ESG SHOWCASE

Operationalizing MITRE ATT&CK with Detection Posture Management

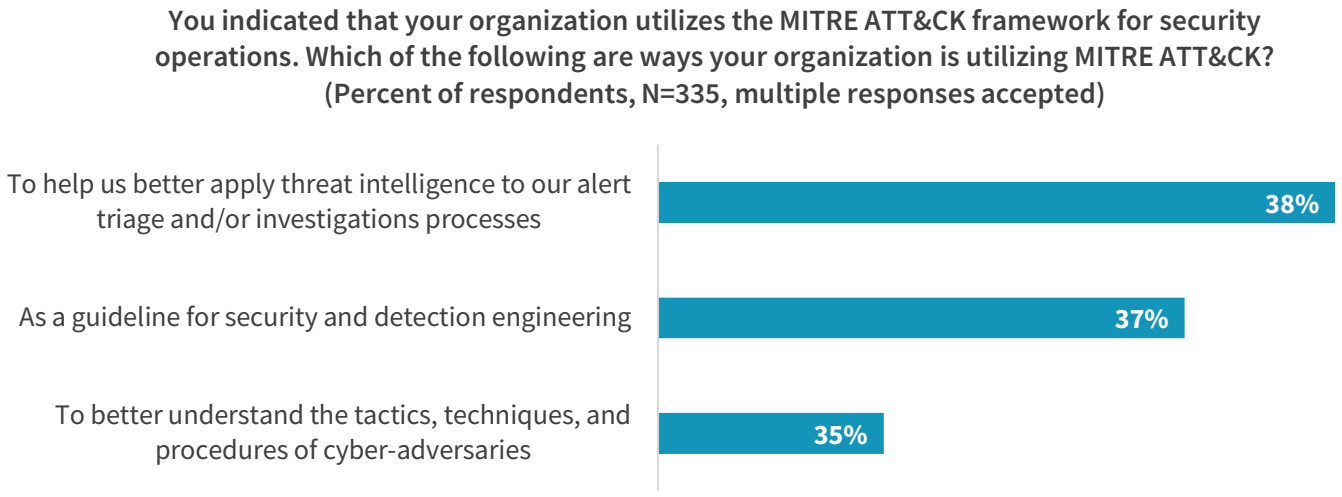
Date: October 2022 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Security operations teams are at a crossroad. Organizations need unprecedented security operations scale and efficiency but continue to be dragged down by manual processes, skills shortages, and suboptimal technology usage. The MITRE ATT&CK framework can help, as it introduces an adversary view and structure for security operations. Organizations seeking to operationalize MITRE ATT&CK as a framework for identifying and remediating control gaps may want to consider detection posture management with CardinalOps.

Overview

According to ESG research, 89% of organizations are using the MITRE ATT&CK framework to reduce risk for numerous security operations use cases, including applying threat intelligence to alert triage, as a guideline for detection engineering, and gaining a better understanding of adversary tactics, technique, and procedures (TTPs, see Figure 1).[1]

Figure 1. Top Use Cases for the MITRE ATT&CK Framework



Source: ESG, a division of TechTarget, Inc.

[1] Source: ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022. All ESG research references and charts in this showcase are from this survey results set unless otherwise noted.

While the MITRE ATT&CK framework has become a lingua franca and an aspirational model for security operations, many organizations haven't gotten beyond using it only as a reference source. SOC modernization initiatives can take this a step further by operationalizing MITRE ATT&CK for use cases like controls assessment and proactively identifying hidden coverage gaps that can lead to compromise.

Detection engineering is especially timely as organizations face dangerous threats and cyber-attacks that follow a kill chain progression from reconnaissance and exploitation to lateral movement, privilege escalation, and, eventually, data exfiltration. As a countermeasure, organizations need accurate, complete, and timely detection rules derived from the right data sources across security information and event management (SIEM) systems, endpoint detection and response (EDR), and extended detection and response (XDR) tools.

Operationalizing MITRE ATT&CK and Detection Engineering Challenges

Threat detection and response is a core component of modern security programs, driving investment in tools to improve visibility, efficacy, and efficiency. When looking at all the tools used for threat detection and response, more than half of respondents say that their SIEM is one of their most effective tools.[2] Additionally, ESG research demonstrates that there is a correlation between security program maturity and MITRE ATT&CK utilization.[3] More mature security organizations/programs use security hygiene and posture management to operationalize MITRE ATT&CK, identify cyber-risks, and uncover coverage gaps.

While organizations may want to operationalize MITRE ATT&CK and drive improvement in their detection engineering processes, they face many challenges, including:

- Detection gaps. ESG research indicates that 34% of cybersecurity teams spend most of their time addressing high priority/emergency issues and not enough time on strategy and process improvement. For example, many organizations don't spend enough time asking questions like "Are we developing the right detections for the APT groups targeting our organization and that are aligned with our business priorities (e.g., cloud)?" "How do we measure and deliver board-level reporting about our readiness to defend against our highest-priority threats?" For this and other reasons, many overwhelmed organizations continue to have gaps in detection rules coverage—especially in areas like identity and access management (IAM) and cloud threat detection. These gaps minimize the value of the MITRE ATT&CK framework, and can lead to system compromises, adversary dwell time, and, eventually, devastating cyber-attacks.

- A reliance on manual processes. Security operations tend to be based on manual processes, tribal knowledge, and individual "heroes," rather than formal, documented workflows. For MITRE ATT&CK and detection engineering, manual processes add operational overhead as individuals scramble to gather data, learn the nuances of multiple security monitoring technologies, develop new rule sets, add exclusions and conditional logic to tune noisy rules, and then test them against real world attacks. Effective detection engineering for MITRE ATT&CK should also be continuous, but organizations burdened by manual processes and inefficiencies can't keep up. The result? Constant cyber-risk growth.

- Lots of data sources. Nearly one-third (30%) of organizations use 16 or more data sources for security operations activities like detection engineering today. The top sources included endpoint security data, threat intelligence feeds, log data from security devices, cloud security data, email security data, IAM logs, and network security data (i.e., NetFlow/IPFIX, VPC cloud logs, etc.). While this provides a lot of data to work with, detection engineers must

[2] Source: ESG Research Report, *The Impact of XDR in the Modern SOC*, March 2021.
[3] Source: Ibid

constantly review whether they are utilizing the optimal data sources and fields and including them into the right detection rules. This is an arduous task requiring security and data management skills, along with MITRE ATT&CK knowledge. Many organizations have deficiencies in one or several areas.

- Broken and noisy rules. Many SIEM and XDR rules are misconfigured or written incorrectly or can become silently broken over time due to constant changes in hybrid IT infrastructure, vendor log format changes, or superseding ruleset conflict. As a result, detection rules tend to fire too often or not at all. This leads to missed attacks that are lost in a cacophony of noise on the one hand and a false sense of security on the other. These issues need attention for MITRE ATT&CK operations, but many organizations don't have the time, resources, or any automated mechanisms to either identify or fix broken and noisy rules, so the number only increases over time.

While these challenges already increase cyber-risk, things will get worse because of macro trends like:

- The cybersecurity skills shortage. Recent ESG research indicates that 57% of organizations report being impacted by the cybersecurity skills shortage. Cited impacts from this shortage include increased workload, high burn-out rates, and an inability to recruit and hire additional security staff. The skills shortage has a direct impact on detection engineering: 22% of organizations claim that they have an acute shortage of security engineers.[4]

- The growing attack surface. One-third (33%) of organizations say the SOC team is challenged by monitoring security across a growing and changing attack surface. This growth can be attributed to connecting IT to third parties and using more public cloud computing resources. Gathering the right data and developing detection rules is more difficult when the attack surface is constantly expanding and changing.

As a result, many organizations aren't using their security tools to their full potential and lack the coverage they need to detect multi-phased cyber-attacks. This limits their ability to operationalize MITRE ATT&CK effectively.

SOC Teams Need to Improve Detection Posture Management

To alleviate detection engineering complexity and overhead, organizations can benefit from detection posture management, which can provide visibility into MITRE ATT&CK control gaps along with automated management of detection rules across SIEM and XDR. This investment can complement ongoing detection engineering, as ESG research indicates that 91% of organizations are developing their own custom detection rules/logic today.

Detection posture management includes:

- MITRE ATT&CK alignment. Leading detection posture management solutions use artificial intelligence and machine learning (AI/ML) to analyze existing SIEM and XDR rules and then map them to the MITRE ATT&CK framework. This is especially important for mapping custom detections to MITRE ATT&CK, which is typically not addressed by out-of-the-box functionality from SIEM and XDR vendors. MITRE ATT&CK alignment can be helpful for SOC teams to identify coverage gaps related to security controls, missing data sources, or known cyber-adversary behaviors. Armed with this knowledge, SOC teams can prioritize actions based on specific APT groups identified by their threat intel teams, vulnerabilities exposed by Red Team exercises, emerging threats, or specific log source types aligned with their crown jewels and business priorities. They can also utilize MITRE ATT&CK

[4] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.

coverage metrics to generate cyber-risk reports for executives and the board, pinpoint gaps needing further investment, and drive continuous improvement over time.

- Blind spot identification. Beyond MITRE, detection posture management solutions can help SOC teams not only identify coverage gaps but also recommend data sources and detection rules needed for more comprehensive coverage. This is especially useful for mitigating risk across a growing attack surface.

- Rules auditing. While new detection rules extend protection, SOC teams must also do a better job of auditing and fixing a growing stockpile of existing detection rules. Detection posture management provides continuous assessment of rules to identify noisy or broken rules. Leading solutions go even further by providing ML-driven recommendations for tuning noisy rules and fixing broken ones.

- Automated rule creation. To scale detection engineering to address the growing attack surface, detection posture management solutions must include capabilities for process automation. For example, leading solutions can create specific rules for detection technologies used at an organization. These rules should be generated in the native query languages of the SIEM/XDR (SPL, KQL, AQL, etc.) and customized to the organization's unique environment (indexes, naming conventions, exclusions, etc.) so they can be easily deployed to production with minimal effort.

Detection posture management solutions can be beneficial in several ways. First, organizations can improve their preparation for cyber-attacks by improving their utilization of existing SIEM/XDRs, while helping them operationalize MITRE ATT&CK with common references across detection technologies. Detection management can also help SOC teams extend detection engineering coverage across a growing attack surface. Finally, analytics-based detection posture management technology can help increase overall SOC productivity by reducing complexity while augmenting security engineers with automation assistance, freeing up their time and creativity to work on higher value activities like researching new and novel adversary techniques.

Introducing CardinalOps

CISOs face a dilemma—sound detection engineering is critical for operationalizing MITRE ATT&CK to reduce risk, but few firms have the advanced skills necessary. Most modern SOC teams rely on SIEM and XDRs to drive their detection and response processes, but the development of new detection content can lack the intelligence context and prioritization abilities provided by MITRE ATT&CK.

CardinalOps can help organizations address detection engineering shortcomings with a SaaS-based offering designed to help customers automate detection engineering for SIEM and XDR platforms such as Splunk, Microsoft Azure Sentinel, IBM QRadar, Sumo Logic, and CrowdStrike LogScale. By doing so, CardinalOps customers can benefit by:

- Uncovering MITRE ATT&CK coverage gaps. CardinalOps's SaaS platform takes less than an hour to deploy because it integrates via the SIEM and XDR native API and doesn't require agents (the platform supports both cloud-based and on-premises SIEM and XDR). Once it's connected, the platform audits prevailing detection rules and uses an AI engine to align these rules with the tactics and techniques defined in the MITRE ATT&CK framework. It then presents this data in a MITRE ATT&CK heatmap format, displaying actual coverage across the entire framework. Since covering the entire framework is unrealistic, the heatmap can filter by APT groups and asset types (Windows, Linux, containers, etc.) most relevant to the organization. The platform can also recommend missing detections and log sources that can be onboarded to address the highest-priority gaps. This

can help SOC teams prepare for specific cyber-adversaries and attack campaigns targeting organizations in their geography and industry.

- Uncovering gaps caused by broken and noisy rules. Beyond revealing MITRE ATT&CK gaps, CardinalOps can also detect broken and noisy detection rules that create false positive/negative conditions. This is a bigger problem than most SOC teams realize—CardinalOps estimates that, on average, 15-20% of detection rules are broken. Noisy rules also increase risk because adversaries can "hide" in the cacophony of noisy alerts that are often ignored by overworked SOC analysts. What's more, vendor-provided out-of-the-box rules are often disabled as they tend to be too generic and inaccurate without customization for each organization's unique environment.

  CardinalOps goes beyond detecting broken/noisy rules, however, by providing guidelines for tuning. For example, CardinalOps may suggest adding additional exclusions and conditional logic for tuning a noisy ruleset—such as excluding specific privileged users that regularly execute admin commands that can appear suspicious—improving threat detection accuracy and reducing alert fatigue. CardinalOps can also allow security teams to visualize the impact of changes before and after deployment, helping them test new and remediated detections on historical traffic before deployment (this can also be used as a lightweight threat hunting mechanism to identify past intrusions that may have been missed). Dashboards are also provided to help teams measure and drive continuous improvement of their detection engineering processes.

- Rapidly responding to high-profile vulnerabilities. According to CISA,[5] malicious cyber actors can develop an exploit within 48 hours of a vendor patch being released and quickly begin exploiting disclosed vulnerabilities in unpatched devices. This causes added pressure on detection engineering teams to develop new detections for high-profile vulnerabilities and zero-days as soon as they're announced (past examples include SolarWinds, Follina, Okta PassBleed, NotProxyShell, Exchange, etc.). CardinalOps can help by delivering deployment-ready, auto-customized detections within 24-48 hours of disclosure, thereby saving engineers time and effort in researching and developing these detections from scratch.

- Reducing SIEM licensing costs and optimizing utilization of existing security stacks. Security operations is complex, requiring lots of technologies and advanced skills. CardinalOps SaaS is designed to help organizations automate detection posture management to address security operations complexity. Aside from remediating coverage gaps and auditing and tuning existing detection rules, CardinalOps also provides recommendations for reducing growing data ingestion and storage costs, which have become problematic for security budgets in many organizations. For example, it does this by identifying log sources that are being ingested by the SIEM and XDR but not used for any detections, redundant log sources that are no longer required, and inefficient queries that can drive up Splunk Virtual Compute (SVC) costs.

In summary, by automating detection posture management, CardinalOps can help improve the utilization and optimization of SIEM/XDR and other threat detection technologies in use today. Additionally, CardinalOps aligns these technologies with MITRE ATT&CK. In this way, CardinalOps can help organizations advance their operationalization of MITRE ATT&CK.

[5] Source: U.S. Cybersecurity & Infrastructure Security Agency Press Release, *CISA Issues Emergency Directive and Releases Advisory Related to VMware Vulnerabilities*, May 2022.

The Bigger Truth

Driven by a growing attack surface and the dangerous threat landscape, security operations teams need an unprecedented level of scale, automation, efficacy, and efficiency. The MITRE ATT&CK framework is designed to help organizations address these requirements, as it provides structure and an adversary perspective to security operations. This could be a big help, but before operationalizing MITRE ATT&CK, organizations must address security operations complexity to better utilize their existing security stacks.

ESG believes that organizations can address security operations complexity and operationalize MITRE ATT&CK by improving threat detection management. This requires more focus on detection engineering by auditing/assessing existing threat detection methods, fixing broken detections, discovering/filling gaps, mapping and prioritizing missing detections with MITRE ATT&CK, and striving for continuous improvement.

This type of program won't be easy, requiring advanced skills, process automation, and strong knowledge of MITRE ATT&CK. Many organizations will need help in one or several of these areas. The CardinalOps SaaS offering is built to support organizations in each of these areas while improving the utilization of existing security stacks.

CISOs looking to operationalize MITRE ATT&CK by leveraging its intelligence to proactively drive the creation of new controls most relevant to their organizations—versus only using threat intelligence in a reactive way to investigate attacks—may want to learn more about how CardinalOps can help.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188