Configurazione dell'integrazione di Secure Malware Analytics (in precedenza Threat Grid) con Umbrella

Sommario

Introduzione

In questo documento viene descritto come integrare Secure Malware Analytics (in precedenza Threat Grid) con Umbrella.

Panoramica dell'integrazione di Cisco Secure Malware Analytics (Threat Grid) per Cisco Umbrella

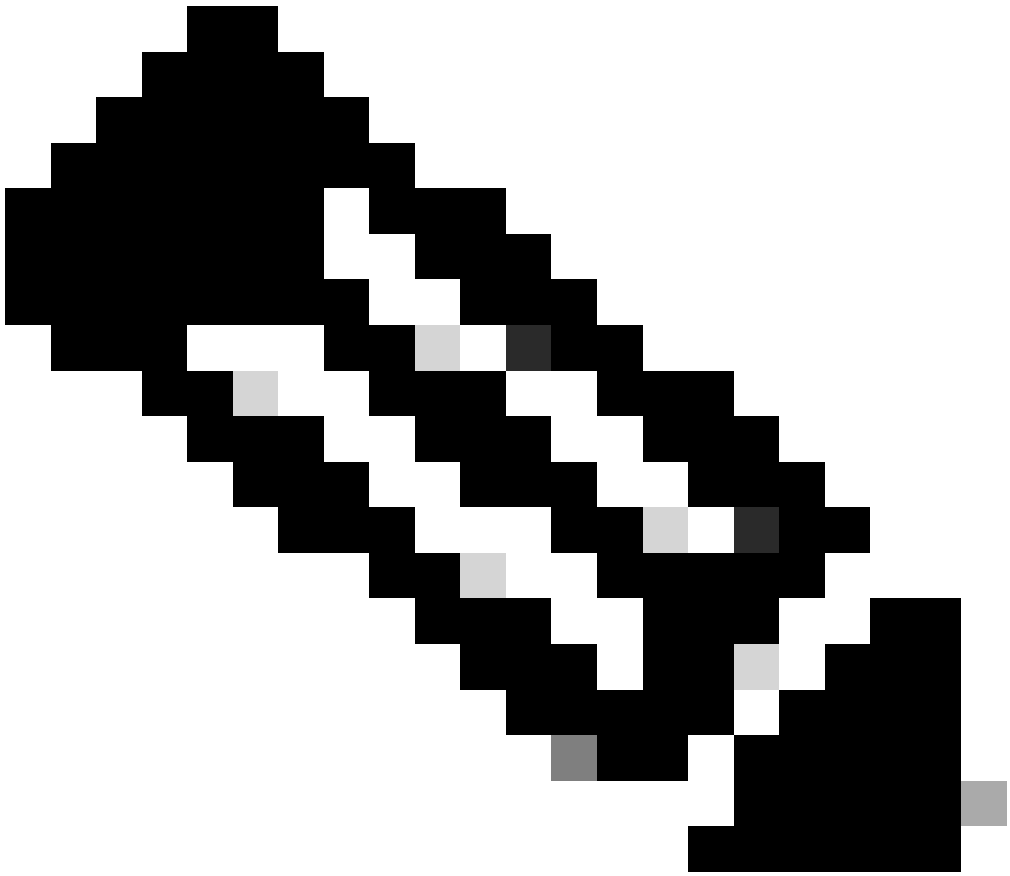
Con l'integrazione tra Cisco Secure Malware Analytics (in precedenza Threat Grid) e Cisco Umbrella, i team di sicurezza sono ora in grado di estendere la loro visibilità e di applicare la protezione dalle minacce avanzate odierne a notebook, tablet o telefoni in roaming, fornendo anche un altro livello di imposizione a una rete aziendale distribuita.

Questa guida illustra come configurare Cisco Secure Malware Analytics (Threat Grid) per

comunicare con Cisco Umbrella in modo che l'intelligence sulle minacce generata da Cisco Secure Malware Analytics (Threat Grid) possa essere integrata automaticamente nelle policy in grado di proteggere i client sotto Cisco Umbrella.

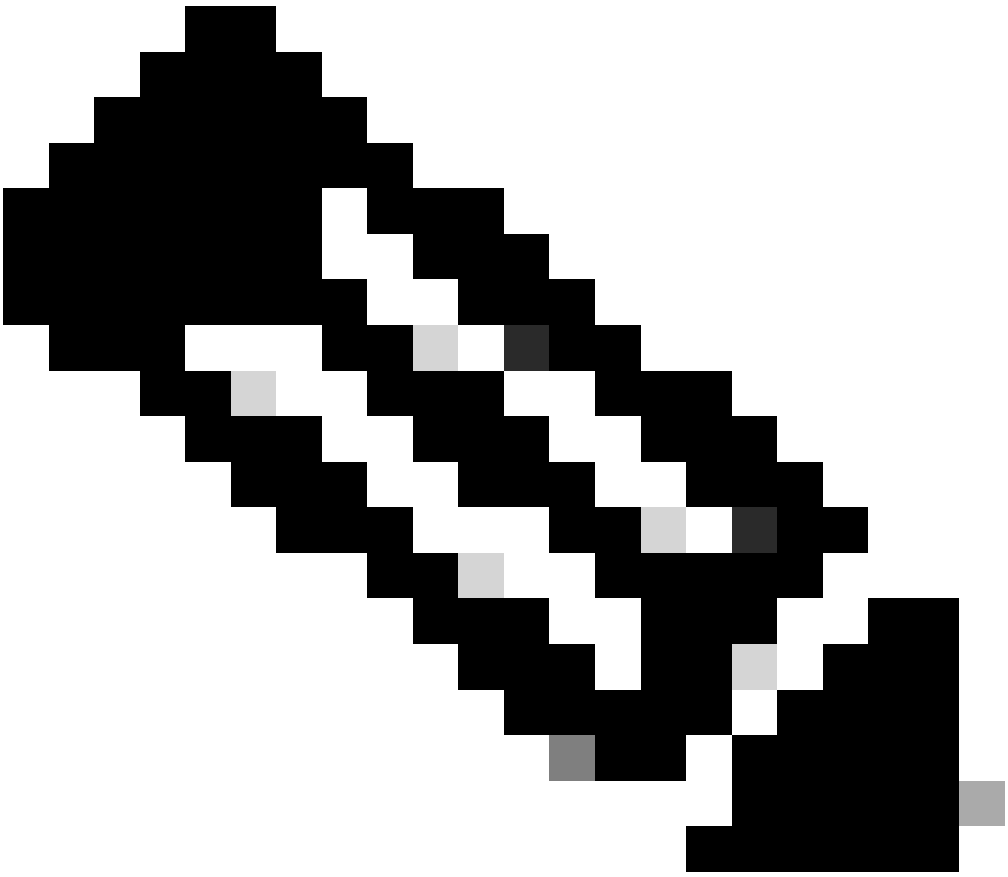
Prerequisiti

- Un dashboard Cisco Secure Malware Analytics (Threat Grid) funzionale con accesso alla chiave API dell'account.



Nota: Gli endpoint e gli accessori Cisco Secure Malware Analytics (Threat Grid) non sono al momento supportati.

- Diritti amministrativi di Cisco Umbrella Dashboard.
- Sul dashboard Cisco Umbrella deve essere abilitata l'integrazione di Cisco Secure Malware Analytics (Threat Grid).



Nota: L'integrazione di Cisco Secure Malware Analytics (Threat Grid) è inclusa solo nei pacchetti Cisco Umbrella come DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Se non disponi di un pacchetto Cisco Umbrella e desideri ricevere questa integrazione, contatta il tuo Cisco Umbrella Account Manager. Se disponi di un pacchetto Cisco Umbrella ma non vedi Cisco Secure Malware Analytics (Threat Grid) come integrazione per il tuo dashboard, contatta il supporto Cisco Umbrella.

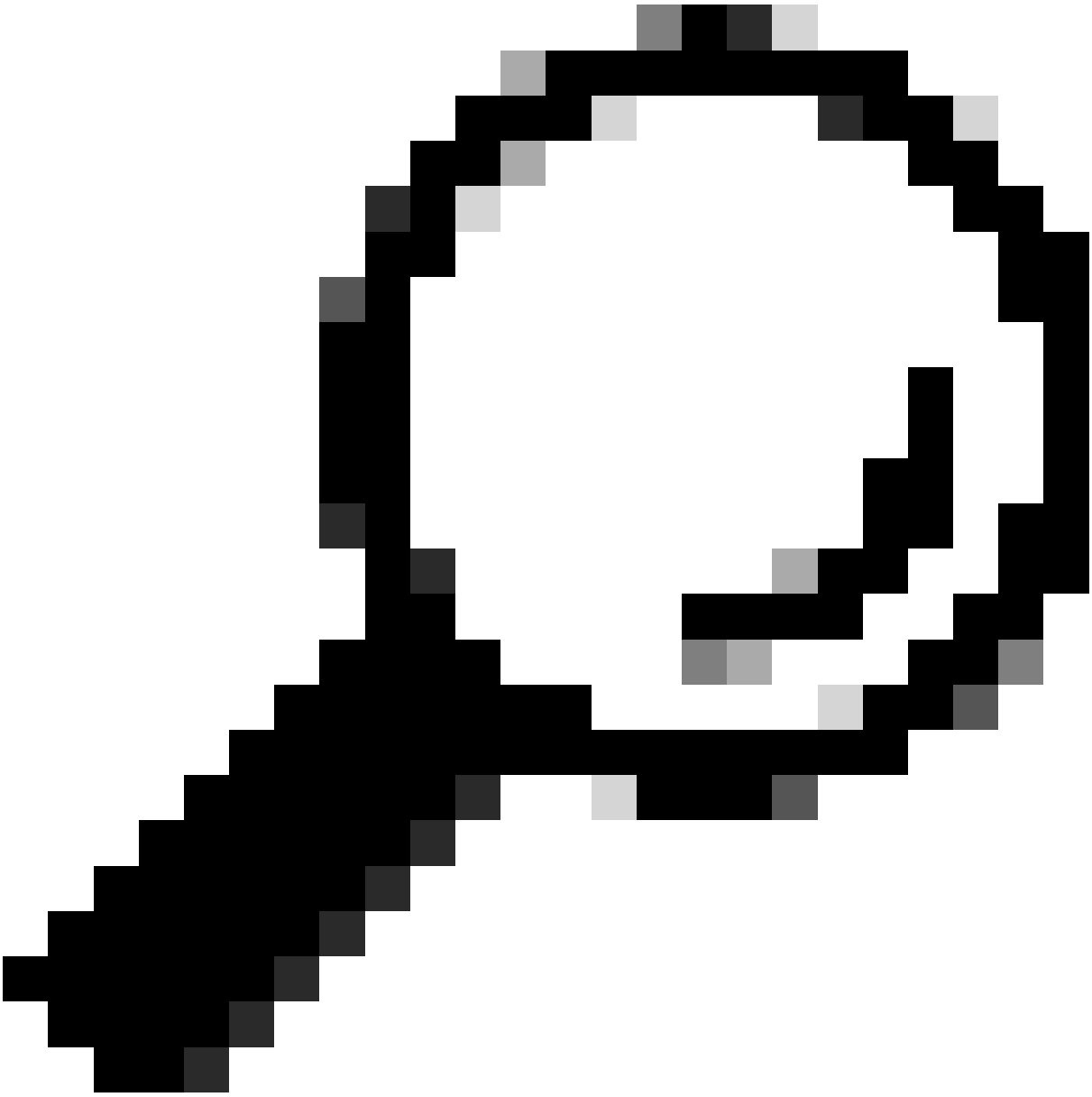
Come funziona questa integrazione?

Cisco Umbrella raggiunge l'API Cisco Secure Malware Analytics (Threat Grid) e recupera gli elenchi di domini generati dall'analisi di campioni dannosi. Cisco Umbrella importa quindi questo elenco tramite l'API Cisco Umbrella Enforcement. Questo approccio è diverso da come funzionano le altre integrazioni in cui Cisco Umbrella tira le informazioni sulle minacce eseguendo query API sull'API Cisco Secure Malware Analytics (Threat Grid), piuttosto che accettare incidenti da altri sistemi che spingono le informazioni sulle minacce nel servizio Cisco Umbrella.

Cisco Umbrella convalida quindi la minaccia per accertarsi che possa essere aggiunta alla policy. Se le informazioni provenienti da Cisco Secure Malware Analytics (Threat Grid) sono confermate

come minacce o non sono un dominio valido conosciuto, l'indirizzo del dominio viene aggiunto all'elenco di destinazione di Cisco Secure Malware Analytics (Threat Grid) come parte di un'impostazione di sicurezza che può essere applicata a qualsiasi criterio Cisco Umbrella. Questa policy viene applicata immediatamente a qualsiasi richiesta proveniente da dispositivi che utilizzano policy che sfruttano l'integrazione di Cisco Secure Malware Analytics (Threat Grid).

Cisco Umbrella riceve due feed distinti da Cisco Secure Malware Analytics (Threat Grid): un feed pubblico (globale) e un feed solo cliente (privato, specifico di un singolo cliente).



Suggerimento: Mentre Cisco Umbrella cerca il meglio per convalidare e consentire i domini che sono noti per essere generalmente sicuri (ad esempio, Google e Salesforce), per evitare interruzioni indesiderate, ti suggeriamo di aggiungere qualsiasi dominio che non vorresti mai aver bloccato all'elenco globale dei domini consentiti o ad altri elenchi di destinazione secondo la tua policy.

Alcuni esempi:

- Home page dell'organizzazione.
- Domini che rappresentano i servizi forniti che possono avere record interni ed esterni. Ad esempio, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Le applicazioni cloud meno note dipendono in modo significativo dal fatto che Cisco Umbrella potrebbe non essere al corrente o non essere inclusa nella convalida automatica dei domini. Ad esempio, "localcloudservice.com".

Questi domini devono essere aggiunti all'elenco globale degli oggetti autorizzati, che si trova in Criteri > Elenchi di destinazione in Cisco Umbrella.

Configurazione di Cisco Umbrella Dashboard per ottenere informazioni da Cisco Secure Malware Analytics (Threat Grid)

Il primo passaggio consiste nel trovare o generare la chiave API nel dashboard Cisco Secure Malware Analytics (Threat Grid):

1. Accedere al dashboard di Cisco Secure Malware Analytics (Threat Grid) e selezionare i dettagli dell'account.
2. In Dettagli account potrebbe essere già visibile una chiave API se ne è già stata creata una. In caso contrario, selezionare "Generate New API Key" (Genera nuova chiave API).

   La chiave API è quindi visibile in Dettagli utente > Chiave API.

Quindi, aggiungere la chiave API a Cisco Umbrella Dashboard per estrarre i dati da Cisco Secure Malware Analytics (Threat Grid):

1. Accedere al dashboard di Cisco Umbrella come amministratore.
2. Selezionare Policy > Policy Components > Integrations (Policy componenti > Integrazioni) e selezionare "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) nella tabella per espanderla.
3. Selezionare Attiva, incollare la chiave API nella casella Chiave API, quindi selezionare Salva.

A questo punto, se viene visualizzato un errore, è probabile che si sia verificato un problema con la chiave API o con le comunicazioni tra i servizi. Controllare la chiave API e riprovare. Se il problema persiste, contattare il supporto Cisco Umbrella.

Se viene visualizzato un messaggio di operazione riuscita, significa che il servizio Cisco Umbrella è stato in grado di utilizzare la chiave API per effettuare una connessione iniziale all'API Cisco Secure Malware Analytics (Threat Grid). Il servizio Cisco Umbrella utilizza un intervallo di polling di cinque minuti per recuperare i dati da Cisco Secure Malware Analytics (Threat Grid).

Anche dopo l'intervallo di cinque minuti, se non sono disponibili dati o eventi di minaccia validi per il pull da parte di Cisco Umbrella Dashboard, le informazioni potrebbero non essere visualizzate.

Quando l'integrazione viene abilitata per la prima volta, inizia semplicemente tornando indietro di cinque minuti sia per i feed globali che per quelli delle sole organizzazioni e la prima volta che riceve i dati è al successivo intervallo di cinque minuti, quindi i dati potrebbero non apparire immediatamente.

Se la chiave API sul lato Cisco Secure Malware Analytics (Threat Grid) viene disattivata o rimossa, l'integrazione viene disabilitata. Per ripristinare l'integrazione, è necessario fornire una nuova chiave API in Cisco Umbrella Dashboard. In caso di timeout o di errore interno del servizio tra Cisco Umbrella e Cisco Secure Malware Analytics (Threat Grid), viene generato un tipo di eccezione diverso e l'integrazione non viene disabilitata, ma al contrario le connessioni continuano a essere tentate ogni cinque minuti come in condizioni normali.

Dettagli tecnici

Di seguito sono elencate le query API esatte utilizzate per estrarre informazioni da Cisco Secure Malware Analytics (Threat Grid). Si noti che vengono raccolti solo gli eventi con un livello di gravità maggiore di 90, un livello di confidenza maggiore di 90 e del tipo Domini. In questo esempio viene utilizzato un intervallo di cinque minuti incrementato per la query successiva. La variabile `api_key` fornita in Cisco Umbrella viene utilizzata in sostituzione della `<key>`:

- Pubblico (feed globale):

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

- Solo cliente (feed privato):

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

o:

- Pubblico (feed globale):

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

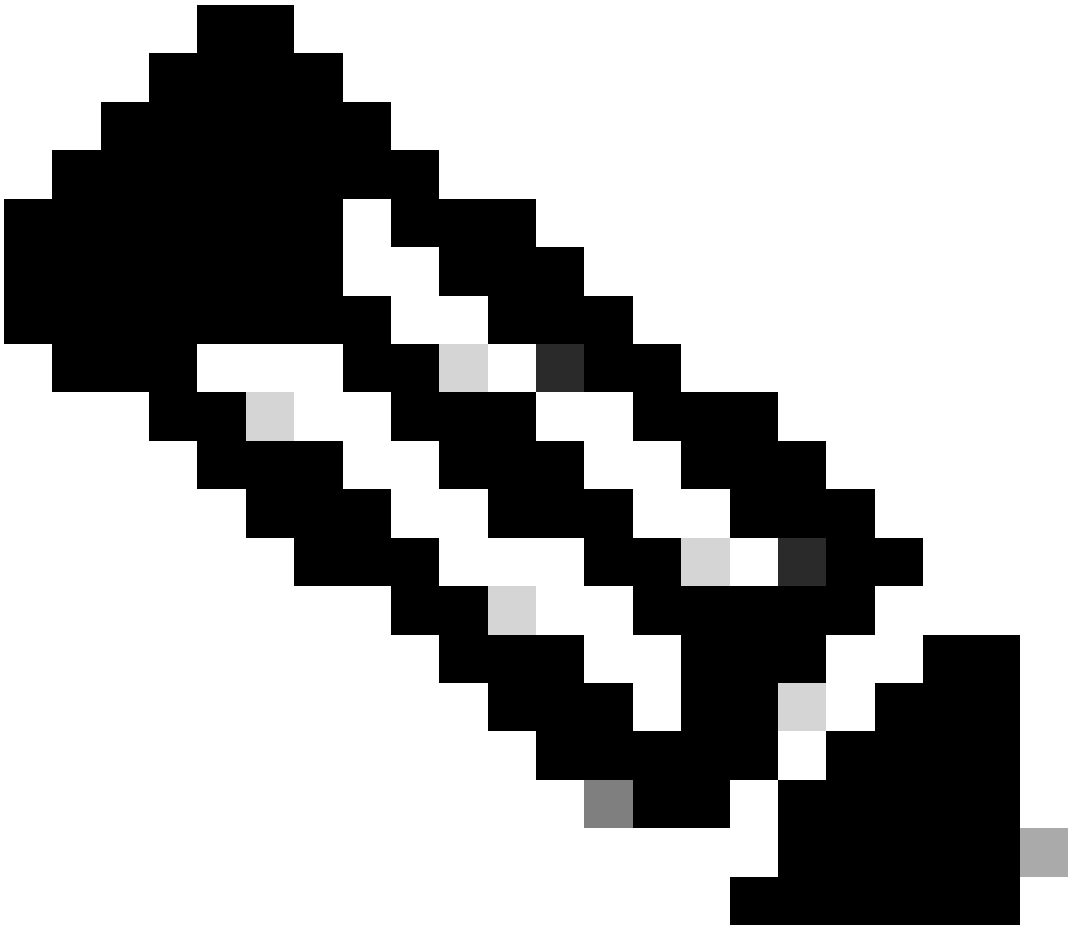
- Solo cliente (feed privato):

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

Osservazione degli eventi aggiunti a Cisco Secure Malware

Analytics (Threat Grid) in "modalità di controllo"

Nel tempo, gli eventi generati da Cisco Secure Malware Analytics (Threat Grid) iniziano a popolare un elenco di destinazioni specifiche che possono essere applicate ai criteri come categoria Cisco Secure Malware Analytics (Threat Grid). Per impostazione predefinita, l'elenco di destinazione e la categoria di protezione sono in "modalità di controllo" e non vengono applicati ad alcun criterio, pertanto nessuna richiesta viene bloccata. Tuttavia, è possibile visualizzare le richieste associate (e che potrebbero essere state bloccate) dalla categoria di sicurezza Cisco AMP Threat Grid.



> Nota: La "modalità di controllo" può essere attivata solo se necessario o anche in modo indefinito, a seconda del profilo di installazione e della configurazione di rete.

Esamina elenco di destinazione

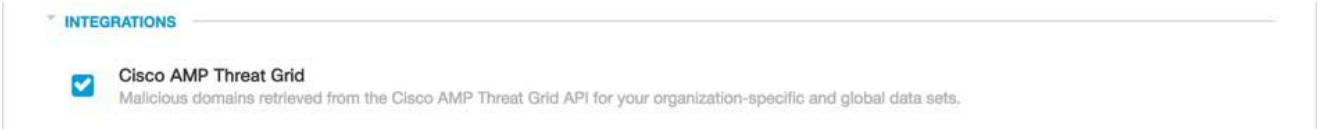
È possibile esaminare l'elenco di destinazione di Cisco Secure Malware Analytics (Threat Grid) in qualsiasi momento.

1. Passare a Criteri > Componenti dei criteri > Integrazioni.
2. Espandere "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) nella tabella e selezionare "Vedere domini".

Rivedere le impostazioni di protezione per un criterio

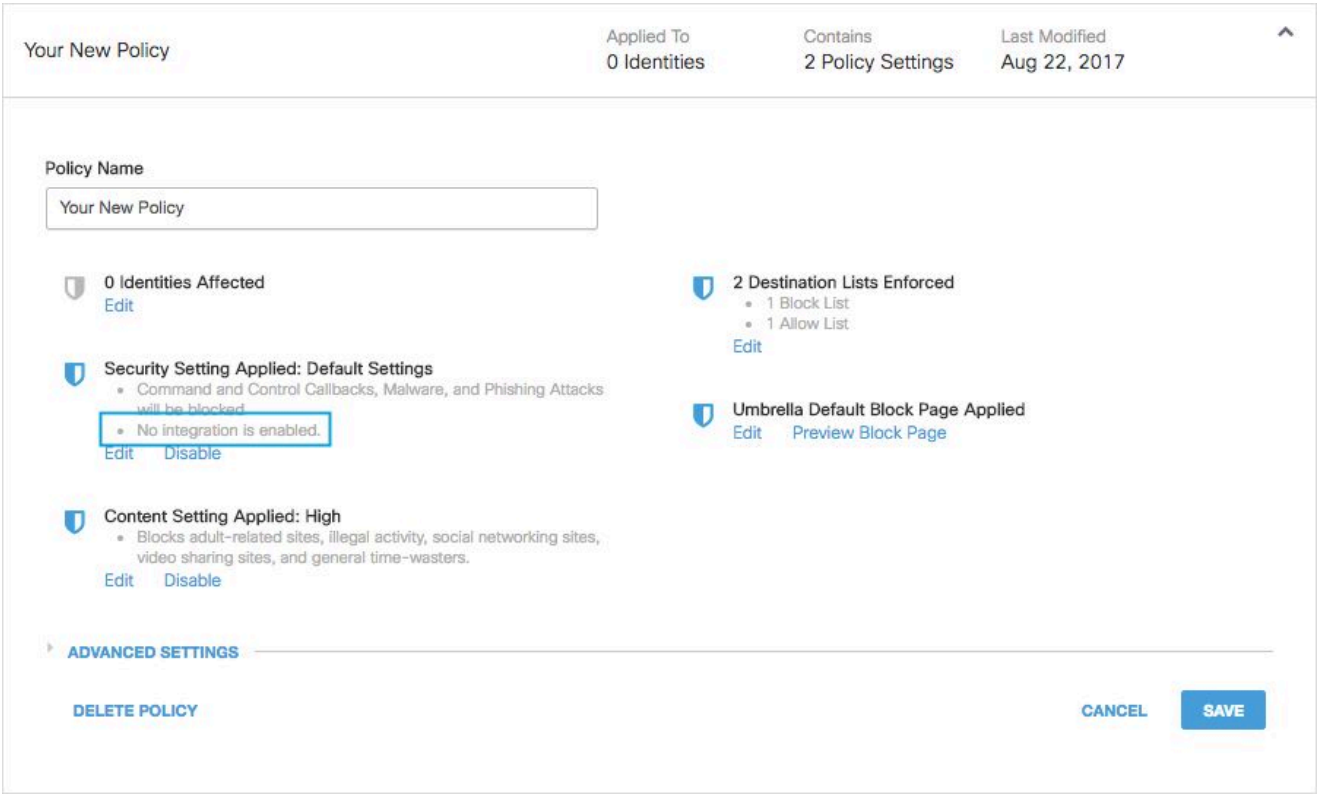
È possibile rivedere le impostazioni di sicurezza che possono essere abilitate per un criterio in qualsiasi momento in Cisco Umbrella:

1. Passare a Criteri > Componenti criterio > Impostazioni protezione.
2. Fare clic su un'impostazione di protezione nella tabella per espanderla.
3. Scorrere la sezione Integrazioni ed espandere la sezione per visualizzare l'integrazione di Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)).
4. Selezionare la casella per l'integrazione Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)), quindi selezionare Save (Salva).

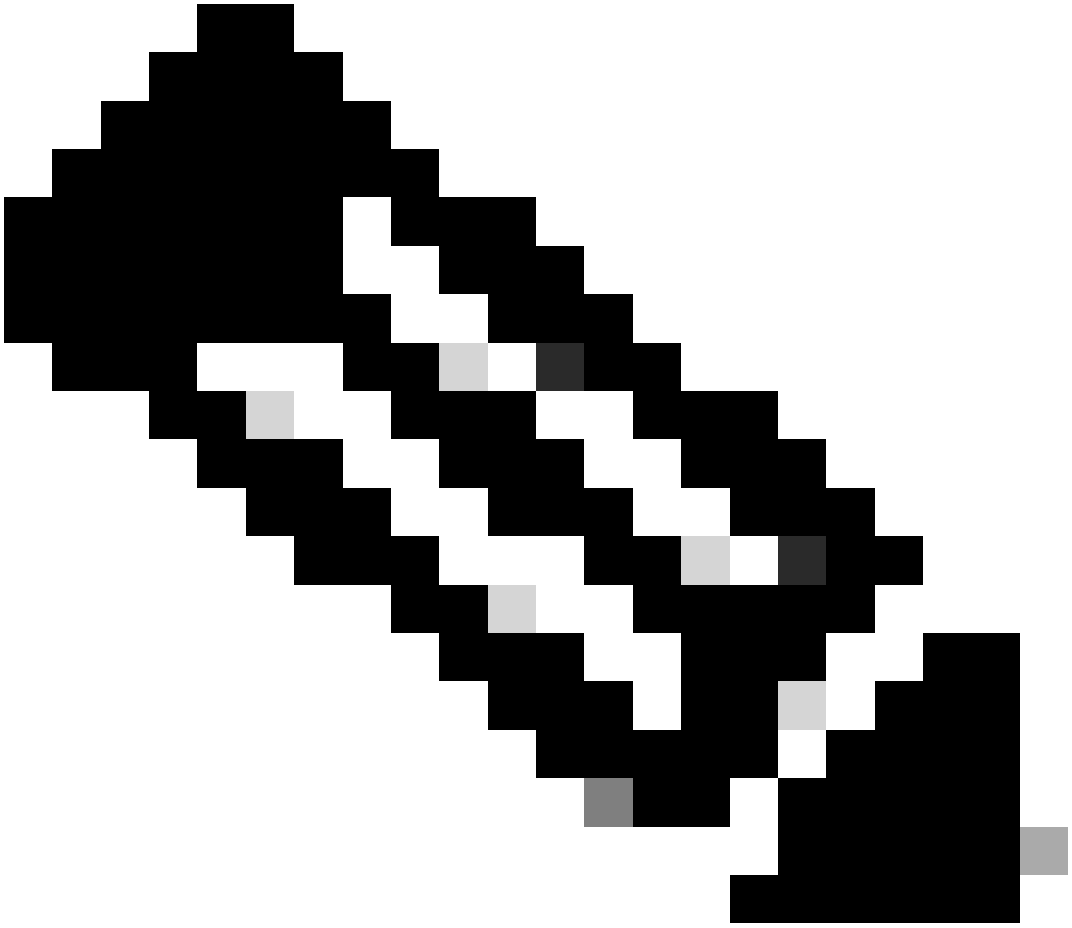


115014151543

È inoltre possibile esaminare le informazioni sull'integrazione tramite la pagina Riepilogo impostazioni di protezione.



20993269073556

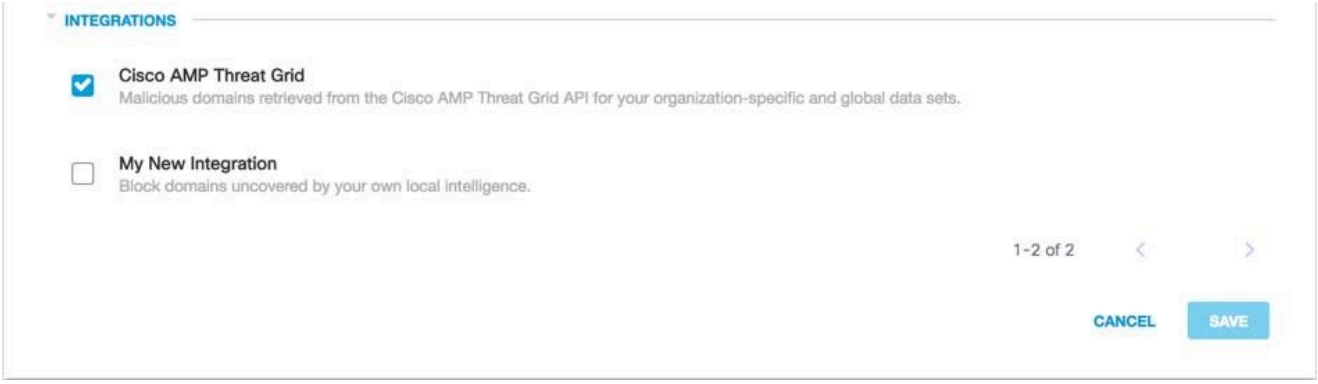


Nota: L'applicazione delle impostazioni può richiedere fino a cinque minuti e se non vengono inseriti nuovi eventi nel sistema Cisco Secure Malware Analytics (Threat Grid), è possibile che i nuovi domini non vengano aggiunti all'integrazione.

Applicazione dell'impostazione di sicurezza Cisco Secure Malware Analytics (Threat Grid) in "modalità blocco" a un criterio per client gestiti

Quando sei pronto a bloccare questi domini per i client gestiti da Cisco Umbrella, modifica le impostazioni di sicurezza su un criterio esistente o crea un nuovo criterio che si trovi al di sopra del tuo criterio predefinito per assicurarti che venga applicato per primo.

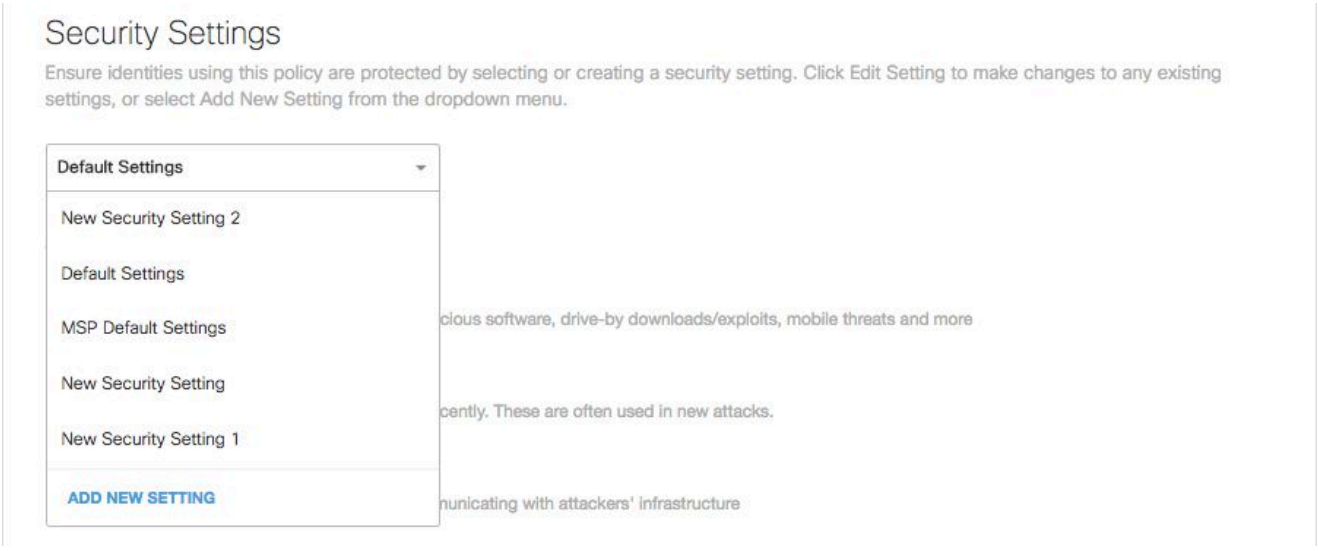
1. Passare a Criteri > Componenti criterio > Impostazioni di protezione.
2. In Integrazioni, verificare che la casella "Cisco AMP Threat Grid" sia selezionata. In caso contrario, selezionare la casella e scegliere Salva.



115013987086

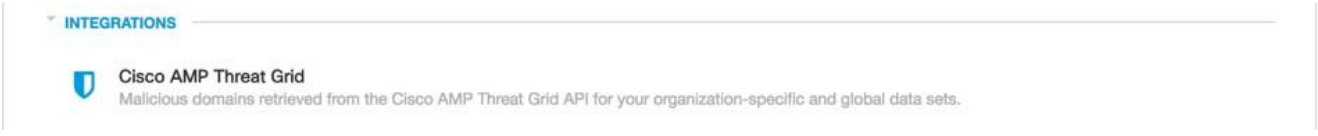
Successivamente, nella procedura guidata Criteri Cisco Umbrella, aggiungere un'impostazione di protezione al criterio che si sta modificando:

1. Passare a Criteri > Gestione > Tutti i criteri.
2. Espandere un criterio e in Impostazioni di protezione applicate selezionare Modifica.
3. Nell'elenco a discesa Security Settings (Impostazioni di protezione), selezionare un'impostazione di protezione che includa l'impostazione "Cisco AMP Threat Grid" (Griglia minacce AMP Cisco).



20993282642708

L'icona a forma di scudo sotto Integrations viene aggiornata in blu.



115013987446

4. Selezionare Set & Return.

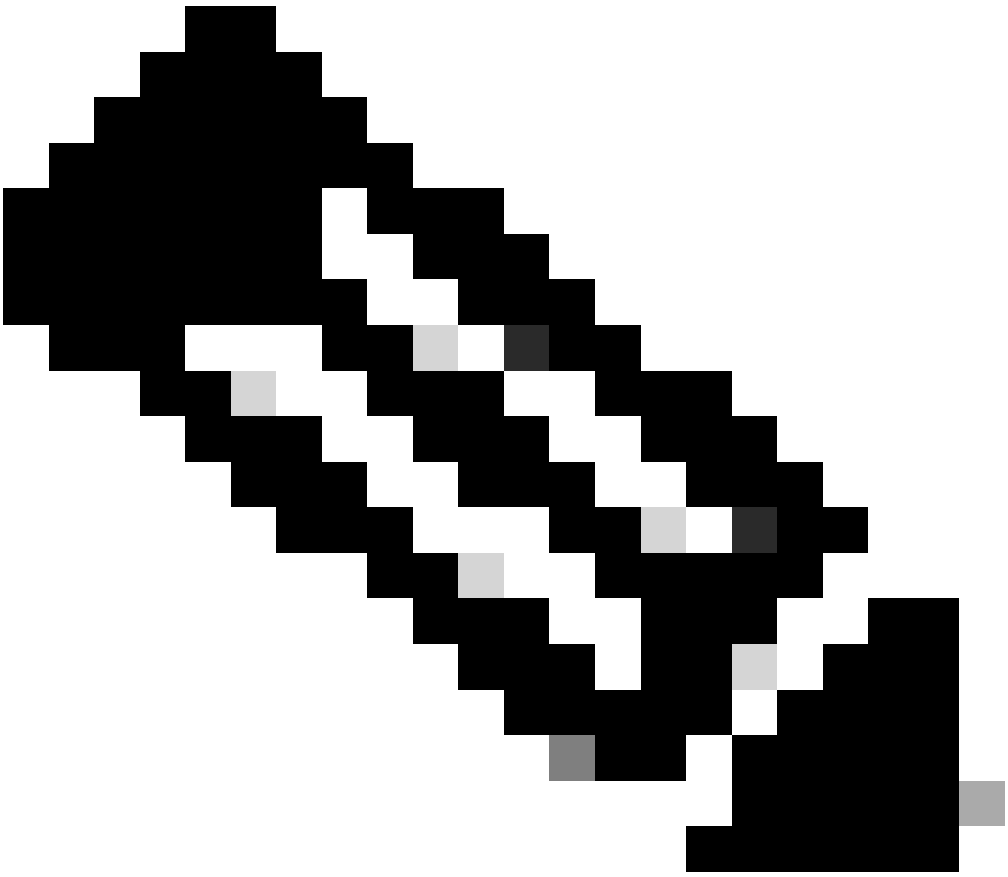
   I domini Cisco Secure Malware Analytics (Threat Grid) contenuti nelle impostazioni di sicurezza di Cisco Secure Malware Analytics (Threat Grid) sono bloccati per le identità che usano il criterio.

Segnalazione in Cisco Umbrella degli eventi di Cisco Secure Malware Analytics

Segnalazione di eventi di sicurezza di Cisco Secure Malware Analytics (Threat Grid)

L'elenco di destinazione Cisco Secure Malware Analytics (Threat Grid) è uno degli elenchi di categorie di sicurezza per cui è possibile creare un report. La maggior parte o tutti i report utilizzano le categorie di protezione come filtro. Ad esempio, è possibile filtrare le categorie di sicurezza per visualizzare solo le attività relative a Cisco Secure Malware Analytics (Threat Grid).

1. Selezionare Reporting > Core Reports > Activity Search e in Categorie di sicurezza selezionare "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) per filtrare il report in modo da visualizzare solo la categoria di sicurezza per Cisco Secure Malware Analytics (Threat Grid).



Nota: Se l'integrazione Cisco AMP Threat Grid è disabilitata, non viene visualizzata nel filtro Categorie di sicurezza.

115014210123

2. Selezionare Applica.

Segnalazione di quando i domini sono stati aggiunti all'elenco di destinazione di Cisco Secure Malware Analytics (Threat Grid)

Il log di controllo di Cisco Umbrella Admin include gli eventi dal dashboard Cisco Secure Malware Analytics (Threat Grid) quando aggiunge i domini all'elenco di destinazione. Gli eventi sono generati da un utente di nome "Cisco AMP Threat Grid Domain List", anch'esso contrassegnato con il logo Cisco. Tali eventi includono il dominio aggiunto e l'ora in cui è stato aggiunto.

Se si seleziona la voce Log di controllo di amministrazione, questa viene espansa in modo da visualizzare i dettagli, incluso il dominio specifico aggiunto.

È possibile filtrare in modo da includere solo le modifiche di Cisco Secure Malware Analytics (Threat Grid) applicando un filtro per l'utente "Cisco AMP Threat Grid Domain List".

Gestione di rilevamenti indesiderati o falsi positivi

Due tipi di rilevamento di Cisco Secure Malware Analytics (Threat Grid) e due risoluzioni

Al momento, sono disponibili due tipi di blocchi Cisco Secure Malware Analytics (Threat Grid): Una con una risoluzione possibile e una seconda con una risoluzione corrente per un rilevamento indesiderato.

1. Voce Griglia minacce globali (pubblica): A questo punto, l'unico metodo per consentire al dominio è aggiungerlo all'elenco degli oggetti autorizzati.
2. Feed solo cliente (privato): può essere indirizzato con una voce dell'elenco Consenti o eliminato dall'elenco di integrazione di AMP Threat Grid.

Elenchi di destinazioni autorizzate

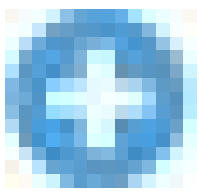
Anche se improbabile, è possibile che i domini aggiunti automaticamente dall'integrazione di Cisco Secure Malware Analytics (Threat Grid) attivino potenzialmente un rilevamento indesiderato che blocca l'accesso degli utenti a determinati siti Web. In una situazione come questa, si consiglia di aggiungere i domini a un elenco di indirizzi consentiti (Criteri > Elenchi di destinazione), che ha la precedenza su tutti gli altri tipi di elenchi di indirizzi bloccati, incluse le impostazioni di protezione.

Ci sono due ragioni per cui questo approccio è preferito. In primo luogo, nel caso in cui il dashboard Cisco Secure Malware Analytics (Threat Grid) dovesse aggiungere di nuovo il dominio dopo la rimozione, l'elenco Consenti protegge da questo problema e causa ulteriori problemi. In secondo luogo, l'elenco degli indirizzi consentiti mostra una registrazione cronologica di domini problematici che possono essere utilizzati per le relazioni di analisi legale o di audit.

Per impostazione predefinita, esiste un elenco di indirizzi consentiti globale che viene applicato a tutti i criteri. L'aggiunta di un dominio all'elenco globale degli indirizzi consentiti comporta che il dominio sia consentito in tutti i criteri.

Se l'impostazione di protezione Cisco Secure Malware Analytics (Threat Grid) in modalità blocco viene applicata solo a un sottoinsieme delle identità Cisco Umbrella gestite (ad esempio, solo a computer mobili e dispositivi mobili in roaming), è possibile creare un elenco di indirizzi consentiti specifico per queste identità o policy.

Per creare un elenco Consenti:

1. Passare a Criteri > Componenti criterio > Elenchi di destinazione e selezionare 

   25463394696852

   (Aggiungi).

2. Selezionare Consenti e aggiungere il dominio all'elenco.
3. Selezionare Salva.

Una volta salvato l'elenco, è possibile aggiungerlo a un criterio esistente relativo ai client interessati dal blocco indesiderato.

Eliminazione dei domini dall'elenco di destinazione di Cisco Secure Malware Analytics (Threat Grid)

Accanto a ciascun nome di dominio nell'elenco Cisco Secure Malware Analytics (Threat Grid) è disponibile un'icona ("Elimina"). L'eliminazione dei domini consente di pulire l'elenco di destinazione di Cisco Secure Malware Analytics (Threat Grid) in caso di rilevamento indesiderato.

L'eliminazione non è permanente se il dashboard Cisco Secure Malware Analytics (Threat Grid) deve inviare nuovamente il dominio a Cisco Umbrella.

1. Selezionare Policies > Policy Components > Integrations (Policy Componenti > Integrazioni) e selezionare "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) per espanderlo.
2. Selezionare Vedere Domini.
3. Cercare il nome di dominio da eliminare.
4. Selezionare l'icona "Elimina".
5. Selezionare Chiudi.
6. Selezionare Salva.

Nel caso di un rilevamento indesiderato o di un falso positivo, si consiglia di creare immediatamente un elenco degli oggetti autorizzati in Cisco Umbrella e quindi di correggere il falso positivo nel dashboard di Cisco Secure Malware Analytics (Threat Grid). In seguito, è possibile rimuovere il dominio dall'elenco delle destinazioni di Cisco Secure Malware Analytics (Threat Grid).

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).