SIEM TECHNOLOGY

INFOSHEET

This Infosheet describes SIEM technology; explains how Absolute integrates with and complements a SIEM solution; and provides information on the data sent to SIEM by Absolute.

SIEM TECHNOLOGY

Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM) technologies:

- SIM technologies enable the consolidation of logs, analysis of data, and reporting of findings for policy and standards compliance
- SEM technologies involve real-time monitoring, correlation of events, notifications, console views, and the management of threats, events and security incidents

Today's SIEM solutions gather, analyze and present a holistic view of information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; external threat data; and information from endpoint security applications such as Absolute.

ABSOLUTE AND SIEM SOLUTIONS

Absolute is a key part of your defense-in-depth security strategy that relies on multiple technologies to protect against a range of potential threats. Alert data generated by Absolute and other security solutions can be fed into your SIEM solution and analyzed in context, offering a holistic view of the entire security posture of your organization.

When Absolute is integrated with a SIEM solution such as RSA Security Analytics, Splunk®, McAfee® Enterprise Security Manager, IBM®, and IBM Security QRadar®, alerts created in Absolute will be sent to the SIEM system. This data is sent in a standard 'Syslog' format that all major SIEM products can interpret. This process ensures that alert data generated by Absolute is compatible with all major SIEM systems.

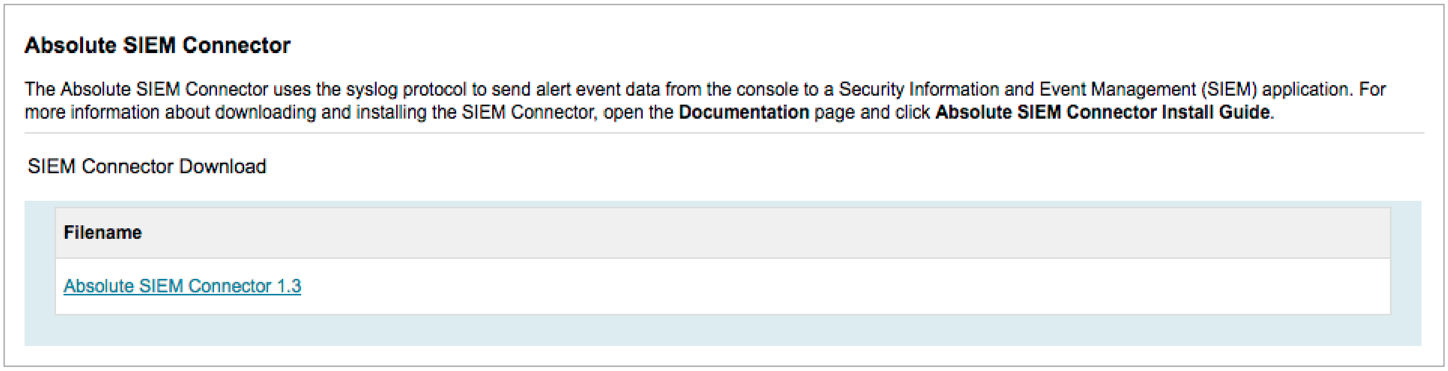
Examples of alerts include:

- Notifications that other security solutions have been damaged or disabled (anti-malware, encryption, SCCM)
- Notifications of changes to a device (e.g. username change, OS change, hardware change)
- Notifications of blacklisted software installations
- Notifications that required software has been removed
- Any custom alert created by an Absolute customer

INTEGRATING ABSOLUTE WITH YOUR SIEM SOLUTION

Customers that use a SIEM application can download the Absolute SIEM connector to export alerts generated in Absolute to their SIEM solution for incident management. The SIEM Connector uses the syslog protocol to send these alert events.

The integration is created by installing the Absolute SIEM Connector on a computer within your network. The Absolute SIEM Connector configures a Windows service that sends SOAP requests to the Absolute Gateway Server to retrieve alert event data from the Customer Center database. The alert events are then transmitted in syslog messages to your SIEM's Syslog server to allow SIEM users to view, analyze, and report on these events, along with other events within your system.



Absolute SIEM Connector

The Absolute SIEM Connector uses the syslog protocol to send alert event data from the console to a Security Information and Event Management (SIEM) application. For more information about downloading and installing the SIEM Connector, open the **Documentation** page and click **Absolute SIEM Connector Install Guide**.

SIEM Connector Download

Filename
Absolute SIEM Connector 1.3

Detailed instructions for downloading, installing, and managing the Absolute SIEM Connector are available in the **Absolute SIEM Connector Install Guide** on the Documentation page in the Absolute console. This connector is a great way to integrate Absolute into the overall security stack, rather than to try to position Absolute as another 'separate' layer and console.

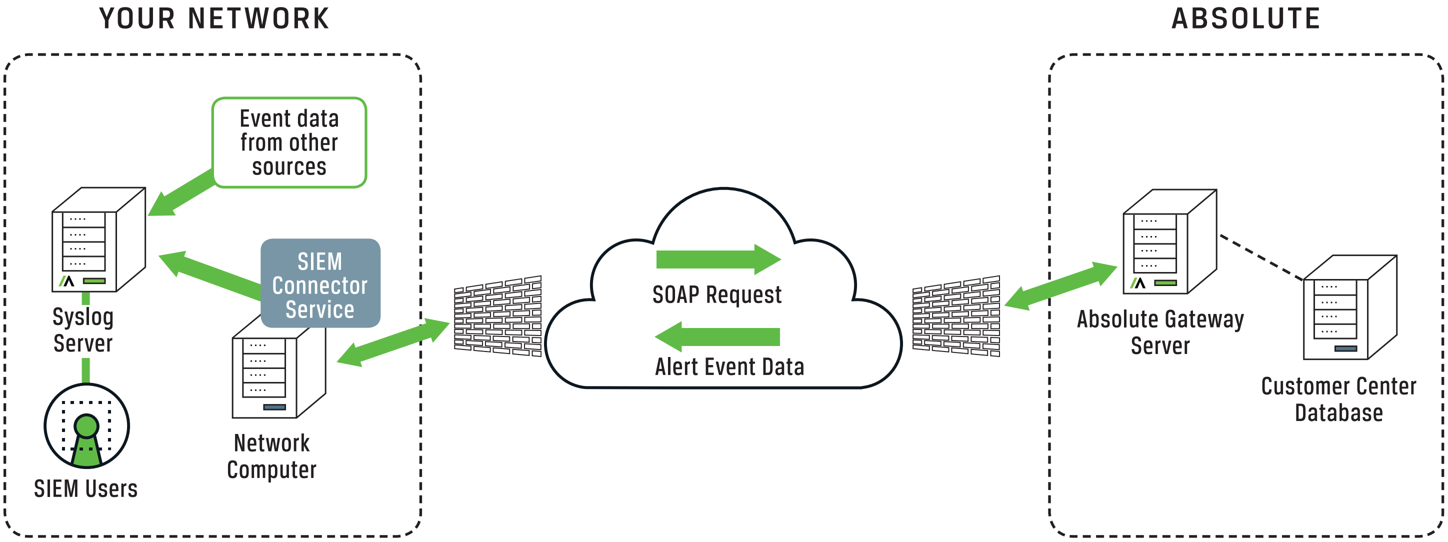


Figure 1: SIEM integration using Absolute SIEM Connector

DATA SENT TO SIEM BY ABSOLUTE

After you install the SIEM Connector, it retrieves all Absolute console alert events logged within the past 24 hours and sends them to the Syslog server.

Going forward, the SIEM Connector retrieves new alert events at the interval set in the SIEM Connector. You can set the interval to any value between two minutes and 24 hours – the default value is 60 minutes.

The following alert event data is retrieved from the Absolute console:

- Information about the device that triggered the alert event, including:
  - Identifier
  - Device name
  - Serial number
- Alert name
- Date and time when the alert event was triggered

SYSTEM REQUIREMENTS FOR SIEM CONNECTOR

The Absolute SIEM Connector can be installed on a computer running any of the following Windows (64- or 32-bit) operating systems:

- Windows Server 2012
- Windows Server 2008
- Windows 8 or 8.1
- Windows 7

These prerequisites must also be met:

- .NET Framework 4.0 is required
- Alerts must be activated in the Absolute console
- The Syslog server and the computer on which you intend to install Absolute SIEM Connector must reside within the same network
- An Internet connection is required