SIEM SOLUTIONS FOR SECURITY
WHAT VENDORS WON’T TELL YOU

MANAGED DETECTION AND RESPONSE SOLUTIONS OFFER MANY OF THE BENEFITS WITH FEWER HEADACHES
# TABLE OF CONTENTS

- Executive Summary ......................................................................................................................................................3
- Are SIEMS Relevant to Today’s Assets and Attack Surface? ...............................................................................4
- Aligning SIEM with Today’s Security Challenges ...................................................................................................5
- Garbage In, Garbage Out ...........................................................................................................................................6
- SIEM Alerts Require Interpretation and Triage ......................................................................................................8
- What SIEM Vendors Won’t Tell You ..........................................................................................................................9
- About Alert Logic .......................................................................................................................................................10
EXECUTIVE SUMMARY

Mid-sized businesses seeking to get ahead of the security game are increasingly looking to evaluate Security Incident and Event Management (SIEM) technology. SIEMs promise to make use of your abundance of endpoint, network and system log data while empowering you with direct control to configure what constitutes a real threat in your unique environment. Like a late-night infomercial for the latest breakthrough exercise system, SIEMs appeal to our optimistic sense of the possible. Long after the vendor has moved on most companies realize they aren’t able to feed their beasts fast enough, and so won’t be seeing accurate threat detection (or the beach-ready bodies of their dreams) anytime soon.

A SIEM is a powerful platform that requires continuous security content development, making it a good choice for Managed Security Service Providers and large enterprises with dedicated SIEM content developers. For most enterprises with more limited security resources, SIEMs either fail to detect the most common and damaging attack vectors, cost too much to maintain, take too long to show value or all three.

Factors often overlooked when considering a SIEM:

- Challenges of aligning SIEM with today’s security challenges
- Difficulty of improving outputs to be accurate, actionable, relevant
- Underestimating total effort and cost required to meet objectives

Before jumping head first into the SIEM tool “pool”, give yourself the time and space to identify the security outcomes your organization needs and the security resources you will have for your programs. For most companies, desired outcomes circle around shrinking the attack surface, accurate threat detection, reducing dwell time and most importantly, addressing the current threat landscape. These goals are achievable at lower cost in terms of TCO, staff hours and infrastructure management burden. Simply put, there is a better way.
ARE SIEMS RELEVANT TO TODAY’S ASSETS AND ATTACK SURFACE?

Today’s SIEMs are powerful tools whose success depends upon the thought and effort that goes into how they are configured, deployed, used, and maintained. Early SIEM technology was developed before the world became so dependent upon the internet and web applications, and before public cloud became a widely used infrastructure choice and the SIEM 2.0 solutions that are available today carry that legacy with them. Modern attacks leverage vulnerabilities in your attack surface differently than they did five or even three years ago. SIEM solutions have adapted by adding on to their core technology—for a price.

Traditional SIEM technology, especially when deployed without costly machine learning bolt-on modules, is not the best solution to detect today’s multi-stage attacks which take advantage of web application vulnerabilities. To stay current and protected, you will require additional capabilities that will further push the cost and scale of your SIEM initiative.

**WEB APP ATTACKS**

- POS Intrusions: 207
- Miscellaneous Errors: 222
- Privilege Misuse: 277
- Cyber-espionage: 289
- Everything Else: 184
- Payment Card Skimmers: 88
- Physical Theft / Loss: 74
- Crimeware: 47
- Denial of Service: 5

**MODERN ATTACK SURFACE**
ALIGNING SIEM WITH TODAY’S SECURITY CHALLENGES: MODERN APPLICATION THREATS REQUIRE INSIGHT BEYOND BASIC SIEM CAPABILITIES

Because attackers can use any layer of the application stack to gain access, build footholds, and move laterally within your systems, applications are a prime target. Verizon’s widely followed 2017 Data Breach Investigation Report says, “Attacks on web apps accounted for over 40% of incidents resulting in a data breach, and were the single-biggest source of data loss”, up 300% since 2014. Reinforcing this point, Data collected by Alert Logic shows web application attacks were 75% of all customer incidents from August 2015 to January 2017. The most prevalent attack methods were SQL Injection and remote code execution, sophisticated attack methods which likely would have been missed by the average SIEM implementation.

To identify threats, a SIEM must ingest data about your assets and activities and correlate that information to current threats using detection rules. A SIEM is only as good as its inputs. Many SIEM implementations fail because these inputs are flawed, lacking breadth from the full application stack and lacking depth beyond basic logs. Even more often, SIEMs lack robust application threat detection rules out-of-the-box. These rules are customized and maybe implemented poorly. They also require constant monitoring and tuning by highly skilled security experts (consultants or highly-paid staff) to ensure that they operate properly over time. Additional application security tools, such as a Web Application Firewall (WAF), and additional SIEM configuration are required, requiring additional time and money.
GARBAGE IN, GARBAGE OUT: THE NEED TO IMPROVE OUTPUTS TO BE ACCURATE, ACTIONABLE, AND RELEVANT
To be effective, your security program must be able to recognize threats and convey information to those who will remediate the threat. It must explain the priority, along with steps necessary for remediation. These threat assessment capabilities must include events in real-time and be capable of correlating patterns of events over many weeks or months. These ‘low and slow’ attacks are often the most damaging to organizations, harvesting data and company assets for months or even years. The sophisticated analytics required to detect these “low and slow” attacks are typically found in add-on UBA or UBEA modules or other big data solution extras for additional cost.

THE ANALYTICS CHALLENGE FOR SIEM
The analytics challenge for SIEM is often its infrastructure and architecture. SIEM is intended to identify threats in real-time. Yet to identify targeted, multi-stage attacks that cross several weeks or months requires large and disparate volumes of data. SIEM is limited by the number of events it can capture and store without impacting real-time correlation performance. It becomes a trade-off. Subsequently, even for SIEMs with modern analytics capabilities, practical limitations of an organization’s infrastructure quickly bring this trade-off to light.

To capture, store, and analyze more data, a separate UBA or UBEA module is usually required, for additional cost. Because of the high expense, some organizations have opted for a do-it-yourself approach using big data. However, that approach requires Data Science expertise and its own infrastructure.

KEY POINT: Security analytics is a necessity but its infrastructure requirements conflict with those of real-time SIEM correlation, making it an add-on for many SIEMs. The added cost of analytics modules as well as added storage, infrastructure, effort and expertise must be factored into your SIEM consideration.

COSTLY ANALYTICS ARE NECESSARY ADD-ONS TO BUOY-UP CORE SIEM
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” is substantial. Many attacks look like noise so they can better hide in the grey area. Achieving detection 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.”

BEN CANNER, SOLUTIONS REVIEW

---
ANALYTICS ARE IMPORTANT BECAUSE THEY MORE ACCURATELY DETECT ATTACKS USING THREE DIFFERENT 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.

As Anton Chuvakin of Gartner explains in his blog 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.

You will need to add additional staff or resources to keep up. The reasoning is simple. 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.

**KEY POINT:** You must staff to implement and run a SIEM but also to investigate incidents uncovered by it. If you cannot, a managed security service would be a better solution.

*The Target breach of 2013 is a highly-visible example of a failure of alerts and ‘actionable intelligence’. Despite million dollar security systems, the security analysts ignored security alerts.*
SIEM SOLUTIONS FOR SECURITY: WHAT VENDORS WON’T TELL YOU

WHAT SIEM VENDORS WON’T TELL YOU: NEARLY EVERYONE UNDERESTIMATES THE TOTAL EFFORT AND COST REQUIRED TO MEET THE OBJECTIVES OF A SIEM PROJECT

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. The question that must be asked prior to determining if a SIEM approach is right for your organization is: Do you really want to stand up and maintain an expensive, time consuming platform?

ASK YOURSELF: Do you really want to stand up and maintain an expensive, time consuming platform?

TOTAL COST OF OWNERSHIP IS UNPREDICTABLE AND DEEP

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)

MONITORING AND INVESTIGATING ALERTS IS A HUGE, ONGOING BURDEN THAT REQUIRES ADDITIONAL INVESTMENT BEYOND THE INITIAL TECHNOLOGY SPEND

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 two-thirds of their time investigating unreliable alerts while actual breaches go undetected an average of 146 days, according to M-Trends 2016 – EMEA 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 FireEye indicating they were under attack, but they were not investigated.
**KEY POINT:** As part of your evaluation and approach to SIEM, map out a resource plan. This will enable you to see the long-term investment and staff required to manage and maintain your SIEM effort.

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.

**CONSIDER ALTERNATIVES TO YOUR SIEM EFFORT**

A Managed Detection and Response (MDR) service is a simpler, modern alternative to SIEM. An MDR service delivers immediate threat detection, response and monitoring capabilities, delivered as a service, to help organizations save time, money and frustration. Without getting caught up in the care and feeding and ongoing commitment of a SIEM platform, you get accurate, actionable threat insight and remediation advice, aligned with today’s threat environment, delivered predictably as a service. The cost and effort of this approach is a fraction of that required by a SIEM and brings immediate value.

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.