splunk>

TECH BRIEF

USING SPLUNK® FOR CDM AND CMAAS

Under the Continuous Diagnostics and Mitigation (CDM) Tools and Continuous Monitoring as a Service (CMaaS) program, the Department of Homeland Security (DHS) envisions a comprehensive risk and security management solution for deployment across the U.S. federal government landscape. The solution will consist of 15 functional areas. Each functional area may be fulfilled by any number of commercial, open source or custom applications and systems.

The level of visibility required to deliver risk intelligence, reporting and other capabilities across the federal government will require vertical and horizontal integrations of numerous solutions. To deliver true continuous monitoring capabilities, a solution in the CDM tool portfolio must provide the means to aggregate, visualize and alert on data from all sources. Splunk Enterprise is enterprise-class software that natively provides these capabilities and much more.

Splunk Software's Value in CDM/CMaaS

Splunk Enterprise is uniquely positioned to deliver key functionality for CDM/CMaaS while greatly reducing the overall risk assumed by CDM/CMaaS prime contractors.

Splunk has identified three major value areas for integrator teams seeking CDM/CMaaS program success:

1. The integration of all point systems across all technology domains
2. Delivery of category-specific capabilities or enhancement of existing CDM solution sets
3. Comprehensive analytics and intelligence capabilities to address emerging requirements

The Platform for Machine Data

Splunk Enterprise is the platform for machine data. Splunk software enables the collection, indexing and correlation of any text-based data source, regardless of the manufacturer. Splunk software is built upon a schema-on-the-fly technology that enables the collection of heterogeneous machine data without the need for connectors, adapters or parsers. This eliminates the traditional upfront data normalization and scalability constraints associated with a backend database. Once data is collected and indexed, Splunk software provides the means to easily search across extremely large data sets using the comprehensive Search Processing Language (SPL®). SPL enables users to create real-time alerts, conduct advanced statistical reporting and create data visualizations on machine-generated data.

The aggregation of machine data, such as server and security events, network device logs, configuration data and credentialed user activity, enhances existing network and security operations and continuous monitoring systems, enabling the automation of many common alerting and reporting tasks. Splunk software provides the definitive record of activity and behavior across all categories in the operational environment (see Figure 1). This allows agencies to

Figure 1. Splunk software provides the record of activity across operational environments.

identify trends, troubleshoot and perform root cause analysis that would be practically impossible to piece together from a conglomeration of individual tools.

Splunk software alleviates the risk, time and cost associated with developing custom connectors and serves as a platform that regulates and unifies data from a diverse array of solutions.

Splunk software's real-time architecture delivers indexing and search capability at a speed and degree of scalability that cannot be cost-effectively obtained using legacy relational database applications. This architecture makes Splunk Enterprise the ideal platform for providing comprehensive security posture reporting across all data sources, including integration with legacy and custom developed applications.

In this way, the Splunk platform serves as the "glue" that enables the integration of the various solutions that comprise the CDM functional areas. It enables agencies to organize and analyze massive amounts of data generated by these solutions to achieve true continuous monitoring.

Beyond Splunk software's core functionality, hundreds of Splunk apps are available at no additional cost. These apps provide searches, dashboards and other functionality for third-party technologies. All apps certified to run on Splunk Enterprise version 6.X are compatible. Apps should also be considered part of an ecosystem that allows you to create your own specialized dashboards. Splunk apps reduce deployment time and result in a faster time-to-value.

The Splunk REST API, SDKs and web framework enable integrators to leverage or integrate Splunk software as part of a custom solution (see Figure 2). The REST API, for example, provides a method for every feature in Splunk Enterprise. Integrators can use the API to make applications, phone apps, widgets and other projects that interact with Splunk software.

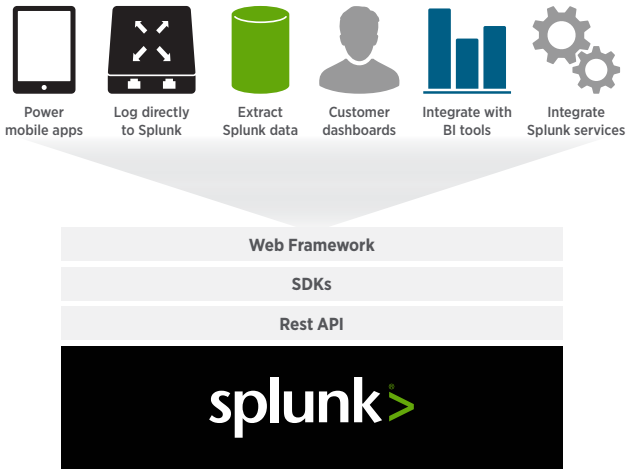


Figure 2. Splunk product architecture.

Extensible Architecture

While this document does not explore the components of a Splunk deployment, nor provide architectural guidance, the scope and breadth of the CDM program necessitates the use of scalable, extensible and open solutions. Splunk software provides integrators with unmatched architectural flexibility and granular control (see Figures 3 and 4). Splunk software is able to scale vertically, horizontally and is well suited for multi-data center deployments.

Details on Splunk solution architecture may be found in the Distributed Deployment Manual.

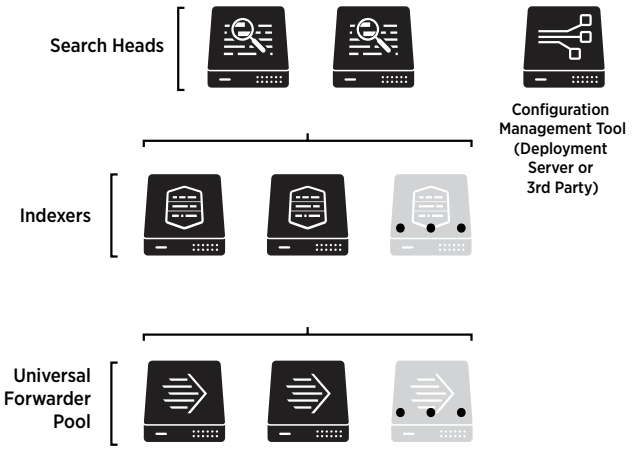


Figure 3. Splunk's three architecture tiers.

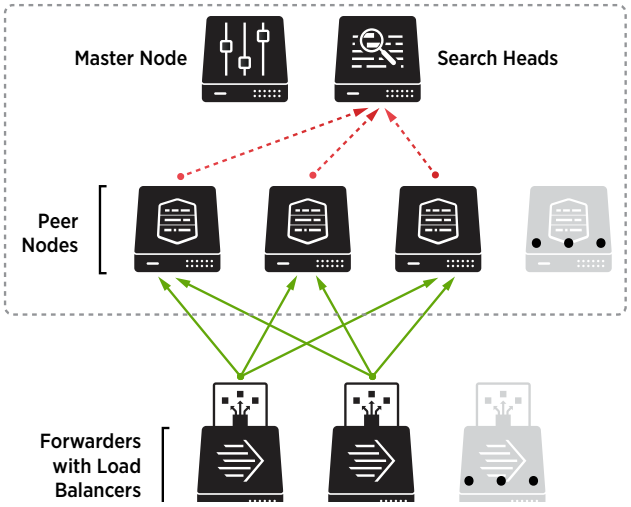


Figure 4. Scaling the Splunk architecture.

Splunk Value by CDM Functional Area

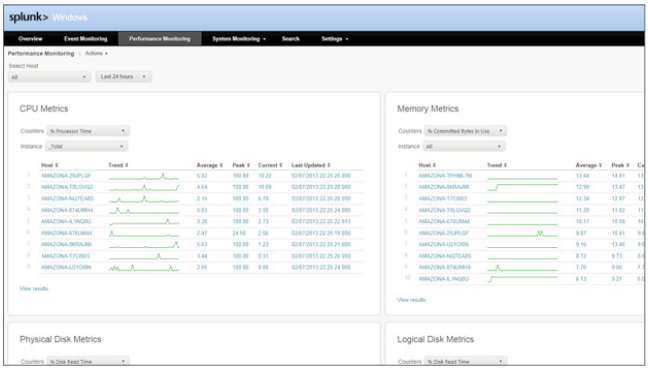
Splunk delivers compelling value for integrators and agencies by enhancing commodity point products or incumbent solutions that may not meet requirements or objectives. While Splunk software is able to integrate all the tools across CDM functional areas, below are examples of how it applies to the categories identified in GSA's RFQ #GSC-QF0B-13-32662.

Hardware Asset Management, Software Asset Management, Configuration Management

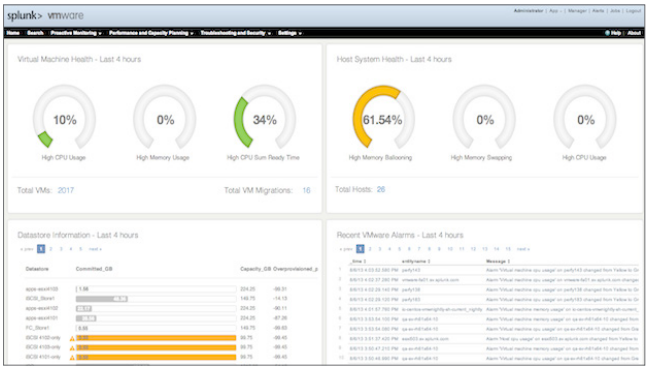
CDM Functional Areas 1 - 3

Splunk software can collect asset information from Active Directory (AD), enterprise configuration management databases (CMDB), management systems, network scanning tools, and configuration management identified as functional areas 1, 2 and 3 respectively.

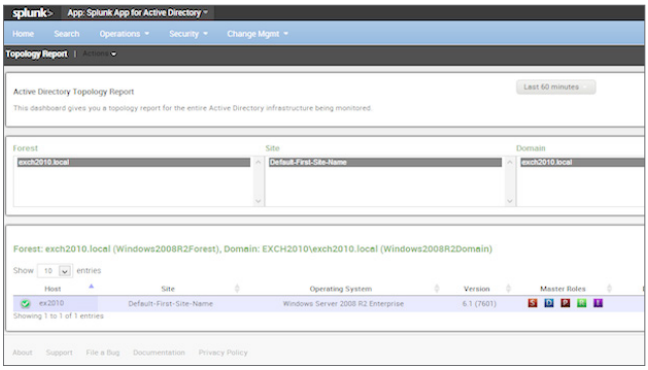
Splunk software will integrate with any hardware or software configuration management system that is part of an integrator's CDM solution or an agency's incumbent toolset (see example screenshots at right). One example of this capability is the ability to ingest more than 163 log files generated by Microsoft SCCM and its modules. Splunk software will correlate and visualize file system changes, security policy modifications, network access, system health and faults relating to the SCCM deployment itself.



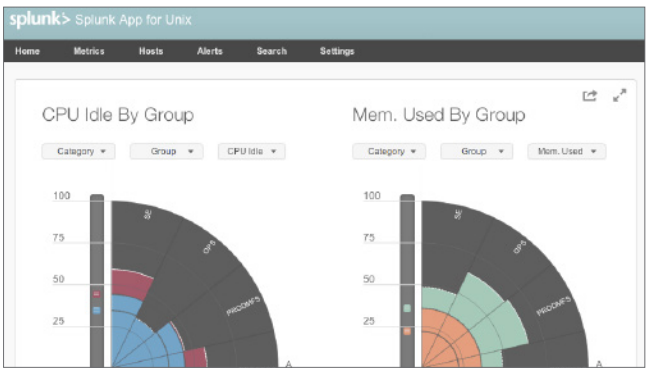
Splunk App for Microsoft Windows



Splunk App for VMware



Splunk App for Microsoft Windows Active Directory

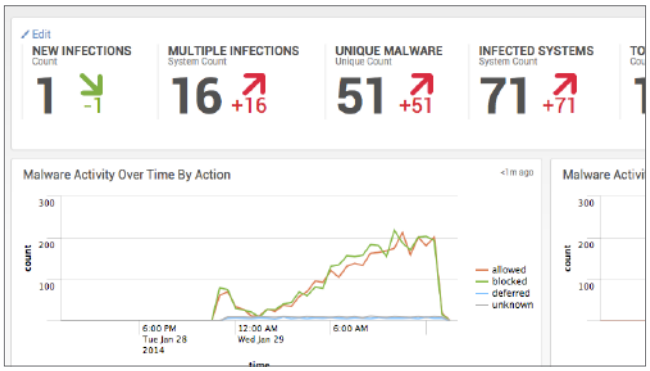


Splunk App for Unix and Linux

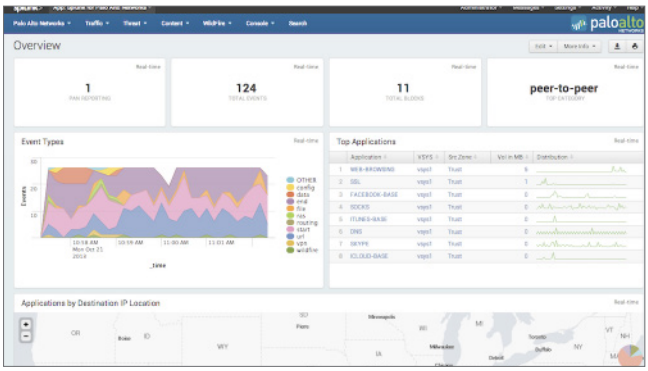
Vulnerability Management

CDM Functional Area 4

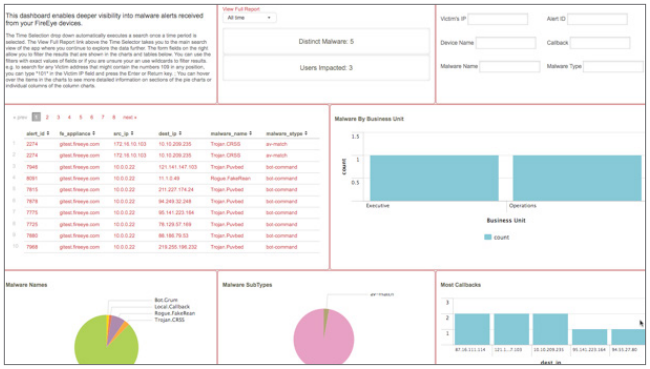
Output from vulnerability scanning solutions can be ingested by Splunk software to provide a comprehensive view of risk across IP-addressable assets. Using SPL, security professionals can quickly search through assets, asset network activity, intrusion and firewall activity, and any open vulnerabilities on the assets that might make them targeted for exploitation (see example screenshots below).



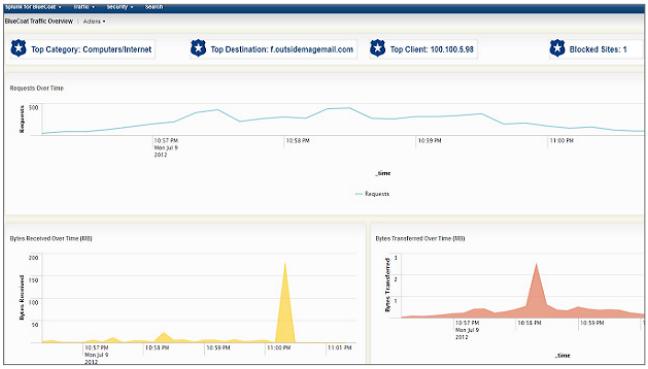
Splunk Enterprise Security



Splunk App for Palo Alto Networks



Splunk App for FireEye



Splunk App for BlueCoat ProxySG

Manage Trust in People Granted Access, Manage Security Related Behavior

CDM Functional Areas 6 - 7

Through correlation of identification, authentication, authorization and accounting (IAAA) data, as well as other network-based activity, Splunk software can monitor for and alert on difficult-to-detect malicious insider activity. Splunk software supports IAAA across AD infrastructures, workstations, email systems and other sources to allow identification of a single user identity across multiple online nomenclatures such as email addresses, LAN accounts and social media profiles.

Splunk identity correlation will capture and log attempted access across a multitude of platforms and network devices, tracking unwanted users in the network with multiple repeated login failures, unauthorized access attempts and inappropriate privilege escalation. By monitoring use of credentials across multiple domains and authorization granted to those credentials, Splunk software ensures that identities on the network are who they claim to be and are only accessing resources to which they are entitled. Splunk Enterprise Security Identity Center dashboard (see Figure 5) expedites reporting on these and other dimensions of IAAA.

Splunk software indexes every field, word, character (including punctuation) and whitespace of the data it ingests. By analyzing the patterns of data, trends in network and host access behaviors, an analyst can quickly identify activity and patterns that lie outside of the norm and drill down to the original source events for corroboration and additional granularity (see Figure 6).

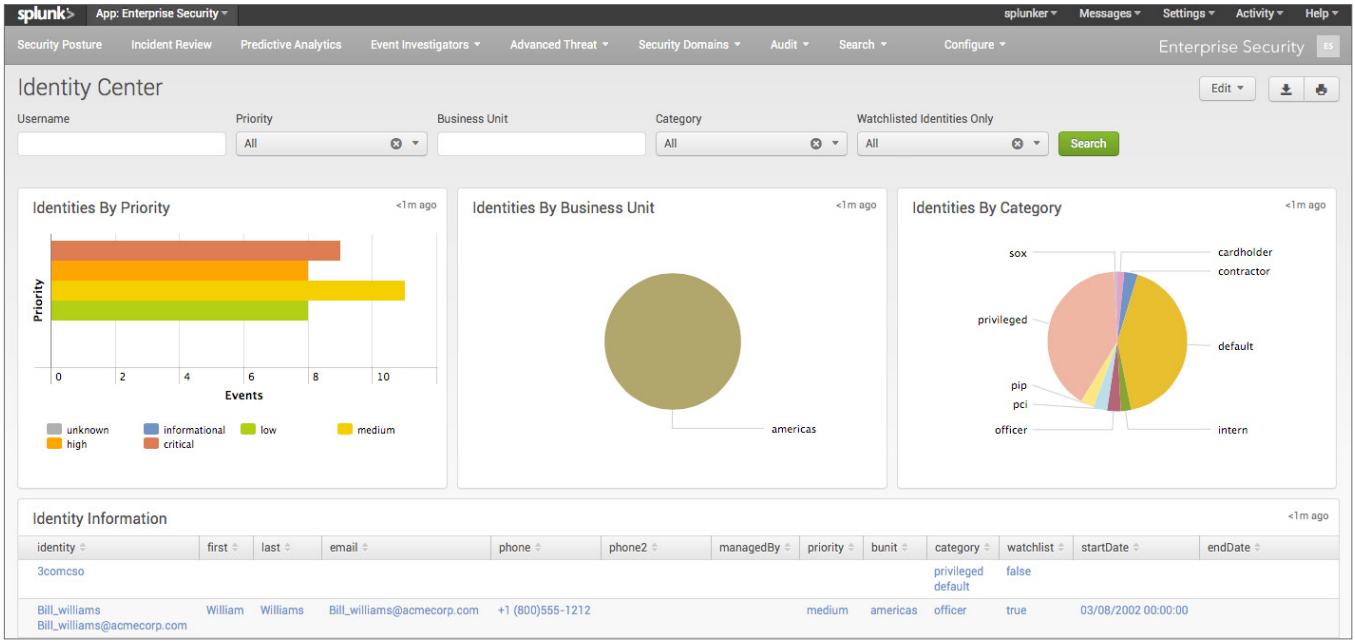


Figure 5. Splunk Enterprise Security – Identity Center dashboard.

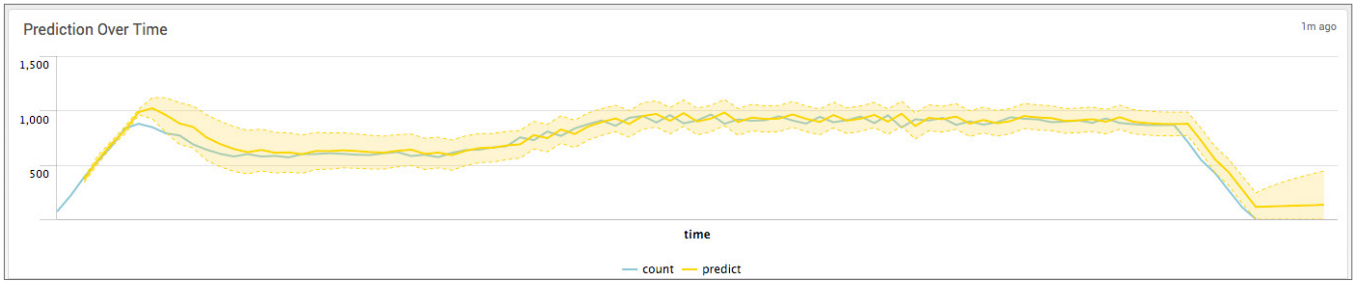


Figure 6. Sample visualization of Splunk predictive analysis

Prepare for Contingencies and Incidents, Respond to Contingencies and Incidents

CDM Functional Areas 10 - 11

Incidents can be identified through real-time alerting and tracked throughout the network and hosts regardless of operating system, platform or other logical boundaries. If a device's data is being collected by Splunk software, it becomes a contributor to the investigation and can be accessed from a single search interface (see Figure 7). Splunk software can integrate with existing help desk and incident reporting systems to automatically open incident tickets and automate the workflow of responding to an incident event, allowing mitigating actions to take place before information has been compromised.

Splunk software's pattern detection and historical trending capabilities, coupled with the collection and indexing of other rich data sources, make it a valuable resource in the incident handler's toolkit. Analysts are no longer required to visit multiple management interfaces and log repositories for each of the many network and security systems found in the enterprise. Splunk software includes a single interface that provides access to all indexed information sources, spanning all enterprise systems.

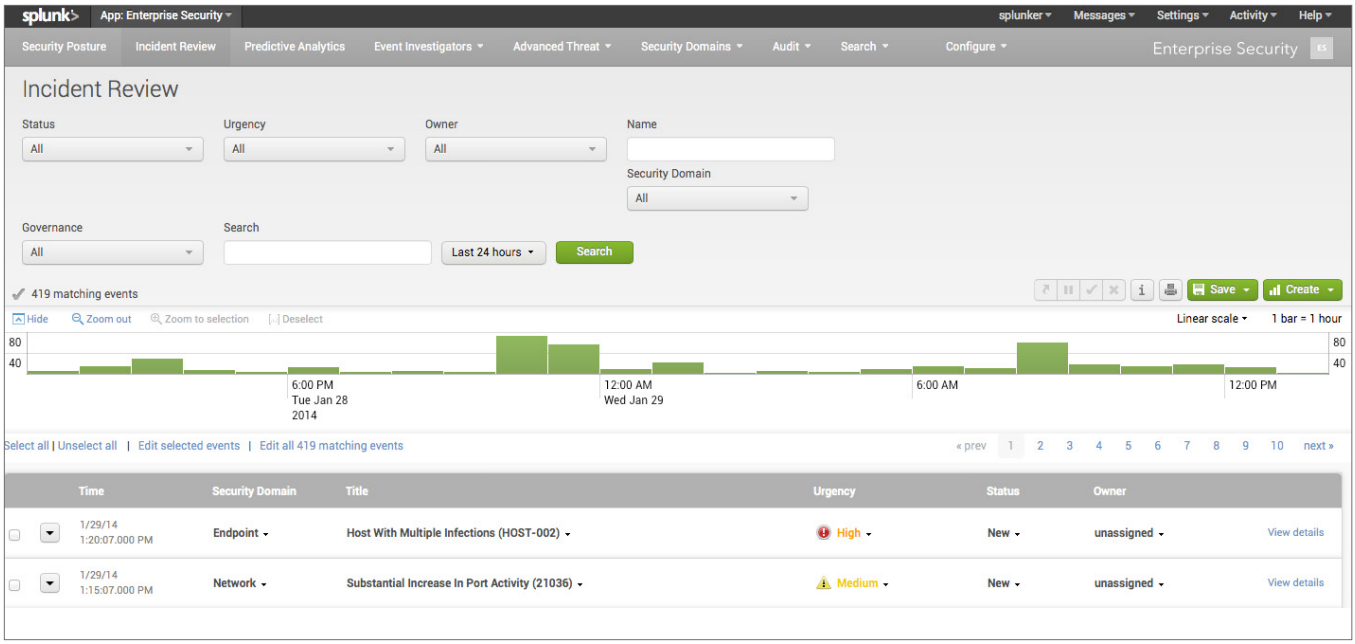


Figure 7. Splunk Enterprise Security – Incident Review dashboard.

Manage Audit Information

CDM Functional Area 14

Splunk software collects and indexes the machine data generated by almost every device and platform on the network, making auditing of events quick and efficient (see Figure 8). It provides a consistent interface and experience across all tiers of the infrastructure and offers a single location to examine all audit logs, including both real-time and historical events.

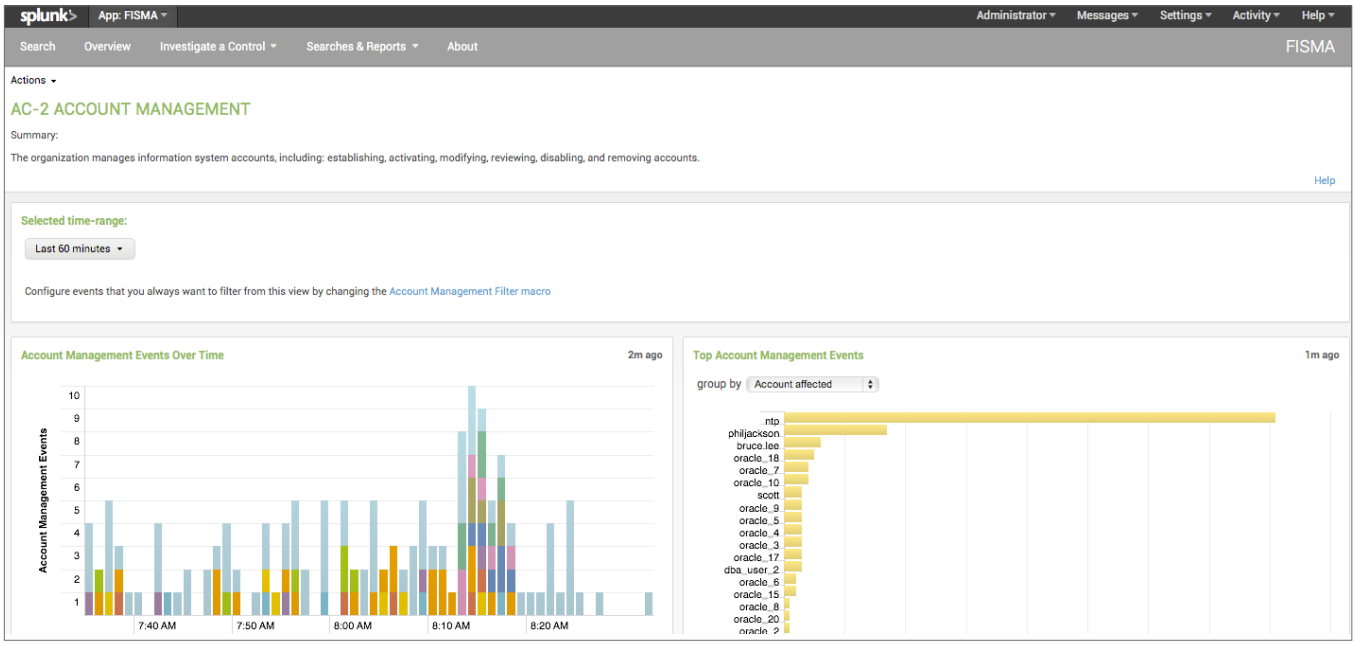
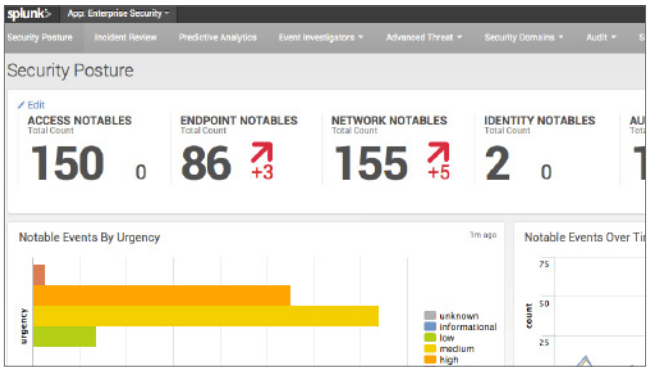


Figure 8. The Splunk App for FISMA supports compliance and auditing requirements.

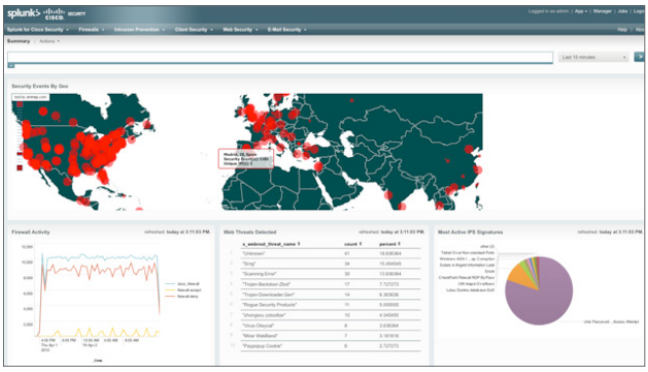
Manage Operation Security

CDM Functional Area 15

Splunk software's core strength is the ability to consume large volumes of machine data and make it accessible and usable by all communities of interest within your agency. It generates reports that are valuable to security analysts and executives alike. Splunk software excels at the collection, correlation, visualization and analysis of data from a myriad of sources within the enterprise environment.



Splunk Enterprise Security



Cisco Security Suite

Thousands of public and private sector enterprises rely on Splunk products to improve security, increase efficiencies, make data-driven decisions and gain tactical and strategic advantages. Learn more.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com