ACHIEVING SIEM EFFICIENCY THROUGH PROACTIVE VALIDATION

CYNODE.

WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Security Information and Event Management (SIEM) has been a key technology in managing cyber risk over the last 15 years and enterprises have been allocating large sums to SIEM solutions in both capital and operational budget lines. Nevertheless, industry surveys year after year reveal that SIEM users are not satisfied with their investments. SIEM solutions are often perceived as difficult to manage, prone to generating excessive alerts, and slow to detect malicious activities. Concepts such as "intelligence-driven SOC", "orchestration and automation," and "managed SIEM" help alleviate some of the challenges but fall short in ensuring consistent, precise, and timely detection performance.

Proactive Validation: the most effective way to get the most out of a SIEM solution and enhance the efficacy of a SOC. The proactive nature of this concept provides continuous validation, as well as scheduled or ad-hoc assessment capabilities. Utilising real cyber-attack simulations helps to identify gaps in the SIEM functionality, SOC processes and provides numerous opportunities to prevent real attacks:

- can apply threat-centric analytics to identify detection gaps at the adversary behaviour level.
- can automate and therefore diversify emulation to thousands of scenarios.
- provide detection and prevention content for instant risk mitigation;
- and enable purple teaming as an easily repeatable capability.

Proactive Validation powered SIEM

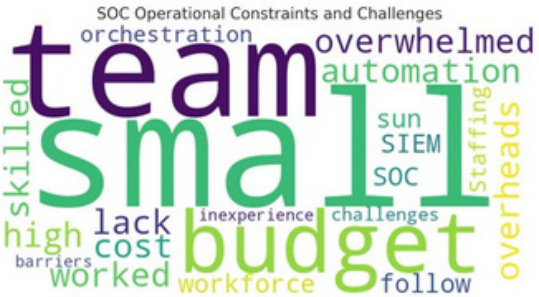
The concept of proactive validation is not new; it began to gain traction around 2013 and has steadily attracted interest from many organisations since then. Initially, its application was primarily limited to assessing Next-Generation Firewalls (NGFW) and Web Application Firewall (WAF) solutions. With technological advancements, this threat-centric approach can now be applied to email gateways, Endpoint Detection and Response (EDR), and SIEM platforms. This evolution enhances SIEM efficiency and improves return on investment (ROI) benefiting a broad range of stakeholders, including CIOs, CISOs, SOC managers, security analysts, and compliance teams.

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/

INTRODUCTION

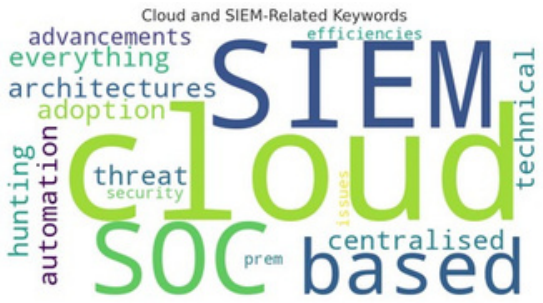
Security Operations Centres (SOCs) are integral to an organisation's cyber security strategy, serving as the hub for monitoring and responding to security threats. With the SIEM solution acting as a central point for telemetry and log data from a wide range of IT systems including network security devices like firewalls, WAF as well as more complex security solutions like CASB and EDR. SIEM technology was introduced as a new category in 2005, and much has changed since then. Networks have grown, become more interconnected, and versatile and as a result, cyber criminals can exploit these characteristics, gain greater impact and take advantage of an expanded attack surface

- The most common SOC size remains small, with 2–10 staff members, consistent with trends
- Staffing challenges are prominent, with the lack of automation and orchestration identified as the top barrier followed by high staffing requirements and a lack of skilled staff
- Most SOCs operate 24/7, with about half employing a "follow-the-sun" model and allowing remote work for SOC staff.
- Visibility remains a challenge, particularly with decreasing use of TLS interception technologies and reliance shifting towards endpoint protection tools



Even with the technological advances that have been made these interesting quotes from a recent SANS study show organisations still struggle to effectively manage, cyber security incidents, and many of the issues relate to staffing issues, lack of automation and visibility. The issues highlighted here have been made more complicated by technological advancements that have happened alongside the progress made in the SIEM field. Cloud infrastructure wasn't even invented when SIEM solutions were initially being deployed, "cloud" is now ubiquitous and thriving, it brings new efficiencies and new issues to deal with.

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/



- Cloud-based SOC architectures have overtaken single, centralised SOCs as the most common setup, reflecting a broader IT trend towards cloud adoption.
- The approach of "SIEM everything" is gaining traction, with 38% of respondents in 2024 indicating a strategy of ingesting all available data into the SIEM, up from 29% in 2023. This shift suggests a preference for comprehensive data analysis over selective data filtering.
- There is a notable rise in vendor-based threat hunting automation, with 46% of respondents indicating partial automation of threat hunting activities, up from 38% in 2023.

To Further complicate matters other, new technologies like Machine Learning (ML) and Artificial Intelligence (AI) have been integrated in existing technologies including SIEM tools and did not provide all the expected results leading to a lack of satisfaction. This low satisfaction score may have been made worse because it is so difficult to provide meaningful reporting and metrics.

- Artificial Intelligence and Machine Learning (AI/ML) technologies have seen declining satisfaction, with a GPA dropping from 2.17 in 2023 to 1.99 in 2024. AI/ML Generative technologies (GPT) ranked lowest, with a GPA of 1.80.
- This decline in satisfaction with AI/ML suggests either unmet expectations or a maturing understanding of the technology's limitations within SOC environments.
- 67% of respondents (260 out of 384) indicated that they provide metrics to senior management to justify SOC resources. This is a slight increase from 66% in 2023 but a notable decrease from 74% in 2022.
- The decline in the use of metrics may reflect a shift towards more sophisticated approaches or changes in organisational priorities regarding SOC performance measurement.

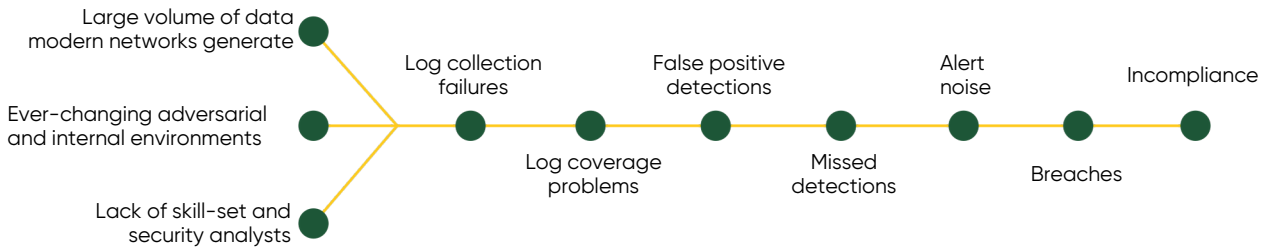
The observations from the SANS SOC Survey report represent the issues faced by organisations trying to manage a SIEM solution as part of its overarching SOC initiative and these issues are broadly similar to those experienced by those in the past and much of this relates to the complexity in validating logs, difficulty in improving the detection baseline and inability to provide meaningful monthly reporting.

This situation adds weight to the argument that utilising threat centric proactive validation will provide a way to increase both the usability and effectiveness of existing SIEM infrastructure and a way to more readily configure new SIEM solutions during the initial deployment.

CHALLENGES IN EFFECTIVELY OPERATIONALISING SIEM

Three Main Obstacles For Efficiency

In the discussion of SIEM efficacy or rather inefficacy, three fundamental challenges put a strain on SIEM capabilities. Extensively debated SOC problems of false positives, alert noise, missing detections, long dwell time, and other issues that are related to the SIEM efficacy are the symptoms of not combating these three challenges effectively in the first place.



1) The Large Volume of Data Modern Networks Generate Regardless of how advanced a SIEM technology may be, it fundamentally relies on the scope and quality of data it collects and processes. Even though "the more log, the better" sounds like a reasonable proposition, the massive volume of data modern networks generate today requires SOC teams to handle log management more creatively and selectively.

On average, the network of a thousand-employee organisation with a moderate infrastructure generates over 6GB of data a day6, in large organisations, this number goes up to level of terabytes. The good news is not every log has the same importance for cybersecurity practices. The bad news is selecting the right logs with the right level of verbose is not such a straightforward task. SOC teams need to strike the right balance where licensing, processing and storage capacities of a SIEM are not put under strain, and at the same time, logs of malicious activities are not kept out of scope.

2) Ever-Changing Adversarial and Internal Environments

Data sets and detection rules on SIEMs are susceptible to being out of date due to the rapid changes happening in networks and the adversarial landscape. Each new application, network and user device may mean a new vulnerability and data source at the same time. New attack techniques and threats may also require new data sources to be ingested to detect them.

Adapting detection rules to external and internal changes is a challenge of its own. This is a process similar to and as hard as software development. Firstly, detection engineers need to have advanced cybersecurity and software skills to develop rules. Secondly, rule development is a tedious process by nature. It takes time to develop rules and if not handled well, they can cause false alerts or may not generate alerts when they should have.

3) Lack of Skill Set and Security Analysts

While SIEMs heavily rely on human power for planning, setting processes and successful execution, Gartner ranks "SIEM expertise" among the most difficult to find skill sets in its 2020 IT Skills Roadmap report7.

Assigning right priorities to alerts, managing log sources, quick and effective detection engineering, improving processes, ensuring collaboration between junior and senior team members and other key SIEM tasks require the right level of expertise to be in place.

Organisations need to find ways to empower SIEM users by ways of training, automation, and taking a proactive approach to preempting repetitive tasks.

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/

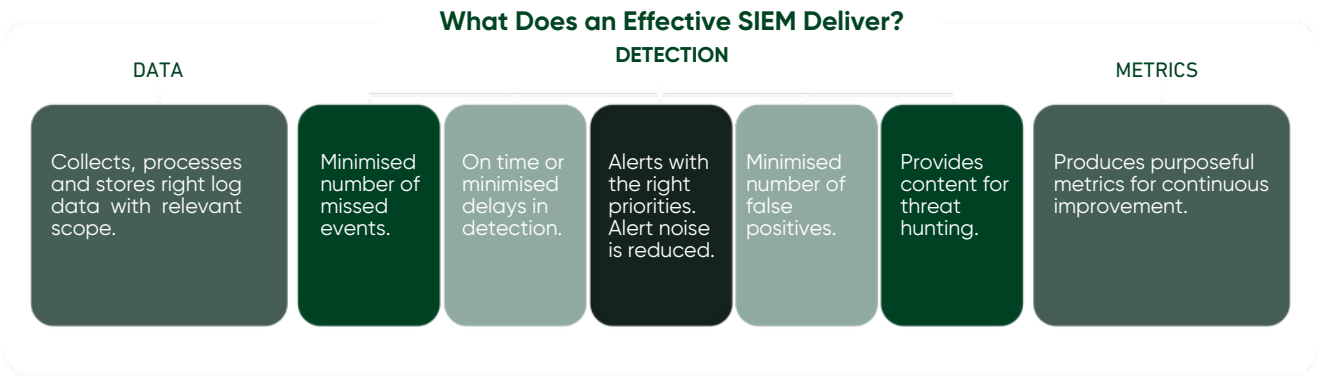
CYNODE.

WHAT
AN EFFECTIVE SIEM DELIVERS

"SIEM Everything"

In the SANS 2024 SOC Survey reveals a trend where organisations increasingly opt to ingest all available data into their Security Information and Event Management (SIEM) systems rather than selectively filtering relevant data. This approach, termed "SIEM Everything," has grown in popularity as it may be more economical than spending extensive engineering resources to determine what data is necessary before collection. In 2023, 29% of 600 respondents reported using this strategy, while in the current year, 38% of 403 respondents indicated the same approach, showing a notable increase in adopting this method.

The shift towards ingesting all data into SIEM systems, while potentially reducing the upfront effort and cost, raises challenges such as increased noise, false positives, and higher storage and processing demands. These challenges can lead to alert fatigue among SOC analysts and potential performance issues. However, organisations may find the comprehensive data set beneficial for detecting unknown threats. While the survey shows that this "SIEM Everything" method is a trend and suggests that while this method may reduce the initial costs associated with engineering efforts, it requires careful management and advanced SIEM capabilities to handle the large volumes of ingested data effectively and maintain a robust security posture.



Going Deeper in Detection Analytics

Having an effective SIEM comes down to keeping detection on par with internal IT and adversarial changes. The next chapter lays out five practical guidelines for SOC managers and engineers in running SIEM platforms effectively.

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/

FIVE KEY SIEM USE CASES ENABLED BY A THREAT-CENTRIC APPROACH

USE CASE 1:

VALIDATE LOGS AND SELECTIVELY ADD NEW LOG SOURCES

USE CASE 2:

IMPROVE THE DETECTION BASELINE

USE CASE 3:

EMPLOY THE DETECTION AS CODE PRINCIPLE

USE CASE 4:

ESTABLISH AGILE THREAT HUNTING PROCESSES

USE CASE 5:

DEVELOP METRICS THAT MATTER

CYNODE.

USE CASE 1:
VALIDATE LOGS AND SELECTIVELY ADD NEW LOG SOURCES

Right Log Versus Not So Right Log

The quality of SIEM outputs depends on the quality of data it processes. Ideally, SOCs should deal with advanced attack behaviors. Low-level indicators of compromises (IoC) such as hash values, domains, IP addresses should be either detected or prevented by defense technologies such as firewalls and web proxies. Using SIEMs for detecting quickly changing IoCs would mean using event per second licensing capacity, storage and data processing resources inefficiently. Creating low-quality alerts would steal away from the valuable analyst time. SOC teams employ a risk-based log management policy that will continuously provide the right logs so that SIEMs can process required data to detect advanced adversarial techniques, tactics, and procedures.

"Efficient" Log Management

Efficient log management makes sure that SIEMs consistently ingest logs from the right log sources with the right detail at the right time.

RIGHT SOURCE	RIGHT DETAIL	RIGHT TIME
The log coverage should be comprehensive enough not to miss important security events and also specific enough to discard data that does not add relevant or good-enough context.	A SIEM may have received the logs but the event types and event attributes may be poor to detect events. Or, conversely, logging may be in the verbose level that burdens the SIEM platform with unnecessary details.	Timing of the log delivery is another key factor in detecting incidents early on. There are multitude of reasons why logs may not be delivered in time. For instance, infrastructural network issues or policy misconfigurations may delay the log delivery.

Change is Your Enemy if You Cannot Keep Up

Networks live with change. At any time, a new machine or network device can be deployed, or cloud instances can be launched for a few days or hours and then get shut down. Every change may mean a new or obsolete log source. New attack techniques and campaigns may also require new log sources and attributes to be included. For example, attackers started obfuscating PowerShell commands to evade security controls and stay under the radar. Once this new TTP activity is identified, it has become necessary to collect logs from Windows Event ID 4104 to detect obfuscated PowerShell commands, which was not a required log source before.

Today's most widely adapted log validation approach is based on detecting interruptions in the log flow by defining a time threshold. This approach falls short of providing proactivity in linking the existing log content with changes that happen in internal and adversarial environments.

Focusing on TTPs Can Help Build Robust Log Management!

An integrated and TTP-centric log validation helps SIEM practitioners keep up with the changes, consistently identify the right sources, define the right detail, and ensure timely delivery.

Log Management Best Practices:

Proactively validate log status for a particular threat or an adversary group	It is critical that SIEM platforms receive logs that new threats may generate. Threat actors and groups such as FIN7, Lazarus, Nobelium continuously update their sophisticated and staged attacks such as Carbanak, PowerRatankba, Sunburst. As an example, APT-38 Power Ratankba contains 12 unique actions, starting with System Information Discovery, continuing with System Network Configuration Discovery, System Network Connections Discovery, and going all the way to C2 Over HTTPS Port 443. Using an integrated attack simulation platform, a security analyst can safely replicate APT38 Power Ratankba actions or analyse the findings of scheduled assessments. If there are actions that no logs are identified for, SOC teams can proactively request IT teams to fix the log gaps.
Look for new detection opportunities in your security stack	If a threat is not detected on the defense layer, no logs are generated and SOC teams have no way of knowing what type of malicious events that particular threat may be generating in the network. Simulating a wide set of threats across the security stack regularly on a 24/7 basis reveals gaps on the defense layer that SOC teams were not aware of.
Look for new detection opportunities in your IT environments	Many organisations do not leverage log sources such as windows security events, sysmon, and PowerShell. This is mainly related to the high volume of logs generated from these sources. Selectively adding endpoint logs to SIEMs helps identify advanced threats that hide in networks. Enabling relevant log sources based on the guidance provided by ad-hoc assessments can help quickly address logging gaps. Additionally, 24/7 validation helps build a SOC capability for monitoring gaps, tracking changes, and logging enhancements on a daily or weekly basis.
Visualise and measure log coverage based on MITRE ATT&CK	Mapping log coverage to MITRE ATT&CK techniques helps identify gaps against new threats, new variants and monitor positive and negative log coverage changes.
Proactively identify missing or delayed logs due to delivery & collection problems	Due to configuration mistakes, network-related delays, API limitations, changes made by the IT teams, and other possible reasons, a SIEM may not have received some logs despite logs being generated at the source. Such problems may also create time gaps in log delivery. Continually or frequently running attack simulations by using a large threat sample database, reporting the delta between how security controls responded and what the SIEM has seen help spot such failures with no delay.

CYNODE.

USE CASE 2:
IMPROVE THE DETECTION BASELINE

What is Your Detection Baseline?

Quality and scope of detection rules are the most important factors in efficient alert management. If detection rules are missing, narrow in scope, or poorly written, no alerts are generated, malicious activities go undetected and create a significant level of cyber risk. If the scope of detection rules is too broad, with no precise intent, the number of false positives and alert noise increases. Therefore, it is imperative that SOC teams first identify and improve their detection baselines.

Exercises such as cyber tabletop and purple teaming provide attack readiness visibility that different security teams can benefit from and boost coordination and alignment. As a result, prevention and detection baselines can be improved. However, the challenges with such exercises are related to repeatability and scope. While internal and adversarial environments are constantly changing, time-bound practices become outdated soon after they are completed. Furthermore, these practices can assess only a limited number of attack scenarios.

Automated Validation: The Only Sensible Way

Alert triage is an after-the-fact process. Manual handling of alerts does not scale. Automated alert triage does not go deep enough to identify new, sophisticated and targeted indicators of compromises. SOC teams require a proactive alert validation process to identify redundant and obsolete rules and incomplete and ambiguous use-cases while adding new high-quality detection rules to address new adversarial tactics, techniques, and procedures. Automated validation is the only sensible way to lower the number of alerts and ensure that security analysts receive relevant alerts.

An integrated threat-centric approach, utilising a comprehensive and carefully curated threat library, can effectively challenge and refine detection rules and help:

- identify missing, redundant, and obsolete rules against the adversarial TTPs;
- identify the time gap between event generation and alerting;
- challenge and train teams with new scenarios; and
- kick start the detection rule generation process.

Look For The Quick Fixes & Establish Further Processes

Applying a threat-centric approach to challenge detection rules with a comprehensive set of threats can help identify missed detections based on MITRE ATT&CK tactics and techniques, threat categories (such as malware/ransomware, vulnerability exploits, and web application attacks/cross-site scripting), as well as targeted applications and operating systems. To identify quick fixes, SIEM teams should use search filters to shortlist attacks that:

- are detected but not blocked by security controls;
- their logs exist in the SIEM platform; and
- no alerts generated.

For the short-listed attacks, moving the policy to prevention at the control level would lower the workload of the SOC teams. Secondly, as logs exist on the SIEM, detection rules should be implemented against these attacks to improve the detection baseline quickly. Once quick fixes are implemented, SIEM users should attend to prevention and log level gaps, and establish regular processes to proactively address t hem.

CYNODE.

USE CASE 3:
EMPLOY THE "DETECTION AS CODE" PRINCIPLE

How Quickly Can You Develop Detection Rules?

Identifying detection gaps is a good start on the route to SIEM efficacy but closing those gaps is a task of its own. The capability of building high-quality rules in a short time and maintaining a robust rule base eliminates inefficiency symptoms of false positives, alert noise, missed events, and regulatory noncompliance. On the other hand, detection engineering is no easy task. It requires meticulous and long hours of work, a rare comprehensive set of information technology, software, and security skills.A 2020 survey by Picus Security's Customer Success Team found out that it takes seven hours on average to write a detection rule. This duration is longer if the detection rule aims to address complicated advanced threats. Due to the cost, length, and complexity of developing and adding new rules, companies either work with a limited or a generic ruleset.

Detection As Code

"Detection as Code" is relatively a recent concept laid out by Anton Chuvakin. Detection as Code is not a shortcut or a silver bullet, but rather, it proposes to build a model to tackle detection engineering challenges wisely. As the terms suggest, it proposes to build an infrastructure based on software development principles. Mr. Chuvain sets "detection content versioning", "proper QA", "content reuse and modularity" and "continuous improvement & development" as the main characteristics of this model. The bottom line is to develop or obtain high-quality detection rules consistently as an organisational capability.

What is a High-Quality Detection Rule?

David Bianco's Pyramid of Pain and MITRE ATT&CK framework provide the principles of keeping a high-quality rule base. In developing detection rules, focusing on the TTPs and attack campaigns' behavioral patterns, rather than easily changing attributes such as IP and domain name, increases the efficacy, precision, and life span of detection rules. MITRE ATT&CK as a framework provides an excellent base in tracking to what extent TTPs are covered in the detection rule set.

"Detection as Code" Supported by Proactive Validation

Proactive validation using a threat-centric approach enables SIEM teams to develop an iterative detection engineering infrastructure and provides three key benefits:

- Automated gap analysis help prioritise where detection engineering efforts;
- It offers proper quality assurance through in-depth validation of defense capabilities; and
- Continuous improvement to keep up with the changing threat landscape becomes an organisational capability.

Utilise Third-Party Detection Rules

SIEM users can obtain detection rules from both free and paid sources. SIEM managers should prioritise using detection rules from reliable sources and promptly address any detection gaps.

USE CASE 4:
ESTABLISH AGILE THREAT HUNTING PROCESSES

CYNODE.

A Crucial Step For Proactivity

The 2024 SANS SOC Survey highlights an increase in the automation of threat hunting activities using vendor-provided tools. Threat hunting aims to detect compromises that alerting systems miss, often through retroactive analysis of historical data with newly discovered indicators of compromise (IOCs). Automating these processes can make threat detection more efficient, but there are limitations to this approach.

The survey suggests that while automating retroactive analysis is useful, it represents only the "bare minimum" for effective threat hunting. True threat hunting requires a more sophisticated, proactive approach that actively seeks out previously undiscovered threats. The recommendation is to continue automating routine tasks to reduce workload but also to invest in advanced threat hunting techniques that enable the detection of more complex and emerging cyber threats.

46%

reported their threat hunting activities are at least partially automated using vendor-provided tools

38%

reported partial automation with vendor tools in 2023.

8%

rise in the adoption of vendor-provided threat hunting automation tools.

Why Has The Adoption of Threat Hunting slow?
Threat hunting is reasonably straightforward as a concept, but, it is technically challenging and therefore its adoption has been slow.

Some of the challenges:

- Developing the right hypothesis and deciding where to start from, needs contextual understanding.
- Acquiring and verifying the syntax that identifies threats and TTPs is time-consuming.
- Threat hunting is dependent on the availability of data.
- Threat hunting is dependent on highly skilled cyber security professionals.

Some Threat Hunting Hypotheses Examples

- There may be an APT29 related activity in my network.
- Sunburst malware was first released last April. As a result, there may be relevant events in our network dated back to April.
- There is a new Trickbot malware variant out in the wild. This new variant may be in our network.
- This specific malicious URL may have been accessed from our endpoints.
- Some of our applications in our infrastructure may have accessed this malicious IP address.

Threat-Centric Threat Hunting Improves SIEM Log and Detection Coverage

SIEM platforms are one of the most relied-on technologies by threat hunters. A SIEM pulls together a huge pool of data from the environment, and can apply advanced analytics, providing the opportunity to look for traces of adversary behaviour. Subsequently the findings of threat hunting practices help improve logging and detection gaps in numerous ways:

- provides information about specific procedures used by a threat group to execute an attack technique;
- provides specific search queries to detect a technique and show relevant data sources;
- helps validate log collection for each TTP and threat specifically; and
- findings can guide threat hunters in building hypotheses

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/

USE CASE 5:
DEVELOP METRICS THAT MATTER

Metrics or No Metrics

The use of SIEM and SOC metrics remains staggeringly weak to convey actionable and meaningful insights. The "Common and Best Practices for Security Operations Centers: Results of the 2019 Survey"10 by SANS reveals that most SOC users settle with the metric of "the number of incidents handled" solely because that is easy to quantify. A lesser number of SIEM users go after more difficult metrics such as "incidents closed in a shift" or "time from detection to containment." Yet, those metrics are far from depicting SIEM efficacy for tackling advanced threats.

Another Survey11 by SANS revealed that three top barriers for using metrics effectively are:

- lack of appropriate automation;
- lack of well-defined requirements for metrics; and
- desired metrics not easily measurable.

Threat-Centric Simulation Produces Actionable Metrics

Metrics focused on fundamental SIEM processes have the potential to improve SIEM efficacy bottom up. Utilising a threat-centric approach can help address the issues covered here on different levels and help build metrics to ensure a healthy SIEM foundation, while providing:

- *baseline metrics for log coverage*
- *metrics to ensure a healthy log collection infrastructure and*
- *metrics for detection coverage vis a vis MITRE ATT&CK TTP coverage.*

CONCLUSION

If you have a SIEM solution, it means you have a very powerful tool in your arsenal to tackle advanced cyber attacks. Utilising a threat-centric approach can help address the fundamental challenges security teams face in making effective use of SIEM solutions, build new capabilities for continually improving detection performance and optimise ROI. CISOs, SOC Managers, SOC Teams, and Risk & Compliance Teams collectively benefit from this preemptive approach strengthens the overall security posture and lowers cyber risk.

CYNODE.

ABOUT CYNODE.

Who We Are We are a dedicated technology provider operating in the Nordics and the UK, offering robust cyber security services to swiftly enhance our clients' security posture and develop long-term cyber risk mitigation capabilities through cost-effective subscription models.

Cyber Risk Factors We Tackle:

- **L**ack of security posture visibility: The seemingly straightforward question, "are we secure", is challenging for many organisations to answer. Cyber security practitioners often operate in the dark and need empowerment.
- Inefficient use of the technology investments: The under utilisation of technology investments is a common issue across various industries. Companies invest in solutions like EDR, SIEM, WAF, NIPS, and others, but these defensive capabilities are often not used to their full potential.
- Talent scarcity and unaffordable services: Numerous independent reports suggest a shortage of up to 4 million employees in the cyber security field. Organisations struggle to hire or gain access to experienced domain experts because they are either non-existent or too expensive to employ.
- Difficulty of detecting and responding to advanced attacks: Many organisations either lack detection and response capabilities, or struggle to mobilise these functions quickly and effectively.

CYNODE.

www.cynode.com

CYNODE.