Lacework for AWS CloudTrail

Automatically detect anomalies in AWS account activity

Lacework for AWS CloudTrail protects AWS deployments by automatically detecting any anomalous activity in the millions of events logged by CloudTrail. Lacework Polygraph baselines AWS account activity, detects deviations from the baseline, alerts on anomalies, and simplifies the investigation of incidents.

Lacework for CloudTrail enables you to make sense of the millions of events captured in CloudTrail and is the perfect antidote to cloud security complexity: no rules, no policies, and no time spent on tedious event analysis.

Unauthorized Activity on AWS Resources

- Changes to AWS S3 buckets
- Unusual activity in new regions or accounts
- Activation of new AWS services
- Changes to AWS access control lists (ACLs)

Suspicious Changes to Users, Roles, or Access

- Adding users or roles to AWS
- Activation of new services, new users, and new APIs
- New users changing security groups or IAM policies
- Bypass of two-factor authentication (2FA)

Manipulation of AWS Infrastructure Services

- Changes to network interfaces and services
- Modifications to route table or new VPNs
- CloudTrail service stopped or logs deleted
- Access or customer master key tampering
Unprecedented Insights Into AWS Accounts

By deploying Lacework’s Polygraph on AWS CloudTrail, you instantly gain a better understanding of what’s happening in your AWS deployment. Our approachable visualization highlights the who, when, what, and how for all AWS account activity. No more tedious log correlation or guesswork. With Polygraph, your cloud infrastructure and security staff can work faster and smarter.

EFFICIENT

Zero-touch implementation, configuration, and operations: no rules, no policies, no log analysis. Operate without tuning, tweaking, or whitelisting.

SIMPLE

Categorize, group, analyze, and correlate AWS CloudTrail events automatically. Reduce security staff grunt work.

POWERFUL

Lacework automatically evaluates every AWS account event for you. You are only presented with what matters: anomalies, with easy access to insights.
Real-World Use Cases: Stopping AWS Account Exploits

**BITCOIN MINING**

Bitcoin mining operates by converting computing resources into digital cash. This makes AWS EC2 an inviting target.

Cybercriminals have learned to capitalize on the mistakes of software developers: AWS keys left open in source code published on GitHub. Criminals can simply help themselves and fire up unauthorized EC2 instances to dig for digital gold.

Administrators are left in the dark until they open their AWS bill. With Lacework for AWS CloudTrail, you will be automatically notified of EC2 instances unusual activity and can shut down currency miners before they dig up a single bitcoin.

**RANSOM DEMANDS**

Organizations are increasingly moving strategic projects to the cloud. Unfortunately, this makes them targets to hostage takers.

In a noted ransomware case, an attacker gained control of Cloudspace's AWS account and demanded ransom. The company tried to stop the attack and regain control. In retaliation, the attacker wiped out Cloudspace's data. All of it.

It's a tragic story with an important lesson: monitoring AWS accounts can prevent devastating consequences. Lacework for AWS CloudTrail spots unauthorized activities early so you can stop an attack before it damages your business.

**DATA LOSS**

Migrating to AWS goes along with moving data to the cloud. Stealing data, of course, has been a cybercrime goal since the Internet began.

2017 saw a rash of reports about poorly protected S3 buckets, exposing millions of sensitive records. Cybercriminals are still combing AWS for insecure S3 buckets, and it's a sure bet they’ll find them.

AWS highlighted CloudTrail as a key technology to combat these mistakes. Lacework augments CloudTrail capabilities with automatic anomaly detection and alerting that will let you benefit from the events captured in CloudTrail.