Integrazione di Umbrella con FireEye

Sommario

Introduzione

Questo documento descrive come integrare Cisco Umbrella con FireEye.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Appliance FireEye con accesso alla rete Internet pubblica.
- Diritti amministrativi di Cisco Umbrella Dashboard.
- L'integrazione FireEye deve essere abilitata in Cisco Umbrella Dashboard.

Componenti usati

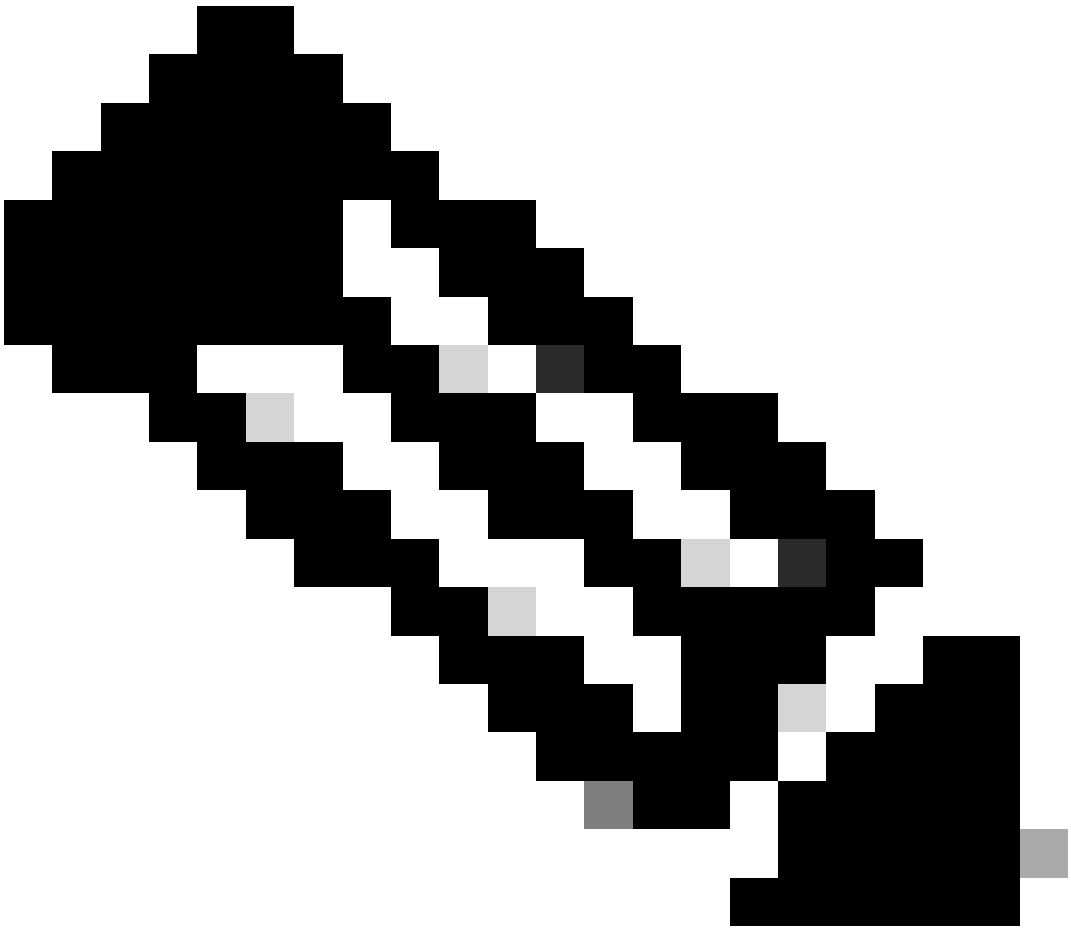
Le informazioni fornite in questo documento si basano su Cisco Umbrella.

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.

Panoramica

Grazie all'integrazione tra l'appliance di sicurezza FireEye e Cisco Umbrella, gli addetti alla sicurezza e gli amministratori sono ora in grado di estendere la protezione dalle minacce avanzate a notebook, tablet o telefoni in roaming, fornendo al contempo un altro livello di imposizione a una rete aziendale distribuita.

Questa guida descrive come configurare FireEye per comunicare con Cisco Umbrella in modo che gli eventi di sicurezza di FireEye siano integrati in policy che possono essere applicate ai client protetti da Cisco Umbrella.



Nota: L'integrazione FireEye è inclusa solo nei pacchetti Cisco Umbrella come DNS

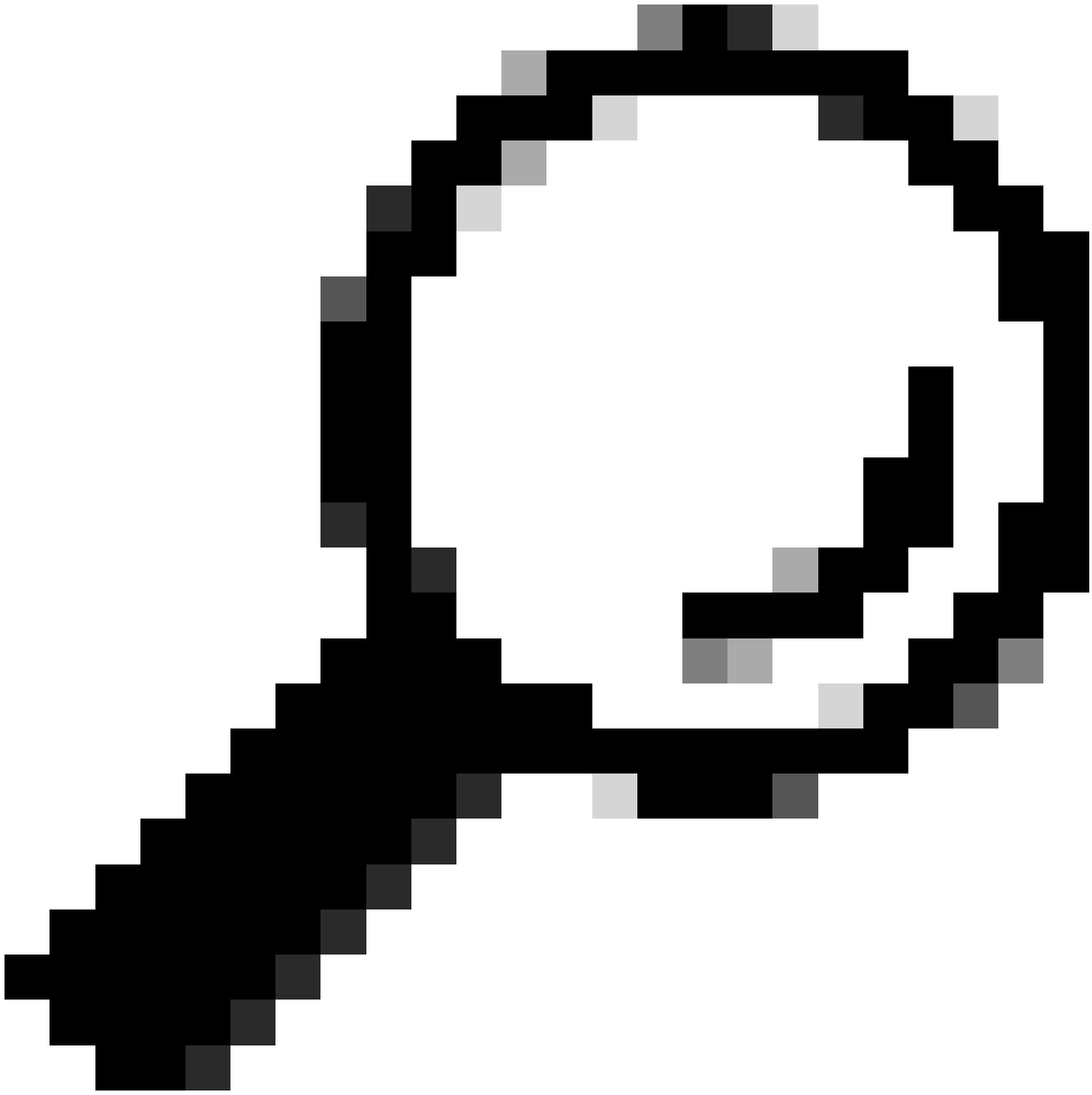
Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Se non si dispone di uno di questi pacchetti e si desidera ottenere l'integrazione FireEye, contattare il proprio Cisco Umbrella Account Manager. Se disponi del pacchetto Cisco Umbrella corretto ma non vedi FireEye come integrazione per il tuo dashboard, contatta il supporto Cisco Umbrella.

Funzionalità di integrazione

Per prima cosa, l'appliance FireEye invia a Cisco Umbrella le minacce basate su Internet rilevate, ad esempio domini che ospitano malware, comandi e controllo di botnet o siti di phishing.

Cisco Umbrella convalida quindi le informazioni passate a Cisco Umbrella per verificarne la validità e la possibilità di aggiungerle a un criterio. Se viene confermato che le informazioni di FireEye sono formattate correttamente (ad esempio, non si tratta di un file, di un URL complesso o di un dominio molto popolare), l'indirizzo del dominio viene aggiunto all'elenco di destinazione di FireEye come parte di un'impostazione di sicurezza che può essere applicata a qualsiasi policy di Cisco Umbrella. Questo criterio viene applicato immediatamente a qualsiasi richiesta effettuata da dispositivi che utilizzano criteri con l'elenco di destinazione FireEye.

Nel futuro, Cisco Umbrella analizza automaticamente gli allarmi FireEye e aggiunge i siti dannosi all'elenco di destinazione FireEye. In questo modo la protezione FireEye viene estesa a tutti gli utenti e i dispositivi remoti e viene fornito un altro livello di applicazione alla rete aziendale.



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 domini che non vorresti mai aver bloccato all'Elenco globale consentiti o ad altri elenchi di destinazione secondo la tua policy. Alcuni esempi:

- Home page dell'organizzazione
- Domini che rappresentano i servizi forniti e che possono avere record interni ed esterni. Ad esempio, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Le applicazioni basate su cloud meno note da cui si dipende non vengono incluse nella convalida automatica del dominio. Ad esempio, "localcloudservice.com".

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

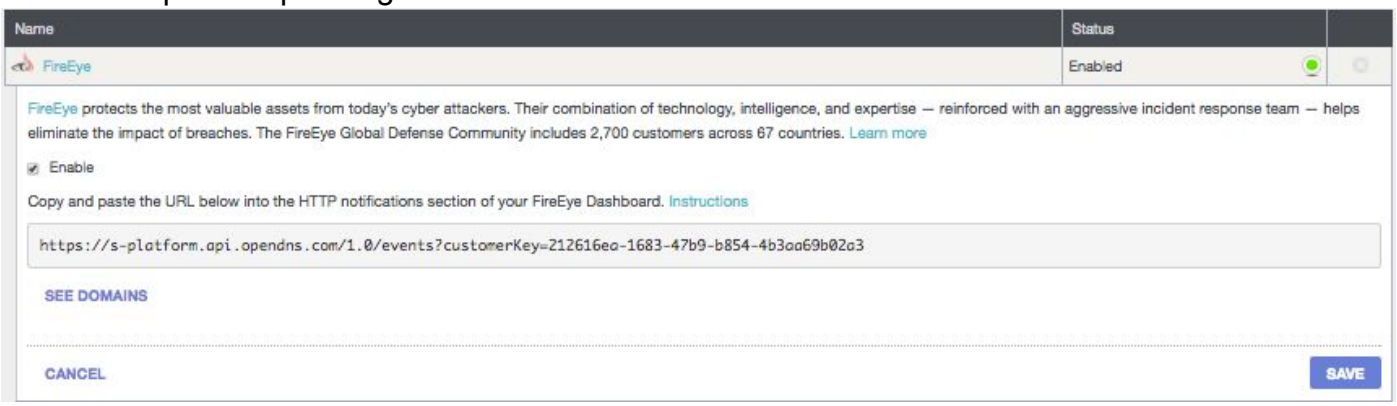
Configurazione di Cisco Umbrella Dashboard per ricevere informazioni da FireEye

Il primo passaggio consiste nel trovare il proprio URL univoco in Cisco Umbrella con cui l'appliance FireEye può comunicare.

1. Accedere a Cisco Umbrella Dashboard come amministratore.

2. Passare a Criteri > Componenti dei criteri > Integrazioni e selezionare FireEye nella tabella per espanderla.

3. Selezionare la casella Abilita, quindi selezionare Salva. In questo modo viene generato un URL univoco e specifico per l'organizzazione in Cisco Umbrella.

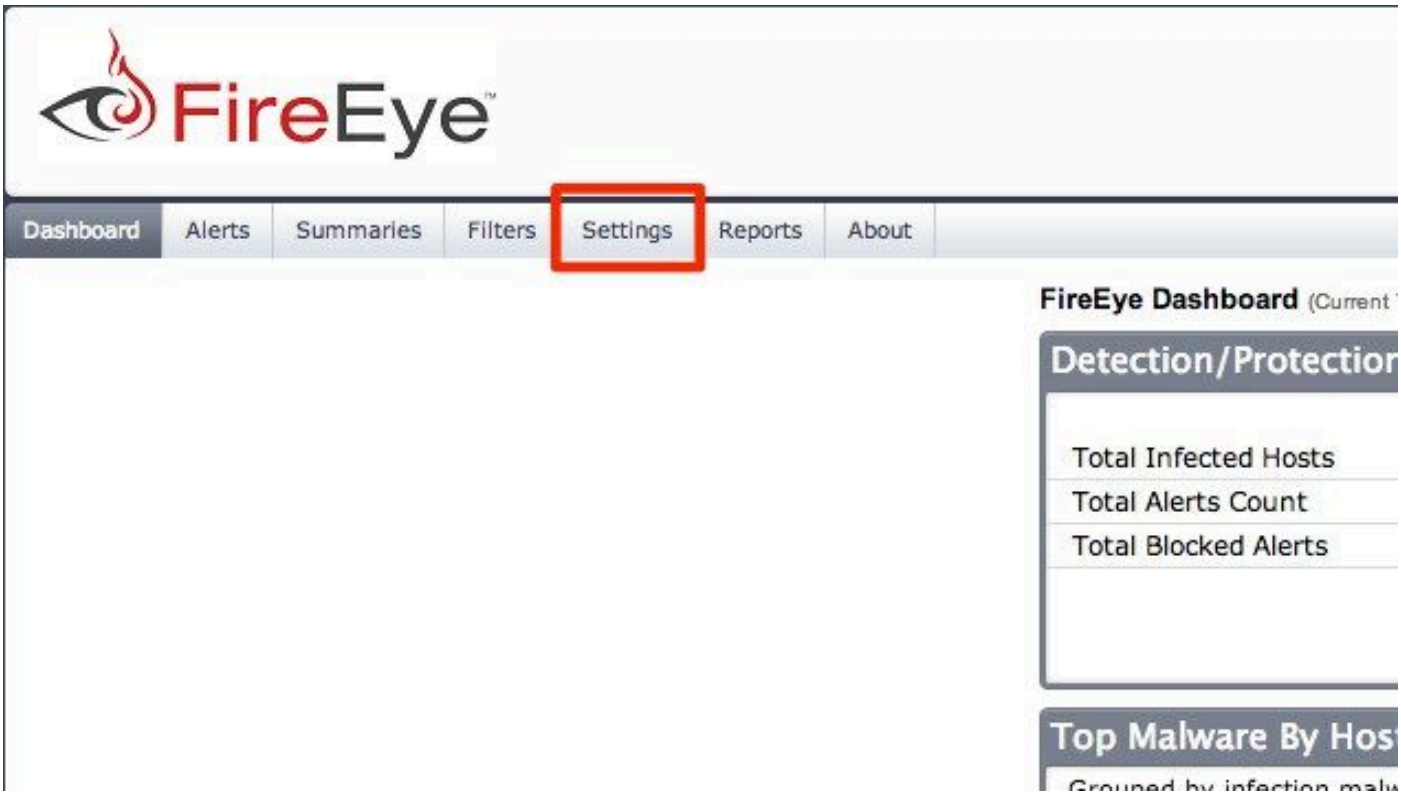


È possibile usare questo URL in un secondo momento per configurare l'appliance FireEye in modo che invii i dati a Cisco Umbrella, quindi accertarsi di copiare l'URL.

Configurazione di FireEye per comunicare con Cisco Umbrella

Per iniziare a inviare il traffico dall'appliance FireEye a Cisco Umbrella, è necessario configurare FireEye con le informazioni sull'URL generate nella sezione precedente.

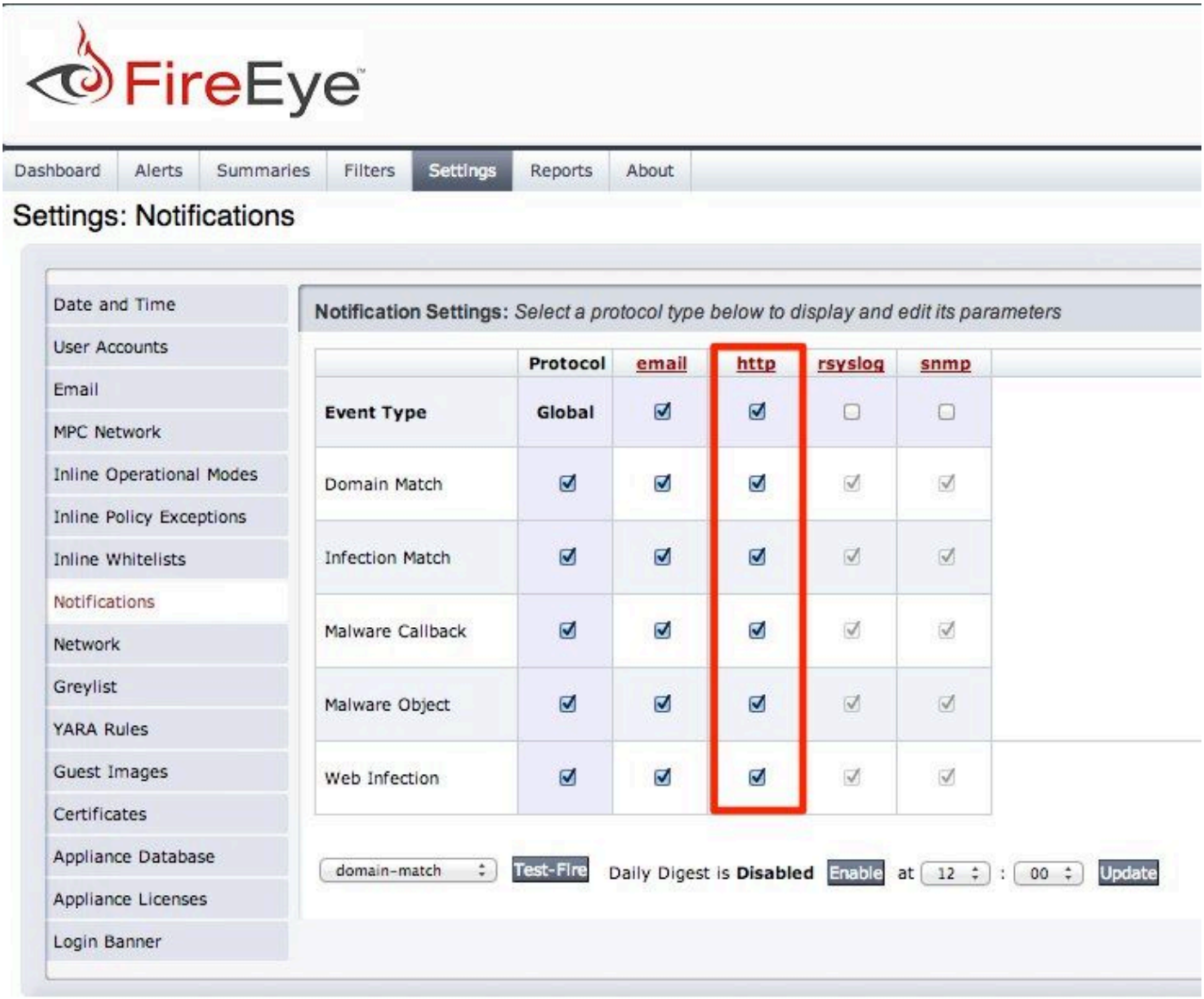
1. Accedere a FireEye e selezionare Settings (Impostazioni).



2. Selezionare Notifiche dall'elenco di impostazioni:

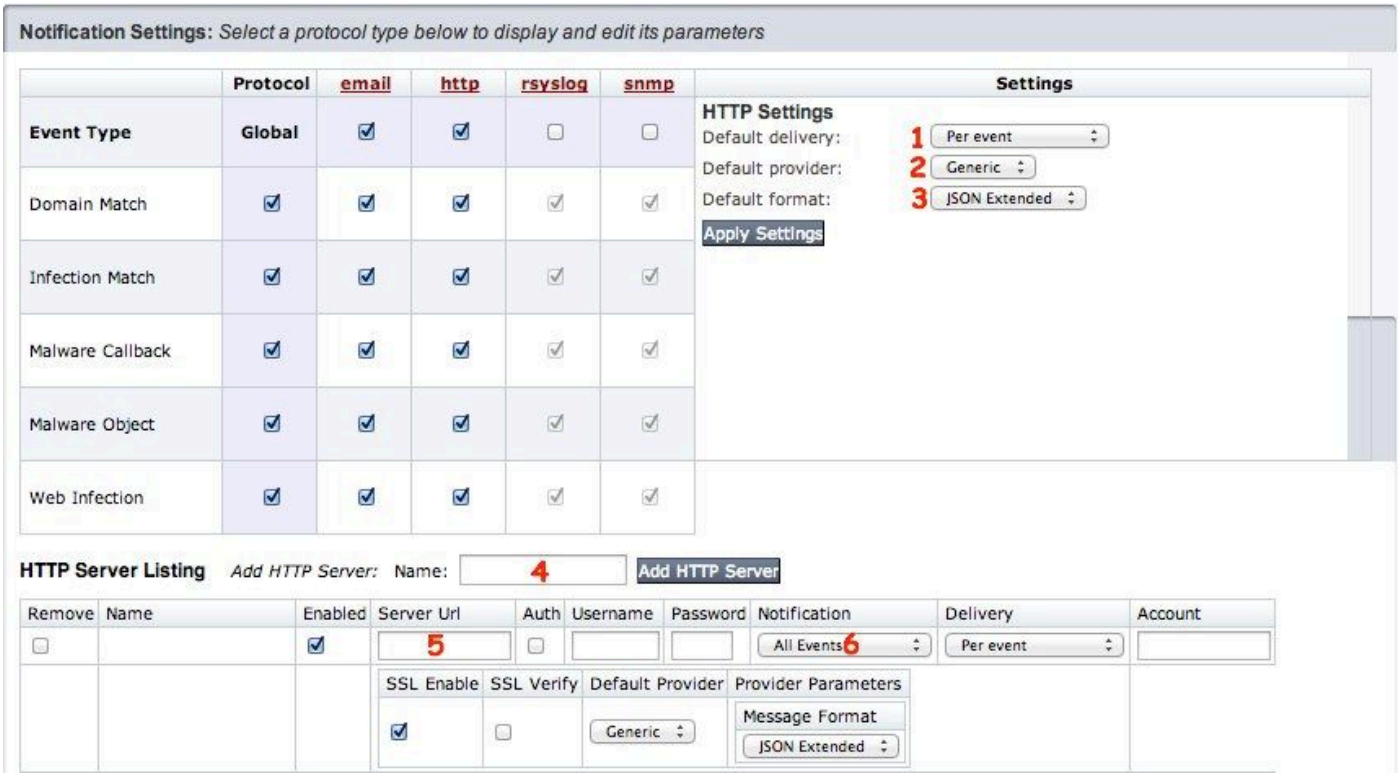

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance Licenses
Login Banner
Date and Time Settings
Manually set the date, time, and time zone. Or, op
synchronization.
(Current Time: 11/11/13 17:29:24 UTC)
Set Manually:
November
11
2013
17
Enable NTP:
Add NTP Server:
NTP Server
Delete
Update T
pool.ntp.org
Update T
time.nist.gov
Update T
Remove Selected NTP Servers
Set Time Zone:
UTC
Set Time Zone

3. Verificare che tutti i tipi di evento da inviare a Cisco Umbrella siano selezionati (Umbrella consiglia di iniziare con tutti), quindi selezionare il collegamento HTTP nella parte superiore della colonna.



4. Quando il menu si espande, selezionare queste opzioni per abilitare Notifica evento. I passi numerati sono delineati nello screenshot:

1. Consegna predefinita: Per evento
2. Provider predefinito: Generico
3. Formato predefinito: JSON esteso
4. Assegnare al server HTTP il nome "OpenDNS".
5. URL server: Incolla qui l'URL di Cisco Umbrella generato dal tuo dashboard Cisco Umbrella.
6. Elenco a discesa Notifica: Selezionare Tutti gli eventi per garantire la massima copertura.



5. Verificare che gli elenchi a discesa Recapito, Provider predefinito e Parametri provider corrispondano tutti alle impostazioni predefinite oppure che vengano utilizzati più server di notifica:

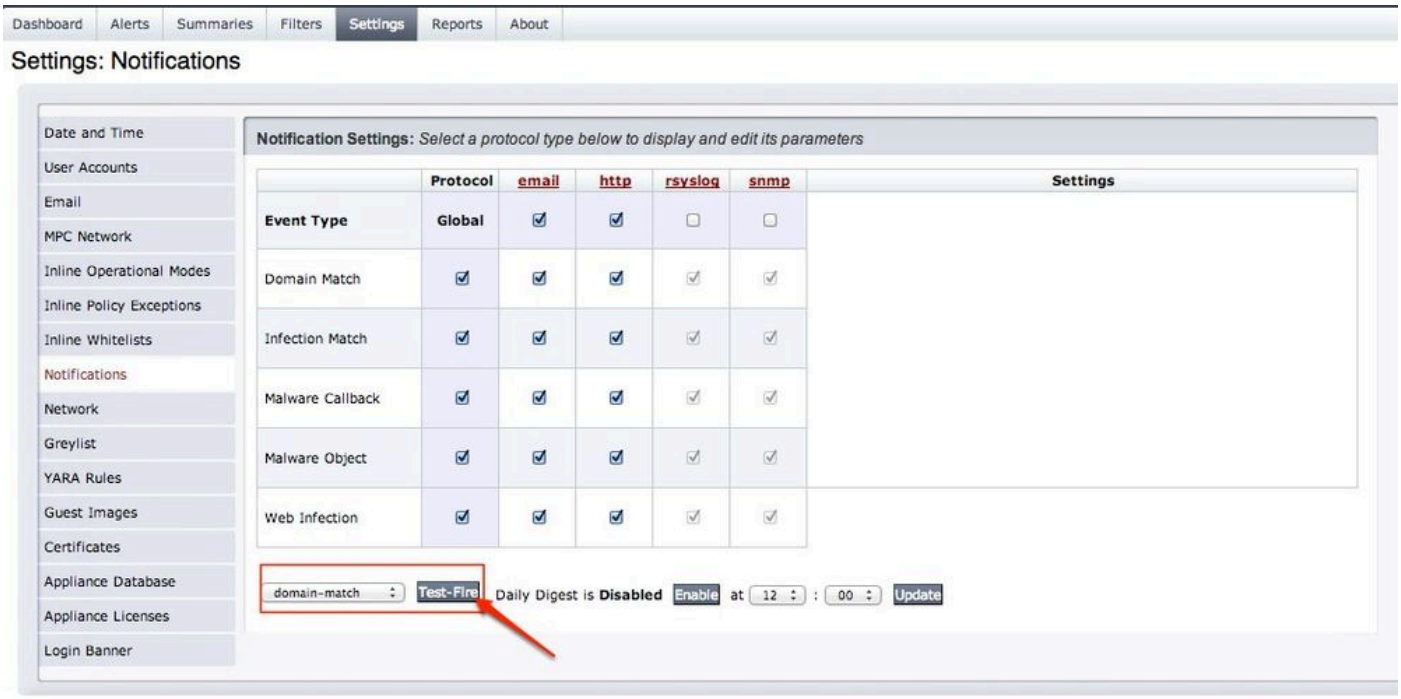
- Consegna: Base per evento
- Provider predefinito: Generico
- Parametri provider: Formato messaggio JSON esteso
- (Facoltativo) Se si preferisce inviare il traffico su SSL, selezionare SSL Enable (Abilita SSL).

A questo punto, l'appliance FireEye è impostata per inviare i tipi di evento selezionati a Cisco Umbrella. Quindi, scopri come visualizzare queste informazioni nel tuo Cisco Umbrella Dashboard e impostare un criterio per bloccare il traffico.

Garanzia di connettività: "Test Fire" tra FireEye e Cisco Umbrella

A questo punto, è consigliabile verificare la connettività e assicurarsi che tutto sia configurato correttamente:

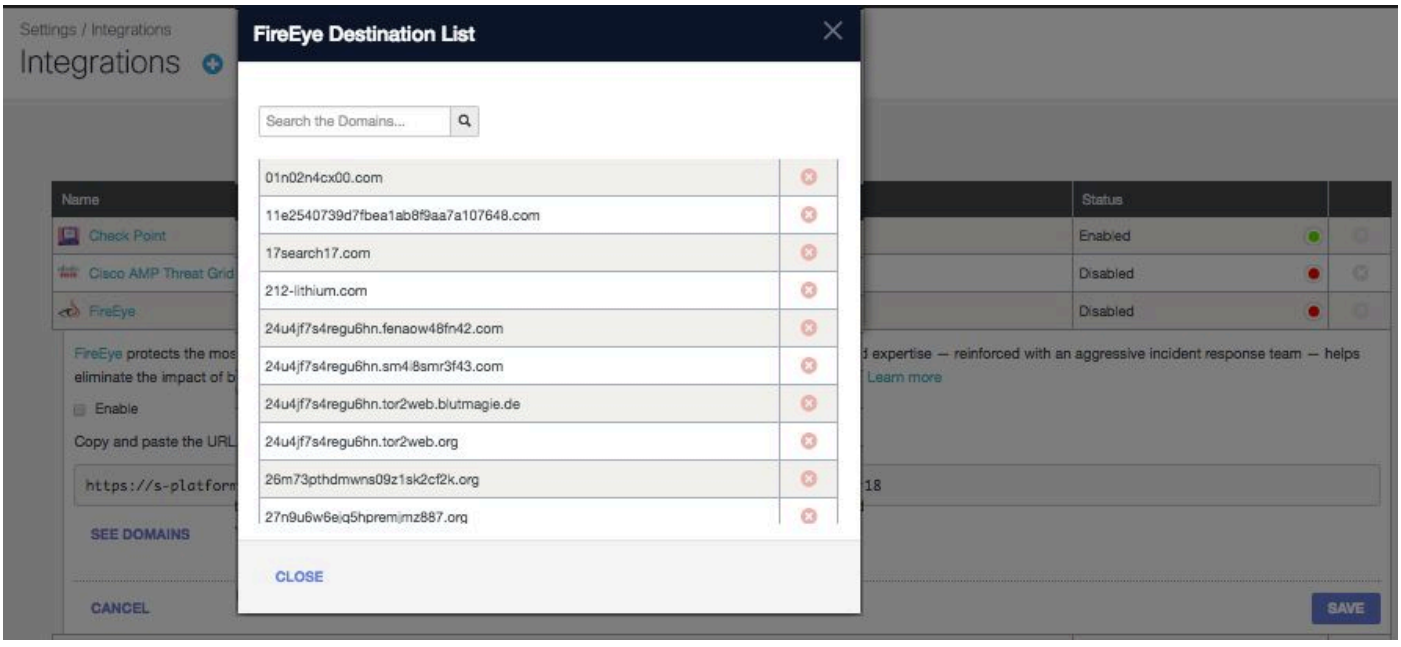
1. In FireEye, selezionare domain-match dal menu a discesa Test Fire e selezionare Test Fire:



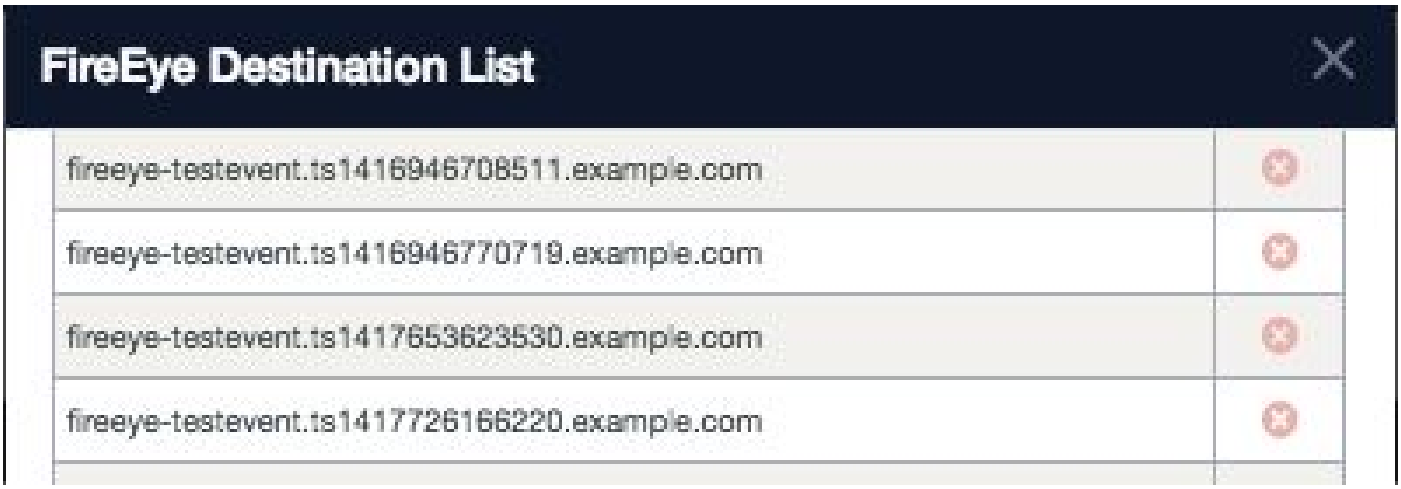
In Cisco Umbrella, l'integrazione FireEye include un elenco di domini forniti dall'appliance FireEye per individuare i domini che vengono aggiunti attivamente.

2. Dopo aver selezionato Test Fire, in Cisco Umbrella passare a Settings > Integrations (Impostazioni > Integrazioni) e selezionare FireEye nella tabella per espanderla.

3. Selezionare Vedere Domini.



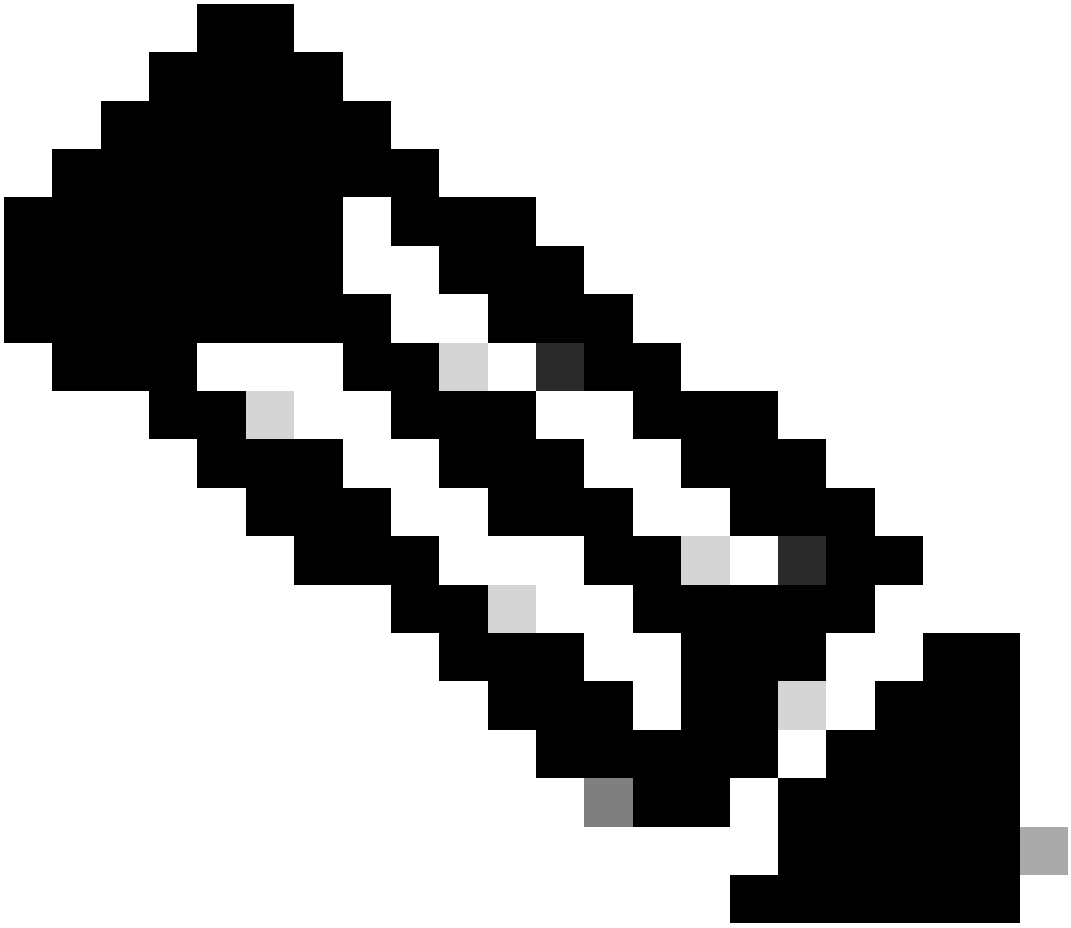
Se si seleziona Test Fire, nell'elenco delle destinazioni FireEye viene generato un dominio denominato "fireeye-testevent.example.com-[date]". Ogni volta che si seleziona Test Fire in FireEye, viene creato un dominio univoco con la data in UNIX Epoch time associata al test, in modo che i test futuri possano avere un nome di dominio di test univoco.



Se il test FireEye ha esito positivo, viene inviato un numero maggiore di eventi da FireEye a Cisco Umbrella e un elenco in cui è possibile eseguire ricerche inizia a essere popolato e a crescere.

Osservazione degli eventi aggiunti all'impostazione di protezione FireEye in "modalità di controllo"

Gli eventi generati dall'accessorio FireEye iniziano a compilare un elenco di destinazioni specifico che può essere applicato ai criteri come categoria di sicurezza FireEye. Per impostazione predefinita, l'elenco di destinazione e la categoria di sicurezza sono in "modalità di controllo" e non vengono applicati ad alcun criterio. Pertanto, non è possibile modificare i criteri Cisco Umbrella esistenti.



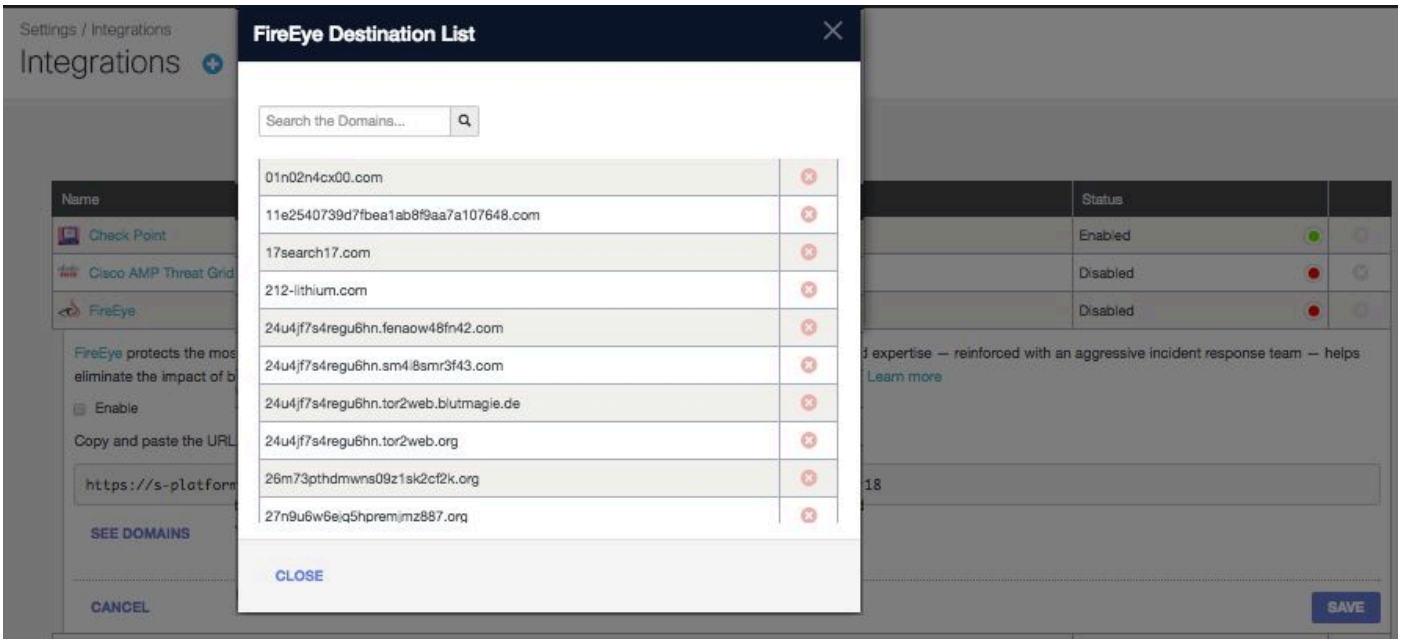
Nota: La "modalità di controllo" può essere attivata per il tempo necessario in base al profilo di distribuzione e alla configurazione di rete.

Esamina elenco di destinazione

È possibile rivedere l'elenco delle destinazioni di FireEye in qualsiasi momento:

1. Passare a Criteri > Componenti dei criteri > Integrazioni.

2. Espandere FireEye nella tabella e selezionare Vedere Domini.

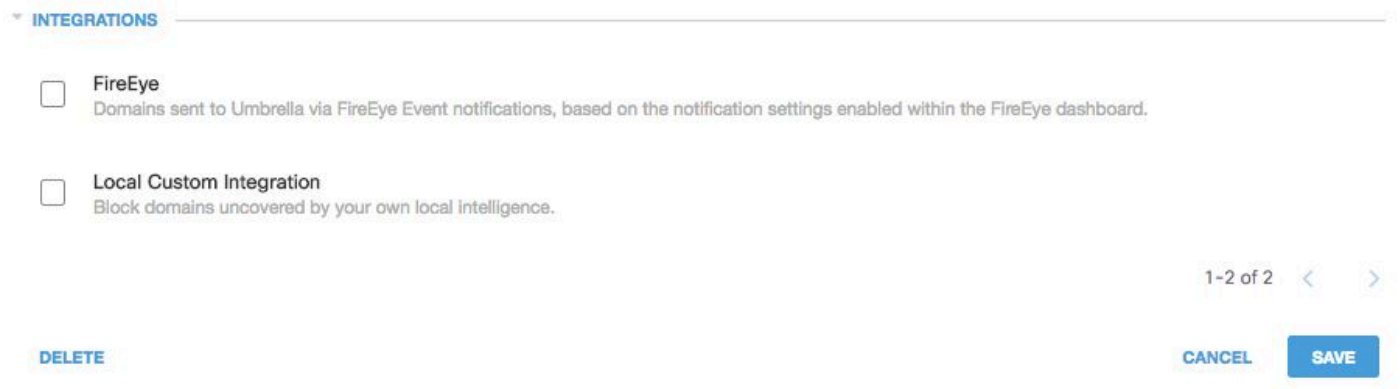


Rivedere le impostazioni di protezione per un criterio

È possibile rivedere le impostazioni di protezione che possono essere aggiunte a un criterio in qualsiasi momento:

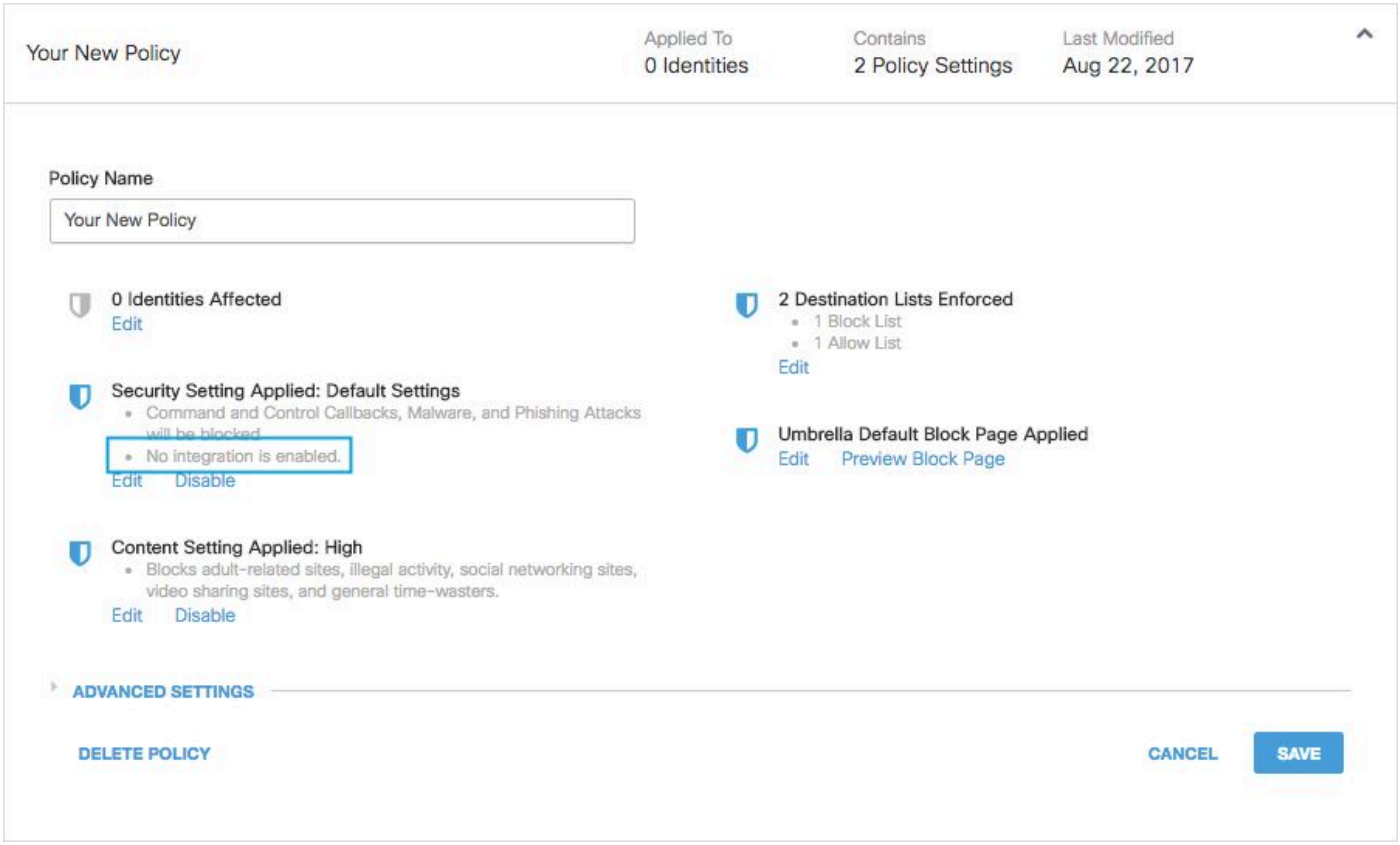
1. Passare a Criteri > Componenti criterio > Impostazioni protezione.

2. Selezionare un'impostazione di protezione nella tabella per espanderla e scorrere fino a Integrations per individuare l'impostazione FireEye.



115014080803

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



115013920526

Quando si inizia, è consigliabile lasciare deselezionata questa impostazione di protezione per garantire che i domini vengano popolati correttamente in modalità di controllo.

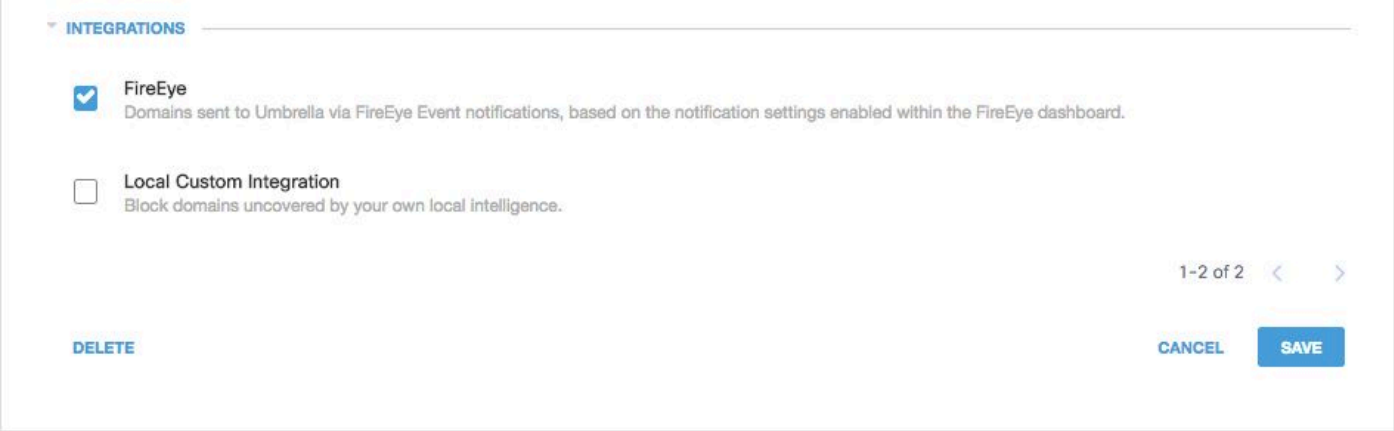
Applicazione delle impostazioni di protezione di FireEye in "Modalità blocco" a un criterio per client gestiti

Quando sei pronto a far applicare queste minacce alla sicurezza aggiuntive dai 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.

Creare o aggiornare innanzitutto le impostazioni di protezione:

1. Passare a Criteri > Componenti criterio > Impostazioni protezione.

2. In Integrazioni, selezionare FireEye e selezionare Salva.



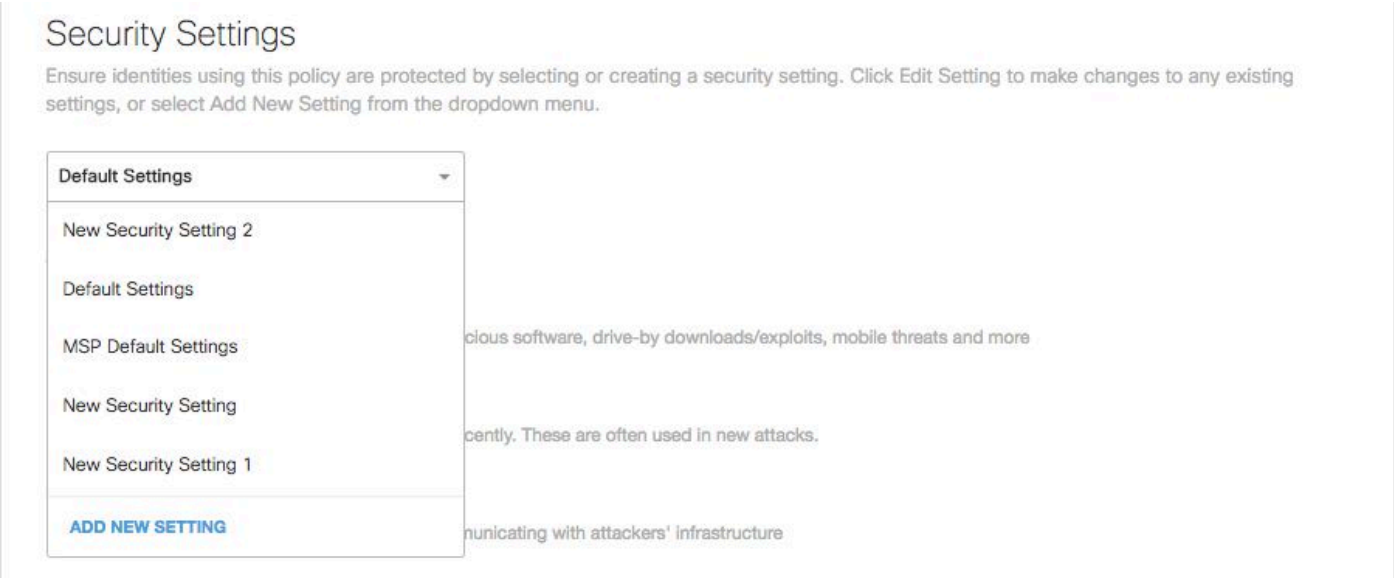
115013921406

Successivamente, nella Creazione guidata criteri, aggiungere questa impostazione di protezione al criterio che si sta modificando:

1. Passare a Criteri > Elenco criteri.

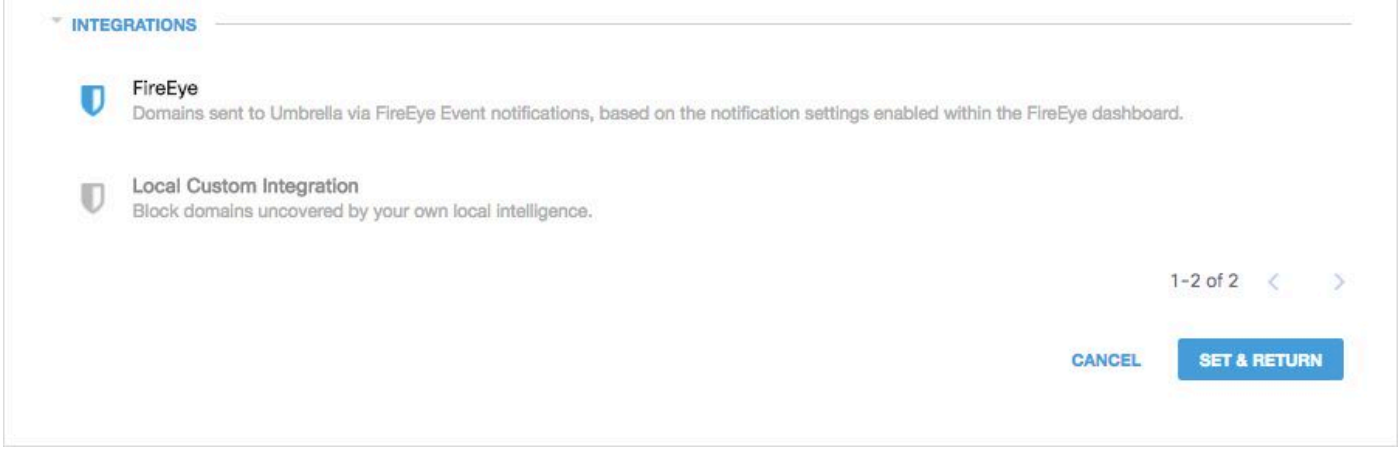
2. Espandere un criterio e in Impostazioni di protezione applicate selezionare Modifica.

3. Nell'elenco a discesa Security Settings (Impostazioni di sicurezza), selezionare un'impostazione di sicurezza che includa l'impostazione FireEye.



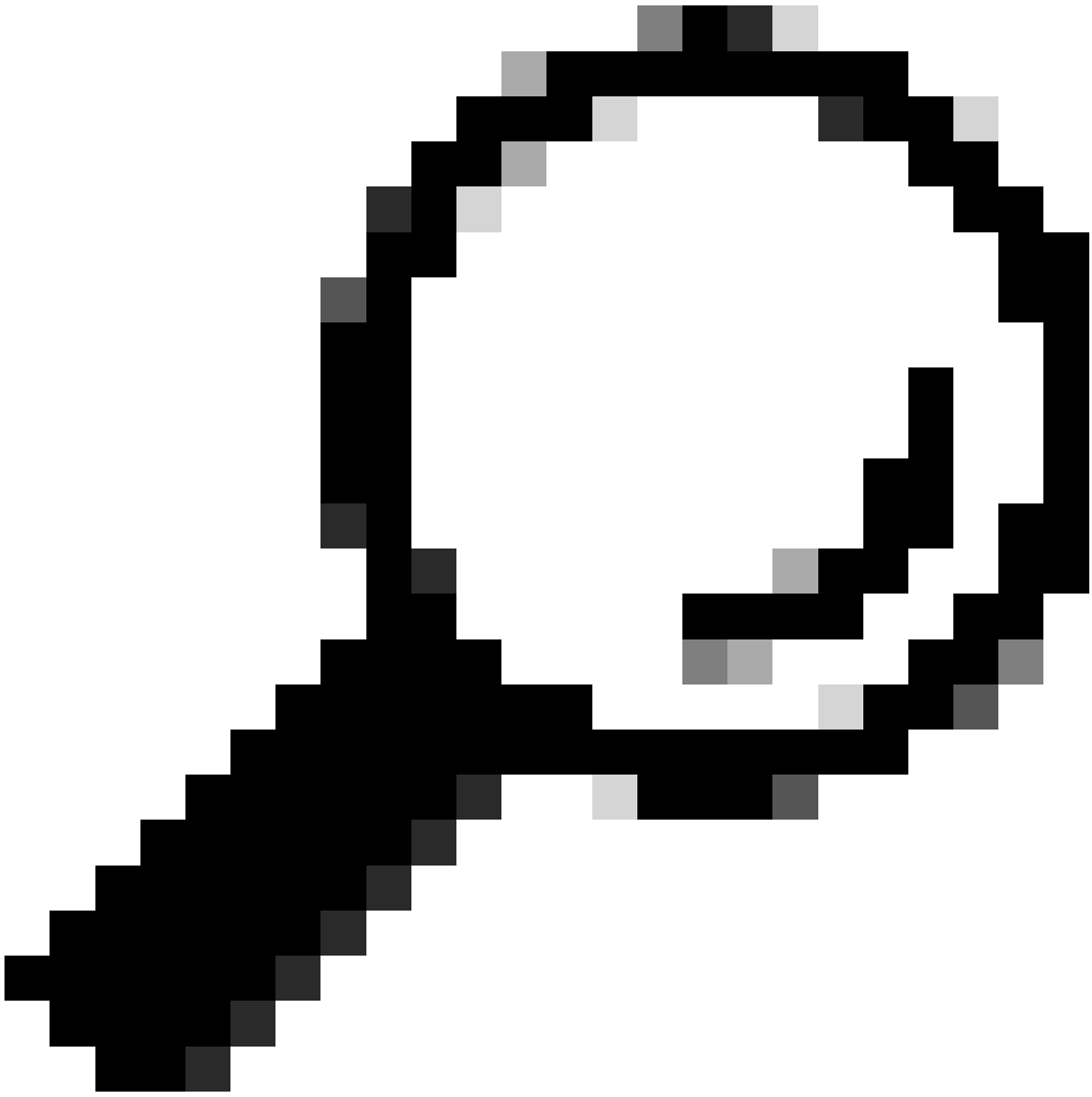
115014083083

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



115013922146

4. Selezionare Imposta &valore restituito.



Suggerimento: È inoltre possibile modificare le impostazioni di protezione tramite la Creazione guidata criteri.

I domini FireEye contenuti nell'impostazione di sicurezza di FireEye vengono bloccati per le identità che utilizzano il criterio.

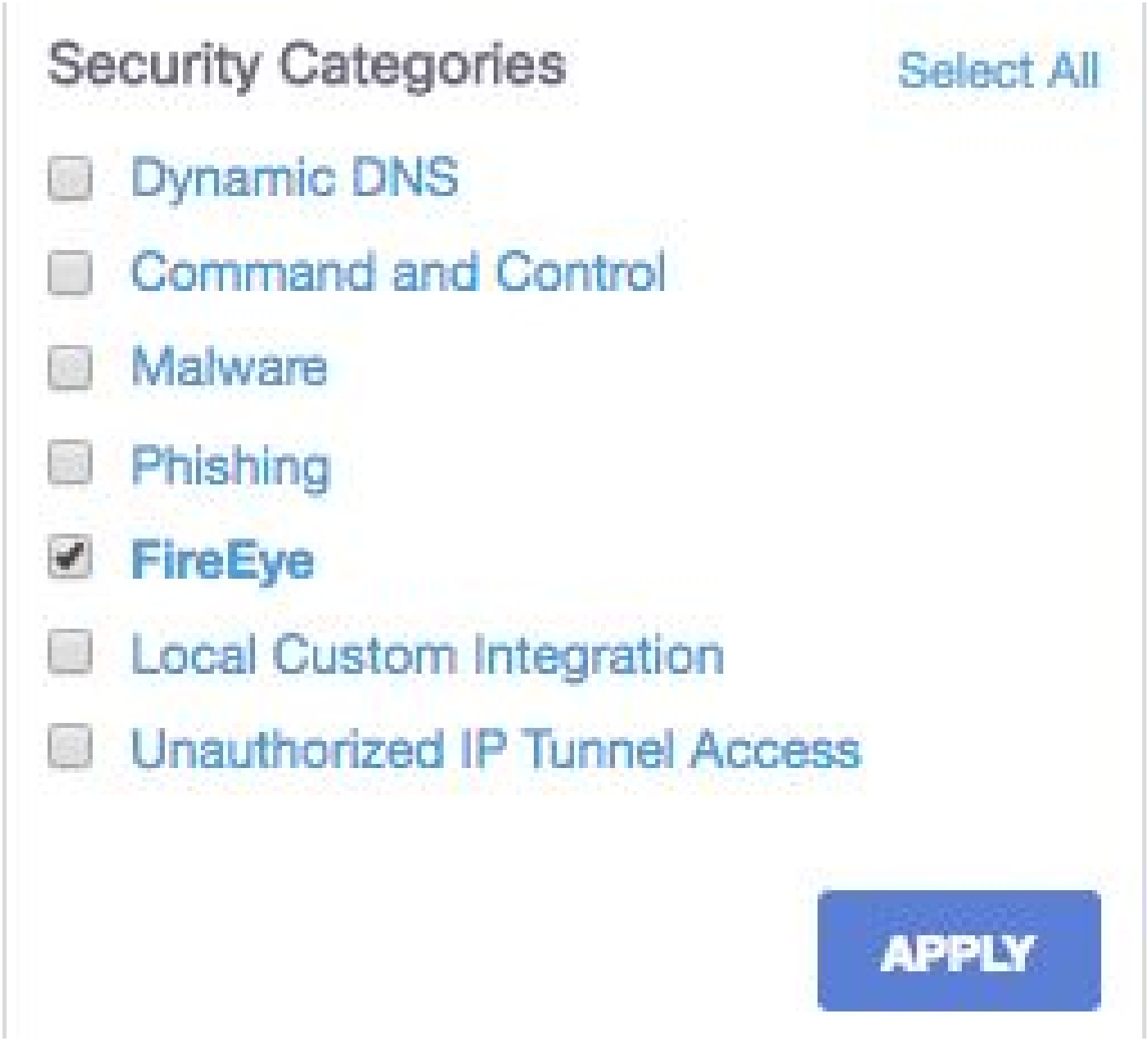
Segnalazione di eventi FireEye in Cisco Umbrella

Creazione di report sugli eventi di sicurezza FireEye

L'elenco delle destinazioni FireEye è una delle categorie di protezione disponibili per i 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 FireEye:

1. Passare a Reporting > Ricerca attività.

2. In Categorie di sicurezza, selezionare FireEye per filtrare il report in modo da visualizzare solo la categoria di sicurezza di FireEye.



115013924986

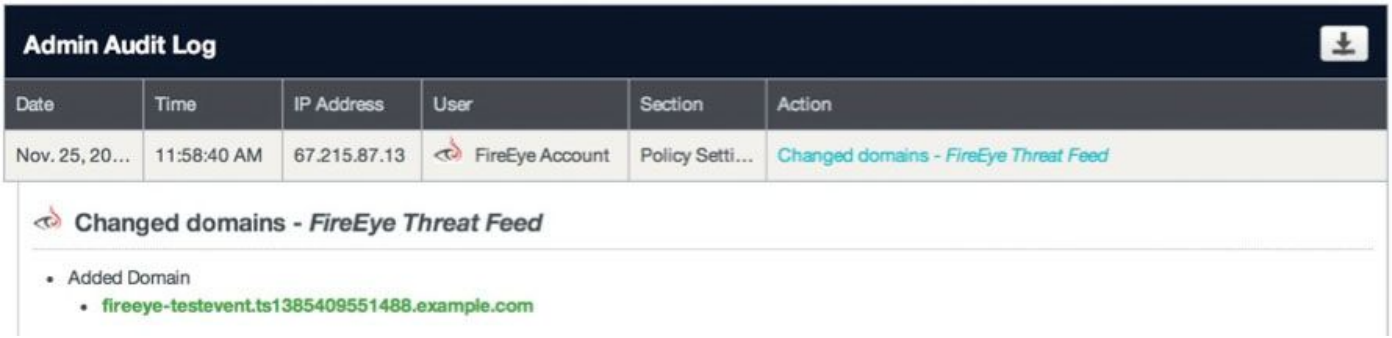
3. Selezionare Applica per visualizzare l'attività relativa a FireEye per il periodo selezionato nel rapporto.

Segnalazione dell'aggiunta di domini all'elenco di destinazione FireEye

Il registro di controllo Admin include gli eventi generati dall'accessorio FireEye durante l'aggiunta di domini all'elenco di destinazione. L'evento viene generato da un utente di nome "FireEye Account", anch'esso contrassegnato con il logo FireEye. Tali eventi includono il dominio aggiunto e l'ora in cui è stato aggiunto.

È possibile filtrare per includere solo le modifiche FireEye applicando un filtro per l'utente "FireEye Account".

Se il passaggio "Test Fire" è stato eseguito in precedenza, l'aggiunta del dominio di test FireEye può essere visualizzata nel registro di controllo.



Gestione di rilevamenti indesiderati o falsi positivi

Elenchi di destinazioni autorizzate

Benché improbabile, è possibile che i domini aggiunti automaticamente dall'accessorio FireEye attivino potenzialmente un rilevamento indesiderato che impedisca agli utenti di accedere a determinati siti Web. In una situazione come questa, Umbrella 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 preferibile.

- In primo luogo, nel caso in cui l'appliance FireEye dovesse aggiungere nuovamente il dominio dopo la rimozione, l'elenco Consenti protegge da questo problema causando ulteriori problemi.
- In secondo luogo, l'elenco degli indirizzi consentiti mostra una registrazione cronologica di domini problematici che possono essere utilizzati per analisi legali o report 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 FireEye in modalità blocco viene applicata solo a un sottoinsieme delle identità Cisco Umbrella gestite (ad esempio, viene applicata solo a computer mobili e dispositivi mobili in roaming), è possibile creare un elenco di autorizzazioni specifico per tali identità o criteri.

Per creare un elenco Consenti:

1. Passare a Criteri > Elenchi di destinazione e selezionare l'icona Aggiungi.

2. Selezionare Allow (Consenti), quindi aggiungere il dominio all'elenco.

3. Selezionare Salva.

Una volta salvato l'elenco di destinazione, è possibile aggiungerlo a un criterio esistente che copre i client interessati dal blocco indesiderato.

Eliminazione di domini dall'elenco delle destinazioni FireEye

Accanto a ciascun nome di dominio nell'elenco di destinazione FireEye è visualizzata l'icona Delete. L'eliminazione dei domini consente di pulire l'elenco di destinazione di FireEye in caso di rilevamento indesiderato.

Tuttavia, l'eliminazione non è permanente se l'appliance FireEye invia nuovamente il dominio a Cisco Umbrella.

Per eliminare un dominio:

1. Passare a Impostazioni > Integrazioni, quindi selezionare "FireEye" per espanderlo.

2. Selezionare Vedere Domini.

3. Cercare il nome di dominio che si desidera eliminare.

4. Selezionare l'icona Elimina.

5. Selezionare Chiudi.

6. Selezionare Salva.

Nel caso di un rilevamento indesiderato o di un falso positivo, Umbrella consiglia di creare immediatamente un elenco degli accessi consentiti in Cisco Umbrella e quindi di correggere il falso positivo all'interno dell'appliance FireEye. In seguito, è possibile rimuovere il dominio dall'elenco di destinazione di FireEye.

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).