INTEGRATION BRIEF

Achieve Unmatched Visibility of Your Cloud Environment

With Amazon GuardDuty and Rapid7 InsightIDR

Amazon GuardDuty is a continuous security monitoring service that analyzes AWS logs to detect potentially unauthorized, malicious activity. This includes events such as privilege escalation, misuse of credentials, and communication with malicious URLs. Rapid7 InsightIDR empowers you to detect intruders earlier in the attack chain with advanced user behavior analytics (UBA), giving you the SIEM you always wanted. By integrating Amazon GuardDuty with InsightIDR, you will be able to investigate GuardDuty alerts more comprehensively, create dashboards and reports using GuardDuty data to operationalize your AWS security, and contextualize and triage InsightIDR alerts. The result? Unmatched visibility of your cloud environment.

Why use the cloud over on-premise computing? You gain the ability to instantaneously change the entire makeup of your infrastructure. There's just one catch—the challenge of securing your environment to keep pace with the speed of the cloud. By using the powerful combination of Amazon GuardDuty and Rapid7 InsightIDR, you are able to spot misconfigurations in your cloud and get alerted to malicious user activity more efficiently than ever before.

HOW IT WORKS

1. Begin operating Amazon GuardDuty
2. Create an event source within InsightIDR to start ingesting logs
3. GuardDuty logs will now be stored within InsightIDR log search
4. Use built-in dashboards in InsightIDR to investigate GuardDuty findings

INTEGRATION BENEFITS

- Store Amazon GuardDuty logs within InsightIDR for search and visualization
- Create reports on GuardDuty findings that show trends over time, alert types, and instance types
- Create a single pane of glass for both Amazon cloud-based and on-premise threats
- Effectively investigate attacks by combining logs from GuardDuty, CloudTrail, on-premise technology, and other security solutions

WHAT YOU NEED

- Rapid7 InsightIDR
- Amazon GuardDuty

About Amazon

Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Fire tablets, Fire TV, Amazon Echo, and Alexa are some of the products and services pioneered by Amazon.

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. To learn more about Rapid7 or get involved in our threat research, visit us at www.rapid7.com.

112017