



ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: Establish a new Logging and Vulnerability Management category within the Software Factory (SWF) Utility framework and designate Splunk as the Enterprise Standard utility for this category

Approved by the VA Chief Architect (OIT/OCTO) on March 2024

Context

Splunk has served as the enterprise standard for logging and vulnerability management since the initial set of utilities was identified in 2024, and this ADR documents that designation.

Splunk is a software tool widely used for monitoring, searching, analyzing, and visualizing machine-generated data in real time. This tool captures, indexes, then correlates data in a searchable container and produces graphs, alerts, dashboards and visualizations.

Decision

Establish Logging and Vulnerability Management as a category under the Software Factory Utility framework and designate Splunk as the Enterprise Standard utility for this category. Splunk provides a powerful platform for searching, monitoring, and analyzing machine-generated data in real-time, thereby supporting incident response, security monitoring, and operational insights.

Rationale

Splunk's robust log management and analysis capabilities are critical for maintaining operational excellence and ensuring security. Its scalability, real-time data processing, and integration with existing VA systems make it an ideal choice. By consolidating log management onto Splunk, the VA can reduce complexity, enhance security posture, and improve incident response times.

Impact(s)

- Update TRM to add a new product category "Logging and Vulnerability Management" and add "Splunk" as a utility.
- Inform relevant teams of this recommendation to ensure necessary changes to pages are made upon approval.



Architecture and Engineering Services (AES)
Office of the Chief Technology Officer (OCTO)
Office of Information and Technology (OIT)

- No direct technical or system-level impacts are anticipated aside from TRM updates.

For questions or further clarification, contact the Enterprise Architecture team at ea@va.gov.

Sam Kaldawi
Chief Architect
Office of the Chief Technology Officer (OCTO)

**Disclaimer: The Architecture and Engineering Services (AES) team's recommendation in this ADR is provided solely as architectural guidance. It does not imply AES ownership of operational support, licensing, or cost responsibilities for a recommended tool. These responsibilities remain with a designated operational owner(s) within VA.*

This ADR does not establish a recommended tool as the sole solution for the defined use case. Other tools that meet VA requirements may continue to be used or evaluated as part of VA's enterprise technology strategy.