How Cisco Uses Splunk on Cisco UCS for IT Operations

Faster incident resolution and fewer system problems with big data and analytics solutions for IT operations

EXECUTIVE SUMMARY

CHALLENGE

- Replace systems used for monitoring security incidents and IT operations
- Gain new monitoring capabilities and improved correlation of security events
- Reduce time for detecting and resolving operational problems

SOLUTION

- A global deployment of Splunk Enterprise on Cisco UCS servers to collect and correlate event and log data
- Internally-developed EventPro application for operations monitoring

RESULTS

Security

- 33% reduction in the time required to conduct security investigations
- Centralized data and automated tasks help security analysts work more effectively

IT Operations

- 80% reduction in operations costs
- 50% reduction in high-priority system issues due to faster problem analysis and resolution
- 25% improvement in system stability and availability

LESSONS LEARNED

- Design the data collection system deployment to support continuous operation
- Prepare to expand indexing capacity to support higher data volumes and more users
- Determine appropriate data retention schedules

NEXT STEPS

- Implement a resilient design for selected EventPro applications
- Expand data collection and storage capacity as needed

Challenge

Monitoring security incidents and routine operations for our network and computing infrastructure are two vital, everyday responsibilities for Cisco IT. By 2015, it was clear that we needed to replace the monitoring systems we had been using for these functions.

For security monitoring, we used an externally-developed security information and event management (SIEM) system, which had significant limitations for data capture and access. For routine operations, the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) we had been using was no longer sold by Cisco.

We wanted capabilities in a new monitoring solution that would help:

- Create a framework for self-servicing and self-healing capabilities.
- Reduce mean time to problem detection (MTTD) and mean time to resolution (MTTR) for problems.
- Offer capabilities to monitor, manage, protect, and proactively avoid security incidents with a central source for correlating security event data and automating alerts.
- Provide enhanced tools for routine analysis of system and application logs for Cisco UCS deployments.
- Support a service that offers system management data and analysis capabilities to users of the Cisco IT Elastic Infrastructure Services (CITEIS) internal cloud.

The new monitoring solution would particularly need to address the challenges for two primary use cases: Monitoring and managing security incidents and supporting routine analysis of Cisco UCS and other system logs (syslogs).

Security Incident Monitoring and Management

Syslog data is integral to all investigations conducted by the Cisco Computer Security Incident Response Team (CSIRT). However, the team's activity was hampered because there was no central source for security event data and the previous event management system could not keep up with the team's information needs. For example, the system was very difficult to use for indexing non-security data such as logs from custom applications. Search speed wasn't adequate and the system's prebuilt rules generated too many false positives.

CSIRT needed a single analytics platform for real-time monitoring of the network and IT systems, as well as capabilities for automated correlation of events and alerts.

PRODUCT LIST
Servers – Unified Computing
• Cisco UCS C-Series servers
Security
• Cisco Web Security Appliance

Centralized Visibility Across Applications and Infrastructure

Multiple operations teams in Cisco IT were frustrated by the limited ability to quickly detect and find the root cause of problems. These limitations were reflected in the number of recurring incidents, which ranged from 15 percent to 45 percent over a one-year period.

The teams also had difficulty identifying the business impact of an incident because of the complex footprint for most applications, which involve multiple servers, databases, interfaces, and integrations. The teams needed better capabilities for preventative alerting and monitoring, correlating events, identifying system dependencies, and managing the impact of change requests.

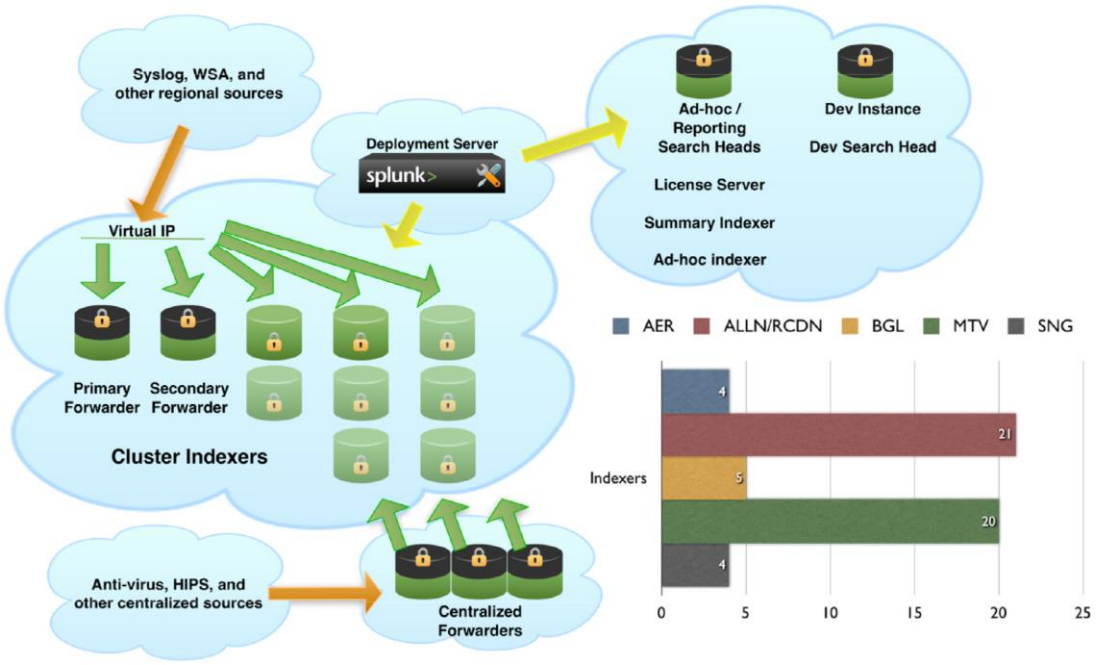
Solution

To collect and correlate event data for security monitoring, CSIRT now uses the Splunk Enterprise solution. For operations monitoring, Cisco IT developed a new system management solution, called EventPro, that combines commercial and internally developed software to deliver monitoring, self-servicing, and self-healing capabilities for the Cisco UCS infrastructure. This solution also uses the Splunk Enterprise software to correlate events and manage and analyze system logs.

The EventPro and Splunk software are installed as virtual machines (VMs) on Cisco UCS C-Series servers. Figure 1 shows how the collected data is indexed and made available for ad hoc queries and defined reports.

The Splunk infrastructure encompasses five VM pools that serve as search heads, primarily located in a single data center. Also in the infrastructure are 20 individual VMs that serve as Splunk indexers, configured in a load-balanced and failover cluster design across two Cisco data centers.

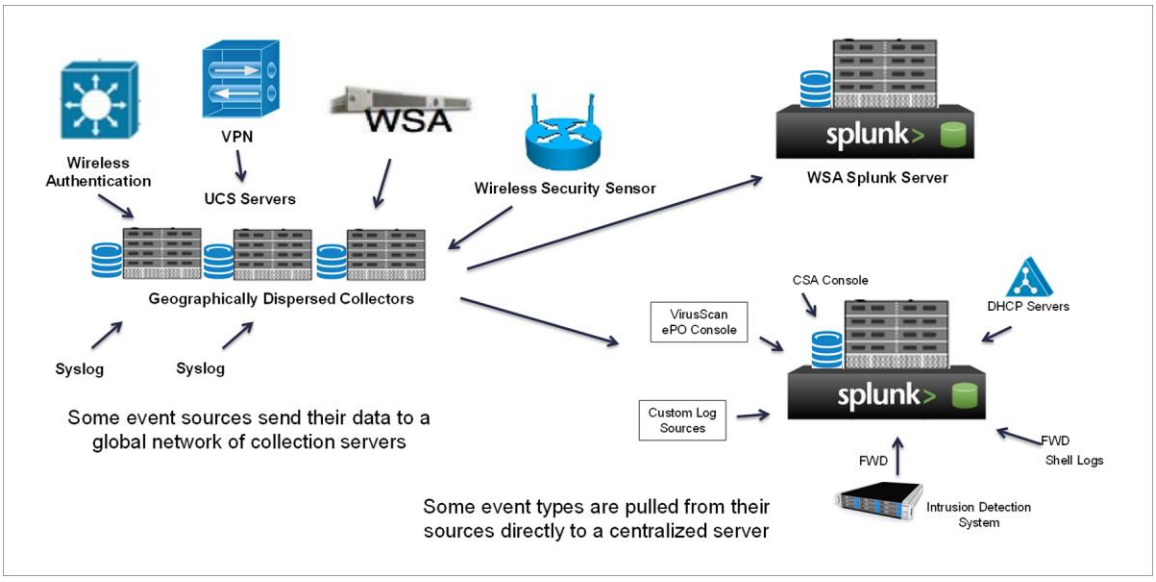
Figure 1. Splunk Deployment for Data Logging



For security monitoring, our Splunk deployment includes 25 Cisco Web Security Appliances (Cisco WSA) that are configured in seven clusters around the world. The clusters are in a high-availability, load-balanced, and scalable deployment that monitors more than 70 applications, indexes approximately 900 GB of data each day, and connects with 350 TB of stored data.

Figure 2 shows how the Splunk infrastructure collects log data from multiple security systems.

Figure 2. Security Data Collection for Processing by Splunk



Splunk Deployment for Security Incident Monitoring

The Splunk Enterprise product analyzes and correlates system log events to provide real-time alerts for sensitive investigations and advanced persistent threat (APT) incidents. It easily indexes any type of machine data from any source, helping CSIRT protect our IT infrastructure and business information with better capabilities for incident response, forensics, and threat detection.

CSIRT conducts investigations through flexible queries and correlations of data from the numerous sources that send security events and logs to Splunk. Nearly all incidents reviewed by CSIRT analysts and investigators make use of log analysis tools. Additionally, almost 500 regularly scheduled reports mine the log messages to extract relevant security data.

EventPro Solution for System Visibility Across Applications and Infrastructure

Cisco IT uses Splunk to index a broad range of system logs for networking devices, operating systems, unified communications and video systems, and applications. Based on the indexing, Splunk correlates events and generates two types of alerts: exceptions and warnings. These alerts are routed to the appropriate teams by email and also appear on the EventPro dashboard for immediate analysis, research, and action. EventPro presents both virtual and physical stacks in a single dashboard view.

We also use Splunk Enterprise specifically to monitor Cisco UCS server deployments. Splunk gives us a unified way to organize the large volume of log messages generated within a Cisco UCS domain, covering servers, hypervisors, operating systems, applications, storage resources, and other infrastructure components. That data can be presented to the security and operations teams as well as CITEIS users via saved searches, the user's preferred management application, or real-time alerts on the EventPro dashboard.

"Previously, the different IT operations teams had their own management tools and data could come from multiple logs, even for a single application. Sometimes the log data would expire before you could find the source of a problem," says Piyush Bhargava, Cisco IT distinguished engineer. "Now, Splunk pulls data from all the logs and the EventPro dashboard gives our operations teams a single place to look and work together to solve problems."

With faster and improved visibility into log data, Cisco IT operations teams are able to:

- Implement self-servicing and self-healing capabilities that increase availability of IT services
- Centrally monitor, alert, report, and analyze metrics, logs, and events in real time across all physical, virtual, and cloud resources to reduce MTTD for active or potential problems
- Correlate and connect events across every level and technology including Cisco UCS
- Proactively predict and detect performance problems and prevent them from affecting users
- Determine root causes of outages and performance problems to reduce MTTR
- Facilitate real-time reporting when changes are made to mission-critical systems
- Provide transparency for system issues across all IT teams

Cisco IT offers implementation and ongoing support for the EventPro solution as a service to users of the CITEIS internal cloud. This service includes data gathering and modeling as well as standard dashboard access. Options for data visualization, optimizing searches and solution performance, configuring alerts, and integrating with other data platforms are also available to CITEIS users. Internal budget charges are made for a one-time implementation fee and a quarterly support fee to cover EventPro infrastructure and licensing costs, software and user support services, and data storage.

> "Splunk pulls data from all the logs and the EventPro dashboard gives our operations teams a single place to look and work together to solve problems."
> — Piyush Bhargava, Cisco IT distinguished engineer

Results

Splunk and the EventPro monitoring dashboard give us improvements for security and operations visibility, intelligence, and efficiency. In turn, these improvements have produced significant results for Cisco.

Results for security incident monitoring from incorporating Splunk data include:

- Cost savings compared to the expense of a traditional SIEM
- 33 percent reduction in the time required to conduct security investigations because most data searches take less than a minute, even in huge log files
- All security data is readily available in a single, centralized portal for faster and simpler access
- Substantially easier correlation allows for more thorough investigations
- Ability to automate routine tasks and search log data allows CSIRT analysts to work more effectively

For the systems monitored with the EventPro dashboard, results include:

- 50 percent reduction in high-priority system problems and improved ability to avoid critical incidents because operational intelligence can be obtained in minutes instead of hours
- 80 percent reduction in operations costs
- 90 percent improvement in times for root cause analysis and problem resolution
- 25 percent improvement in system stability and availability
- 10 percent improvement in overall system performance

Lessons Learned

From our experience in deploying the Splunk Enterprise product and the EventPro dashboard, we offer the following lessons:

- Implement a "round robin" backup among the data collection systems within each server cluster to mitigate the potential for data loss.
- Design load balancing to allow one or more systems within the cluster to be unavailable without interrupting data collection.
- Add more virtual machines or Cisco UCS servers as needed to expand indexing capacity based on growth of log data volumes or adding more applications for monitoring.
- Lengthen retention schedules by adding Cisco UCS servers and storage or by rolling data to an archive. For security monitoring, CSIRT retains data for 1-3 years depending on the data source and forensics needs. For routine operations, Cisco IT typically retains syslog data for 90 days, but certain data may be kept for as long as one year.

Next Steps

Cisco IT will implement a resilient design for selected EventPro applications across two data centers and monitor the deployment's capacity for any needed sizing adjustments.

For More Information

Products: Cisco UCS servers and Cisco Web Security Appliance

Solutions: Splunk on UCS

Case Study: Cisco IT Elastic Infrastructure

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT http://www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**