Informazioni sull'API di applicazione Umbrella per integrazioni personalizzate

Sommario

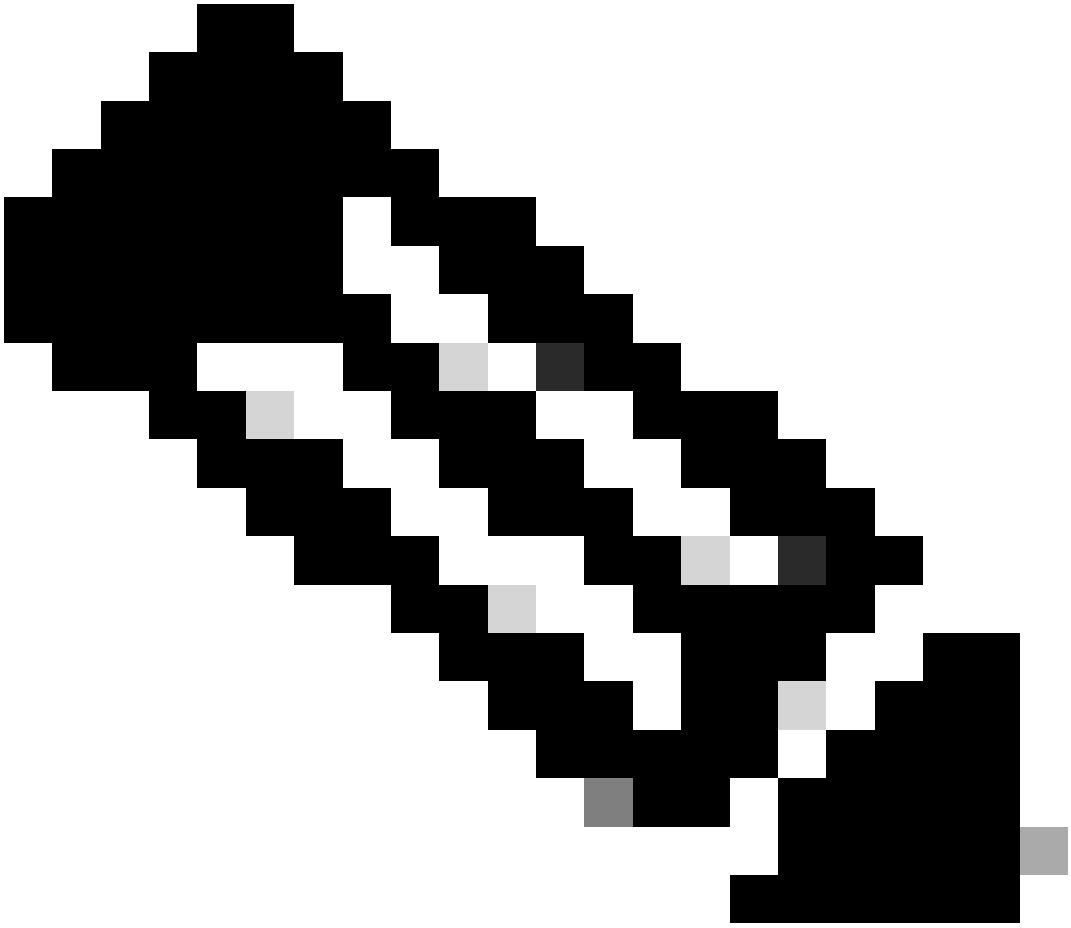
Introduzione

In questo documento viene descritta l'API di imposizione Umbrella per le integrazioni personalizzate.

Che cos'è l'API di applicazione Umbrella?

L'API Umbrella Enforcement consente ai partner e ai clienti con i propri ambienti SIEM/Threat Intelligence Platform (TIP) interni di inserire eventi e/o informazioni sulle minacce nel proprio ambiente Umbrella. Questi eventi vengono poi immediatamente convertiti in visibilità e applicazione che possono estendersi oltre il perimetro e quindi la portata dei sistemi che potrebbero aver generato questi eventi o l'intelligence delle minacce.

L'API di imposizione può acquisire gli eventi nel formato di evento generico descritto nella documentazione dell'API e può supportare le funzioni ADD, DELETE o LIST.



Nota: Se non disponi dell'API di imposizione Umbrella per le integrazioni personalizzate nel dashboard Umbrella e desideri accedervi, [contatta il rappresentante Cisco Umbrella.]

Perché dovrei usarlo?

È possibile che l'utente elabori, gestisca e gestisca il proprio sistema di intelligence delle minacce e i processi che determinano il desiderio di intraprendere azioni su domini identificati come dannosi o sospetti. In tal caso, una volta presa la decisione che un evento deve essere attivato (ad esempio, convertito in protezione), anziché aggiungere manualmente la protezione a Umbrella per scopi di imposizione, è possibile utilizzare l'API di applicazione per automatizzare questo processo e applicare immediatamente la protezione in base ai domini associati all'evento.

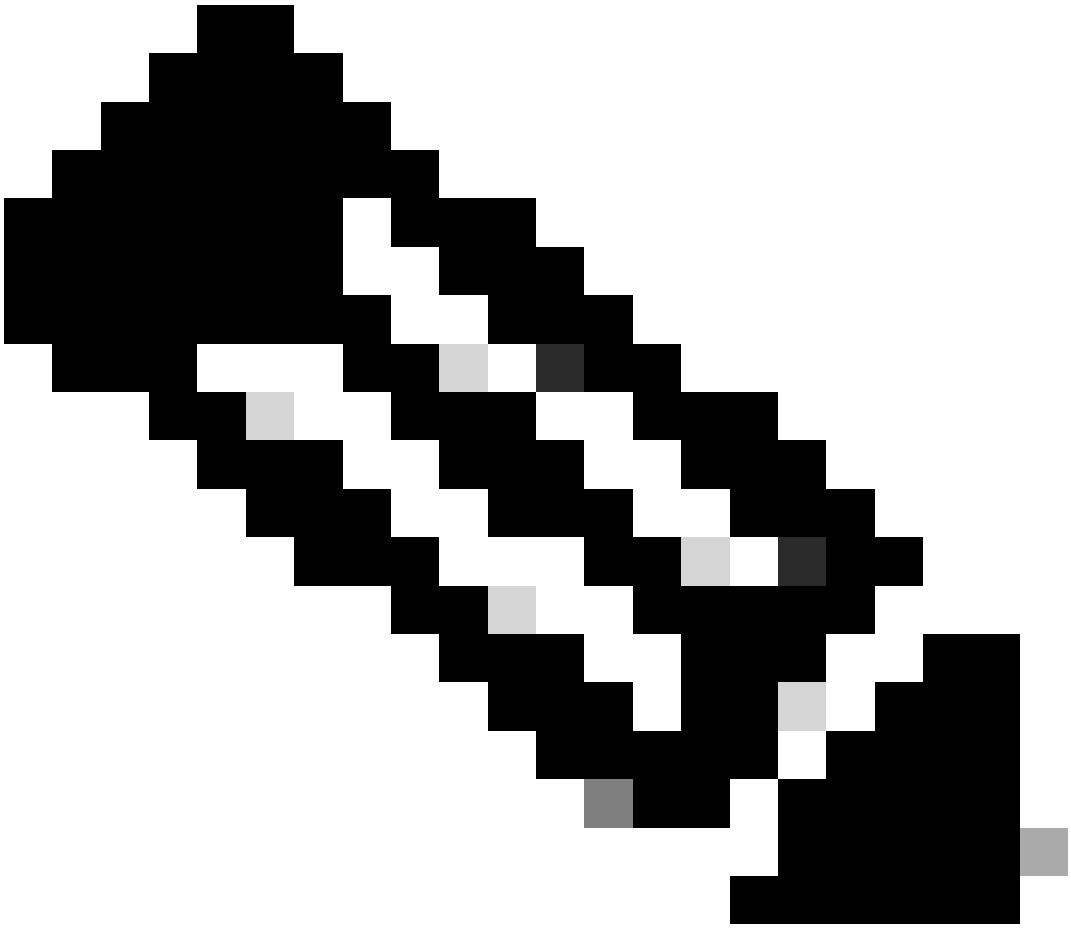
Ciò consente al team di sicurezza di concentrare il proprio tempo e impegno sull'indagine piuttosto che sulla configurazione in corso di Umbrella. Consente al team addetto alla sicurezza di rimanere all'interno dei propri strumenti e processi, senza dover passare direttamente al dashboard Umbrella per aggiornare gli elenchi di destinazione. In sostanza, è possibile creare un elenco di

destinazioni in Umbrella da un'origine esterna che si gestisce direttamente tramite l'API, quindi scegliere di bloccare tali destinazioni per le identità all'interno di Umbrella.

Come La Userei?

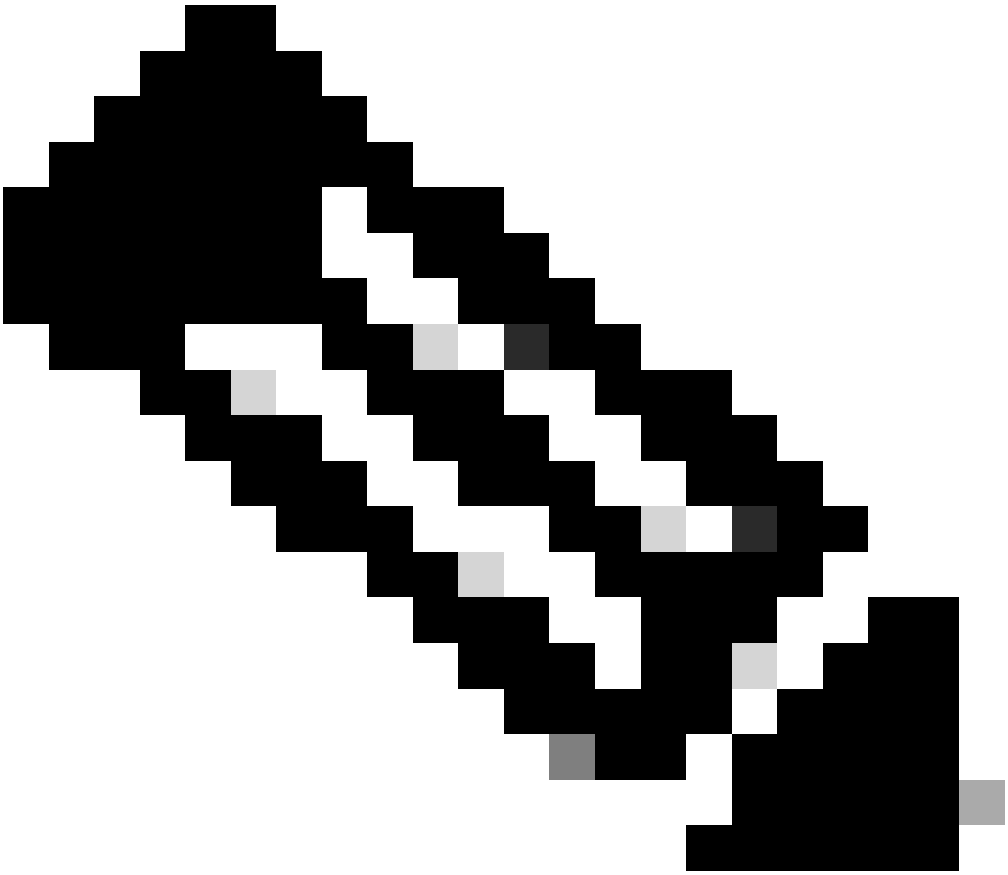
AGGIUNGERE un evento all'API di imposizione

Una volta aggiunto un evento, l'applicazione tenta di estrarre i domini dall'evento.



Nota: Il supporto per gli indirizzi IP e gli URL verrà aggiunto in futuro.

- Un evento può contenere tutti i dettagli dell'evento originale desiderati, ma è necessario attenersi alle specifiche descritte nella documentazione API.



Nota: In futuro è possibile aggiungere il supporto per i dettagli degli eventi di superficie all'interno del dashboard Umbrella.

- Se un dominio viene estratto, viene convalidato dal grafico di sicurezza Cisco Umbrella per garantire che non sia un dominio sicuramente funzionante che potrebbe causare falsi positivi o già ritenuto dannoso dal grafico di sicurezza Cisco Umbrella.
- Se supera la convalida (ad esempio, è sconosciuto e sicuro da bloccare), viene aggiunto a un elenco di destinazione associato a tale integrazione personalizzata e visualizzato all'interno del dashboard Umbrella come categoria di sicurezza personalizzata.
- La categoria di protezione personalizzata può essere bloccata o consentita in base a criteri specifici, per consentire l'applicazione attiva o il controllo passivo delle richieste sospette.

ELENCA i domini per un elenco di API di imposizione

- Se il flusso di lavoro include lo sblocco dei domini bloccati a causa di eventi inseriti in precedenza, una richiesta LIST fornisce tutti i domini attualmente inclusi nell'elenco di destinazione associato a tale integrazione.

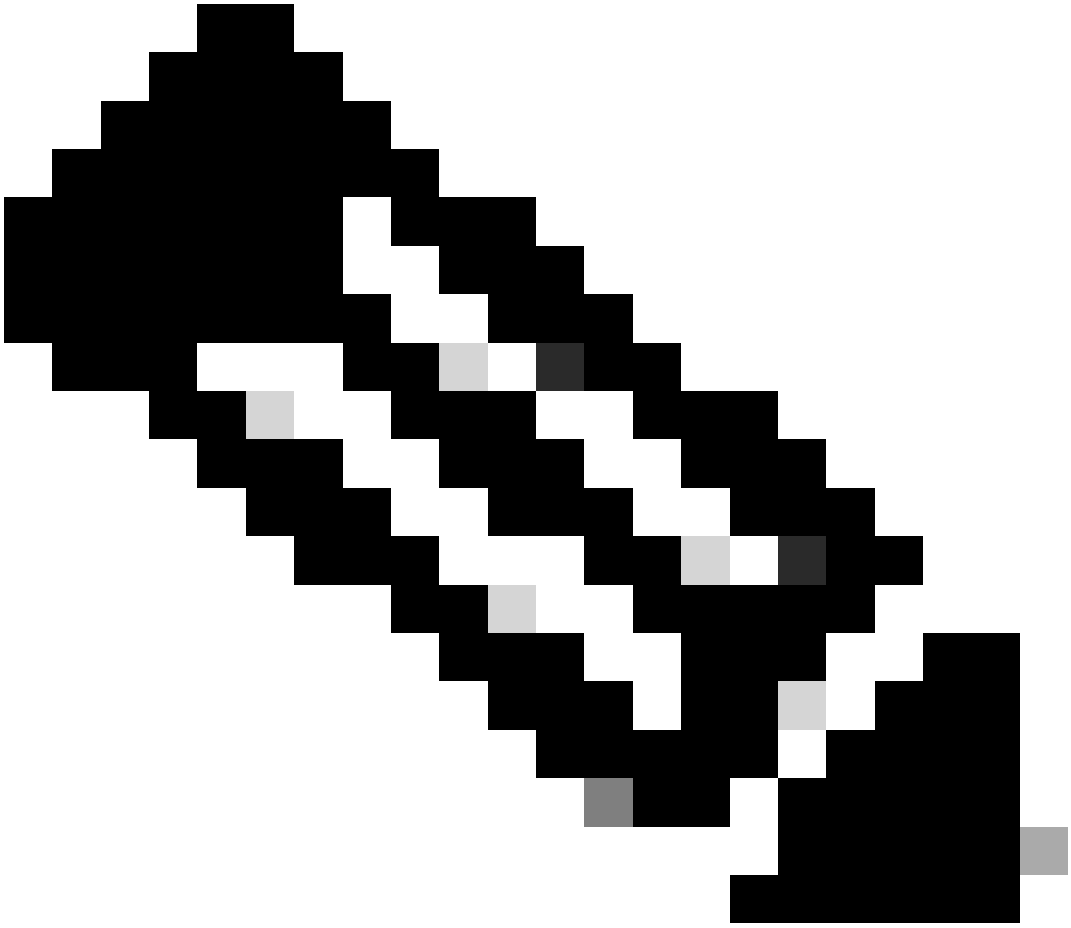
ELIMINA dominio dall'elenco API di imposizione

- Se il flusso di lavoro include lo sblocco dei domini bloccati a causa di eventi inseriti in precedenza, una richiesta DELETE consente di rimuovere un dominio dall'elenco di destinazione associato all'integrazione.
- Se una richiesta DNS in ingresso da una delle identità Umbrella è destinata a un dominio nell'elenco di destinazioni di integrazione personalizzate, viene bloccata o consentita a seconda delle impostazioni di protezione dell'integrazione personalizzata associate al criterio che l'ha attivata.
- I risultati sono registrati insieme a tutti gli altri eventi Umbrella, accessibili tramite Activity Search, o tramite Amazon S3 utilizzando l'integrazione S3. In questo modo, il traffico associato all'integrazione personalizzata può essere riacquisito nel SIEM/TIP e il ciclo di feedback chiuso.

Utilizzo dell'API di imposizione

Passaggio 1: Creazione di un'integrazione personalizzata

È possibile avere fino a 10 integrazioni personalizzate alla volta.



Nota: Se l'organizzazione è un'organizzazione figlio di un MSP, MSSP o MOC Umbrella, le integrazioni personalizzate condivise dal livello della console vengono visualizzate prima delle integrazioni create a livello dell'organizzazione figlio.

1. In Umbrella, passare a Policy > Policy Components > Integrations e fare clic su Add.
2. Aggiungere un nome per l'integrazione personalizzata e fare clic su Crea.
3. Espandere la nuova integrazione personalizzata, selezionare Abilita, copiare l'URL di integrazione e quindi fare clic su Salva.

Passaggio 2: Creare gli script personalizzati.

1. Vedere gli script di esempio generate_event e delete_domain nell'appendice di questo documento o utilizzare la documentazione API per creare script personalizzati per generare richieste formattate correttamente per la generazione di eventi o per l'eliminazione o la creazione di elenchi di domini. È possibile utilizzare l'URL di integrazione personalizzato in questi script.

Passaggio 3: Inserire un evento di esempio

1. Utilizzare lo script creato per inserire un evento nell'integrazione personalizzata. Nell'esempio riportato sotto, è stato inserito un evento contenente il dominio "creditcards.com".

Passaggio 4: Controllare l'elenco di destinazione nel dashboard Umbrella

1. Tornate a Impostazioni > Integrazioni e nella tabella espandete l'integrazione personalizzata.
2. Fare clic su Vedere domini. Verrà visualizzato un elenco in cui è possibile eseguire ricerche dei domini aggiunti e l'evento di esempio del passaggio 4 sarà ora presente nell'elenco.

Passaggio 5: Controllare il registro di controllo dell'amministratore.

1. Un altro modo per verificare l'attività associata all'integrazione personalizzata consiste nell'esaminare il registro di controllo dell'amministratore.
2. Passare a Report > Log di controllo di amministrazione.
3. In Filtri, immettere il nome dell'integrazione personalizzata in Filtro in base a identità e impostazioni, quindi fare clic su Esegui filtro.

Quando si espande la voce, viene visualizzato l'evento che ha determinato l'aggiunta dell'evento di esempio (creditcards.com) all'integrazione personalizzata.

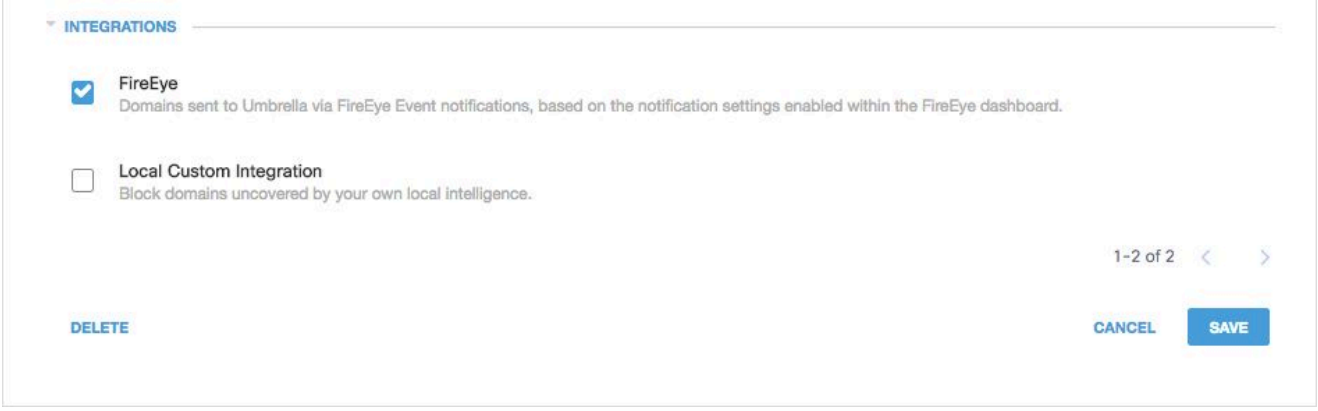
Passaggio facoltativo: Elenca o elimina domini

È inoltre consigliabile verificare di essere in grado di elencare i domini nell'integrazione personalizzata ed eliminare i domini nel caso in cui non si desideri più applicarli al dominio o se si desidera che siano inclusi nell'integrazione. Per elencare ed eliminare i domini, attenersi alla procedura descritta nella documentazione dell'API.

Configura impostazioni di protezione

Dopo aver verificato che è possibile inserire eventi (ed eventualmente elencare ed eliminare domini), è possibile configurare l'azione da eseguire sulle richieste DNS provenienti dalle identità dell'utente e destinate ai domini nella categoria di sicurezza dell'integrazione personalizzata.

1. Passare a Policies > Security Settings (Policy > Impostazioni di sicurezza) e in Integrations (Integrazioni), verificare l'integrazione abilitata (in questo esempio, FireEye) e fare clic su Save (Salva).

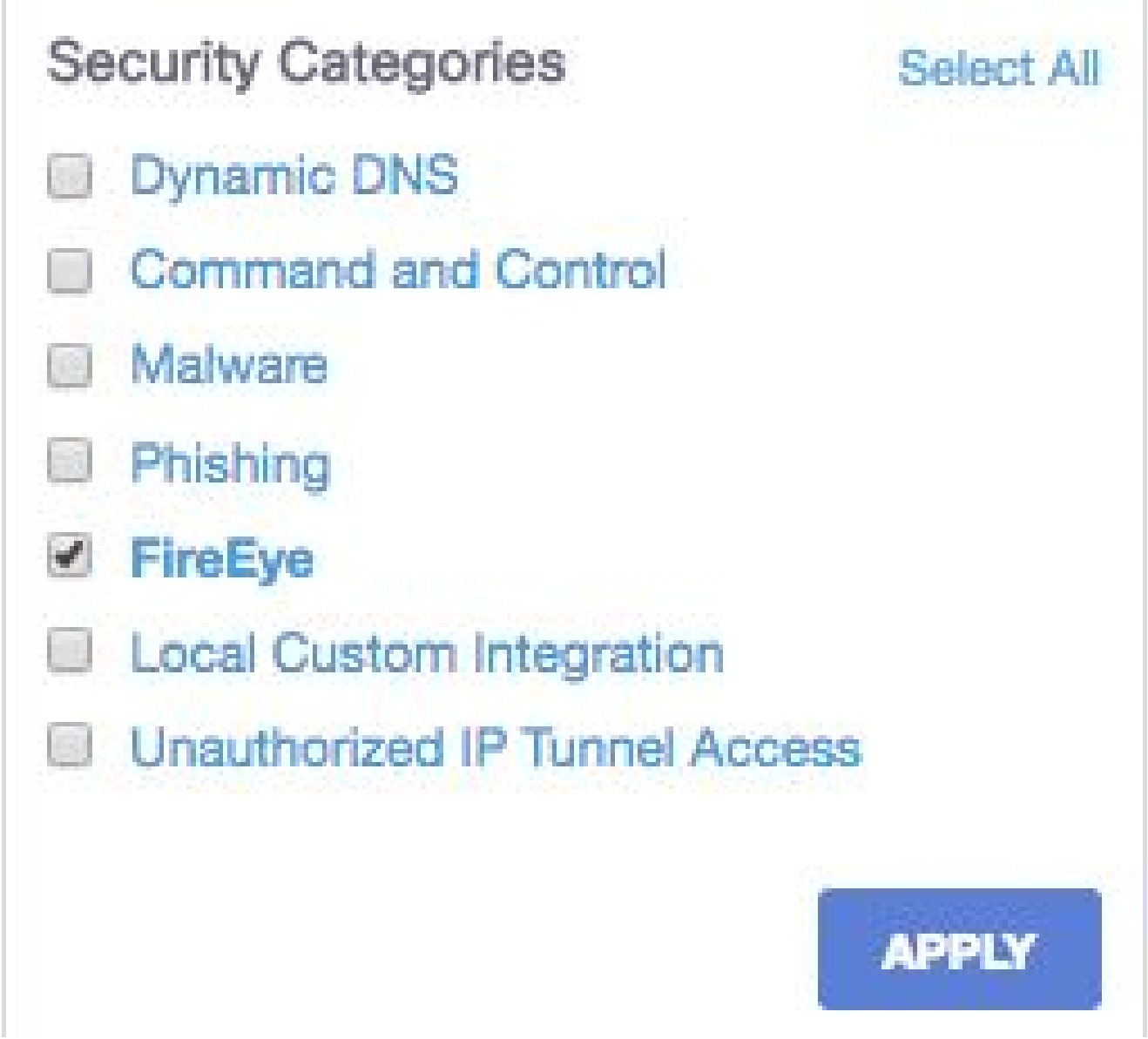


115014145103

Visualizza report per l'integrazione personalizzata

Genera richieste DNS da una delle identità (ad esempio, reti o computer in roaming) destinate al dominio nell'integrazione personalizzata ("creditcards.com" nell'esempio). Dal punto di vista del client, è ora possibile visualizzare il blocco appropriato o il risultato consentito a seconda di come sono state configurate le impostazioni di sicurezza.

1. Passare a Reporting > Ricerca attività e in Categorie sicurezza selezionare l'integrazione personalizzata (in questo esempio FireEye) per filtrare il report in modo da visualizzare solo la categoria di sicurezza per FireEye.

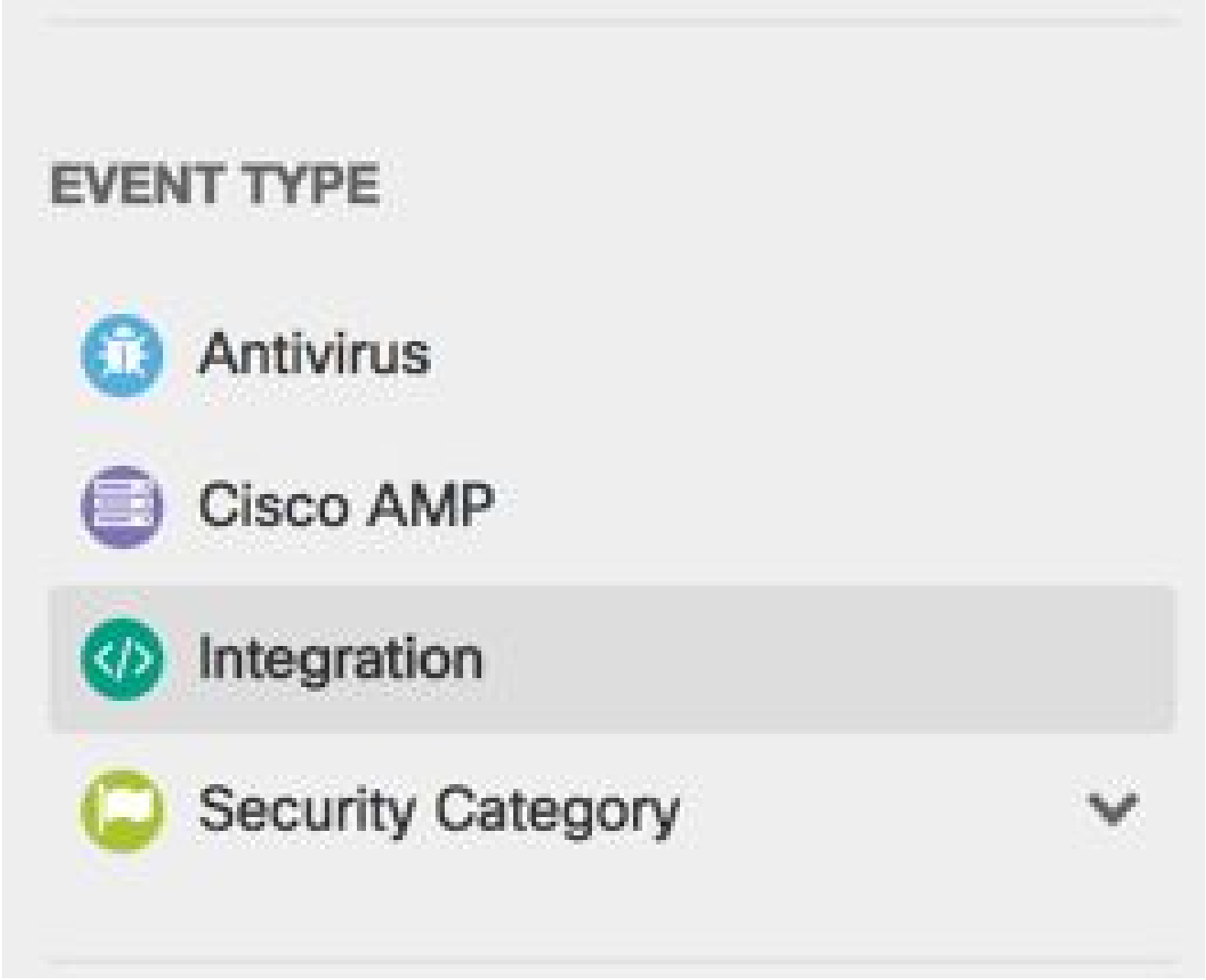


115013981706

2. Fare clic su Applica per visualizzare l'attività per il periodo di tempo selezionato nel report.

È inoltre possibile visualizzare il report Volume attività per visualizzare lo snapshot o i report di conteggio della tendenza nel tempo, incluse le integrazioni personalizzate.

1. Passare a Reporting > Volume attività sicurezza.
2. In Tipo di evento, selezionare Integrazione.



115013982286

Configurazione dell'integrazione S3 per l'archiviazione e l'utilizzo dei log (opzionale)

Se si desidera inserire i registri Umbrella contenenti tutte le richieste per l'ambiente nell'ambiente SIEM/TIP, è possibile utilizzare l'integrazione S3, che consente di trasmettere in streaming gli eventi attività DNS.

Appendice: Script di esempio

Questi script Perl forniscono indicazioni su come generare un evento per l'integrazione personalizzata. Sostituire il valore customerKey dell'integrazione in entrambi gli script. Si noti che questi script vengono forniti come esempi e potrebbero essere necessari aggiornamenti o personalizzazioni.

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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).