

دی دهتلا عبّتت عبّتت ةزيم ىلع فرعت
7.6 رادص إلأ يف Talos ماظن مادختساب

تایوتیم

٦٥

وقد أتى بـ[البيان](#)

تاتل طت ملا

قم دختن ملایان و کمالا

قزملا لیصافت

مختصر FMC

لِمَعِي فِيكَ

3 ترفن

ثادح أول جل اعم

لِمَعِي فِي كِ

اھالص او عاطخآل ا فاش کتسا

زاهجلا - اهحالص او ثادحألا جلاعم عاطخأ فاشكتسأ

احالص او زاهجلانی وکت عاطخاً فاش رکتسا

ةمدقملا

7.6. "Talos" تادی دهت بقوعت رثأ عبعت عبعت ۃزم دنتسملا اذه فصی

ةي س، اس، ئلا تاب ل طت مل

مالی طبلات

ةيسيس، ألا ةزه جألاو جمار بـلـلـ يـنـ دـأـلـاـ دـحـلـاـ

Minimum Supported Manager Version	Managed Devices	Min. Supported Managed Device Version Required	Notes
cdFMC/FMC 7.6.0	FTD in Native Mode/HA/Cluster	<ul style="list-style-type: none"> 7.6.0 	Snort 3 only

- نم ۋېزملا ئىباجى إىلا تارابتخارا او ئىتارابختسى إىلا تامولعملا عەمجىلۇ ۋەدقىلا رفويى.
 - ئىرانلا ۋقااطلۇ ۋەزەجأىلى اھعفدىتى يىتلە دعاووقلا نم ۋەصاخ ۋەمۆجم لالخ.
 - ئەطس اوپ اھكالەتسى مەتىي و، SSX لصۈم ربىع ۋېباخسلىنىڭ ئادىجەنەن سەرەتلىك طققى.
 - ئەسايىسلى نېۋەكت نم عزجك تادىدەتلىنىڭ ۋەچبىلا دعاووق نەمىضىتت ئەدىدەن زېيم رايىت خانىخ.
 - لېجىستل instance-* لىلە لىخاد (threat_telemetry_snort-unified.log.*) دىدەج لىجىس فىلم دەجۇيى.
 - تادىدەتلىنىڭ ۋەچبىلا دعاووق، نم عزجك أش بىنەت يىتلە قارتبخالا ئادىجەنەن سەرەتلىك طققى.

- يـف دـيـدـج لـجـس عـونـك تـادـيـدـهـتـلـا نـع ثـحـبـلـا دـعـأـوـقـل IPS لـقـتـقـفـمـلـا نـزـاخـمـلـا غـيـرـفـتـبـ مـقـةـيـفـاـضـإـلـا تـانـاـيـبـلـا.
- ىـلـا IPS/Packet/Extradata ثـادـحـأـ لـاسـرـال دـيـدـج كـلـهـتـسـم EventHandler طـوـغـضـوـنـمـضـمـوـ، لـمـاـكـلـابـ لـهـفـمـ قـيـسـنـتـبـ ةـبـاحـسـلـا FMC مـدـخـتـسـمـ ةـهـجـاـوـ يـف ثـادـحـأـلـا هـذـهـ ضـرـعـ مـتـيـ الـ.

ةـمـدـخـتـسـمـلـا تـانـوـكـمـلـا

ةـنـيـعـم ةـيـدـام تـانـوـكـمـوـجـمـارـب تـارـادـصـا ىـلـع دـنـتـسـمـلـا اـذـهـ رـصـتـقـيـ الـ.

ةـصـاخـ ةـيـلـمـعـم ةـئـيـبـ يـف ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـم دـنـتـسـمـلـا اـذـهـ يـف ةـدـرـاـوـلـا تـامـوـلـعـمـلـا عـاشـنـا مـتـ تـنـاـكـ اـذـاـ (ـيـضـاـرـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـف ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـم دـكـأـتـفـ، لـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

ةـزـيـمـلـا لـيـصـاـفـتـ

ةـمـدـخـتـسـمـ ةـهـجـاـوـ FMC

- مـاظـنـلـا / نـيـوـكـتـلـا / لـفـطـتـلـا جـهـنـ لـيـضـفـتـ ةـحـفـصـ يـف ةـدـيـدـجـ ةـزـيـمـ ةـمـالـعـ رـايـتـخـاـ ةـنـاخـ مـاظـنـبـ تـادـيـدـهـتـلـا Talos.
- تـيـبـثـتـلـا تـايـلـمـعـ نـم لـكـلـ، يـضـاـرـتـفـاـ لـكـشـبـ لـيـغـشـتـلـا دـيـقـ ةـزـيـمـلـا ةـمـالـعـ نـوـكـتـ 7.6.0.
- نـيـكـمـتـ" يـرـايـخـ نـم لـكـ نـيـكـمـتـ بـجـيـ Cisco". حاجـنـ ةـكـبـشـ نـيـكـمـتـ" ىـلـع ةـزـيـمـلـا دـمـتـعـتـ تـادـيـدـهـتـ نـع ثـحـبـلـا عـاطـخـأـ عـبـتـتـ عـبـتـتـ" وـ" حاجـنـ ةـكـبـشـ Telemetry".
- لـصـوـمـ ىـلـا اـهـعـفـ دـوـ ثـادـحـأـلـا ةـجـلـا عـمـلـ SSE_ThreatHunting.json دـوـجـوـ مـزـلـيـوـ، لـيـغـشـتـلـا SSE.
- رـادـصـ إـلـا مـادـخـتـسـابـ ةـرـادـمـلـا ةـزـهـجـأـلـا عـيـمـجـ ىـلـا ةـزـيـمـلـا ةـمـالـعـ ةـمـيـقـ نـمـاـزـتـتـ 7.6.0.

لمـعـيـ فـيـكـ

Firewall Management Center

System / Configuration

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Access List
Access Control Preferences
Audit Log
Audit Log Certificate
Change Management
Change Reconciliation
DNS Cache
Dashboard
Database
Email Notification
External Database Access
HTTPS Certificate
Information
Intrusion Policy Preferences
Language
Login Banner
Management Interfaces
Network Analysis Policy Preferences
Process
REST API Preferences
Remote Storage Device
SNMP
Session Timeout

Comments on policy change: Optional

Write changes in Intrusion Policy to audit log:

Retain user overrides for deleted Snort 3 rules:

Talos Threat Hunting Telemetry:

Firewall Management Center

Integration / Cisco Security Cloud

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Cisco Security Cloud Integration

This feature allows Cisco Secure Firewall Management Center to integrate with Cisco cloud services using Cisco cloud integration.

Integration

Select Cloud Region: staging-sse.cisco.com

After enabling Cisco Security Cloud, come back to this page to complete the settings, and click Save.

Enable Cisco Security Cloud

Settings

Event Configuration:

- Send events to the cloud
 - Intrusion events
 - File and malware events
 - Connection events
 - Security
 - All

+AI Assistant

The +AI Assistant enables administrators to retrieve and understand policy rule attributes and configurations. This tool facilitates in-depth policy investigation that helps administrators manage firewall configurations and strengthen network security. Learn more ↗

Enable +AI Assistant

Cisco Security Cloud Support

Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco. Learn more ↗

> Enable Cisco Success Network

> Enable Cisco Support Diagnostics

Cisco XDR Automation

Enable Cisco XDR Automation to allow Cisco XDR user to build automated work flows that interact with various resources in the Secure Firewall Management Center.

Note that Cisco XDR, which integrates with the broad Cisco security portfolio to provide extended detection and accelerated response capabilities, is a licensed product. Learn more ↗

Enable Cisco XDR Automation

- يف ۋەزىملا ۋەمالۇ نېزخەت مەتى - /etc/sf/threat_hunting.conf ىلۇغۇ FMC.
- ياف ۋەزىملا ۋەمالۇ "threat_hunting" ىلۇغۇ اپىيأ ھەذە ۋەزىملا ۋەمالۇ ۋەمىق ظەفحەت مەتى يف ۋەرەدەملا ۋەزەجىڭلار ىلۇغۇدا چۈنەتىملىك كەلذى دەب مەتى يىذلەو، /ngfw/var/tmp/tds-cloud-events.json.
- ياف ۋەزىملا ۋەمالۇ ئەنمازىت ئەل ۋەمالۇ ۋەمىق تىنالىك اذى امەم قىقەتلىلىك تالىجىسى:

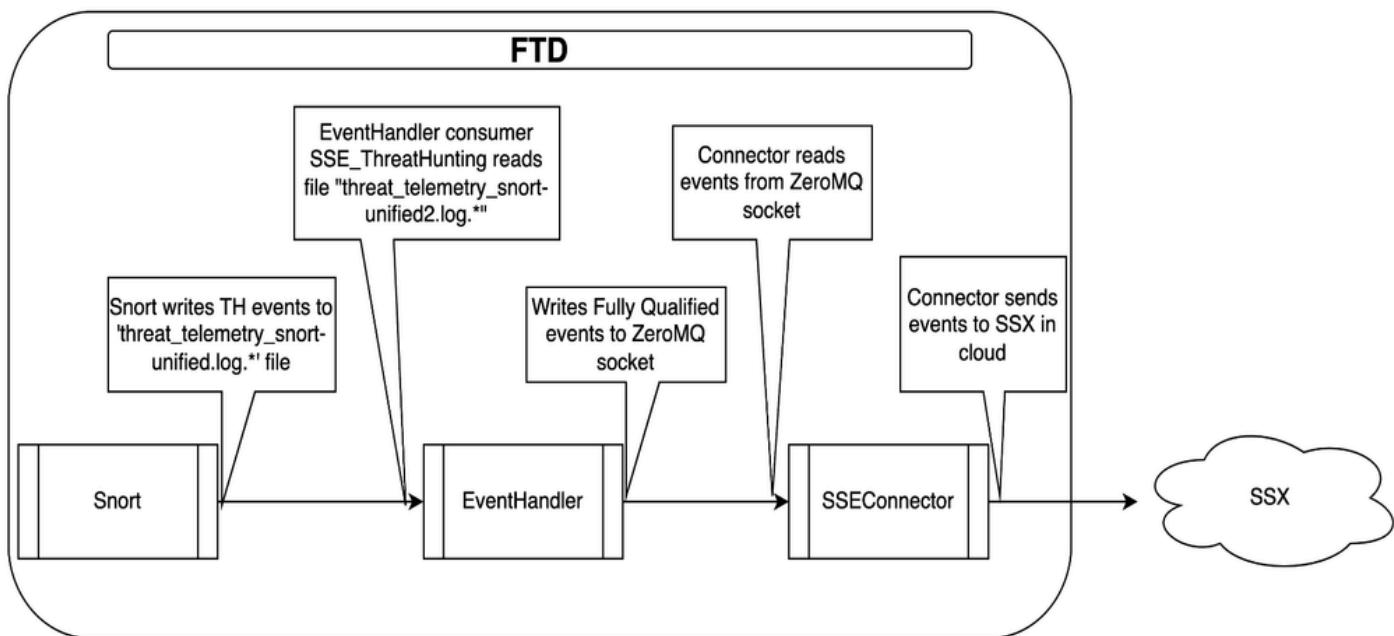
 - /var/log/sf/data_service.log ىلۇغۇ FMC.
 - /ngfw/var/log/sf/data_service.log ىلۇغۇ FTD.

- يتل ا ظقير طلا سفن ب (THT) تادي ده تلا تاع و مجم مادختس ا عب ت دع او ق ظج لاعم متت
وعي اشلا IPS دع او ق ظج لاعم اه ب متت.
 - ىل ا طقف دع ب نع تادي ده تلا ساي قب ظصا خلا IPS ثادحأ FTD U2Unified Logger بتكي
مدختسم ل ظيئرم ريق غ ثادحألا هذه نإف ، يلاتل اب و .*. THREAT_Telemetry_snort-unified.log.*
 - غيرفت ىلع تادي ده تلا مادختس ا عب ت دع او ق ظج لاعم ديجوم لي ل دلا سفن يف دوجوم ديجوم فلمل ا FTD snort-unified.log.*
 - دع اقل ا مييقتل ظدم دختسم ل (IPS) قارت خالا عنم ماظنل ظتق فمل ن زاخمل ا
 - عب ت دع او ق ظج لاعم تان اي ب ، قارت خالا عنم ماظنل دع اق اه رابتعاب و
نك مي ال ، كل ذ عم و . رخش للا بناج ىلع ثادحألا ظي فصل عوض و م يه تادي ده تلا
ي ف ظجردم ريق اهن أ ، دع او قل event_filter ن يو كت ي ئاهن للا مدختس ملل FMC.

ثادح أول جلاغم

- ڈھومنا فلملا ئىداب يف Packet و Extradataevents threat_telemetry_snort-unified.log.*.
 - لصوم رباع ئېباخسلا ئىل اهل اس را و ئادحألا هذه ئەجلاع مب زاھىل ئىلۇم موقي SSX.
 - ئادحألا هذه دىدجىل ئەجلاع ئەت سىم:
 - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
 - ئەجلاع ملار دنۇر رفوت طقىف هلېغىشت مەتىي - ئې يولوألا ضفخىنم طبارت رشۇم ئەفاضالا (CPU) ئىزكىرمىلار

لمعي فيك



اھالص او ءاطخآل ا فاشڪتسا

زاهجلا - اححالص او ثادح الـ جـ لـ اعـمـ عـاطـخـ اـ فـ اـشـ كـ تـسـ

- تالجسل /ngfw/var/log/messages يف ثحبلا EventHandler

```
Jan 11 21:26:01 firepower SF-IMS[39581]: [10055] EventHandler:EventHandler[INFO] Consumer SSE_ThreatHun
```

- ثدحلا ةجلام لياصافت ىلع لوصح لـ /ngfw/var/log/EventHandlerStats

```
{"Time": "2024-01-11T21:26:01Z", "ConsumerStatus": "Start SSE_ThreatHunting", "TID": 10055}  
{"Time": "2024-01-11T21:31:56Z", "Consumer": "SSE_ThreatHunting", "Events": 9, "PerSec": 0, "CPUsec": 0}  
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionExtraData", "InTransforms": 0}  
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionPacket", "InTransforms": 0}  
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionEvent", "InTransforms": 0}
```

- ثادحأ عاشناب موقـي Snort ناك اذا امم قـقحتـف ، ثـادـحـأـيـ مـلـ اذاـ تـادـيـ دـهـتـ بـعـ ثـحـبـلـاـ

```
ls -l /ngfw/var/sf/detection_engines/*/instance-1 | grep unified
```

- جـارـخـإـلـاـ اـذـهـ صـحـفـ قـيـرـطـ نـعـ ةـبـولـطـمـلـاـ ثـادـحـأـلـ تـافـلـمـلـاـ نـمـ قـقـحـتـ
- "threat_telemetry_snort-unified.log"

```
u2dump output:u2dump/ngfw/var/sf/detection_engines/*/instance-1/threat_telemetry_snort-unified.log.1704
```

- نـمـ قـقـحـتـفـ ، ةـبـولـطـمـلـاـ ثـادـحـأـلـاـ ىـلـعـ تـافـلـمـلـاـ يـوـتـحـتـ مـلـ اذاـ
 - الـ مـأـ تـادـيـ دـهـتـلـاـ بـعـ ثـحـبـلـاـ نـيـوـكـتـ نـيـكـمـتـ مـتـ اذاـ اـمـ
 - الـ مـأـ لـيـغـشـتـلـاـ دـيـقـ Snortprocess نـاكـ اذاـ اـمـ

اـحـالـصـ اوـ زـاهـجـلـاـ نـيـوـكـتـ عـاطـخـأـ فـاشـكـتـسـأـ

- تـادـيـ دـهـتـلـاـ بـقـعـتـ عـبـتـتـ ثـادـحـأـ نـكـمـيـ SNORTـ نـيـوـكـتـ نـاكـ اذاـ اـمـ قـقـحـتـلـاـ

```
/ngfw/var/sf/detection_engines/
```

```
/snort3 --plugin-path /ngfw/var/sf/detection_engines/
```

```
/plugins:/ngfw/var/sf/lsp/active-so_rules-c /ngfw/var/sf/detection_engines/
```

```
/snort3.lua --dump-config-text 2>/dev/null | grep "sfUnified2_logger.threat_hunting_telemetry_g
```

- ةدوجوم تاديدهتلا نع ثحبلاء يللمع عبّتت عبّتت دعاؤق تناك اذا امم ققحت اال مؤنكم و:

```
/ngfw/var/sf/detection_engines/
```

```
/snort3 --plugin-path /ngfw/var/sf/detection_engines/
```

```
/plugins:/ngfw/var/sf/lsp/active-so_rules -c /ngfw/var/sf/detection_engines/
```

```
/snort3.lua -lua "process=nil" --dump-rule-state 2>/dev/null | grep "\"gid\": 6,"
```

- ديـدـحـتـتـاـيـيـاصـحـاـيـفـتـاـيـدـهـتـلـاـنـعـثـحـبـلـاـتـايـلـمـعـعـبـّـتـتـدـعـاؤـقـنـيـمـضـتـمـتـيـ،ـيـزـكـرـمـلـاـةـجـلـاعـمـلـاـةـدـحـوـتـقـوـنـمـارـيـبـكـاـرـدـقـدـعـاؤـقـلـاـتـكـلـهـتـسـاـاـذـافـ،ـاـذـلـ.ـدـعـاؤـقـلـاـتـامـسـةـجـلـاعـمـلـاـةـدـحـوـقـحـفـصـىـلـعـدـعـاؤـقـلـاـتـامـسـدـيـدـحـتـتـاـيـيـاصـحـاـيـفـةـيـئـرـمـحـبـصـتـاـهـنـافـةـيـزـكـرـمـلـاـ(ـFMCـ).

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).