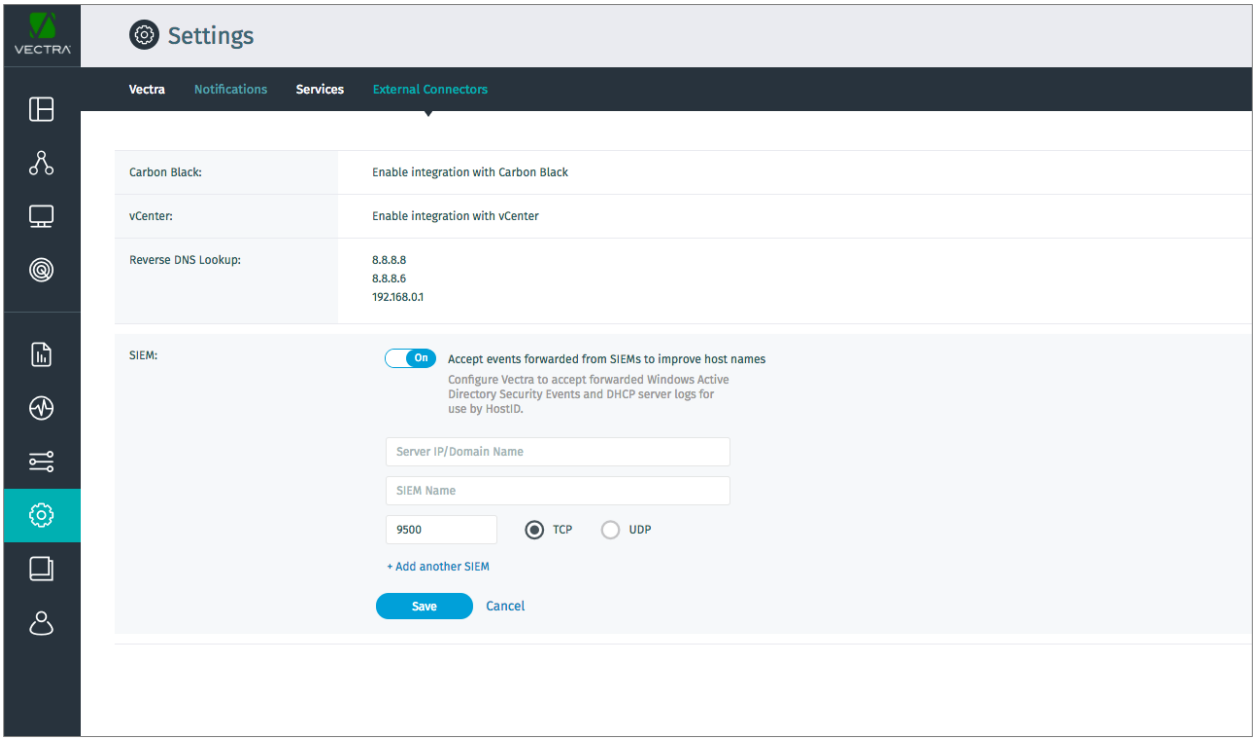
Event forwarding reference guide

Overview

Administrators can configure the Vectra® Networks X-series platform to accept forwarded events from SIEM or central log manager (CLM) sources to improve HostID performance.

One or more sources can be configured on the X-series, and both TCP and UDP transports are supported. Events received by unconfigured event sources will be dropped. An optional SIEM Name can be configured for use when HostID artifacts are displayed. If SIEM Name is not provided the configured IP/Domain Name of the SIEM will be displayed.



SIEM event forwarder configuration

Supported events

The Vectra-X supports the forwarding of DHCP and Kerberos events for HostID.

DHCP

DHCP events are supported in Infoblox and other ISC (Internet Systems Consortium) standard syslog format. Windows DHCP logs are currently unsupported.

Examples of supported DHCP formats:

18-Aug-2015 10:40:16.194 ###DHCPSERVER### ###PROCESS###: DHCPRELEASE of ###IP### from ###MAC### (###HOSTNAME###) via ###RELAY### (found)
18-Aug-2015 10:14:16.194 ###DHCPSERVER### ###PROCESS###: DHCPACK on ###IP### to ###MAC### (###HOSTNAME###) via ###RELAY### relay ###IP2### lease-duration 2000 (RENEW) uid ###UID###
18-Aug-2015 10:16:16.194 ###DHCPSERVER### ###PROCESS###: DHCPACK on ###IP### to ###MAC### via ###RELAY###
18-Aug-2015 10:17:16.194 ###DHCPSERVER### ###PROCESS###: DHCPACK to ###IP### (###MAC###) via ###RELAY###
18-Aug-2015 10:18:16.194 ###DHCPSERVER### ###PROCESS###: DHCPACK on ###IP### to ###MAC### (###HOSTNAME###) via ###RELAY###
18-Aug-2015 10:19:16.194 ###DHCPSERVER### ###PROCESS###: DHCPINFORM from ###IP### via ###RELAY###
18-Aug-2015 10:22:16.194 ###DHCPSERVER### ###PROCESS###: DHCPREQUEST for ###IP### from ###MAC### (###HOSTNAME###) via ###RELAY### uid ###UID### (RENEW)
18-Aug-2015 10:27:16.194 ###DHCPSERVER### ###PROCESS###: DHCPREQUEST for ###IP### from ###MAC### via ###RELAY###
18-Aug-2015 10:28:16.194 ###DHCPSERVER### ###PROCESS###: DHCPDISCOVER from ###MAC### (###HOSTNAME###) via ###RELAY###
18-Aug-2015 10:29:16.194 ###DHCPSERVER### ###PROCESS###: DHCPDISCOVER from ###MAC### via ###RELAY###

Kerberos

Kerberos events are supported in ISC (Internet Systems Consortium) standard syslog format. Vectra has validated forwarded Kerberos events from Splunk and IBM QRadar platforms.

Examples of supported Kerberos formats:

May 15 03:11:51 ###DOMAINCONTROLLER IP### May 6 21:04:00 ###HOSTNAME### microsoft-windows-security-auditing[success] 4768 A Kerberos authentication ticket (TGT) was requested. Account Information: Account Name:

###ACCOUNTNAME### Supplied Realm Name: ###REALM### User ID: ###UID### Service Information: Service Name: ###SVCNAME### Service ID: ###SID### Network Information: Client Address: ###CLIENT IP ADDR### Client Port: ###CLIENT PORT### Additional Information: Ticket Options:0x40810010 Result Code:0x0 Ticket Encryption Type:0x12 Pre-Authentication Type:2 Certificate Information: Certificate Issuer Name: Certificate Serial Number: Certificate Thumbprint: Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

<13>Jun 07 13:01:46 10.48.1.50 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=1.0.14 Source=Microsoft-Windows-Security-Auditing Computer=###HOSTNAME### User= Domain= EventID=4768 EventIDCode=4768 EventType=8 EventCategory=14339 RecordNumber=2093536389 TimeGenerated=1496854905 TimeWritten=1496854905 Message=A Kerberos authentication ticket (TGT) was requested. Account Information: Account Name: ###ACCOUNTNAME### Supplied Realm Name: ###REALM### User ID: ###UID### Service Information: Service Name: ###SVCNAME### Service ID: ###SID### Network Information: Client Address: ###CLIENT IP ADDR### Client Port: ###CLIENT PORT### Additional Information: Ticket Options: 0x40810010 Result Code: 0x0 Ticket Encryption Type: 0x12 Pre-Authentication Type: 2 Certificate Information: Certificate Issuer Name: Certificate Serial Number: Certificate Thumbprint: Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types

SIEM forwarding configuration
Configuration of event forwarding will be specific to each SIEM vendor. Vectra has validated event forwarding by Splunk and IBM QRadar.

Configuring Splunk event forwarding
See 'Forward syslog data to a third-party host' section:
http://docs.splunk.com/Documentation/SplunkCloud/6.6.0/Forwarding/Forwarddatatothird-partysystemsd

Configuring IBM QRadar event forwarding
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_frwd_event_data.html

For more information

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

Vectra Networks
support@vectranetworks.com
+1 (408) 326-2022

Vectra Networks GmbH
support@vectranetworks.com
+41 (44) 508-3049

About Vectra Networks
Vectra Networks is the leader in automating the hunt for in-progress cyber attacks. Using artificial intelligence, Vectra correlates threats against hosts that are under attack and provides unique context about what attackers are doing so organizations can quickly prevent or mitigate loss. Vectra prioritizes attacks that pose the greatest business risk, enabling organizations to make rapid decisions on where to focus time and resources. www.vectranetworks.com.