Security Analytics on Cisco UCS with Splunk: Improve Threat Detection and Accelerate Response

What You Will Learn

The task of maintaining infrastructure and data security has never been more challenging. Today's networks extend farther than ever before and constantly evolve to spawn new attack vectors. By 2020, 50 billion connected, data-producing devices will dramatically increase an enterprise's potential attack surface.

The stakes have never been higher. The number of security breaches is dramatically increasing.[1] In 2014, the number of detected incidents rose to 42.8 million, almost a 50 percent increase from 2013. And those incidents also generated a greater financial toll, with a 51 percent increase in the number of companies reporting a loss of US$10 million or more.[2]

Mitigation of security risk in today's advanced threat environment is a race against time. Staying ahead of external attacks, malicious insiders, and costly fraud demands a security analytics solution that's designed for advanced threat environments.

Security Analytics on the Cisco Unified Computing System™ (Cisco UCS®) with Splunk will help put time back on your side. The combination of continuous and comprehensive visibility across security- and nonsecurity-related data and an infrastructure optimized for big data and analytics will help your organization quickly detect and respond to known, unknown, and advanced threats and significantly reduce your security risk.

Unprecedented Security Risk Creates Unprecedented Business Risk

Security is a priority for every enterprise, and it has never been more challenging. Today's networks extend beyond traditional walls and include data centers, endpoints, virtual environments, branch offices, and the cloud. They constantly evolve and spawn new attack vectors, including mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and an increasing number of smart devices.

With 50 billion connected devices by 2020, the security challenge will become even greater. New connections will generate data, simultaneously creating the opportunity for economic gain and increasing an enterprise's potential attack surface. The chief information security officer (CISO) will need to protect a dynamic perimeter that is creating a nearly-infinite number of points of vulnerability.

As enterprises adapt to this changing security environment, they face formidable obstacles. Hacking has become industrialized. Attacks are often profit-based, sophisticated efforts using tools developed specifically to circumvent their target's security infrastructure.

Security breaches also originate from within: accidental or malicious breaches caused by employees and physical losses also contribute to the growing problem. The combination of external and internal attacks has resulted in a

[1] "Cybersecurity 2014 Breaches and Costs Rise, Confidence and Budgets Are Low," CSO Magazine, November 5, 2014
[2] Verizon 2014 Data Break Investigations Report

dramatic increase in the number and financial impact of security breaches, with a 51 percent increase in the number of companies reporting a loss of US$10 million or more in 2014 compared to the previous year.

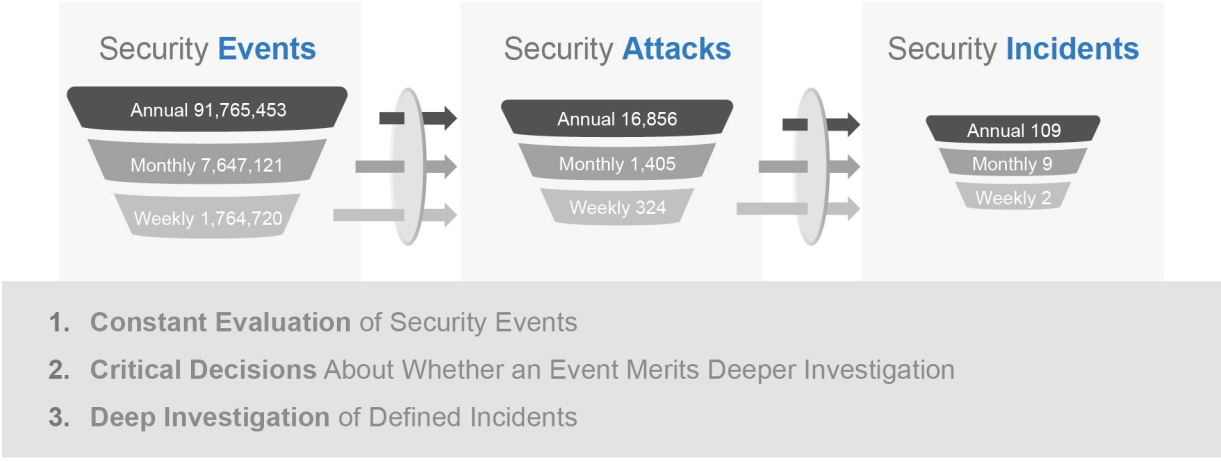
A Race Against Time

Advanced threats that enter and persist within an environment are among the biggest security challenges. Analysts need to be able to trace the different stages of an advanced threat and link the sequence of events together by finding relationships—using any field, across any data, over any time frame. To stay ahead of external attacks, malicious insiders, and costly fraud, organizations require continuous security and compliance monitoring, fast incident response, and the capability to detect and respond to known, unknown, and advanced threats.

Enterprises are in a race against time. Seventy-five percent of all attacks begin data exfiltration in just minutes, but take much longer to detect. More than 50 percent of attacks persist without detection for months or years before discovery.[3] The longer a threat evades detection, the greater the potential financial losses. Yet in an environment in which seconds count, enterprises face considerable challenges in securing their infrastructure and data.

Security analysts work in an environment of constant triage (Figure 1), often encountering millions of potential security events each week that they must evaluate and prioritize.

Figure 1. Millions of Potential Security Events Mandate Faster Analysis



Upon investigation, the analyst may discover only one or two real threats. To work effectively, the analyst must be able to quickly distinguish the real threats from insignificant events. To accomplish this, however, a security analyst must:

- Filter through a massive amount of data
- Make the right decisions about which issues to investigate more deeply to detect a threat
- Conduct forensic searches to identify the root cause of the event
- Contain and remediate the threat

And the analyst must do this all while the clock is ticking.

[3] Cisco Annual Security Report, 2014

The Security Visibility Challenge

Unfortunately, the process of detecting breaches is complex and time consuming because advanced threats are often long-term efforts in which the hacker can appear to be a normal user. Recognizing anomalies and the sequence of the attack is no small task in environments in which multidimensional cyber attacks often traverse a multitude of systems, networks, protocols, files, and behaviors.

To address today's dynamic threat landscape, security must be embedded at the center of the intelligent network infrastructure and across the extended network—from the data center; to the mobile endpoint; and onto the factory floor, oil rig, retail outlet, or banking kiosk. This extensive infrastructure protection is one of Cisco's strengths: Cisco offers the broadest set of security solutions available—addressing the comprehensive security needs of your infrastructure from the network to the data center, cloud, branch location, and endpoints.

Recent Cisco research revealed, however, that the average large enterprise has 54 security vendors.[4] Often multivendor solutions don't—and can't—work together. As strong as each of your security solutions may be independently, if they are not integrated you can't obtain a holistic view of real-time and historical data from all these sources. The use of multiple security solutions from multiple vendors means that security analysts must conduct "swivel chair management"—using multiple tools to access and correlate silos of data, and often writing proprietary code to identify patterns. The process is slow and manual in an environment that requires real-time analysis.

In addition, many traditional security products can reliably detect only known threats for which signatures exist; they can't detect unknown threats for which no signature exists. The tiny fingerprints of these advanced threats are often found only in nonsecurity-related data from business transactions and operations. For this reason, your security team must be able to access nonsecurity-related data from a broad range of sources.

Legacy SIEMS Are Insufficient

Many enterprises have invested in security information and event management (SIEM) systems (Figure 2) to provide comprehensive infrastructure and data visibility.

Figure 2. Legacy SIEMs Are Unsuited to Advanced Threat Environments

Unfortunately, legacy SIEMs fall short of what is required for advanced threat environments.

- **Difficult to deploy, requiring a long time to deliver value:** Legacy SIEMs take many months to implement. After they are established, they lack the flexibility needed to easily add new data sources—a feature critical to detect advanced threats.

[4] Investors.com, July 14, 2015

- **Lack enterprise-scale capabilities:** SIEMs typically use a SQL database or a single data store with a fixed schema. This data store is a single point of failure, with scalability and performance limitations, so it's unsuited to a security analytics environment producing massive quantities of data.
- **Not designed to detect unknown threats:** Legacy SIEMs specialize in detection of known threats, but they don't protect against the increasing number of unknown threats. Most SIEMS don't address all the areas through which an advanced threat might potentially penetrate the enterprise. Unless the SIEM was designed to integrate with your existing security infrastructure from the outset, your defense will have some fragmentation that creates gaps.
- **Limited capabilities:** Legacy SIEMS are useful only for monitoring and alerting, and they don't incorporate compliance use cases. They typically track only traditional security data such as logs from firewalls, intrusion prevention systems, and antimalware, limiting their ability to detect advanced threats.

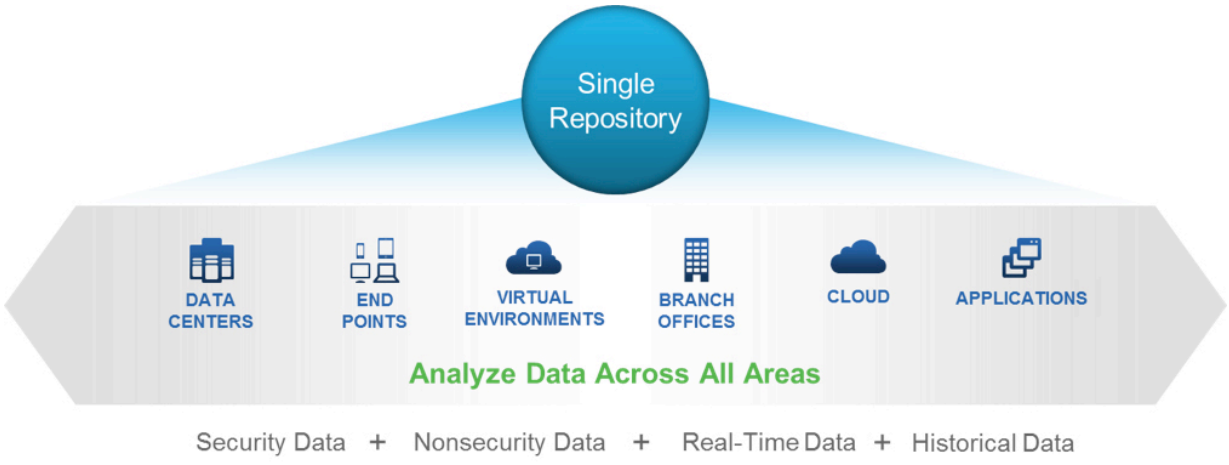
Requirements for an Advanced Security Analytics Solution

To address the challenges of today's advanced threat environments, you need the combined power of next-generation SIEM capabilities in your analytics software and an infrastructure that's designed to put time and resources back on your side.

Comprehensive, Continuous Visibility

Your security team needs to analyze data across all areas: from the network core to the edge (Figure 3).

Figure 3. A Single Repository Provides Comprehensive and Continuous Visibility



Your security analytics solution needs to collect both security and nonsecurity data from a wide variety of sources—logs, traffic flows, network packets, endpoint forensics, identity systems, physical security systems—and make it available to all members of the security group. Because multidimensional attacks can occur over long time periods, your security analytics solution must incorporate historical data so that analysts can determine the root cause and the breadth of a data breach.

To accelerate detection of advanced threats, all nonsecurity and security data should reside in a single repository that is monitored in real time. This repository will include large volumes of data and provide a baseline of normal user and traffic activity. Using this baseline, real-time analytics can automatically detect anomalies and outliers that may be advanced threats.

Full Security Management Capabilities

You'll want your security analytics solution to deliver a complete range of security management functions, including:

- **Continuous monitoring and alerting capabilities** that create integrated security intelligence from an unlimited range of data types and sources while integrating with all existing security solutions
- **Incident management capabilities** that quickly determine whether the event is a real incident and the extent of its business impact
- **Computer security incident response team (CSIRT) capabilities** that align people and data to identify the specific source and impact of a breach, contain the threat, and remediate the threat quickly
- **Security compliance and posture assessment capabilities** that validate your ability to meet regulations and policy requirements; can assert, monitor, and report on the ability to protect the right assets; and can verify your organization's security posture, controls, and approach

Powered By an Infrastructure Optimized for Big Data and Analytics

Because speed of detection, containment, and remediation is so critical, your security analytics solution needs a powerful, efficient infrastructure that's optimized for big data. This foundation should be:

- **Highly and rapidly scalable** to support massive quantities of real-time and historical information to keep pace with the growth of data sources and compliance requirements
- **Delivering predictably exceptional performance** to quickly process high data volumes and complex queries and support large numbers of simultaneous users
- **Designed for efficiency,** conserving capital expenditures (CapEx); reducing operating expenses (OpEx) associated with system management and deployment, facility space, and power and cooling requirements; and integrating with existing security solutions

Security Analytics on Cisco UCS with Splunk

The Security Analytics on Cisco UCS with Splunk solution meets all these requirements, providing:

- **A highly effective way to defend against multidimensional cyber attacks and known and unknown threats** by creating a single data repository that integrates with your existing security solutions: Security analysts can obtain comprehensive, continuous visibility and analyze unlimited types of real-time and historical security and business data. They can create integrated security intelligence by indexing the data and creating queries and visualizations.
- **Next-generation SIEM functions designed for today's advanced threat environments:** Next-generation functions help accelerate identification, investigation, containment, and remediation of security issues.
- **Massive scalability, outstanding performance, and low total cost of ownership (TCO):** The solution provides the capabilities needed to successfully support your analytics requirements today and over the long term.
- **Fast time to value:** The solution helps you quickly reduce the likelihood and impact of security breaches.

A Next-Generation SIEM

Splunk has extensive experience in the security analytics market and has been named a leader in the Gartner Magic Quadrant for SIEMS for the past three years. Used extensively for security use cases, Splunk has integrations across approximately 250 security platforms and products, including 10 Cisco® Security platforms.

Enterprises can choose from two ways to use Splunk for security analytics. You can build a customized security analytics solution by using Splunk Enterprise and its wide range of free applications and connectors, or you can use the Splunk App for Enterprise Security, which provides out-of-the-box, next-generation SIEM functions. The Splunk App for Enterprise Security builds on the use cases provided by a legacy SIEM, adding features such as monitoring and alerting for fraud detection, incident response, CSIRT, and compliance. It delivers immediate support for the most common security data sources, including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence, to accelerate deployment and adoption. Unlike legacy SIEMs, the Splunk App for Enterprise Security can help enterprises achieve results quickly, with the flexibility to add more data sources and make changes. It includes more than 45 prebuilt searches; 37 prepackaged dashboards; 160 reports; and incident-response workflows, analytics, and correlations that support the most common security use cases.

Cisco UCS Provides a Powerful, Scalable Analytics-Ready Foundation

Cisco UCS Integrated Infrastructure for Big Data provides an excellent foundation for big data use cases such as security analytics. Cisco UCS is a leading server platform in the industry. It's currently ranked number one in the Americas for market share in x86 blades, with more than 46,500 unique customers, including more than 85 percent of the Fortune 500. It delivers:

- **Industry-leading scalability:** As analysts perform forensic searches, they often find additional data sources that add value. With the growing numbers of threats, data sources, and data volumes, massive and efficient infrastructure scalability is essential. The Cisco UCS platform can scale to more than 6000 servers, so enterprises can be confident that they can scale their analytics workloads as the volume of data grows exponentially. In addition, Cisco service profiles allow you to add a new Cisco UCS server in minutes, so you can scale quickly and cost effectively.
- **Predictable and outstanding performance for Splunk at scale:** In a security operations center (SOC), analysts need to perform large numbers of forensics investigations—known as "needle in a haystack" searches—that require outstanding and consistent performance. The breakthrough design of Cisco UCS, integrating computing, network, and storage, delivers consistently outstanding performance even for very large Splunk deployments with large numbers of simultaneous users. Cisco UCS has won more than 100 world-record performance benchmarks, including the recent new TPCx-HS benchmark, which provides verifiable performance and price-to-performance metrics for big data systems. In this audited test, Cisco demonstrated outstanding linear performance and exceptional price-to-performance ratios for real-life big data workloads of 1, 3, and 10 terabytes (TB).
- **Low TCO:** Cisco UCS helps reduce TCO by conserving precious CapEx and OpEx. Its integrated design allows enterprises to reduce the costs of infrastructure cabling and switches by up to 77 percent. Advanced management automation capabilities allow enterprises to reduce provisioning times by up to 83 percent and management costs by approximately 61 percent compared to the costs for traditional servers. And the efficient design of Cisco UCS reduces power and cooling costs by up to 54 percent.

Security Analytics on Cisco UCS with Splunk in Action

Cisco has been a long-term and extensive user of Splunk software, so it's not surprising that the Cisco CSIRT decided to use Security Analytics on Cisco UCS with Splunk to improve its ability to monitor, correlate, detect, and resolve security issues.

Cisco had been using an externally developed SIEM system that had significant limitations. CSIRT lacked a central source for security event data, and the SIEM could not scale to support the information needs. The SIEM could not effectively index nonsecurity data (for example, logs from custom applications), search speed was inadequate, and the prebuilt rules generated too many false positives. Multiple operations teams in Cisco IT were also frustrated by the SIEM system's limited ability to quickly detect and find the root cause of problems.

CSIRT needed a single analytics platform that would deliver:

- Real-time monitoring of the network and IT systems
- Automated correlation of events and alerts
- Centralized visibility across applications and infrastructure to provide better capabilities to provide preventative alerting and monitoring, correlate events, identify system dependencies, and manage the impact of change requests

Security Analytics on Cisco UCS with Splunk addressed all the team's requirements. The CSIRT environment includes 25 Cisco Web Security Appliances that are con d in seven clusters throughout the world. The clusters comprise 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. The Cisco UCS and Splunk solution analyzes and correlates system log events to provide real-time alerts for sensitive investigations and advanced persistent threat incidents. It indexes any type of machine data from any source, helping CSIRT protect the Cisco IT infrastructure and business information with better incident response, forensics, and threat detection. Results include:

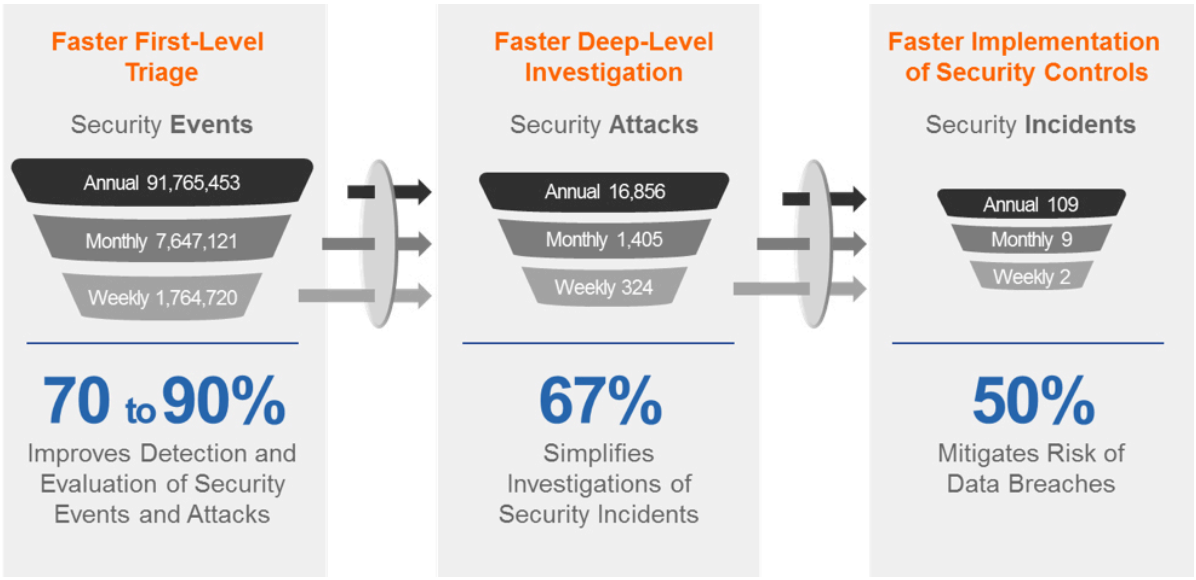
- 33 percent less time needed to conduct security investigations
- Faster, simpler data access because all security data is readily available at a single, centralized portal
- Substantially easier correlation for more thorough investigations
- Cost savings compared to the expenses of a traditional SIEM
- Greater CSIRT analyst productivity because analysts can automate routine tasks

Put Time Back on Your Side with Security Analytics on Cisco UCS with Splunk

Seconds count in today's advanced threat security environment. Security Analytics on Cisco UCS with Splunk can help you:

- Eliminate complexity and lack of integration with a single repository that delivers comprehensive, continuous visibility so that you can analyze all data: security related, nonsecurity related, real time, and historical
- Help ensure faster incident detection and response (Figure 4) through automated anomaly and outlier detection and advanced incident management capabilities
- Deliver the agility needed to respond to known and unknown threats with a full range of next-generation SIEM capabilities
- Deploy an infrastructure designed to deliver outstanding performance and scale efficiently as data volumes grow

Figure 4. Security Analytics on Cisco UCS with Splunk Delivers Measureable Results



Next Steps

For effective security, speed is essential. Cisco and Splunk make it easy to get started:

- Use tested and proven Cisco UCS configurations for Splunk Enterprise security deployments and get detailed deployment guidance in the Cisco UCS Integrated Infrastructure for Big Data with Splunk Enterprise Cisco Validate Design.
- Visit Splunk's security website to learn more about Splunk security solutions and gain access to Splunk's range of security applications.
- If you are a Cisco Security customer, all of Splunk's applications for Cisco are free. Search on https://splunkbase.splunk.com/apps/#/search/cisco and download a free application.

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.**

Printed in USA C22-735894-00 10/15