Quantifying the Gap Between Perceived Security and Comprehensive MITRE ATT&CK Coverage

AUTHOR: Yair Manor, Co-Founder & CTO @ CardinalOps

The Security Information and Event Management system (aka SIEM) is usually the centerpiece of the Security Operations Center (SOC), which is tasked with detecting and responding to attacks that circumvent an organization's threat prevention layer. While it is commonly observed that most SIEM deployments are ineffective, this new research validates beyond a doubt the truly poor efficacy of the average SIEM deployment.

Organizations spend over $3 Billion annually on SIEM software, and expect this investment to result in comprehensive threat coverage. However, analysis done by CardinalOps of SIEM deployment across multiple industry verticals reveals that threat coverage remains, in practice, far below what organizations expect and far below what the SIEM and detection tools can provide. Worse, organizations are often unaware of the gap between the theoretical security they assume they have and the actual security they get in practice, creating a false sense of security.

> **Buying security technologies seems to be a much easier task than utilizing them and 'operationalizing' them for many organizations. In fact, there is a lot more guidance on 'Which tool to buy?' and 'How to buy security right?' than on how to actually make use of the tool in a particular environment.**
>
> **– Anton Chuvakin, Google Chronicle / Former Research VP and Distinguished Analyst at Gartner**

SIEM MITRE ATT&CK Coverage

SIEM Configurations Miss 84% MITRE | ATT&CK® Tactics & Techniques

The most revealing data point in this research is that on average a SIEM deployment has rules associated with only 16% of the techniques listed in MITRE ATT&CK, an industry-standard catalog of tactics, techniques and procedures used by attackers. Considering that multiple rules may be required to fully cover a particular attack technique, we can conclude that the actual MITRE coverage of the average SIEM deployment is even less than 16%.

SIEM Rules

Many of the rules and policies organizations have in place are not effective. The research data shows that an average of 25% of SIEM rules are broken and will never fire, primarily due to fields that are not extracted correctly or log sources that are not sending the required data. However, organizations are completely unaware

25% of SIEM Rules are Broken /Nonfunctional

that these rules are not functioning. Additionally, just 15% of SIEM rules lead to 95% of the tickets handled by the SOC, demonstrating that a small percentage of noisy rules overwhelm SOC analysts with distracting false positive (FP) alerts.

95% of SIEM Tickets Are Driven by Only 15% of Rules

SIEM Maintenance & Support

From an operational perspective, SIEM and SOC tool configurations must be continuously maintained and updated due to the highly-dynamic nature of enterprise IT infrastructure and the organization-specific challenges that constantly arise. Unfortunately, most organizations are unable to commit sufficient engineering resources required to maintain and manage their SIEM. The research data supports this assertion in that a full 78% of SIEM vendors' "out-of-the-box" default rules are disabled by customers given that tuning and customizing these rules to fit the organization-specific needs is too time-consuming. On average, organizations add just 1 rule to their SIEM every month, which is not enough to close existing threat coverage gaps, let alone handle new threats.

78% Default Vendor Configurations Are Disabled by Users

The data also demonstrates that there is no correlation between the number of log source types sending data to the SIEM and the number of SIEM rules, which suggests that despite growing amounts of SIEM data and license fees paid to vendors there has not been a comparable improvement in threat coverage. This is hardly surprising considering that today's security engineering is a manual and error prone process, with organizations averaging just a single security engineering headcount for every 63 log source types.

Premise Health.

> **I evaluate emergent security solutions all the time, and the dynamic nature of systems feeding the SOC is as dynamic as the threat landscape itself. So the SOC infrastructure and the engineering that drives it has to be equally dynamic and automated, and it has to be able to compensate for high turnover and the challenges of finding qualified security engineering staff. CardinalOps is solving this core security operations business problem.**
>
> **– Joey Johnson, CISO of Premise Health**

Only 1 Security Engineering FTE is Allocated per 63 Log Source Types

Survey Methodology

This research study is based upon data analysis from large enterprise SIEM deployments. The data was collected from numerous large enterprise customer deployments, including deployments representing all the leading SIEM vendors - Splunk, IBM Qradar, SumoLogic, and others (For more about the data set, see the footnote below.) The baseline data set normalizes data inputs across the various proprietary vendor schema so that it could be analyzed as a single data set.

The data set was used to identify operational trends in live security operations centers (SOCs) in order to illustrate SIEM effectiveness. While it is generally assumed that the SIEM functions as both the ultimate data repository for event logs and the core incident ticketing system for security analyst triage, we wanted to understand if live deployments support those assumptions.

The data set includes a broad array of general information about the Enterprise SIEM deployments referenced in our study, including the following:

	# active rules	# active source types	# active sources	# daily tickets
Median	74	80	904	95
Mean	137	85	1533	7278

***About the Data Presented**: The research data presented in this paper represents an aggregated, anonymized summary of ten select CardinalOps customers. All but one of these selected customers are multi-billion dollar multinational corporations representing numerous industry verticals, including healthcare, media, financial services, hospitality and beverages. The aggregate data was collected directly from these customers' SIEM systems and related IT tools.

CARDINALOPS

About CardinalOps:
CardinalOps Threat Coverage Optimization (TCO) Platform delivers AI-based analytics and automation to critical security engineering functions to ensure comprehensive threat coverage by SIEM and SOC tools. The TCO Platform quantifies and enumerates the gap that exists between theoretical optimum threat coverage, represented by the MITRE ATT&CK framework, and actual threat coverage, measured by actual SIEM and SOC tool configurations. The TCO Platform was built to close that Threat Coverage Gap by providing real-time configuration change and misconfiguration fix recommendations that are unique to each organization's capabilities and threats. CardinalOps was founded in 2020 by a team of cybersecurity veteran entrepreneurs, is backed by blue-chip investors, and is based in Silicon Valley and Israel. For more information, please visit: www.cardinalops.com.

cardinalops.com | info@cardinalops.com