Splunk for Risk Management Framework

Assessing and Monitoring NIST 800-53 Controls

"...Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence and business operations..."

— The National Strategy for Cyberspace Operations, Office of The Chairman, Joint Chiefs of Staff, U.S. Department of Defense

In 2014, the Department of Defense (DoD) issued instructions that replaced DoD Information Assurance Certification and Accreditation Process (DIACAP) with the Risk Management Framework (RMF). The RMF is designed to be managed as a continual process as the risk posture evolves over time for each information system.

Step 1: Categorize

Categorize the information system and the information processed, stored and transmitted by that system based on an impact analysis.[1]

Step 2: Select

Select an initial set of baseline security controls for the information system based on the security categorization — tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.[2]

Step 3: Implement

Implement the security controls and document how the controls are deployed within the information system and environment of operation.

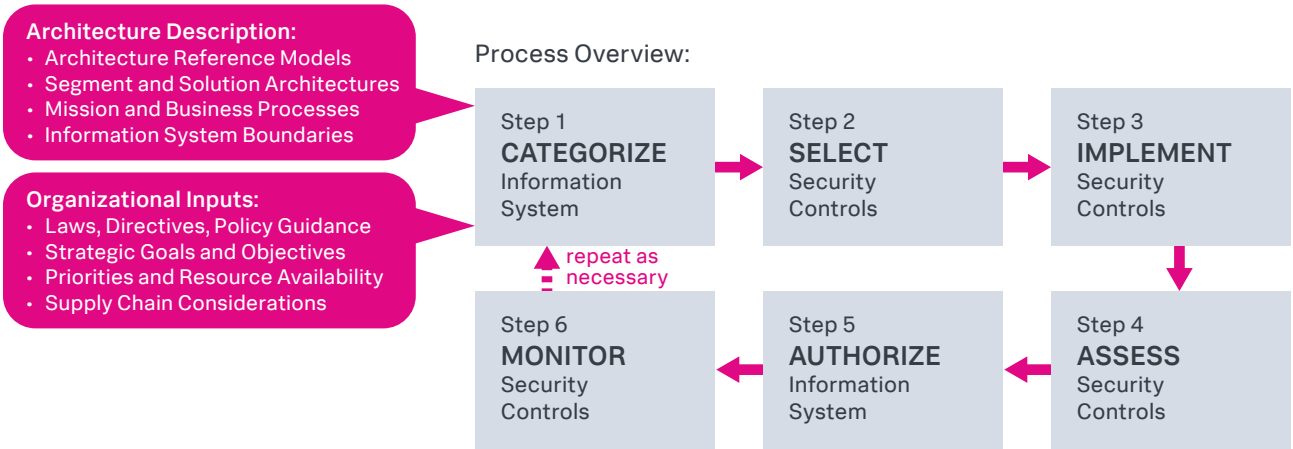
Step 4: Assess

Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Step 5: Authorize

Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the nation resulting from the operation of the information system and the decision that this risk is acceptable.

Risk Management Framework



1. FIPS 199 provides security categorization guidance for non-national security systems while CNSS Instruction 1253 provides similar guidance for national security systems.

2. NIST Special Publication 800-53 provides security control selection guidance for non-national security systems. CNSS Instruction 1253 provides similar guidance for national security system.

Step 6: Monitor

Monitor and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes and reporting the security state of the system to appropriate organizational officials.

Enter Splunk

The RMF process is carried out as a set of well-defined, risk related tasks by individuals or groups with well-defined roles within the organization. Splunk® can be leveraged to assist agencies in facilitating and enabling their RMF process, specifically with Steps 4 (Assess) and 6 (Monitor).

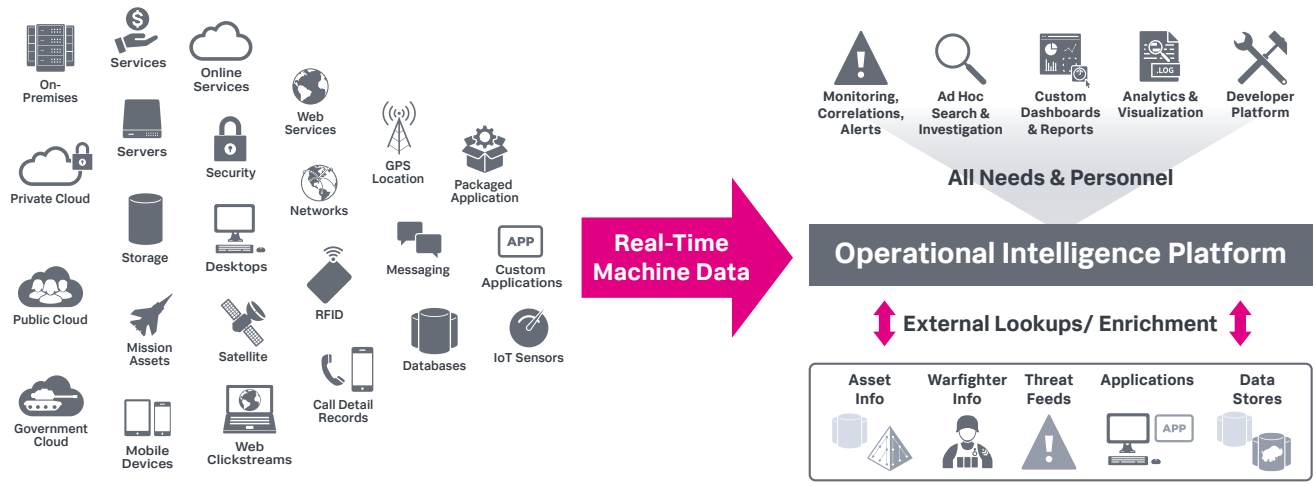
Splunk is a cost effective, flexible and integrated solution that can help meet a variety of compliance requirements and beyond. Some of the ways Splunk helps meet mandates include:

- Continuous monitoring of security controls and their effectiveness
- Audit trail collection and reporting
- Determine acceptability of security controls in terms of risk levels
- Enable assessment of implementation and effectiveness of controls
- Collect, retain, search, alert and report on logs from all assets and activities

Splunk ensures public sector agencies have access to their data, can interpret them and ensure agency transparency. Audits are made much simpler with quick generation of reports and dashboards that offer an instant, real-time view into implementations and their effectiveness.

Splunk is unique in that it collects machine data from any source and any format across the enterprise and has it available for search and analysis through a single intuitive interface with powerful visualization features. Machine data contains a definitive record of all the activity and behavior of your users, citizens, transactions, applications, servers, networks, mobile devices, sensors and more. And it's more than just logs. It includes configurations, data from APIs, message queues, call detail records and sensor data. Some key capabilities of Splunk that helps promote and ease the adoption of RMF includes:

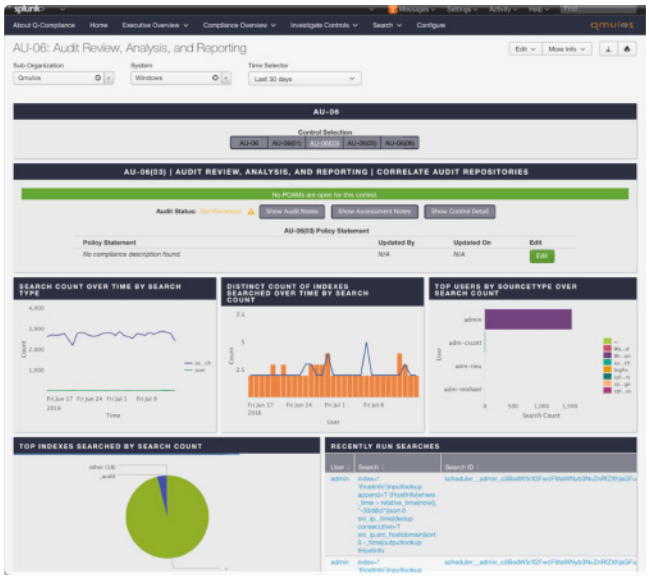
- Ability to ingest data volumes ranging from megabytes to petabytes per day
- Reliably collect and index machine data, from a single source to tens of thousands of sources – regardless of type or format
- Real-time end-to-end visibility cutting across information silos through a single interface
- Search and analyze across all your data – with powerful search technology
- Powerful reporting and visualization capabilities



After an agency has implemented their security controls, they need to determine acceptable risk levels. Splunk can collect the machine data from these various security controls to help assess risk as well as provide a single location for all data-centric security.

Once a system has been authorized, monitoring of the security controls needs to happen on a continual basis. This is a core competency of Splunk and due to the iterative nature of RMF, continuous monitoring is necessary. Automated tools to streamline this approach is looked upon favorably as well, and Splunk can provide automation for collecting, monitoring and alerting of machine data.

With Splunk, you can meet requirements to automate monitoring of security events. Index audit trails across firewalls, applications, access control, IDS and other components, then simply save, schedule and set alerting rules for a search. Alerts can send notifications via email, RSS, SMS or trigger scripts for easy integration with your existing monitoring consoles. As new mandates create new monitoring requirements, simply add new data sources and searches.



Splunk Assessment of Mitigation Implementations (SAMI)

In order to counter cyberthreats and help agencies under its purview adopt sound threat mitigation strategies and enhance their security posture, the NSA's Information Assurance Directorate (IAD) has issued a list of Top 10 Information Assurance Mitigation strategies. In order to ensure that agencies are implementing these strategies correctly and effectively, the IAD has built an app using Splunk — SAMI — Splunk Assessment of Mitigation Implementations. The goals of SAMI are:

- Evaluate implementation of mitigations using machine data
- Track progress deploying mitigations through continuous monitoring
- Track and report security posture
- Identify configuration drift
- Identify specific actions to improve security posture

SAMI monitors data related to the implementation of specific mitigations and returns prioritized recommendations. The application can be used to determine a network's mitigation implementation status and can be monitored over time to demonstrate improvements and identify changes that negatively impact mitigations. Desired actions mapped to findings can give a course of actions to mitigate issues. Since different mitigation actions require different measures, this makes it much easier from an implementation perspective.

With the Splunk platform, governments can gain the visibility and intelligence to lower costs, improve security, streamline IT operations and ensure compliance and better serve the public. **Learn more**.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

2020-Splunk-PF-Splunk-for-risk-management-framework-104-TB