ALERT LOGIC®

5 TOP RECOMMENDATIONS FOR EFFECTIVE THREAT DETECTION

Early and effective threat detection are often the key to minimizing the impact of an attack. In any threat detection effort, organizations must focus on visibility, assessment of risk and potential impact to the business. This informed context is particularly important in cloud and hybrid environments where a security response must be tailored to the unique deployment considerations.

In today's threat landscape, attackers are using a wider range of more sophisticated methods to infiltrate vulnerable systems. With this shift in techniques, detecting these threats requires expertise and the ability to corollate data from multiple sources over weeks or even months. What's more, this analysis must be conducted with near zero-impact on system performance—something that traditional SIEM technology can't provide.

If you are looking to improve the effectiveness of your threat detection program, consider the following recommendations:

1 ASSESS YOUR BUSINESS OBJECTIVES AND UNIQUE ATTACK SURFACE.

How critical is the security of your web apps, especially those in the cloud? Are you relying on public cloud infrastructure? Choose a detection method that can address your workloads. For instance, cloud servers spin up and spin down constantly. Your detection must follow the provision and deprovision actions of AWS and Azure and collect meta data to follow events as they traverse this dynamic environment. Most SIEMs cannot do this.

2 ELIMINATE VULNERABILITIES BEFORE THEY NEED THREAT DETECTION.

Use vulnerability assessments to identify and remove weaknesses before they become exploited. Assess your full application stack including your code, third party code, and code configurations. Regular vulnerability assessment and remediation is one of the most fundamental and impactful processes any organization can use to reduce risk. Some of the most infamous and recent exploits like WannaCry, Heartbleed and Apache-struts (Equifax) were potentially avoidable with frequent vulnerability scanning and patching.

As an Approved Scan Vendor (ASV) for PCI, Alert Logic can look for vulnerabilities in software and devices, monitor cloud environments for misconfigurations and provide external scanning for PCI compliance. WordPress and Magenta carry inherent risk, yet many users don't even know their software incorporates it. An Alert Logic vulnerability assessment will find it.

3 ALIGN DATA FROM MULTIPLE SOURCES TO ENHANCE YOUR USE CASES AND DESIRED OUTCOMES.

Collect and inspect all three kinds of data for suspicious activity: web, log, and network. Each data type has unique strengths in identifying certain kinds of threats and together present a whole picture for greater accuracy and actionable context. Your data sources should include those environments that are most critical: WAF for applications, IPS/IDS for network, endpoint for users, and log management for systems.

The Alert Logic Security-as-a-Service solution includes implementation, maintenance and integration of the systems needed to monitor web apps, network, endpoints and systems. Much like SalesForce.com in the business environment, Alert Logic removes the burden of the integrating components so you can focus on the end results.

4 USE ANALYTICS TO DETECT TODAY'S SOPHISTICATED ATTACKS.

To detect focused multi-staged attacks, ensure your threat detection methods look at both real-time events and patterns in historical events across time. Apply machine learning to find what you do not even know to look for. If you use SIEM, enlist machine learning to see what correlation missed and better tune your SIEM rules.

For effective threat detection, Alert Logic analytics use signatures, anomaly detection and machine learning to detect the most sophisticated attacks, including attacks only identified by looking across events over time. In addition, by looking at event data across thousands of customers' security programs, Alert Logic can find patterns an individual site could never see. This allows our experts to intercede quickly in the event of a ramping attack, applying learnings from our vast deployed network of users to stop threats before they arise in your own environment. When threats are detected, Alert Logic goes beyond a SIEM. It shows, in simple terms, what happened and recommended steps, with the ability to drill down into more detail for evidence of interest to security pros. The example below shows the summary information presented by the Alert Logic SOC analyst to the customer.

Nov 28 2017 10:04 GMT

Attack Detail:

Attacker Location: Internal **Targeted Host:** 172.XX.XX.XXX

We have detected an attack against your web application using malicious SQL commands. The nature of these attacks requires further analysis by an Analyst. These attached are designed to map your database and attempt to steal user and company data.

Remediation Recommendations:

The source of this attack was an internal address. Please verify that this was expected and authorized traffic. When designing your SQL database and front end application it's best to follow the below procedures to minimize the risk.

Nov 28 2017 10:10 GMT

Spoke with our customer about this Successful SQL injection attack detected from 172.XX.XX.XXX (XFF 209. XX.XXX.XX) to the host located at 172.XX.XX.XXX. Usernames/Password hashes were witnessed being exfiltrated so I advised him to reset the wordpress passwords asap.

I also advised him to update his Like/Dislike plugin asap to fix this vulnerability.

5

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. The Alert Logic 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.

ALERT LOGIC®