. Navigieren Sie in Umbrella zu Richtlinien > Richtlinienkomponenten > Integrationen, klicken Sie auf Hinzufügen, geben Sie einen Namen ein, und klicken Sie auf Erstellen.
2. Klicken Sie auf den neu erstellten Integrationsnamen, aktivieren Sie das KontrollkästchenAktivieren, undSpeichern.
3. Klicken Sie auf den Integrationsnamen, um die Integrations-URL anzuzeigen. Kopieren Sie die Integrations-URL in das Feld Custom Umbrella Integration URL (URL für die benutzerdefinierte Umbrella-Integration) auf dem Formular Add New Umbrella Module (Neues Umbrella-Modul hinzufügen).



Hinweis: Um die Umbrella Enforcement API zu integrieren, müssen Sie ein Administrator in einer eigenständigen Umbrella-Organisation oder einer untergeordneten Organisation sein, anstatt ein Administrator einer Umbrella-Konsole.

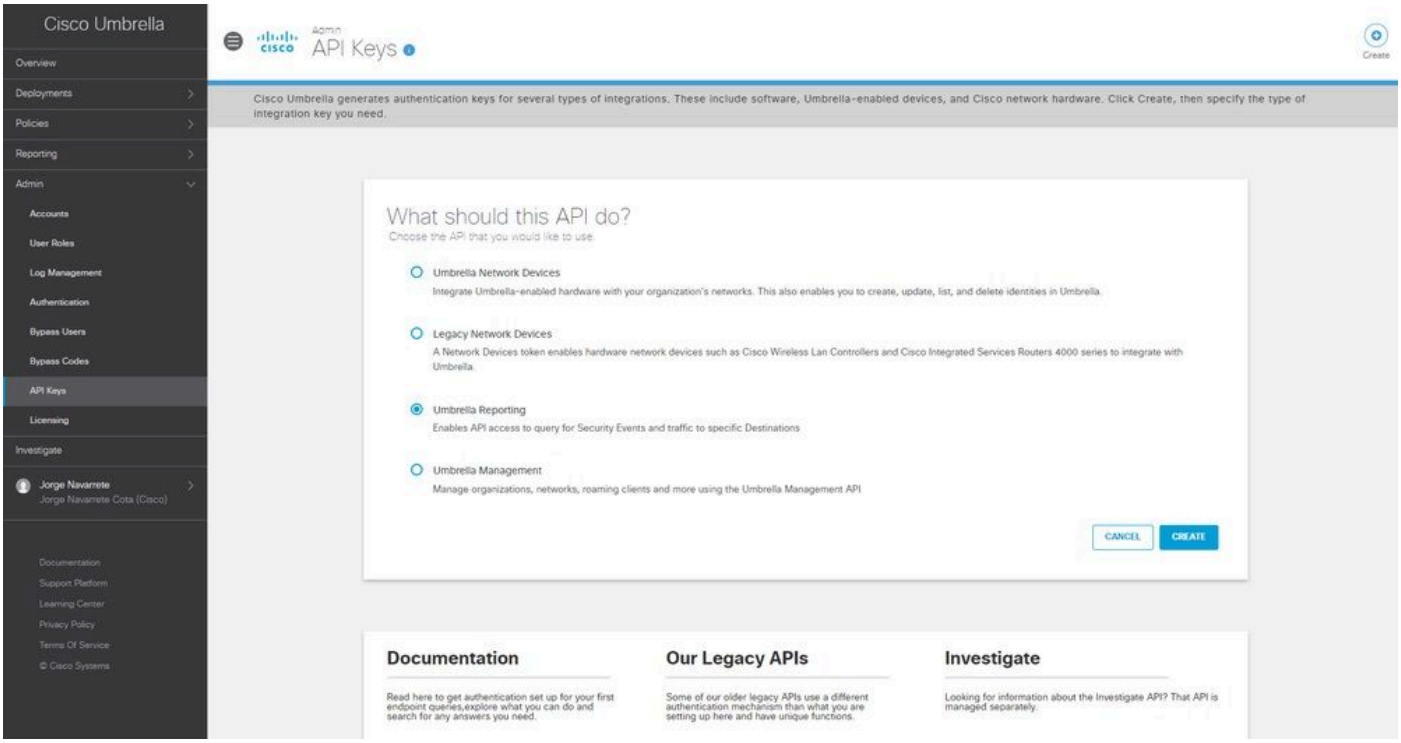
Reporting-API

1. Navigieren Sie in Umbrella zu Admin > API Keys, und klicken Sie auf Create (Erstellen).

2. Klicken Sie unter Was soll diese API tun? auf das Optionsfeld Umbrella Reporting und dann auf Create (Erstellen).

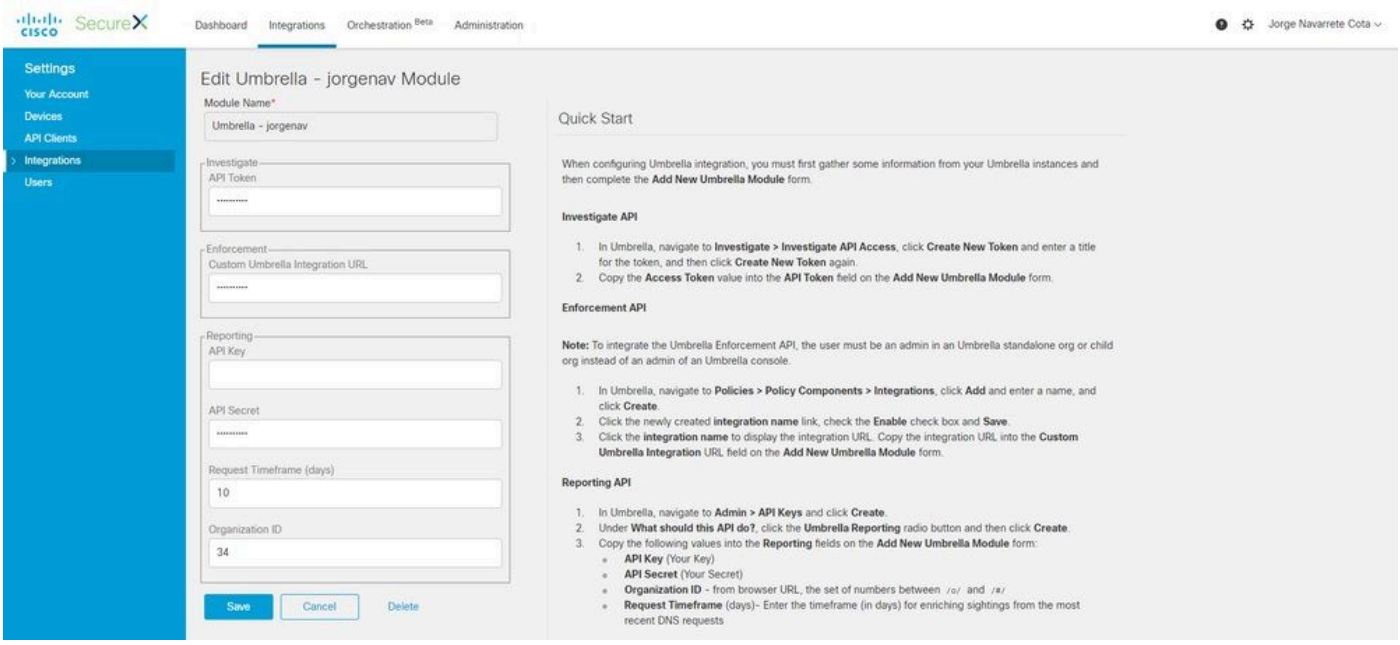
3. Kopieren Sie die nächsten Werte in die Felder Reporting auf dem Formular Add New Umbrella Module:

    - API-Schlüssel (Ihr Schlüssel)
    - API-Schlüssel (Ihr Schlüssel)
    - Organisations-ID - aus der Browser-URL die Anzahl der Nummern zwischen`/o/`und`/#/`
    - Anforderungszeitrahmen (Tage) - Geben Sie den Zeitrahmen (in Tagen) für die Bereicherung der Sichtungen der letzten DNS-Anfragen ein.



Modul speichern

1. Füllen Sie die API-Informationen in Ihrem Umbrella-Modul, klicken Sie auf Speichern.

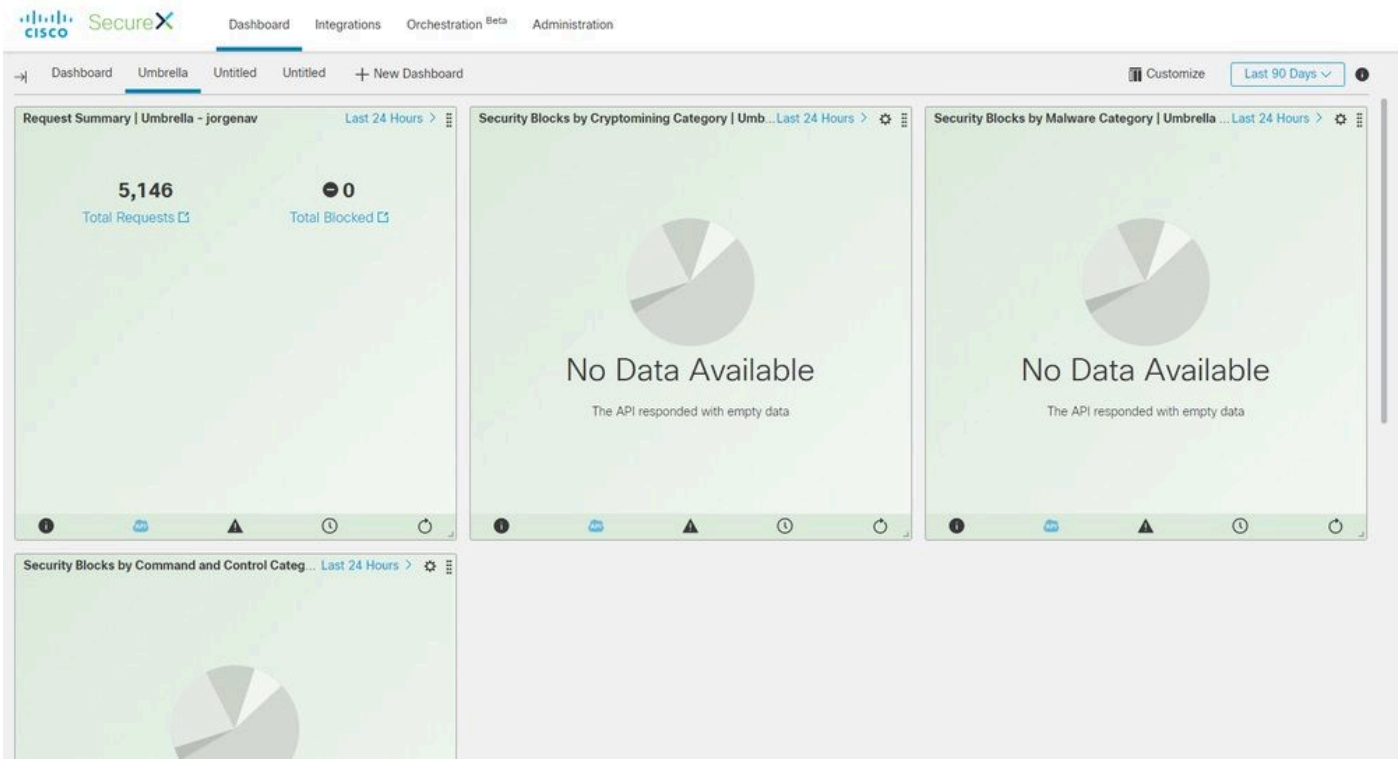


SecureX Dashboard erstellen

1. Nachdem Sie Ihr Modul hinzugefügt haben, können Sie zu Secure X navigieren und ein neues Dashboard erstellen.

2. Wählen Sie unter den verfügbaren Dashboards Ihr Umbrella-Modul aus, und fügen Sie die Kategorien hinzu, die Sie sehen möchten.

3. Klicken Sie auf Speichern, und sehen Sie Ihre Informationen über die API aufgefüllt.



Überprüfung

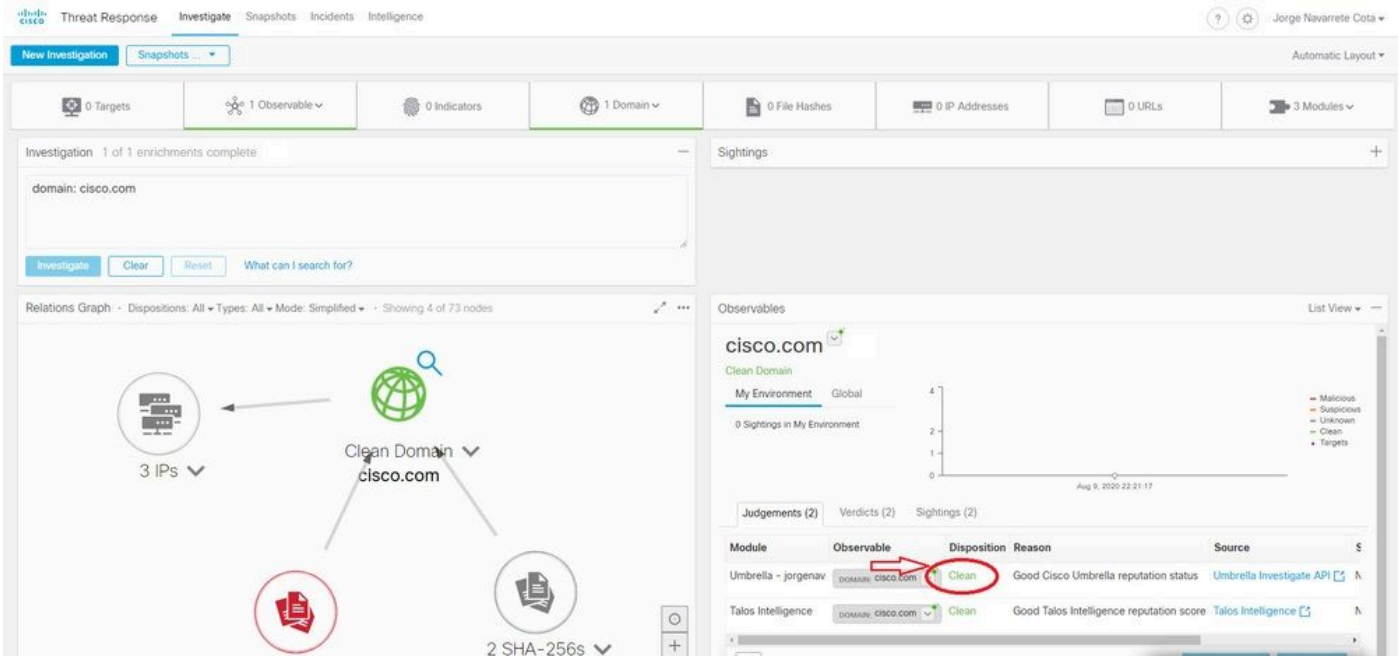
Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

untersuchen

Mit der Investigate-API können Sie einen Feed zu einer CTR-Untersuchung hinzufügen, um die Disposition einer Domäne zu sehen und die Untersuchung mit anderen Modulen zu bereichern.

1. Um diese Integration zu überprüfen, führen Sie eine neue Untersuchung in Cisco Threat Response durch. Eine Disposition von Umbrella kann mit einer Suche nach einer bekannten Domain, wie cisco.com, gefunden werden.

2. Wenn Sie im Beziehungsdiagramm unter die Domäne klicken, können Sie von dort auch zum Investigate Dashboard in Umbrella wechseln.

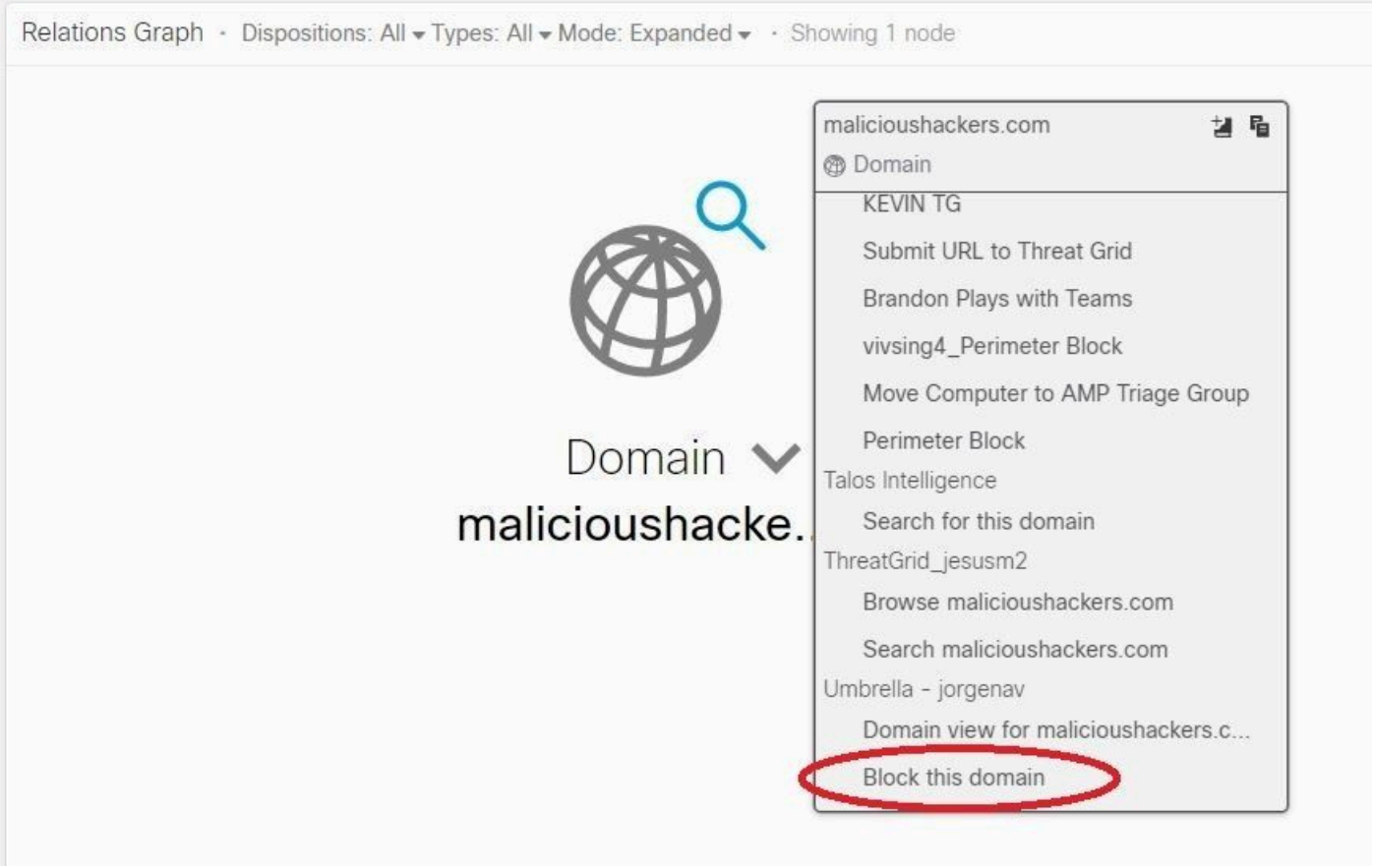


Durchsetzung

Mit der Durchsetzungs-API können Sie eine Domäne direkt bei einer Untersuchung blockieren oder die Blockierung aufheben.

1. Um zu überprüfen, ob die API funktioniert, können Sie eine Domäne blockieren, die in einer Untersuchung zu sehen ist und die Domäne zur Richtlinienblockliste in Umbrella hinzufügt.

2. Um zu überprüfen, ob die URL der Sperrliste hinzugefügt wurde, navigieren Sie zu Policies > Policy Components > Integrations. Wählen Sie Ihre SecureX-Integration aus, und klicken Sie auf Domains anzeigen. Es wird ein Fenster mit den hinzugefügten Domänen aus CTR angezeigt.



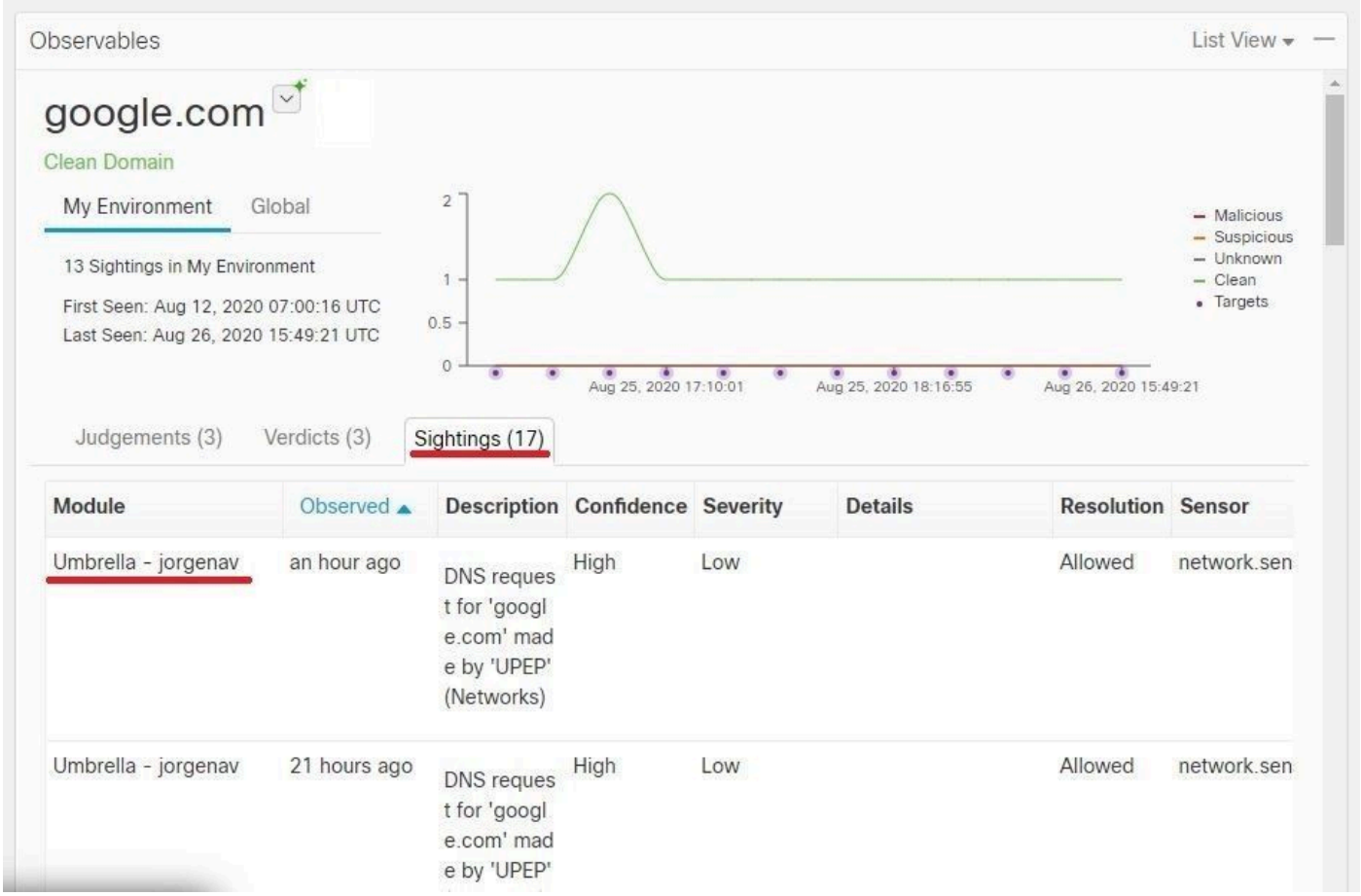
3. Wenn die Domänen nicht blockiert sind, navigieren Sie in Ihrem Umbrella Dashboard zu Richtlinien > Richtlinienkomponenten > Sicherheitseinstellungen. Stellen Sie unter Integrationen sicher, dass Sie Ihre gewünschte Liste angewendet haben.

Berichterstellung

Über die Reporting-API können Sie die Informationen Ihrer Umbrella-Bereitstellungen in SecureX anzeigen.

Sie können die Integration einer bekannten Domäne in Ihre CTR-Umgebung bei einer Untersuchung überprüfen.

In der CTR-Untersuchung wird die Liste der Computer, die auf eine bestimmte Domäne zugegriffen haben, unter Sichtungen angezeigt.



Video

Die Konfigurationsinformationen in diesem Artikel finden Sie in diesem Video.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

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.