Spectrum ENTERPRISE | Navisite™

5 TOP RECOMMENDATIONS FOR EFFECTIVE THREAT DETECTION AND RESPONSE

Early and effective threat detection is 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, response, and remediation 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, for example, Azure and collect metadata 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 Navisite clients who are required to meet PCI compliance. WordPress, Drupal and Magento carry inherent risk, yet many users don't even know their software incorporates it. An Alert Logic vulnerability assessment will find it and Navisite's SOC will assess the threat and quickly remediate it for you.

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.

Navisite leverages the Alert Logic Security-as-a-Service solution that 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 integrating security components so you can focus on the end results. Navisite's Managed Security Services provide you the tools to better leverage your newfound insight into your security posture.

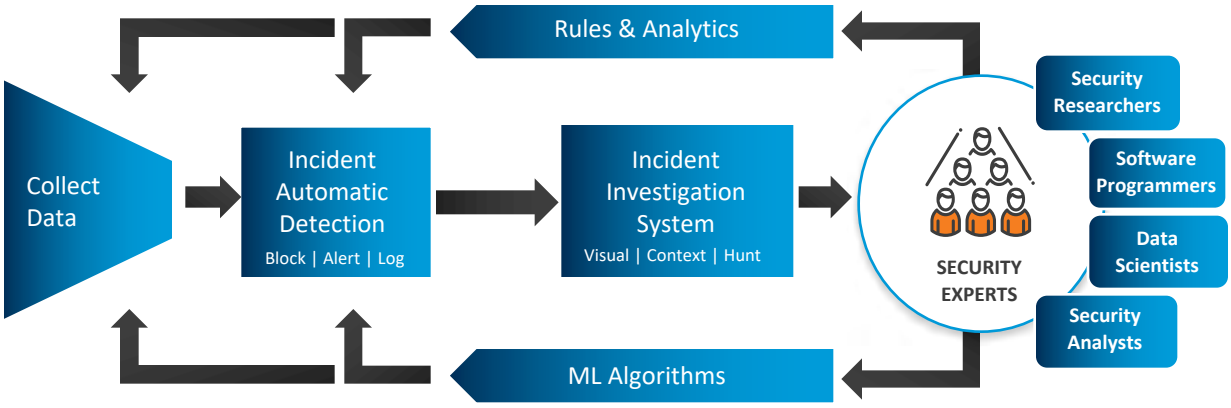
4 USE ANALYTICS TO DETECT TODAY'S SOPHISTICATED ATTACKS.

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. Once Alert Logic identifies a threat in your environment, Navisite's SOC intercedes on your behalf to stifle the ramping attack, utilizing the collective decades of expertise and the learnings of Alert Logic and Navisite's vast security partnership network.

MDR: INTEGRATED PLATFORM AND SERVICE MODEL

Alert Logic SIEMless Threat Management + Navisite Managed Security Expertise



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 intensive requiring a substantial commitment of time and security expertise. The full commitment may not be apparent at the outset. Choosing a trusted managed service partner may be a good avenue to follow to leverage their resources and expertise to mitigate your risk.

A Managed Detection and Response (MDR) service is a simpler, modern alternative to SIEM. Navisite's 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, has partnered with Navisite, a leading managed cloud service provider, with 20+ years of experience in securing clients' managed cloud and hosting environments, to deliver a best-of-breed MDR service. Navisite's MDR Service uses Alert Logic's SIEMless Threat Management platform to monitor your managed IT environment, leveraging advanced analytics to identify threats, which are assessed by Alert Logic and Navisite's security experts. Navisite's security operations center then expediently addresses all security concerns. This powerful service provides immediate results, at a fraction of the cost of DIY security or SIEM approaches and with greater budgetary predictability.

Spectrum ENTERPRISE | Navisite ALERT LOGIC