Justifying the Need for a SOC Model

A security operations center (SOC) is a large capital and ongoing operational investment for an organization. Exactly what it is supposed to do, and how it will accomplish those objectives, can waiver in the varying operational deployment models of information technology (IT) and the uncertainty of adaptive threats in the environment.

To this end, most organizations rely upon some authoritative reference of what the SOC is supposed to provide. For example, interim responses from the ongoing 2020 SOC survey suggest that organizations are currently using the MITRE ATT&CK® framework to define SOC capabilities (see Figure 1).

These models usually define what needs to be done, but not how it is done. Further, these models often leave the effort of collecting the appropriate technology to the reader of the model.

Figure 1. 2020 SOC Survey Responses to “… Model to Determine Capabilities…”

When an organization decides to implement a SOC, there is typically substantial technology procurement consideration, as well as reconciliation of the technology currently in use. This depends on the IT systems in use by the organization, and current IT infrastructure deployment trends have limited visibility through transferring infrastructure management to third parties.

A suitable analogy is that the architecture of a residence requires (more or less) consideration and can be implemented at varying price points. One option is a site-appropriate, heavily customized structure using green construction and energy-efficient methods that takes into account every need of the future inhabitants. Alternatively, a double-wide trailer can be ordered and delivered to the site overnight.

To help you consider the right mix of capability, technology and staffing, this paper will discuss some existing capability models for security operations. It will then identify shortcomings, both generically and specific to each model. Finally, the paper will discuss the value each model would provide to organizations that implement a new SOC or enhance their existing SOC.

**Existing Models**

The first two models we discuss—NIST Cybersecurity Framework (CSF) and MITRE ATT&CK—are not SOC specific but instead form the basis of the larger program of cybersecurity that warrants a SOC implementation. The remaining models—SOC-CMM, SOC-Class, Gartner Visibility Triad and CrowdStrike-Splunk-Vectra Triad—focus on various aspects of SOCs.

**NIST CSF**

The U.S. National Institute of Standards and Technology (NIST) has a mission to advance economic capability by “… advancing measurement science, standards and technology in ways that enhance economic security…”

To that end, NIST has published hundreds of papers on information technology and information assurance (an older and partially deprecated term in favor of cybersecurity).

The framework consists of three tiers: core, implementation tiers, and profile. This model is extensive, and exerts substantial effort organizing and collecting information around organization risk management and strategy—the idea being delivery of prioritized protection to the most important assets at the greatest risk.
MITRE ATT&CK

MITRE is a private, not-for-profit organization working primarily with U.S. government agencies but also with academic institutions, businesses and other organizations. MITRE’s efforts tend to take the form of U.S. federally funded research and development centers (FFRDC) with a mission of enhancing public safety.5

MITRE ATT&CK is a knowledge base comprised of matrices, tactics, techniques, mitigations, attribution to named intrusion actors, and tools. ATT&CK is frequently translated into other forms (such as STIX and TAXII).6

The effort is attempting to be an exhaustive catalogue of what attackers do so that defenders can refer to an authoritative source for this information. It also proposes mitigations to attacker capability to help prioritize cybersecurity resources to areas most likely to be targeted by attackers.

As such, many industry vendors and tools have used ATT&CK as a basis for their technology, tool or project.

SOC-CMM

The SOC-CMM7 is a model composed of five domains: Business, People, Process, Technology and Services. It was originally developed through literature review but was revised with an abstracted aggregated view that assigned the elements from the original review into one of the five current domains.

A set of assessment questions was developed for objective and self-assessment to be performed to determine if a specific SOC has implemented the identified elements. Each SOC also may weight the importance of elements of the SOC-CMM, indicating that some elements are not appropriate for the organization’s requirements or culture.

The project is maintained by a single individual with community support.8

SOC-Class

The author of this paper developed a model for designing, building and implementing a SOC as the SANS Institute course MGT517.9 After retirement by the SANS Institute, the course material was made available as SOC-Class.10 The model proposes eight components: Steering Committee, Command Center, SOC Operations, Monitoring, Threat Intelligence, Incident Response, Forensics and Self-Assessment.11

This model provides a staff, process and technology-focused mapping that is intended to enumerate all needed elements for a SOC. The organization and implementation of the details are identified as candidates, but the actual selection of staff, processes and technology are flexible based on the organization’s needs.

---

5 MITRE background and mission, www.mitre.org/about/corporate-overview
6 MITRE ATT&CK, https://attack.mitre.org/resources/working-with-attack
7 SOC-CMM, https://soc-cmm.com
10 SOC-Class, www.soc-class.com
11 SOC-Class Functional Areas, www.youtube.com/watch?v=WygM1eui6KQ
Gartner Visibility Triad

Gartner is a for-profit research and advisory organization, included in the S&P 500. It is known for its “Hype Cycle” and “Magic Quadrant” assessments. According to Gartner’s website, the company has clients in 77% of the Global 500.12

In March 2019, Gartner published an article titled “Applying Network-Centric Approaches for Threat Detection and Response,”13 wherein a SOC Visibility Triad is defined as network detection and response, endpoint detection and response, and correlation (SIEM and user and entity behavioral analytics [UEBA]). According to the public outline, the paper focuses on the network technology implementation specifically, but the “triad” is included to provide a comparison of what is missed by the network approach.

CrowdStrike-Splunk-Vectra Triad

The notion of the Gartner SOC Visibility Triad was taken and extended by a partnership of technology vendors—CrowdStrike, Splunk and Vectra (who have sponsored the writing of this paper)—to tactically deploy the triad concept by technical integration between the three products.

CrowdStrike is a cybersecurity company that provides endpoint security, threat intelligence and cyberattack response services, including investigation, response and remediation. The company offers a multitude of modular solutions for cloud-based endpoint security under the Falcon platform, including malware protection, IT hygiene, vulnerability management and threat hunting, among other offerings.14 Services include investigation, response and capabilities assessment. CrowdStrike offers a multitude of solutions for endpoint and cloud-based inspection under the overarching Falcon platform. The Falcon suite of products offers modules for various activities and types of inspection.

Splunk provides services and products focused around its data aggregation platform,15 which can be used for log management as well as SIEM. The company cites that 92 of the Fortune 100 companies use its products. In addition to log aggregation and SIEM, Splunk offers an orchestration and automation product called Phantom Cyber, which it incorporated into its product offering through an acquisition in April 2018.16

Vectra is a network detection and response (NDR) platform that uses AI to empower the enterprise SOC to automate threat discovery, prioritization, hunting and response. The Cognito platform from Vectra enables enterprises to immediately detect and respond to cyberattacks across cloud, data center, IT and IoT networks.17 It offers a product called Cognito, which cites AI-driven detection and response for cloud, SaaS and on-premises devices.18

---

17 Vectra, www.vectra.ai
18 Vectra Cognito, www.vectra.ai/product/what-it-is
In September 2019, Vectra advanced a discussion of the native integration capabilities as a method to gain greater insight for low-level firmware-type implants where endpoint visibility was circumvented.\(^9\)

This model is not a distinct product offering, but rather guidance from the coordinated efforts of the vendors to show their customers how to implement the concept offered by Gartner.

There are two major enhancements that were added in this iteration. First is the inclusion of a Security Orchestration, Automation and Response (SOAR) tool into the “triad.” (I’ll continue to use that branding despite the inclusion of a fourth product.) Since Splunk owns Phantom, SOAR is a natural inclusion. A brief description of what this tool is intended to do. First, automation is the execution of a series of actions without human intervention or input. Orchestration is the automation of action or collection of information across multiple information systems. Response is the most common application of this capability by this tool: kill a process, suspend an account, terminate a network connection, make a configuration change to implement a new firewall rule based on observed network activity. This is what an analyst would authorize after investigation.

The point of the tool is to authorize certain actions, and mobilize the response without human intervention, or perhaps bring the proposed action to an analyst for final verification. If the SOAR is well conceived and well executed, it eliminates the majority of the opportunities for errors through human configuration changes. (A more thorough discussion of the appropriate applicability of SOAR is outside of the scope of this paper, but the author of this paper has written and presented extensively on this subject.)

The second new technology in this version of the triad is artificial intelligence (AI). According to the Vectra published paper “The Data Science Behind Vectra AI Threat Detection Models,”\(^{20}\) the AI techniques include unsupervised and supervised learning, heuristic-based analysis and anomaly/outlier detection. These techniques are applied in various manners globally across all monitored assets and locally to monitored assets to provide insight into attacker trends and anomalies present within the context of the specific deployment. The UEBA portion of the original triad suggests that behavioral analytics are a core component of the needed visibility. This AI deployment is attempting to reduce the cost of differentiation of normal from unwanted activity.

**Other References and Guidance**

There are many other materials available related to SOCs, best practices and implementation guidance. Some are proprietary, while others are free. One worthy of mention is the MITRE book, “Ten Strategies of a World-Class Cybersecurity Operations Center,” by Carson Zimmerman, which is available for free download in PDF format.\(^{21}\) It contains extensive and detailed guidance on how a SOC should run.


Model Shortcomings

Each of the aforementioned models or documents are intended to help organizations select the right sort of protections, then implement those protections. The individuals responsible for doing so are often left with a confusing mix of guidance, direction, and legal or industry requirements that must be met.

This section will air some of the general shortcomings of these model-based approaches before delving into the value proposition of them. This helps to provide balance to the assessment and selection criteria.

**General**

Any model selected might require customization or tailoring. Most of the models are created in a way that specifically allows for right-sizing the solution. The organization may not have the maturity, insight or resources to create the right tailoring, which can result in a poor match for the SOC deployment.

Not all of the models fully address business alignment, staffing, technology and ongoing operational performance. The varying degrees of specific details about how to do any one of these things typically result in something that is so specific that it is no longer viable as general guidance and becomes more of an example of one specific implementation. Or, the model selects only one aspect, such as technology, with scant reference to how to incorporate or perform the other necessary elements.

**Open Source vs. Proprietary**

This can take many different flavors, and there are multiple justifications for choosing one over the other. The term *open source* is used here to indicate freely available with extensive or complete visibility and license to change any aspects deemed misaligned. *Proprietary* means requiring payment for use. Organizations often have a preference between the two.

Unique risks of open source include meddling by powerful but malicious contributors, and the project becoming stale or unsupported because the primary contributors lose interest and there’s no obligation or incentive to maintain it.

Unique risks of a proprietary solution include vendor lock-in, incremental upsell to accomplish the originally expected capability, company failure, purchase by a third party that has a different vision, and feature drift away from original rationale for purchase. There’s not a correct solution to this problem currently. It is simply the reality of the marketplace for cybersecurity guidance, services and products.
Shortcomings of Models Discussed

**NIST CSF** is an open source project with extensive information and elaborate customization opportunities, with an abundance of additional material to direct implementation. Despite all of these resources, there’s not any one product that encompasses NIST CSF implementation.

**MITRE ATT&CK** has accomplished substantial visibility in the five years since its public release in 2015. According to MITRE information, it began research on the process in 2010 and developed the model as ATT&CK in 2013. The tool was conceived as something that “serves as both the adversary emulation playbook and as a method for discovering analytic coverage and defense gaps inside a target network.” Since then, the matrices have expanded in number, adding ICS, cloud and mobile, as well as Linux and macOS. The expansion has been largely positive, but the ongoing visibility boom may be driving the expansion. An additional caution is that the “defensive gap analysis” and SOC maturity guidance don’t have a clearly delineated and openly published methodology for implementation. This is typically offered as a service from MITRE or other third parties. This capability is positive, and can be useful, but is not fully developed in the model yet.

**SOC-CMM** is mapped to NIST CSF. It is the premier open source SOC maturity assessment tool available. It has two primary shortcomings. First, it has no mandate driving its adoption and use. Second, companies will expend effort on its high-density question-based assessment, then perhaps still be left with questions of what to do to resolve identified shortcomings and how to prioritize them.

**SOC-Class** is a proprietary solution that amalgamates several different models into specific direction and operational tactics. Despite extensive resources and a Gantt chart depicting all the action items needed to build a SOC, substantial effort is still required by the organization. The technology selection tiers are intended to be complete across three price points (open source, moderate priced and enterprise) but are not depictions of integrated suites of tools ready to purchase and deploy.

The **Gartner Visibility Triad** is a reference within a proprietary paper on network visibility. It provides excellent guidance on mitigating the shortcomings of network visibility but has no other support from the vendor and no further development path from that vendor.

The **CrowdStrike-Splunk-Vectra Triad** is a specific implementation of the idea from the Gartner Visibility Triad. This model has the benefit of all of the institutional knowledge from three vendors applying lessons learned and experience from each of their customers. But it is not a specific partnership between the companies to develop a unique product, or something like a verified implementation at specific versions with a commitment to assure integration between the products through coordinated releases.

---


23 MITRE ATT&CK use, https://attack.mitre.org/resources/getting-started
Model Value Propositions

These models are not mutually exclusive. But, when an organization selects multiple models, reconciliation between potentially conflicting information should be considered prior to implementation.

NIST CSF

NIST CSF has the longest legacy of development, inheriting extensive development from all previous NIST work from decades of effort across U.S. government agencies and thousands of information systems, and likely hundreds of thousands of endpoints. There is substantial commitment to ongoing development and a virtually indestructible sponsor with a commitment via its long-term mission (U.S. Government Department of Commerce). The components depicted are complete, thorough and agnostic to any specific technology. (But this may be detrimental to your actual implementation of the CSF.)

Advice for use: Long-term organizational alignment in all components of information technology use, risk management, and cybersecurity architecture and operations is necessary to derive the value the NIST CSF offers.

MITRE ATT&CK

MITRE ATT&CK is newer and has a smaller scope of focus than NIST CSF. The primary differentiator between ATT&CK and any other SOC model is the inclusion of threat information in its tools and matrices to help the implementor prioritize immediate term (such as investigation and response), short term (such as vulnerability mitigation and defensive posture adjustments to emerging threats), and strategic actions (such as realigning IT operations and architecture for effective interruption of adversary mission-critical capability) based on vetted, community-based threat intelligence.

Advice for use: Understand that ATT&CK may be used for incident investigation, threat intelligence-informed adversary modeling, defensive/SIEM use case development, threat hunting, defensive gap analysis, SOC maturity assessment and likely others. First, achieve clarity on the various uses of ATT&CK that are available and select one or more uses. Then, maintain rigor in that specific use.
**SOC-CMM**

SOC-CMM is appropriate for use as a maturity assessment tool in self-assessment mode or as a tool for a third party to assess the organization’s SOC. It could also be used as an effective tool for defining the organization’s priorities for the SOC.

**Advice for use:** Consider a three-phase use plan. First, download the advanced assessment spreadsheet and rank the “Importance” attribute of each element of the five domains (there are 50–100 elements per domain, but sub-elements do not have importance). Use this as a discussion tool with the SOC constituents to drive business alignment for the SOC. Next, perform a self-assessment using the defined importance to set prioritization for a 6- or 12-month maturation period. At the end of this period, an objective third party will use the SOC-CMM to assess the SOC’s maturity. This will be compared to the maturity objectives defined by the self-assessment. The assessment should also review the previously defined importance to see if priorities of the SOC constituents have shifted or if the threat landscape warrants an adjustment of the organization’s posture.

**SOC-Class**

SOC-Class is intended as a robust infusion of guidance for new SOC builds or maturation of an existing SOC by assessing the necessary capabilities of every SOC. It questions and provides tools for enhancing business alignment, technology implementation, orchestration/automation/process development, threat hunting, use case development, technology implementations, and staff onboarding/development/retention. It’s intended to deliver years of experience in a short burst.

**Advice for use:** Plan to bring your existing model or plans, and prepare to spend 2 to 3 months after the course to refactor existing plans. Then count on it to take 6 to 12 months to implement the changes you selected.

**Gartner Visibility Triad**

The Gartner Visibility Triad is a concise recapitulation of a well-known issue: Neither network data nor host data alone are adequate for thorough visibility into your environment. Further, attempts to ingest all of the network and host data end in frustration, turmoil and often less clarity than simply focusing on one or the other.

The Gartner solution is curated ingestion of data into analytical capabilities, such as SIEM or UEBA, with additional primary data sources available for in-depth investigation when some suspicious element is identified by the correlation of host artifact and network artifact to eliminate noise and reduce false positives.

Implied within this visibility model is the ability to develop use cases and enrich available source data with threat intelligence and external corroborating data, such as domain, executable or website reputation.

**Advice for use:** This visibility advice is an excellent concept. Strive for inclusion of correlating data in your detections, without swamping your SOC with too much data.
CrowdStrike-Splunk-Vectra Triad

The CrowdStrike-Splunk-Vectra Triad builds upon this sound practical advice with two major enhancements (discussed in detail in the “Existing Models” section earlier in this paper). The technologies are identified as compatible and interactive, but this was not tested in the course of this paper.

There is still work to be done by the implementing organization; however, the tools are provided by vendors with substantial customer base, specific guidance for implementation and experience implementing in many different organizations. The automation capability of Phantom has a proven track record and a large catalogue of automated actions that can be implemented easily. The implementation could be careless, counterproductive or destructive, but that should not happen with some thoughtful application and a cautious, phased implementation of automated actions with the new tool.

This tool combination doesn’t solve any of the organizational alignment or risk management issues by itself. However, it could provide enhanced visibility, which can compel leadership to address those issues with a suite of tools providing strong evidence of actual issues that need cybersecurity architecture, IT operational rigor and risk management attention rather than investigation and response.

Advice for use: If you are currently using one of these tools successfully, consider extending the suite of tools to achieve greater visibility, correlation, enrichment, use case development, cyber investigative maturity and consistency in response. The automation capability is not a set-and-forget tool set. This is a very powerful capability that must be wielded by skilled professionals with clarity of their mission and understanding of their boundary of authority. Feeding and tuning the SIEM has been a perennial problem since solutions of its type were introduced. The inclusion of supervised and unsupervised learning capabilities helps analysts focus on the business alignment aspects of use cases and transfer some of the more tedious differentiation calculations to the information system.

Conclusion

Security operations center (SOC) is a common term that refers to the cybersecurity operational capability of an organization. The exact form this takes for each organization varies. There are multiple resources for defining what that form is based on, and this paper identified several of the more popular ones available. These models are mixed between for-profit and nonprofit publishers, and the relative strengths and weaknesses of these models were discussed.

The models share some depiction of capabilities or the responsibilities for action that the SOC embodies. The models may include depiction of the level of performance through maturity assessment or coverage of adversary techniques. In the case of the CrowdStrike-Splunk-Vectra Triad, it extends that notion of responsibility and performance into a tactical tool deployment methodology with the support of a trio of vendors committed to implementing a shared vision of capability.
**About the Author**

Christopher Crowley, a senior SANS instructor and course author for courses in Managing Security Operations and Incident Response Team Management, holds multiple certifications. He received the SANS 2009 Local Mentor of the Year award for excellence in providing mentor classes to his local community. Chris is a consultant based in Washington, D.C., who has more than 15 years of experience in managing and securing networks. His areas of expertise include security operations, network and mobile penetration testing, mobile device deployments, incident response and forensic analysis.

**Sponsors**

SANS would like to thank this paper’s sponsors:

- [CrowdStrike](#)
- [Splunk](#)
- [ Vectra](#)
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Essentials Australia 2021</td>
<td>Melbourne, AU</td>
<td>Feb 15, 2021 - Feb 20, 2021</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>