FALCON SIEM CONNECTOR

Leverage Falcon Host data in any SIEM

Simplify and automate consumption of Falcon Host data into your SIEM

Organizations need to collect and archive log data for purposes ranging from regulatory compliance, to log management, to the aggregation of events from multiple security products. SIEMs (Security Information and Event Management) have become the tool of choice to gather these type of data. But the disparity of log formats and number of connectivity methods between a SIEM and its data sources can make data collection arduous and lengthy for SIEM users.

OPTIMIZED SECURITY EVENT GATHERING ON THE ENDPOINT

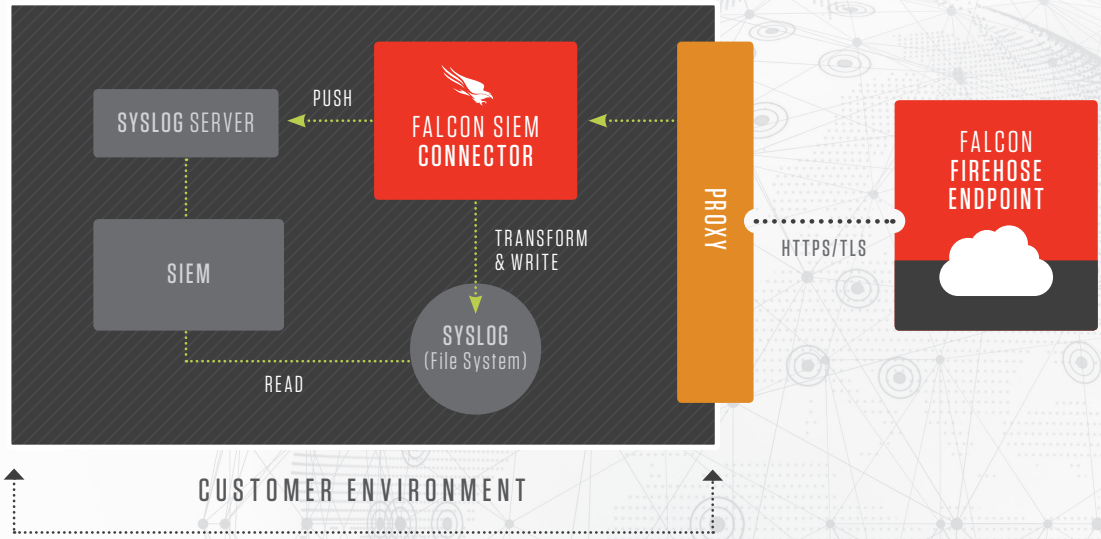
Using Falcon Host in conjunction with the Falcon SIEM Connector offers a fast, simple and reliable way to optimize the collection of relevant security events across hundreds of thousands endpoints. The lightweight Falcon Host Sensor will perform the otherwise hard work of collecting the data from distributed endpoints with no additional infrastructure deployment. Falcon Host Sensors will send that data from your environment into the Cloud. Then, the Falcon SIEM Connector will seamlessly pull that data from the Cloud to your SIEM.

SIMPLE AND AUTOMATED DATA CONSUMPTION

The Falcon SIEM Connector streamlines and automates the process of gathering Falcon Host data into SIEMs. Instead of having to write custom connectors, customers can now simply deploy and configure the Falcon SIEM Connector to securely retrieve their Falcon Host data from the Cloud and add them into their SIEM.

The Falcon SIEM Connector automatically connects to the CrowdStrike Cloud and normalizes the data in formats that are immediately usable by SIEMs: JSON, Syslog, CEF (common event format) or LEEF (log event extended format).

FALCON SIEM CONNECTOR DIAGRAM



CUSTOM IMPLEMENTATION

For customers who still want to write their own custom connectors, the Falcon Firehose API is available.

REQUIREMENTS

The Falcon SIEM Connector is deployed on premise on a system with running either CentOS or RHEL 6.x-7.x Internet connectivity to the CrowdStrike Cloud is also required.

CROWDSTRIKE

CONTACT US TO LEARN MORE ABOUT
FALCON HOST and FALCON SIEM CONNECTOR
1.888.512.8906 | sales@crowdstrike.com

The Falcon SIEM Connector gives you the flexibility to choose how to insert the data in your SIEM. For customers who are already using, or who intend to use a syslog server to collect data, the Falcon SIEM Connector sends the data to a syslog server. For customers who need to store data locally, the Falcon SIEM Connector can write the data to a syslog file on disk.

SECURE DATA TRANSFER

Falcon SIEM Connector automatically establishes a secure TLS (Transport Layer Security) connection with the CrowdStrike Cloud to preserve the confidentiality of the data.

Making sure that all of the expected data is received is crucial to guarantee the accuracy of the SIEM's information. To ensure no data is lost, the Falcon SIEM Connector continuously monitors the connection with the Cloud, automatically reestablishing the connection and picking up the data stream where it left off in case it is disconnected.

Ver: 04-24-16