Risoluzione dei problemi relativi all'integrazione del CCP con il CTR

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al processo del connettore SSE (Security Services Exchange) quando viene disabilitato su dispositivi Firepower Management Center (FMC) o Firepower Threat Defense (FTD) per l'integrazione con Cisco Threat Response (CTR).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CCP
- FTD
- Integrazione CTR

Componenti usati

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

- FMC sul software versione 6.4.0 o superiore
- FTD su software versione 6.4.0 o superiore
- Cisco Security Services Exchange
- Account CTR

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

Connettore SSEC

SSEConnector è un processo sui dispositivi Firepower dopo la 6.4.0 che consente di registrare i dispositivi nel portale SSE. Quando Cisco Cloud Configuration è impostato su On o Off, il FMC trasmette a tutti gli FTD gestiti. Dopo aver abilitato Cisco Cloud, il servizio SCEConnector avvia la comunicazione tra il portale SSE e i dispositivi Firepower. Ogni FTD richiede al CCP un token di registrazione che consente l'integrazione dei dispositivi nel portale SSE. Dopo questa integrazione, il contesto SSE viene attivato sui dispositivi e EventHandler viene riconfigurato per inviare eventi di intrusione al cloud Cisco.

CTR

Threat Response è un hub di orchestrazione per la risposta a minacce in caso di incidenti che supporta e automatizza le integrazioni tra più prodotti Cisco Security. Threat Response accelera le principali attività di sicurezza: rilevamento, analisi e risoluzione dei problemi, ed è un elemento chiave dell'architettura di sicurezza integrata.

Lo scopo di Threat Response è quello di aiutare i team operativi di rete e i responsabili degli incidenti a comprendere le minacce presenti sulla rete tramite tutte le informazioni sulle minacce raccolte e combinate disponibili da Cisco e da terze parti.

Ma più di ogni altra cosa, Threat Response è progettato per ridurre la complessità degli strumenti di sicurezza, aiutare a identificare le minacce e accelerare la risposta agli incidenti.

Threat Response è una piattaforma di integrazione (https://visibility.amp.cisco.com/). Il sistema funziona tramite "moduli", che sono parti di codice indipendenti che gestiscono le comunicazioni con diversi sistemi integrati (ad esempio Threat Grid, o AMP). Questi moduli gestiscono tutte e tre le funzioni che un sistema integrato può fornire (arricchimento, contesto locale e risposta).

Per quali scopi è possibile utilizzare CTR?

- Risposta all'incidente
- Indagini
- Caccia alle minacce
- Gestione dei casi

Quando si cerca un osservabile, tutti i moduli configurati richiedono ai sistemi di cui sono responsabili di cercare qualsiasi record di tali osservabili. Quindi prendono le risposte fornite e le restituiscono a Threat Response, poi prende i risultati raccolti da tutti i moduli (in questo caso il modulo Stealthwatch), e ordina e organizza i dati e li visualizza in un grafico.

Per integrare CTR con diversi prodotti sono coinvolti altri due portali "https://castle.amp.cisco.com/" (Castle) e "https://admin.sse.itd.cisco.com/app/devices" (Security Services Exchange)

Portale Castello

Qui è possibile gestire gli account di sicurezza Cisco:

Un account Cisco Security consente di gestire più applicazioni all'interno del portafoglio Cisco Security. In base ai diritti della licenza, ciò può includere:

- AMP for Endpoints
- Threat Grid
- Risposta alle minacce

Security Services Exchange Portal

Questo portale è un'estensione del portale CTR, dove è possibile gestire i dispositivi che sono stati registrati nel portale CTR, in modo da poter creare i token necessari per integrare i prodotti.

Security Services Exchange fornisce la gestione di dispositivi, servizi ed eventi quando si integrano determinati prodotti di sicurezza Cisco con Cisco Threat Response, inclusi questi prodotti e funzionalità:

- Gestire l'elenco di appliance di gestione della sicurezza integrate con Cisco Threat Response.
- Raccogliere i dati degli eventi dai dispositivi Cisco Firepower integrati per poterli inoltrare (automaticamente o manualmente) a Cisco Threat Response.

Risoluzione dei problemi

Verificare che i servizi cloud siano abilitati

Nel FMC verificare innanzitutto che in **System> Licenses > Smart Licenses** non sia attiva la modalità di valutazione.

In **System > Integration** (Sistema) nella scheda **Smart Software Satellite**, verificare che l'opzione selezionata sia **Connect direct to Cisco Smart Software Manager** (Connetti direttamente a Cisco Smart Software Manager) poiché questa funzione non è supportata in ambienti con spazi vuoti.

Spostarsi su **System> Integration** (Sistema) nella scheda **Cloud Services** (Servizi cloud) e verificare che l'opzione **Cisco Cloud Event Configuration** sia attivata.

Verifica della connettività tra FMC/FTD e il portale SSE

Poiché gli IP possono cambiare, è necessario consentire i seguenti URL:

Regione USA

- api-sse.cisco.com
- est.cisco.com (comune a più aree geografiche)
- mx*.sse.itd.cisco.com (attualmente solo mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (per il successo del cliente)
- eventing-ingest.sse.itd.cisco.com (per CTR e CDO)

Regione UE

- api.eu.sse.itd.cisco.com
- est.cisco.com (comune a più aree geografiche)
- mx*.eu.sse.itd.cisco.com (attualmente solo mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (per il successo del cliente)
- eventing-ingest.eu.sse.itd.cisco.com (per CTR e CDO)

Area APJ

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (comune a più aree geografiche)
- mx*.apj.sse.itd.cisco.com (attualmente solo mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (per il successo del cliente)
- eventing-ingest.apj.sse.itd.cisco.com (per CTR e CDO)

Sia FMC che FTD necessitano di una connessione agli URL SSE sull'interfaccia di gestione. Per verificare la connessione, immettere questi comandi sulla CLI di Firepower con accesso root:

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

Dopo l'esecuzione di ogni comando, è necessario visualizzare questa riga alla fine della connessione: **connessione n. 0 all'host "URL" lasciata intatta**.

Se la connessione scade o non si riceve questa riga nell'output, verificare che le interfacce di gestione siano autorizzate ad accedere a questi URL e che non vi siano dispositivi upstream che bloccano o modificano la connessione tra i dispositivi e questi URL.

Il controllo del certificato può essere ignorato con questo comando:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
```

```
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

> **Nota:** Viene visualizzato il messaggio 403 Forbidden poiché i parametri inviati dal test non corrispondono a quanto previsto da SSE, ma questo è sufficiente per convalidare la connettività.

Verifica stato SSEConnector

Èpossibile verificare le proprietà del connettore come indicato di seguito.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

Per verificare la connettività tra SSConnector e EventHandler, è possibile utilizzare questo comando, ad esempio:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

Nell'esempio di una connessione stabilita, è possibile vedere che lo stato del flusso è connected (connesso):

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

Verifica dei dati inviati al portale SSE e al CTR

Per inviare eventi dal dispositivo FTD a SEE una connessione TCP deve essere stabilita con https://eventing-ingest.sse.itd.cisco.com Questo è un esempio di connessione non stabilita tra il portale SSE e FTD:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

Nei log di connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **Nota:** Notato che gli indirizzi IP visualizzati 18.205.49.246 e 18.205.49.246 appartengono a https://eventing-ingest.sse.itd.cisco.com e potrebbero cambiare, ecco perché si consiglia di consentire il traffico verso il portale SSE in base all'URL anziché agli indirizzi IP.

Se la connessione non viene stabilita, gli eventi non vengono inviati al portale SSE. Si tratta di un esempio di connessione stabilita tra FTD e il portale SSE:

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

Problemi comuni

Dopo l'aggiornamento alla versione 6.4, il connettore SSE non comunica con il portale SSE. Connector.log fornisce errori simili agli eventi:(*Service).Start] Impossibile connettersi all'endpoint PUSH ZeroMQ: impossibile chiamare \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: connetti: file o directory non esistente\n"

Riavviare il servizio SCEConnector:

1) sudo pmtool disablbyid SSEConnector

2) sudo pmtool enablebyid SSEConnector

3) Riavviare il dispositivo. Al riavvio, il dispositivo comunica al cloud.

Posizioni importanti dei file di log

Registri di debug: visualizza i messaggi di connessione o errore

```
/ngfw/var/log/connector/connector.log
```

Impostazioni di configurazione

```
/ngfw/etc/sf/connector.properties
```

Impostazioni di configurazione

```
curl localhost:8989/v1/contexts/default
```

Informazioni correlate

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Documentazione e supporto tecnico – Cisco Systems