SentinelOne eBook

SentinelOne™

Proactive Attack Surface Management for AWS Workloads with SentinelOne and Amazon Inspector

© 2022 SentinelOne. All Rights Resered.

aws

Cloud Misconfigurations Are The No. 1 Cause Of Cloud Security Breaches

Over the last decade, digital transformation has fueled the adoption of cloud services, which provide unmatched agility and reduce time to market when compared with legacy on-premises infrastructure. However, agile development practices that emphasize iteration and speed can overwhelm security teams that are not prepared to secure workloads as fast as they are created. As a result, governance is often performed once when workloads are deployed, or sometimes not at all. Today, misconfigurations remain the number one cause of cloud security breaches.

> Misconfigurations are not always easy to detect. A survey showed that just 1% of internet-as-a-service misconfigurations are reported.[1]

Even organizations that have a vulnerability scanning tool deployed to their cloud environments often struggle in three areas:

- **Observing:** Ingesting infrastructure vulnerability data and correlating with endpoint detection and response (EDR) telemetry from within the application workload
- **Operationalizing:** Visualizing the most critical vulnerabilities to prioritize remediation
- **Acting:** Performing remediation across the cloud environment at scale

SentinelOne + Amazon Inspector Provide Unified Visibility Into Vulnerabilities



Amazon Inspector

The SentinelOne integration for Amazon Inspector provides unified visibility of vulnerabilities within Amazon Web Services (AWS) infrastructure through the SentinelOne Data Platform.

Amazon Inspector is a vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. Once enabled, Amazon Inspector automatically discovers all running Amazon Elastic Cloud Compute (Amazon EC2) instances and container images residing in Amazon Elastic Container Registry (Amazon ECR) at any scale and immediately starts assessing them for known vulnerabilities. All findings are aggregated and pushed to AWS Security Hub and Amazon EventBridge to automate workflows.

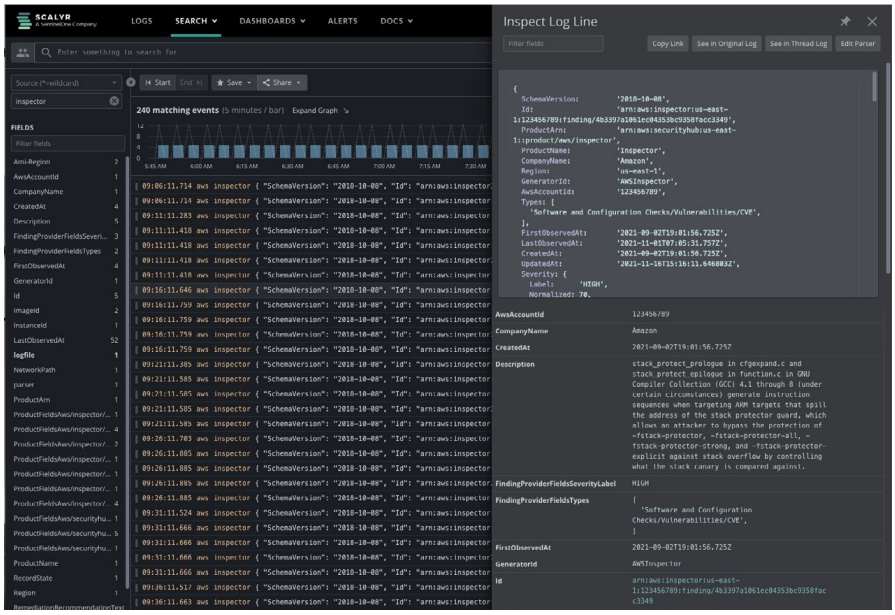
The **SentinelOne Data Platform** is a massively scalable, cloud-native logging and analytics platform built on AWS that is designed to ingest, normalize, correlate, and action limitless datasets. It provides powerful querying and threat hunting features to make searching and pivoting within the datasets simple for security and cloud teams. SentinelOne provides visibility into your environment with 365 days and beyond of EDR data to let your team analyze incident activities and conduct historical analysis within the same platform.

The SentinelOne integration with Amazon Inspector enables a single solution to help you proactively identify vulnerabilities in your AWS workloads, then protect, detect, and respond to active exploits of vulnerable applications. Together, security and DevOps teams can innovate securely and embrace cloud adoption with confidence.

[1] Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report

Maximize Observability With EDR Telemetry

SentinelOne ingests Amazon Inspector findings from Amazon EventBridge and correlates against logs from additional security and DevOps data sources. Context-rich EDR telemetry from SentinelOne can be queried alongside vulnerability information from Amazon Inspector, giving security analysts a single dataset for identifying open vulnerabilities and detecting successful vulnerability exploits.



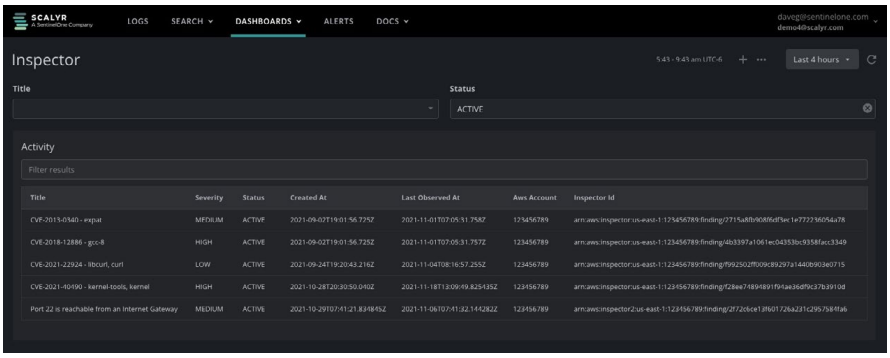
The SentinelOne Data Platform provides powerful querying and threat hunting features.

Identifying Vulnerabilities

In today's era of widespread cloud adoption, vulnerability scanning is crucial to protect cloud workloads against exploits like the Log4j vulnerability, which has affected 44 percent of corporate networks. Amazon Inspector automatically scans for and identifies vulnerabilities such as Log4j, then SentinelOne allows you to take action and respond to any active exploits.

Operationalize Remediation With A Dashboard View

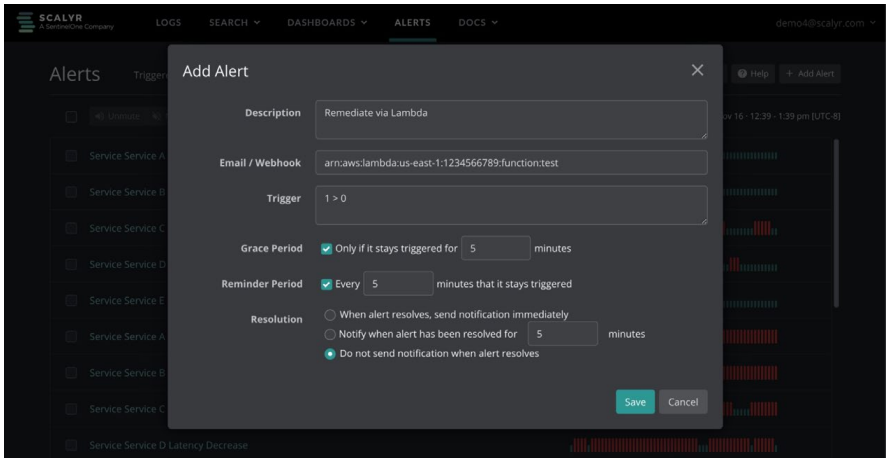
Within SentinelOne, analysts can use prebuilt dashboards to view high priority vulnerabilities from Amazon Inspector. Data from Amazon Inspector is enriched with links to view additional information about common vulnerabilities and exposures (CVE) from the MITRE National Vulnerability Database. With this data, analysts can view the most common vulnerabilities within their environment, the most severe, and additional context about a given CVE from a single pane of glass.



Sorting and viewing vulnerabilities from Amazon Inspector.

Take Action To Remediate Vulnerabilities—At Scale

When a vulnerability needs to be remediated, the SentinelOne Data Platform issues alerts allowing you to not only identify issues quickly but accelerate vulnerability remediation. When a vulnerability needs to be remediated, the SentinelOne Data Platform's alerting is ready with native support for AWS Lambda, Amazon EventBridge, Amazon Simple Queue Service (Amazon SQS), and Amazon Simple Notification System (Amazon SNS)— allowing you to not only identify issues quickly but accelerate vulnerability remediation.



AWS Lambda remediation function triggered from webhook.

Start Bridging Workload Protection And Vulnerability Assessments

Prioritizing and remediating vulnerabilities will go a long way toward reducing the total attack surface. However, when it comes to legacy custom applications that have been lifted and shifted to the cloud, you may not be able to update them fast enough to address open vulnerabilities. Regardless of the application, you should have security measures in place to protect, detect, and respond to exploited vulnerabilities in your cloud workloads.

Cloud VMs, cloud instances, and containers are just as susceptible to known vulnerabilities, zero-day attacks, and malware as user endpoints. Runtime protection, detection, and response are critical to effective cloud workload security.

With SentinelOne, security and DevOps teams can operate from a single platform that unifies threat discovery with prevention, detection, and response for active exploitations. Working together, Amazon Inspector helps you proactively assess vulnerabilities, while Singularity Cloud Workload Security delivers layered, enterprise-grade protection, EDR, and Application Control to keep your AWS workloads secure.

Find SentinelOne in AWS Marketplace.

