Top 5 Recommendations for Effective Threat Detection

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 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 security information and event management (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 down constantly. Your detection must follow the provision and deprovision actions of AWS and Microsoft® 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.

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 as a way to identify what you don't yet know to look for. If you use SIEM, enlist machine learning to see what the correlation process missed and better tune your SIEM rules.

The example below shows the summary information presented by the 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 attacks 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 frontend 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 with well-staffed security programs. A SIEM alone is not the best solution for monitoring threats against today's web applications and cloud environments. Analytics and additional effort are generally required. These 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, feeding and ongoing commitment of a SIEM platform, you get accurate, actionable threat insight and remediation advice, aligned with today's threat environment and 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.

6. Explore Rackspace Managed Security and Alert Logic, in your choice of data centers.

Rackspace Managed Security, supported by Alert Logic's award-winning security platform and threat intelligence, helps protect your applications and workloads through continuous monitoring and swift response.

Whether your IT resides in a dedicated environment, private cloud, public cloud or a multi-cloud environment — anywhere around the globe — you can rely on Rackspace and Alert Logic to help protect your business.

Rackspace and Alert Logic

Rackspace and Alert Logic® help customers protect their businesses from cyber-security threats with Rackspace Managed Security's Proactive Detection and Response Service (RMS-PDR). This flagship full-service security offering is enabled in-part by Alert Logic's award-winning security platform and backed by Rackspace's 24x7 Security Operations Center (SOC) for continuous threat detection, remediation, and cyber-hunting in real time. Whether your applications and data reside in a dedicated environment, private or public cloud, the Alert Logic and Rackspace partnership can help your business increase your cyber-security maturity fast, and for a fraction of the effort and cost of a do-it yourself approach.

Take the Next Step

Let's talk about how Rackspace and Alert Logic can help improve the effectiveness of your threat detection program.

Learn more: **www.rackspace.com/security**
Call: **1-800-961-2888**