AWS CloudTrail

Detection Strategy Guide

July 2025

Product Overview

AWS CloudTrail is an AWS service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. CloudTrail records actions taken by users, roles, or AWS services as events, including actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

These records provide a history of both API and non-API account activity, capturing who made the call, what actions were taken, which resources were affected, and where and when the activity happened. CloudTrail works across nearly all AWS services and regions, supporting both real-time and historical analysis. CloudTrail logs are stored in Amazon S3 and can be routed to other tools like Amazon CloudWatch Logs for monitoring or integrated with AWS Lake Formation for advanced analysis.

In order for Expel to gain access to your AWS CloudTrail logs you will need to create or leverage a trail and then make your S3 bucket available to Expel. Learn more in Get Started with AWS CloudTrail Setup.

Detection Strategy for Cloud Integrations

Detection

Our cloud security detection strategy focuses on two common signal types at the control plane and resource levels: authentication events and API events. In limited cases, we also ingest certain data plane events such as network activity. We do this by integrating directly with cloud providers as well as cloud security service providers to gain a complete view of your cloud footprint.

We consume these events through a mix of raw log analysis and security alert processing, which are then run through our detection engine to look for signs of post-exploitation activity. When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence. Additional Ruxie actions query a wide span of technologies in order to directly arm analysts with key pieces of investigative information and related events.

Response

In addition to verbose evidence collection for cloud alerts, cloud technologies are useful for triaging SaaS and identity alerts as well. User activities within the cloud providers, along with

related alerts for anomalous indicators, help analysts gain a full picture of the activity that occurred within a session.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for AWS CloudTrail

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** exp**e**ct **t**his) that we support for AWS CloudTrail, you can visit the Detections page in Workbench, or ask your Sales or Support rep for the most recent download.

Supported event log sources	■ API Gateway ■ CloudWatch (limited) ■ Elastic Block Storage (EBS) ■ EC2 ■ EKS ■ Lambda ■ RDS ■ Redshift ■ S3
AWS CloudTrail detection rules support	No.
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include: ■ Deactivate Access Keys To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help

	understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

Additional Details & Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

DUET Rules

A DUET (**d**id yo**u** exp**e**ct **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.