AWS CloudTrail vs Amazon GuardDuty

A SOC Analyst Deep■Dive Guide

1. AWS CloudTrail – The Audit & Forensic Log Source

AWS CloudTrail is a logging and audit service that records every API activity performed in an AWS account. It captures who did what, when, from where, and whether the action was successful or denied. CloudTrail is the source of truth for AWS forensic investigations.

What CloudTrail Records:

1. IAM actions (CreateUser, AttachRolePolicy, ConsoleLogin)
2. AWS service control plane operations (EC2, S3, VPC, RDS)
3. Source IP address, user agent, region, and timestamp
4. Success or failure of each API call

Types of CloudTrail Events:

1. Management Events – Control■plane operations (enabled by default)
2. Data Events – S3 object access and Lambda invokes (not default)
3. Insights Events – Detects unusual spikes in API behavior

CloudTrail does not provide threat detection or alerting by itself. It requires SIEM, correlation rules, or security services to interpret the data.

2. Amazon GuardDuty – Managed Threat Detection

Amazon GuardDuty is a managed threat detection service that continuously analyzes CloudTrail logs, VPC Flow Logs, DNS logs, and EKS audit logs using threat intelligence and machine learning. GuardDuty produces security findings instead of raw logs.

What GuardDuty Detects:

1. Credential compromise and anomalous IAM behavior
2. Reconnaissance and enumeration activity
3. Malware, crypto■mining, and command■and■control traffic
4. Privilege escalation and persistence attempts

GuardDuty assigns severity levels, maps activity to MITRE ATT&CK; techniques, and provides remediation guidance, making it SOC■ready.

3. Key Differences – CloudTrail vs GuardDuty

1. CloudTrail logs activity; GuardDuty detects threats
2. CloudTrail outputs raw JSON events; GuardDuty outputs findings
3. CloudTrail has no intelligence; GuardDuty uses ML and threat intel
4. CloudTrail is forensic■focused; GuardDuty is detection■focused

4. How SOC Teams Use Them Together

In real■world SOC operations, GuardDuty raises the alert while CloudTrail is used to validate, investigate, and reconstruct the attack timeline. GuardDuty identifies suspicious behavior, and CloudTrail provides evidentiary proof.

5. Interview■Ready Summary

CloudTrail is the foundational audit log that records everything happening inside an AWS account. GuardDuty is the intelligent detection layer that analyzes those logs and network telemetry to identify malicious activity. GuardDuty depends on CloudTrail, and CloudTrail alone cannot detect threats.