splunk>

TECH BRIEF

# SPLUNK AND THE CYBERSECURITY FRAMEWORK

In response to Presidential Executive Order 13636, NIST worked with the private sector to develop the **Framework for Improving Critical Infrastructure Cybersecurity.** It references industry standards and best practices to manage cybersecurity risks. The framework can be used to strengthen an existing risk management program or be used as a guide to establish one.

## The Framework

The framework is a risk based approach and has three parts. The *Core* specifies a set of functions and categories that map to informative resources to achieve certain desired outcomes. The *Profile* represents outcomes based on business needs, risk tolerances and resources. An organization would determine its current profile (or state) based on the degree of adherence to the Core activities and put in measures to achieve a target profile (or state). *Implementation* Tiers provide a mechanism for organizations to view and understand their degrees of adherence to and maturity against the framework.

The Framework Core identifies five functions (see *Table 1*), each with specific activities across categories, which when considered together provide a high-level strategic view of the organization's risk management lifecycle.

- **Identify:** enables understanding of the business context, the resources that support key functions and related risks so efforts can be focused and prioritized accordingly
- **Protect:** provides guidance on the safeguards necessary to limit or contain the impact of a potential security event
- **Detect:** details the appropriate activities to identify, in a timely fashion, a cybersecurity event should it occur

| Unique Identifier | Function | Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Management |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Stragegy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness & Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies & Events |
| | | DE.CM | Security Continuous Monitorring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |

*Table 1 – Framework Core*

- **Respond:** encompasses the activities to counter a cybersecurity event and contain its impact once it is detected
- **Recover:** details the actions necessary to restore and remediate services that may have been impacted by the event

Not all organizations will have the same profiles or functional categories to focus on implementation tiers. This is due to a variety of risk tolerances within agencies and will vary based on the context, business environment and other characteristics that define their mission goals. The goal of the framework is to help the organization reduce risk and be cost effective by first understanding its

current state and maturity towards a target profile, which are defined across four tiers – from *Partial (Tier 1)* to *Adaptive (Tier 4)*. While *Tier 1 (Partial)* organizations exhibit informal and ad-hoc risk management processes, *Tier 2 (Risk Informed)* organizations have an awareness of risk but lack organization-wide policies to manage it. Risk management practices in *Tier 3 (Repeatable)* organizations are more formalized with consistent methods in place to respond effectively. Last, *Tier 4 (Adaptive)* organizations engage predictive indicators, are agile, and risk management is engrained in their culture.

## State of Federal Agencies

Risk management is a continuous process and dictates the ability of an organization to respond to an event that can adversely impact the organization. Federal Agencies are very familiar with risk management processes, having been mandated to demonstrate compliance with NIST 800-53 SP4. Depending on the agency, this could be FISMA or RMF. Demonstrating compliance can be challenging given the tedious data collection requirements, disparate and heterogeneous technologies strewn across the agencies, lack of real-time visibility into systems and inability to customize and scale to organizational needs. For effective risk management, information sharing and collaboration are critical to creating end-to-end views so leadership can observe what is transpiring across the agency's systems, determine any deviations or non-compliance and take necessary action quickly.

## The Splunk Platform

Splunk is a cost effective, integrated yet customizable solution that can help meet an agency's objective in employing the NIST Cybersecurity Framework. It can provide the visibility to help assess your current profile,

### SOLUTION REQUIREMENTS

"The most effective way to implement the risk management guidance per the Cybersecurity framework is a solution that can meet real-time data collection, monitoring and reporting requirements across the infrastructure and organizational processes. At its core this solution should be:

**Flexible:** Must offer the capability to mirror the organizational profiles based on the framework including representation, in real-time, of alignment with desired outcomes

**Scalable:** Must account for growth, including the ability to quickly incorporate new activities, users and processes

**Central Management and Federated Access:** Must provide centralized management through a single pane-of-glass to ensure consistent, easy management and self-reporting and organization-wide access to stakeholders through role-based access control

**Data Source Agnostic:** Must quickly interface with any and all data sources required to monitor, assess and meet risk management requirements

**Extensible:** Must provide the ability to enable measures to move up the implementation tiers (towards desired target states) as the organization matures and accommodate measures to enhance information protection against any and all threats— internal and external—and extend ROI.

**Real-Time Architecture:** Must aggregate log data and other relevant information from across the agency in real time to achieve accurate situational awareness and alert on deviations from desired outcomes or states

**Customization:** Must be able to query and build inquisition mechanisms and visualizations based on stakeholders needs and a changing environment to effect quick decisions."

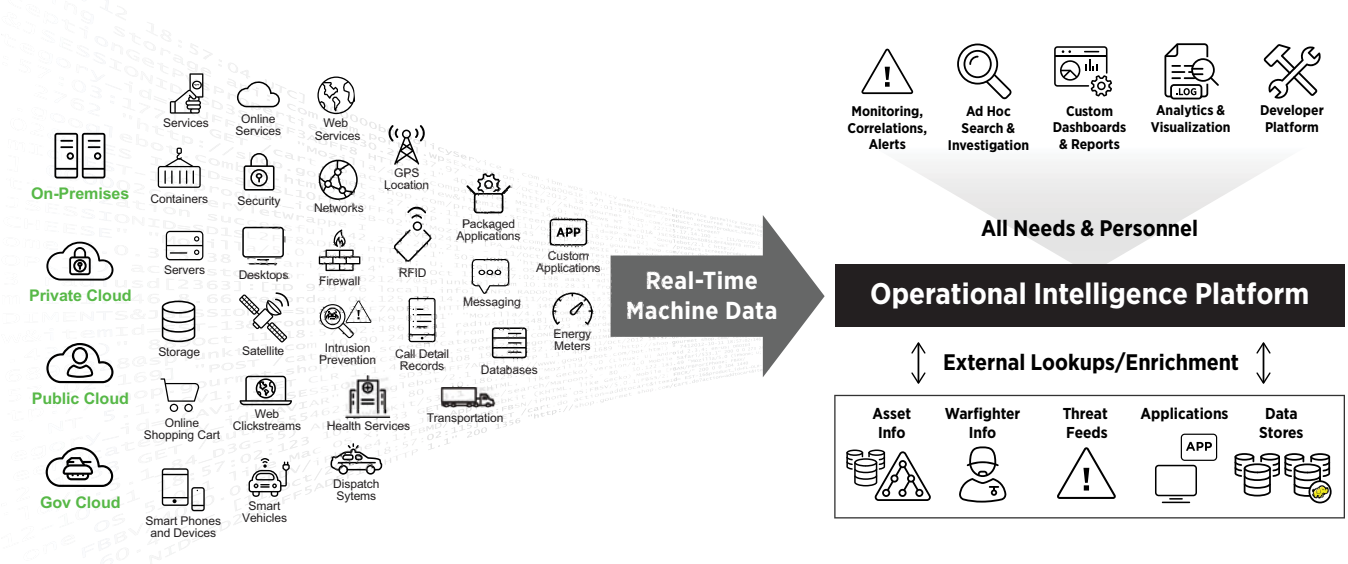
*Table 2 – Solution Requirements*

continuously monitor events and metrics, and deliver real-time visualizations and dashboards across the organization for fast and informed decision making to manage risk effectively.

Some of the ways Splunk helps meet the Framework guidance include:

- Collecting asset inventory data including physical devices, software platforms and applications assisting with building profiles
- Deploying role-based dashboards and visualizations to communicate risk posture, activity status and outcomes across the organization from executive to operational levels
- Monitoring access control and user behaviors (internal and external) to detect any abnormal or unauthorized activities
- Monitoring network and data flows to detect potential cybersecurity events
- Detecting anomalies and events to provide contextual enrichment for prioritization and alert stakeholders to take corrective action
- Continuously monitor security controls and their effectiveness to determine adherence to the Framework and maturity against Implementation Tiers
- Collecting audit data and providing self-reporting capabilities
- Collecting, aggregating and correlating event data from multiple sources and sensors to assist in determining acceptability of activities in terms of Implementation Tiers

Splunk is a leader in compliance and security solutions with proven success helping agencies meet CDM, RMF and FISMA requirements. Its extensibility, scalability and flexibility have assisted many agencies to monitor their compliance requirements and ease audits while enhancing an organization's overall security posture. And Splunk's unique capability as a platform to ingest data once and make it available across the agency, enables users to go beyond just the Framework – comply with other mandates, enhance security posture and solve other mission challenges.




Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com