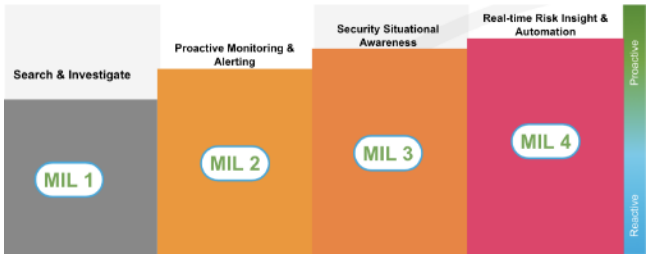
Splunk Security Maturity Methodology (S2M2)

Executive Summary

The purpose of the **Splunk Security Maturity Methodology (S2M2)** is to assess the maturity of a Security Operations Program, using measures pertaining to the various disciplines to effectively deliver a security service, and then provide guidance on how to mature their operations based upon business priorities. It covers the technologies that the customer uses, and the processes used to leverage those technologies to deliver security services. The outcome of S2M2 provides a security roadmap that the customer can use to improve their security program maturity to the next level. The maturity model in the roadmap uses a multi-level model, signified by "Maturity Indicator Levels (MIL)", to assess the current state and to identify the areas that need to be worked on.



Customer Perspective

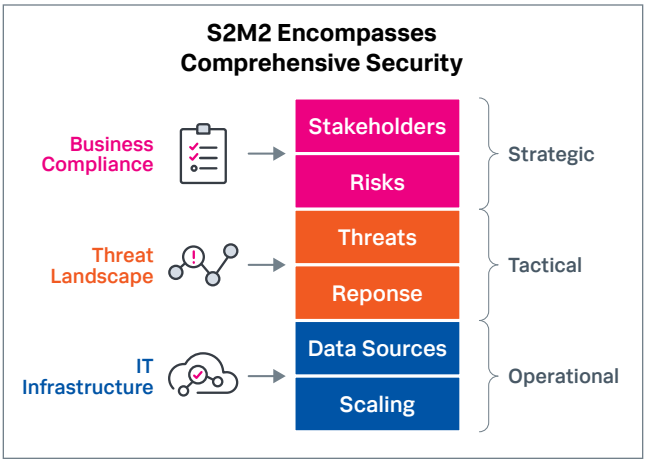
A Security Operations Center (SOC), as defined by SANS in their most recent SOC survey, is "A combination of people, processes and technology protecting information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state and minimizing damage from unwanted effects.1" We can directly impact these three areas of people, process and technology through a combination of Splunk Training and Professional Services. Most SOC's (31%[1]) utilize anywhere from 2-5 analysts, given the low number of analysts to the high number of security events, technology must be an augmentation to the analysts. In order to effectively utilize our technology, solid processes and automation have to be in place in order to get the SOC to a state where everything is fully repeatable.

Technology enhancements and industry trends are also seeing more widespread use of augmentation from additional technologies like machine learning and artificial intelligence.

S2M2 is the methodology to help customers scale their Security Operations. Increasingly, customers are looking to Splunk to provide guidance on improving their security posture and aligning with their strategic vision and business goals. S2M2 provides the prescriptive path forward utilizing the knowledge of Splunk Security experts who are equipped to provide expert security advice. Areas covered throughout this process include the following:

- **People.** Deriving maximum value from any security platform requires that users be properly trained. Proper training will allow analysts to use their time efficiently, and ultimately reduce time to respond/ triage. Additionally, consistently providing analysts with training opportunities will promote employee retention. Splunk will review analyst skill sets as they pertain to incident triage/management processes across Splunk technologies, and identify opportunities to up-level customer knowledge in those areas.
- **Process.** An effective security program requires processes to address incident response, workflow/ case management, content lifecycle, etc. Splunk will review existing processes and make recommendations for the various operational facets of your SOC to achieve desired state using Splunk's Security suite of technologies.
- **Technology.** Splunk's suite of technologies (Splunk Enterprise, Splunk Enterprise Security (ES), User Behavior Analytics (UBA), Splunk SOAR, IT Service Intelligence (ITSI) and Victor Ops) are market leaders and best suited to help customers achieve their goals as a Security Operations Team. S2M2 takes a holistic view of your Security Operations and will provide technology recommendations to reach your desired maturity state.

1. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570, p. 2.

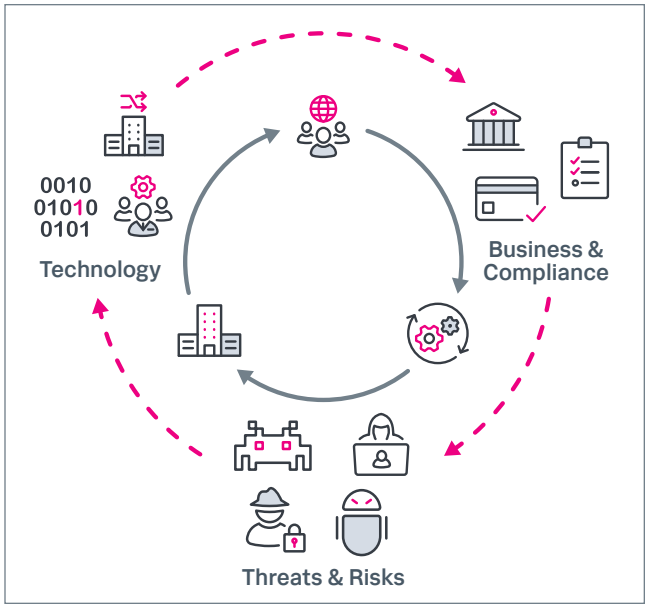


The Process

As an optional precursor to the S2M2, customers may start their security journey with the Security Prescriptive Value Path (PVP) offering (https://www.splunk.com/pdfs/professional-services/splunk-security-prescriptive-value-path-offering.pdf), which will evaluate current technology capabilities and allow Splunk to determine security maturity state. Splunk will then provide the customer with a customized security roadmap that defines the activities required to progress up the maturity scale. The PVP will start with a review of the following:

- **Business and Compliance.** Review strategic business objectives, as defined by appropriate stakeholders, and align with near and long term initiatives of the security organization.
- **Threat Landscape.** Discuss potential cyber security risks from external and internal threats across malicious threat actors or human errors. Then we examine the processes in place for response and security analytics. We do this by incorporating industry knowledge and market reports enhanced with experience gained across global customers and every business vertical.
- **IT Landscape.** This will determine the available data sources and supporting systems/services to support the initiatives of the security program. In addition, this will support the various detection mechanisms and security monitoring rules that will be required to meet the customers needs.

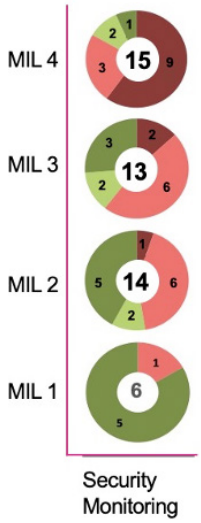
Customers can first go through the PVP exercise with the assistance of Splunk Sales; existing customers will be able to utilize their Customer Success Manager



(CSM) for this to help guide them through this process. Then, S2M2 continues this process by providing a deeper understanding of how to help the customer progress up the maturity scale to their desired operational state and further aligning them with their desired security and/or detection framework.

After completion of S2M2 (approximately 2-4 hour exercise in collaboration with the customer), the sales team or the CSM will provide a customized security roadmap that clearly defines the activities associated with each security maturity level, and how to effectively level-up using Splunk PS resources (On-Demand, Assigned Expert, and/or scoped projects through Statements of Work).

Score it like it's 1999



This methodology provides a way to score customers' security maturity in a way that is both iterative and cumulative. Each maturity level is a reflection of the progress the customer has achieved in each domain. The goal is to get the customer from a state of where things are highly manual with very little automation or processes in place, to a state where nearly automation is implemented where possible and applicable, processes are fully

refined and repeatable, and thoroughly documented. The Splunk S2M2 report is a roadmap that illustrates the customer journey through maturity indicator levels, and shows all the associated accomplishments required for them to get from level to level.

There are four levels of maturity ranking. For example, a customer that has centralized logging and monitoring of some traditional security relevant data sources, and is performing security tasks in an ad-hoc manner, would likely be scored at a Maturity Indicator Level of 1 (MIL1). In this example, the S2M2 report provides the customer with the blueprint that they will use to build and/or modernize and optimize their Security Operations using Splunk as the platform for Security Operations. This will not only help their organization progress up the maturity scale but also prove the value of security to the entire company.

Key Benefits of S2M2

The S2M2 methodology aims to provide the customer with a seamless approach to security maturity as they begin their security journey with Splunk, from first contact with Splunk, all the way through to operationalization of the product.

The customer can now clearly envision the path to achieve:

- Demonstrable decreased business risk
- High fidelity, contextual security alerts
- Discover true positives faster
- Identify and remediate gaps in SOC operations
- Proactively detect, investigate, and defend against threat actors
- Automations that decrease response time and team effort
- Achieve internal and external compliance

Case Study

Splunk was recently engaged by a large existing customer, which was interested in overhauling their security operations program using Splunk. They had been using Splunk for IT operations, and some ad-hoc security tasks in the past, and they were ready to expand and mature their security program.

After thorough discovery discussions between the customer and the Splunk Account team, in conjunction with Splunk Professional Services, we were able to build a plan of approach to meet the customer's security needs.

Splunk Professional Services was engaged early in the project to conduct a use case and process workshop. Through this workshop, we were able to determine the customer's immediate needs regarding use cases, and automated workflows. The output of this workshop drove the implementation of this project.

Throughout the project, there were touch points across several products within the Security Suite. Splunk Enterprise was addressed, as the customer required additional architecture, and to remediate some performance concerns on the existing indexer tier. Enterprise Security was implemented, along with 100+ use cases within the Risk Based Alerting (RBA) framework. Splunk Phantom was implemented to address the customer's needs around incident management workflow, to enrich RBA alerts, and to provide case management metrics back into Splunk.

To conclude, in close collaboration with this customer, as well as multiple different teams within Splunk, we were able to implement a comprehensive security operations program, leveraging multiple components of Splunk's Security Suite (Splunk Enterprise, Enterprise Security, and Splunk Phantom). This type of collaboration, in a project with several dependencies and requirements, is the outcome possible using S2M2.

Learn more about S2M2 and Splunk Security and Compliance Services or chat with an expert about Splunk's Security offerings.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-20344-Splunk-Security Maturity Methodology-DS-101