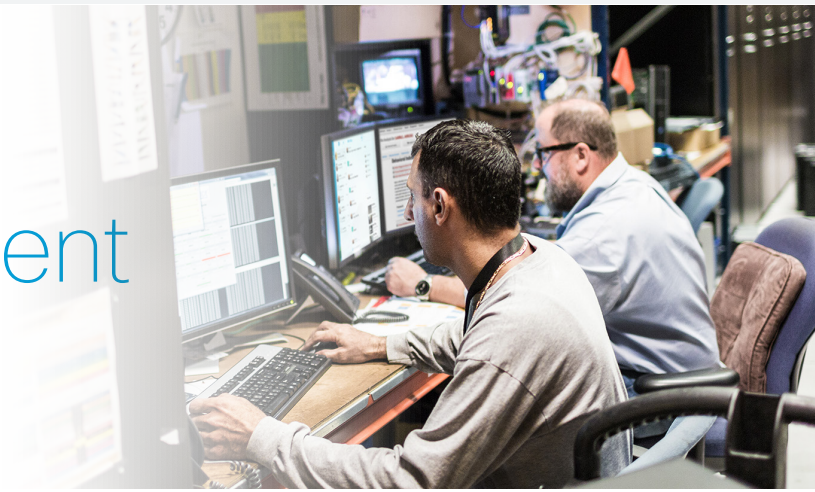
Cisco Stealthwatch Security Information Event Management Integration Service



Benefits

- Gain deep network visibility into your network by displaying suspicious IP address activity, such as what the most often visited destination (peer) was by IP address.
- Identify used protocols, quantify the amount of data transmitted, and determine the time of communication to help detect threatening, anomalous network behavior.
- Create top summary reports such as top peers (IP destinations), top conversations, and top services so you can quickly summarize large sets of data and receive it in an intuitive, consumable format.
- Streamline integration with security information event management (SIEM), including Splunk, QRadar, ArcSight, LogRhythm, AlienVault and many others, so you can reduce the time to implement from weeks to days, and save valuable resources.

SIEM integration augments traditional sources of SIEM data with flow-based information so you can see deeper into the network. The result is a reduction in cost and complexity of incident resolution and improvement of overall security measures through greater visibility. By integrating a SIEM with Stealthwatch, you can support compliance initiatives, enhance network forensics for incident investigation, and significantly improve network and application availability and performance.

Cisco® Stealthwatch Security Information Event Management (SIEM) Integration Service provides additional context around potential threats by combining alarm notification with flow data, so that customers can classify a threat and take appropriate action. By aggregating alarm notification with Cisco Stealthwatch flow data, the SIEM Integration Service can enable a quick, complete description of network traffic related to a suspicious IP address.

This service also supports the acceptance of alarm notifications from any security system – intrusion prevention systems (IPS), packet capture (PCAP), and SIEM will automatically query Stealthwatch by integrating with standard representational state transfer (REST) APIs. As a result, customers gain data necessary to investigate the host and take mitigation actions against the suspicious host. This data can be displayed on the Stealthwatch console or transmitted to another system, as determined by security protocol.

Gain Full Context and Visibility into Your SIEM Appliance with Stealthwatch

The service includes:

Visibility into anomalous IP activity on your network within your SIEM console is a critical aspect of your threat detection capabilities. Integrating any SIEM solution into your instance of Stealthwatch allows your security team to investigate alarms from your IDS, IPS, or other solution in your security stack by simply clicking on a button to open a Stealthwatch window. Once you do, an investigation begins. From the Stealthwatch window, your security team can pull back critical information detailing:

- Who caused the alarm to fire
- How much data was transmitted
- When the alarm occurred
- What applications were involved in the active alarm

The information is delivered with a rich set of data elements that the Cisco Professional Services team creates. They can configure the logic to fetch these key reports:

- Top hosts
- Top peers
- Top conversations

When you take advantage of this service, our professional services team provides you exclusive access to this critical data, which reduces your mean time to know (MTTK) in fighting advanced threats.

Next Steps

To learn more about Cisco Security Services and how our Stealthwatch deployment services can benefit your business, contact your local account representative or authorized Cisco reseller. For more information on how Cisco can help you protect your organization from today's dynamic threats, visit http://www.cisco.com/go/services/security.

C45-736856-02 04/17