Cisco Success Network Telemetry Data Collected from Cisco Firepower Management Center, Version 7.1

First Published: 2022-05-31

Last Modified: 2023-08-16

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

Cisco Success Network allows enrolled FMC 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 FMC in Cisco Success Network, selected telemetry data about the enrolled FMC 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 FMCs.

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 Firepower 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 FMC enabled?	1

Software Version Data

Cisco Success Network collects software information that pertains to the enrolled FMC 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
FMC 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 FMC. 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.	FMC
Managed Device Model.	Cisco Firepower 2130 NGFW Appliance Cisco FTD 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 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
Number of AC Rules with Malware Policy.	10
Number of AC Rules with Malware Policy That Use Malware License.	5

Data Point	Example Value
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 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

Data Point	Example Value
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
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

Data Point	Example Value
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
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

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 4: Deployment Information

Data Point	Example Value
Job ID	8589936079
Number of Devices Selected for Deployment	3
Number of Devices with Deployment Failure	1
Number of Devices with Deployment Success	2
End Time	1523993913001
Start Time	1523993840445
Status	SUCCEEDED
Target Device UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
Policy Types Deployed	NetworkDiscovery NGFWPolicy DeviceConfiguration
Last Deployment Job ID Collected in Current Run	8589936079
Container Type (Standalone or HA Pair)	STANDALONE HAPAIR
Container UUID	5e006633-30fe-11e9-8a70-cd88086eeac0
Device Model	Cisco FTD for VMWare
Device Version	6.4.0
Policy Bundle Size	3588153

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 5: 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
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

Data Point	Example Value
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 6: 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 FMC?	True

Certificate Status

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

Table 7: 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 8: 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 9: 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 10: 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 11: 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

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 FMC. You can click directly from an event in the event viewer or dashboard in the FMC 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 12: Contextual Cross-Launch Telemetry Data

Data Point	Example Value
The count of the Contextual Cross-Launch resources configured on the FMC.	An integer value of 0 or greater
The count of the Contextual Cross-Launch resources enabled on the FMC.	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 FMC.	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 FMC.	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
Count of legacy for theme.	An integer value of 0 or greater

VPN Data

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

Table 13: 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 FTD 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.	

Telemetry Example File

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


```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "7.1.0",
    "recordedAt" : 1568961395861,
    "fmc" : {
      "deviceInfo" : {
        "deviceModel" : "Cisco Firepower Management Center for VMWare",
        "deviceName" : "liverpool",
        "deviceUuid" : "c9a7877c-da65-11e9-956f-cc1767fe73df",
        "isSsoEnabled" : 1,
        "numberOfSsoUsers" : 2,
        "ssoIdentityProvider" : "okta",
        "serialNumber" : "None",
        "smartLicenseProductInstanceIdentifier" : "1077ac5d-619f-49eb-a6a9-6ad61c30a481",
        "smartLicenseVirtualAccountName" : "FTD-ENG-SJC",
        "systemUptime" : 114808000,
        "udiProductIdentifier" : "FS-VMW-SW-K9",
        "SecureX": {
            "isSecureXEnabled": 1
        }
      },
      "versions" : {
        "items" : [
          {
            "type" : "SOFTWARE",
            "version" : "6.6.0-1034"
```

```
      },
      {
        "lastUpdated" : 0,
        "type" : "SNORT_RULES_DB",
        "version" : "2019-08-12-001-vrt"
      },
      {
        "lastUpdated" : 1568847127000,
        "type" : "VULNERABILITY_DB",
        "version" : "309"
      },
      {
        "type" : "GEOLOCATION_DB",
        "version" : "None"
      }
    ]
  }
},
"managedDevices" : {
  "items" : [
    {
      "deviceInfo" : {
        "deviceManager" : "FMC",
        "deviceModel" : "Cisco Firepower 4125 Threat Defense",
        "deviceName" : "192.168.1.165",
        "deviceVersion" : "6.6.0-1034",
        "serialNumber" : "FCH22197RU0"
      },
      "malware" : {
        "malwareLicenseUsed" : true,
        "numberOfACRulesNeedMalwareLicense" : 0,
        "numberOfACRulesWithMalware" : 0
      },
      "sslCacheStats" : {
        "clientHelloDigestCacheEntries" : 3,
        "clientHelloDigestCacheEvicted" : 0,
        "clientHelloDigestCacheHit" : 7,
        "clientHelloDigestCacheMemoryUsed" : 720460,
        "clientHelloDigestCacheMiss" : 7,
        "endpointCertCacheEntries" : 0,
        "endpointCertCacheMemoryUsed" : 960,
        "externalCertCacheEntries" : 0,
        "externalCertCacheMemoryUsed" : 960,
        "internalCACacheEntries" : 1,
        "internalCACacheMemoryUsed" : 1049,
        "objectListCacheEntries" : 2,
        "objectListCacheMemoryUsed" : 1278,
        "originalCertCacheEntries" : 3,
        "originalCertCacheEntriesMemoryUsed" : 9120,
        "originalCertCacheEvicted" : 0,
        "originalCertCacheHit" : 7,
        "originalCertCacheMemoryUsed" : 80460,
        "originalCertCacheMiss" : 0,
        "resignedCertCacheEntries" : 3,
        "resignedCertCacheEntriesMemoryUsed" : 4270,
        "resignedCertCacheEvicted" : 0,
        "resignedCertCacheHit" : 14,
        "resignedCertCacheMemoryUsed" : 720484,
        "resignedCertCacheMistt" : 2,
        "serverNameCacheEntries" : 6,
        "serverNameCacheEvicted" : 0,
        "serverNameCacheHit" : 14,
        "serverNameCacheMemoryUsed" : 16731,
        "serverNameCacheMiss" : 0,
```

```
   "sessionIDCacheEntries" : 1,
   "sessionIDCacheEvicted" : 0,
   "sessionIDCacheHit" : 0,
   "sessionIDCacheMemoryUsed" : 720428,
   "sessionIDCacheMiss" : 14,
   "sessionTicketCacheEntries" : 1,
   "sessionTicketCacheEvicted" : 0,
   "sessionTicketCacheHit" : 0,
   "sessionTicketCacheMemoryUsed" : 720393,
   "sessionTicketCacheMiss" : 0,
   "sslCachesTotalMemory" : 14000000,
   "sslCachesTotalMemoryUsed" : 2999399,
   "urlRetryCacheEntries" : 0,
   "urlRetryCacheEvicted" : 0,
   "urlRetryCacheHit" : 0,
   "urlRetryCacheMemoryUsed" : 16176,
   "urlRetryCacheMiss" : 0
 },


snort3RuntimeStatistics": {
   "sessionStatistics": {
   "midStreamSessions": 2,
   "prunedSessions": 9,
   "maxTCPSessions": 1045,
   "maxElephantFlows" : 3,
   "tcpDataBytesProcessed": 2558555,
   "maxUDPSessions": 450,
   "udpDataBytesProcessed": 332458,
   "maxIPSessions": 227,
   "ipDataBytesProcessed": 221084
},
"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" : 1,
   "httpDeniedFlows" : 0,
   "imapAllowedFlows" : 0,
   "imapDeniedFlows" : 0,
   "modbusAllowedFlows" : 0,
   "modbusDeniedFlows" : 0,
   "otherAllowedFlows" : 99,
   "otherDeniedFlows" : 0,
   "popAllowedFlows" : 0,
   "popDeniedFlows" : 0,
   "quicAllowedFlows" : 11,
   "quicDeniedFlows" : 0,
   "rpcAllowedFlows" : 0,
   "rpcDeniedFlows" : 0,
   "sipAllowedFlows" : 0,
   "sipDeniedFlows" : 0,
   "smtpAllowedFlows" : 0,
   "smtpDeniedFlows" : 0,
   "sshAllowedFlows" : 0,
   "sshDeniedFlows" : 0,
   "sslAllowedFlows" : 0,
```

```
            "sslDeniedFlows" : 0
          },
          "snortLatency": {
             "packetTimeout": 4,
             "totalPacketsMonitored": 4009872,
             "totalTimeSpentInDetection": 322456620,
             "maximumTimeSpent": 3345,
             "totalNumberRulesEvalauated": 2047,
             "rulesExceededLatency": 2,
             "rulesReenabled": 2
          },
          "ftpStatistics": {
             "maxFTPSessions": 422,
             "ftpDataBytesProcessed": 399212
          },
          "httpStatistics": {
             "maxHTTPSessions": 536
          },
          "smtpStatistics": {
             "maxSMTPSessions": 215,
             "smtpDataBytesProcessed": 23342
          },
          "popStatistics": {
             "maxPOPSessions": 205,
             "popDataBytesProcessed": 22311
          },
             "sshStatistics": {
             "maxSshSessions": 57,
             "sshDataBytesProcessed": 108715
          },
          "sslStatistics": {
             "packetsProcessed": 20312,
             "sessionsIgnored": 5,
             "maxSslSessions": 35
          }
        "snortExitStatistics": {
            "cleanExits": 0,
            "unexpectedExits": 3
        },
        "snortCrashInfoStatistics": [
            {
                "appid_version": "75",
                "backtrace": [
                    "#0 0x14c2b7c206d0 in nanosleep+0x40 (/lib64/libpthread.so.0
@0x14c2b7c0f000)",
                    "#1 0x55f2d78079f9
(/ngfw/var/sf/detection_engines/c976095a-d89c-11ea-a29b-d7a1e06ce5bc/snort3 @0x55f2d772c000)",

                    "#2 0x14c2b72940ab in __libc_start_main+0xeb (/lib64/libc.so.6
@0x14c2b7270000)",
                    "#3 0x55f2d781caaa in _start+0x2a
(/ngfw/var/sf/detection_engines/c976095a-d89c-11ea-a29b-d7a1e06ce5bc/snort3 @0x55f2d772c000)"

                ],
                "daq_msg_data_len": 0,
                "daq_msg_header_len": 0,
                "daq_msg_type": 0,
                "ims_build": "1973",
                "ims_version": "6.7.0",
                "lsp_version": "lsp-dev-20200807-1948",
                "model": "Cisco Firepower Threat Defense for VMWare",
                "model_number": "75",
                "navl_version": "99",
                "pid": 32070,
```

```
      "signal": 6,
      "snort_build": "4.107",
      "snort_version": "3.0.1",
      "ssp_build": "99.15.1.222",
      "timestamp": "1597033269.500086",
      "vdb_build": "337",
      "vdb_version": "4.5.0"
    }
  ]
},
"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" : 1,
    "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" : 0,
          "isTIDEnabled" : true,
          "numberOfACRulesNeedThreatLicense" : 0,
          "threatLicenseUsed" : true
        },
        "urlFiltering" : {
          "acRulesWithURLFiltering" : 0,
          "numberOfACRulesNeedThreatLicense" : 0,
          "numberOfACRulesNeedURLLicense" : 0,
          "urlFilteringLicenseUsed" : true
        }
      }
    ]
  },
  "deploymentData" : { },
  "analysis" : {
    "crossLaunchInfo" : {
      "count" : 28,
      "enabledCount" : 28,
      "iocInfo" : [
        {
          "domain" : 10,
          "ip" : 9,
          "sha256" : 9
        }
      ]
    },
    "stealthwatchConfig" " {
      "crossLaunchEnabled" : 1
    }
  },
  "theme" : {
    "legacy" : 1
  },
  "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" : 887,
      "decrypt_with_known_key" : 0,
      "do_not_decrypt" : 0
    },
    "cache_status" : {
      "cached_session" : 60,
      "cert_validation_cache_hit" : 0,
      "cert_validation_cache_miss" : 887,
      "orig_cert_cache_hit" : 771,
```

```
          "orig_cert_cache_miss" : 0,
          "resigned_cert_cache_hit" : 887,
          "resigned_cert_cache_miss" : 17,
          "session_cache_hit" : 0,
          "session_cache_miss" : 700
        },
        "cert_status" : {
          "cert_expired" : 0,
          "cert_invalid_issuer" : 1,
          "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" : 886
        },
        "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" : 887,
          "tls_v13" : 0
        }
      },
      "snortRestart" : {
        "appDetectorSnortRestartCnt" : 0,
        "appSnortRestartCnt" : 0
      }
    },
    "localUrlCount" : {
      "items": [
          {
              "url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks",
              "count": 10
          },
          {
              "url": "/api/local/fmc_platform/v1/info/serverversion",
              "count": 2
          }
      ]
    } ,
  "policyData" : {
        "AccessPolicyInfo" : [
          {
            "assignedSnort2Devices" : 0,
            "assignedSnort3Devices" : 2,
            "customIpsPolicyCount" : 0,
            "customNapPolicyCount" : 0,
            "enabledIpsSyslog" : false,
            "overrideSyslogDestination" : false,
            "systemIpsPolicyCount" : 1,
```

```
        "systemNapPolicyCount" : 1
      },
      {
        "assignedSnort2Devices" : 0,
        "assignedSnort3Devices" : 0,
        "customIpsPolicyCount" : 0,
        "customNapPolicyCount" : 0,
        "enabledIpsSyslog" : false,
        "overrideSyslogDestination" : false,
        "systemIpsPolicyCount" : 1,
        "systemNapPolicyCount" : 1
      },
      {
        "assignedSnort2Devices" : 0,
        "assignedSnort3Devices" : 0,
        "customIpsPolicyCount" : 0,
        "customNapPolicyCount" : 0,
        "enabledIpsSyslog" : false,
        "overrideSyslogDestination" : false,
        "systemIpsPolicyCount" : 1,
        "systemNapPolicyCount" : 1
      },
      {
        "assignedSnort2Devices" : 0,
        "assignedSnort3Devices" : 0,
        "customIpsPolicyCount" : 0,
        "customNapPolicyCount" : 0,
        "enabledIpsSyslog" : false,
        "overrideSyslogDestination" : false,
        "systemIpsPolicyCount" : 1,
        "systemNapPolicyCount" : 1
      }
    ],
    "MigratedSnort3IntrusionPolicyInfo" : {
      "migratedPolicies" : 0,
      "policiesFailureCount" : 0,
      "policiesFailureReason" : [
        "N/A"
      ],
      "policiesPartialFailureCount" : 0,
      "policiesPartialFailureReason" : [
        "N/A"
      ],
      "policiesSuccessCount" : 0
    },
    "Snort3IntrusionPolicyInfo" : {
      "Snort3IpsList" : [
        {
          "assignedSnort3Devices" : 0,
          "enabledCustomRuleGroupCount" : 0,
          "excludedRuleGroupsCount" : 0,
          "includedRuleGroupsCount" : 0,
          "overridenRules" : 2
        },
        {
          "assignedSnort3Devices" : 0,
          "enabledCustomRuleGroupCount" : 0,
          "excludedRuleGroupsCount" : 0,
          "includedRuleGroupsCount" : 0,
          "overridenRules" : 0
        }
      ],
      "customRuleGroups" : 2,
      "customRules" : 1,
```

```
        "rulesWithSuppression" : 0,
        "rulesWithThreshold" : 0
      },
      "Snort3NetworkAnalysisPolicyInfo" : [
        {
          "assignedSnort3Devices" : 0,
          "customInstancesAdded" : [
            "N/A"
          ],
          "defaultInstancesEdited" : [
            "N/A"
          ],
          "userDisabledInspectors" : [
            "N/A"
          ],
          "userEditedInspectors" : [
            "N/A"
          ],
          "userEnabledInspectors" : [
            "N/A"
          ]
        }
      ]
    },
    "vpnData" : {
      "certificate" : {
        "certificateEnrollmentESTObjects" : 2,
        "certificateEnrollmentManualObjects" : 0,
        "certificateEnrollmentPKCS12Objects" : 3,
        "certificateEnrollmentSCEPObjects" : 2,
        "certificateEnrollmentSelfSignedObjects" : 3,
        "certificateEnrollments" : 17,
        "devicesWithCertificateEnrollments" : 4
      },
      "remoteAccessVpn" : {
        "connectionProfilesWithFallbackToLocal" : 2,
        "connectionProfilesWithLocalAuthentication" : 2,
        "connectionProfilesWithRADIUS" : 6,
        "connectionProfilesWithRealm" : 1,
        "connectionProfilesWithSAML" : 0,
        "devicesConfiguredWithRAVPN" : 3,
        "devicesEnabledWithLoadBalancing" : 2,
        "dynamicAccessPolicies" : 2,
        "dynamicAccessPolicyRecords" : 7,
        "ravpnConnectionProfiles" : 9,
        "ravpnPolicies" : 2,
        "ravpnPoliciesWithIKEv2" : 2,
        "ravpnPoliciesWithSSL" : 2
      },
      "siteToSiteVpn" : {
        "devicesConfiguredWithS2SVpn" : 3,
        "s2sIKEv1VpnWithCertificateAuthentication" : 1,
        "s2sIKEv2VpnWithCertificateAuthentication" : 1,
        "s2sVpnExtranetEndpoints" : 6,
        "s2sVpnFullMeshTopologies" : 1,
        "s2sVpnHubAndSpokeTopologies" : 2,
        "s2sVpnIKEv1Topologies" : 4,
        "s2sVpnIKEv2Topologies" : 7,
        "s2sVpnPointToPointTopologies" : 6,
        "s2sVpnVTITopologies" : 2
      }
    }
}
```