ALERT LOGIC®

WHY SIEMS CAN FAIL YOU IN HYBRID IT

TABLE OF CONTENTS

INTRODUCTION

This paper outlines the most commonly overlooked factors when evaluating whether “to SIEM” or “Not to SIEM”. 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:

- Alignment with today’s security challenges
- Efficacy (is the information they provide accurate, actionable and relevant for your organization)
- Total effort and investment required to meet objectives.

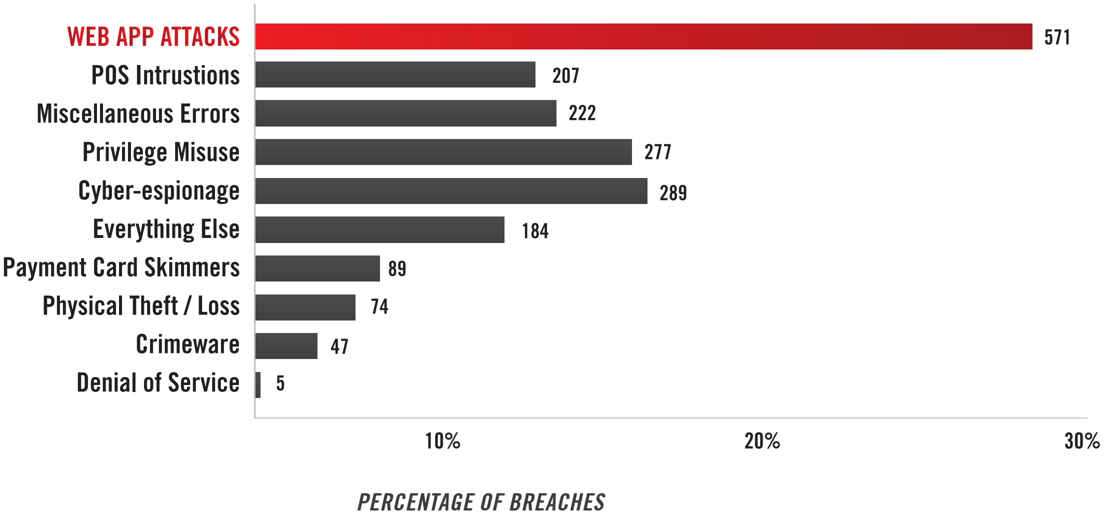
Before jumping head first into the SIEM tool “pool”, give yourself the time and space to identify the security outcomes your organization needs and the security resources you will have for your programs. For most companies, desired outcomes circle around shrinking the attack surface, accurate threat 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.

QUESTION: HOW EFFECTIVELY WILL A SIEM TOOL RESPOND TO TODAY'S THREATS?

The success of any SIEM effort depends upon how it is configured, deployed, used, and maintained. Traditional SIEM technology, especially when used without costly machine learning bolt-on modules, is not the best solution to detect today's multi-stage attacks. These attacks take advantage of web application vulnerabilities and chaining attack activity to compromise a system. To detect these threats, SIEMs require additional capabilities that will further push the cost and scale of your SIEM initiative.

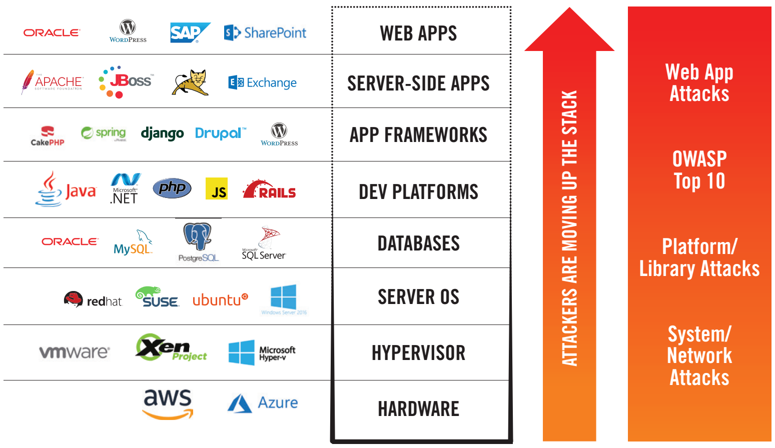
APPLICATION THREATS REQUIRE INSIGHT BEYOND BASIC SIEM CAPABILITIES

Because attackers can use any layer of the application stack to gain access, build footholds, and laterally move within your system, applications are a prime target. 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 that would have likely been missed by the average SIEM implementation.



To identify threats, a SIEM must ingest data about your assets and activities and relate those to current threats using detection rules. Many SIEM implementations fail to include sufficient application information as an input, lacking breadth from the full application stack and lacking depth beyond basic logs. Even more often, they lack robust application threat detection rules out-of-the-box. Additional application security tools, such as a Web Application Firewall (WAF), and additional SIEM configuration are required, costing you time and money. Here's why it matters.

Today's automated and often multi-stage web application attacks are hard to prevent and detect. They look innocent to the host and network and use the application's own functionality and flaws to trick the application into giving up control. There is more complexity than what meets the eye. A web server essentially runs the web server itself (e.g. Apache or IIS) and the user application (what you see when you go to that website), plus the tools used to develop the user application (e.g. PHP, WordPress templates, Java). All of these vectors must be monitored for potential exploit. This requires full stack visibility into application vulnerabilities including those in your code, your application configurations,

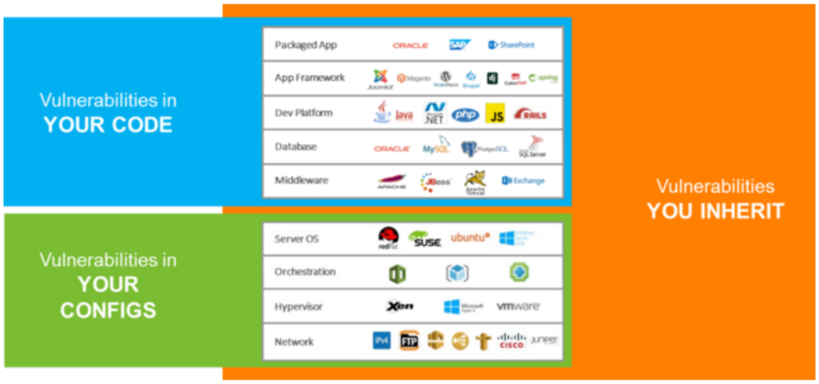


1. Wide range of attacks at every layer of the stack
2. Rapidly changing codebase can introduces unknown vulnerabilities
3. Long tail of exposures inherited from 3rd party development tools
4. Extreme shortage of cloud and application security expertise

and the code you inherit. It is not easy.

The OWASP consortium (Open Web Application Security Project) identifies the ten most serious web application security risks in an effort to help organizations assess and prioritize their application security efforts. The OWASP Top 10 risks are represented across the full application stack and indicate the scope required to protect yourself from the most important risks, highlighted below:

- Your own code - Ideally all your applications would be carefully built according to secure coding best practices. Yet, the failure rate of applications to pass audits just for the OWASP Top 10 is 61%.
- Third party code – No one writes applications entirely from scratch anymore. Sonatype estimates that 90% of all software development requires the downloading of components. You rely on plug-ins, servlets and code libraries that can contain inherited vulnerabilities. Yet these elements bring inherent risk. External Entities and Components are #4 and #9, respectively, in the OWASP Top 10 risks. Strengthening this point, TechBeacon shows how third-party libraries are one of the most insecure parts of an application.
- Configurations – Vulnerabilities from insecure configurations can provide an attacker points for entry and for data theft. Examples include open S3 buckets, overly permissive identity policies, and weak ciphers on elastic load balancers. Misconfiguration is #6 in the OWASP top 10 risks.



LOGS ALONE ARE NOT ENOUGH

Many SIEM implementations will rely on logs alone yielding insufficient insight into application security. Demonstrating this issue, the OWASP latest analysis adds a new set of risks to the Top 10: "Insufficient Logging and Monitoring, coupled with missing or ineffective integration with incident response." These vulnerabilities allow attackers to "further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data."

To improve this situation, OWASP has provided guidance for developers on building application security logging mechanisms. It points out that, "Many systems enable network device, operating system, web server, mail server and database server logging, but often custom application event logging is missing, disabled or poorly configured. It provides much greater insight than infrastructure logging alone. Web application (e.g. web site or web service) logging is much more than having web server logs enabled (e.g. using Extended Log File Format)." Similarly, Peter Freiberg, Principal Consultant of OWASP, points out that many applications have poor security logs, or none at all and goes on to identify 4 key challenges for application security logging:

- Security logging frameworks are missing or incomplete
- Limited guidance and consensus regarding what and how to log
- Lack of requirements for security logging including log retention
- Correlation and alerting capabilities are not mature

It is clear that application logs, even if they do exist, are insufficient to monitor applications for threats.

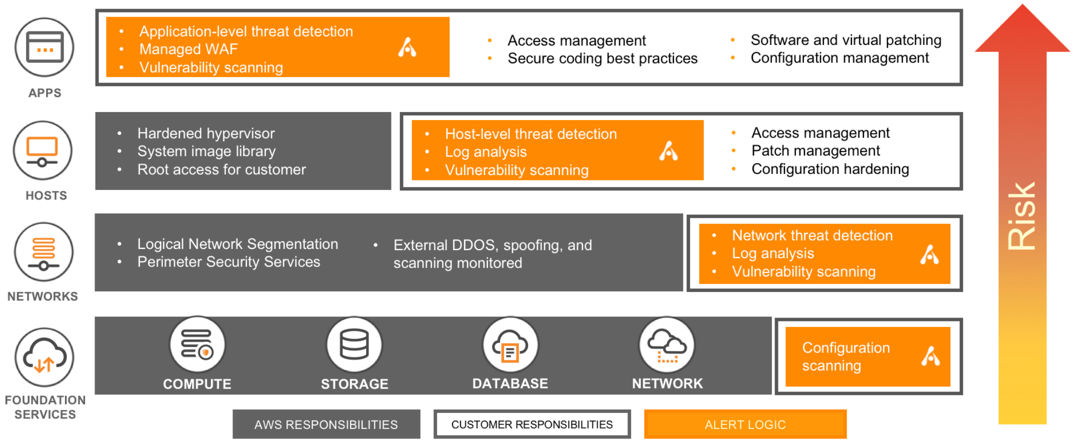
For quality insights, you need more data about the application's behavior and you need analysis that understands it. Attacks may inject commands to gain access to resources on the server or to cause the application to act in a different way. You must have visibility into application behavior and logic, traffic both to and from the app, what is being requested, and what is being returned. A Web Application Firewall (WAF) is needed to inspect the traffic flow at the application layer, to understand web application protocol logic, and to distinguish if a request is normal or malformed. If the SIEM is to have this application visibility, more time and money will be needed to connect the WAF data to the SIEM.

KEY POINT: A top-notch SIEM with a fully staffed Security Operations Center (SOC) may catch some SQL injections, but a Web Application Firewall (WAF), coupled with multi-layer security analytics applied to the full application stack, would be a better solution.

MEETING THE SHARED RESPONSIBILITIES OF CLOUD ENVIRONMENTS

At the same time that applications have become a focus of attackers, web apps have become especially fluid in the cloud, and the challenge is growing. Synergy estimates that together the use of public IaaS and public PaaS continue to grow at almost 50% per year. Despite this growth, CSO Online finds that only 46% of companies have a cloud computing security strategy.

Cloud security must be a shared responsibility. Amazon and Azure are responsible for "security of the cloud" (the cloud platform), you are responsible for "security in the cloud" (workloads you run on those platforms).



To secure cloud applications, your threat detection method must ingest cloud telemetry, be able to comprehend unique cloud data, and provide visibility into the full application stack described previously (this part is your responsibility). Let's look a little closer at these.

Cloud telemetry is provided by AWS and Azure but your SIEM must ingest it. Microsoft recently published instructions for integrating their Cloud App Security data with the MicroFocus ArcSight SIEM and Common Event Format (CEF) files for other SIEMs but additional configuration is required. More importantly, the SIEM must be able to comprehend its use. Traditional security tools rely on IP address and assume that the application's server and its IP address are persistently linked. This is not the case in cloud, making it impossible to identify the source of a threat unless your SIEM has this comprehension capability.

Meanwhile, AWS removed some risks from their services with DDoS mitigation, network segmentation and hardened system images, which helps explain why Wannacry and NotPetya are not issues in the cloud. It is therefore common to misinterpret this as "AWS has good-enough security built in". But they leave the hardest parts to you – you control the configuration, communications within your network, you control host management, and the application layer. In short, the basic cloud platform is hardening, but the workloads run on it and the configurations you control remain exposed and are your responsibility. As evidence, cloud services are still being misconfigured by users. For example, open S3 buckets have left data up for grabs at Verizon, the DNC, Alteryx, and the World Wrestling Federation.

KEY POINT: To adequately monitor and protect your cloud workload, your SIEM must ingest and comprehend cloud-specific telemetry along with attributes unique to cloud applications. You are still responsible for monitoring the security of the full application stack.

QUESTION: CAN A SIEM ALONE OFFER EFFECTIVE THREAT DETECTION WITH USEFUL, ACTIONABLE INSIGHT?

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. Part of recognizing a threat involves knowing what to look for and having the necessary data available. Threat assessment must include events in real-time and also patterns of events over many weeks or months. The sophisticated analytics required to detect "low and slow" attacks crossing multiple events over time is typically found in an additional UBA or UBEA module or another big data solution.

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.

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.

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.

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. Yet Gartner Analyst, Anton Chuvakin, says in his blog that some of the UBA use cases are very rule-based and do not extend beyond basic correlations. Alternatively, 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.

SIEM ALERTS REQUIRE INTERPRETATION AND TRIAGE

Once threats are detected, you need clear 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.

The best example of this, is the Target breach of 2013. Despite million dollar security systems, the security analysts ignored security alerts. In his blog, security expert Aviv Raff asks the obvious and then provides the answer:
What might have caused Target's security team to ignore the alert? "In two words: 'actionable intelligence,'" said Seculert's Raff via email. "With today's amount of detection data, just signaling an alarm isn't enough. The operator/analyst should be able to understand the risk as well as the recommendation of each incident, in order to be able to prioritize[1]."

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.

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.

1: Source: http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html; January 16, 2014.

QUESTION: DO YOU REALLY WANT TO STAND UP AND MAINTAIN AN EXPENSIVE, TIME CONSUMING PLATFORM?

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.

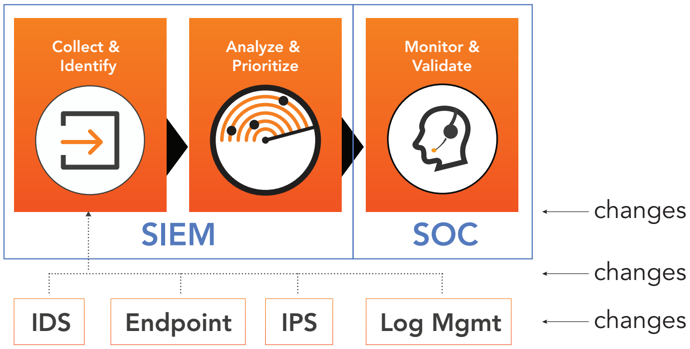
TOTAL COST OF OWNERSHIP IS UNPREDICTABLE AND DEEP

Although a SIEM can be purchased for less than $100,000, it is common for fully operationalized implementations to cost close to $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)

TIME TO VALUE IS UNCERTAIN AND LENGTHY

Cost and time to value go hand-in-hand. An on-premise SIEM is going to require architecture planning, implementation, tuning and training. Even under the best circumstances, a SIEM deployment can take 3-4 months before performing effectively while 6-12 months seems to be more typical.



Analysts indicate that SIEM investments relying on a single security professional for installation and maintenance are almost always destined to become shelf-ware. Yet even for those with a team of skilled Security Analysts, SIEM can consume analyst time on mundane tasks like programming new rules, learning syntax of searches, and running reports. Your security team will require training if they are to configure SIEM rules to be useful for your environment. Valuable security analyst time will be consumed maintaining the SIEM application environment to add storage, apply and test updates, and more, time that could be better spent focusing on higher value efforts like risk management and security education.

KEY POINT: When evaluating a SIEM, your total cost of ownership must include not only the initial purchase price of software and hardware, but also ongoing maintenance and everyday use of the platform. Remember the necessary add-ons such as threat intelligence feeds and analytics.

THE TRUTH BEHIND WHAT A SIEM INVESTMENT REALLY REQUIRES (WHAT SIEM VENDORS WON'T TELL YOU)

SIEM is best for organizations with a strong bench of in-house security professionals. It is a powerful platform for use by security analysts who have the expertise needed to apply the tool to their unique environment as part of their detection, triage, and response effort. It is not the best solution for organizations lacking sufficient in-house security resources.

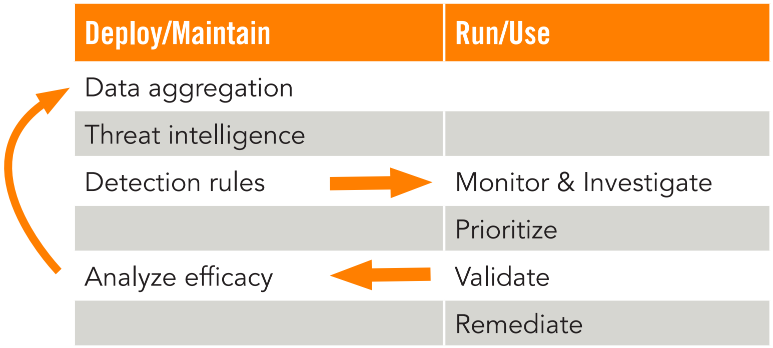
Several steps are required to deploy and maintain such a platform and to use it on a 24x365 basis. You should understand the effort required before choosing to invest in SIEM. Let's look at the challenges to achieve success with SIEM.

DATA AGGREGATION IS FRAGILE TO MAINTAIN

A SIEM can only correlate data that it receives. While it is tempting to assume that operations data already collected can be used to feed security correlation, operations logs alone are only sufficient for the narrowest of use cases. A SIEM typically ingests data from multiple security devices and sources. Each source is provided by its own system (e.g. FireEye or Cisco Firewall for IDS data, Splunk for log management data) with connectors (interfaces) installed and maintained to feed the data into the SIEM. This data aggregation is critical, but it does not happen on its own and it is fragile to maintain. When any of the devices and systems sending data change their output format, the SIEM interfaces and rules will require modification, troubleshooting, and re-testing.

THREAT INTELLIGENCE REQUIRES EXPERTISE TO APPLY, EVEN MORE SO WHEN IT IS FREE

Security analysts must assess the latest threat intelligence for changes in attack landscape and trends. This is the secret sauce behind effective detection rules and requires added cost to procure threat feeds and to apply them. Manual effort and security expertise are needed to interpret the potential effect of new threat intel on data feeds, rules and alerts and to apply changes to rules and connectors.



Deploy/Maintain	Run/Use
Data aggregation	
Threat intelligence	
Detection rules	Monitor & Investigate
	Prioritize
Analyze efficacy	Validate
	Remediate

In addition, while open source community intelligence is free, it is notoriously noisy and inaccurate. It lacks the quality of more proprietary efforts and is not effective without added effort. For example, community-based rules may identify an attack but may not show if it was successful or not and will not tell you how to remediate the threat. A security resource must figure this out. In short, substantial effort and expertise is still required to apply "free" threat intelligence.

DETECTION RULES REQUIRE CUSTOMIZATION AND SUPPLEMENTAL ANALYTICS

A SIEM relies on correlation rules to identify suspicious events and their urgency. SIEMs ship with rule sets to detect vulnerabilities for all kinds of systems and with templates for many regulatory frameworks. Because of their broad use, effort is typically needed to tailor the rules and reports for your environment. For example, out-of-the-box, the SIEM may assess all start-up traffic. You may find that you need to suppress traffic from PCs and limit inspection to servers due to event volume. Numerous tweaks like this become time consuming.

While correlation excels at real-time event identification, as explained previously, more advanced and persistent attacks over time require analytics for detection. In fact, many SIEM users are adding analytics to retrospectively find what their correlation rules missed. Similarly, Cloudera is a company primarily targeting Splunk implementations, to overcome their lack of scale, flexibility and analytics capabilities. The necessary addition of analytics requires its own installation, integration, and ongoing maintenance efforts.

MONITORING AND INVESTIGATING ALERTS IS A HUGE, ONGOING BURDEN

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. 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.

CONSIDER ALTERNATIVES TO SIEM

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.

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.