# Splunk and the SANS Top 20 Critical Security Controls

## Mapping Splunk Software to the SANS Top 20 CSC Version 4.1

splunk>

Published by Splunk Inc., 250 Brannan St., San Francisco, CA 94107

Editor/Analyst: Splunk Inc.
Copyeditor: Splunk Inc.
Production Editor: Splunk Inc.
Cover: Splunk Inc.
Graphics: Splunk Inc.

First Edition: April 2014



**Disclaimer**

This book is intended as a text and reference book for reading purposes only. The actual use of Splunk's software products must be in accordance with their corresponding software license agreements and not with anything written in this book. The documentation provided for Splunk's software products, and not this book, is the definitive source for information on how to use these products. Although great care has been taken to ensure the accuracy and timeliness of the information in this book, Splunk does not give any warranty or guarantee of the accuracy or timeliness of the information and Splunk does not assume any liability in connection with any use or result from the use of the information in this book. The reader should check at docs.splunk.com for definitive descriptions of Splunk's features and functionality.

# Table of Contents

# Abstract

Splunk provides a single, integrated, security intelligence platform that allows today's security professionals to ensure that their organizations are meeting Critical Security Controls requirements. The software can verify incoming data, execute the requirements needed, or support human activities associated with a control. Security professionals find Splunk software uniquely suited to support these controls in a number of ways, including: universal data ingestion with no specific vendor preference; a real-time schema-less architecture; unparalleled scaling capabilities for big data; and an agile and flexible reporting interface.

# Introduction

Splunk Software and the Top 20 Critical Security Controls

The Top 20 Critical Security Controls (CSC) are a time-proven, prioritized, "what works" list of 20 controls that can be used to minimize security risks to enterprise systems and the critical data they maintain. These controls are derived from and "cross-walked" to controls in NIST Special Publication 800-53. They are also known as the Consensus Audit Guidelines (CAG).
The list was originally authored by the U.S. National Security Agency (NSA) in 2008, and has since been revised by a consortium of U.S. and international agencies such as the Center for the Protection of National Infrastructure in the U.K., the Australian government's Department of Defense and experts from private industry. Formerly managed by SANS, the Top 20 CSC are currently governed by the Council on CyberSecurity and are considered the "de facto yardstick by which corporate security programs can be measured," according to the Cybersecurity Law Institute. The current version of the controls is 4.1 as of January 2014.

These controls function across security processes, products, architectures and services, and have been proven in real-world scenarios. According to surveys conducted by the U.S. State Department, organizations that fully implement, automate and measure themselves against the Top 20 CSC can reduce risk by up to 94%.

For more information on the history of the Top 20 CSC, please see: http://www.sans.org/critical-security-controls/history.

The Top 20 CSC are ranked in order of overall importance and application to a corporate security strategy. For example, the first two controls, surrounding known inventory, are at the top of the list and are foundational in nature, ranking "very high" for attack mitigation. Conversely, the final item on the list, surrounding pen testing and "red team" exercises, ranks "low" for attack mitigation. More information and deep analysis on each control can be found here: http://www.sans.org/critical-security-controls/guidelines.

## Why are the Top 20 CSC Important?

There are several reasons that organizations embrace the Top 20 CSC as they develop security strategies:

- Implementation of the controls can reduce the risk of currently-known high priority attacks as well as attacks expected in the near future.
- The controls were generated by consensus from experts in both the federal government and private industry.
- The controls are well written, approachable and distill common security requirements into a list that is easy to understand and implement.
- The controls are reasonably comprehensive and address the most important areas of concern.

*Figure 1* is an example of how the NSA applies the Top 20 CSC to actions taken during attacks. Each of the controls applies to one or more of the following categories: Reconnaissance, Get In, Stay In and Exploit.


Figure 1. NSA's attack mitigation view of the Top 20 CSC.

## How Splunk Software Maps to the Top 20 CSC: Four Approaches

Splunk software maps to each control in the Top 20 CSC (see *Figure 2*). There are four major ways in which the Splunk platform supports the controls:

- **Verification:** As Splunk software ingests data, it can generate reports and dashboards that show compliance or non-compliance with controls. Incidents of non-compliance can generate alerts to SOC personnel.
- **Execution:** In the case of an attack or non-compliance, Splunk software can carry out recommended actions to meet controls.
- **Verification & Execution:** Data from third-party sources can be correlated with data ingested in Splunk software to meet the control.
- **Support:** The Splunk platform provides flexible features that help security professionals with controls that are largely policy and process based.

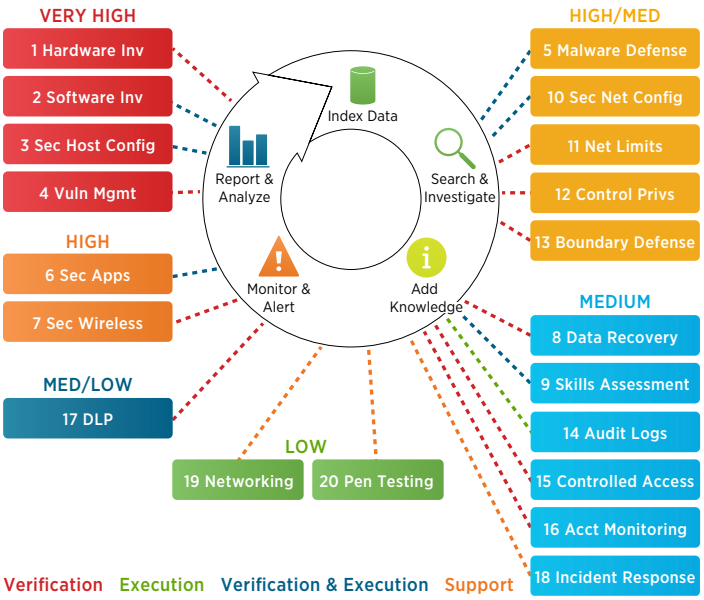


Figure 2. Splunk software maps to each control in the Top 20 CSC.

## How Customers Use Splunk for Security

Splunk Enterprise™, the platform for machine-generated data, supports security use cases in a number of ways:

- Splunk Enterprise:
  - Indexes data from any machine data source
  - Searches through machine data from a centralized console
  - Allows the security professional to add tags, create event types and correlate the incoming data with business context
  - Proactively monitors and alerts on security incidents, with automatic remediation of security issues—for example, changing a firewall rule in response to Splunk search results
  - Allows for the creation of reports, dashboards and other forms of analytics to communicate security information throughout the organization
- Splunk Enterprise can be augmented with free Splunk apps[1] that are specific to one or more security technologies or vendors.
- Splunk Enterprise with the Splunk App for Enterprise Security (ES) provides an extensive security intelligence application on top of the core Splunk platform. This gives customers all of the capabilities of a traditional SIEM solution combined with the power of analyzing vast amounts of normal, credentialed user data to detect advanced threats.

There are also a number of free security technology and vendor-specific apps available for download at http://apps.splunk.com. While apps are not required for Splunk software to map to the Top 20 CSC, in most cases apps will accelerate ramp time (for example, the Checkpoint, Palo Alto or Cisco apps to support Control 13: Boundary Defense). Apps allow you to quickly gain value from data already ingested in Splunk software and can provide customized ways to onboard data via specific binaries and technology add-ons (TAs).

### Splunk App for Enterprise Security

The Splunk App for Enterprise Security (ES) supports mapping Splunk deployments to the Top 20 CSC, **but is not required**. However, using the app *significantly reduces implementation time* when mapping Splunk software to the Top 20 CSC requirements. Key areas that the app supports are highlighted in separate call-out boxes like this one.

## The Big Picture

What makes the Splunk platform unique for organizations that need to implement the Top 20 CSC? **Splunk software makes all data in your organization security relevant (see *Table 1*)**. As data is indexed by Splunk Enterprise, it becomes instantly searchable and security professionals can easily correlate all of these seemingly disparate data sources. Furthermore, the different data types can be seen in the context of data locked in business systems, which is often the key factor in determining correct root causes. Security professionals can then build dashboards and reports on top of the data, and set up actions and alerts to be executed on specific thresholds. In addition, any analysis can be operationalized to proactively protect your organization from emerging threat.

| | |
|---|---|
| Log data | Outputs from scripts that run regularly on servers |
| Context data | Authentication data |
| Binary (flow) data | Information from structured data sources |
| Log files | Endpoint data |
| Application stack traces | Configurations |
| GPS | RFID |
| Call Data Records (CDR) | Email |
| Web Proxy | Active Directory |
| Threat intelligence data | Firewall data |

Table 1: Examples of data types that Splunk software makes security relevant.

The remainder of this document details how Splunk software's capabilities apply to each of the Top 20 CSC. At the beginning of each section, the document maps Splunk software's capabilities to the control(s) in NIST Special Publication 800-53 and in the NSA Manageable Plan Milestones.

1. There are 120+ security-oriented apps and add-ons as of April 2014.

# The Top 20 CSC

How Splunk Software Supports the Top 20 CSC

## Control 1: Inventory of Authorized and Unauthorized Devices

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6*

*Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops and remote devices.*

**Role of Splunk Software: Verification**

An inventory of authorized and unauthorized devices is primarily accomplished with discovery and vulnerability management tools such as Nmap, Nessus, RedSeal, Qualys and Nexpose. Traditional configuration management database (CMDB) products with discovery engines, such as IBM TADDM and BMC Atrium Discovery, can also be used here.

- Splunk software accepts regularly generated reports from any discovery or vulnerability management tool. These reports are usually in XML, CSV or similar formats and they contain timestamps for each entry, providing in-depth analysis of what was discovered.
- TA or app support is provided for the following:
  - Splunk Add-on for Nessus
  - Nmap
  - Ncircle (Tripwire) IP360
  - Other VA/VM/discovery applications such as Qualys can easily be integrated into Splunk software via log file/ report ingestion
- The Splunk for Asset Discovery app is also available and leverages Nmap.
- By ingesting these data sources, a record of each discovered device is kept in Splunk Enterprise. Every time a new scan is run, information is deposited into Splunk software and it is easy to find the deltas between scans to find new or different devices.
- With Splunk software, it is simple to correlate inventory data with other data sources. Two examples are a CMDB that contains a list of authorized devices or a maintained list of MAC addresses that "should not appear" on the network.
- It is also easy to correlate other important data types, including audit logs, change logs, traffic patterns or the output of malware detection solutions, against unauthorized devices found.

### Control 1: Using the Splunk App for Enterprise Security (ES)

- Device inventory information within the environment that has been ingested into Splunk software can be leveraged in ES as "assets" from within the Asset Center of the Splunk App for Enterprise Security (see *Figure 3*), a pre-built view into asset-relevant data. This allows Splunk software to correlate any incoming information against this list of known assets. A security investigator can instantly access asset information such as asset priority, category, business unit, owner and other context-sensitive data. The asset list can also be automatically populated by an external source, such as a directory server or CMDB.
- ES contains an interactive data visualization called the Asset Investigator (see *Figure 4*). This visualization allows a security investigator to view an asset and all notable events related to that asset over time. Information available from external sources is also brought into this view to provide business context

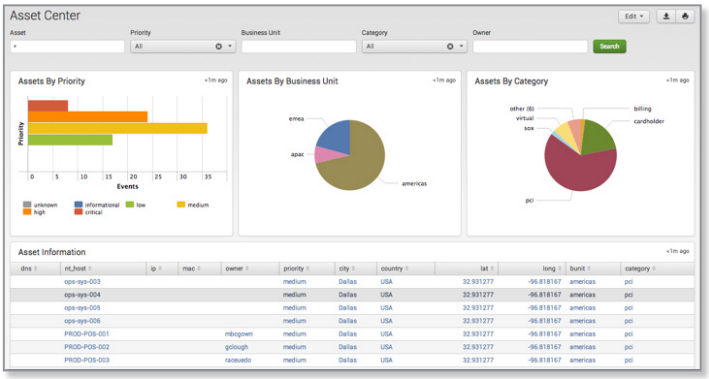


Figure 3. Splunk App for Enterprise Security: Asset Center.

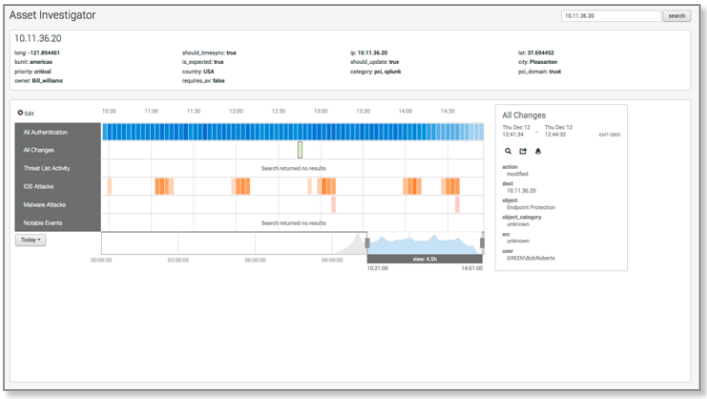


Figure 4. Splunk App for Enterprise Security: Asset Investigator.

## Control 2: Inventory of Authorized and Unauthorized Software

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 7: Baseline Management: Executable Content Restrictions*

*Identify vulnerable or malicious software to mitigate or root out attacks: devise a list of authorized software for each type of system, and deploy tools to track software installed (type, version and patches) and monitor for unauthorized or unnecessary software.*

**Role of Splunk Software: Verification & Execution**

Inventory of authorized and unauthorized software is typically accomplished with software change management, whitelisting and vulnerability management tools, such as IBM BigFix, Microsoft System Center and Bit9 Parity. Splunk software's scripted input capability can also assist with these tasks.

- Splunk software can gather all information about installed software and patches on a given system through scripted inputs and the standard scripts provided in the Splunk Add-on for Microsoft Windows and the Splunk Add-on for Unix and Linux. This data is ingested into Splunk software on a regular basis and is made available for reporting and alerting.
- Splunk software accepts regularly generated reports from any software change management, whitelisting or vulnerability management tool. These reports are usually in XML, CSV or similar formats and contain timestamps for each entry, providing in-depth analysis of what was discovered.
- Splunk software can correlate data from scripted inputs or third-party tools against other enterprise data sources, such as a CMDB or a hash-based whitelist of approved software applications, and display and alert on any violations.
- Splunk software can calculate and display the deltas in asset information, allowing security practitioners to get a good picture of the software processes and services that are coming and going on an individual host or a group of hosts.

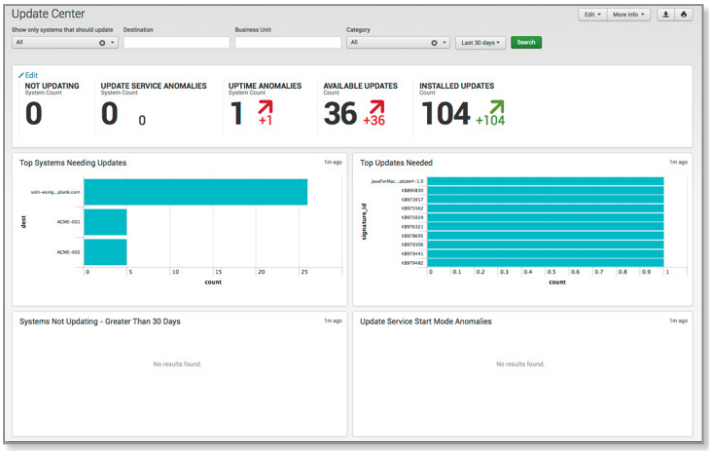


Figure 5. Splunk App for Enterprise Security: Update Center.

### Control 2: Using the Splunk App for Enterprise Security

- ES provides ways of defining "interesting" processes and services within your environment via lookup files that can be statically or dynamically populated. Lookup files can define processes that are either whitelisted or blacklisted, such as adding fields like "is_secure" and "is_prohibited." When data containing the specific process or service name is processed, it is correlated against these lists so that a security investigator can instantly know if a given piece of software is authorized.
- Update Center and Update Search dashboards that display information about the patch levels of systems are also available in ES (see *Figures 5* and *6*). The Endpoint Changes dashboard is also useful for getting an idea of the number of changes happening in the environment (see *Figure 7*). These dashboards, driven by Splunk-derived change information or from patch management systems, allow SOC personnel to determine which systems are in the greatest need of an update

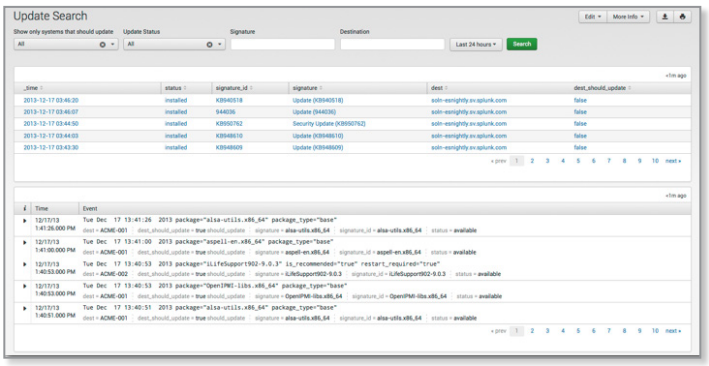


Figure 6. Splunk App for Enterprise Security: Update Search.

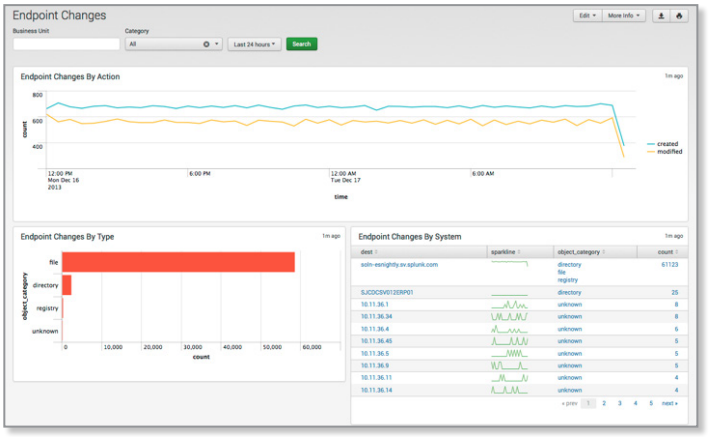


Figure 7. Splunk App for Enterprise Security: Endpoint Changes.

## Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations and Servers

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 7: Baseline Management*
*Configuration and Change Management*

*Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.*

### Role of Splunk Software: Verification & Execution

Securing hardware and software configurations is typically accomplished with security configuration management tools (SCM) such as IBM BigFix, Tripwire CCM and Enterprise, and Symantec CSP. Many security configurations can be evaluated by Splunk software's ability to run scripted inputs or look for evidence of misconfiguration in data.

- The Splunk platform accepts scheduled reports generated from any security configuration management tool, whether in XML, CSV or similar formats.
- These reports and data sources contain a record of each device's security configuration. Every time a new scan is run, the information is ingested into Splunk software and it is easy to find the differences between scans to identify new or different configurations.
- Splunk software can easily correlate SCM data with other data sources. One example is a CMDB that contains the compliance policy a particular device should be configured against.
- Via scripted inputs and monitoring log files, Splunk software assesses the configuration of hosts for evidence of misconfiguration. This is done extensively in the Splunk App for PCI Compliance using the add-on for Access Protection.
- Splunk software can look for evidence of systems not meeting standards. For example, if a desktop machine within the network suddenly starts to generate web requests with a non-compliant user agent (available by analyzing proxy logs), then an alert or a notable event can be generated.

### Control 3: Using the Splunk App for Enterprise Security

- When misconfigured services and settings are exploited, there is generally anomalous behavior in the environment that can be tied back to rogue services, processes or other kinds of misconfigurations. ES contains correlation rules to identify this behavior and misconfigurations such as improper password lengths or expiry timeframes. It also includes several dashboards, such as Traffic Search, System Center and Time Center, which can display systems that do not meet the secure configuration standards (see *Figures 8, 9* and *10*).

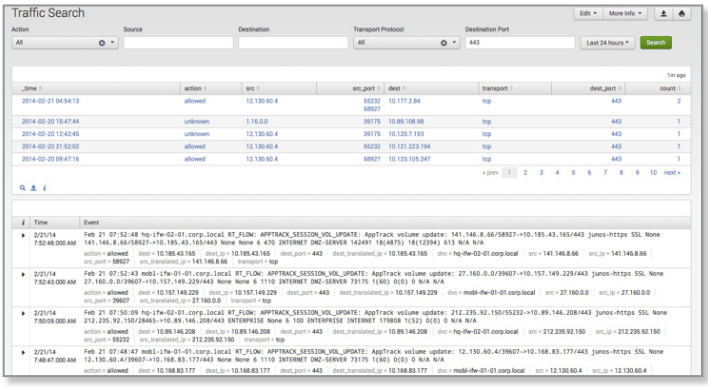


Figure 8. Splunk App for Enterprise Security: Traffic Search.

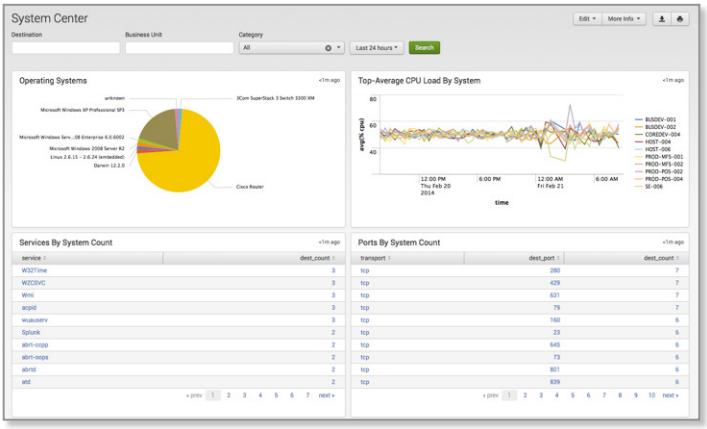


Figure 9. Splunk App for Enterprise Security: System Center.

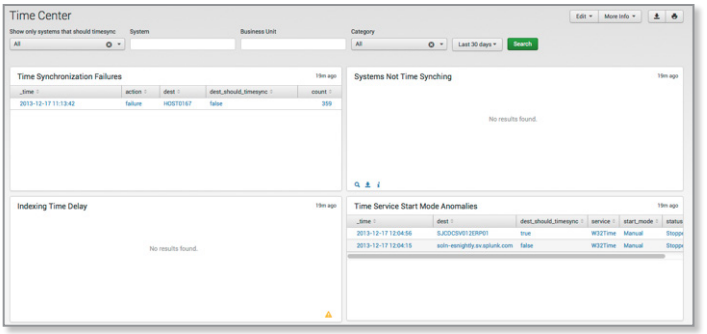


Figure 10. Splunk App for Enterprise Security: Time Center.

## Control 4: Continuous Vulnerability Assessment and Remediation

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 6: Patch Management*

*Proactively identify and repair software vulnerabilities reported by security researchers or vendors: regularly run automated vulnerability scanning tools against all systems and quickly remediate vulnerabilities, with critical problems fixed within 48 hours.*

**Role of Splunk Software: Verification**

Continuous vulnerability assessment (VA) and remediation is primarily accomplished with vulnerability management (VM) tools such as Rapid7 Nexpose, Tenable Nessus, Qualys and Tripwire IP360.

- Splunk accepts regularly scheduled reports from any discovery or vulnerability management tool in XML, CSV or similar formats.
- Technology add-ons or app support are provided for the following:
  - Splunk Add-on for Nessus
  - Nmap
  - Ncircle (Tripwire) IP360
- Other VA/VM/discovery applications can easily be integrated into Splunk software via log file and report ingestion.

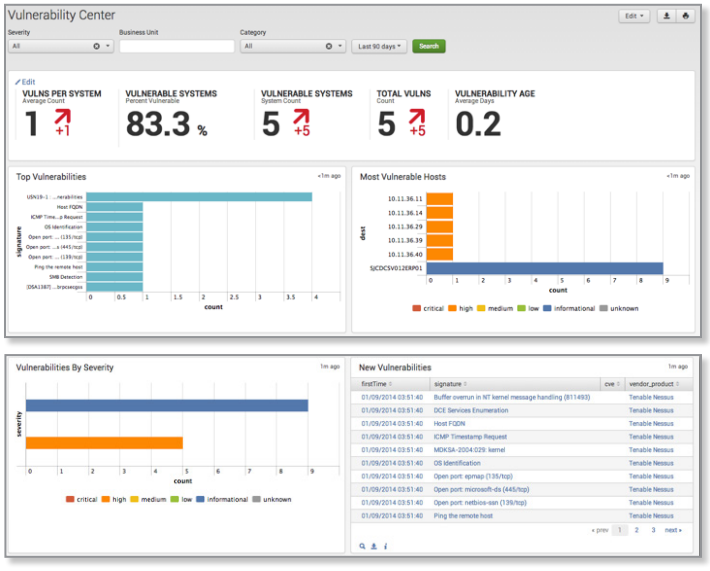


Figure 11. Splunk App for Enterprise Security: Vulnerability Center.

### Control 4: Using the Splunk App for Enterprise Security

- Information from vulnerability scans drives the Vulnerability Center, Operations and Profiler dashboards within the Splunk App for Enterprise Security (see *Figures 11* and *12*). These dashboards provide a complete view of vulnerability management activities and sourced data across the entire environment. With these dashboards, SOC personnel can verify that scans are running and determine the newest and most critical vulnerabilities. Since the dashboards display first time vulnerabilities and allow filtering to show vulnerabilities by age, personnel can also determine whether specific vulnerabilities have been remediated.
- ES compiles information from approximately 18 (configurable) threat lists and correlates the information with threat list data found in the environment (see *Figure 13*). For example, if any devices are found communicating with an IP address on this regularly updated list: http://rules.emergingthreats.net/blockrules/compromised-ips.txt, an alert or a notable event will be generated.

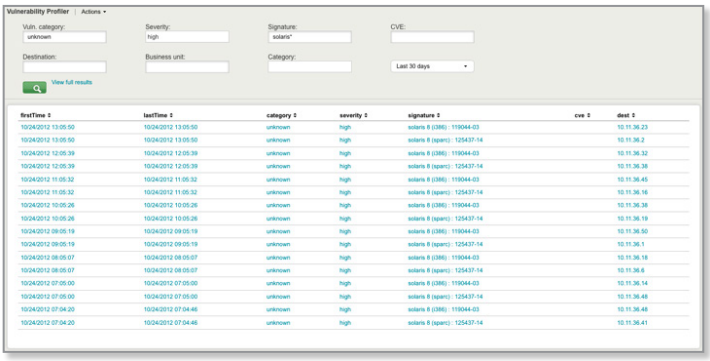


Figure 12. Splunk App for Enterprise Security: Vulnerability Profiler.

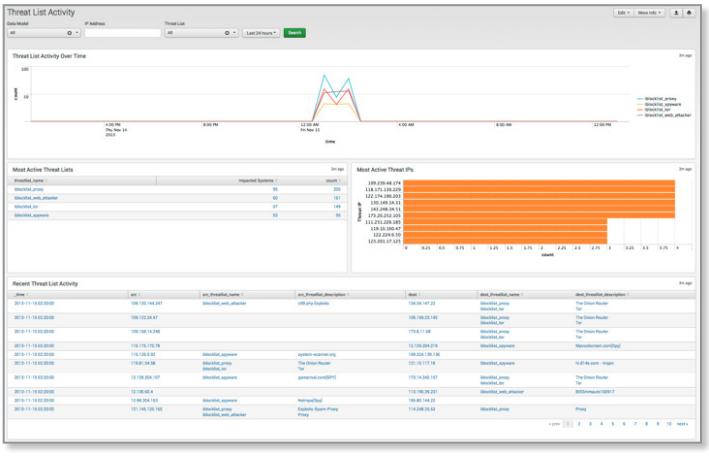


Figure 13. Splunk App for Enterprise Security: Threat List Activity.

## Control 5: Malware Defense

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Virus Scanners and Host Intrusion Prevention Systems (HIPS)*
*Personal Electronic Device (PED) Management*
*Network Access Protection/Control (NAP/NAC)*
*Security Gateways, Proxies and Firewalls*
*Network Security Monitoring*

*Block malicious code from tampering with system settings or contents, capturing sensitive data or spreading: use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

### Role of Splunk Software: Verification & Execution

Malware defense is accomplished with endpoint protection programs from vendors like McAfee, Symantec, Sophos and others. Whitelisting products from vendors like Bit9 also play a supporting role. However, the monitoring of removable media activity can be accomplished by monitoring the appropriate log files and/or registry settings with Splunk software. Splunk can also confirm that anti-virus software is running and is installed based on process or log file monitoring.

- Splunk software parses log files from any anti-virus or anti-malware management tool. These log files are often in syslog or Windows Event Log formats and contain timestamps for each entry, providing in-depth information on the status of malware discovery and quarantine activities on individual hosts. Several technology add-ons are available for free download from apps.splunk.com, supporting popular anti-virus products like Sophos, TrendMicro, and Symantec Endpoint Protection and Antivirus.
- Splunk software can access anti-virus scan information in vendor-specific databases. These databases contain individual workstation information and provide malware discovery and quarantine activities on specific hosts. One example of a Splunk technology add-on that works in this manner is the App for McAfee Web Gateway (Epolicy Orchestrator and IDS).
- Through the use of scripted inputs and monitoring of log files, Splunk software can assess the configuration of a particular server and look for evidence that the system has mounted removable storage or if changes have been made to the system to allow for removable storage.
- Splunk software can also use scripted inputs to ensure that the appropriate anti-virus or anti-malware executables and services are running.

### Control 5: Using the Splunk App for Enterprise Security

- Information from anti-virus and anti-malware products drives the Malware Center, Malware Search and Malware Operations dashboards within ES (see *Figures 14, 15* and *16*). These dashboards include information from firewalls, IDS, system logs, Windows domain information and related network sources to give a complete view of malware management activities and sourced data across the entire environment. By using these dashboards, SOC personnel can verify that clients have anti-virus and anti-malware products with updated definitions deployed. This allows SOC personnel to quickly identify the newest and most prevalent malware in the environment.
- Many organizations have multiple anti-virus or anti-malware products. ES maps the data available from disparate products into a common information model (CIM), allowing information from these products to be displayed on the same dashboards and easily correlated.

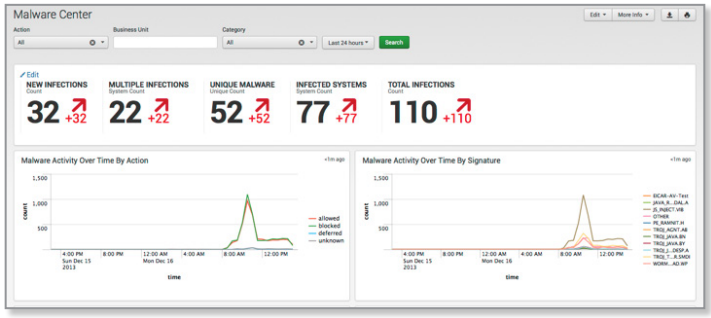


Figure 14. Splunk App for Enterprise Security: Malware Center.

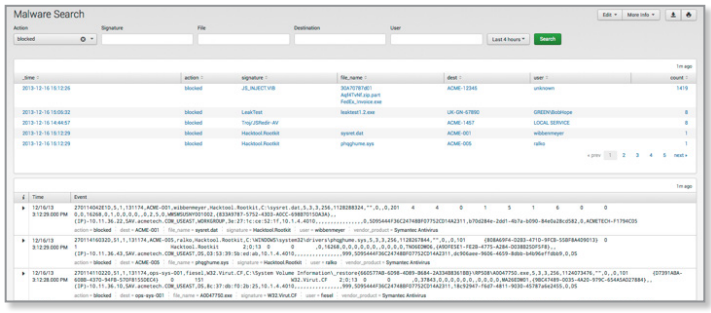


Figure 15. Splunk App for Enterprise Security: Malware Search.

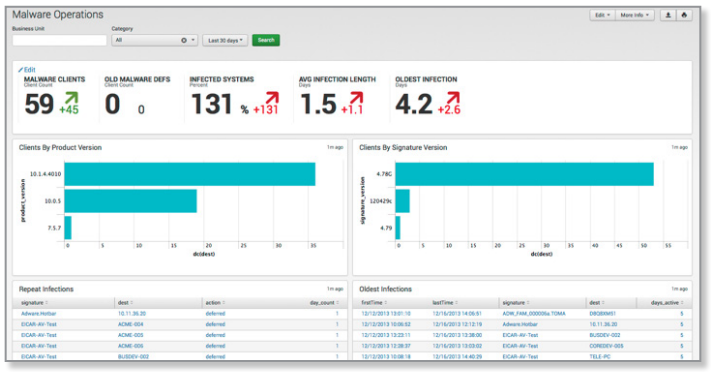


Figure 16. Splunk App for Enterprise Security: Malware Operations.

## Control 6: Application Software Security

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*
*Milestone 7: Baseline Management*
*Security Gateways, Proxies and Firewalls*

*Neutralize vulnerabilities in web-based and other application software: carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic and explicitly check for errors in all user input (including by size and data type).*

**Role of Splunk Software: Verification & Execution**

Application software security is usually accomplished with tools that perform static and dynamic application security testing, such as web application scanners like QualysGuard WAS, Whitehat Sentinel and Tripwire Webapp360. Web application firewalls include products like Imperva SecureSphere, Barracuda WAF Vx and Cisco ACE. Most of these tools focus on the OWASP Top 10 Vulnerabilities and others. Splunk software can monitor the log file output from these tools as well as traffic inspection firewalls, and can analyze user input coming into web applications in real time.

- Splunk accepts regularly generated reports from any application scanner. These reports are usually in XML, CSV or similar formats.
- Web application firewalls provide web firewall, access, audit and system logs, all of which can be gathered in Splunk software for analysis.
- During application development, penetration testing is often part of the QA cycle. Developers should use Splunk software to analyze the application logs during this process and to understand how the application responds to the scans, allowing them to identify vulnerabilities before production.
- Once an application is in production, Splunk software can help detect common application attacks, such as SQL injection and cross-site scripting. With SQL injection, for example, there are many different sources that Splunk software can consume in real time to help detect this activity, including:
  - IDS/IPS logs
  - Web vulnerability scanners
  - Network capture
  - Application logs
  - Authentication logs
  - Database error logs
- When monitoring for SQL injection, searching your web application logs for patterns of misuse, evidence of the semicolon or the word JOIN or UNION within “GET” and “POST” requests in a web access log are grounds for investigation. Extensive information on Splunk and SQL injection detection can be viewed here.

### Control 6: Using the Splunk App for Enterprise Security

- ES contains several correlation searches and dashboards to assist with finding vulnerabilities in and attacks against web-based applications. Two examples are the HTTP User Agent Analysis and URL Length Analysis dashboards (see *Figures 17* and *18*). With the HTTP User Agent Analysis, unusual user agents (based on standard deviation and Z score) are easily discovered. These user agent strings can then be evaluated for evidence of SQL injection and other threats. With the URL Length Analysis, any information in Splunk that contains URL strings can be discovered, again based on standard deviation and Z score. URLs that have abnormal length can often include evidence of embedded SQL, XSS and more.

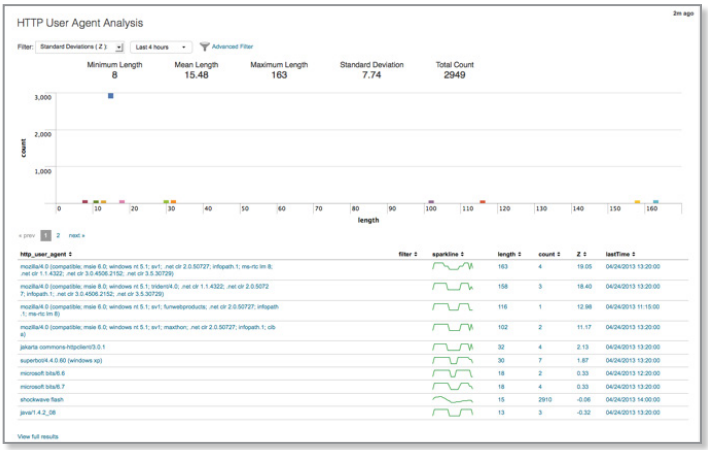


Figure 17. Splunk App for Enterprise Security: HTTP User Agent Analysis.

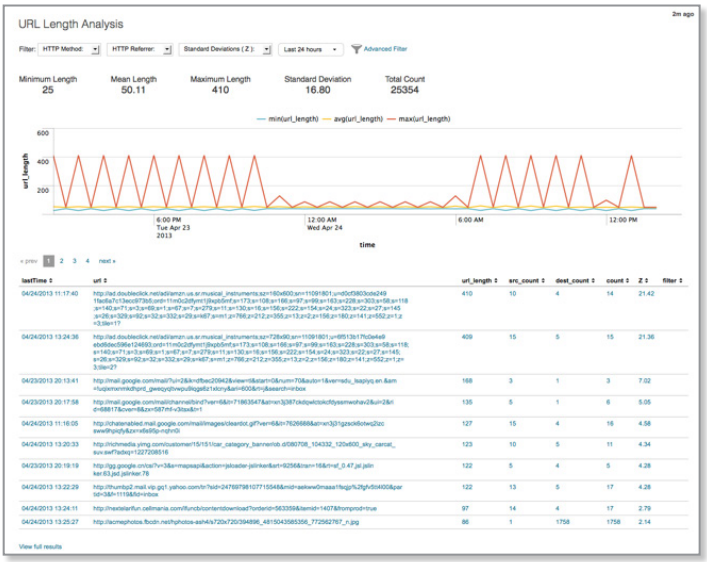


Figure 18. Splunk App for Enterprise Security: URL Length Analysis.

## Control 7: Wireless Device Control

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Remote Access Security*

*Protect the security perimeter against unauthorized wireless access: allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.*

**Role of Splunk Software: Verification**

Wireless device control is accomplished with wireless-protection specific tools (WIPS) or generic tools that scan networks for new and unknown devices, such as IDS/IPS systems, network discovery tools or network access control (NAC) logs. Splunk software can monitor the log file output from these tools and leverage the information in correlation searches to alert about rogue access points.

- Splunk software accepts regularly generated log files from WIPS tools and has free technology add-ons for specific WIPS, such as Motorola AirDefense, available in the Splunk App for Enterprise Security.
- When a wireless access point is detected, Splunk software can correlate the MAC address with an asset database to ensure that it is an authorized device. If the CMDB contains the management status of the device, Splunk can correlate that information as well.
- The Splunk App for PCI-DSS contains a Rogue Wireless Access Point Detection report (see *Figure 19*). This report can be easily copied to Splunk Enterprise or to the Splunk App for Enterprise Security.

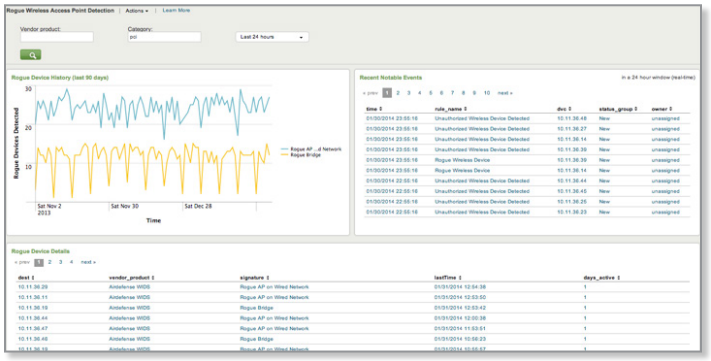


Figure 19. Splunk PCI-DSS: Rogue Wireless Access Point Detection.

## Control 8: Data Recovery Capability

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CP-9 (a, b, d, 1, 3), CP-10 (6)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Backup Strategy*

*Minimize the damage from an attack: implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.*

**Role of Splunk Software: Verification**

Data recovery is accomplished with enterprise backup solutions. Most backup solutions create detailed logs of all of their activity. Splunk software can monitor the log file output from these tools and leverages the information in searches and dashboards to confirm that critical systems are being backed up. Alerts can be generated if expected backup activity is not seen.

- Splunk software can consume regular backup activity logs from any backup solution. Popular solutions include products from vendors like EMC, IBM, CommVault, Symantec and HP.
- Dashboards can be created to display critical and sensitive systems (for example, those designated as containing or processing cardholder data) and their backup status.
- An example of a dashboard created from EMC Networker log files is displayed below (see *Figure 20*).

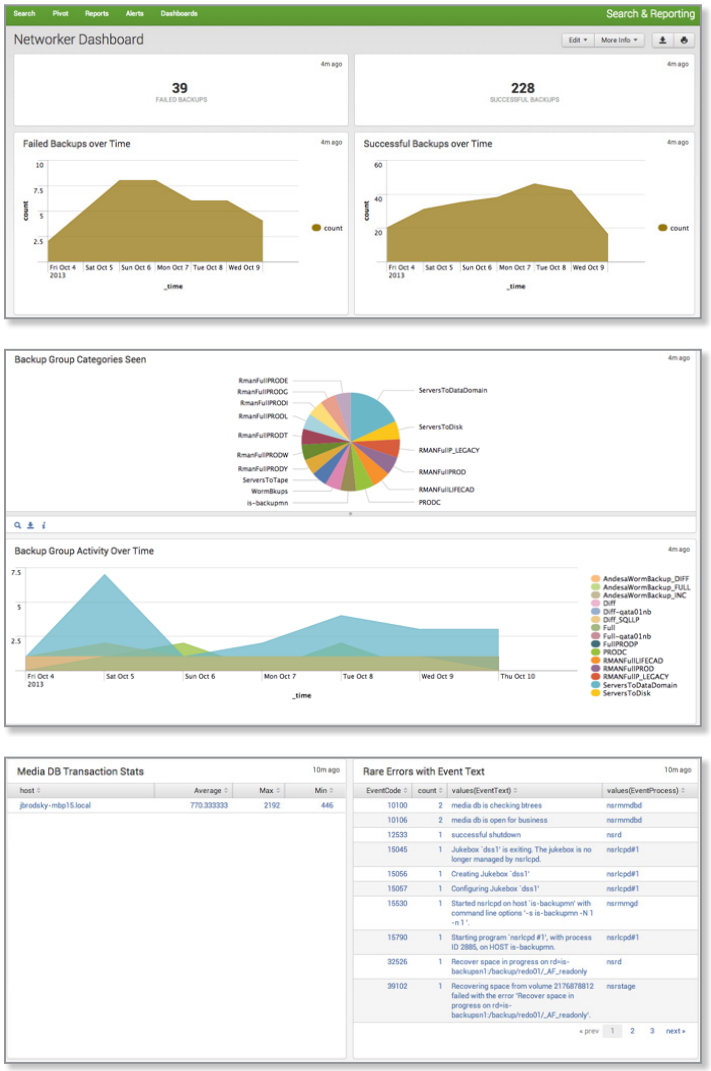


Figure 20. Splunk Enterprise: EMC Networker Example Dashboard, Backup Activity.

## Control 9: Security Skills Assessment

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AT-1, AT-2 (1), AT-3 (1)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Training*

*Find knowledge gaps and fill them with exercises and training: develop a security skills assessment program, map training against the skills required for each job and use the results to allocate resources effectively to improve security practices.*

**Role of Splunk Software: Verification & Execution**

A security skills assessment is generally accomplished via manual processes executed by staff resources. Policies need to be put in place to generate security awareness across the organization. These policies are usually carried out by the HR department, with support from information security staff. However, Splunk software can assist in the gap analysis to determine where security training is required, and then assess its effectiveness.

- Splunk software can be used to assess user behavior and determine which populations of users require security awareness training. For example, by looking at the following types of behavior available from Splunk searches against activity and web access/proxy logs, additional required training can be identified:
  - Which users are accessing inappropriate websites?
  - Which users are accessing resources with default/shared account names?
  - Which users are using unapproved web browsers?
  - Which users clicked on a link in a fake phishing email?
  - Which users are putting the company at risk with long VPN sessions?
- If data regarding security awareness and other security-specific training is placed in a corporate directory, Splunk software can access this data for correlation purposes. A Splunk search detecting improper system access, for example, can be correlated against the identity of a user, and whether or not the user has attended security awareness training.
- When an organization tests security awareness, Splunk software can identify which employees have taken the test and roll up this information into reports organized by agency or business unit for accountability and transparency.
- Once security awareness training has been rolled out, Splunk software can be used to assess behavior and identify users who are not following guidelines. These individuals may need to be subject to corrective action.

### Control 9: Using the Splunk App for Enterprise Security

- ES contains several dashboards that assist in understanding access patterns across the corporate environment. The Session Center dashboard is very useful for identifying users with long VPN sessions (see *Figure 21*).
- Identity information ingested into Splunk can be used in ES as an "identity" within Identity Center (see *Figure 22*) and Splunk software can correlate any incoming information against this list of known identities. This enables a security investigator to instantly access identity information such as name, phone, business unit, category, email, manager and so forth. This asset list can be automatically populated by an external source, such as a directory server or CMDB, and it also compensates for multiple username formats via identity matching.

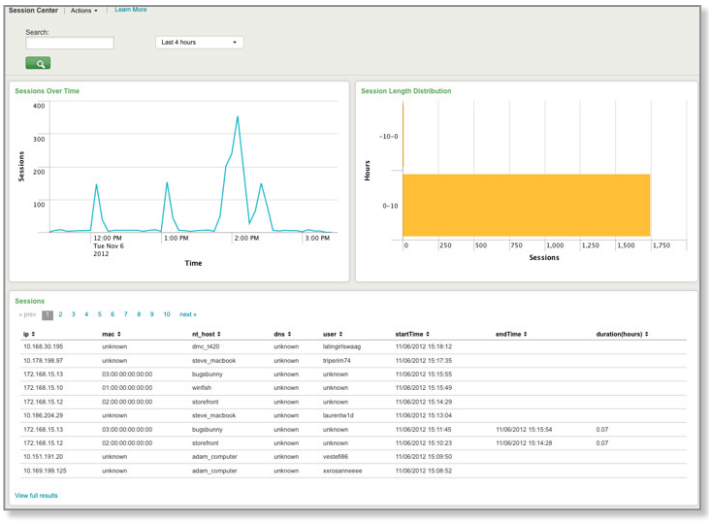


Figure 21. Splunk App for Enterprise Security: Session Center.

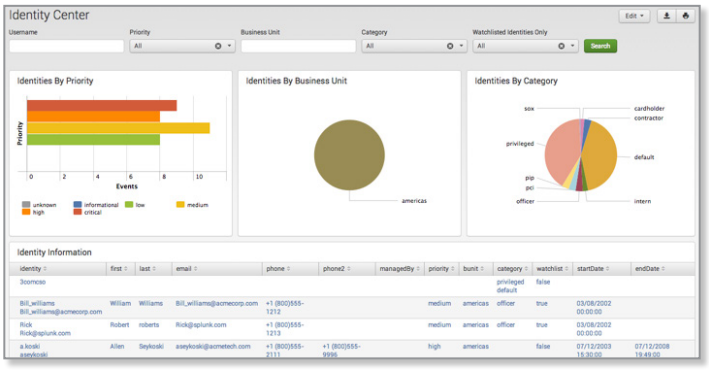


Figure 22. Splunk App for Enterprise Security: Identity Center.

## Control 10: Secure Configurations for Firewalls, Routers and Switches

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), IA-2 (1, 6), IA-5, IA-8, RA-5, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC-9*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 7: Baseline Management*
*Configuration and Change Management*

*Preclude electronic holes from forming at connection points with the Internet, other organizations and internal network segments: compare firewall, router and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.*

**Role of Splunk Software: Verification & Execution**

Maintaining secure configurations is accomplished with network policy management tools (NPM) such as Tripwire Enterprise, Firemon, RedSeal and AlgoSec. Splunk software can support security configurations by identifying evidence of misconfiguration in log data, traffic on ports or from addresses that are unauthorized.

- Splunk software accepts regularly generated reports from any network policy management tools.
- By ingesting these data sources, a record of each device's security configuration is kept in Splunk software. This makes it easy for Splunk software to see changes between scans to identify new or different configurations.
- Splunk software can correlate NPM data with other data sources, such as a CMDB containing the compliance policy that a particular device should be configured against.
- By monitoring log files, Splunk software can assess the configuration of devices for evidence of misconfiguration.
- Splunk software can help provide evidence of systems not meeting standards. For example, if a network device suddenly has telnet enabled (determined by analyzing vulnerability management logs), then an alert or a notable event can be generated.

### Control 10: Using the Splunk App for Enterprise Security

- When a misconfigured network device is exploited, generally anomalous ports or traffic will be seen in the environment, which can be tied back to the unauthorized configurations. ES contains several correlation rules to look for this kind of behavior. Additionally, Traffic Center, Port and Protocol Tracker, Network Changes, Web Center and Time Center dashboards can all be used to display evidence of network devices that do not meet the secure configuration standards (see *Figures 23, 24* and *25*).

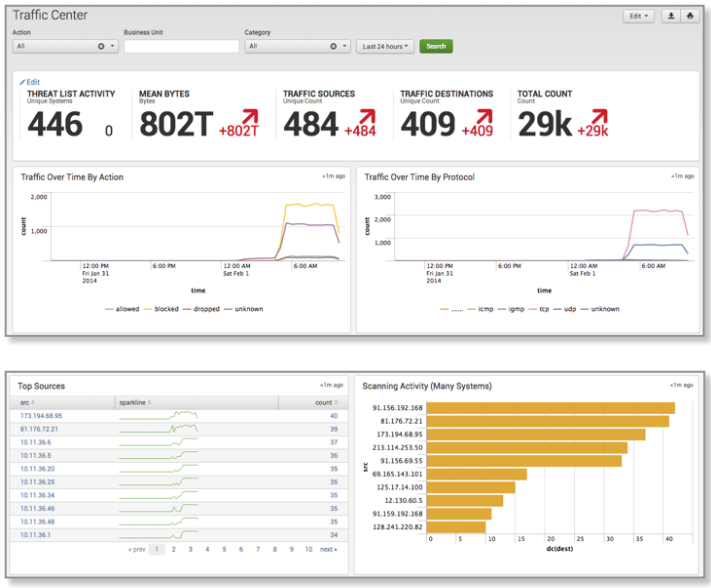


Figure 23. Splunk App for Enterprise Security: Traffic Center.

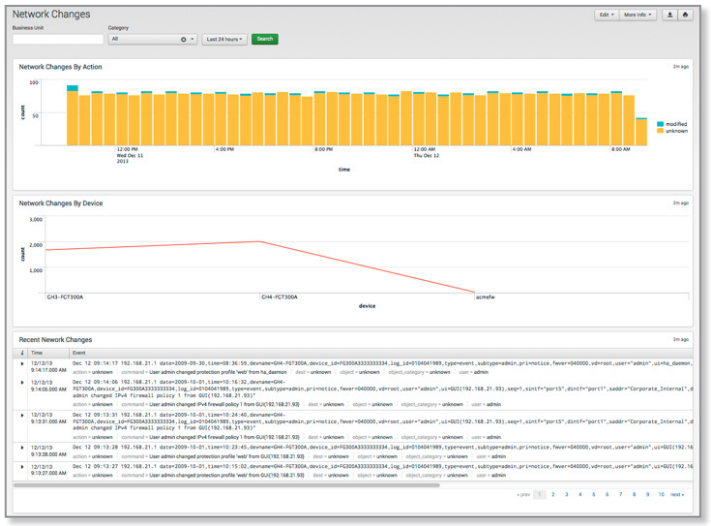


Figure 24. Splunk App for Enterprise Security: Network Changes.

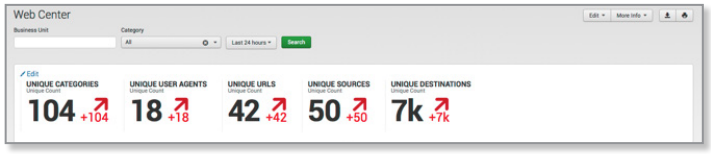


Figure 25. Splunk App for Enterprise Security: Web Center.

## Control 11: Limitation and Control of Network Ports, Protocols and Switches

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*
*Security Gateways, Proxies and Firewalls*

*Allow remote access only to legitimate users and services: apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.*

**Role of Splunk Software: Verification**

Limitation and control of network ports is primarily accomplished with discovery and vulnerability management tools such as Nmap, Nessus, RedSeal, Qualys and Nexpose.

- Splunk software accepts regularly generated reports from any discovery or vulnerability management tool. This data often includes descriptions of network ports and protocols found.
- Technical add-on or app support is provided for the following:
  - Splunk Add-on for Nessus
  - Nmap
  - Ncircle (Tripwire) IP360
  - Other VA/VM/discovery applications can easily be integrated into Splunk via log file and report ingestion.
- Once discovery and vulnerability data has been ingested, a record of each discovered protocol and port is kept in Splunk. As new data is ingested, Splunk software makes it easy to identify changes made between scans.
- Splunk software can correlate discovered port and protocol data with other data sources, such as a lookup table that contains a list of authorized ports or a maintained list of protocols that should not appear on the network.
- Splunk software can ingest converted network capture data from sources like NetFlow and PCAP data. The Splunk App for Enterprise Security supports v5 and v9 of NetFlow and captures data from Bro IDS. This data can also be analyzed for unauthorized ports and protocols.

### Control 11: Using the Splunk App for Enterprise Security

- ES contains various lookups, correlation searches and dashboards that can assist in detecting improper/unauthorized ports, protocols and traffic on your network.
  - ES contains two add-ons for network protection and threat intelligence. These add-ons include lookup files for application protocols, ports of interest and prohibited processes. Splunk software's correlation searches and dashboards consult these lists to determine whether ports, protocols and services seen in the environment are authorized or unauthorized. These lookups can be populated manually or automatically via an existing data source.
  - Correlation searches within ES that detect unusual or unauthorized network activity include, but are not limited to:
    - High Volume of Traffic from Critical Host
    - Network Change Detected
    - SANS Block List Activity Detected
    - Substantial Increase in Network Events
    - Substantial Increase in Port Activity
    - Unapproved Port Activity Detected
    - Unusual Volume of Network Activity
  - Dashboards specific to unauthorized port and protocol activity include Port and Protocol Tracker, Traffic Center, Network Center and three vulnerability dashboards.
  - Another dashboard that can be used to find anomalous network behavior is the Traffic Size analysis dashboard (see *Figure 26*). This finds connections with large byte counts per request, as well as devices with lots of connection attempts but small byte sizes. Unusual activity showing up on this dashboard can be indicative of data loss problems.

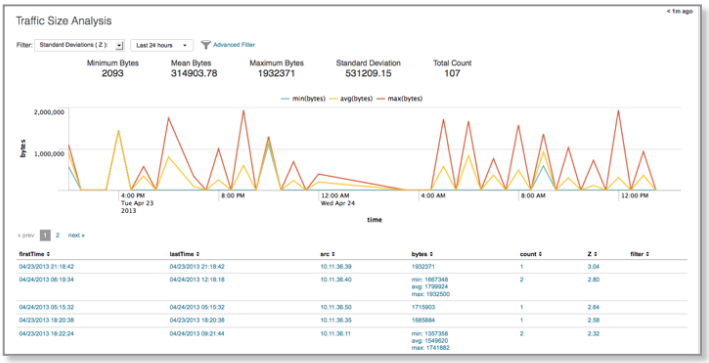


Figure 26. Splunk App for Enterprise Security: Traffic Size.

## Control 12: Controlled Use of Admin Privileges

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 5: User Access*
*Milestone 7: Baseline Management*

*Protect and validate administrative accounts on desktops, laptops and servers to prevent two common types of attack: (1) enticing users to open a malicious email, attachment or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

**Role of Splunk Software: Verification**

Controlled use of admin privileges can be accomplished with a number of toolsets that restrict the use of administrative accounts. The simplest methods are OS-level tools, like Sudo, and controls that can be put in place with vendor-supplied tools like Active Directory. There are also commercial applications that search for misconfigurations, such as enabled guest accounts, too-lenient Sudo configurations, and failure to rename administrative or default accounts.

- Splunk consumes authentication logs from across the technology environment that detail account activity, including how accounts are being accessed and from where. Authentication logs come from, but are not limited to: host devices, domain controllers, directory servers, network devices, Radius, TACACS, application logs and many others. All of this machine data will be ingested into Splunk software for searching and correlation.
- Any use of known administrative accounts like "Administrator" and "root" and "sa" can easily be searched across the entire environment and reported or alerted upon.

### Control 12: Using the Splunk App for Enterprise Security

- ES provides a pre-built dashboard that tracks "default account" usage across common default accounts for hosts, network devices, databases and more. Default accounts should be disabled as a standard practice, or at least have their passwords changed (see *Figure 27*).

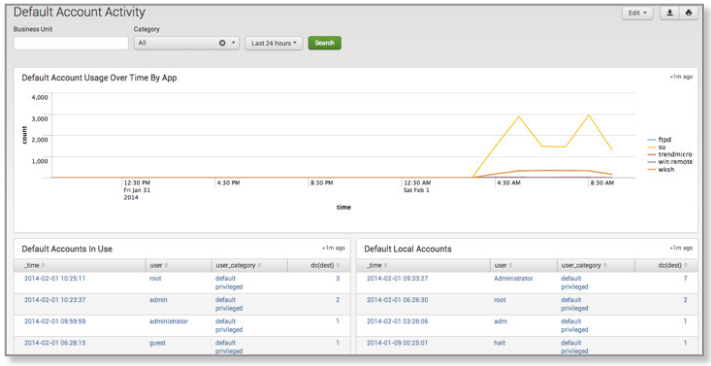


Figure 27. Splunk App for Enterprise Security: Default Account Activity.

## Control 13: Boundary Defense

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*
*Security Gateways, Proxies and Firewalls*
*Remote Access Security*
*Network Security Monitoring*

*Control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines: establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks and other network-based tools. Filter inbound and outbound traffic, including traffic through business partner networks ("extranets").*

**Role of Splunk Software: Confirmation**

Boundary defense can be accomplished with properly configured firewalls augmented with intrusion detection and prevention systems (IDS/IPS). Common firewall vendors include Cisco, Palo Alto, Fortinet and Checkpoint. Common IDS/IPS include managed next-gen firewalls, HP TippingPoint, Snort, Sourcefire and FireEye.

- Firewalls and IDS/IPS produce vast amounts of log data that Splunk can easily ingest. Most commonly, this data arrives at Splunk in the form of syslog data, but some firewalls, such as Checkpoint, have proprietary logging mechanisms that Splunk software can also use. There are a number of free apps available on apps.splunk.com that support common firewall vendors including Cisco, Palo Alto and Fortinet.
- IDS/IPS is supported by free technology add-ons and apps as well. Apps and add-ons are available for FireEye, Snort, Sourcefire, TippingPoint and others. Furthermore, if a device or application can get log data into Splunk software in some way, an add-on or app is not necessary.
- Proxy servers, such as BlueCoat, also generate a significant amount of log data that can be consumed and analyzed by Splunk software to get a good feel for an organization's web traffic.
- Splunk software can analyze traffic for possible exfiltration to dump servers or communication with command and control machines (C&C machines), which are often registered with new, transient domain names. Control 17 covers this in further detail.

### Control 13: Using the Splunk App for Enterprise Security

- ES normalizes all machine data coming from firewalls, proxy servers and IDS/IPS against the Splunk Common Information Model, which standardizes field names across the data, even if it came from multiple vendors. From there, Splunk software can use the common field names to drive correlations, alerts and searches on the data. Dashboards within the Splunk App for Enterprise Security that are driven from firewall, IDS/IPS and proxy data include Traffic Center (previously mentioned), Intrusion Center (see *Figure 28*), Intrusion Search and Web Center (previously mentioned).

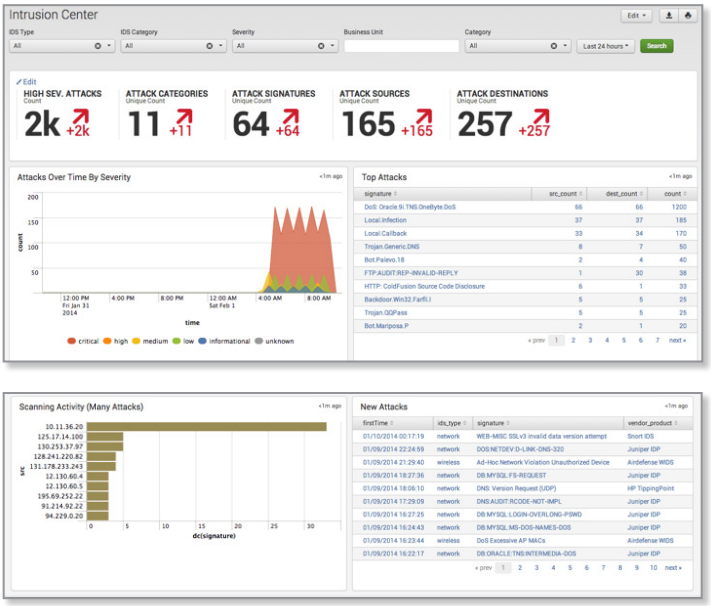


Figure 28. Splunk App for Enterprise Security: Intrusion Center.

## Control 14: Maintenance, Monitoring and Analysis of Audit Logs

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Remote Access Security*
*Log Management*

*Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed and activity on victim machines: generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses and other information about each packet and/or transaction. Store logs on dedicated servers and run biweekly reports to identify and document anomalies.*

**Role of Splunk Software: Execution**

Maintenance, monitoring and analysis of audit logs are a core competency of Splunk software. The Splunk platform consumes logs from any source within an enterprise architecture, regardless of the format, frequency or volume, and safely and efficiently indexes the data into a series of centralized, high-performance flat files. The indexed data is immediately searchable, reportable and can be alerted upon to any number of security investigators in an organization.

- Log data can be delivered to Splunk software in flat-file format, Windows Event Logs, syslog, direct REST API ingestion and a multitude of other methods.
- Logs can be delivered in a compressed and optionally encrypted manner.
- Tools are provided to ensure the security and tamper-proof nature of the centralized log store.
- Splunk software allows the security investigator to apply security and audit logic at will, with options for real-time or historical modes.
- Security and audit logic can be converted into reports, alerts, dashboards, feeds and actions—for example, creating an incident in a security workflow system.
- Logs can be analyzed in full fidelity and can be kept as long as necessary, provided you have the disk space—there is no data "rollup," so you do not lose any granularity.

### Control 14: Using the Splunk App for Enterprise Security

- ES provides a Data Protection dashboard that verifies that ingested log data, and the resulting correlated notable events, have not been tampered with (see *Figure 29*).

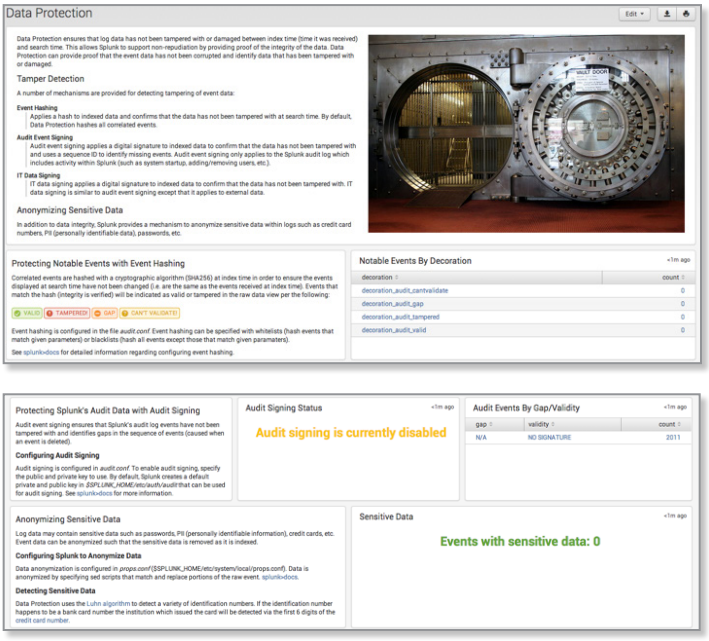


Figure 29. Splunk App for Enterprise Security: Data Protection.

## Control 15: Controlled Access Based on the Need to Know

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*

*Prevent attackers from gaining access to highly sensitive data: carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.*

**Role of Splunk Software: Verification**

Controlled access based on the need-to-know is primarily the domain of enterprise access management solutions, such as those from vendors like HyTrust, Vormetric, CyberArk, IBM, Oracle and Microsoft.

- Splunk ingests authentication logs from all systems to determine who is signing into which applications and where access is taking place. Object (usually file, registry or database) access auditing logs are also ingested in Splunk software, which can then correlate across the data to report on who is rightfully (and wrongfully) accessing sensitive information.
- Correlation can be done against usernames seen in the data and directory servers and CMDB to determine whether a user should have access to data, based on an established classification scheme.

### Control 15: Using the Splunk App for Enterprise Security

- As previously mentioned, ES contains an Identity Center and Asset Center. This functionality allows Splunk administrators to map assets and identities to business units and categories. ES then correlates any activity seen back to these assets and identities so the security investigator can tell at a glance whether a particular identity should be accessing a particular asset.
- ES also contains two interactive data visualization tools called Asset Investigator (previously mentioned) and Identity Investigator that allow the security investigator to view an asset and all notable events that have occurred surrounding that identity or asset over time (see *Figure 30*). Information available from external sources is also brought into this view to provide business context, such as the business unit.


Figure 30. Splunk App for Enterprise Security: Identity Investigator.

## Control 16: Account Monitoring and Control

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 5: User Access*

*Keep attackers from impersonating legitimate users: review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

**Role of Splunk Software: Verification**

Account monitoring and control is generally accomplished with identity management solutions and the proper use of built-in authentication mechanisms.

- Splunk software ingests authentication logs from all systems to determine who is logging into which applications and where access is taking place. Splunk software can then correlate across the data to report on when accounts are being used that are not on a whitelist. Other interesting correlations include being able to determine:
  - Whether multiple accounts are accessing data all using one IP address
  - Whether an account that belongs to an "expired" user is being used
  - Whether an account that has long been dormant is suddenly showing activity
  - Whether new accounts are being used to access critical resources
  - Whether accounts are being used to access critical resources that are associated with users that have had a change in life status (marital, death in family) or that have been placed on a performance plan or termination list

### Control 16: Using the Splunk App for Enterprise Security

- ES contains several correlation searches that are directly applicable to this control (see *Figure 31*), including:
  - Activity from Expired User Identity
  - Completely Inactive Account
  - Inactive Account Activity Detected
- ES contains the Account Management dashboard, which allows the security investigator to see overall account management activities across the environment (see *Figure 32*).
- ES contains the Access Tracker dashboard, which helps monitor and correlate user activities across multiple user names often prevalent in organizations without a single-sign-on (SSO) solution.

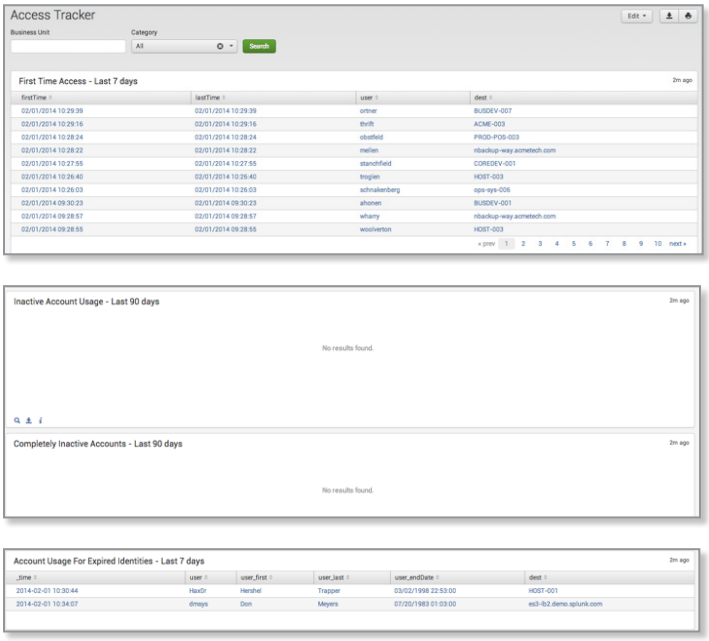


Figure 31. Splunk App for Enterprise Security: Access Tracker.

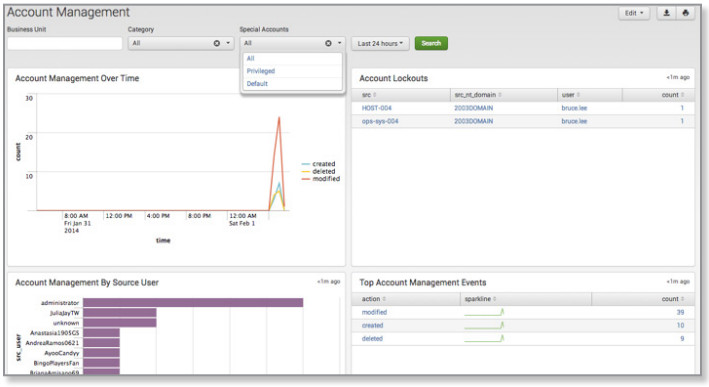


Figure 32. Splunk App for Enterprise Security: Account Management.

## Control 17: Data Loss Prevention

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Personal Electronic Device (PED) Management*
*Data-at-rest Protection*
*Network Security Monitoring*

*Stop unauthorized transfer of sensitive data through network attacks and physical theft: scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes and systems using a centralized management framework.*

**Role of Splunk Software: Verification**

Data loss prevention (DLP) is generally accomplished by a DLP system (for electronic monitoring) with surveillance methods and physical security measures for physical monitoring. However, DLP solutions are not a panacea. Proprietary information crossing from one internal host to another on the same network segment is not detectable if DLP has been implemented at the perimeter. Host-based DLP can be remotely disabled by malicious code in a BYOD environment. This may go undetected outside a corporate network.

- By ingesting firewall logs, proxy logs and flow data (usually via syslog and a dedicated flow collector), Splunk software has a good picture of the overall traffic flows inside and outside of the organization's network boundaries. Once this data is ingested, it can be analyzed in an automated fashion for such anomalous behavior as:
  - New or rare addresses or communication to unauthorized geographies
  - New or rare ports appearing in the traffic patterns
  - A critical host sending out lots of data when it normally doesn't
  - Host communicating with a host listed within a threat list
  - Host communicating with a recently registered DNS domain
- Splunk software automatically extracts source, destination and port information, as well as byte counts where available. If the Splunk App for Enterprise Security is set to ingest flow and packet data, Splunk software can provide even more detail for network traffic data searches.
- Splunk software can help investigators understand the scope of a data leakage.
- Splunk software can watch for the usage of removable media via standard host log file and registry monitoring, and alert or report when removable media is detected.
- The Splunk platform can consume data concerning physical security systems, such as motion detectors, pressure pad sensors, proximity badge access logs and other "non IT" sources of data to provide insight into user location and time of access. This information can be correlated with other data within Splunk—for example, an authorized employee badges into a secure area and then accesses systems outside of the secure area.

### Control 17: Using the Splunk App for Enterprise Security

- ES includes various correlation searches that are directly applicable to Control 17 and can assist in finding attempts to exfiltrate data, such as:
  - High Volume of Traffic from High or Critical Host Observed
  - Substantial Increase in Network Events
  - Substantial Increase in Port Activity
  - Unusual Volume of Network Activity
- ES includes several dashboards that can help detect data loss, including Traffic Center, Traffic Search and Traffic Size, as well as New Domain Analysis (see *Figure 33*).

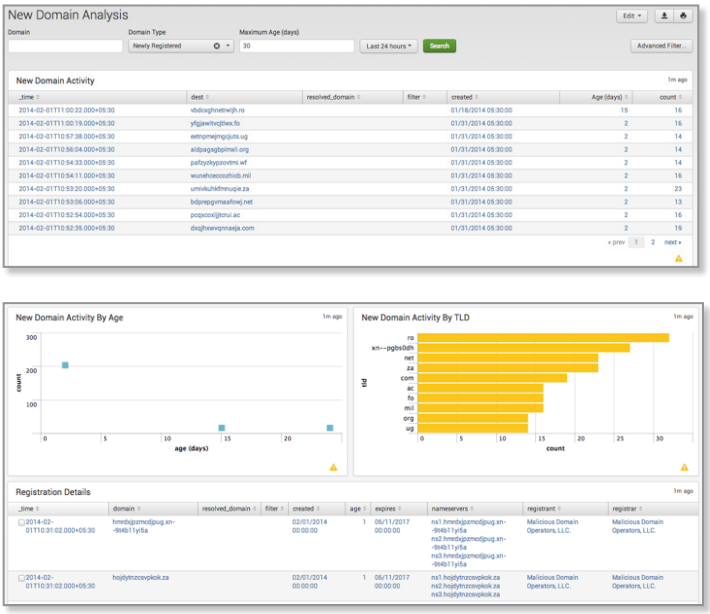


Figure 33. Splunk App for Enterprise Security: New Domain Analysis.

## Control 18: Incident Response and Management

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Incident Response and Disaster Recovery Plans*
*Training*

*Protect the organization's reputation as well as its information: develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence and restoring the integrity of the network and systems.*

**Role of Splunk Software: Support**

Incident response and management are focused on policies and procedures that are instituted in your organization, rather than a direct technical requirement. However, during an incident, it is important to be able to quickly detect the incident, get to the root cause and respond.

- Splunk software's ability to quickly search through mountains of security and non-security related data and apply business context to it is invaluable when time is of the essence and false positives cannot be tolerated.
- Security professionals need to have all data at their fingertips when investigating an incident. By having all of the information centralized and searchable, Splunk software allows individuals and teams to respond quickly and accurately, limiting the organization's exposure.

### Control 18: Using the Splunk App for Enterprise Security

- There are a number of dashboards and visualizations within ES, highlighted throughout this document, that can be viewed in real time, instantly providing feedback to security professionals during an incident.

## Control 19: Secure Network Engineering

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*

*Keep poor network design from enabling attackers: use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy network architecture with at least three tiers: DMZ, middleware and private network. Allow rapid deployment of new access controls to quickly deflect attacks.*

**Role of Splunk Software: Support**

Secure network engineering is about a philosophy of design and does not have a direct technical requirement.

- Splunk software can ingest data from the various tiers of the network, such as vulnerability scans. While each portion of the network will have a different set of security requirements, Splunk software can correlate the results of the scans against known network tiers to provide an overview of the security posture for each tier.
- By correlating data from network and vulnerability scans with traffic analysis, Splunk software can help to identify insecure network design. Examples include:
  - Workstations being used to send e-mail directly
  - Workstations using unusual or unauthorized protocols
  - Workstations or servers that expose MAC addresses known to be associated with virtualization software
  - Rogue access points
  - Rogue DHCP servers

### Control 19: Using the Splunk App for Enterprise Security

- ES provides a lookup function to define whitelists/blacklists for network ports and services. Correlation searches provided within ES can leverage those lists to determine when unauthorized ports and services are seen in the environment.

## Control 20: Pen Testing and Red Team Exercises

***Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls***
*CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)*
***Associated NSA Manageable Network Plan Milestones and Network Security Tasks***
*Milestone 3: Network Architecture*

*Use simulated attacks to improve organizational readiness: conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.*

**Role of Splunk Software: Support**

Pen testing and red team exercises are meant to ensure that your organization is prepared to respond in the case of an attack. These exercises do not have a direct technical requirement.

- During penetration tests, Splunk software gives team members significant information about the environment. Splunk software provides deep granularity into real-time and historical (often a year or more is available online for instant searching) data. Using this data, pen testers/red team members can better plan a target list or create new target lists from dashboards such as Traffic Analysis.
- During pen testing and red team activities, Splunk software can display the status of any successful or failed breach attempts.
- Accounts associated with successful or failed breach attempts found during pen testing and red team activities can be fed back into Splunk software to understand how the account has been used historically.

### Control 20: Using the Splunk App for Enterprise Security

- ES contains Asset Center and Identity Center capabilities, where known information about assets and identities is centralized into a series of lookup tables. Pen testers and red team members can use this information after activities are carried out to understand which assets or identities are of high value to the organization.

# Conclusion

Throughout this document, we have shown how Splunk software can assist your organization with executing requirements confirming or supporting activities surrounding each of the Top 20 Critical Security Controls. The Splunk platform is a flexible and versatile solution and plays an integral role in protecting your organization from known, advanced and emerging cyber threats.

Splunk Enterprise is a software-based solution that can be up and running within minutes in your organization, allowing you to index, explore and analyze your security data like never before. For more information, please contact your local Splunk sales team, or email us at sales@splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.apps.splunk.com

splunk> listen to your data™

www.splunk.com



Item # EB-Splunk-Top20Security-106