SER SOLUTIONS FOR SECURITYOU



INTRODUCTION

Security Information and Event Management (SIEM) solutions have been around for over a decade. These types of solutions promise a holistic view of what is happening in near real-time across an organization's IT estate by ingesting log and event data generated by assets across an organization's infrastructure. Once the data is collected correlation rules (sometimes called rule sets) are applied to detect and categorize threats. When a rule is matched an alert is triggered indicating a security incident to be investigated. Given the data is centralized, the SIEM may also be used to investigate the security incidents eliminating the need to log into dozens of consoles.

For many organizations SIEM's appeal to their optimistic sense of what is possible. Unfortunately, many organizations realize after their purchase the full cost and resource burden. For security professionals and strategists it's important to understand these challenges as well as understand there are other ways to achieve the desired security outcomes.





MODERN THREATS REQUIRE INSIGHT BEYOND BASIC SIEM CAPABILITIES

To identify threats, a SIEM as only as good as the inputs and detection rules which were originally designed for onpremise environments. They have evolved a bit over the years but still have significant challenges when it comes to securing the cloud. One the these areas is securing web applications which have become a prime target for bad actors the past few years to gain access, build footholds, and move laterally. According to the Verizon 2019 Data Breach Investigations Report, web application attacks are the number one attack vector and have been for multiple years. The most prevalent attack methods were SQL Injection and remote code execution, sophisticated attack methods which likely would have been missed by a SIEM.

		· ·		
ORACLE 🛞 SAP SharePoint	WEB APPS			
APACHE Beschange	SERVER-SIDE APPS	ž	Web App Attacks	1. Wide range of attacks at every layer of the stack
Catepre Cspring django Drupol"	APP FRAMEWORKS	THE STA	0WASP	2 Rapidly changing codebase can
🐇 Java 👷 極 🧏 🍘	DEV PLATFORMS	L UD DN	Top 10	introduces unknown vulnerabilities
ORACLE MySQL PastersQL SQL Server	DATABASES	KE MOVI	Platform/	3. Long tail of exposures inherited from
🧠 redhat 🛛 🕄 USE Ubuntu®	SERVER OS	KERS AF		3rd party development tools
vmware Reproject	HYPERVISOR	ATTAC	System/ Network	4. Extreme shortage of cloud and
aws 🔥 Azure	HARDWARE		Allauns	application security expertise
			and the second	

SIEM TOOLS ARE CHALLENGED WHEN TASKED WITH PROVIDING FULL STACK VULNERABILITY DATA AND INSIGHT

In order to protect against web application attacks the organization would need to purchase a Web Application Firewall (WAF), deploy it, send data to the SIEM, and write new rules. This holds true for all additional security controls added to protect against modern threats.



CONSTANT TUNING FOR ACCURATE AND ACTIONABLE INSIGHTS

In the early stages of a SIEM deployment there will a set of rules for common use cases. When a rule is matched an alert is triggered indicating a security issue to be investigated. However, the volume of alerts quickly becomes overwhelming making the task of investigating each of them near impossible. A 2019 study by the Ponemon Institute reveals only 45% of alerts from SIEM deployments can be investigated on a daily basis. The problem is there is little to no context about the alert so every alert is treated with the same level of criticality. Eventually the security team will be drowning in a sea of alerts causing alert fatigue which allows attacks to slip by because the analysts are ignoring the alerts.

This is where the ongoing maintenance burden comes into play because SIEMs require constant tuning. Correlation rules need to be tweaked and new ones need to be written to increase accuracy to reduce the number of alerts to investigate. This must be done by a person with strong expertise. If they don't have this expertise they pay extra to get this done as the tuning is needed to start filtering out some of the noise to find the needles in the haystack as well as actionable insights for the people responsible for remediation. While this phase of tuning will help reduce some of the noise and surface the needles in they haystack there are still lots of needles all of which are important so additional context is needed to help prioritize the needles. This is where advanced analytics gets introduced which is an additional cost.

COSTLY ANALYTICS NECESSARY FOR CONTEXT

It seems obvious that you want to block all known bad activity and allow all known good activity. But the grey matter in the middle that is "suspicious" or unknown is substantial. Many attacks look like noise so they can better hide in the grey area. Achieving context with SIEM requires expertise and often additional analytics modules with added expense and complexity.

"SIEM is complex and requires serious expertise to maintain and deploy properly. They require resources and knowledge to write good rules. The out of the box correlations rules solutions come with, which some enterprises may rely on to avoid the hard work of deployment, are often not sufficient to cover your enterprises' needs.¹"

BEN CANNER, SOLUTIONS REVIEW

The SIEM may offer a User Behavioral Analytics (UBA) or a User and Entity Behavioral Analytics (UEBA) module to enrich large data sets and use data models to add context and prioritize the alerts. Some vendors call this combination of technologies "Next Generation SIEM" which requires more infrastructure, more professional services for deployment, and another technology that will require tuning. In many cases it will also require the most advanced support level as well due to the complexity level of the solution. This new solution of Next Generation SIEM or SIEM with UEBA is necessary to gain valuable insights by providing the following detection methods:



- Signatures and rules that detect known malicious patterns such as exploits against vulnerabilities or transactions that violate specified parameters.
- Anomaly detection that compares real time activity against baselines to flag unusual behavior such as HTTP requests and responses with characteristics beyond the established normal range.
- Machine learning that detects new threats and improves detection accuracy without being explicitly programmed where to look by iteratively using computer-generated algorithms. Machine learning is particularly good at detecting multi-stage, multi-vector attacks that don't match existing signature patterns or anomaly parameters. It can also help overcome the fragility of SIEM rules that are not properly maintained.

In fact, The Ponemon Institute surveyed SIEM users and provided valuable insights into the importance of security analytics. It found that organizations are 2.25X more likely to identify a security incident within hours or minutes when they are a heavy user of big data cybersecurity analytics". At the same time the study found that security analytics is considered difficult by 64% of respondents with the greatest challenges being lack of in-house expertise, insufficient technologies, and insufficient resources.

SIEM ALERTS REQUIRE INTERPRETATION AND TRIAGE

A critical and often over looked factor in getting value from a SIEM effort is the requirement for interpretation and triaging of events and alerts. Once threats are detected, organizations require clear event and incident information to understand their potential impact, to triage, and to respond with remediation. SIEM alerts require interpretation and validation by security professionals in order to determine what to do about the alert. If you lack security experts to turn detection into response, a SIEM will not help you. Difficult to staff and retain, security analysts are an expensive cost component that is frequently overlooked.

The organizations that have this component find them drowning in alerts as it's not possible to investigate all of the alerts regardless of the amount of tuning and advanced analytics. In fact, they spend 25% of their time chasing false positives according to the 2019 Ponemon Institute Report mentioned earlier. Anton Chuvakin (former Vice President and Distinguished Analyst at Gartner) once wrote in a blog explaining that alerts "need to be reviewed via an alert triage process in order to decide whether they indicate an incident, a minor "trouble" to be resolved immediately, a false alarm or a cause to change the alerting rules". Only after an alert has been reviewed does it become an incident requiring immediate incident response. The Target breach of 2013 is a highly-visible example of a failure of alerts and 'actionable intellegence'. Despite million dollar security systems, the security analysts were drowning in alerts and unable to prioritze the ones that had the highest impact on the organization.

You will need to add additional staff or resources for interpretation and triage. With today's amount of detection data, just signaling an alarm isn't enough. The operator/analyst must be able to understand the risk as well as provide recommendations for each incident, in order to be able to prioritize action.



UNDERSTANDING THE FULL COST BURDEN OF SIEM

SIEM is a powerful platform, requiring substantial investment of time and money to implement, configure, keep current, to learn, and to use. Despite SIEM technology's long tenure, many SIEM initiatives simply fail to launch while many others grossly exceed planned budgets and timelines.

Although a SIEM can be purchased for less than \$100,000, it is common for fully operationalized implementations to cost around \$1 million with \$30,000/year in software maintenance fees alone. In addition, you will need to add analytics, threat intelligence feeds and more. Your storage, network and compute infrastructure will need to accommodate growth as your SIEM use matures. Professional services are typically required to stand up a SIEM and often for ongoing updates, new rules, new assets and changing workloads.

Gartner says, "Many security organizations underestimate the amount of planning required before purchasing, implementing and operating a SIEM solution, and hit a hard stop once this becomes clear." They go on to estimate, "For a typical midsize bank, a minimum staff of eight to 10 is required to run a dedicated 24/7 security event monitoring operation". (Gartner, Overcoming Common Causes for SIEM Solution Deployment Failures, May 2017)

OPERATIONALIZING SIEM REVEALS MORE RESOURCE BURDENS

A SIEM will typically prioritize threats detected to help the Security Analyst focus on issues of most concern. Yet expertise is still required to triage and respond to incidents as they arise and to refine and tune detection rules.

The bulk of the on-going effort required of a SIEM is to monitor and investigate identified alerts. Security and IT staff typically waste 25% of their time investigating unreliable alerts while actual breaches go undetected an average of 206 days, according to 2019 Ponemon Institute report. Again, the Target breach of 2013 is the most famous example of the importance of reviewing security alerts. Target did have alerts triggered by various security controls indicating they were under attack, but they were not investigated. O

Once you have evaluated the costs and commitment required to implement SIEM, consider your alternatives There is more than one way to improve your security posture and detect threats. While SIEMs are a traditional approach, they are most useful for organizations that have a well-staffed security program. A SIEM alone is not the best solution for monitoring threats against today's web applications and cloud environments. Analytics and additional effort is generally required. They are expensive and labor intense requiring a substantial commitment of time and security expertise. The full commitment may not be apparent at the outset.



ALTERNATIVES TO ACHIEVE NEEDED OUTCOMES

Every organization wants to increase their security while reducing risk and reducing costs. Security leaders would be wise to self evaluate to understand what outcomes they want and where they may be gapped to achieve those outcomes. In many cases organizations come to realize they either don't have the expertise to fully understand how to solve their security and compliance problems or they know exactly what to do but don't have the time or the staff to deliver the security outcomes they need.

An alternative quickly gaining popularity is Managed Detection and Response (MDR). This is a service that delivers the outcome of quickly letting the customer know what incidents matter and what to do about it. The MDR vendor typically uses a platform to collect the data, in-house security expertise analyzes and enriches the data, they provide the remediation guidance, and also handle the constant tuning to reduce false positives. An MDR provider can also provide community defense and rapid protection for critical threats by actively tracking new vulnerabilities and emerging threats across their large install-base. These functions enable organization to achieve 24/7 monitoring in a predictable pricing model at a fraction of the cost of owning a SIEM.

Alert Logic, a pioneer in MDR, provides managed threat detection as a service, fully deployed and operational in days at predictable monthly subscription costs. The service monitors your IT environment and uses advanced analytics to identify threats. It includes all the necessary effort behind the scenes such as implementation and maintenance of monitoring systems like WAF and IDS, their integration with the threat detection analytics, and the everyday use of rules and alerts. Alert Logic's own Security Operations Center investigates alerts and provides meaningful insight and remediation advice. Alert Logic can help you sidestep the SIEM money pit by using a modern solution that can quickly provide results, at a fraction of the cost, and with greater predictability for your budget.

