AvMC Splunk Factsheet

What is Splunk?

Splunk software provides you with a platform that enables agencies to monitor, search, correlate, analyze, and visualize large amounts of data.

Splunk is an advanced technology which searches any machine data captured from any system, app, or other data source. The industry leader for IT Operations and IT Security, Splunk has also many mission focused uses and it does not suffer from the same legacy shortcomings of similar technologies that use SQL or relational databases, manual connectors or limited data import controls.

Splunk can be leveraged to assist AvMC 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

What kinds of questions can Splunk help answer?

IT Operations

How do I provide more transparency around IT operations to customers and better predict service-level degradation before they impact mission?

Application Performance Analytics

Is poor app performance due to code-level errors or infrastructure? Where are the integrations between my app and other centralized IT components (e.g. network, Active Directory, etc.)

Security and Compliance

How can I augment security investigations to be more efficient and effective and reduce the impact of insider threats?

Mission Analytics

Can I use data to drive my mission decisions, improve business intelligence, and empower better decision-making.

AvMC Splunk Products and Services

Products & Services	Description	Notes
Splunk Enterprise (Core) w/ Standard Support Entitlements	700 GB / Day, Term	1-Term Year
Splunk Fundamentals Part 1 and Part 2 (Free for all Veterans & Active Duty)		Free Training Splunk Fundamentals 1: https://www.splunk.com/en_us/training/courses/splunk-fundamentals-1.html Splunk Fundamentals 2: https://workplus.splunk.com/veterans

Splunk Success Program	Description
Splunk Dedicated Customer Success Associate	Dedicated agency advocate and business advisor, responsible for helping customers define use cases, drive adoption, realize value, and overcome obstacles with Splunk
Splunk OnDemand Services	10 Credits / quarter. Remote consultative services to support platform or specialty IT Ops, IT Security needs.
.conf Event Passes	Passes for .conf Event & Splunk University
Splunk Standard Support	https://www.splunk.com/en_us/support-and-services/support-programs.html

Splunk Workshops	Descriptions
Security Lunch and Learn: (January 21st) • This modular, hands-on workshop is designed to familiarize participants with how to leverage Splunk to search security events. This workshop provides users a way to gain familiarity with searching in Splunk, as well as a introducing a set of commands that allow a user to effectively exam their security events.	

AvMC Splunk FAQs

What is in the AvMC Splunk Enterprise License? What's included? How do I access it?

The Enterprise License includes 700GB of average daily data ingestion per day (in aggregate for the entire organization).

Who is responsible for distributing the license? What options do AvMC customers have for accessing the license? How is the license cut?

At this time, the CIO/G6 is managing the Enterprise and all license requests. Please reach out to the below POCs via email with Subject line "ATTN: Splunk License"

Current POCs for the Splunk Enterprise License:

Software Asset Manager:
William Mellgren
Phone: 256.336.2083
william.p.mellgren.ctr@mail.mil

IT Asset Management (ITAM) Program Manager:
Kenny Duff
Office: 256-336-1928
kenneth.a.duff.civ@mail.mil

Splunk team: devcomavmc@splunk.com

If a group wants to leverage Splunk, how will CIO/G6 support requests for specific program dashboards, additional Splunk apps, assistance with Splunk searches, and data ingestion issues?

In the short term, the best way to accomplish this goal would be for a given program to purchase their own Splunk professional services.

Additional details on obtaining Splunk professional services via the can be found below.

https://www.splunk.com/en_us/support-and-services/splunk-services/offerings/implementation-services.html

https://www.splunk.com/en_us/support-and-services/splunk-services/offerings/adoption-services.html

How much does Splunk cost?

Example costs associated with operating an individual Splunk instance include Splunk software license, infrastructure (physical or virtual machines), and trained resources who can admin and operate the Splunk platform.

In FY20 AvMC signed an Enterprise License Agreement for Splunk license. This ELA provides anyone in AvMC a single acquisitions vehicle for procuring Splunk software licenses and benefits all with discounts through bulk purchasing economies of scale. More details on the Enterprise License (including a cost calculator to obtain your own Splunk license for your own Splunk instance) can be provided by the G6 Contacts.

Where can I find introductory or general Splunk help ?

Splunk Lantern Knowledge Base - https://lantern.splunk.com/hc/en-us

Can Splunk operate in the cloud?

Yes, Splunk has been FedRamp certified at the Moderate impact level

https://www.splunk.com/en_us/newsroom/press-releases/2019/splunk-cloud-attains-fedramp- authorization.html

Are there release notes for the latest Splunk Version 8.x?

https://docs.splunk.com/Documentation/Splunk/8.0.0/ReleaseNotes/MeetSplunk

Where can I get general Splunk Answers to my questions?

https://community.splunk.com/t5/Community/ct-p/en-us

Where can I download Splunk Apps and Essentials?

https://splunkbase.splunk.com/

Where do I find out more about .conf events?

https://conf.splunk.com/

Splunk Huntsville User Group

https://usergroups.splunk.com/huntsville-splunk-user-group/

Once I get a license, where can I get Support?

https://www.splunk.com/en_us/support-and-services/support-programs.html

Will Splunk solve all my problems?

I can't believe you are still reading this document. The answer is some. Maybe a lot. Not all.

What Other Capabilities does Splunk Have?

Enterprise Security (SIEM) – Splunk Enterprise Security is the nerve center of the cybersecurity ecosystem, giving teams the insight to quickly detect and respond to internal and external attacks, simplify threat management minimizing risk. ES helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk.

IT Service Intelligence – Leverage machine learning, adaptive thresholds, and mission and business oriented Key Performance Indicators to created service models that visualize an entire tech stack or provide real-time predictive insights into an entire ecosystem. Create a platform for true operational intelligence.

Phantom – A security orchestration, automation and response (SOAR) platform designed to help organizations dramatically scale their security operations. With Phantom, you can automate tasks, orchestrate workflows and support a broad range of SOC functions including event and case management, collaboration and reporting.

User Behavior Analytics (Insider Threat) – A machine learning-driven solution that helps organizations find hidden threats and anomalous behavior across users, devices and applications. Its data science driven approach produces actionable results with risk ratings and supporting evidence, augmenting Special Agents and Intelligence Analysts' existing techniques.

AIOps/Machine Learning – Is the practice of applying analytics and machine learning to big data to automate and improve IT operations. AI can automatically analyze massive amounts of network and machine data to find patterns, both to identify the cause of existing problems and to predict and prevent future ones.

Splunk Lantern - A knowledge base lights the way with comprehensive guidance for any use case, any task, and any objective. Search for help with a specific scenario or requirement you are faced with or browse the categories below for ideas on how you can benefit from your data. Everyone in your organization from the CEO to a novice incident responder, case agent and intel analyst.

Who do I contact at Splunk if I need help?

Program Manager	Tim O'Toole	M: 703-477-9950 Email:totoole@splunk.com	Contract Governance, software pricing, professional services engagement
Inside Program Manager	Alicia Campos	Email:aliciac@splunk.com	
Senior Engineer	Ray Cruciata	M: 407-314-0456 Email:rcruciata@splunk.com	Pre-sales technical advisement, product demos
Customer Success Advisor	TBD	TBD	Post-sales advisement & adoption, Admin on Demand engagement, Splunk Success Framework, enablement planning, best practices
Support	Open a Support Case	1-855-775-8657 (P1) Splunkcommunities.force.com (P2,P3,P4)	
Admin On Demand	Engage Through PM (Tim O'Toole)	Task based admin assistance	Build Dashboards Build a lookup Create a drilldown Create workflows Data on-boarding assistance More info: Splunk.com/Aod
Professional Services	Engage Through PM (Tim O'Toole)	Project based and advanced services	Implementation Customer Configs Compliance Analytics App Premium App installation More Info: https://www.splunk.com/en_us/support-and-services/splunk-services.html

Learn more about Splunk by contacting devcomavmc@splunk.com