Amazon Web Services: CloudTrail and CloudWatch

CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. You can use it to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. In the Common Information Model, CloudTrail log data is typically mapped to the Authentication and Change data models.

CloudWatch is a service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. CloudWatch enables you to monitor your complete stack and leverage alarms, logs, and events data to take automated actions and reduce Mean Time to Resolution (MTTR). CloudWatch collects, aggregates, and summarizes compute utilization information like CPU, memory, disk, and network data, as well as diagnostic information like container restart failures, to help DevOps engineers isolate issues and resolve them quickly.

Data visibility

CloudTrail data provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. It increases visibility into your user and resource activity by recording AWS Management Console actions and API calls so you can detect unusual activity.

CloudWatch gives you actionable insights that help you optimize application performance, manage resource utilization, and understand system-wide operational health. It allows you to perform historical analysis for cost optimization and derive real-time insights into optimizing applications and infrastructure resources.

Configuration

Media, iframe, embed and object tags are not supported inside of a PDF.

Media, iframe, embed and object tags are not supported inside of a PDF.

Additional guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud).

Application

When your Splunk deployment is ingesting Amazon CloudTrail data and Amazon CloudWatch data, you can use the data to achieve the following AWS security objectives:

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
• Monitoring AWS EC2 for unusual modifications
• Verifying multifactor authentication usage
• Analyzing AWS service action errors
• Monitoring AWS S3 for suspicious activities
• Monitoring AWS and AWS EC2 for suspicious login activities
• Detecting AWS suspicious provisioning activities
• Detecting suspicious new instances in your EC2 environment
• Detecting AWS network ACL activity
• Monitoring user activity spikes in AWS

Amazon CloudWatch data can also be used to achieve these objectives:

• Detecting Kubernetes scanning activity
• Monitoring AWS Lambda

You may also be interested in the following:

• Troubleshooting AWS CloudWatch metrics observability
• Managing an Amazon Web Services environment
• Complying with General Data Privacy Regulation