ALERT LOGIC™

WHITEPAPER

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 assets. Detecting these threats requires visibility to different attack vectors and expertise to create correlation rules to identify them. It also requires expertise to constantly tune to reduce false positives and gain context in order to efficiently deploy resources to mitigate these attacks.

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.

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.

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.

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 and advanced analytics 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.

5 Consider Your Options

There is more than one way to improve your security posture and detect threats. The traditional option is to implement Security Information and Event Management (SIEM). This type of solution is typically useful for organizations with strong security programs that include highly skilled expertise. It's important to note this solution will require dedicated headcount due to the labor intensive requirements and they can also get expensive with advanced analytics options as well as the additional security controls that will need to be integrated to gain visibility to certain attack vectors.

An option quickly gaining popularity is Managed Detection and Response (MDR). This option 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 at a predictable cost which is typically a fraction of the cost of purchasing and maintaining a SIEM.

About Alert Logic

Alert Logic is the industry's first SaaS-enabled managed detection and response (MDR) provider, delivering unrivaled security value. Since no level of investment prevents or blocks 100% of attacks, you need to continuously identify and address breaches or gaps before they cause real damage. With limited budget and expertise, this level of security can seem out of reach. Our purpose-built technology and team of MDR security experts protect your organization and empower you to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas, with offices in Austin, Cardiff, London, and Cali, Colombia, and online at alertlogic.com. **Alert Logic – our knowledge is your advantage.**