ALERT LOGIC™

aws

AWS Vulnerability and Threat Detection Checklist

Securing web applications in the AWS cloud environment relies on the cloud service provider and the customer working together in a shared responsibility model. Effective security for web applications on AWS requires full visibility into the environment in which the apps live, while also proactively monitoring for attacks without causing delays in application development and delivery. For some customers this may be a challenge due to limited personnel resources or expertise. This is where Alert Logic can help. We will automatically show you why, where, and how to respond to vulnerability findings and provide you with short- and long-term recommendations to stop active attacks.

To help guide the way, following are key considerations for providing sound web application security running on the AWS cloud.

☐ **UNDERSTAND THE CHALLENGES OF CLOUD SECURITY**

AWS handles securing services, such as compute power, storage, and networking. Customers, however, are fully responsible for securing the applications that the cloud platform hosts. This means you must provide sound identity and access management (IAM), and follow best practices for secure coding and configuration management. Additionally, you need to monitor for attacks that specifically target the application layer.

☐ **CONSIDER APPLICATION VALUE AND RISK**

For proper security, customers must understand the business value of data in each of their applications and prioritize which are critical to the success of the company and ensure the top apps are protected with top-tier security. Determine which applications are important to protect from a business perspective. Examples could include apps that are critical to business operations, account for revenue generation or those that support intellectual property or other sensitive information.

IDENTIFY & FIX CONFIGURATION VULNERABILITIES

AWS instances use security groups to control what network traffic an instance is permitted to accept or send but it's up to the customer to configure their security groups correctly, by deciding which ports should accept traffic and from which sources.

Once you make those choices, AWS is responsible for enforcing them. Additionally, properly protecting who has access to your cloud-based applications and infrastructure, and ensure individuals have only the level of permission they need.

IDENTIFY & FIX THIRD-PARTY SOFTWARE VULNERABILITIES

Software vulnerabilities are inherited through third-party libraries, frameworks and platforms throughout your application and infrastructure stack. Employ a vulnerability management solution that continuously identifies vulnerabilities and remediate them.

You must be cognizant of known common vulnerabilities and exposures (CVEs) and common weakness enumeration (CWE), which is a list of software weakness types. CVEs and CWEs can apply to major operating systems, OS configurations, server applications, and standard web applications.

ASSESS THE APPLICATION'S THREAT PROFILE

Understanding the application's threat profile can also help you determine how best to secure it because it shows the threats to which an application is most likely to be vulnerable. If an app relies on a SQL database, you need to protect it against SQL injection attacks, but if not then you don't have to be concerned about it. Vulnerability assessments can help you understand the threats to which your applications are most susceptible.

In addition, consider how applications are used and accessed, with the goal being to identify those that are at greater risk of a breach. Apps that can be accessed by any customer or complex ones integrated with third-party components present a higher degree of risk.

ENSURE YOU MEET COMPLIANCE REQUIREMENTS

Organizations that are subject to industry or government regulations such as PCI-DSS, HIPAA, and Sarbanes-Oxley should thoroughly vet how their applications will work in an AWS environment.

Expect to share responsibility for compliance with AWS, and get a clear understanding of what the cloud service provider is responsible for, and what you the customer must handle.

MONITOR MULTIPLE SOURCES FOR SECURITY DATA

No single source of data will allow you to detect the range of potential attacks. The key is gathering data from multiple sources including network packets, logs and HTTP transactions -- and making sense of it.

THINK THROUGH YOUR THREAT DETECTION TEAM AND PROCESSES

Security tools generate enormous amounts of information, maybe tens of thousands of alerts per day for a large enterprise. Most of those alerts are benign, but the key to defending against intruders is being able to identify the handful that represent the highest risk.

When integrated with Amazon GuardDuty, Alert Logic will automatically show you why, where, and how to respond to GuardDuty findings—and provide your staff with short- and long-term recommendations to stop active attacks now and to prevent similar attacks in the future.

Alert Logic is integrated with AWS Security Hub to enable AWS customers to incorporate verified security incidents from Alert Logic's 24/7 Security Operations Center (SOC) team. These incidents will include expert analysis and remediation guidance for both security and compliance.

Assess the level of your staff's expertise and determine whether it includes security experts in areas including network, applications, and cloud.

CONSIDER AUTOMATION REQUIREMENTS

Today, companies are investing heavily in rapid application development processes and DevOps. As a result, application releases happen in minutes, perhaps several times per day. Integrating and automating the delivery of security in applications significantly reduces security risk and supports rapid application development and deployment.

ABOUT ALERT LOGIC

Alert Logic is the industry's first SaaS-enabled managed detection and response (MDR) provider, delivering unrivaled security value. 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, we are headquartered in Houston, Texas.

available on: aws marketplace

You can get started right away and try the vulnerability and asset visibility capability and the threat detection and incident management capability for FREE FOR 30 DAYS.

ALERT LOGIC™