Vectra AI

Quadrant UX Syslog Guide

VECTRA

Revision History

DATE	COMMENT
June 2024	Release 8.4 • Adds MITRE T-Number(s) associated with Detections within Host and Account Detection Enhanced Detail messages
September 2022	Release 7.1 • Adds Kerberoasting: Weak Cipher and Kerberoasting: SPN Sweep detections to $d_type_vname fields. • Adds “quadrant” value to Host and Account Enhanced scoring log events.
March 2022	Release 6.17 • Adds new field for “proxied destination” under enhanced detail message detail for account and host detection syslog messages.
August 2020	Release 6.0 • Adds enhanced detail for detection syslog messages
July 2020	Release 5.9 • Adds enhanced detail for host/account syslog messages
June 2020	Release 5.8 • Adds Microsoft Defender ATP Lockdown log events and Observed Privilege level and decreasing score fields to Account and Host scoring logs.
March 2020	Release 5.6 • Adds detection names for Host and Account detection message details
February 2020	Release 5.5 • Adds details for Account Lockdown log events
January 2020	Release 5.4 • Adds Type details for Health log events • Updates Account Detection example message
October 2019	Release 5.2 • Adds support for Account Detections • Removes timestamp and vectra_ prefix for all syslog message examples
September 2019	Release 5.0

- Adds support for Account Scoring
- Adds JSON examples for all types

Table of Contents

Overview

Administrators can configure the Vectra® AI X-series platform to send host and account scoring information, detection details, campaign details, and audit logs over syslog to external collectors for storage and analysis.

The X-series can be configured to use a standard syslog, the HP ArcSight Common Event Format (CEF) syslog or JSON message format. Syslog messages include information displayed in the X-series user interface, although in some cases the representations in the user interface may consist of derived values. Syslog messages can reflect a host scoring, account scoring, detection event, campaign event, audit log or system health alert.

Host scoring messages are generated when a host score is changed, which occurs upon initial threat detection, discovery of additional detections, and updates to any discovered detections. A host scoring message contains information on whether the host is marked as a key asset or has a detection that targets a key asset. The host score is also reduced over time if the underlying detection behavior subsides, either because of user intervention or because the host has left the network.

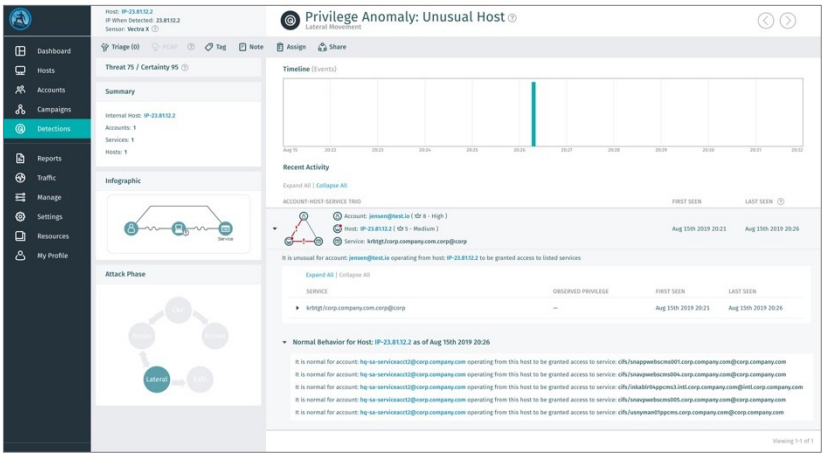
Account scoring messages are generated when an account score is changed, which occurs upon initial threat detection, discovery of additional detections, and updates to any discovered detections. The account score is reduced over time if the underlying detection behavior subsides, either because of user intervention or because the account has left the network.

Detection messages are created upon initial detection and for each update of the detection. Campaign messages are generated upon initial creation of a campaign, and on campaign closure.

Audit logs are generated for login events (both successful and failed), logout events, as well as other user actions that can impact the security posture of the product (such as creating a triage filter, marking detections as fixed, creating users, creating roles).

System health logs are generated for specific events that can impact the health and operation of the product. These include changes to sensor connectivity, capture interface status and disk health status. Further, system health syslog includes periodic heartbeat messages that indicate the status of the headend.

Using the default sort order in the X-series user interface, the first row of the Recent Activity table reflects the most recent update, while the last row reflects the oldest tracked detection.



An example of a detection report from the Vectra X-series platform.

Since the X-series platform limits the amount of data it maintains for individual detections, the last detection instance in the table may be the first instance of observed behavior or, for a very active detection, may simply be the oldest one currently tracked.

The Recent Activity table is fully sortable, so clicking on the Last Seen column heading will place the oldest detection at the top of the table.

Most detection messages contain event updates and summary fields (e.g. bytesSent, totalBytesSent). Event fields are displayed in the Recent Activity table while summary fields are displayed directly above the table in the Detection Summary portion of the user interface.

Customers can enable one or more log types for each syslog destination. If chosen, the relevant logs are sent to the syslog destination per the specified format.

Host Scoring log events

Host Scoring Standard syslog message example

```
HOST [host@41261 category="$category" hostName="$host_name" currentIP="$host_ip"
dvchost="$dvchost" threat="$threat" certainty="$certainty" privilege="$privilege"
scoreDecreases="$score_decreases" URL="$href" UTCTime="$UTCTimeEnd"
sourceKeyAsset="$src_key_asset" destKeyAsset="$dst_key_asset"]
```

Host Scoring Standard syslog message detail

Key	Type	Description
$category	str	Always the string 'HOST SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this host
$dst_key_asset	bool	Whether there is a detection that is targeting this host and this host is a key asset
$dvchost	str	The hostname of the Brain
$host_ip	str	The IP of the host being scored
$host_name	str	The name of the host being scored
$href	str	A link to see this host in the UI
$privilege	int	The observed privilege level of the host.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$src_key_asset	bool	Whether the host being scored is marked as a key asset
$threat	int	Newly calculated host threat
$UTCTimeEnd	int	Seconds since epoch for event end

Host Scoring CEF syslog message example

```
CEF:0|Vectra |X Series|$version|hsc|Host Score Change|3|externalId=$host_id cat=$category
dvc=$headend_addr dvchost=$dvchost shost=$host_name src=$host_ip dst=$host_ip
flexNumber1Label=threat flexNumber1=$threat flexNumber2Label=certainty
flexNumber2=$certainty flexNumber3Label=privilege flexNumber3=$privilege
cs3Label=scoreDecreases cs3=$score_decreases cs4Label=Vectra Event URL cs4=$href
start=$UTCTimeStartCEF end=$UTCTimeEndCEF cs1Label=sourceKeyAsset cs1=$src_key_asset
cs2Label=destKeyAsset cs2=$dst_key_asset
```

Host Scoring CEF syslog message detail

Key	Type	Description
$category	str	Always the string 'HOST SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this host
$dst_key_asset	bool	Whether there is a detection that is targeting this host and this host is a key asset
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$host_id	int	The ID of the host
$host_ip	str	The IP of the host being scored
$host_name	str	The name of the host being scored
$href	str	A link to see this host in the UI
$privilege	int	The observed privilege level of the host.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$src_key_asset	bool	Whether the host being scored is marked as a key asset
$threat	int	Newly calculated host threat
$UTCTimeEndCEF	int	Milliseconds since epoch for event end
$UTCTimeStartCEF	int	Milliseconds since epoch for event start
$version	str	The version of Vectra platform running the Vectra Brain

Host Scoring JSON syslog message example

```
{"version": "$version", "dvchost": "$dvchost", "host_ip": "$host_ip", "href": "$href",
"src_key_asset": $src_key_asset, "host_id": $host_id, "headend_addr": "$headend_addr",
"category": "$category", "dst_key_asset": $dst_key_asset, "privilege": $privilege,
"certainty": $certainty, "score_decreases": $score_decreases, "vectra_timestamp": "$timestamp",
"host_name": "$host_name", "threat": $threat}
```

Host Scoring JSON syslog message detail

Key	Type	Description
$category	str	Always the string 'HOST SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this host
$dst_key_asset	bool	Whether there is a detection that is targeting this host and this host is a key asset
$dvchost	str	The hostname of the Vectra Brain

$headend_addr	str	The IP of the Vectra Brain
$host_id	int	The ID of the host
$host_ip	str	The IP of the host being scored
$host_name	str	The name of the host being scored
$href	str	A link to see this host in the UI
$privilege	int	The observed privilege level of the host.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$src_key_asset	bool	Whether the host being scored is marked as a key asset
$threat	int	Newly calculated host threat
$timestamp	int	Timestamp in seconds since epoch
$version	str	The version of Vectra platform running the Vectra Brain

Host Scoring Enhanced details

Enhanced details are available for host system logs in each of three formats: Standard, CEF, and JSON. In the case of Standard, the fields are appended to the end of the system log message.

```
vectra_standard_v2 -: HOST [host@41261 category="$category" hostName="$hostName"
currentIP="$currentIP" dvchost="$dvchost" threat="$threat" certainty="$certainty"
privilege="$privilege" scoreDecreases="$scoreDecreases" URL="$url" UTCTime="$UTCTime"
sourceKeyAsset="$sourceKeyAsset" destKeyAsset="$destKeyAsset" sensor="$sensor"
detectionProfile="$detectionProfile"  hostGroups=[$hostGroups]  tags="$tags"
accountAccessHistory="$accountAccessHistory"    serviceAccessHistory="$serviceAccessHistory"
macAddress="$macAddress"  macVendor="$macVendor"  lastDetectionType="$lastDetectionType"
quadrant="$quadrant"]
```

In the case of CEF, the new fields are represented as a JSON string inside the msg field.

```
vectra_cef_v2 -: CEF:0|Vectra |X Series|$version|hsc|Host Score
Change|3|externalId=$host_id cat=$category dvc=$headend_addr dvchost=$dvchost
shost=$host_name src=$host_ip dst=$host_ip flexNumber1Label=threat flexNumber1=$threat
flexNumber2Label=certainty flexNumber2=$certainty flexNumber3Label=privilege
flexNumber3=$privilege  cs3Label=scoreDecreases cs3=$score_decreases cs4Label=Vectra Event
URL cs4=$href start=$UTCTimeStartCEF end=$UTCTimeEndCEF cs1Label=sourceKeyAsset
cs1=$src_key_asset cs2Label=destKeyAsset cs2=$dst_key_asset msg="{'sensor': $sensor,
'detectionProfile':  $detectionProfile,  'hostGroups':[$hostGroups],  'tags':[$tags],
'accountAccessHistory':[$accountAccessHistory],
'serviceAccessHistory':[$serviceAccessHistory],  'macAddress':  $macAddress,  'macVendor':
$macVendor, 'lastDetectionType': $lastDetectionType, 'quadrant': $quadrant}"
```

In the case of JSON, the new fields appear throughout the JSON object.

```
vectra_json_v2 -: {"account_access_history": [$accountAccessHistory], "tags": [$tags],
"service_access_history": [$serviceAccessHistory], "dvchost": "$dvchost", "host_ip":
"$hostIP", "last_detection_type": "$lastDetectionType", "href": "$href", "src_key_asset":
$src_key_asset, "host_id": $host_id, "headend_addr": "$headend_addr", "category":
"$category", "dst_key_asset": $dst_key_asset, "detection_profile": $detectionProfile,
```

```
"score_decreases": $scoreDecreases, "host_groups": [$hostGroups], "mac_vendor":
$macVendor, "certainty": $certainty, "vectra_timestamp": "$vectra_timestamp", "threat":
$threat, "host_name": "$host_name", "version": "$version", "macAddress":$mac_address,
"privilege": $privilege, "sensor": "$sensor", "quadrant": "$quadrant"}
```

Host Scoring Enhanced Fields detail

Key	Type	Description
$sensor	str	The sensor associated with this host.
$detectionProfile	obj	The detection profile associated with this host.
$hostGroups	list	A list of the host groups that the host is a member of.
$tags	list	A list of tags applied to the host.
$accountAccessHistory	list	The account access history associated with this host.
$serviceAccessHistory	list	The service access history associated with this host.
$macAddress	str	The MAC address of this host.
$macVendor	str	The vendor of the MAC address of this host.
$lastDetectionType	str	The most recent type of detection associated with this host.
$quadrant	str	The values for this field are Low, Medium, High, or Critical, and reflect the status of the given host in the UI.

Account Scoring log events

Account Scoring Standard syslog message example

```
ACCOUNT [account@41261 category="$category" threat="$threat" certainty="$certainty"
privilege="$privilege" scoreDecreases=$score_decreases URL="$href" UTCTime="$UTCTimeEnd"]
```

Account Scoring Standard syslog message detail

Key	Type	Description
$category	str	Always the string 'ACCOUNT SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this account
$href	str	A link to see this account in the UI
$privilege	int	The observed privilege level of the account.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$threat	int	Newly calculated account threat

$UTCTimeEnd	int	Seconds since epoch for event end

Account Scoring CEF syslog message example

```
CEF:0|Vectra Networks|X Series|$version|asc|Account Score Change|3|externalId=$account_id
cat=$category dvc=$headend_addr saccount=$account_uid flexNumber1Label=threat
flexNumber1=$threat flexNumber2Label=certainty flexNumber2=$certainty
flexNumber3Label=privilege flexNumber3=$privilege cs3Label=scoreDecreases cs3=$score_decreases
cs4Label=Vectra Event URL cs4=$href start=$UTCTimeStartCEF end=$UTCTimeEndCEF"""
```

Account Scoring CEF syslog message detail

Key	Type	Description
$account_id	int	The ID of the account
$account_uid	str	The user account identifier.
$category	str	Always the string 'ACCOUNT SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this account
$headend_addr	str	The IP of the Vectra Brain
$href	str	A link to see this account in the UI
$privilege	int	The observed privilege level of the account.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$threat	int	Newly calculated account threat
$UTCTimeEndCEF	int	Milliseconds since epoch for event end
$UTCTimeStartCEF	int	Milliseconds since epoch for event start
$version	str	The version of Vectra platform running the Vectra Brain

Account Scoring JSON syslog message example

```
{"category": "$category", "account_id": $account_id, "href": "$href", "certainty": $certainty,
"privilege": $privilege, "score_decreases": $score_decreases, "version": "$version",
"vectra_timestamp": "$timestamp", "headend_addr": "$headend_addr", "threat": $threat,
"account_uid": "$account_uid"}
```

Account Scoring JSON syslog message detail

Key	Type	Description
$account_id	int	The ID of the account

$account_uid	str	The user ID of the account
$category	str	Always the string 'ACCOUNT SCORING'. Used internally to differentiate between account, host and detection messages.
$certainty	int	The certainty of the score assigned to this account
$headend_addr	str	The IP of the Vectra Brain
$href	str	A link to see this account in the UI
$privilege	int	The observed privilege level of the account.
$score_decreases	bool	Indicates whether both Threat and Certainty scores are decreasing.
$threat	int	Newly calculated account threat
$timestamp	int	Timestamp in seconds since epoch
$version	str	The version of Vectra platform running the Vectra Brain

Account Scoring Enhanced details

Enhanced details are available for account system logs in each of three formats: Standard, CEF, and JSON. In the case of Standard, the fields are appended to the end of the syslog message.

```
vectra_standard_account_v2 -: ACCOUNT [account@41261 category="$category"
accountName="$accountName " threat="$threat" certainty="$certainty" privilege="$privilege
" scoreDecreases=$scoreDecreases URL="$url" UTCTime="$UTCTime" tags="[$tags]"
hostAccessHistory="[$hostAccessHistory]"    serviceAccessHistory="[$serviceAccessHistory]"
lastDetectionType="$lastDetectionType"   quadrant="$quadrant"]
```

In the case of CEF, the new fields are represented as a JSON string inside the msg field.

```
vectra_cef_account_v2 -: CEF:0|Vectra Networks|X Series|$version|asc|Account Score
Change|3|externalId=$account_id cat=$category dvc=$headend_addr saccount=$account_uid
flexNumber1Label=threat flexNumber1=$threat flexNumber2Label=certainty
flexNumber2=$certainty flexNumber3Label=privilege flexNumber3=$privilege
cs3Label=scoreDecreases cs3=$score_decreases cs4Label=Vectra Event URL cs4=$href
start=$UTCTimeStartCEF end=$UTCTimeEndCEF
msg="{'tags':[$tags],'hostAccessHistory':[$hostAccessHistory],'serviceAccessHistory':[$ser
viceAccessHistory],  'lastDetectionType':  $last_detection_type,  'quadrant':  $quadrant}"
```

In the case of JSON, the new fields appear throughout the JSON object.

```
vectra_json_account_v2 -: {"account_id": $account_id, "tags": [$tags],
"service_access_history": [$serviceAccessHistory], "version": "$version",
"last_detection_type": "$lastDetectionType", "href": "href", "headend_addr":
"$headend_addr", "category": "$category", "score_decreases": $scoreDecreases, "certainty":
$certainty, "vectra_timestamp": "$vectra_timestamp", "host_access_history":
[$hostAccessHistory], "threat": $threat, "privilege": $privilege, "account_uid":
"$account_uid", "quadrant": "$quadrant"}
```

Account Scoring Enhanced Fields detail

Key	Type	Description
$tags	list	A list of tags applied to the host.
$hostAccessHistory	list	The host access history associated with this account.
$serviceAccessHistory	list	The service access history associated with this account.
$lastDetectionType	str	The most recent type of detection associated with this account.
$quadrant	str	The values for this field are Low, Medium, High, or Critical, and reflect the status of the given account in the UI.

Host Detection log events

Host Detection Standard syslog message example

```
DETECT [detection@41261 category="$category" type="$d_type_vname" hostname="$host_name"
currentIP="$host_ip" dvchost="$dvchost" threat="$threat" certainty="$certainty"
URL="$href" DestinationIP="$dd_dst_ip" DestinationDomain="$dd_dst_dns"
DestinationPort="$dd_dst_port" Proto="$dd_proto" triaged="$triaged" BytesSent="$dd_bytes_sent"
BytesRcvd="$dd_bytes_rcvd" UTCTimeStart="$UTCTimeStart" UTCTimeEnd="$UTCTimeEnd"]
```

Host Detection Standard syslog message detail

Key	Type	Description
$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection
$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan

		Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio Protocol Abuse Pulling Instructions Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client

		Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control

		Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance Custom model smbfiles botnet_activity Custom model smbfiles command_and_control Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance

		Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0
$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event
$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$dd_proto	str	The protocol over which this detection fired (e.g., tcp). Does not apply to all detections. Defaults to empty string
$dvchost	str	The hostname of the Vectra Brain
$host_name	str	The hostname for attacking host
$host_ip	str	The IP of the host that triggered the detection
$href	str	A link to this detection in the UI
$threat	int	The threat score of this detection
$triaged	bool	Whether the detection has been triaged yet or not
$UTCTimeEnd	int	Seconds since epoch for event end
$UTCTimeStart	int	Seconds since epoch for event start

Host Detection CEF syslog message example

```
CEF:0|Vectra |X Series|$version|$d_type|$d_type_vname|$severity|externalId=$detection_id
cat=$category dvc=$headend_addr dvchost=$dvchost shost=$host_name src=$host_ip
flexNumber1Label=threat flexNumber1=$threat flexNumber2Label=certainty flexNumber2=$certainty
cs4Label=Vectra Event URL cs4=$href cs5Label=triaged cs5=$triaged dst=$dd_dst_ip
dhost=$dd_dst_dns proto=$dd_proto dpt=$dd_dst_port out=$dd_bytes_sent in=$dd_bytes_rcvd
start=$UTCTimeStartCEF end=$UTCTimeEndCEF
```

Host Detection CEF syslog message detail

Key	Type	Description
$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection
$d_type	str	The Vectra internal representation of detection name (e.g., smash_n_grab, or sql_injection)
$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer

		Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio Protocol Abuse Pulling Instructions Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity

		Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement

		Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance Custom model smbfiles botnet_activity Custom model smbfiles command_and_control Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0

$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event
$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$dd_proto	str	The protocol over which this detection fired (e.g., tcp). Does not apply to all detections. Defaults to empty string
$detection_id	int	The ID of the detection
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$host_ip	str	The IP of the host that triggered the detection
$host_name	str	The hostname for attacking host
$href	str	A link to this detection in the UI
$severity	int	A score proportional to threat
$threat	int	The threat score of this detection
$triaged	bool	Whether the detection has been triaged yet or not
$UTCTimeEndCEF	int	Milliseconds since epoch for event end
$UTCTimeStartCEF	int	Milliseconds since epoch for event start
$version	str	The version of Vectra platform running the Vectra Brain

Host Detection JSON syslog message example

```
{"d_type_vname": "$d_type_vname", "dvchost": "$dvchost", "host_ip": "$host_ip", "href": "$href",
"detection_id": $detection_id, "dd_bytes_sent": $dd_bytes_sent, "headend_addr": "$headend_addr",
"dd_dst_port": $dd_dst_port, "category": "$category", "dd_bytes_rcvd": $dd_bytes_rcvd,
"dd_dst_dns": "$dd_dst_dns", "severity": $severity, "certainty": $certainty, "triaged":
$triaged, "vectra_timestamp": "$timestamp", "version": "$version", "host_name": "$host_name",
"threat": $threat, "dd_dst_ip": "$dd_dst_ip", "dd_proto": "$dd_proto", "d_type": "$d_type"}
```

Host Detection JSON syslog message detail

Key	Type	Description
$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection
$detection_id	int	The ID of the detection
$d_type	str	The Vectra internal representation of detection name (e.g.,

		smash_n_grab, or sql_injection)
$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio

		Protocol Abuse Pulling Instructions Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control

		Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance

		Custom model smbfiles botnet_activity Custom model smbfiles command_and_control Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0
$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event
$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$dd_proto	str	The protocol over which this detection fired (e.g., tcp). Does not

		apply to all detections. Defaults to empty string
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$host_ip	str	The IP of the host that triggered the detection
$host_name	str	The hostname for attacking host
$href	str	A link to this detection in the UI
$severity	int	A score proportional to threat
$threat	int	The threat score of this detection
$timestamp	int	Timestamp in seconds since epoch
$triaged	bool	Whether the detection has been triaged yet or not
$version	str	The version of Vectra platform running the Vectra Brain

Host Detection Enhanced Detail

When enabling enhanced details for Host Detections, the enhanced fields will be appended to the end of the existing syslog message for Standard and CEF formats. By convention, JSON objects are unordered.

General Host Detection Enhanced Detail message detail

Key	Type	Description
$MITRE	str	The MITRE T-Number(s) associated with the detection.

Host Detection per Detection Type Enhanced Detail message detail

Detection	Standard	CEF	JSON	Description
Cryptocurrency Mining	Count="$count"	cnt=$count	"count": $count	The number of attempts.
Outbound Dos	DosType="$dos_type"	msg=$dos_type	"dos_type": "$dos_type"	The DOS type.
Outbound Port Sweep	NumAttempts="$num_attempts"	cnt=$num_attempts	"num_attempts": $num_attempts	The number of attempts.
	Networks="$networks"	msg=$networks	"networks": "$networks"	The target subnets.
Brute-Force	Count="$count"	cnt=$count	"count": $count	The number of attempts.
Ransomware File Activity	Count="$count"	cnt=$count	"count": $count	The number of files affected.
	Shares="$shares"	msg=$shares	"shares": "$shares"	The related files shares.

	Extensions="$extensions"		"extensions": "$extensions"	File extensions used.
	RansomNotes="$ransom_notes"		"ransom_notes": "$ransom_note"	Ransome notes found.
Shell Knocker Client	SentPattern="$sent_pattern"		"sent _pattern": "$sent _pattern"	The sent pattern.
	SentNormalPattern="$sent_normal_pattern"		"sent_normal_pattern": "$sent_normal_pattern"	Example sent normal pattern.
	ReceivedPattern="$received_pattern"		"received _pattern": "$ received _pattern"	The received pattern.
	ReceivedNormalPattern="$received_normal_pattern"		"received_normal _pattern": "$ received _normal_pattern"	Example received normal pattern.
SMB Brute-Force	Count="$count	cnt=$count	"count": $count	The number of attempts.
	Reason="$reason"	msg=$reason	"reason": "$reason"	The error code.
	Accounts="$accounts"		"accounts": "$accounts"	The related accounts.
	Shares="$shares"		"shares": "$shares"	The related shares.
SQL Injection Activity	SQLFragment="$sql_fragment"	msg=$sql_fragment	"sql_fragment": "$sql_fragment"	The SQL fragment.
	HTTPSegment="$http_segment"		"http_segment": "$http_segment"	The HTTP segment.
	UserAgent="$user_agent"		"user_agent": "$user_agent"	The user agent.
	ResponseCode="$response_code"		"response_code": "$response_code"	The HTTP response code.
Suspicious Admin	NormalServers="$normal_servers"		"normal_servers": "$normal_servers"	The normal servers observed.
	NormalAdmins="$normal_admins"		"normal_admins": "$normal_admins"	The normal admins observed.
Suspicious Remote Desktop	Reason="$reason"	msg=$reason	"reason": "$reason"	The reason this is suspicious.
	ClientToken="$client_token"		"client_token": "$client_token"	The RDP client token.
	ClientName="$client_name"		"client_name": "$client_name"	The RDP client name.
	KeyboardID="$keyboard_id"		"keyboard_id": "$keyboad_id"	They keyboard layout ID.
	KeyboardName="$keyboard_name"		"keyboard_name": "$keyboad_name"	They keyboard layout name.
	ProductID="$product_id "		"product_id": "$product_id"	The unusual product ID.
Suspicious Remote Execution	Function="$function"	msg=$function	"function": "$function"	The executed function.
	Account="$account"		"account": "$account"	The related user account.

	UUID="$uuid"		"uuid": "$uuid"	The RPC UUID.
	NamedPipe="$namedpipe"		"namedpipe": "$namedpipe"	The named pipe.
Internal Stage Loader	StageLoaderBytesSent="$bytes_sent"		"bytes_sent": $bytes_sent	The bytes of data sent.
	StageLoaderBytesReceived="$bytes_received"		"bytes_received": $bytes_received	The bytes of data received.
Suspicious LDAP Query	Count="$count"	cnt=$count	"count": $count	The number of objects received.
	Request="$request"	msg=$request	"request": "$request"	The LDAP request.
	BaseObject="$base_object"		"base_object": "$base_object"	The base distinguished name.
	ResponseCode="$response_code"		"response_code": "$response_code"	The response code.
RPC Recon	UUID="$uuid"	msg=$uuid	"uuid": "$uuid"	The RPC UUID.
	Count="$count"	cnt=$count	"count": $count	The number of internal targets.
RDP Recon	Count="$count"	cnt=$count	"count": $count	The number of attempts.
	ClientName="$client_name"	msg=$client_name	"client_name": "$client_name"	The RDP client name.
	Cookie="$cookie"		"cookie": "$cookie"	The RDP client token.
SMB Account Scan	Count="$count"	cnt=$count	"count": $count	The number of attempts.
	Accounts="$accounts"	msg=$accounts	"accounts": "$accounts"	The related accounts.
Port Sweep	NumAttempts="$num_attempts	cnt=$num_attempts	"num_attempts": $num_attempts	The number of attempts.
	DstIPs="$dst_ips"	msg=$dst_ips	"dst_ips": "$dst_ips"	The target subnets.
Port Scan	Scans="$scans"	cnt=$scans	"scans": $scans	The number of attempts.
	Ports="$ports"	msg=$ports	"ports": "$ports"	Ports scanned.
	Successes="$successes"		"successes": $successes	The number of successes.
File Share Enumeration	Count="$count"	cnt=$count	"count": $count	The number of file shares enumerated.
	Shares="$shares"	msg=$shares	"shares": "$shares"	The shares enumerated.
	Accounts="accounts"		"accounts": "$accounts"	The related accounts.
External Remote Access	Count="$count"	cnt=$count'	"count": $count	The number of sessions.
Hidden DNS Tunnel	Count="$count"	cnt=$count'	"count": $count	The number of sessions.
TOR Activity	Count="$count"	cnt=$count'	"count": $count	The number of sessions.

Hidden HTTPS Tunnel	TunnelType="$tunnel_type"	msg=$tunnel_type	"tunnel_type": "$tunnel_type"	The type of hidden tunnel.
Threat Intelligence Match	ThreatFeeds="$threat_feeds"	msg=$threat_feeds	"threat_feeds": "$threat_feeds"	The name of the threat feed.
	Reason="$reason"		"reason": "$reason"	The indicating reason.
	MatchedDomain="$matched_domain" (CNC)		"matched_domain": "$matched_domain"	The matched domain.
	MatchedIP="$matched_ip" (Exfil)		"matched_ip": "$matched_ip"	The matched IP.
	MatchedUserAgent="$matched_user_agent" (Lateral)		"matched_user_agent": "$matched_user_agent"	The matched user-agent.
Suspicious HTTP	HttpMethod="$http_method"		"http_method": "$http_method"	The HTTP method.
	URL="$url"		"url": "$url"	The suspicous URL.
	Referer="$referer"		"referer": "$referer"	The referer.
	Host="$host"		"host": "$host"	The suspicous host.
	ReplyCacheControl="$reply_cache_control"		"reply_cache_control": " $reply_cache_control "	The replay cache control setting.
Suspicious Relay	IP="$ip"		"ip": "$ip"	The internal target host.
	Protocol="$protocol"		"protocol": "$protocol"	The external protocol used.
	Port="$port"		"port": "$port"	The external port used.
Data Smuggler	ProxiedDst=”foo.com”	msg=foo.com	“proxied_dst”: “foo.com”	The domain name or IP of the proxy.
Smash and Grab	ProxiedDst=”foo.com”	msg=foo.com	“proxied_dst”: “foo.com”	The domain name or IP of the proxy.

Account Detection log events

Account Detection Standard syslog message example

```
DETECT [detection@41261 category="$category" type="$d_type_vname" account="$account"
threat="$threat" certainty="$certainty" URL="$href" DestinationIP="$dd_dst_ip"
DestinationDomain="$dd_dst_dns" DestinationPort="$dd_dst_port" triaged="$triaged"
BytesSent="$dd_bytes_sent" BytesRcvd="$dd_bytes_rcvd" UTCTimeStart="$UTCTimeStart"
UTCTimeEnd="$UTCTimeEnd"]
```

Account Detection Standard syslog message detail

Key	Type	Description

$account	str	The account associated with this detection.
$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection

$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio Protocol Abuse Pulling Instructions

		Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info

		Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance Custom model smbfiles botnet_activity Custom model smbfiles command_and_control

		Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0
$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event
$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$href	str	A link to this detection in the UI
$threat	int	The threat score of this detection

$triaged	bool	Whether the detection has been triaged yet or not
$UTCTimeEnd	int	Seconds since epoch for event end
$UTCTimeStart	int	Seconds since epoch for event start

Account Detection CEF syslog message example

```
CEF:0|Vectra |X Series|$version|$d_type|$d_type_vname|$severity|externalId=$detection_id
cat=$category dvc=$headend_addr account=$account flexNumber1Label=threat flexNumber1=$threat
flexNumber2Label=certainty flexNumber2=$certainty cs4Label=Vectra Event URL cs4=$href
cs5Label=triaged cs5=$triaged dst=$dd_dst_ip dhost=$dd_dst_dns dpt=$dd_dst_port
out=$dd_bytes_sent in=$dd_bytes_rcvd start=$UTCTimeStartCEF end=$UTCTimeEndCEF
```

Account Detection CEF syslog message detail

Key	Type	Description
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0
$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event
$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$detection_id	int	The ID of the detection
$headend_addr	str	The IP of the Vectra Brain
$href	str	A link to this detection in the UI
$severity	int	A score proportional to threat
$threat	int	The threat score of this detection
$triaged	bool	Whether the detection has been triaged yet or not
$UTCTimeEndCEF	int	Milliseconds since epoch for event end
$UTCTimeStartCEF	int	Milliseconds since epoch for event start
$version	str	The version of Vectra platform running the Vectra Brain
$account	str	The account associated with this detection.
$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection
$d_type	str	The Vectra internal representation of detection name (e.g., smash_n_grab, or sql_injection)

$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio Protocol Abuse Pulling Instructions

		Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info

		Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance Custom model smbfiles botnet_activity Custom model smbfiles command_and_control

		Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance

Account Detection JSON syslog message example

```
{"d_type_vname": "$d_type_vname", "dvchost": "$dvchost", "href": "$href", "detection_id": $detect
ion_id, "dd_bytes_sent": $dd_bytes_sent, "headend_addr": "$headend_addr", "dd_dst_port": $dd_dst_
port, "category": "$category", "dd_bytes_rcvd": $dd_bytes_rcvd, "dd_dst_dns": "$dd_dst_dns", "sev
erity": $severity, "certainty": $certainty, "triaged": $triaged, "vectra_timestamp": "$timestamp"
, "account_uid": "$account_uid", "version": "$version", "threat": $threat, "dd_dst_ip": "$dd_dst_
ip", "d_type": "$d_type"}
```

Account Detection JSON syslog message detail

Key	Type	Description
$account_uid	str	The account name

$category	str	The category of the detection (e.g., EXFILTRATION)
$certainty	int	The certainty of the detection
$detection_id	int	The ID of the detection
$d_type	str	The Vectra internal representation of detection name (e.g., smash_n_grab, or sql_injection)
$d_type_vname	str	The name of the detection, which may include the following: Abnormal Ad Activity Abnormal Web Activity Automated Replication Brute-Force Cryptocurrency Mining Data Smuggler External Remote Access Fake Browser Activity File Share Enumeration Hidden DNS Tunnel Hidden HTTP Tunnel Hidden HTTPS Tunnel Hidden Tunnel Internal Darknet Scan Internal Port Scan Internal Stage Loader Kerberoasting: Weak Cipher Kerberoasting: SPN Sweep Kerberos Account Scan Kerberos Brute-Force Kerberos Client Activity Kerberos Server Access Kerberos Server Activity Malware Update Multi-home Fronted Tunnel Outbound DoS Outbound Port Sweep Outbound Scan Outbound Spam Peer-to-Peer Port Scan Port Sweep Privilege Anomaly: Unusual Account on Host

		Privilege Anomaly: Unusual Host Privilege Anomaly: Unusual Service Privilege Anomaly: Unusual Service from Host Privilege Anomaly: Unusual Trio Protocol Abuse Pulling Instructions Push Instructions RDP Recon RPC Recon Ransomware File Activity SMB Account Scan SMB Brute-Force SQL Injection Activity Shell Knocker Client Shell Knocker Server Smash and Grab Stealth HTTP Post Suspect Domain Activity Suspicious Admin Suspicious HTTP Suspicious Kerberos Account Suspicious Kerberos Client Suspicious LDAP Query Suspicious Relay Suspicious Remote Desktop Suspicious Remote Execution TOR Activity Threat Intelligence Match Custom Model detection names may include the following: Custom model dcerpc botnet_activity Custom model dcerpc command_and_control Custom model dcerpc exfiltration Custom model dcerpc info Custom model dcerpc lateral_movement Custom model dcerpc reconnaissance Custom model dhcp botnet_activity Custom model dhcp command_and_control Custom model dhcp exfiltration Custom model dhcp info

		Custom model dhcp lateral_movement Custom model dhcp reconnaissance Custom model dnsrecordinfo botnet_activity Custom model dnsrecordinfo command_and_control Custom model dnsrecordinfo exfiltration Custom model dnsrecordinfo info Custom model dnsrecordinfo lateral_movement Custom model dnsrecordinfo reconnaissance Custom model httpsessioninfo botnet_activity Custom model httpsessioninfo command_and_control Custom model httpsessioninfo exfiltration Custom model httpsessioninfo info Custom model httpsessioninfo lateral_movement Custom model httpsessioninfo reconnaissance Custom model isession botnet_activity Custom model isession command_and_control Custom model isession exfiltration Custom model isession info Custom model isession lateral_movement Custom model isession reconnaissance Custom model kerberos_txn botnet_activity Custom model kerberos_txn command_and_control Custom model kerberos_txn exfiltration Custom model kerberos_txn info Custom model kerberos_txn lateral_movement Custom model kerberos_txn reconnaissance Custom model ldap botnet_activity Custom model ldap command_and_control Custom model ldap exfiltration Custom model ldap info Custom model ldap lateral_movement Custom model ldap reconnaissance Custom model ntlm botnet_activity Custom model ntlm command_and_control Custom model ntlm exfiltration Custom model ntlm info Custom model ntlm lateral_movement Custom model ntlm reconnaissance Custom model rdp botnet_activity Custom model rdp command_and_control

		Custom model rdp exfiltration Custom model rdp info Custom model rdp lateral_movement Custom model rdp reconnaissance Custom model smbfiles botnet_activity Custom model smbfiles command_and_control Custom model smbfiles exfiltration Custom model smbfiles info Custom model smbfiles lateral_movement Custom model smbfiles reconnaissance Custom model smbmapping botnet_activity Custom model smbmapping command_and_control Custom model smbmapping exfiltration Custom model smbmapping info Custom model smbmapping lateral_movement Custom model smbmapping reconnaissance Custom model ssh botnet_activity Custom model ssh command_and_control Custom model ssh exfiltration Custom model ssh info Custom model ssh lateral_movement Custom model ssh reconnaissance Custom model ssl botnet_activity Custom model ssl command_and_control Custom model ssl exfiltration Custom model ssl info Custom model ssl lateral_movement Custom model ssl reconnaissance Custom model x509 botnet_activity Custom model x509 command_and_control Custom model x509 exfiltration Custom model x509 info Custom model x509 lateral_movement Custom model x509 reconnaissance
$dd_bytes_rcvd	int	Meaning differs depending on detection type. Does not apply to all detections. Defaults to 0
$dd_bytes_sent	int	The number of bytes in the traffic that caused the detection. Does not apply to all detections. Defaults to 0
$dd_dst_dns	str	The destination domain name of detection event

$dd_dst_ip	str	The destination IP address of detection event
$dd_dst_port	int	The port of the attacked host. Defaults to 80
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$href	str	A link to this detection in the UI
$severity	int	A score proportional to threat
$threat	int	The threat score of this detection
$timestamp	int	Timestamp in seconds since epoch
$triaged	bool	Whether the detection has been triaged yet or not
$version	str	The version of Vectra platform running the Vectra Brain

Account Detection Enhanced Detail

When enabling enhanced details for Account Detections, the enhanced fields will be appended to the end of the existing syslog message for Standard and CEF formats. By convention, JSON objects are unordered.

General Account Detection Enhanced Detail message detail

Key	Type	Description
$MITRE	str	The MITRE T-Number(s) associated with the detection.

Account Detection per Detection Type Enhanced Detail message detail

Detection	Standard	CEF	JSON	Description
Privilege Anomaly	AccountName="$account_name"	msg=$account_name	"account_name": "$account_name"	The account name.
	AccountInfo="$account_info"		"account_info": [$account_privilege_score, $account_privilege_level]	The account information, consisting of account privilege score and privilege level.
	ServiceName="$service_name"		"service_name": "$service_name"	The service name.
	ServiceInfo="$service_info"		"service_info": [$service_privilege_score, $service_privilege_level]	The service information, consisting of service privilege score and privilege level.
Data Smuggler	ProxiedDst=”foo.com”	msg=foo.com	“proxied_dst”: “foo.com”	The domain name or IP of the proxy.
Smash and Grab	ProxiedDst=”foo.com”	msg=foo.com	“proxied_dst”: “foo.com”	The domain name or IP of the proxy.

Account Lockdown Log Events

Account Lockdown Standard syslog message example

```
LOCKDOWN [lockdown@41261 category="$category" accountName="$account_name" action="$action"
success="$success" dvc="$headend_addr" user="$user" URL="$href" UTCTime="$UTCTime"]
```

Account Lockdown Standard syslog message detail

Key	Type	Description
$account_name	str	The name of the account.
$action	str	The action taken on the account (e.g., lock or unlock)
$category	str	The category of the event (e.g., LOCKDOWN)
$headend_addr	str	The IP of the Vectra Brain.
$user	int	The username of the person that performed the lockdown action.
$success	bool	Confirmation if the lockdown action was successful.
$href	str	A link to the account in the UI.
$UTCTime	int	Seconds since epoch for this event

Account Lockdown CEF syslog message example

```
CEF:0|Vectra Networks|X Series|$version|lockdown|Account Lockdown|3|externalId=$account_id
cat=$category dvc=$headend_addr suser=$user account=$account_name cs1Label=action
cs1=$action cs2Label=success cs2=$success cs4Label=Vectra Event URL cs4=$href
start=$UTCTimeStart end=$UTCTimeEnd
```

Account Lockdown CEF syslog message detail

Key	Type	Description
$account_id	int	The ID of the account.
$account_name	str	The name of the account.
$action	str	The action taken on the account (e.g., lock or unlock)
$category	str	The category of the event (e.g., LOCKDOWN)
$headend_addr	str	The IP of the Vectra Brain.
$user	int	The username of the person that performed the lockdown action.
$success	bool	Confirmation if the lockdown action was successful.
$href	str	A link to the account in the UI.

$UTCTimeStart	int	Seconds since epoch for event start.
$UTCTimeEnd	int	Seconds since epoch for event end.
$version	str	The version of Vectra platform running the Vectra Brain

Account Lockdown JSON syslog message example

```
{"category": "$category", "account_id": $account_id, "success": $success, "href": "$href",
"vectra_timestamp": "$UTCTime", "headend_addr": "$headend_addr", "user": "$user", "version":
"$version", "action": "$action", "account_uid": "$account_name"}
```

Account Lockdown JSON syslog message detail

Key	Type	Description
$account_id	int	The ID of the account.
$account_name	str	The name of the account.
$action	str	The action taken on the account (e.g., lock or unlock)
$category	str	The category of the event (e.g., LOCKDOWN)
$headend_addr	str	The IP of the Vectra Brain.
$user	int	The username of the person that performed the lockdown action.
$success	bool	Confirmation if the lockdown action was successful.
$href	str	A link to the account in the UI.
$UTCTime	int	Seconds since epoch for this event
$version	str	The version of Vectra platform running the Vectra Brain

Host Lockdown log events

Host Lockdown Standard syslog message example

```
LOCKDOWN [host_lockdown@41261 category="$category" hostName="$host_name" action="$action"
success="$success" willRetry="$retry" dvc="$headend_addr" user="$user" URL="$href"
UTCTime="$UTCTime"]
```

Host Lockdown Standard syslog message detail

Key	Type	Description
$action	str	The action taken on the account (e.g., lock or unlock)
$category	str	The category of the event (e.g., HOST_LOCKDOWN)

$headend_addr	str	The IP of the Vectra Brain.
$host_name	str	The name of the host.
$user	int	The username of the person that performed the lockdown action.
$success	bool	Confirmation if the lockdown action was successful.
$href	str	A link to the account in the UI.
$retry	bool	When a Lockdown action has failed, this indicates whether the system will retry the action.
$UTCTime	int	Seconds since epoch for this event

Host Lockdown CEF syslog message example

```
CEF:0|Vectra Networks|X Series|$version|host lockdown|Host Lockdown|3|externalId=$host_id
cat=$category dvc=$headend_addr suser=$user host=$host_name cs1Label=action cs1=$action
cs2Label=success cs2=$success cs3Label=willRetry cs3=$retry cs4Label=Vectra Event URL
cs4=$href start=$UTCTimeStart end=$UTCTimeEnd
```

Host Lockdown CEF syslog message detail

Key	Type	Description
$action	str	The action taken on the host (e.g., lock or unlock)
$category	str	The category of the event (e.g., HOST_LOCKDOWN)
$headend_addr	str	The IP of the Vectra Brain.
$host_id	int	The ID of the host.
$hostt_name	str	The name of the host.
$href	str	A link to the account in the UI.
$retry	bool	When a Lockdown action has failed, this indicates whether the system will retry the action.
$success	bool	Confirmation if the lockdown action was successful.
$user	int	The username of the person that performed the lockdown action.
$UTCTimeStart	int	Seconds since epoch for event start.
$UTCTimeEnd	int	Seconds since epoch for event end.
$version	str	The version of Vectra platform running the Vectra Brain

Host Lockdown JSON syslog message example

```
{"category": "$category ", "version": "$version ", "success": $success, "vectra_timestamp":
"$UTCTime", "will_retry": $retry, "href": "$href", "host_name": "$host_name", "action":
```

```
"$action", "host_id": $host_id, "headend_addr": "$headend_addr", "user": "$user"}
```

Host Lockdown JSON syslog message detail

Key	Type	Description
$action	str	The action taken on the host (e.g., lock or unlock)
$category	str	The category of the event (e.g., HOST_LOCKDOWN)
$headend_addr	str	The IP of the Vectra Brain.
$host_id	int	The ID of the host.
$host_name	str	The name of the host.
$href	str	A link to the account in the UI.
$user	int	The username of the person that performed the lockdown action.
$retry	bool	When a Lockdown action has failed, this indicates whether the system will retry the action.
$success	bool	Confirmation if the lockdown action was successful.
$UTCTime	int	Seconds since epoch for this event
$version	str	The version of Vectra platform running the Vectra Brain

Campaign log events

Campaign Standard syslog message example

```
CAMPAIGN [campaign@41261 id="$campaign_id" action="$action" reason="$reason" dvc="$headend_addr"
dvchost="$dvchost" detectionId="$det_id" hostname="$src_name" currentIP="$src_ip"
source_id="$src_hid" URL="$campaign_link" dstHost="$dest_name" DestinationIP="$dest_ip"
destID="$dest_id" timestamp="$timestamp"]
```

Campaign Standard syslog message detail

Key	Type	Description
$action	str	The action that caused the message to be logged (e.g., START, TRIAGED, TIMEOUT)
$campaign_id	int	The id of the campaign
$campaign_link	str	The link to the campaign in the UI
$dest_id	str	The destination of the campaign. Defaults to 'external'
$dest_ip	str	The destination IP address the campaign is targeting
$dest_name	str	The external domain of the campaign destination
$det_id	int	The ID of the detection that caused the campaign creation
$dvchost	str	The hostname of the Vectra Brain

$headend_addr	str	The IP of the Vectra Brain
$reason	str	The event name of the campaign
$src_hid	int	The original host ID of the member host in this campaign
$src_ip	str	The host IP of the source host
$src_name	str	The host name of the source host
$timestamp	int	Timestamp in seconds since epoch

Campaign CEF syslog message example

```
CEF:0|Vectra |X Series|$version|campaigns|$campaign_name|2| externalId=$campaign_id cat=CAMPAIGNS
act=$action dvc=$headend_addr dvchost=$dvchost shost=$src_name src=$src_ip suid=$src_hid
cs4Label=VectraEventURL cs4=$campaign_link dhost=$dest_name dst=$dest_ip  duid=$dest_id
rt=$timestamp reason=$reason cs6Label=VectraDetectionID cs6=$det_id
```

Campaign CEF syslog message detail

Key	Type	Description
$action	str	The action that caused the message to be logged (e.g., START, TRIAGED, TIMEOUT)
$campaign_id	int	The id of the campaign
$campaign_link	str	The link to the campaign in the UI
$campaign_name	str	The name of the campaign
$dest_id	str	The destination of the campaign. Defaults to 'external'
$dest_ip	str	The destination IP address the campaign is targeting
$dest_name	str	The external domain of the campaign destination
$det_id	int	The ID of the detection that caused the campaign creation
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$reason	str	The event name of the campaign
$src_hid	int	The original host ID of the member host in this campaign
$src_ip	str	The host IP of the source host
$src_name	str	The host name of the source host
$timestamp	int	Timestamp in seconds since epoch
$version	str	The version of Vectra platform running the Vectra Brain

Campaign JSON syslog message example

```
{"src_hid": $src_hid, "timestamp": $syslog_timestamp, "dvchost": "$dvchost", "campaign_id":
$campaign_id, "reason": "$reason", "src_name": "$src_name", "campaign_name": "$campaign_name",
"campaign_link": "$campaign_link", "headend_addr": "$headend_addr", "dest_name": "$dest_name",
"dest_id": "$dest_id", "vectra_timestamp": "$vectra_timestamp", "src_ip": "$src_ip", "version":
"$version", "action": "$action", "dest_ip": "$dest_ip", "det_id": $det_id}
```

Campaign JSON syslog message detail

Key	Type	Description
$action	str	The action that caused the message to be logged (e.g., START, TRIAGED, TIMEOUT)
$campaign_id	int	The id of the campaign
$campaign_link	str	The link to the campaign in the UI
$campaign_name	str	The name of the campaign
$dest_id	str	The destination of the campaign. Defaults to 'external'
$dest_ip	str	The destination IP address the campaign is targeting
$dest_name	str	The external domain of the campaign destination
$det_id	int	The ID of the detection that caused the campaign creation
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$reason	str	The event name of the campaign
$src_hid	int	The original host ID of the member host in this campaign
$src_ip	str	The host IP of the source host
$src_name	str	The host name of the source host
$syslog_timestamp	int	The epoch timestamp for when syslog received the message (e.g., 1550014653)
$vectra_timestamp	int	The epoch timestamp for when the event occurred (e.g., 1550014653)
$version	str	The version of Vectra platform running the Vectra Brain

Audit log events

Audit Standard syslog message example

```
AUDIT [dvc="$headend_addr" dvchost="$dvchost" version="$version" user="$user" role="$role"
```

```
source="$source_ip" type="user_action" outcome="$result" message="$message]
```

Audit Standard syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explaining the cause/nature of the log
$result	bool	True, False, or pending
$role	str	Role of the user who caused the log (e.g., admin, super admin, etc.)
$source_ip	str	IP address of the machine that initiated the user action
$user	str	Username of the user who caused the log
$version	str	The version of Vectra platform running the Vectra Brain

Audit CEF syslog message example

```
CEF:0|Vectra |X Series|$version|audit|user_action|0|dvc=$headend_addr dvchost=$dvchost
suser=$user spriv=$role src=$source_ip deviceFacility=13 cat=user_action outcome=$result
msg=$message
```

Audit CEF syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explaining the cause/nature of the log
$result	bool	True, False, or pending
$role	str	Role of the user who caused the log (e.g., admin, super admin, etc.)
$source_ip	str	IP address of the machine that initiated the user action
$user	str	Username of the user who caused the log
$version	str	The version of Vectra platform running the Vectra Brain

Audit JSON syslog message example

```
{"source_ip": "$source_ip", "dvchost": "$dvchost", "version": "$version", "role": "$role",
"user": "$user", "message": "$message", "vectra_timestamp": "$vectra_timestamp", "headend_addr":
"$headend_addr", "result": $result}
```

Audit JSON syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explaining the cause/nature of the log
$result	bool	True, False, or pending
$role	str	Role of the user who caused the log (e.g., admin, super admin, etc.)
$source_ip	str	IP address of the machine that initiated the user action
$user	str	Username of the user who caused the log
$vectra_timestamp	int	The epoch timestamp for when the event occurred (e.g., 1550014653)
$version	str	The version of Vectra platform running the Vectra Brain

Health log events

Health Standard syslog message example

```
HEALTH [dvc="$headend_addr" dvchost="$dvchost" version="$version" type="$type" outcome="$result"
message="$message"]
```

Health Standard syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explains the cause/nature of the log
$result	str	A string indicating either a success or failure
$type	str	A string to indicate what type of health message this is. Valid types include sensor_connectivity, disk_hardware_raid_check, system_cpuflags_valid, disk_ro_mount_check, capture_interface_flap_status, capture_interface_bandwidth_status, colossus_packet_drop_rate, heartbeat_check, and stream_health
$version	str	The version of Vectra platform running the Vectra Brain

Health CEF syslog message example

```
CEF:0|Vectra |X Series|$version|health|$type|0|dvc=$headend_addr dvchost=$dvchost
deviceFacility=14 outcome=$result msg=$message
```

Health CEF syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explains the cause/nature of the log
$result	str	A string indicating either a success or failure
$type	str	A string to indicate what type of health message this is. Valid types include sensor_connectivity, disk_hardware_raid_check, system_cpuflags_valid, disk_ro_mount_check, capture_interface_flap_status, capture_interface_bandwidth_status, colossus_packet_drop_rate, heartbeat_check, and stream_health
$version	str	The version of Vectra platform running the Vectra Brain

Health JSON syslog

```
{"vectra_timestamp": "$vectra_timestamp", "version": "$version", "result": "$result", "type":
"$type", "source_ip": "$source_ip", "message": "$message", "dvchost": "$dvchost", "headend_addr":
"$headend_addr"}
```

Health JSON syslog message detail

Key	Type	Description
$dvchost	str	The hostname of the Vectra Brain
$headend_addr	str	The IP of the Vectra Brain
$message	str	A message explains the cause/nature of the log
$result	str	A string indicating either a success or failure
$source_ip	str	IP address of the machine that initiated the action
$type	str	A string to indicate what type of health message this is. Valid types include sensor_connectivity, disk_hardware_raid_check, system_cpuflags_valid, disk_ro_mount_check, capture_interface_flap_status,

		capture_interface_bandwidth_status, colossus_packet_drop_rate, heartbeat_check, and stream_health
$vectra_timestamp	int	The epoch timestamp for when the event occurred (e.g., 1550014653)
$version	str	The version of Vectra platform running the Vectra Brain

For more information

If you have questions or need additional assistance, please contact Vectra support at:

Vectra
support@vectra.ai
+1 (408) 326-2022

Vectra, GmbH
support@vectra.ai
+41 (44) 551 0143

About Vectra

Vectra uses artificial intelligence to automate real-time cyberattack detection and response – from network users and IoT devices to data centers and the cloud. All internal traffic is continuously monitored to detect hidden attacks in progress. Detected threats are instantly correlated with host devices that are under attack and unique context shows where attackers are and what they are doing. Threats that pose the biggest risk to an organization are automatically scored and prioritized based on their severity and certainty, which, enables security operations teams to quickly focus their time and resources on preventing and mitigating loss. https://vectra.ai