tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4
SYSLOG SPEC

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Syslog Spec Revisions

Rev	Date	Owner	Author	Revisions
Rev 1	March 2021	Pini Shanzer	Beth Stolper	Initial version

Table of Contents

1 Introduction

TIV can be configured to send syslog messages to external tools such as SIEM solutions, analytics tools, and log collectors. Syslog messages can be configured to be sent automatically for:

- Alerts and alert resolutions
- Events (of which an alert is composed)
- Baselines
- System status checks
- System health monitoring information.

The system sends raw information to syslog, allowing users to monitor the values and create alarms, analytics, and dashboards in other systems.

> Note Currently TLS 1.2 is supported through Syslog

Syslog Configuration

For information on Syslog configuration, see the *TIV User Guide: Configuring Syslog*.

2 Syslog Alert Examples

2.1 Known Threat Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Known Threat Alert|5| cn1Label=SiteId
cn1=1 cs1Label=Site cs1=Default cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs5Label=Src Zone cs5=Default Zone
cs6Label=Dst Zone cs6=Default Zone cs7Label=Category cs7=Security
cs8Label=AlertUrl cs8=https://<IP.Address>/detection/alert/1-1
outcome=Unresolved request= https://<IP.Address>/detection/alert/1-1
cn2Label=Alert Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.5.22.101
cs11Label=PrimaryAssetType cs11=Endpoint
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:08:02:1c:47:ae cs14Label=PrimaryAssetOS cs14=Windows 7/Server
2008 R2 cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=185.52.2.154
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=20:e5:2a:b6:93:f1
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Netgear cn3Label=StoryId cn3=1  src=10.5.22.101
smac=00:08:02:1c:47:ae shost=N/A dst=185.52.2.154
dmac=20:e5:2a:b6:93:f1 dhost=N/A externalId=1 cat=Create rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Out of working hours Known
Threat: Threat Claroty Rule: GranCrab Ransomware - C2 Certificate was
detected from 10.5.22.101 to 185.52.2.154
```

Table 1: Known Threat Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name	The type of event.	Known Threat Alert
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default

Name	Description	Value in Example
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
Src Zone	The source zone	Default Zone
Dst Zone	The destination zone	Default Zone
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/1-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/1-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.5.22.101
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:08:02:1c:47:ae
PrimaryAssetOS	The OS of the primary asset	Windows 7/Server 2008 R2
PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	185.52.2.154
NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	20:e5:2a:b6:93:f1
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Netgear
storyID	The ID of the story for this event	1
src	The IP address of the primary asset involved in the event	10.5.22.101
smac	The MAC address of the primary asset involved in the event	00:08:02:1c:47:ae
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	185.52.2.154
dmac	The MAC address of the secondary asset involved in the event	20:e5:2a:b6:93:f1
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	1
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Update
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Out of working hours Known Threat: Threat Claroty Rule: GranCrab Ransomware - C2 Certificate was detected from 10.5.22.101 to 185.52.2.154

2.2 Login Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Login|5| cn1Label=SiteId cn1=1
cs1Label=Site cs1=site-1 cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs5Label=Src Zone cs5=Endpoint:
Other cs6Label=Dst Zone cs6=Endpoint: Other cs7Label=Category
cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/14-1 outcome=Unresolved request=
https://<IP.Address>/detection/alert/14-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.1.31.12 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=00:50:56:8d:df:b8
cs14Label=PrimaryAssetOS cs14=N/A cs15Label=PrimaryAssetVendor
cs15=VMware cs16Label=NonPrimaryAssetIP cs16=10.1.31.1
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=28:63:36:26:f0:74
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Siemens cn3Label=StoryId cn3=1 duser=N/A
destinationServiceName=S7COMM  src=10.1.31.12 smac=00:50:56:8d:df:b8
shost=N/A dst=10.1.31.1 dmac=28:63:36:26:f0:74 dhost=N/A externalId=14
cat=Security rt=Nov 17 10:18:55 start=Oct 12 2020 17:28:33 msg=Failed
Login: Failed Login attempts were made to asset 10.1.31.1 from
10.1.31.12
```

Table 2: Login Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Login
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
	Src Zone	The source zone	Endpoint: Other
	Dst Zone	The destination zone	Endpoint: Other

Name	Description	Value in Example
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/14-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/14-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.1.31.12
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	00:50:56:8d:df:b8
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.31.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	28:63:36:26:f0:74
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Siemens
storyID	The ID of the story for this event	1
duser	The username of this attempted login	N/A
destinationServiceName	The name of the destination service	S7COMM
src	The IP address of the primary asset involved in the event	10.1.31.12
smac	The MAC address of the primary asset involved in the event	00:50:56:8d:df:b8
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.31.1
dmac	The MAC address of the secondary asset involved in the event	28:63:36:26:f0:74
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	14
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Security
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Failed Login: Failed Login attempts were made to asset 10.1.31.1 from 10.1.31.12

2.3 Configuration Download Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Configuration Download|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-1
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Engineering Station: Rockwell cs6Label=Dst Zone
cs6=PLC: Rockwell cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8= https://<IP.Address>/detection/alert/40-1 outcome=Unresolved
request= https://<IP.Address>/detection/alert/40-1 cn2Label=Alert
Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.1.30.40
cs11Label=PrimaryAssetType cs11=Engineering Station
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAssetIP
cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cn3Label=StoryId cn3=2  src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=40 cat=Integrity rt=Nov 17 10:18:55 start=Oct 12
2020 17:28:33 msg=Configuration Download: Configuration Download
critical change operation was performed for the first time by
10.1.30.40 on 10.1.30.1
```

Table 3: Configuration Download Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Login
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
Timestamp		Timestamp of the alert	rt=Nov 01 2020 11:04:44
SiteID		The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved:	Unresolved

Name	Description	Value in Example
	▪ Resolved or Unresolved	
Src Zone	The source zone	Engineering Station: Rockwell
Dst Zone	The destination zone	Rockwell
Category	The type of event: Integrity or Security	Integrity
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/40-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/40-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.1.30.40
PrimaryAssetType	The asset type of the primary asset	Engineering Station
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:50:56:b9:e2:ad
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	PLC
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	00:1d:9c:c0:04:9d
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Rockwell Automation
storyID	The ID of the story for this event	2
src	The IP address of the primary asset involved in the event	10.1.30.40
smac	The MAC address of the primary asset involved in the event	00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.0.40
dmac	The MAC address of the secondary asset involved in the event	00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	40
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Integrity
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 on 10.1.30.1

2.4 Host Scan Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Host Scan|5|cn1Label=SiteId cn1=7
cs1Label=Site cs1=ZZZ cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs5Label=Src Zone cs5=10.77.109.0/24 - Endpoint: Other
cs6Label=Dst Zone cs6=10.77.119.0/24 - Endpoint: Other
cs7Label=Category cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/286659-71 outcome=Unresolved
request= https://<IP.Address>/detection/alert/286659-71 cn2Label=Alert
Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.77.109.112,10.77.109.9
cs11Label=PrimaryAssetType cs11=Endpoint
cs12Label=PrimaryAssetHostname cs12=Host-abc cs13Label=PrimaryAssetMAC
cs13=84:a9:3e:8c:57:d7,84:a9:3e:8c:6d:86,c8:d3:ff:bc:46:0c
cs14Label=PrimaryAssetOS cs14=Windows 10/Server 2016
cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=Multiple Assets
cs17Label=NonPrimaryAssetType cs17=Multiple Assets
cs18Label=NonPrimaryAssetHostname cs18=Multiple Assets
cs19Label=NonPrimaryAssetMAC cs19=Multiple Assets
cs20Label=NonPrimaryAssetOS cs20=Multiple Assets
cs21Label=NonPrimaryAssetVendor cs21=Multiple Assets cn3Label=StoryId
cn3=58 {}src=10.77.109.112 smac=84:a9:3e:8c:57:d7 shost= ABC-DEF
dst=Multiple Assets dmac=c4:34:6b:62:60:b7 dhost= GHI-JKL
externalId=999999 cat=Create rt=Nov 17 10:18:55 start=Oct 12 2020
17:28:33 msg=TCP Host scan: Asset 10.77.109.9 sent packets to
different IP destinations on the same port: 7680
```

Table 4: Host Scan Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Host Scan
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	7
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	ZZZ
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved:	Unresolved

Name	Description	Value in Example
	▪ Resolved or Unresolved	
Src Zone	The source zone	10.77.109.0/24 - Endpoint: Other
Dst Zone	The destination zone	10.77.119.0/24 - Endpoint: Other
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/286659-71 outcome=Unresolved request= https://<IP.Address>/detection/alert/
Alert Score	The score for this alert	100
	NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**	
PrimaryAssetIP	The IP address of the primary asset	10.77.109.112, 10.77.109.9
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	Host-abc
PrimaryAssetMAC	The MAC address of the primary asset	84:a9:3e:8c:57:d7, 84:a9:3e:8c:6d:86, c8:d3:ff:bc:46:0c
PrimaryAssetOS	The OS of the primary asset	Windows 10/Server 2016
PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
	NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**	
NonPrimaryAssetIP	The IP address/es of the non-primary asset	Multiple Assets
NonPrimaryAssetType	The asset type/s of the non-primary asset	Multiple Assets
NonPrimaryAssetHostname	The host name/s of the non-primary asset	Multiple Assets
NonPrimaryAssetMAC	The MAC address of the non-primary asset	Multiple Assets
NonPrimaryAssetOS	The OS/es of the non-primary asset	Multiple Assets
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Multiple Assets
storyID	The ID of the story for this event	58 {}
src	The IP address of the primary asset involved in the event	10.77.109.112
smac	The MAC address of the primary asset involved in the event	84:a9:3e:8c:57:d7
shost	The host name of the primary asset involved in the event	ABC-DEF
dst	The IP address of the secondary asset involved in the event *NOTE:* In scan alert types, the dst asset data is "multiple assets" to avoid spam and to comply with the CEF format	Multiple Assets
dmac	The MAC address of the secondary asset involved in the event	c4:34:6b:62:60:b7
dhost	The host address of the secondary asset involved in the event	GHI-JKL
externalId	The ID of the alert which this event is part of.	999999
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Create
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	TCP Host scan: Asset 10.77.109.9 sent packets to different IP destinations on the same port: 7680

2.5 Suspicious File Transfer Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Suspicious File Transfer|5|rt=Nov 01
2020 11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Endpoint: Other cs6Label=Dst Zone cs6=Endpoint:
Other cs7Label=Category cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/60-1 outcome=Unresolved request=
https://<IP.Address>/detection/alert/60-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.20.6.205 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=f0:18:98:66:5a:0c
cs14Label=PrimaryAssetOS cs14=N/A cs15Label=PrimaryAssetVendor
cs15=Apple cs16Label=NonPrimaryAssetIP cs16=10.10.10.10
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=N/A cs20Label=NonPrimaryAssetOS
cs20=N/A cs21Label=NonPrimaryAssetVendor cs21=N/A cn3Label=StoryId
cn3=4
filePath=/private/var/lib/icsranger/master/workers/known_threats/yara_
exported_files/matched_yara_files/1/smb/1597600276270606_0.bin
src=10.20.6.205 smac=f0:18:98:66:5a:0c shost=N/A dst=10.10.10.10
dmac=N/A dhost=N/A externalId=60 cat=Create rt=Nov 17 10:18:55
start=Oct 12 2020 17:28:33 msg=Suspicious file transfer found! File
'/Teams/QA/all/imain.bin' was transferred via 'smb' and matched the
following Yara rules: ['ics_cert_hatman.yara/hatman_payload',
'ics_cert_hatman.yara/hatman'], Transferred from 10.20.6.205
```

Table 5: Suspicious File Transfer Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Suspicious File Transfer
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
	SiteID	The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network	The network of the primary asset involved in the alert	Default

Name	Description	Value in Example
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
Src Zone	The source zone	Endpoint: Other
Dst Zone	The destination zone	Endpoint: Other
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/60-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/60-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.20.6.205
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	f0:18:98:66:5a:0c
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	Apple
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.10.10.10
NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	N/A
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	N/A
storyID	The ID of the story for this event	4
filepath	The filepath for the suspicious file transfer	/private/var/lib/icsranger/master/workers/known_threats/yara_exported_files/matched_yara_files/1/smb/1597600276270606_0.bin
src	The IP address of the primary asset involved in the event	10.20.6.205
smac	The MAC address of the primary asset involved in the event	f0:18:98:66:5a:0c
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.10.10.10
dmac	The MAC address of the secondary asset involved in the event	N/A
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	60
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Create
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Suspicious file transfer found! File '/Teams/QA/all/imain.bin' was transferred via 'smb' and matched the following Yara rules: ['ics_cert_hatman.yara/hatman_payload', 'ics_cert_hatman.yara/hatman'], Transferred from 10.20.6.205

2.6 New Asset Alert (CEF format)

Syslog Message String

```
CEF:0|Test_Brand|CTD|4.2.3|Alert|New Asset|5| cn1Label=SiteId cn1=1
cs1Label=Site cs1=Default cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs4Label=SiteId cs4=1
cs5Label=SrcZone cs5=Endpoint: Other cs6Label=DstZone cs6=Endpoint:
Other cs7Label=Category cs7=Integrity cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/105-1 cs9Label=Score cs9=80
cs10Label=PrimaryAssetIP cs10=10.10.6.121 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=N/A cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=N/A cs16Label=NonPrimaryAssetIP
cs16=10.20.10.166 cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=ac:bc:32:d1:40:b7
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=N/A cs22Label=StoryId cs22=2 src=10.10.6.121 smac=N/A shost=N/A
dst=10.20.10.166 dmac=ac:bc:32:d1:40:b7 dhost=N/A externalId=105
cat=Create rt=Nov 17 10:18:55 start=Oct 12 2020 17:28:33 msg=A new
asset has been detected: 10.10.6.121.
```

Table 6: New Asset Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Test_Brand
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name	The type of alert. There are several types of alerts (e.g. 'baseline deviation', 'new asset', 'configuration downloaded to PLC', 'known attack signature detected', etc. See Appendix A for common alerts.	New Asset
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters.	
	Site — The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network — The network of the primary asset involved in the alert	Default
	ResolvedAs — How the alert was treated; whether or not the alert was resolved: (Resolved or UnResolved)	UnResolved
	SiteID — The ID of the site	1
	SrcZone — The source zone	Endpoint: Other
	DstZone — The destination zone	Endpoint: Other
	Category — The type of event: Integrity or Security	Integrity

Name	Description		Value in Example
	AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/105-1
	Score	The alert score for this alert	80
	NOTE: **The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:** `ip1, ip2, ip3 …`		
	PrimaryAssetIP	The IP address of the primary asset	10.10.6.121
	PrimaryAssetType	The asset type of the primary asset	Endpoint
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	N/A
	PrimaryAssetOS	The OS of the primary asset	N/A
	PrimaryAssetVendor	The vendor of the primary asset	N/A
	NOTE: **The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:** `asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;`		
	NonPrimaryAssetIP	The IP address of the non-primary asset	10.20.10.166
	NonPrimaryAssetType	The asset type of the non-primary asset	Endpoint
	NonPrimaryAssetHostname	The host name of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address of the non-primary asset	ac:bc:32:d1:40:b7
	NonPrimaryAssetOS	The OS of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor of the non-primary asset	N/A
StoryID	The ID of the story (i.e. the chain of events that provide the context for this alert)		2
src	A randomly selected IP address of the primary asset involved in the alert *		10.10.6.121
smac	A randomly selected MAC address of the primary asset involved in the alert *	*	N/A
shost	A randomly selected host name (if known) of the primary asset involved in the alert*	Note that the asset may have additional addresses	N/A
dst	A randomly selected IP address of the secondary asset involved in the alert *		10.20.10.166
dmac	A randomly selected MAC address of the secondary asset involved in the alert *		ac:bc:32:d1:40:b7
dhost	A randomly selected host name (if known) of the secondary asset involved in the alert *		N/A
externalId	The ID of the corresponding alert. For example: An event with externalId 7 is associated with an alert with externalId 7		105
cat	The type of notification, depending on whether this event: • Is a new event in the system (Create) *or* • Is an existing event being updated (Update)		Create
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the alert		A new asset has been detected: 10.10.6.121

3 Syslog Event Examples

3.1 Known Threat Event (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Known Threat Event|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Default Zone cs6Label=Dst Zone cs6=Default Zone
cs7Label=Category cs7=Security cs8Label=AlertUrl
cs8=http://localhost:4200/alert/1-1 outcome=Unresolved
request=http://localhost:4200/alert/1-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.5.22.101 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=00:08:02:1c:47:ae
cs14Label=PrimaryAssetOS cs14=Windows 7/Server 2008 R2
cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=185.52.2.154
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=20:e5:2a:b6:93:f1
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Netgear cn3Label=StoryId cn3=1  src=10.5.22.101
smac=00:08:02:1c:47:ae shost=N/A dst=185.52.2.154
dmac=20:e5:2a:b6:93:f1 dhost=N/A externalId=1 cat=Update rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Claroty Rule: GranCrab
Ransomware - C2 Certificate (10.5.22.101:49201 -> 185.52.2.154:443).
Signature:  content:"www|2e|kakaocorp|2e|link"; depth:200;
```

Table 7: Known Threat Event

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Event
Name	The type of event.	Known Threat Event
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	SiteID The ID of the site	1

Name	Description		Value in Example
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
	SrcZone	The source zone	Default Zone
	DstZone	The destination zone	Default Zone
	Category	The type of event: Integrity or Security	Security
	AlertUrl	The URL for this alert	http://localhost:4200/alert/1-1 outcome=Unresolved request=http://localhost:4200/alert/1-1
	Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**			
	PrimaryAssetIP	The IP address of the primary asset	10.5.22.101
	PrimaryAssetType	The asset type of the primary asset	Endpoint
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:08:02:1c:47:ae
	PrimaryAssetOS	The OS of the primary asset	Windows 7/Server 2008 R2
	PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**			
	NonPrimaryAssetIP	The IP address/es of the non-primary asset	185.52.2.154
	NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
	NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address of the non-primary asset	20:e5:2a:b6:93:f1
	NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Netgear
storyID	The ID of the story for this event		1
src	The IP address of the primary asset involved in the event		10.5.22.101
smac	The MAC address of the primary asset involved in the event		00:08:02:1c:47:ae
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		185.52.2.154
dmac	The MAC address of the secondary asset involved in the event		20:e5:2a:b6:93:f1
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		1
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Update
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the event		Claroty Rule: GranCrab Ransomware - C2 Certificate (10.5.22.101:49201 -> 185.52.2.154:443). Signature: content:"www|2e|kakaocorp|2e|link"; depth:200;

3.2 Baseline Deviation Event (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Baseline Deviation|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-2
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs4Label=SiteId cs4=2 cs5Label=SrcZone cs5=Engineering Station:
Rockwell cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category
cs7=Integrity cs8Label=AlertUrl cs8=https://10.91.1.186:5000/alert/25-
2 cs9Label=Score cs9=100 cs10Label=PrimaryAssetIP cs10=10.1.30.40
cs11Label=PrimaryAssetType cs11=Engineering Station
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAssetIP
cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cs22Label=StoryId cs22=3 src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=25 cat=Update rt=Nov 17 10:18:55 start=Oct 12
2020 17:28:33 msg=CIP : Service Get Attribute All called on
ExtendedDevice
```

Table 8: Baseline Deviation Event

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Event
Name		The type of event.	Baseline Deviation
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-2
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or UnResolved	UnResolved
	SiteID	The ID of the site	2
	SrcZone	The source zone	Engineering Station: Rockwell

Name	Description	Value in Example
DstZone	The destination zone	PLC: Rockwell
Category	The type of event: Integrity or Security	Integrity
AlertUrl	The URL for this alert	https://10.91.1.186:5000/alert/25-2
Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.1.30.40
PrimaryAssetType	The asset type of the primary asset	Engineering Station
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	00:50:56:b9:e2:ad
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	PLC
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	00:1d:9c:c0:04:9d
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Rockwell Automation
storyID	The ID of the story for this alert	3
src	The IP address of the primary asset involved in the event	10.1.30.40
smac	The MAC address of the primary asset involved in the event	00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.0.40
dmac	The MAC address of the secondary asset involved in the event	00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	25
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Update
rt	The timestamp of the current time (not of the baseline)	Nov 17 10:18:55
start	The baseline creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	CIP : Service Get Attribute All called on ExtendedDevice

3.3 Protocol Specific OT Alert (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Protocol|5|rt=Nov 01 2020 11:04:44
cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-2 cs2Label=Network
cs2=Default cs3Label=Resolved
As cs3=Unresolved cs4Label=SiteId cs4=2 cs5Label=SrcZone
cs5=Engineering Station: Rockwell cs6Label=DstZone cs6=PLC: Rockwell
cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.91.1.186:5000/alert/25-2 cs9Label=Score cs9=100
cs10Label=PrimaryAssetIP cs10=10.1.30.40 cs11Label=PrimaryAssetType
cs11=Engineering Station cs12Label=Prim
aryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAss
etIP cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d cs20Label
=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cs22Label=StoryId cs22=3 src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 d
mac=00:1d:9c:c0:04:9d dhost=N/A externalId=25 cat=Update rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Editing was done on DataTable
object (Operation: Create Instance).format(ctd_version, site_name,
alertURL)
```

Table 9: Protocol Specific OT Alert

Name	Description	Value in Example
Protocol	The name **of the syslog** message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Event
Name	The type of event.	Protocol
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-2
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or UnResolved	UnResolved
SiteID	The ID of the site	2
SrcZone	The source zone	Engineering Station: Rockwell
DstZone	The destination zone	PLC: Rockwell
Category	The type of event:	Integrity

Name	Description	Value in Example
	▪ Integrity or Security	
	AlertUrl The URL for this alert	https://10.91.1.186:5000/alert/25-2
	Score The score of this event	100
	NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: `ip1, ip2, ip3 …`	
	PrimaryAssetIP The IP address of the primary asset	10.1.30.40
	PrimaryAssetType The asset type of the primary asset	Engineering Station
	PrimaryAssetHostname The host name of the primary asset	N/A
	PrimaryAssetMAC The MAC address of the primary asset	00:50:56:b9:e2:ad
	PrimaryAssetOS The OS of the primary asset	N/A
	PrimaryAssetVendor The vendor of the primary asset	VMware
	NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: `asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;`	
	NonPrimaryAssetIP The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
	NonPrimaryAssetType The asset type/s of the non-primary asset	PLC
	NonPrimaryAssetHostname The host name/s of the non-primary asset	N/A
	NonPrimaryAssetMAC The MAC address/es of the non-primary asset	00:1d:9c:c0:04:9d
	NonPrimaryAssetOS The OS/es of the non-primary asset	N/A
	NonPrimaryAssetVendor The vendor/s of the non-primary asset	Rockwell Automation
StoryId		3
src	The ID of the story (i.e. the chain of events that provide the context for this event)	10.1.30.40
smac	The MAC address of the primary asset involved in the event	00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.0.40
dmac	The MAC address of the secondary asset involved in the event	00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	25
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Update
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Editing was done on DataTable object (Operation: Create Instance).format(ctd_version, site_name, alertURL)

4 Syslog New Baseline Examples

Syslog Message String (CEF format)

```
CEF:0|Claroty|CTD|4.2.3|Baseline|None|1|rt=Nov 01 2020 11:04:44
cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default cs2Label=Network
cs2=Default cs3Label=Transmission cs3=None cs5Label=Src Zone cs5=Default
Zone cs6Label=Dst Zone cs6=Default Zone cs7Label=Category cs7=Network
cs8Label=CategoryAccess cs8=None cs9Label=Frequency cs9=NotTimed
cs10Label=FirstSeen cs10=Aug 16 2020 17:50:52 src=N/A
smac=00:80:f4:12:8b:10 shost=N/A dst=N/A dmac=ff:ff:ff:ff:ff:ff dhost=N/A
externalId=41 cat=Create rt=Aug 16 2020 17:50:52 msg=ARP : Gratuitous ARP
for ipv4 address 84.18.139.16 with mac address 00:80:f4:12:8b:10
```

Table 10: Baseline Example

Name	Description		Value in Example
Protocol	The name of the syslog message format in use		CEF
Vendor	The name of the vendor of the product		Claroty
Product	The name of the product in use		CTD
Product version	The version number of the product in use		4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck		Baseline
Name	The type of baseline		None
Approved	Whether this baseline is approved or not, represented as an integer of 0 or 1 where: ▪ 0 = Baseline Approved ▪ 1 = Baseline Unapproved		1
SiteID	The ID of the site		1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters		
	SiteID	The ID of the site	1
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network	The network involved	Default
	Transmission	The type of transmission protocol in use	None
	Src Zone	The source Virtual Zone	Default Zone
	Dst Zone	The destination Virtual Zone	Default Zone
	Category	The type of alert: ▪ Integrity/Security/Network/Other For baseline the category shall be Network	Network
	CategoryAccess	Access type: None, Read, Write, Execute, Publish	None
	Frequency	Frequency of recurrence if timed. Otherwise: NotTimed	NotTimed
	FirstSeen	Timestamp of when the baseline was first detected	Aug 16 2020 17:50:52
src	The IP address of the primary asset involved in the event		N/A
smac	The MAC address of the primary asset involved in the event		00:80:f4:12:8b:10
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		N/A
dmac	The MAC address of the secondary asset involved in the event		ff:ff:ff:ff:ff:ff
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		41
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Create
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
msg	The message containing the description of the status check		msg=ARP : Gratuitous ARP for ipv4 address 84.18.139.16 with mac address 00:80:f4:12:8b:10

5 Syslog Sniffer Status Check Example

This is a type of system event.

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|SnifferStatus|SnifferStatus|3|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=SiteName cs1=site-1
cs2Label=SiteId cs2=1 cs3Label=InterfaceName cs3=ens224
cs4Label=Network cs4=Default cs5Label=IPaddress cs5=10.10.6.207
cs6Label=SnifferStatus cs6=down rt=Jul 15 2020 09:04:53 msg=interface
ens224 is currently not receiving any packets
```

Table 11: Sniffer Status Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/Health Check	SnifferStatus
Name	The name of the message	Sniffer Status
Severity	The severity of the status message For a Sniffer Status alert, the Severity is always 3. For a Site Status alert: • Site Down = 8 • Site Up = 0	
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value>, *where:* N is incremental according to the number of parameters.	
Site Name	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1
Site ID	The ID of the site	1
Interface Name	The name of the interface in use	Ens224
Network	The network involved	Default
IPaddress	The IP address involved	10.10.6.207
Sniffer Status	Whether the sniffer is currently active: ▪ Up or Down	down
rt	The timestamp of the status check	Jul 15 2020 09:04:53
msg	The message containing the description of the status check	interface ens224 is currently not receiving any packets

6 Syslog Health Check Monitoring Example

Below is an example of a Syslog message for Health Check monitoring. Note that this message structure is dependent on your environment and on your TIV configuration. For example, Site output will differ from Central output; as there are no dissectors in the EMC.

> Note The labelling in the values in this example changes according to the user's running environment.

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|HealthCheck| cn1Label=SiteId cn1=1
cs1Label=Site cs1=Default cs2Label=cpu cs2=0.19 cs3Label=mem cs3=54.3
cs4Label=used__opt_icsranger cs4=9.23 cs5Label=used__var cs5=9.23
cs6Label=used__tmp cs6=9.23 cs7Label=used__etc cs7=9.23
cs8Label=busy_sda cs8=0.84 cs9Label=busy_sda1 cs9=0.0
cs10Label=busy_sda2 cs10=0.84 cs11Label=busy_sr0 cs11=0.0
cs12Label=busy_dm-0 cs12=0.93 cs13Label=busy_sdb cs13=0.19
cs14Label=busy_sdb1 cs14=0.19 cs15Label=drop_ens192 cs15=0
cs16Label=drop_lo cs16=0 cs17Label=service_mariadb cs17=Up
cs18Label=service_postgres cs18=Up cs19Label=service_redis cs19=Up
cs20Label=service_rabbitmq cs20=Up cs21Label=service_icsranger cs21=Up
cs22Label=service_watchdog cs22=Up cs23Label=q_baseline_tracker cs23=0
cs24Label=q_bridge cs24=0 cs25Label=q_central_bridge cs25=0
cs26Label=q_concluding cs26=0 cs27Label=q_diode_feeder cs27=0
cs28Label=q_dissector-0 cs28=0 cs29Label=q_dissector-1 cs29=0
cs30Label=q_dissector-2 cs30=0 cs31Label=q_dissector_ng cs31=0
cs32Label=q_enricher cs32=0 cs33Label=q_leecher cs33=0
cs34Label=q_monitor cs34=0 cs35Label=q_packets cs35=0
cs36Label=q_packets_errors cs36=0 cs37Label=q_preprocessing cs37=0
cs38Label=q_processing cs38=0 cs39Label=q_processing_errors cs39=0
cs40Label=q_processing_high cs40=0 cs41Label=q_zordon_updates cs41=0
cs42Label=queue_purge cs42=0 cs43Label=rd_bridge cs43=11
cs44Label=rd_dissector-0 cs44=0 cs45Label=rd_dissector-1 cs45=0
cs46Label=rd_dissector-2 cs46=0 cs47Label=rd_dissector_ng cs47=0
cs48Label=rd_preprocessing cs48=0 cs49Label=unhandled_events cs49=0
cs50Label=conclude_time cs50=0 cs51Label=exceptions cs51=0
cs52Label=mysql_query cs52=0.02 cs53Label=postgres_query cs53=0.0
cs54Label=dropped_entities cs54=0 cs55Label=workers cs55=26
cs56Label=workers_stop cs56=0 cs57Label=workers_restart cs57=0
msg=Successfully ran health monitoring
```

Table 12: Health Check Monitoring Example

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Healthcheck
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters.	
Site	The site from which the information contained in the message is being sent.	Default
cpu	CPU Utilization: CPU load average as a percentage of the total available CPU capacity (including all available cores)	0.19
mem	Memory Usage: The percent of current memory consumption. The value is a number between 0 and 100	54.3
Disk Utilization The percent of disk space currently used in this particular directory		
used__opt_icsranger		9.23
used__var		9.23
used__tmp		9.23
used__etc		9.23
Disk Busy Percent How frequently the particular disk partition is in use (as a percentage between 0 and 1)		
busy_sda		0.84
busy_sda1		0.0
busy_sda2		0.84
busy_sr0		0.0
busy_dm-0		0.93
busy_sdb		0.19
busy_sdb1		0.19
Network Interface Packet Drops The number of packets that are dropped when using this network interface		
drop_ens192		0
drop_lo		0
Services Running Whether the service is running (Up or Down)		
service_mariadb		Up
service_postgres		Up
service_redis		Up
service_rabbitmq		Up
service_icsranger		Up
service_watchdog		Up

Name	Description	Value in Example
	Queue Message Counts Each worker has its own read queue	
	q_baseline_tracker	0
	q_bridge	0
	q_central_bridge	0
	q_concluding	0
	q_diode_feeder	0
	q_dissector-0 . . n	0 . . .
	q_dissector_ng	0
	q_enricher	0
	q_leecher	0
	q_monitor	0
	q_packets	0
	q_packets_errors	0
	q_preprocessing	0
	q_processing	0
	q_processing_errors	0
	q_processing_high	0
	q_zordon_updates	0
	Queue Purges Queue purges counted in the last 24 hours	
	queue_purge	0
	Queue Read Count The queue read count for each component	
	rd_bridge	11
	rd_dissector-0	0
	rd_dissector-1	0
	rd_dissector-2	0
	rd_dissector_ng	0
	rd_preprocessing	0
	Event Handling The number of events that have not been handled by the system	
	unhandled_events	0
	Conclusion Time	
	conclude_time	0
	Logs Exceptions The number of new logged exceptions	
	exceptions	0
	MySQL Query time, in seconds	
	mysql_query	0.02
	PostgreSQL Query time, in seconds	
	postgres_query	0.0
	Dropped entities Number of entities dropped by the system due to reaching the limit of number of entities	
	dropped_entities	0
	Workers Stopped/Restarted	
	workers — The total number of workers (processes) in the system	26
	workers_stop — The number of stopped workers	0
	workers_restart — Total number of workers restarted	0
msg	The message containing the description of the health check monitoring test	Successfully ran health monitoring

7 Appendix A: Common Alert Types

Process Integrity Alerts

- New Asset — A new asset has been added into the environment (vendor laptops, virtual machines, physical servers, network switches, PLCs, etc.)
- Baseline Deviation — New traffic occurs between devices that has never occurred before within the baseline. The baselines are categorized by their communication type, access type and frequency
- Policy Rule Match – This occurs when an explicit policy rule defined with an 'Alert' action is matched by the detected communication.
- Policy Unmatched Violation – This type of alert is triggered when the detected communication was not matched to any rule with an 'Allow' action, and as a result the implicit Alert on Anything rule was hit. This means that there was no pre-existing policy rule to allow such communication.
- Asset Information Change — Occurs when information associated with an asset is changed (e.g. new IP/MAC address)
- Mode Change — When a user changes the state of a PLC from an engineering workstation or other software application. Mode state examples: Run, Stop, Program
- Configuration Upload — When a user uploads the configuration from a PLC to an engineering workstation or other software package Commonly contains the following types of alert information: code segments being uploaded; code differences; users performing code changes; project name / identifier
- Configuration Download— When a user downloads the configuration from an engineering workstation or other software package to a PLC. See above for common types of alert information
- Monitor Debug — When a user utilizes an engineering workstation or other software package to put a PLC into monitor or debug mode.
  (Note: This is typically a troubleshooting function built into some PLCs)
- New Asset Conflict — When new information occurs that conflicts with existing asset information. Typically occurs when assets have the same IP/MAC addresses or other identical information
- Firmware Upgrade — When firmware is changed for an asset. Generally performed by an engineering workstation or other software on a PLC
- Online Edit — When a user connects to the PLC from an engineering station and performs changes in the settings
- Suspicious Activity — Suspicious behavior that is generally indicative of malware

Security Alerts

Security alerts represent a malicious behavior and are not generally supposed to occur within the OT environment and should always be evaluated at the highest priority.

- Login — Occurs with certain makes / models of PLCs that support authentication functions
- Man-in-the-Middle Attack — When an attacker inserted a new machine into the communication pathway between two assets within the network. This new machine will use this position to either monitor the communication between these assets, or to alter the communication between these assets
- Network Scan — When an attacker scans either the OT network, or assets within the OT network, looking for attack pathways. Shows the source of the network scan and the affected assets
- TCP Scan – Suspicious activity of an asset that is performing port scanning in the network
- UDP Scan – Suspicious activity of an asset that is performing port scanning in the network
- Known Threat Alerts – TIV utilizes a sophisticated signatures-based database in order to enhance its capability for identifying known attacks
- Threats – Collection of known malware commands and control servers