splunk> turn data into doing

PROFESSIONAL SERVICES

Splunk Security Prescriptive Value Path Offering

The Splunk Security Maturity Methodology (S2M2) - Prescriptive outcomes for your Security Operations

- Prescriptive outcomes delivered by Splunk expert Consultants to achieve success, with flexibility to meet your needs
- A recommended sequence to achieve value in your environment
- Aligned with the right resources for the right tasks

Many customers wish to deploy defined outcomes based on years of experience and best practices delivered to our customers. Splunk Professional Services Expert Consultants have the expertise to deliver outcomes after initial implementation. Splunk has identified 8 primary categories that align with the **Splunk Security Maturity Methodology (S2M2)**. This is designed to meet the ever changing needs of businesses along their security Journey and help them progress up the Maturity Ladder.

Splunk Security experts have global experience building and maintaining security programs and Security Operations Centers (SOC). Our experts are trained to help you accomplish your goals, grow your expertise, increase your security maturity and security posture while using the Splunk Security Suite (Enterprise Security + Security Analytics + Phantom). This offering is designed to layer the right type of services to meet your needs.

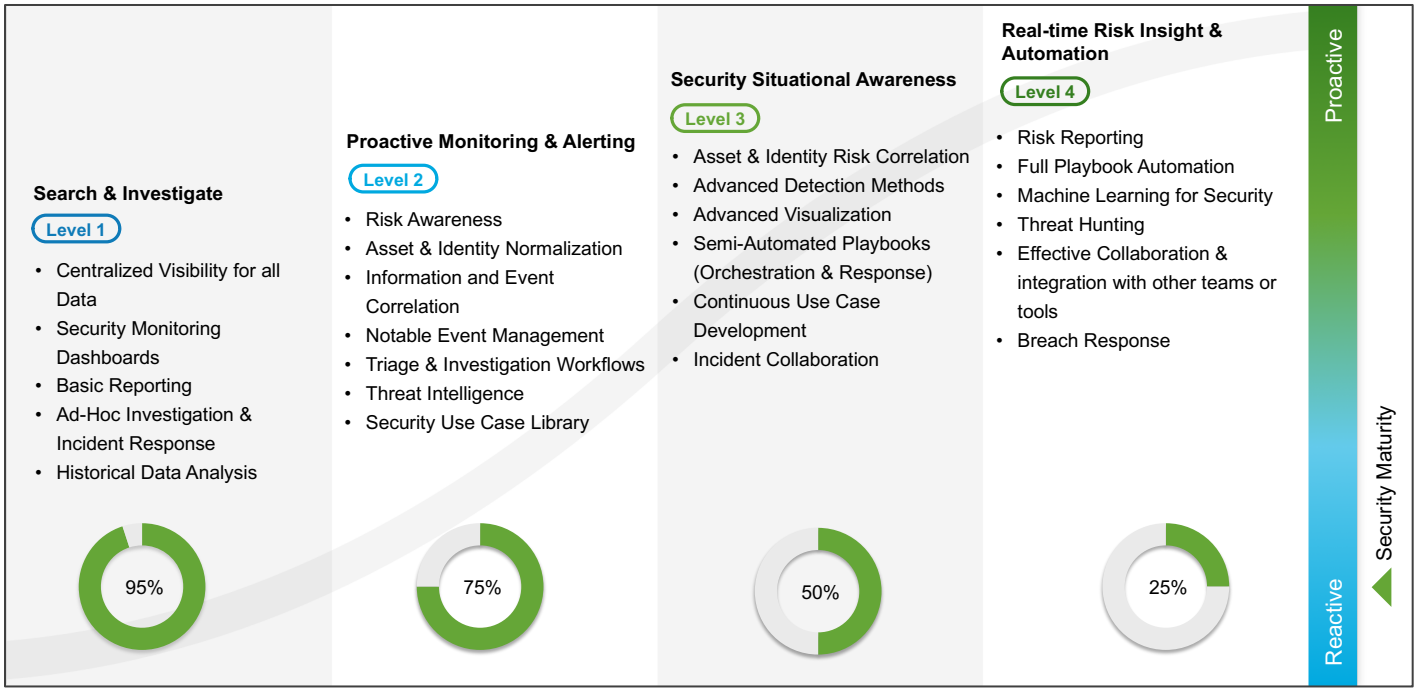
Prescriptive Value Path

Leveraging the experience from thousands of Splunk deployments, the Splunk Security Prescriptive Value Paths will quickly bring you to your desired level of maturity. The customer journey begins by discussing what the customer's objectives with their security program are. We then align the operational requirements, compliance regulations, i.e. constraints into the requirements and then using the Splunk Security platform to determine the current capabilities of the customer in terms of observability and visibility into their security environment with People-Process-Technology.

Splunk has created a proprietary methodology that assesses your organizations Security Maturity in regard to our Security Suite across 8 categories and from a basic Maturity Indicator Level (**MIL1**) through a more advance Maturity Indicator Level 4 (**MIL4**). The categories that we asses against are: Security Monitoring, Advanced Threat Detection, Incident Investigations and Forensics, Insider Threat Detection, SOC Automation, Incident Response, Compliance and Fraud Detection.

Different Levels for Different Outcomes

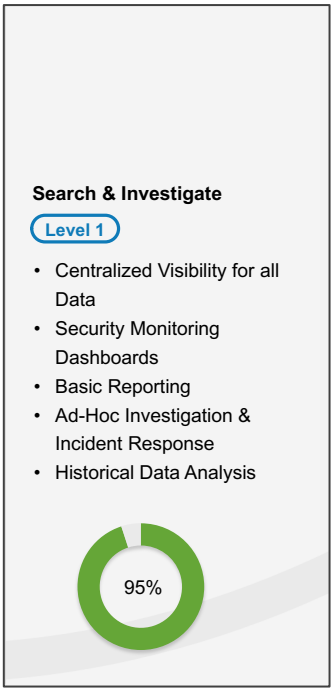
We realize that not everyone can be MIL4, but everyone should at least be able to achieve MIL1 by implementing Splunk ES with basic data sources, Asset and Identity configuration, basic dashboards, etc. with the desire, capabilities and budget to get to MIL2 at a minimum. This is designed in order to help the customer identify particular areas or strength within their cybersecurity program as well as what deficiencies may exist in order to bolster their overall security posture by prioritizing their efforts into more focused areas. This offering addresses those different needs and creates an achievable roadmap to help the customer to maintain the desired level of security throughout the security lifecycle.



Each stage of the maturity journey has specific tasks/activities associated with that level, as the customer chooses to progress up each level encompasses all the activities of the previous level so this will a la carte, i.e. the customer will choose what activities they wish to prioritize and implement in order to get to the next level. Every customer should start off at MIL1 with MIL2 being the next desired state.

Maturity Indicator Level 1 (MIL1)

Category	Activities
Security Monitoring	• Security visibility and observability is centralized • Some dashboards with security relevant data have been deployed
Advanced Threat Detection	• The triage process for investigations begins in splunk
Incident Investigation and Forensics	• Splunk is fed all security data and is used as the beginning of the triage and investigation processes
Insider Threat Detection	• ES, SA-investigator or similar app is in production and used as part of the investigation process
Incident Response	• NO defined activities for MIL1
SOC Automation	• NO defined activities for MIL1
Compliance	• Data retention has been determined and is centralized
Fraud Detection	• Data for web and transactional fraud detection is centralized and tracked



This offering implements the various activities associated with each level. MIL1 is accomplished by most customers implementing the market leading features in Splunk Enterprise Security through basic data sources. This Professional Services offering helps the customer move through the subsequent levels: MIL2, MIL3, and MIL4. The activities outlined in each corresponding Maturity Level would be the activities that Splunk Professional Services would perform. Please note, as the customer progresses to higher MIL levels that additional data sources, customer skill sets, and the use of additional Security Suite Products like Splunk Phantom or Security Analytics might be required.

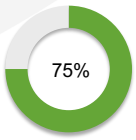
Maturity Indicator Level 2 (MIL2)

Category	Activities
Security Monitoring	• Top 6 data sources have been onboarded and Data Models are populated • Basic correlation searches have been deployed • Cloud data sources have been integrated for visibility and basic observability
Advanced Threat Detection	• Next Gen Endpoint, Endpoint Detection and Response or sysmon is integrated • Integration of advanced Threat Intel system (like Anomali, Threat Connect) or other 3rd party providers • Integration of pre-built content like Security Essentials, Risk Based Alerting (RBA), ES-Content Update, etc. • Ability to aggregate alerts with statistics like RBA or event sequencing
Incident Investigation and Forensics	• Capability to look for rare or unusual CPU processes exists, sysmon 4688, endpoint use case development • Implement RBA or leverage risk index. Having correlation searches that reference risk levels as decision criteria. Ex. If risk_score is > 100
Insider Threat Detection	• Capability to look for rare or unusual CPU processes • Reduce alert fatigue by tuning and combing similar types of alerts • Implement alerts based on Machine Learning for outlier detection
Incident Response	• Detection and investigation are being performed • Defined workflow for searches in the triage queue
SOC Automation	• SOP has been identified and implemented for critical and high alerts • Defined and automated workflow for searches in the triage queue • Correlation searches are providing high fidelity results that can easily actioned
Compliance	• Data is reviewed for accuracy, anomalies or suspicious behavior regularly • Normalize log data for compliance and reporting • Data at rest and in transit is protected (as required) • Create dashboards (or use apps) to demonstrate compliance to applicable regulations • Security use case(s) to track activity of privileged users across in-scope devices and users • Vulnerability data is logged and use case(s) implemented
Fraud Detection	• Security use case(s) to support basic fraud detection like account takeovers are implement

Proactive Monitoring & Alerting

Level 2

- Risk Awareness
- Asset & Identity Normalization
- Information and Event Correlation
- Notable Event Management
- Triage & Investigation Workflows
- Threat Intelligence
- Security Use Case Library



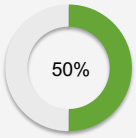
Maturity Indicator Level 3 (MIL3)

Category	Activities
Security Monitoring	• All security events are fed into a centralized, single platform for visibility and observability • Assets and Identities (A&I) are integrated and categories and priorities for at least 50% of Assets and Identities have been defined (at least critical infrastructure) • Implementation of dashboards for security data with filterable data
Advanced Threat Detection	• Dashboards to monitor application activity like Databases, Salesforce, Box, Dropbox, Azure, O365, etc. • Implement more advanced detections from Splunk Security Essentials (SSE) or Enterprise Security Content Updates (ESCU) and customize as necessary for the detection of new entities (combination of user/host/dest/etc.) • Update Assets and Identities as required for additional enrichment • Utilize a framework like Lockheed Martin Kill Chain, Mitre Att&ck, CIS TOP 20, NIST, etc.
Incident Investigation and Forensics	• Collaboration of incidents across platform • Provide data enrichment for common alerts and investigative searches via Splunk Security Suite
Insider Threat Detection	• Utilize Machine Learning to augment the capabilities of the analyst through graph mining and unsupervised ML • Utilize Machine Learning and Artificial Intelligence to detect previously unknown patterns or risks
Incident Response	• Create a single pane of glass interface for the Analyst to utilize during triage/investigation
SOC Automation	• Create data enrichment for common alerts and investigative searches via Splunk Security Suite • Create orchestration for common security events • Implement human and machine (automated) based decision making during triage and investigation
Compliance	• Create reports for personal data processing to include access, storage and proper deletion of data
Fraud Detection	• Use case(s) to support more advanced fraud detection like land speed violations and outliers • Create reporting and metrics to Executive Management (value, status, recent fraud losses, etc.) • Create aggregated data insights in order to support risk attribution and prioritize activity • Create a consolidated view of transactions across multiple different systems • Utilize orchestration and automation to triage and investigate incidents with minimal analyst interaction

Security Situational Awareness

Level 3

- Asset & Identity Risk Correlation
- Advanced Detection Methods
- Advanced Visualization
- Semi-Automated Playbooks (Orchestration & Response)
- Continuous Use Case Development
- Incident Collaboration



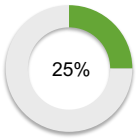
Maturity Indicator Level 4 (MIL4)

Category	Activities
Security Monitoring	• Create risk dashboards to be used a part of the triage and investigation process • Create dashboards that utilize Machine Learning to provide deeper data analysis
Advanced Threat Detection	• Leverage data science models for Threat Hunting • Leverage Machine Learning for more advanced pattern / baseline based detections
Incident Investigation and Forensics	• Leverage orchestration and automation to enhance and augment the investigative process • Integrate data from forensics tools for enhanced data analysis
Insider Threat Detection	• Create custom use cases that aggregate results from statistical analysis and ML Models • Generate custom ML Models • Create use cases to detect malicious activity in custom built line-of-business applications
Incident Response	• Create metrics around the highest frequency alerts, longest time to triage, etc. • Create feedback loop for each rule fired • Create Custom Case Management / Workbook templates and mechanism to auto create/close tickets
SOC Automation	• Create custom API integrations with 3rd party vendors as required (custom App) • Create playbooks to automate ticket creation/closure
Compliance	• Provide mechanism to report on breach response (Mean time to detect, contain and respond) aligned with compliance requirements
Fraud Detection	• Create Machine Learning Use case(s) to support fraud detection for spotting outliers and cluster data • Integrate with all cross-functional tools to improve overall program in heterogenous environments

Real-time Risk Insight & Automation

Level 4

- Risk Reporting
- Full Playbook Automation
- Machine Learning for Security
- Threat Hunting
- Effective Collaboration & integration with other teams or tools
- Breach Response



Target Customer Attributes

This offering is targeted at customers who are existing Splunk ES customers. In this scenario, the customer already has installed Enterprise Security and on-boarded basic data sources (Proxy-Firewall-Active, Directory-Windows, Event/Security Logs-IDS/IPS-Malware), has some basic OOTB content enabled and some Assets and Identities information in the platform. However, the customer may be struggling on where to go next or how to up-level their detection/investigation/response/SOAR programs. The customer ideally would have just performed a Security PVP with their Sales team, if not Splunk Professional Services can come in and perform the Splunk Security Maturity Methodology (S2M2) to provide a more in depth view of their current state and provide a clear roadmap with established milestones to guide their security maturity journey. This is where this offering is ideal, the customer may or may not want to perform each activity identified for each level, as they may have different priorities, so each activity can be picked a-la-carte. However, to fully move to the next level from a previous level the customer must perform all of the described activity in order to level-up their security maturity and enhance their security posture.

Splunk Professional Services

Our services are backed by Splunk Accredited Consultants, Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.