Integrazione di Cisco SecureX con Cisco Umbrella

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione e verifica dell'integrazione di Umbrella con SecureX con le 3 API disponibili.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Umbrella
- Cisco Secure X
- Cisco Threat Response

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Account Umbrella con licenza DNS Advantage
- Secure X

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per configurare completamente l'integrazione con tutte le funzionalità, è necessario accedere alle 3 API

- API di reporting (inclusa in tutte le licenze)
- API di imposizione
- Analizza API

Per configurare l'integrazione Umbrella, è necessario innanzitutto raccogliere alcune informazioni dalle istanze Umbrella e quindi completare il modulo Aggiungi nuovo modulo Umbrella.

Configurazione

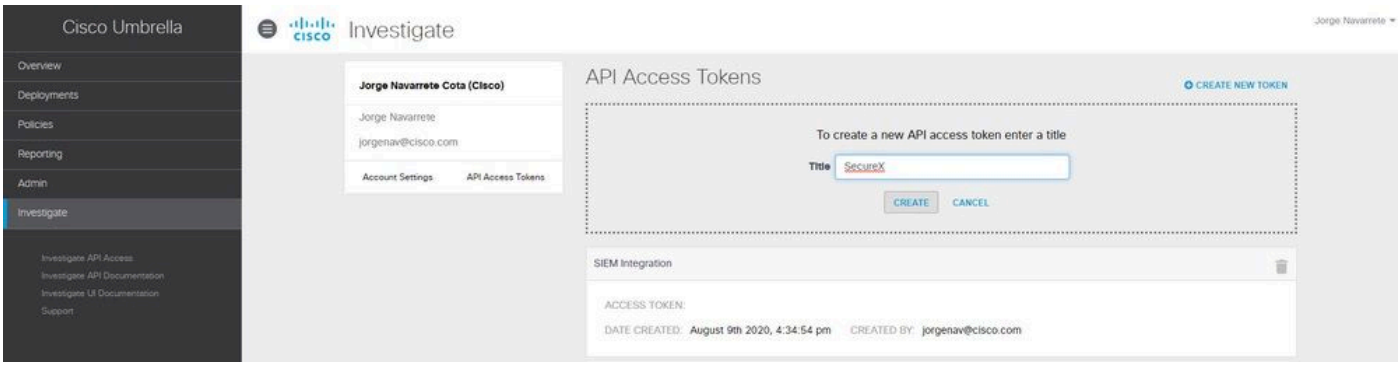
Crea modulo

1. Accedere all'account Secure X. Se non si dispone ancora di un account, è possibile crearne uno con Cisco Secure Sign-On.
2. Passare a Integrations > Add New Module (Integrazioni > Aggiungi nuovo modulo). Nella pagina Integrazioni disponibili scorrere verso il basso fino all'opzione Umbrella e fare clic su Aggiungi nuovo modulo.

Utilizzare questi passaggi per raccogliere le informazioni necessarie dal proprio account Umbrella da inviare nel modulo Aggiungi nuovo modulo Umbrella.

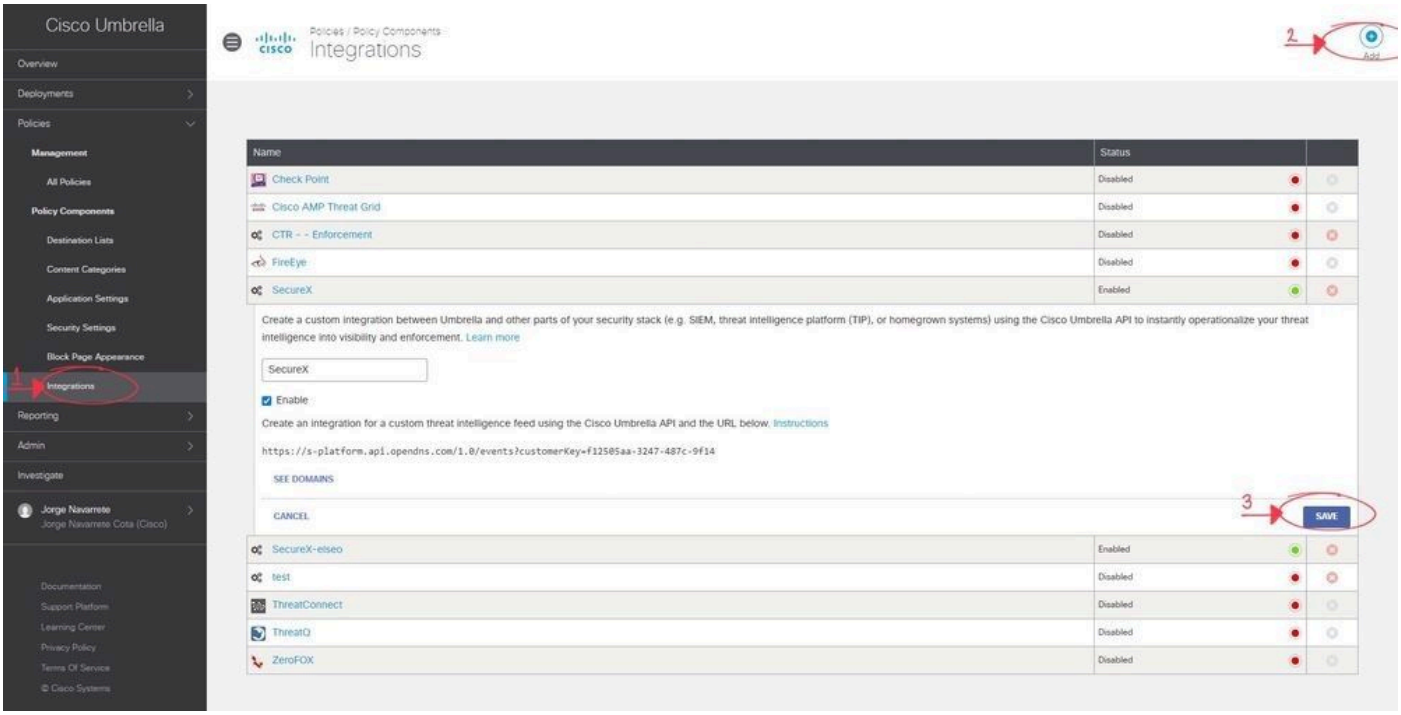
Analizza API

1. In Umbrella, selezionare Indaga > Indaga sull'accesso all'API, fare clic su Crea nuovo token, immettere un titolo per il token e quindi fare di nuovo clic su Crea nuovo token.
2. Copiare il valore del token di accesso nel campo Token API della maschera Aggiungi nuovo modulo Umbrella.



API di imposizione

1. In Umbrella, passare a Criteri > Componenti criterio > Integrazioni, fare clic su Aggiungi e immettere un nome, quindi fare clic su Crea.
2. Fare clic sul nuovo collegamento nome integrazione, selezionare la casella di controllo Abilita e quindi fare clic su Salva.
3. Fare clic sul nome dell'integrazione per visualizzare l'URL di integrazione. Copiare l'URL di integrazione nel campo Custom Umbrella Integration URL del modulo Add New Umbrella Module.



Nota: per integrare l'API di applicazione Umbrella, è necessario essere un amministratore in un'organizzazione Umbrella standalone o un'organizzazione figlio anziché un amministratore di una console Umbrella.

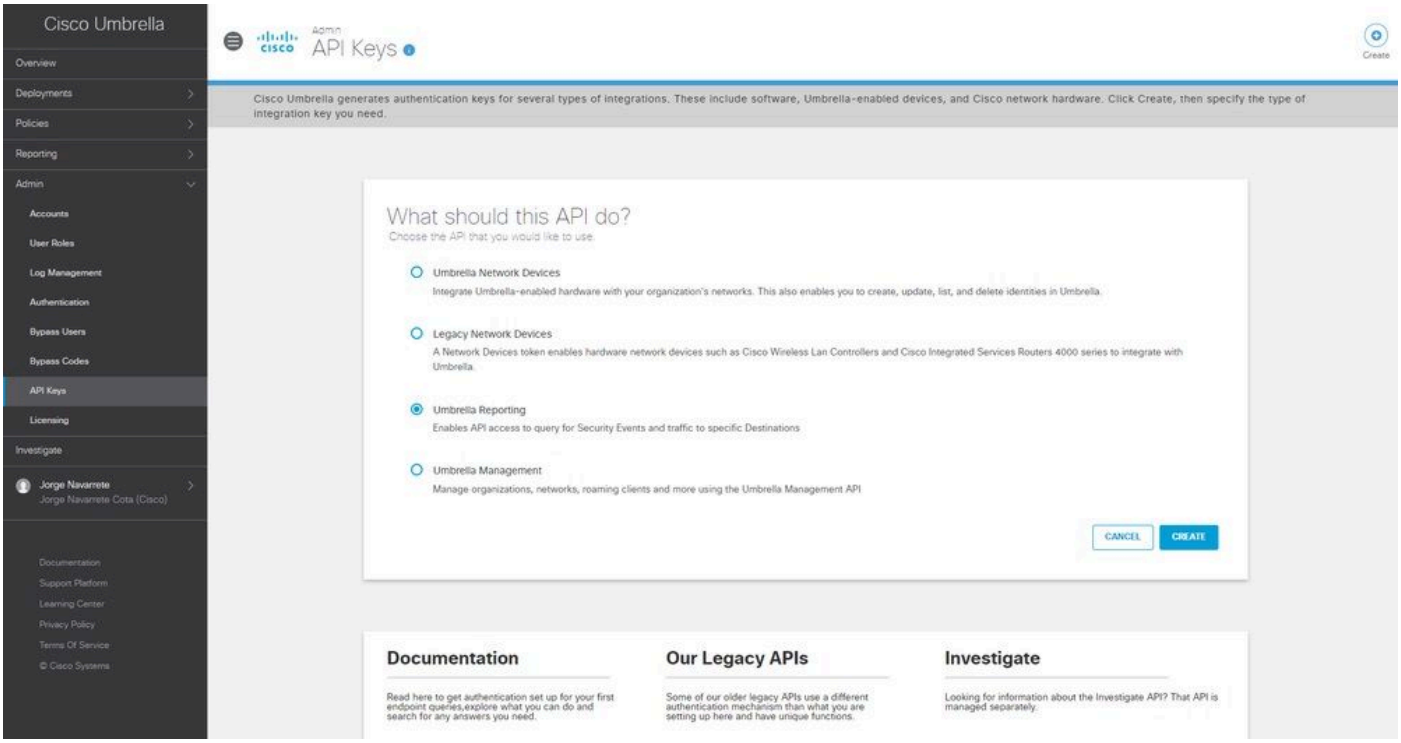
API di reporting

1. In Umbrella, selezionare Admin > API Keys (Amministratore > Chiavi API), quindi fare clic su Create (Crea).

2. In Funzionamento dell'API fare clic sul pulsante di opzione Umbrella Reporting e quindi su Crea.

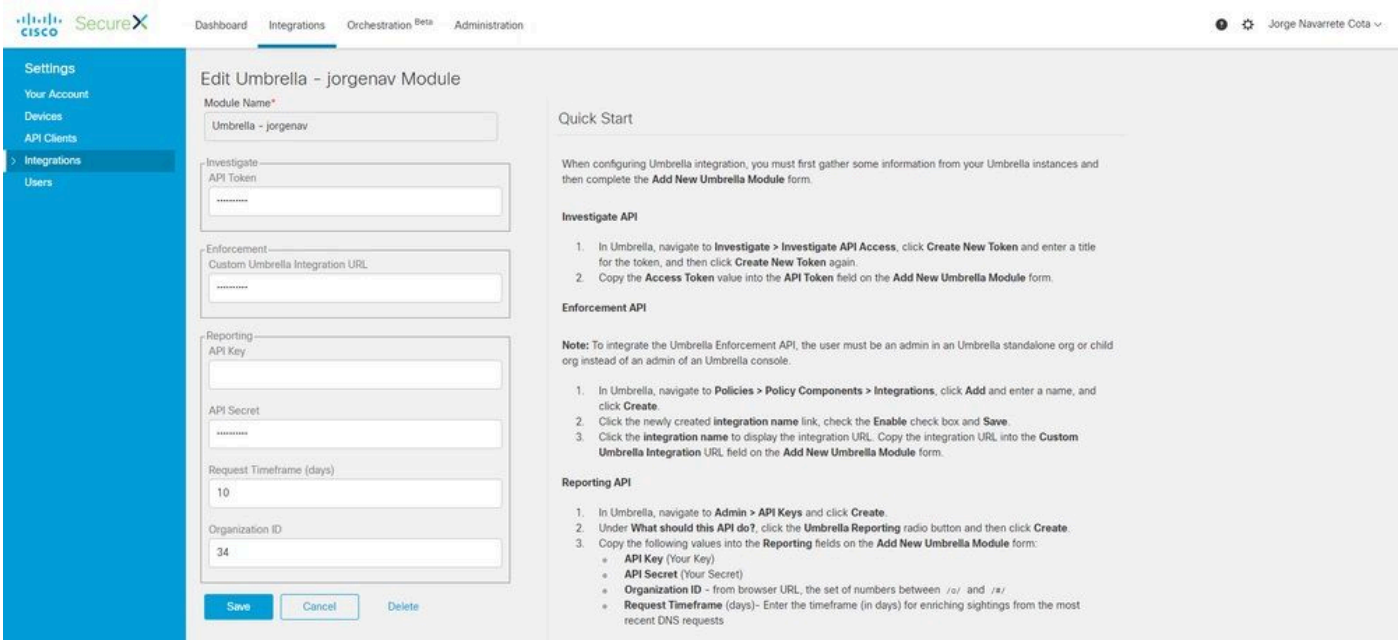
3. Copiare i valori successivi nei campi Reporting del modulo Aggiungi nuovo modulo Umbrella:

    - Chiave API (la chiave)
    - Segreto API (segreto personale)
    - ID organizzazione: dall'URL del browser, l'insieme di numeri tra`/o/e/#/`
    - Tempo di richiesta (giorni): immettere il tempo (in giorni) per l'arricchimento degli avvistamenti dalle richieste DNS più recenti



Salva modulo

1. Compilare le informazioni API nel modulo Umbrella, quindi fare clic su Salva.

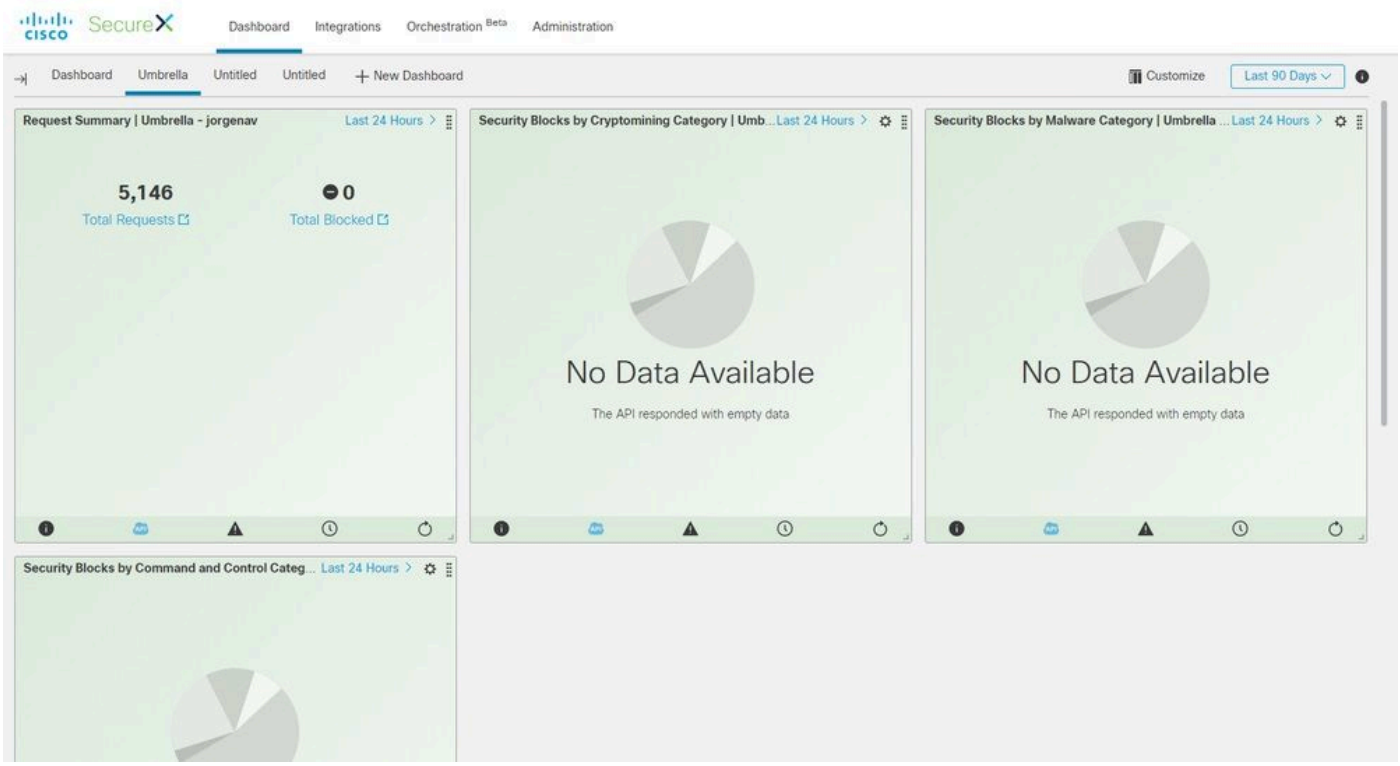


Crea dashboard SecureX

1. Una volta aggiunto il modulo, è possibile passare a Secure X e creare un nuovo dashboard.

2. Sotto i dashboard disponibili, selezionare il modulo Umbrella e aggiungere le categorie che si è interessati a vedere.

3. Fare clic su Save (Salva) per visualizzare le informazioni inserite tramite l'API.



Verifica

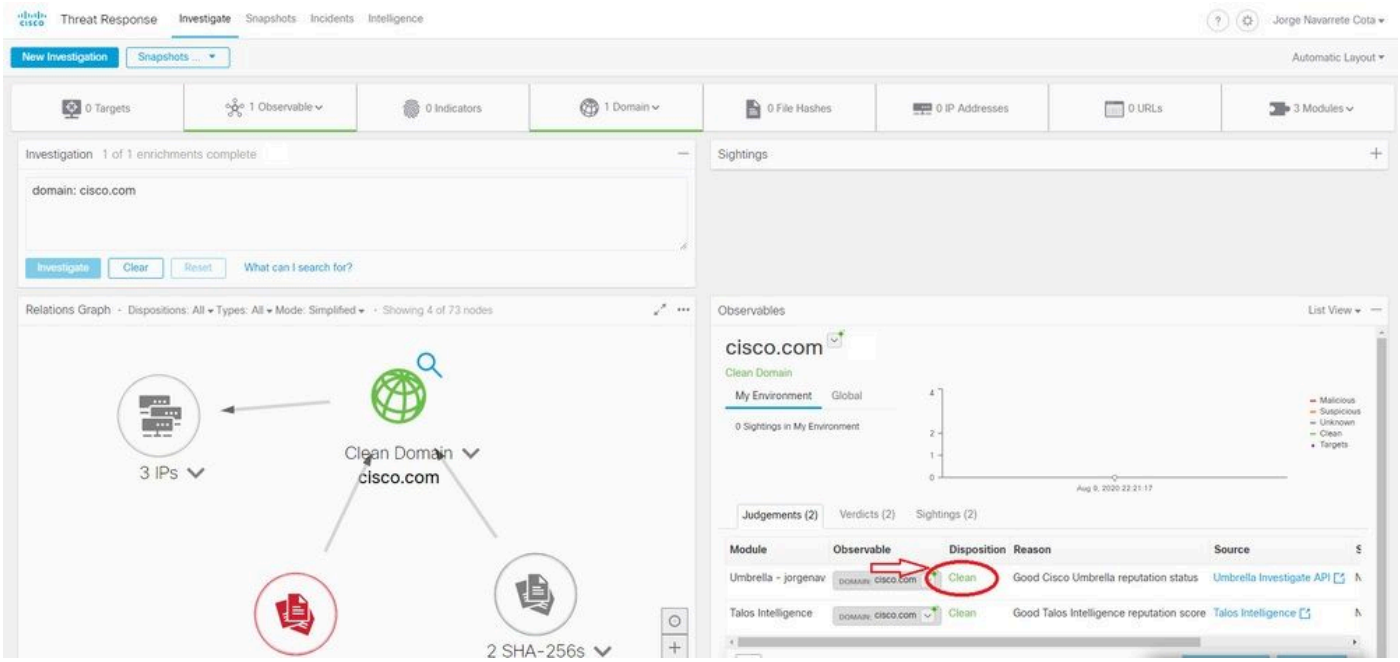
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Indaga

L'API Investigate consente di aggiungere un feed a un'indagine CTR, di visualizzare la disposizione di un dominio e di arricchire l'indagine con altri moduli.

1. Per verificare questa integrazione, eseguire una nuova indagine in Cisco Threat Response. Una disposizione fornita da Umbrella può essere trovata con una ricerca per un dominio noto, come cisco.com.

2. Se si fa clic sotto il dominio nel Grafico relazioni, è possibile eseguire il pivot da lì al Dashboard investigativo in Umbrella.

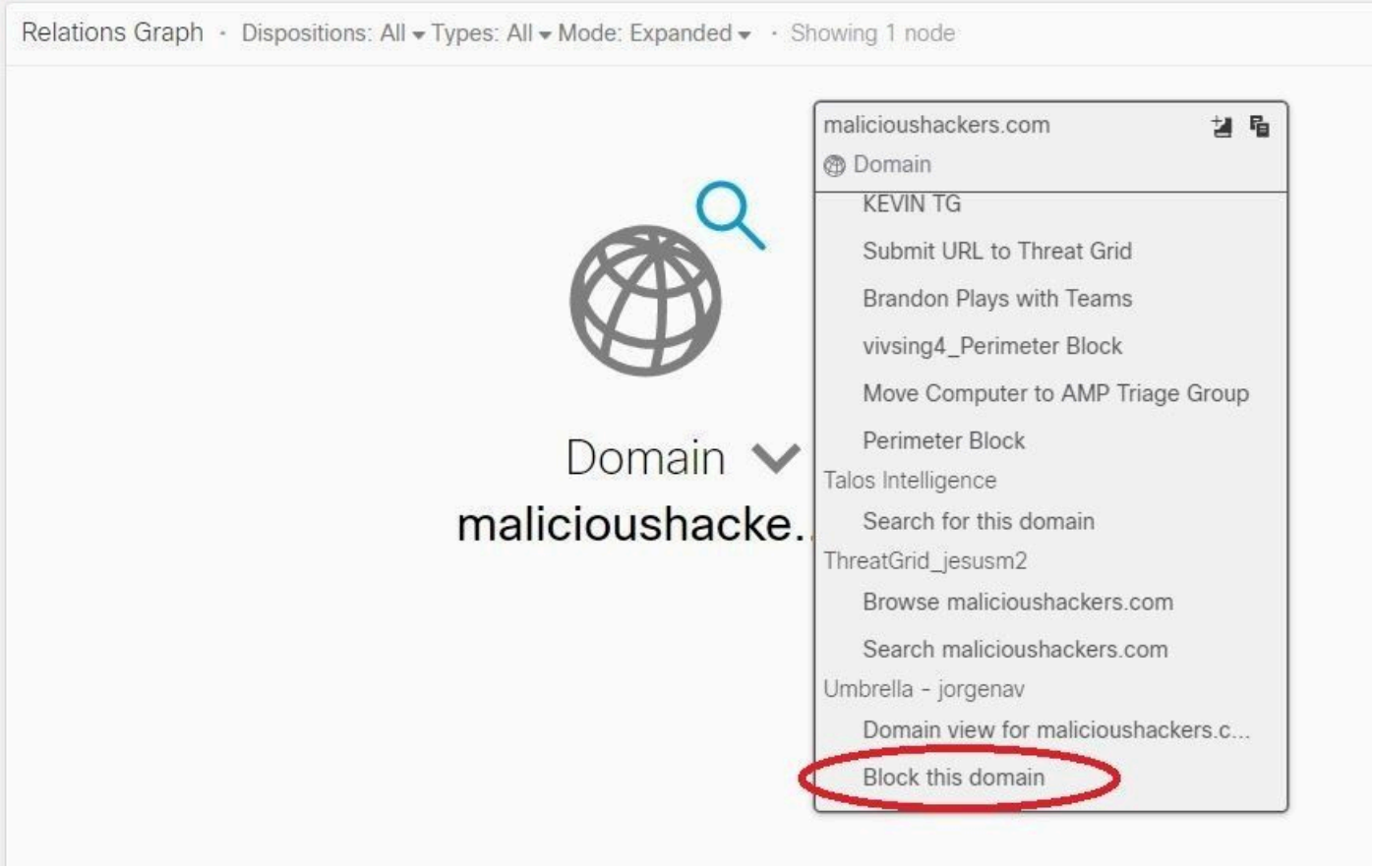


Applicazione

L'API di imposizione consente di bloccare o sbloccare un dominio direttamente da un'indagine.

1. Per verificare il funzionamento dell'API, è possibile bloccare un dominio visualizzato in un'indagine e che aggiunge il dominio all'elenco di blocco dei criteri in Umbrella.

2. Per verificare che l'URL sia stato aggiunto all'elenco di indirizzi bloccati, passare a Policy > Componenti dei criteri > Integrazioni. Selezionare l'integrazione SecureX e fare clic su Vedere domini. Una finestra visualizza i domini aggiunti da CTR.



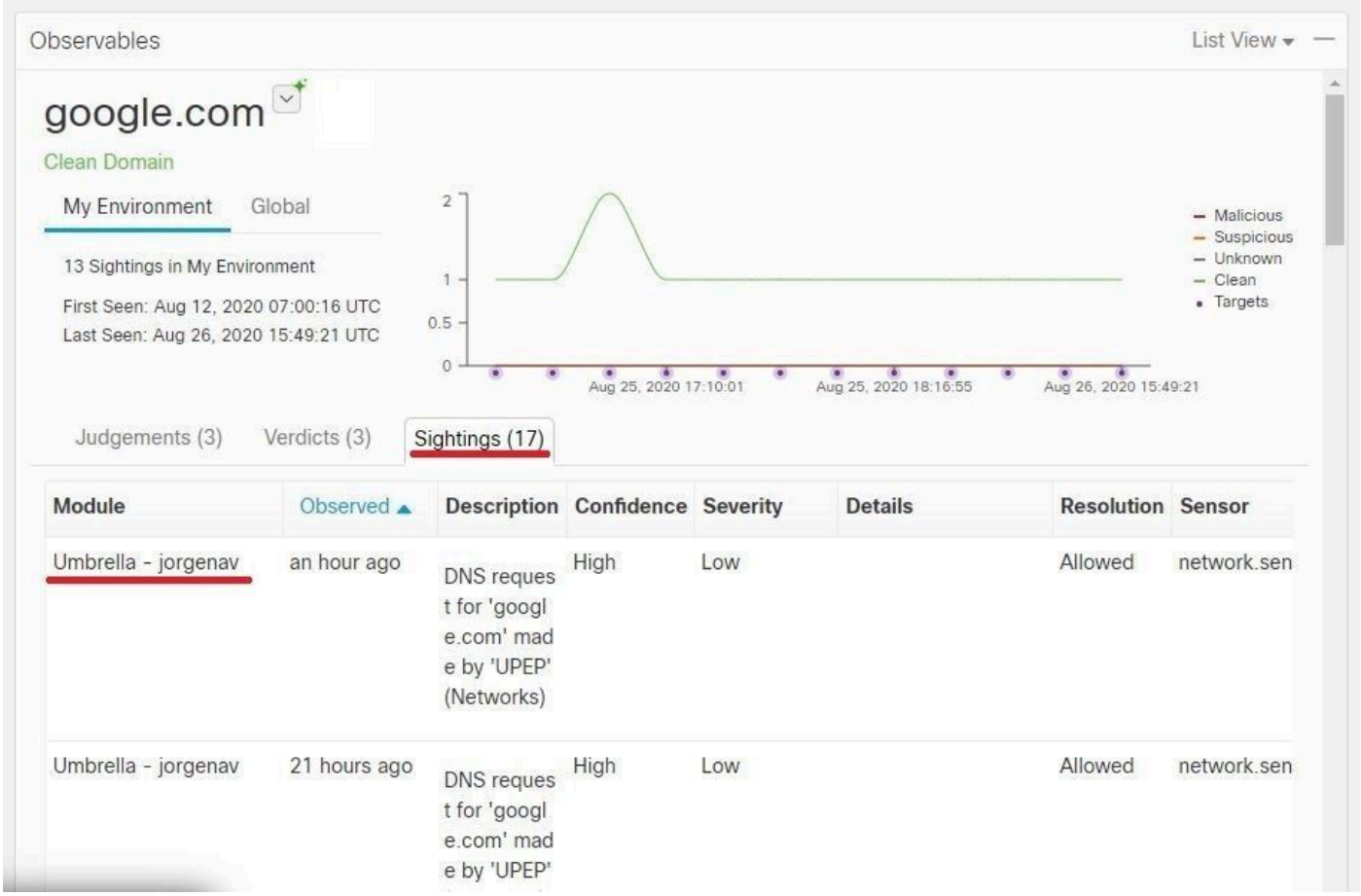
3. Se i domini non sono bloccati, nel dashboard Umbrella passare a Criteri > Componenti criterio > Impostazioni di protezione. In Integrazioni assicurarsi di aver applicato l'elenco desiderato.

Creazione di report

L'API Reporting consente di visualizzare le informazioni delle distribuzioni Umbrella all'interno di SecureX.

È possibile verificare l'integrazione con un'analisi di un dominio che si sa essere stato visto nel proprio ambiente in CTR.

Nell'Indagine CTR, l'elenco dei computer che hanno avuto accesso a un particolare dominio è visualizzato in Avvistamenti.



Video

Le informazioni di configurazione contenute in questo articolo sono disponibili in questo video.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).