Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.4.x

First Published: 2023-09-11

Last Modified: 2023-12-13

Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center

Cisco Success Network allows enrolled management center to continuously stream real-time configuration and operating state information to the Cisco Success Network cloud. This document provides a list of the collected and monitored data.

Enrolled Device Data

Once you enroll the management center in Cisco Success Network, selected telemetry data about the enrolled management center device is streamed to the Cisco cloud. The following table describes the collected and monitored data about the enrolled device. The data includes feature-specific information about intrusion policies (both system-provided and custom) and malware detection for enrolled management centers.

Table 1: Enrolled Device Telemetry Data

Data Point	Example Value
Device Name	Management Center East
Device UUID	24fd0ccf-1464- 491f-a503- d241317bb327
Device Model	Cisco Secure Firewall Management Center for VMWare
Serial Number	9AMDESQP6UN
System Uptime	99700000
Product Identifier	FS-VMW-SW-K9
Smart License PIID	24fd0ccf-1464- 491f-a503- d241317bb327
Virtual Account Identifier	CiscoSVStemp
Smart LicenseVirtual Account Name	FTD-ENG-SJC
Count of SSO is enabled.	1

Data Point	Example Value
Number of SSO users.	2
SSO identity provider.	okta
Is SecureX feature on management center enabled?	1

Software Version Data

Cisco Success Network collects software information that pertains to the enrolled management center device, including software version, rule update version, geolocation database version, and vulnerability database version information. The following table describes the collected and monitored software information about the enrolled device.

Table 2: Software Version Telemetry Data

Data Point	Example Value
Management Center Software Version	{ type: "SOFTWARE", version: "x.x.x.x" }
Rule Update Version	{version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
Vulnerability Database (VDB) Version	{version: "271", lastUpdated: 1468606837000 }
Geolocation Database Version	{version: "850" }

Managed Device Data

Cisco Success Network collects information about all the managed devices associated with an enrolled management center. The following table describes the collected and monitored information about managed devices. This includes feature-specific policy and licensing information, such as URL filtering, intrusion prevention, and malware detection for managed devices.

Table 3: Managed Device Telemetry Data

Data Point	Example Value
Managed Device Name.	firepower
Managed Device Version.	6.2.3-10616
Managed Device Manager.	Management Center
Managed Device Model.	Cisco Firepower 2130 NGFW Appliance Cisco Threat Defense VMware
Managed Device Serial Number.	9AMDESQP6UN
Managed Device PID.	FPR2130-NGFW-K9 NGFWv

Data Point	Example Value
Snort Engine.	SNORT3
Errors for localUrlCount plugin if failed to retrieve data.	"errors": ["Ping DB trial no. 1 ", "SF::SFDBI::ping", "Ping returned 1", "Can't call method \"getPayload\" on an undefined value at /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent.pm line 1906.", "", "Printing stack trace:", " called from /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent. pm (1906)", " called from /usr/local/sf/lib/perl/5.10.1/SF/SSE/devices _plug.pm (409)", " called from /usr/local/sf/bin/devices_plug.pl (76)", " called from /usr/local/sf/bin/devices_plug.pl (93)"]
Is Device Connected to Manager?	True
Container Status (Standalone, cluster, or HA).	"Cluster"
Device on-boarding method	USING_SERIAL_NUMBER_VIA_CDO
Is URL Filtering License Used for Device?	True
AC Rules with URL Filtering Per Device.	10
Number of AC Rules with URL Filtering That Use URL Filtering License.	3
Number of AC Rules with URL Filtering That Use Threat License.	3
Is Threat License Used for Device?	True
Does AC Policy Have Intrusion Rule Attached?	True
Number of AC Rules with Intrusion Policies.	10
Is Malware License Used for Device?	True

Data Point	Example Value
Number of AC Rules with Malware Policy.	10
Number of AC Rules with Malware Policy That Use Malware License.	5
Is Threat Intelligence Director (TID) Used for Device?	True
Number of Static Routes.	4
VRF Count.	0
Is remote deployment of HA on device attempted?	False
Is device certificate visible?	False
Is nsz value set on managed device?	False
Is ogs value set on managed device?	False
NS network count.	2
Count of local URL items.	{"url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks", "count": 10}, {"url": "/api/local/fmc_platform/v1/info/serverversion", "count": 2}

The following table includes all information regarding port scan settings.

Data Point	Example Value
Detection on traffic	"Allowed"
ICMP host	50
Is ICMP host sweep enabled?	TRUE
ICMP interval	50
Inspection mode	"Detection"
IP host	50
IP interval	50
IP protocol	50
Is IP protocol scan enabled?	TRUE
Is IP protocol sweep enabled?	TRUE
Sensitivity type	"Custom"
Shun duration	50

Data Point	Example Value
TCP interval	100
TCP port	56
TCP port host	59
Is TCP port scan enabled?	TRUE
Is TCP port sweep enabled?	TRUE
UDP host	50
UDP interval	50
UDP port	50
Is UDP port scan enabled?	TRUE
Is UDP port sweep enabled?	TRUE

The Cisco Success Network collects information about migrating configurations from one threat defense model to an equivalent or higher-capacity model. The following table describes the information collected regarding threat defense model migration.

Data Point	Example Value
Elapsed time	6366
Errors	An integer value of 0 or greater
Is model migration completed?	True
Is the device reset?	False
Number of interfaces	An integer value of 0 or greater
Source device container status (Standalone, cluster, or HA)	"Standalone"
Model of the source device	"Cisco Firepower 2130 Threat Defense"
UUID of the source device	"a8eee3f4-aa19-11ed-bda9-857788e8d45a"
Is IP protocol scan enabled?	TRUE
Threat Defense version of the source device	"7.2.0"
Target device container status (Standalone, cluster, or HA)	"Standalone"
Model of the target device	"Cisco Secure Firewall 3105 Threat Defense"
Threat Defense version of the target device	"7.3.0"

The following table includes all information as per policy level

Data Point	Example Value
Number of Access Policy devices assigned for Snort2	1
Number of Access Policy devices assigned for Snort3	0
Count of Access Policy custom IPS policy	1
Count of Access Policy custom NAP policy	1
Is IPS syslog is enabled?	False
Is syslog destination is override?	False
Parent Policy UUID	4294967319
Policy UUID	4294977323
Count of Access Policy system IPS policy	0
Count of Access Policy system NAP policy	0
Number of migrated Snort3 intrusion policies	1
Count of policies failure	0
Number of reason of policies failure	N/A
Count of policies partial failure	0
Number of reason of policies partial failure	N/A
Count of policies success	1
Number of devices assigned for Snort2 IPS	0
Number of custom rules enabled	0
Number of dynamic rules configured	0
Is firepower recommendation used	False
Is global threshold disabled	False
Is global threshold updated	False
Snort2 IPS Parent Policy UUID	abba00a0-cf29-425c-9d75-49699aadc898
Snort2 IPS Policy UUID	0e6aa778-69f2-11eb-8e9e-6475e0e0131b
Is sensitive data detection enabled	False
Number of SNMP enabled rules	0
Number of suppression rules configured	0

Data Point	Example Value
Number of threshold rules configured	0
Number of Snort2 IPS custom rule with pass	1
Number of Snort2 IPS custom rule with replace	1
Number of Snort2 IPS custom rules	9
Number of Snort2 network analysis policy devices assigned	0
Number of Snort2 network analysis policy custom instances added	N/A
Last modified time stamp	2021-02-15 14:15:50
Snort2 network analysis Parent Policy UUID	abba00a0-cf29-425c-9d75-49699aadc898
Snort2 network analysis Policy UUID	e889a48c-6f96-11eb-969d-7075e0e0131b
Snort2 network analysis Policy user Disabled Inspectors	dns
Snort2 network analysis Policy user Edited Inspectors	dce_rpc
Snort2 network analysis Policy user Enabled Inspectors	http_inspect, dce_rpc
Number of devices assigned for Snort3 IPS	0
Count of group of custom rule enabled	0
Count of group of custom rule excluded	0
Count of group of custom rule included	0
Number of Snort3 IPS rules override	0
Snort3 IPS Parent Policy UUID	7003
Snort3 IPS Policy UUID	4294973084
Snort3 IPS Policy excluded rule groups	[{ "containerRuleGroupUuid": "c4f4121b-d8e0-5086-9ae3-064062109492", "leafRuleGroupUuids": ["e15f11b4-a2fc-5e7a-9549-b6638972bdf5", "d0ae8e7a-d36d-52bc-b129-a320082fb4f5"] }]

Data Point	Example Value
Snort3 IPS Policy included rule groups	[{ "containerRuleGroupUuid": "c4f4121b-d8e0-5086-9ae3-064062109492", "leafRuleGroupUuids": ["e15f11b4-a2fc-5e7a-9549-b6638972bdf5", "d0ae8e7a-d36d-52bc-b129-a320082fb4f5"] }]
Snort3 IPS Policy overriden rule groups	[{ "containerRuleGroupUuid": "c4f4121b-d8e0-5086-9ae3-064062109492", "leafRuleGroupUuids": ["e15f11b4-a2fc-5e7a-9549-b6638972bdf5", "d0ae8e7a-d36d-52bc-b129-a320082fb4f5"] }]
Count of overriden rule groups	10
Number of groups of Snort3 IPS custom rule	2
Number of Snort3 IPS custom rule	1
Number of Snort3 IPS rules with suppression	0
Number of Snort3 IPS rules with threshold	0
Number of Snort3 network analysis policy devices assigned	0
Number of Snort3 network analysis policy custom instances added	N/A
Number of Snort3 network analysis policy default instances edited	N/A
Snort3 network analysis Parent Policy UUID	7303
Snort3 network analysis Policy UUID	4294978428
Snort3 network analysis policy user Disabled Inspectors	N/A
Snort3 network analysis policy user Edited Inspectors	N/A
Snort3 network analysis policy user Enabled Inspectors	N/A
Number of SSL certificates in the Zero Trust Access policy.	1
Number of zero-trust application groups.	1

Data Point	Example Value
Number of zero-trust applications that uses file policy.	3
Number of zero-trust applications that uses IPS policy	1
Number of target devices for the Zero Trust Access policy.	0
Identity provider URL.	www.okta.com
Number of interface objects configured in the Zero Trust Access policy.	2
Total number of zero-trust enabled applications in the Zero Trust Access policy.	3
Number of ungrouped applications in the Zero Trust Access policy.	2

Managed Cluster Data

Cisco Success Network collects information about all the managed clusters that are associated with an enrolled management center. The following table describes the collected and monitored information about the managed clusters.

Table 4: Managed Cluster Telemetry Data

Data Point	Example Value
Cluster Model	Cisco Threat Defense for VMware
Cluster Name	vFTDCluster
Cluster Size	3
Total Number of Managed Clusters	1

Deployment Information

After you configure your deployment, you must deploy the changes to the affected devices. The following table describes the collected and monitored data about configuration deployment, such as the number of devices affected and the status of deployments, including success and failure information.

Table 5: Deployment Information

Data Point	Example Value
Job ID	8589985199

Data Point	Example Value
Count of policy files of access policy	An integer value of 0 or greater
Count of policy identity of access policy	
Count of policy IPS of access policy	
Count of NS network of access policy	
Count of objects of access policy	
Count of policy SSL of access policy	
Count of UI AC rules of access policy	
Count of interfaces changed	
Count of objects changed	
Count of rules changed	
Container Type	STANDALONE
Duration of CSM Snapshot	1568
End Time of CSM Snapshot	1637750908871
Start Time of CSM Snapshot	1637750907303
Duration of DC Snapshot	24328
End Time of DC Snapshot	1637750933923
Start Time of DC Snapshot	1637750909595
Count of delta CLI	17
Phase 2 Time Generation of delta CLI	523
Total Time Generation of delta CLI	1040
Deployment End Time	1637751003157
Deployment Error message	
Deployment Start Time	1637750906704
Deployment Status	SUCCEEDED
Deployment Type	NORMAL_DEPLOYMENT
Device Model	Cisco Threat Defense for VMWare
Device OS Version	Version "X.X.X"
Duration of device package	5217

Data Point	Example Value
End Time of device package	1637750942073
Start Time of device package	1637750936856
Device UUID	80e4ae98-4ceb-11ec-9593-90baf6bd6a9b
Dirty pages	
Duration of file downloaded from management center.	9699
End Time of file downloaded from management center.	1637750951798
Start Time of file downloaded from management center.	1637750942099
Count files size copied from active	An integer value of 0 or greater
Is deployment full?	True
Count of http status retries on active	An integer value of 0 or greater
Duration of LINA applied	291
End Time of LINA applied	1637751001327
Start Time of LINA applied	1637751001036
Duration of LINA file copied	0
End Time of LINA file copied	0
Start Time of LINA file copied	0

Data Point	Example Value
Page Types	[PIX_INTERFACE_NKP, *_SINGLE_NKP, PG.PLATFORM.PixInterface, PG.FIREWALL.PrefilterPolicy, PG.PLATFORM.NgfwInlineSetPage, PG.PLATFORM.AutomaticApplicationBypassPage, PG.TEMPLATE.TemplatePolicy, PG.PLATFORM.NgfwNetworkVirtualizationEndPoint, PG.PLATFORM.NgfwVirtualRouterPage, PG.PLATFORM.AsaBGPPage, PG.PLATFORM.PixDDnsPage, PG.PLATFORM.NgfwPolicyBasedRouteTablePage, PG.PLATFORM.PixStaticRouteTablePage, PG.PLATFORM.PixMBoundaryPage, PG.PLATFORM.AsaOSPFv3Page, PG.PLATFORM.PixIGMPPage, PG.PLATFORM.PixOSPFPage, PG.PLATFORM.NgfwECMPZonePage, PG.PLATFORM.PixDhcpdPage, PG.PLATFORM.PixPIMPage, PG.PLATFORM.F1IPv6StaticRouteTablePage, PG.PLATFORM.PixDhcpRelayPage, PG.PLATFORM.PixAsaEigrpPage, PG.PLATFORM.PixMroutePage, PG.PLATFORM.PixRipPix72Page, PG.FIREWALL.NGFWAccessControlPolicy, NetworkDiscovery, Snort3IntrusionPolicy, Snort3NetworkAnalysisPolicy, DNSPolicy]
Size of policy bundle	141908
Count of CLI configuration running	163
Count of time configuration running retrieval	An integer value of 0 or greater
List of secondary nodes information	
Selected pages	
Count of Snort export ARC	An integer value of 0 or greater
Count of Snort export Access Control	An integer value of 0 or greater
Count of Snort export advanced Access Control	An integer value of 0 or greater
Count of Snort export applications Access Control	An integer value of 0 or greater
Count of Snort export DNS policy Access Control	An integer value of 0 or greater
Count of Snort export File policy Access Control	An integer value of 0 or greater
Count of Snort export IP Reputation Access Control	An integer value of 0 or greater

Data Point	Example Value
Count of Snort export Identity policy Access Control	An integer value of 0 or greater
Count of Snort export Intelligent App Bypass Access Control	An integer value of 0 or greater
Count of Snort export Intrusion policy Access Control	An integer value of 0 or greater
Count of Snort export Lamp lighter policy of Access Control.	An integer value of 0 or greater
Count of Snort export Network Analysis policy of Access Control	An integer value of 0 or greater
Count of Snort export Network Discovery of Access Control	An integer value of 0 or greater
Count of Snort export prefilter policy of Access Control	An integer value of 0 or greater
Count of Snort export QOS policy as Access Control	An integer value of 0 or greater
Count of Snort export SSL policy Access Control	An integer value of 0 or greater
Count of Snort export Snort3 Intrusion policy of Access Control	An integer value of 0 or greater
Count of Snort export Variable set of Access Control	An integer value of 0 or greater
Count of Snort export Detectors of Access Control	An integer value of 0 or greater
Count of Snort export Beaker.	An integer value of 0 or greater
Count of Snort export Geolocation	An integer value of 0 or greater
Count of Snort export LSP	An integer value of 0 or greater
Count of Snort export NGFW policy	An integer value of 0 or greater
Count of Snort export platform settings	An integer value of 0 or greater
Count of Snort export sensor clustering	An integer value of 0 or greater
Count of Snort export sensor policy	An integer value of 0 or greater
Count of Snort export snort	An integer value of 0 or greater
Count of Snort export state sharing	An integer value of 0 or greater
Duration of Snort preparation on active	27218
End Time of Snort preparation on active	1637750983442
Start Time of Snort preparation on active	1637750956224

Data Point	Example Value
Status of Snort restart	False
Duration of Snort signal on active	17537
End Time of Snort signal on active	1637751000981
Start Time of Snort signal on active.	1637750983444

TLS/SSL Inspection Event Data

By default, the Firepower System cannot inspect traffic encrypted with the Secure Socket Layer (SSL) protocol or its successor, the Transport Layer Security (TLS) protocol. *TLS/SSL inspection* enables you to either block encrypted traffic without inspecting it, or inspect encrypted or decrypted traffic with access control. The following tables describe statistics shared with Cisco Success Network about encrypted traffic.

Handshake Process

When the system detects a TLS/SSL handshake over a TCP connection, it determines whether it can decrypt the detected traffic. As the system handles encrypted sessions, it logs details about the traffic.

Table 6: TLS/SSL Inspection - Handshake Telemetry Data

Data Point	Example Value
The system reports the following applied actions when the traffic **cannot be decrypted** and is: • Blocked • Blocked with a TCP reset • Not decrypted	An integer value of 0 or greater
The system reports the following applied actions when the traffic **can be decrypted**: • With a known private key. • With a replacement key only. • By resigning a self-signed certificate. • By resigning the server certificate.	An integer value of 0 or greater
The number of SSL rules set to block encrypted traffic.	An integer value of 0 or greater
The number of SSL rules set to block encrypted traffic and reset the connection.	An integer value of 0 or greater
The number of SSL rules set to decrypt incoming traffic.	An integer value of 0 or greater

Data Point	Example Value
The number of SSL rules set to decrypt outgoing traffic.	An integer value of 0 or greater
The number of SSL rules set to not to decrypt encrypted traffic.	An integer value of 0 or greater
The number of SSL rules set to log encrypted traffic.	An integer value of 0 or greater
Is AC policy having intrusion?	False
The number of AC rules set with intrusion.	An integer value of 0 or greater
Is Threat IntelligenceDirector (TID) enabled?	True
The number of AC rules that needed threat license to perform traffic intrusion detection and prevention.	An integer value of 0 or greater
Is threat license used for traffic intrusion detection and prevention?	True
The number of AC rules set with URL Filtering.	An integer value of 0 or greater
The number of AC rules need Threat License.	An integer value of 0 or greater
The number of AC rules need URL License	An integer value of 0 or greater
Is threat license used for URL Filtering?	True
The number of actions set to handle SSL handshake message.	An integer value of 0 or greater

Cache Data

After a TLS/SSL handshake completes, the managed device caches encrypted session data, which allows session resumption without requiring the full handshake. The managed device also caches server certificate data, which allows faster handshake processing in subsequent sessions.

Table 7: TLS/SSL Inspection - Cache Telemetry Data

Data Point	Example Value
	An integer value of 0 or greater

Data Point	Example Value
The system caches encrypted session data and server certificate data, and reports on the **cache** per SSL connections, specifically: • The number of times SSL session information was cached. • The number of times the SSL certificate validation cache was hit. • The number of times the SSL certificate validation cache lookup missed. • The number of times the SSL original certificate cache was hit. • The number of times the SSL original certificate cache lookup missed. • The number of times the SSL resigned certificate cache was hit. • The number of times the SSL resigned certificate cache lookup missed. • The number of times the client hello digest cache entries. • The number of times the client hello digest cache evicted. • The number of times the client hello digest cache was hit. • The number of times the client hello digest cache memory used. • The number of times the client hello digest cache miss. • The number of times the endpoint cert cache entries. • The number of times the endpoint cert cache memory used. • The number of times the external cert cache entries. • The number of times the external cert cache memory used. • Internal CA cache entries. • The number of times the internal CA cache memory used. • The number of times the object list cache entries.	

Data Point	Example Value
• The number of times the object list cache memory used. • The number of times the original cert cache entries. • The number of times the original cert cache entries memory used. • The number of times the original cert cache evicted. • The number of times the original cert cache was hit. • The number of times the original cert cache memory used. • The number of times the original cert cache miss. • The number of times the resigned cert cache entries. • The number of times the resigned cert cache entries memory used. • The number of times the resigned cert cache evicted. • The number of times the resigned cert cache was hit. • The number of times the resigned cert cache memory used. • The number of times the resigned cert cache miss. • The number of times the server name cache entries. • The number of times the server name cache evicted. • The number of times the server name cache was hit. • The number of times the server name cache memory used. • The number of times the server name cache miss. • The number of times the session ID cache entries. • The number of times the session ID cache evicted. • The number of times the session ID cache was hit. • The number of times the session ID cache memory used. • The number of times the session ID cache miss • The number of times the session ticket cache entries. • The number of times the session ticket cache evicted. • The number of times the session ticket cache was hit.	

Data Point	Example Value
• The number of times the session ticket cache memory used. • The number of times the session ticket cache miss. • The number of times the SSL caches total memory. • The number of times the SSL caches total memory used. • The number of times the URL retry cache entries. • The number of times the URL retry cache evicted. • The number of times the URL retry cache was hit. • The number of times the URL retry cache memory used. • The number of times the URL retry cache miss.	
Is SSL Usage enabled on the management center?	True

Certificate Status

The system evaluates encrypted traffic and reports the certificate status of the encrypting server.

Table 8: TLS/SSL Inspection - Certificate Status Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic based on the **certificate status** of the encrypting server, and reports. • Number of connections where the SSL certificate is valid. • Number of connections where the SSL certificate is expired. • Number of connections where the SSL certificate has an invalid issuer. • Number of connections where the SSL certificate has an invalid signature. • Number of connections where the SSL certificate is not checked. • Number of connections where the SSL certificate is not yet valid. • Number of connections where the SSL certificate is revoked. • Number of connections where the SSL certificate is self-signed. • Number of connections where the SSL certificate is unknown.	An integer value of 0 or greater

Failure Reason

The system evaluates encrypted traffic and reports the failure reason when the system fails to decrypt traffic.

Table 9: TLS/SSL Inspection - Failure Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the **failure reason** when the system fails to decrypt traffic due to: • A decryption error. • Making a policy verdict during the handshake. • Making a policy verdict before the handshake. • Compression being negotiated. • An uncached session. • An interface in passive mode. • An unknown cipher suite. • An unsupported cipher suite.	An integer value of 0 or greater

Version

The system evaluates encrypted traffic and reports the negotiated TLS/SSL version per connection.

Table 10: TLS/SSL Inspection - Version Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the negotiated **version** per SSL connections where: • SSLv2 was negotiated. • SSLv3 was negotiated. • An unknown version was negotiated. • TLSv1.0 was negotiated. • TLSv1.1 was negotiated. • TLSv1.2 was negotiated. • TLSv1.3 was negotiated.	An integer value of 0 or greater

Snort Restart Data

When the traffic inspection engine referred to as the Snort process on a managed device restarts, inspection is interrupted until the process resumes. Creating or deleting a user-defined application, or activating or deactivating a system or custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains.

Table 11: Snort Restart Telemetry Data

Data Point	Example Value
Count of snort restarts when you enable or disable a custom application detector.	An integer value of 0 or greater
Count of snort restarts when you create or modify a custom application detector.	An integer value of 0 or greater

Snort3 Data

The following table describes the collected and monitored data about the Snort3 process. This includes session-specific information about packet performance monitoring about TCP/IP and other network protocols.

Table 12: Snort3 Telemetry Data

Data Point	Example Value
Count of the number of sessions pruned due to a full cache or flow memory capacity was reached.	An integer value of 0 or greater
Count of the number of sessions for which Snort did not see the start of the flow.	An integer value of 0 or greater
Count of the number of sessions to detect the midstream.	An integer value of 0 or greater
The system reports the following counts related to packet performance monitoring used to determine the basic level of **latency**: • The number of packets that exceeded the total detection time threshold. • The number of packets that exceeded the rule threshold. • The number of SSL packets timeout. • The total packets are monitored. • The total time spent in detection. • The maximum time that a packet spent in detection. • The number of rule trees that exceeded the rule threshold. • The total number of rules evaluated. • The number of rules that are re-enabled post suspension.	An integer value of 0 or greater
The maximum number of TCP sessions.	An integer value of 0 or greater

Data Point	Example Value
The maximum number of Elephant flows	An integer value of 0 or greater
The number of TCP data bytes processed.	An integer value of 0 or greater
The maximum number of UDP sessions.	An integer value of 0 or greater
The number of UDP data bytes processed.	An integer value of 0 or greater
The maximum number of IP sessions (non ICMP/UDP/TCP).	An integer value of 0 or greater
The number of IP data bytes processed (non ICMP/UDP/TCP).	An integer value of 0 or greater
The maximum number of FTP sessions.	An integer value of 0 or greater
The number of FTP data bytes processed	An integer value of 0 or greater
The maximum number of HTTP sessions.	An integer value of 0 or greater
The maximum number of SMTP sessions.	An integer value of 0 or greater
The number of SMTP data bytes processed.	An integer value of 0 or greater
The maximum number of POP sessions.	An integer value of 0 or greater
The number of POP data bytes processed	An integer value of 0 or greater
The maximum number of SSH sessions.	An integer value of 0 or greater
The number of SSH data bytes processed.	An integer value of 0 or greater
The number of SSL packets processed.	An integer value of 0 or greater
The number of SSL packets ignored.	An integer value of 0 or greater
The number of SSL sessions ignored.	An integer value of 0 or greater
The maximum number of SSL sessions.	An integer value of 0 or greater
The maximum number of HTTP/2 sessions.	An integer value of 0 or greater
The maximum number of HTTP/2 data bytes processed (total_bytes).	An integer value of 0 or greater
The maximum number of HTTP data bytes processed (total_bytes).	An integer value of 0 or greater
The data collection start time (in Unix Epoch format).	An integer string
The number of Snort clean exits list.	An integer value of 0 or greater
The number of Snort unexpected exits list.	An integer value of 0 or greater

Data Point	Example Value
Firepower recommendations used for Snort3 intrusion policy.	False
Are disabled rules accepted in the Snort3 intrusion policy recommendation settings.	False
Last time Snort3 intrusion policy recommendation settings are updated.	1625032449791
Count of recommendations for Snort3 intrusion policy.	12
Level of security recommended for Snort3 intrusion policy.	"LEVEL_2"

The following table describes Snort3 runtime XTLS traffic information.

Data Point	Example Value
Certificate dnd verdicts.	1
Certificate dr verdicts .	1
Certificate drk verdicts.	2
Certificate dkk verdicts.	3
Certificate dp verdicts.	4
The number of times the client hello definitive dnd entries.	5
Flow over subscriptions.	6
SSLv3 was negotiated.	7
TLSv1.0 was negotiated.	8
TLSv1.1 was negotiated.	9
TLSv1.2 was negotiated.	10
TLSv1.3 was negotiated.	11
TLSv1.3 flow decrypted.	12
esni was requested.	13
Count of XTLS flows created.	14
Count of SH sessions resumed.	15
Ciphers was negotiated.	{ "TLS_RSA_WITH_AES_128_CBC_SHA": 3},{ "TLS_RSA_WITH_AES_256_CBC_SHA": 1}

Data Point	Example Value
An unsupported cipher suite.	{"DHE-DSS-AES256-GCM-SHA384" }
Dropped ciphers.	{ }
Bad certificate.	{ "www.gmail.com": 4},{ "www.reddit.com": 3}
An unknown certificate.	{ "www.youtube.com": 4}
An unknown certificate authority.	{ "www.youtube.com": 4}

The following table describes Snort3 crash information.

Data Point	Example Value
The version of custom application detector.	An integer value of 0 or greater
The packets trace of data acquisition library (DAQ).	An integer value of 0 or greater
The data message of data acquisition library (DAQ).	An integer value of 0 or greater
The header message of data acquisition library (DAQ).	An integer value of 0 or greater
The type of data acquisition library (DAQ).	An integer value of 0 or greater
IMS Build	1403
IMS Version	6.7.0
ISP Version	lsp-dev-20200710-1754
Model	Cisco Firepower 2120 Threat Defense
Model Number	72
NAVL Version	98
The process ID number (PID)	12368
Signal	6
Snort Build	4.116
Snort Version	3.0.1
SSP Build	99.15.1.245
Time Stamp	15991116699.963031
VDB Build	336
VDB Version	4.5.0

Zero Trust Access Statistics

LINA exports important Zero Trust Access telemetry data such as the number of active users, total number of applications, number of unsuccessful SAML requests or response, and the latency.

The following table describes the collected and monitored data about Zero Trust Access, that is exported by LINA.

Data Point	Example Value
Average number of zero-trust applications active in 24 hours.	2
Maximum number of zero-trust applications active in 24 hours.	3
Average number of zero-trust applications enabled in 24 hours.	2
Maximum number of zero-trust applications enabled in 24 hours.	4
Total number of zero-trust applications.	An integer value of 0 or greater.
Average authentication latency. The average latency is calculated as a cumulative average.	4
Maximum authentication latency.	5
Minimum authentication latency.	4
Average number of zero-trust authentications that are in progress in 24 hours.	An integer value of 0 or greater.
Maximum number of zero-trust authentications that are in progress in 24 hours.	An integer value of 0 or greater.
Total number of zero-trust authentications.	An integer value of 0 or greater.
Number of unsuccessful SAML authentication requests sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Number of successful SAML authentication requests sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Total number of SAML authentication requests sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Number of unsuccessful SAML authentication responses that are sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Number of successful SAML authentication responses that are sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Total number of SAML authentication responses that are sent by the zero-trust enabled applications.	An integer value of 0 or greater.
Total data bytes received after authentication.	1420
Total data bytes sent after authentication.	2140

Data Point	Example Value
Average number of active users with a valid cookie in 24 hours.	5
Maximum number of active users with a valid cookie in 24 hours.	5
Total number of active users with a valid cookie.	An integer value of 0 or greater.
Number of unsuccessful zero-trust sessions.	An integer value of 0 or greater.
Number of successful zero-trust sessions.	An integer value of 0 or greater.
Total number of zero-trust sessions.	An integer value of 0 or greater.

Snort engine exports important Zero Trust Access telemetry statistics such as total number of HTTP flows received, total number of cookie or username messages received, cookie valid, and cookie invalid authorization failures.

The following table describes the collected and monitored data about Zero Trust Access that are exported by Snort.

Total number of zero-trust connections received which is the sum of the allowed flows and the blocked flows.	An integer value of 0 or greater.
Number of successfully authorized zero-trust connections.	An integer value of 0 or greater.
Total number of blocked zero-trust connections. This value is the sum of the all the connections blocked due to the following: • Invalid application. • Unsuccessful processing. • Unsuccessful connection authorization.	An integer value of 0 or greater.
Number of zero-trust connections for which the service is not set.	An integer value of 0 or greater.
Number of blocked connections due to unsuccessful processing.	An integer value of 0 or greater.
Number of blocked non-TLS connections.	An integer value of 0 or greater.
Number of blocked zero-trust connections due to SSL DND events.	An integer value of 0 or greater.
Number of blocked zero-trust connections due to SSL block events.	An integer value of 0 or greater.
Number of blocked zero-trust connections due to invalid session state.	An integer value of 0 or greater.
Number of blocked zero-trust connections due to unsuccessful authorization.	An integer value of 0 or greater.
Number of blocked zero-trust connections due to invalid domain.	An integer value of 0 or greater.
Number of zero-trust connections for which the authorization token is not available.	An integer value of 0 or greater.
Number of zero-trust connections for which the authorization token length is greater than the acceptable value.	An integer value of 0 or greater.

Number of zero-trust connections for which the authorization token is invalid.	An integer value of 0 or greater.
Number of zero-trust HTTP events received.	An integer value of 0 or greater.
Number of zero-trust events that are received with host URI length greater than the acceptable value.	An integer value of 0 or greater.
Total number of blocked zero-trust connections due to unsuccessful redirection.	An integer value of 0 or greater.
Number of zero-trust reload events.	An integer value of 0 or greater.
Total number of zero-trust messages received. This value is the sum of the following zero-trust messages: • Invalid connection. • Invalid data. • Token. • Username.	An integer value of 0 or greater.
Total number of zero-trust messages that do not associate with a connection.	An integer value of 0 or greater.
Total number of zero-trust messages that do not have message type shared by LINA to Snort.	An integer value of 0 or greater.
Number of zero-trust messages with type as cookie.	An integer value of 0 or greater.
Number of zero-trust messages with the type as username.	An integer value of 0 or greater.
Number of zero-trust messages with an unsupported message type. Note that Zero Trust Access supports only username and cookie message types.	An integer value of 0 or greater.

Encrypted Visibility Engine Statistics

Cisco Success Network collects Encrypted Visibility Engine (EVE) telemetry across various threat and confidence levels and protocols. The following table describes the collected and monitored statistics about the encrypted visibility engine.

Data Point	Example Value
Number of packets evaluated by EVE.	An integer value of 0 or greater.
Number of HTTP processes identified by EVE with very high confidence.	An integer value of 0 or greater.
Number TLS processes identified by EVE with very high confidence.	An integer value of 0 or greater.
Number of QUIC processes identified by EVE with very high confidence.	An integer value of 0 or greater.
Number of HTTP connections blocked by EVE with very high threat score.	An integer value of 0 or greater.
Number of TLS connections blocked by EVE with very high threat score.	An integer value of 0 or greater.

Data Point	Example Value
Number of QUIC connections blocked by EVE with very high threat score.	An integer value of 0 or greater.
Number of HTTP malwares identified by EVE with very high threat level.	An integer value of 0 or greater.
Number ofTLS malwares identified by EVE with very high threat level.	An integer value of 0 or greater.
Number of QUIC malwares identified by EVE with very high threat level.	An integer value of 0 or greater.
Number of HTTP processes identified by EVE with high confidence.	An integer value of 0 or greater.
Number of TLS processes identified by EVE with high confidence.	An integer value of 0 or greater.
Number of QUIC processes identified by EVE with high confidence.	An integer value of 0 or greater.
Number of HTTP connections blocked by EVE with high threat score.	An integer value of 0 or greater.
Number of TLS connections blocked by EVE with high threat score.	An integer value of 0 or greater.
Number of QUIC connections blocked by EVE with high threat score.	An integer value of 0 or greater.
Number of HTTP malwares identified by EVE with high threat level.	An integer value of 0 or greater.
Number of TLS malwares identified by EVE with high threat level.	An integer value of 0 or greater.
Number of QUIC malwares identified by EVE with high threat level.	An integer value of 0 or greater.
Number of HTTP processes identified by EVE with medium confidence.	An integer value of 0 or greater.
Number of TLS processes identified by EVE with medium confidence.	An integer value of 0 or greater.
Number of QUIC processes identified by EVE with medium confidence.	An integer value of 0 or greater.
Number of HTTP connections blocked by EVE with medium threat score.	An integer value of 0 or greater.
Number of TLS connections blocked by EVE with medium threat score.	An integer value of 0 or greater.
Number of QUIC connections blocked by EVE with medium threat score.	An integer value of 0 or greater.
Number of HTTP malwares Identified by EVE with medium threat level.	An integer value of 0 or greater.
Number of TLS malwares Identified by EVE with medium threat level	An integer value of 0 or greater.
Number of QUIC malwares identified by EVE with medium threat level.	An integer value of 0 or greater.
Total number of labeled finger prints for HTTP.	An integer value of 0 or greater.
Total number labeled finger prints for TLS.	An integer value of 0 or greater.
Total number of labeled finger prints for QUIC.	An integer value of 0 or greater.
Total number of unlabeled finger prints for HTTP.	An integer value of 0 or greater.
Total number of unlabeled finger prints for TLS.	An integer value of 0 or greater.
Total number of unlabeled finger prints for QUIC.	An integer value of 0 or greater.

Contextual Cross-Launch Data

The contextual cross-launch feature allows you to quickly find more information about potential threats in web-based resources outside of the management center. You can click directly from an event in the event viewer or dashboard in the management center to the relevant information in an external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

Table 13: Contextual Cross-Launch Telemetry Data

Data Point	Example Value
The count of the Contextual Cross-Launch resources configured on the management center.	An integer value of 0 or greater
The count of the Contextual Cross-Launch resources enabled on the management center.	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing a domain variable.	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing an IP variable.	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing a SHA 256 variable.	An integer value of 0 or greater
The count of the Stealthwatch Configuration resources enabled on the management center.	An integer value of 0 or greater
The count of the Stealthwatch Configuration has Log Host.	An integer value of 0 or greater
The count of the Stealthwatch Configuration of the store events on management center.	An integer value of 0 or greater
The type of setup used in SAL integration wizard is One Box.	An integer value of 0 or greater

Event Summary

Intrusion policy and Malware & File policy generate events for matched traffic and logs the captured attack information. The following table describes the statistics that are shared with Cisco Success Network about the intrusion, file, and malware events.

Table 14: Event Summary Telemetry

Data point	Example Value
The system reports the following intrusion event data for the last 24 hours: • Intrusion events with the following applied actions: • Blocked • Partially blocked • Would block • Drop • Dropped • Partially dropped • Would drop • Would have dropped • Alert • React • Would react • Reject • Would Reject • Rewrite • Would Rewrite • Total number of intrusion events.	An integer value of 0 or higher.
The system reports the following malware event data for the last 24 hours: • Number of malware events blocked. • Total number of malware events. • Total number of file events.	An integer value of 0 or higher.
Total number of network discovery hosts.	An integer value of 0 or higher.

Cloud Event Configuration

Cisco Success Network collects information about various type of events that the management center send to the Cisco cloud. The following table describes the collected and monitored statistics about the cloud event configuration.

Table 15: Cloud Event Configuration

Data point	Example Value
Number of devices excluded from sending events to Cisco cloud.	An integer value of 0 or higher.
Is the management center configured to send events to Cisco cloud?	False
Is the management center configured to send security-related connection events?	False
Is management center configured to send all connection events?	False
Is management center configured to send discovery events?	False
Is management center configured to send file and malware events?	False
Is management center configured to send intrusion events?	False
Is sending intrusion packet to Cisco cloud enabled?	False

VPN Data

The following table describes the data reported to Cisco Success Network about the various certificate objects enrolled to the threat defense device.

Table 16: VPN Telemetry Data

Data Point	Example Value
Certificate enrollment of EST objects.	An integer value of 0 or greater
Certificate enrollment of manual objects.	
Certificate enrollment of PKCS12 objects.	
Certificate enrollment of SCEP objects.	
Certificate enrollment of self-signed objects.	
Certificate enrollments.	
Count of device with certificate enrollments.	

The following table describes the data shared with Cisco Success Network about the remote access VPN policies configured in the threat defense devices, including the number of connection profiles and dynamic access policies.

Data Point	Example Value
Connection profiles with fall back to local.	2
Connection profile with local authentication.	2
Connection profile with RADIUS.	An integer value of 0 or greater
Connection profile with Realm.	1403
Connection profile with SAML.	6.7.0
Devices configured with RAVPN.	lsp-dev-20200710-1754
Devices enabled with load balancing.	Cisco Firepower 2120 Threat Defense
Dynamic access policies.	72
Dynamic access policy records.	98
RAVPN connection profiles.	12368
RAVPN policies.	6
RAVPN policies with IKEv2.	4.116
RAVPN policies with SSL.	3.0.1

The following table describes the data shared with Cisco Success Network about different sit-to-site VPN topology configurations in the threat defense device.

Data Point	Example Value
Devices configured with S2S VPN.	An integer value of 0 or greater
S2S IKEv1 VPN with certificate authentication.	
S2S IKEv2 VPN with certificate authentication.	
S2S VPN extranet endpoints.	
S2S VPN full mesh topologies.	
S2S VPN hub and spoke topologies.	
S2S VPN IKEv1 topologies.	
S2S VPN IKEv2 topologies.	
S2S VPN point to point topologies.	
S2S VPN VTI topologies.	

Maria DB Data

Management center uses MariaDB to store configuration data. The following table describes the collected and monitored information about the MariaDB database.

Data Point	Example Value
Maria Db CPU status.	[{ "timestamp" : "123124312", "value" : "1%" }, { "timestamp" : "123124312", "value" : "2%" }, { "timestamp" : "123124312", "value" : "24%" }]
Maria Db memory status.	[{ "timestamp" : "123124312", "value" : "1gb" }, { "timestamp" : "123124312", "value" : "2gb" }, { "timestamp" : "123124312", "value" : "24gb" }]
Count of Db connection.	[{ "timestamp" : "123124312", "value" : 1 }, { "timestamp" : "123124312", "value" : 2 }, { "timestamp" : "123124312", "value" : 24 }]
Size of Db file system.	[{ "location" : "/var/lib/mysql/cfgdb/", "value" : "1gb" }, { "location" : "/var/lib/mysql/sfsnort/", "value" : "2gb" }, { "location" : "/var/lib/mysql/", "value" : "24gb" }]
Size of Db binlog.	"20gb"
Size of Db.	{ "cfgdb" : "5gb", "sfsnort" : "5gb", "Total_Db_size": "25gb" }
Size of Db index.	{ "cfgdb" : "5gb", "sfsnort" : "5gb", "Total_Db_size": "25gb" }
Top ten table by size.	{ "cfgdb": [{ "table_name" : "<tb1>", "row_count" : 4990, "size" : "500mb" }, { "table_name" : "<tb2>", "row_count" : 4990, "size" : "500mb" }], "sfsnort": [{ "table_name" : "<tb1>", "row_count" : 4990, "size" : "500mb" }, { "table_name" : "<tb2>", "row_count" : 4990, "size" : "500mb" }] }
The system captures the slow query of data from EM peers:	
Query.	SELECT * from EM_peers
Query time.	2.37s (4s)
Count of executed queries.	An integer value of 0 or greater.
Count of rows examined.	An integer value of 0 or greater.
Count of rows affected.	An integer value of 0 or greater.
The system captures the slow query of data from sensors:	
Query.	SELECT * from sensors

Data Point	Example Value
Query time.	2.37s (4s)
Count of executed queries.	An integer value of 0 or greater.
Count of rows examined.	An integer value of 0 or greater.
Count of rows affected.	An integer value of 0 or greater.
Global status of CLI.	"STRING"

Management Center Health Monitoring

The health monitor on the management center tracks variety of health indicators to ensure that the hardware and software in your firewall system works correctly. The following table describes the health monitoring status of management center and threat defense.

Data Point	Example Value
The system reports the following health status of management center: • Maximum number of custom dashboards created by a single user • Number of users created dashboard	An integer value of 0 or greater
The system reports the following health status of threat defense: • Maximum number of customers created dashboards by single user • Number of users created dashboard	An integer value of 0 or greater

Identity Usage

User identity information can help you to identify the source of policy breaches, attacks, or network vulnerabilities, and trace them to specific users. The following table provides the description of information shared with Cisco Success Network about identity usage of policies.

Data Point	Example Value
The system reports the following identity usage of access control policy: • Number of access rules. • Number of access policies. • Number of unique realm reference. • Number of unique user group reference. • Number of unique user reference. • Number of rules with ABP. • Number of rules with SGT. • Number of rules with user group reference. • Number of rules with user reference.	An integer value of 0 or greater
The system reports the following identity usage of identity policy status: • Number of active rules. • Number of identity policies. • Number of auth rules. • Number of unique realm sequences. • Number of unique realms. • Number of passive rules.	An integer value of 0 or greater
The system reports the following identity usage of identity source status: • Number of IS is configured. • Number of SXP is enabled. • Number of directory session is enabled.	An integer value of 0 or greater

Data Point	Example Value
The system reports the following identity usage of realm status: • Number of AD realms. • Number of LDAP directories. • Number of LDAP realms. • Number of LDAP directories. • Number of local realms. • Number of realm sequences.	An integer value of 0 or greater
The system reports the following identity usage of proxy: • Number of realms with proxy. • Number of devices used for ISE proxy. • Number of proxy sequences. • Number of standalone proxy devices. • Total number of devices used for realm proxy. • Maximum number of devices used for realm proxy. • Minimum number of devices used for realm proxy. • Number of devices used as proxy.	An integer value of 0 or greater

Telemetry Example File

The following is an example of a Cisco Success Network telemetry file for streaming policy and deployment information about a management center and its managed devices:

```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "7.4.1",
    "recordedAt" : 1669818070342,
    "fmc" : {
      "cloud_service" : {
        "amp_setting" : {
          "enableAutomaticMalwareUpdates" : 1,
          "enableDataSharing" : 0,
```

```
      "lastUpdateTimestamp" : 1669841394,
      "licensed" : 1,
      "proxyEnabled" : 0
    },
    "url_filtering" : {
      "cacheTimeout" : 0,
      "enableAutomaticUpdates" : 1,
      "enableURLFilter" : 1,
      "licensed" : 1,
      "queryVendors" : 2,
      "userPreference" : 1
    }
  },
  "deviceInfo" : {
    "SecureX" : {
      "isSecureXEnabled" : 0
    },
    "deviceModel" : "Secure Firewall Management Center for VMware",
    "deviceName" : "FMC1-FASTPOD",
    "deviceUuid" : "052f72b2-6f3e-11ed-rt4f5-59804da3174c",
    "isSsoEnabled" : 0,
    "serialNumber" : "None",
    "smartLicenseProductInstanceIdentifier" : "9ba0f39d-p07ji-421b-8053-6299fa26f0ab",
    "smartLicenseVirtualAccountName" : "ABC1",
    "systemUptime" : 263436000,
    "udiProductIdentifier" : "FS-VMW-ER-K9",
    "primaryFMCRemoteManagementAccess" : "FQDN",
    "secondaryFMCRemoteManagementAccess" : "FQDN"
  },
  "fmcUpgradeData" : { },
  "scheduleTasks" : {
    "tasks" : [
      {
        "comment" : "This was automatically set up during installation.",
        "creation_date" : 1669656848,
        "name" : "Weekly Software Download",
        "time_data" : {
          "by_day" : [
            6
          ],
          "by_hour" : [
            2
          ],
          "by_minute" : [
            "10"
          ],
          "by_month" : [ ],
          "by_month_day" : [ ],
          "by_set_position" : [ ],
          "by_week_number" : [ ],
          "by_year_day" : [ ],
          "frequency_type" : "weekly",
          "interval" : 1,
          "start_date" : "01/08/2021",
          "support_dst" : 1,
          "timedate" : 1546654200,
          "tz" : "America/New_York"
        },
        "type_name" : "Download Latest Update"
      },
      {
        "comment" : "This was automatically set up during installation.",
        "creation_date" : 1669656852,
        "name" : "Weekly config only backup",
```

```
        "time_data" : {
          "by_day" : [
            0
          ],
          "by_hour" : [
            2
          ],
          "by_minute" : [
            0
          ],
          "by_month" : [ ],
          "by_month_day" : [ ],
          "by_set_position" : [ ],
          "by_week_number" : [ ],
          "by_year_day" : [ ],
          "frequency_type" : "weekly",
          "interval" : 1,
          "start_date" : "01/09/2021",
          "support_dst" : 1,
          "timedate" : 1546740000,
          "tz" : "America/New_York"
        },
        "type_name" : "Backup"
      }
    ]
  },
  "versions" : {
    "items" : [
      {
        "type" : "SOFTWARE",
        "version" : "7.4.1-154"
      },
      {
        "lastUpdated" : 1669866005000,
        "type" : "SNORT_RULES_DB",
        "version" : "2022-11-28-001-vrt"
      },
      {
        "lastUpdated" : 1669881833000,
        "type" : "VULNERABILITY_DB",
        "version" : "361"
      },
      {
        "type" : "GEOLOCATION_DB",
        "version" : "2022-11-21-101"
      }
    ]
  }
},
"managedDevices" : {
  "items" : [
    {
      "deviceInfo" : {
        "containerStatus" : "Standalone",
        "deviceManager" : "FMC",
        "deviceModel" : "Cisco Firepower Threat Defense for VMware",
        "deviceName" : "192.168.7.149",
        "deviceUuid" : "96b75a84-6f3d-12rdc-96a6-e2422bc5a2bf",
        "deviceVersion" : "7.4.0-1475",
        "isConnected" : true,
        "serialNumber" : "9AWE1PEM4P2",
        "snort3Toggled" : false,
        "snort3ToggledWithComment" : "",
        "snortEngine" : "SNORT3",
```

```
    "remoteBranchConnectivity" : "Inbound"
  },
  "deviceSettings" : {
    "attemptedRemoteDeployHA" : false,
    "certVisibility" : false,
    "fmcAccessInfo" : {
      "IPAllocationTypeList" : [
        "N/A"
      ],
      "accessThrough" : "Management interface"
    },
    "mgmtInterfaceConvergence" : true,
    "netFlow" : {
        "netFlowEnabled" : false,
         "numberOfCollectors" : 0,
         "numberOfTrafficClasses" : 0
    },
    "nszValue" : false,
    "ogsValue" : true,
    "vrfInfo" : {
      "literal" : false,
      "numberOfStaticRoutes" : 0,
      "vrfCount" : 0
    },
    "onboardingMethod": "USING_SERIAL_NUMBER_VIA_CDO"
  },
  "ftdMemoryCGroupStatistics" : [
    {
      "meanMemorySwapUsageBytes" : 5.207097946E7,
      "meanMemoryUsageBytes" : 5.206894039E7,
      "memoryCGroupName" : "System/ProcessHigh",
      "peakMemorySwapUsageBytes" : 1574682624,
      "peakMemoryUsageBytes" : 1574674432,
      "stdDevMemorySwapUsage" : 957106.41,
      "stdDevMemoryUsage" : 954302.27
    },
    {
      "meanMemorySwapUsageBytes" : 2.2863022975E8,
      "meanMemoryUsageBytes" : 228563747,
      "memoryCGroupName" : "System/ProcessMedium",
      "peakMemorySwapUsageBytes" : 965337088,
      "peakMemoryUsageBytes" : 960196608,
      "stdDevMemorySwapUsage" : 3854598.89,
      "stdDevMemoryUsage" : 2914561.18
    },
    {
      "meanMemorySwapUsageBytes" : 9.8453439805E8,
      "meanMemoryUsageBytes" : 9.8453448572E8,
      "memoryCGroupName" : "privileged",
      "peakMemorySwapUsageBytes" : 987504640,
      "peakMemoryUsageBytes" : 987504640,
      "stdDevMemorySwapUsage" : 31431.74,
      "stdDevMemoryUsage" : 31265.9
    },
    {
      "meanMemorySwapUsageBytes" : 286504.12,
      "meanMemoryUsageBytes" : 286523.87,
      "memoryCGroupName" : "normal",
      "peakMemorySwapUsageBytes" : 36343808,
      "peakMemoryUsageBytes" : 36343808,
      "stdDevMemorySwapUsage" : 75561.78,
      "stdDevMemoryUsage" : 75584.27
    },
    {
```

```
  "meanMemorySwapUsageBytes" : 3502151.01,
  "meanMemoryUsageBytes" : 3502080,
  "memoryCGroupName" : "restricted",
  "peakMemorySwapUsageBytes" : 77656064,
  "peakMemoryUsageBytes" : 23068672,
  "stdDevMemorySwapUsage" : 2695.67,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 0,
  "meanMemoryUsageBytes" : 0,
  "memoryCGroupName" : "rest-agent",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 5.2469167188E8,
  "meanMemoryUsageBytes" : 5.2469178715E8,
  "memoryCGroupName" : "Detection-Snort3",
  "peakMemorySwapUsageBytes" : 555659264,
  "peakMemoryUsageBytes" : 555659264,
  "stdDevMemorySwapUsage" : 123621.9,
  "stdDevMemoryUsage" : 123587.29
},
{
  "meanMemorySwapUsageBytes" : 1.92944950325E9,
  "meanMemoryUsageBytes" : 1.92877869444E9,
  "memoryCGroupName" : "System",
  "peakMemorySwapUsageBytes" : 3940163584,
  "peakMemoryUsageBytes" : 3192242176,
  "stdDevMemorySwapUsage" : 1.8285574795E8,
  "stdDevMemoryUsage" : 1.8113682802E8
},
{
  "meanMemorySwapUsageBytes" : 0,
  "meanMemoryUsageBytes" : 0,
  "memoryCGroupName" : "System/default",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 0,
  "meanMemoryUsageBytes" : 0,
  "memoryCGroupName" : "qemu",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 1.7874486112E8,
  "meanMemoryUsageBytes" : 1.7870017999E8,
  "memoryCGroupName" : "System/ActionQueueScrape",
  "peakMemorySwapUsageBytes" : 1487872000,
  "peakMemoryUsageBytes" : 1446891520,
  "stdDevMemorySwapUsage" : 5783036.92,
  "stdDevMemoryUsage" : 5530633.87
},
{
  "meanMemorySwapUsageBytes" : 5.0285961409E8,
```

```
      "meanMemoryUsageBytes" : 5.0267548869E8,
      "memoryCGroupName" : "System/ProcessLow",
      "peakMemorySwapUsageBytes" : 1205043200,
      "peakMemoryUsageBytes" : 751620096,
      "stdDevMemorySwapUsage" : 1.7946871779E8,
      "stdDevMemoryUsage" : 1.7939477583E8
    },
    {
      "meanMemorySwapUsageBytes" : 7.9608501366E8,
      "meanMemoryUsageBytes" : 7.9573099445E8,
      "memoryCGroupName" : "System/SFDataCorrelator",
      "peakMemorySwapUsageBytes" : 2138398720,
      "peakMemoryUsageBytes" : 1774387200,
      "stdDevMemorySwapUsage" : 3.437121236E7,
      "stdDevMemoryUsage" : 3.164608653E7
    }
  ],
  "ftdProcessExitStatistics" : [
    {
      "managedRestarts" : 0,
      "processName" : "adi",
      "unexpectedExits" : 0
    }
  ],
  "ftdUpgradeData" : { },
  "malware" : {
    "malwareLicenseUsed" : true,
    "numberOfACRulesNeedMalwareLicense" : 1,
    "numberOfACRulesWithMalware" : 1
  },
  "snort3RuntimeStatistics" : {
    "firewallStatistics" : {
      "dce_rpcAllowedFlows" : 0,
      "dce_rpcDeniedFlows" : 0,
      "dnp3AllowedFlows" : 0,
      "dnp3DeniedFlows" : 0,
      "dnsAllowedFlows" : 0,
      "dnsDeniedFlows" : 0,
      "ftp_telnetAllowedFlows" : 0,
      "ftp_telnetDeniedFlows" : 0,
      "http2AllowedFlows" : 0,
      "http2DeniedFlows" : 0,
      "httpAllowedFlows" : 0,
      "httpDeniedFlows" : 0,
      "imapAllowedFlows" : 0,
      "imapDeniedFlows" : 0,
      "modbusAllowedFlows" : 0,
      "modbusDeniedFlows" : 0,
      "otherAllowedFlows" : 2216,
      "otherDeniedFlows" : 0,
      "popAllowedFlows" : 0,
      "popDeniedFlows" : 0,
      "quicAllowedFlows" : 0,
      "quicDeniedFlows" : 0,
      "rpcAllowedFlows" : 0,
      "rpcDeniedFlows" : 0,
      "sipAllowedFlows" : 0,
      "sipDeniedFlows" : 0,
      "smtpAllowedFlows" : 0,
      "smtpDeniedFlows" : 0,
      "sshAllowedFlows" : 0,
      "sshDeniedFlows" : 0,
      "sslAllowedFlows" : 0,
      "sslDeniedFlows" : 0
```

```
},
"ftpStatistics" : {
  "ftpDataBytesProcessed" : 0,
  "maxFTPsessions" : 0
},
"http2Statistics" : {
  "http2DataBytesProcessed" : 0,
  "maxHTTP2Sessions" : 0
},
"httpStatistics" : {
  "httpDataBytesProcessed" : 0,
  "maxHTTPSessions" : 325
},
"popStatistics" : {
  "maxPOPSessions" : 0,
  "popDataBytesProcessed" : 0
},
"sessionStatistics" : {
  "highCpuUtilisedElephantFlows" : 0,
  "ipDataBytesProcessed" : 27792,
  "maxElephantFlows" : 0,
  "maxIPSessions" : 10,
  "maxTCPSessions" : 13675,
  "maxUDPSessions" : 120,
  "midStreamSessions" : 0,
  "prunedSessions" : 2216,
  "systemUnderDuress" : 0,
  "tcpDataBytesProcessed" : 0,
  "totalElephantFlowsBypassed" : 0,
  "totalElephantFlowsDethrottled" : 0,
  "totalElephantFlowsExempted" : 0,
  "totalElephantFlowsThrottled" : 0,
  "udpDataBytesProcessed" : 0
},
"smbStatistics" : {
  "totalEncryptedSessions" : 0,
  "totalMultichannelSessions" : 0,
  "totalSMB1Sessions" : 0,
  "totalSMB2Sessions" : 0
},
"smtpStatistics" : {
  "maxSMTPSessions" : 5,
  "smtpDataBytesProcessed" : 0
},
"snortLatency" : {
  "maxTimeSpent" : 0,
  "packetTimeouts" : 0,
  "ruleEvaluationsExceededLatency" : 0,
  "rulesReenabled" : 0,
  "totalNumberOfRuleEvalauations" : 4542,
  "totalPacketsMonitored" : 0,
  "totalTimeSpentInDetection" : 0
},
"sshStatistics" : {
  "maxSshSessions" : 80,
  "sshDataBytesProcessed" : 0
},
"sslStatistics" : {
  "maxSslSessions" : 0,
  "packetsProcessed" : 0,
  "sessionsIgnored" : 0
},
"xtlsStatistics" : {
  "badCertificate" : [ ],
```

```
    "cert_dkk_verdicts" : 0,
    "cert_dnd_verdicts" : 0,
    "cert_dp_verdicts" : 0,
    "cert_dr_verdicts" : 0,
    "cert_drk_verdicts" : 0,
    "certificateUnknown" : [ ],
    "client_hello_definitive_dnd" : 0,
    "decrypted_tls_1_3_flows" : 0,
    "droppedCiphers" : [ ],
    "flow_created" : 0,
    "flow_over_subscriptions" : 0,
    "negotiatedCiphers" : [ ],
    "negotiated_ssl_version_3_0" : 0,
    "negotiated_tls_version_1_0" : 0,
    "negotiated_tls_version_1_1" : 0,
    "negotiated_tls_version_1_2" : 0,
    "negotiated_tls_version_1_3" : 0,
    "requested_esni" : 0,
    "sh_session_resume" : 0,
    "unknownCertificateAuthority" : [ ],
    "unsupportedCiphers" : [ ]
  },
  "clientlessZtnaRuntimeStatistics": {
    "applicationsActiveAvg": 2,
    "applicationsActiveMax": 3,
    "applicationsEnabledAvg": 2,
    "applicationsEnabledMax": 4,
    "applicationsTotal": 2,
    "authenticationLatencyAvg": 4,
    "authenticationLatencyMax": 5,
    "authenticationLatencyMin": 6,
    "authenticationsInProgressAvg": 10,
    "authenticationsInProgressMax": 0,
    "authenticationsTotal": 5,
    "samlRequestsFailed": 0,
    "samlRequestsPassed": 5,
    "samlRequestsTotal": 5,
    "samlResponsesFailed": 0,
    "samlResponsesPassed": 5,
    "samlResponsesTotal": 5,
    "totalBytesIn": 1420,
    "totalBytesOut": 2140,
    "usersActiveAvg": 5,
    "usersActiveMax": 5,
    "usersTotal": 5,
    "zeroTrustSessionsFailed": 0,
    "zeroTrustSessionsPassed": 5,
    "zeroTrustSessionsTotal": 5
},
  "zerotrustStatistics":{
    "allowed_flows" : 2,
    "authorization_failures" : 0,
    "blocked_flows" : 0,
    "decrypt_block_flows" : 0,
    "domain_invalid" : 0,
    "http_events" : 2,
    "invalid_app_failures" : 0,
    "invalid_data_messages" : 0,
    "invalid_flow_messages" : 0,
    "invalid_service" : 0,
    "invalid_state" : 0,
    "non_decryptable_flows" : 0,
    "non_tls_flows" : 0,
    "processing_failures" : 0,
```

```
    "redirect_error_events" : 0,
    "reload_events" : 0,
    "token_empty" : 0,
    "token_invalid" : 0,
    "token_too_long" : 0,
    "total_flows" : 2,
    "total_messages" : 4,
    "unsupported_messages" : 0,
    "uri_too_long_events" : 0,
    "username_messages" : 2
    "token_messages" :
},
  "eveRuntimeStatistics": {
    "connBlockHighConfHttp": 0,
    "connBlockHighConfQuic": 0,
    "connBlockHighConfTls": 0,
    "connBlockMediumConfHttp": 0,
    "connBlockMediumConfQuic": 0,
    "connBlockMediumConfTls": 0,
    "connBlockVeryHighConfHttp": 0,
    "connBlockVeryHighConfQuic": 0,
    "connBlockVeryHighConfTls": 0,
    "labeledFingerPrintHttp": 0,
    "labeledFingerPrintQuic": 0,
    "labeledFingerPrintTls": 0,
    "mlwrHighThreatHttp": 0,
    "mlwrHighThreatQuic": 0,
    "mlwrHighThreatTls": 0,
    "mlwrMediumThreatHttp": 0,
    "mlwrMediumThreatQuic": 0,
    "mlwrMediumThreatTls": 0,
    "mlwrVeryHighThreatHttp": 0,
    "mlwrVeryHighThreatQuic": 0,
    "mlwrVeryHighThreatTls": 0,
    "packetsEvaluated": 2748,
    "procHighConfHttp": 0,
    "procHighConfQuic": 0,
    "procHighConfTls": 0,
    "procMediumConfHttp": 0,
    "procMediumConfQuic": 0,
    "procMediumConfTls": 0,
    "procVeryHighConfHttp": 0,
    "procVeryHighConfQuic": 0,
    "procVeryHighConfTls": 0,
    "unlabeledFingerPrintHttp": 0,
    "unlabeledFingerPrintQuic": 0,
    "unlabeledFingerPrintTls": 0
},
"sslCacheStats" : { },
"sslUsage" : {
  "isSSLEnabled" : true
},
"ssl_rules_counter" : {
  "block" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
```

```
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "block_with_reset" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "decrypt_known_key" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "decrypt_resign" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
```

```
      "src_networks" : 0,
      "src_services" : 0,
      "src_zones" : 0,
      "ssl_versions" : 0,
      "subject_dns" : 0,
      "urls" : 0,
      "users" : 0,
      "vlan_tags" : 0
    },
    "do_not_decrypt" : {
      "apps" : 0,
      "cert_statuses" : 0,
      "cipher_suites" : 0,
      "decryption_certs" : 0,
      "dst_networks" : 0,
      "dst_services" : 0,
      "dst_zones" : 0,
      "external_certs" : 0,
      "issuer_dns" : 0,
      "logging" : 0,
      "replace_public_key" : 0,
      "src_networks" : 0,
      "src_services" : 0,
      "src_zones" : 0,
      "ssl_versions" : 0,
      "subject_dns" : 0,
      "urls" : 0,
      "users" : 0,
      "vlan_tags" : 0
    },
    "monitor" : {
      "apps" : 0,
      "cert_statuses" : 0,
      "cipher_suites" : 0,
      "decryption_certs" : 0,
      "dst_networks" : 0,
      "dst_services" : 0,
      "dst_zones" : 0,
      "external_certs" : 0,
      "issuer_dns" : 0,
      "logging" : 0,
      "replace_public_key" : 0,
      "src_networks" : 0,
      "src_services" : 0,
      "src_zones" : 0,
      "ssl_versions" : 0,
      "subject_dns" : 0,
      "urls" : 0,
      "users" : 0,
      "vlan_tags" : 0
    }
  },
  "threat" : {
    "acPolicyHasIntrusion" : false,
    "acRulesWithIntrusion" : 1,
    "isTIDEnabled" : true,
    "numberOfACRulesNeedThreatLicense" : 0,
    "threatLicenseUsed" : true
  },
  "urlFiltering" : {
    "acRulesWithURLFiltering" : 0,
    "numberOfACRulesNeedThreatLicense" : 0,
    "numberOfACRulesNeedURLLicense" : 0,
    "urlFilteringLicenseUsed" : true
```

```
      },
      "ftdModelMigrationStatistics" : [
        {
          "elapsedTime" : 6366,
          "errors" : "",
          "isCompleted" : true,
          "isReset" : false,
          "numberOfInterfaces" : 18,
          "sourceContainerStatus" : "Standalone",
          "sourceDeviceModel" : "Cisco Firepower 2130 Threat Defense",
          "sourceDeviceUuid" : "a8eee3f4-aa19-rt24-bda7-857745t8d45a",
          "sourceDeviceVersion" : "7.2.0",
          "targetContainerStatus" : "Standalone",
          "targetDeviceModel" : "Cisco Secure Firewall 3105 Threat Defense",
          "targetDeviceVersion" : "7.3.0",
        }
      ]
     }
  ]
},
"policyData" : {
  "AccessPolicyInfo" : [
    {
      "assignedSnort2Devices" : 0,
      "assignedSnort3Devices" : 1,
      "customIpsPolicyCount" : 1,
      "customNapPolicyCount" : 1,
      "enabledIpsSyslog" : false,
      "encryptedVisibilityEngine" : true,
      "overrideSyslogDestination" : false,
      "parentPolicyUUID" : "8589935770",
      "policyUUID" : "8589935771",
      "portScanSettings" : {
        "inspectionMode" : "Disabled"
      },
      "systemIpsPolicyCount" : 1,
      "systemNapPolicyCount" : 0
    }
  ],
  "MigratedSnort3IntrusionPolicyInfo" : {
    "migratedPolicies" : 0,
    "policiesFailureCount" : 0,
    "policiesFailureReason" : [
      "N/A"
    ],
    "policiesPartialFailureCount" : 0,
    "policiesPartialFailureReason" : [
      "N/A"
    ],
    "policiesSuccessCount" : 0
  },
  "PrefilterPolicyInfo" : [
    {
      "assignedDevices" : 1,
      "isSytemDefined" : true
    }
  ],
  "Snort2IntrusionPolicyInfo" : {
    "Snort2IpsList" : [
      {
        "isSystemDefined" : true,
        "policyName" : "No Rules Active",
        "policyUUID" : "apqr416e-3127-23ds-9f4v-d463d19aa744"
      },
```

```
      {
        "assignedSnort2Devices" : 0,
        "customEnabledRules" : 0,
        "dynamicConfiguredRules" : 0,
        "firepowerRecommendationsUsed" : false,
        "globalThresholdDisabled" : false,
        "globalThresholdUpdated" : false,
        "isSystemDefined" : false,
        "overridenRules" : 0,
        "parentPolicyUUID" : "apqr416e-3127-11ds-9f4c-d463d19aa744",
        "policyUUID" : "765f93a0-6g42-11ed-5tgf-2e944da3174c",
        "sensitiveDataDetectionEnabled" : false,
        "snmpEnabledRules" : 0,
        "suppressionConfiguredRules" : 0,
        "thresholdConfiguredRules" : 0
      }
    ],
    "customClassification" : 0,
    "customClassificationInUse" : 0,
    "customRuleWithPass" : 0,
    "customRuleWithReplace" : 0,
    "customRules" : 0
  },
  "Snort2NetworkAnalysisPolicyInfo" : [
    "ZtnaPolicyInfo" : [
      {
        "appSSLcertificates" : 1,
        "applicationGroups" : 1,
        "appsUsingFilePolicy" : 3,
        "appsUsingIPS" : 1,
        "assignedDevices" : 0,
        "identityProviders" : [
            "www.okta.com"
        ],
        "interfaceObjects" : 2,
        "totalApplications" : 3,
        "ungroupedApplications" : 2
    {
      "assignedSnort2Devices" : 0,
      "customInstancesAdded" : [
        "N/A"
      ],
      "isSystemDefined" : false,
      "lastModifiedTimestamp" : "2022-11-28 17:31:05",
      "parentPolicyUUID" : "apqr00a0-bv29-425c-9d75-49679aadc898",
      "policyUUID" : "703e0600-6f42-11ed-8d96-2e944da3174c",
      "userDisabledInspectors" : [
        "N/A"
      ],
      "userEditedInspectors" : [
        "N/A"
      ],
      "userEnabledInspectors" : [
        "N/A"
      ]
    }
  ],
  "Snort3IntrusionPolicyInfo" : {
    "Snort3IpsList" : [
      {
        "FirepowerRecommendationsUsed" : false,
        "assignedSnort3Devices" : 1,
        "enabledCustomRuleGroupCount" : 0,
        "excludedRuleGroups" : [ ],
```

```
            "excludedRuleGroupsCount" : 0,
            "includedRuleGroups" : [ ],
            "includedRuleGroupsCount" : 0,
            "overridenRuleGroups" : [ ],
            "overridenRuleGroupsCount" : 0,
            "overridenRules" : 4,
            "parentPolicyUUID" : "7005",
            "policyUUID" : "8589935680"
          }
        ],
        "customRuleGroups" : 1,
        "customRules" : 4,
        "rulesWithSuppression" : 0,
        "rulesWithThreshold" : 0
      },
      "Snort3NetworkAnalysisPolicyInfo" : [
        {
          "assignedSnort3Devices" : 1,
          "customInstancesAdded" : [
            "N/A"
          ],
          "defaultInstancesEdited" : [
            "N/A"
          ],
          "parentPolicyUUID" : "7303",
          "policyUUID" : "8589935556",
          "userDisabledInspectors" : [
            "N/A"
          ],
          "userEditedInspectors" : [
            "N/A"
          ],
          "userEnabledInspectors" : [
            "N/A"
          ]
        }
      ]
    },
    "deploymentData" : { },
    "analysis" : {
      "cloudEventConfig" : {
        "excludedDevices" : 0,
        "sendingConnection" : false,
        "sendingConnectionAll" : false,
        "sendingDiscovery" : false,
        "sendingEvents" : false,
        "sendingFile" : false,
        "sendingIntrusion" : false,
        "sendingPackets" : false
      },
      "crossLaunchInfo" : {
        "count" : 28,
        "enabledCount" : 28,
        "iocInfo" : [
          {
            "domain" : 10,
            "ip" : 9,
            "sha256" : 9
          }
        ]
      },
      "eventCount" : {
        "fileTotal" : 0,
        "ipsAlert" : 1045,
```

```
      "ipsBlock" : 0,
      "ipsDrop" : 0,
      "ipsDropped" : 0,
      "ipsPartialBlock" : 0,
      "ipsPartiallyDropped" : 0,
      "ipsReact" : 0,
      "ipsReject" : 0,
      "ipsRewrite" : 0,
      "ipsTotal" : 1045,
      "ipsWouldBlock" : 0,
      "ipsWouldDrop" : 0,
      "ipsWouldHaveDropped" : 0,
      "ipsWouldReact" : 0,
      "ipsWouldReject" : 0,
      "ipsWouldRewrite" : 0,
      "malwareBlocked" : 0,
      "malwareTotal" : 0,
      "networkDiscoveryHost" : 1198
    },
    "stealthwatchConfig" : {
      "crossLaunchEnabled" : 0,
      "hasLogHost" : 0,
      "isLinaLoggingEnabled" : 0,
      "isOneBox" : 0,
      "numLogHosts" : 0,
      "numUnusedLogHosts" : 0,
      "storeEventsFmc" : 1
    }
  },
  "theme" : {
    "light" : 10
  },
  "SSLStats" : {
    "action" : {
      "block" : 0,
      "block_with_reset" : 0,
      "decrypt_resign_self_signed" : 0,
      "decrypt_resign_self_signed_replace_key_only" : 0,
      "decrypt_resign_signed_cert" : 0,
      "decrypt_with_known_key" : 0,
      "do_not_decrypt" : 0
    },
    "cache_status" : {
      "cached_session" : 0,
      "cert_validation_cache_hit" : 0,
      "cert_validation_cache_miss" : 0,
      "orig_cert_cache_hit" : 0,
      "orig_cert_cache_miss" : 0,
      "resigned_cert_cache_hit" : 0,
      "resigned_cert_cache_miss" : 0,
      "session_cache_hit" : 0,
      "session_cache_miss" : 0
    },
    "cert_status" : {
      "cert_expired" : 0,
      "cert_invalid_issuer" : 0,
      "cert_invalid_signature" : 0,
      "cert_not_checked" : 0,
      "cert_not_yet_valid" : 0,
      "cert_revoked" : 0,
      "cert_self_signed" : 0,
      "cert_unknown" : 0,
      "cert_valid" : 0
    },
```

```
    "failure_reason" : {
      "decryption_error" : 0,
      "handshake_error_before_verdict" : 0,
      "handshake_error_during_verdict" : 0,
      "ssl_compression" : 0,
      "uncached_session" : 0,
      "undecryptable_in_passive_mode" : 0,
      "unknown_cipher_suite" : 0,
      "unsupported_cipher_suite" : 0
    },
    "version" : {
      "ssl_v20" : 0,
      "ssl_v30" : 0,
      "ssl_version_unknown" : 0,
      "tls_v10" : 0,
      "tls_v11" : 0,
      "tls_v12" : 0,
      "tls_v13" : 0
    }
  },
  "snortRestart" : {
    "appDetectorSnortRestartCnt" : 0,
    "appSnortRestartCnt" : 0
  },
  "localUrlCount" : {
    "items" : [ ]
  },
  "vpnData" : {
    "certificate" : {
      "certificateEnrollmentESTObjects" : 0,
      "certificateEnrollmentManualObjects" : 0,
      "certificateEnrollmentPKCS12Objects" : 0,
      "certificateEnrollmentSCEPObjects" : 0,
      "certificateEnrollmentSelfSignedObjects" : 0,
      "certificateEnrollments" : 0,
      "devicesWithCertificateEnrollments" : 0
    },
    "remoteAccessVpn" : {
      "connectionProfilesWithFallbackToLocal" : 0,
      "connectionProfilesWithLocalAuthentication" : 0,
      "connectionProfilesWithOverriddenSAMLIDPCertificate" : 0,
      "connectionProfilesWithRADIUS" : 0,
      "connectionProfilesWithRealm" : 0,
      "connectionProfilesWithSAML" : 0,
      "connectionProfilesWithWebAuthNEnabled" : 0,
      "devicesConfiguredWithRAVPN" : 0,
      "devicesEnabledWithLoadBalancing" : 0,
      "dynamicAccessPolicies" : 0,
      "dynamicAccessPolicyRecords" : 0,
      "ravpnConnectionProfiles" : 0,
      "ravpnPolicies" : 0,
      "ravpnPoliciesWithIKEv2" : 0,
      "ravpnPoliciesWithSSL" : 0
    },
    "siteToSiteVpn" : {
      "devicesConfiguredWithS2SVpn" : 0,
      "s2sIKEv1VpnWithCertificateAuthentication" : 0,
      "s2sIKEv2VpnWithCertificateAuthentication" : 0,
      "s2sVpnExtranetEndpoints" : 0,
      "s2sVpnFullMeshTopologies" : 0,
      "s2sVpnHubAndSpokeTopologies" : 0,
      "s2sVpnIKEv1Topologies" : 0,
      "s2sVpnIKEv2Topologies" : 0,
      "s2sVpnPointToPointTopologies" : 0,
```

```
      "s2sVpnVTITopologies" : 0
    }
  },
  "fmc_healthmon" : {
    "fmc" : {
      "stats" : {
        "maxCustomDashboardsCreatedBySingleUser" : 0,
        "numUsersCreatedDashboard" : 0
      }
    },
    "ftd" : {
      "stats" : {
        "maxCustomDashboardsCreatedBySingleUser" : 0,
        "numUsersCreatedDashboard" : 0
      }
    }
  },
  "identityUsage" : {
    "accessControlPolicyStats" : {
      "accessRules" : 1,
      "numberOfAccessPolicies" : 1,
      "numberOfUniqueRealmReference" : 0,
      "numberOfUniqueUserGroupReference" : 0,
      "numberOfUniqueUserReference" : 0,
      "rulesWithABP" : 0,
      "rulesWithSGT" : 0,
      "rulesWithUserGroupReference" : 0,
      "rulesWithUserReference" : 0
    },
    "identityPolicyStats" : {
      "activeRules" : 0,
      "identityPolicies" : 1,
      "noAuthRules" : 0,
      "numberOfUniqueRealmSequences" : 0,
      "numberOfUniqueRealms" : 1,
      "passiveRules" : 1
    },
    "identitySource" : {
      "isISEConfigured" : 0,
      "isSXPEnabled" : 0,
      "isSessionDirectoryEnabled" : 0
    },
    "proxy" : {
      "devicesUsedAsProxy" : 0,
      "devicesUsedForISEProxy" : 0,
      "devicesUsedForRealmProxy" : {
        "max" : 0,
        "min" : 0,
        "total" : 0
      },
      "proxySequences" : 0,
      "realmsWithProxy" : 0,
      "standAloneProxyDevices" : 0
    },
    "realmStats" : {
      "ADRealms" : 1,
      "LDAPDirectories" : 1,
      "LDAPRealms" : 0,
      "LDAPsDirectories" : 0,
      "localRealms" : 0,
      "realmSequences" : 0
    }
  },
  "managedClusters" : {
```

```
    "totalClusterCount" : 0
  },
  "mariaDBData" : {
    "DBConnection_count" : [ ],
    "Db_file_system_size" : [
      {
        "location" : "/var/lib/mysql/cfgdb",
        "value" : "2.0G"
      },
      {
        "location" : "/var/lib/mysql/sfsnort",
        "value" : "295M"
      },
      {
        "location" : "/var/lib/mysql",
        "value" : "5.1G"
      }
    ],
    "Db_index_size" : {
      "Total_Db_size" : "520.9M",
      "cfgdb" : "431.3M",
      "sfsnort" : "89.5M"
    },
    "Db_size" : {
      "Total_Db_size" : "1402.6M",
      "cfgdb" : "1289.6M",
      "sfsnort" : "112.9M"
    },
    "Global_status_CLI" : "EMPTY",
    "MariaDb_CPU_stats" : [
      {
        "timestamp" : "1669746257",
        "value" : "0.6633333333333331"
      },
      {
        "timestamp" : "1669785857",
        "value" : "0.8"
      },
      {
        "timestamp" : "1669800257",
        "value" : "0.8"
      },
      {
        "timestamp" : "1669803857",
        "value" : "0.8116666666666668"
      },
      {
        "timestamp" : "1669807457",
        "value" : "0.9"
      },
      {
        "timestamp" : "1669811057",
        "value" : "0.9"
      },
      {
        "timestamp" : "1669814657",
        "value" : "0.9"
      },
      {
        "timestamp" : "1669818257",
        "value" : "0.9"
      },
      {
        "timestamp" : "1669821857",
```

```
            "value" : "0.9"
          },
          {
            "timestamp" : "1669825457",
            "value" : "0.9"
        ],
        "MariaDb_memory_stats" : [
          {
            "timestamp" : "1669746257",
            "value" : "1135789875.1999998"
          },
          {
            "timestamp" : "1669749857",
            "value" : "1139567752.5333333"
          },
          {
            "timestamp" : "1669753457",
            "value" : "1154918331.7333333"
          },
          {
            "timestamp" : "1669757057",
            "value" : "1156227072"
          },
          {
            "timestamp" : "1669771457",
            "value" : "1156243456"
          },
          {
            "timestamp" : "1669793057",
            "value" : "1386346837.3333333"
          },
          {
            "timestamp" : "1669796657",
            "value" : "1386582016"
          },
          {
            "timestamp" : "1669800257",
            "value" : "1387066163.1999998"
          },
          {
            "timestamp" : "1669832657",
            "value" : "1389006848"
          }
        ],
        "Slow_query_data" : [
          {
            "query" : "SELECT uuid,revision,type FROM EORevisionStore",
            "query_exec_count" : "2",
            "query_time" : "71.93s (143s)",
            "rows_affected" : "0.0 (0)",
            "rows_examined" : "63075.5 (126151)"
          },
          {
            "query" : "SELECT uuid FROM rule_opts  order by uuid",
            "query_exec_count" : "2",
            "query_time" : "42.18s (84s)",
            "rows_affected" : "0.0 (0)",
            "rows_examined" : "978411.0 (1956822)"
          },
          {
            "query" : "UPDATE rule_header set performance='S' WHERE  uuid IN ( 'S', 'S', 'S',
'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S' )",
            "query_exec_count" : "1",
            "query_time" : "34.09s (34s)",
```

```
          "rows_affected" : "19627.0 (19627)",
          "rows_examined" : "58643.0 (58643)"
        },
        {
          "query" : "select count(*) from rule_opts",
          "query_exec_count" : "2",
          "query_time" : "26.58s (53s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "978411.0 (1956822)"
        },
        {
          "query" : "SELECT  rule_opts.sid,  rule_opts.gid FROM rule_opts LEFT JOIN
rule_header  ON  rule_opts.sid = rule_header.sid AND  rule_opts.gid = rule_header.gid WHERE
 ( rule_header.sid  IS NULL  OR  rule_header.gid  IS NULL )",
          "query_exec_count" : "2",
          "query_time" : "25.58s (51s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "1956822.0 (3913644)"
        },
        {
          "query" : "SELECT *, unix_timestamp(now()) - time_of_last_ping as ping_delta,
HEX(domain_uuid) as domain_uuid FROM sensor WHERE id = 'S'",
          "query_exec_count" : "1",
          "query_time" : "19.28s (19s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "1.0 (1)"
        }
      ],
      "Top_ten_table_by_size" : {
        "cfgdb" : [
          {
            "row_count" : 953876,
            "size" : "464.98M",
            "table_name" : "rule_opts"
          },
          {
            "row_count" : 59190,
            "size" : "346.52M",
            "table_name" : "eorevisionstore"
          },
          {
            "row_count" : 47033,
            "size" : "252.61M",
            "table_name" : "eostore"
          },
          {
            "row_count" : 53196,
            "size" : "107.44M",
            "table_name" : "rule_header"
          },
          {
            "row_count" : 311244,
            "size" : "85.29M",
            "table_name" : "eoattributes"
          },
          {
            "row_count" : 15,
            "size" : "80.52M",
            "table_name" : "sf_policy_pdl"
          },
          {
            "row_count" : 48251,
            "size" : "72.28M",
            "table_name" : "bb_snort3_intrusion_rule_history"
```

```
    },
    {
      "row_count" : 45902,
      "size" : "52.61M",
      "table_name" : "bb_snort3_intrusion_rule_data"
    },
    {
      "row_count" : 71579,
      "size" : "45.70M",
      "table_name" : "ids_event_msg_map"
    },
    {
      "row_count" : 68940,
      "size" : "40.73M",
      "table_name" : "eocontainerstore"
    }
  ],
  "sfsnort" : [
    {
      "row_count" : 60905,
      "size" : "27.70M",
      "table_name" : "ids_event_msg_map"
    },
    {
      "row_count" : 568181,
      "size" : "25.43M",
      "table_name" : "rna_vuln_software"
    },
    {
      "row_count" : 464576,
      "size" : "17.87M",
      "table_name" : "geolocation_ipv4_country"
    },
    {
      "row_count" : 12933,
      "size" : "17.59M",
      "table_name" : "rna_vuln"
    },
    {
      "row_count" : 27328,
      "size" : "13.55M",
      "table_name" : "health_alarm_syslog"
    },
    {
      "row_count" : 171944,
      "size" : "13.30M",
      "table_name" : "geolocation_ipv6_country"
    },
    {
      "row_count" : 116193,
      "size" : "13.18M",
      "table_name" : "cpe_software_map"
    },
    {
      "row_count" : 95676,
      "size" : "13.06M",
      "table_name" : "rna_fp_vuln_map"
    },
    {
      "row_count" : 116193,
      "size" : "11.49M",
      "table_name" : "rna_software_list"
    },
    {
```

```
            "row_count" : 32934,
            "size" : "5.55M",
            "table_name" : "vendor_mac_list"
          }
        ]
      },
      "binlog_size" : "2.6G"
    },
    "csdacInfo" : {
        "CSDACConnectorsConfigured" : [
        [
          "azuread-meta-connector",
          1
        ],
        [
          "aws",
          2
        ],
        [
          "o365",
          2
        ],
        [
          "github",
          1
        ]
      ],
      "CSDACFiltersConfigured" : [
        [
          "aws",
          2
        ]
      ],
      "availableConnectorTypes" : [
        "azure",
        "gcp",
        "azuread-meta-connector",
        "aws",
        "vcenter",
        "azure-servicetags",
        "github",
        "o365"
      ],
      "isCSDAConFMCEnabled" : true,
      "totalCSDACinFMCConnectorsConfigured" : 6,
      "totalCSDACinFMCRulesConfigured" : 2     }
}
}
```