FEATURE BRIEF

Composite alerts

OVERVIEW

Correlate data to find threats in the noise

Lacework composite alerts automatically combine multiple detections to define more specific alert conditions without excessive querying or significant expertise and effort. The platform can accurately detect active cloud attacks by automatically combining multiple low severity alerts that often go unnoticed by security teams into a single, meaningful alert.

To date, Lacework composite alerts have detected attacks like cloud ransomware, cryptomining, and compromised credentials. When applicable, composite alerts integrate Amazon GuardDuty findings to enrich evidence of an ongoing security issue. Composite alerts are also Kubernetes-aware and can point out threats like compromised K8s users.

With Lacework composite alerts, you can:

Save time and costs

Automatically reduce alert volume and eliminate the need for excessive querying, expertise, or effort.

Speed investigation and response

Arm security and DevOps teams with the context required to understand an alert's importance, how to investigate and triage the threat, and quickly mitigate the risk.

Detect elusive threats

Accurately detect early signs of active attack patterns by combining multiple low severity signals into a single, meaningful alert to keep cloud entities safe.

LACEWORK BENEFITS

- **Efficiency**

  Use automation to find real threats, rather than manual, unscalable approaches to detecting modern cloud attacks.

- **Context**

  Gain deep, actionable context on alerts so that security and DevOps teams know what to fix first.

- **Clarity**

  Reduce noise in your cloud environment by tying disparate, low-level events together that point to larger threats.

Designed to catch elusive cyber attacks

Real threats often hide in medium, low, or informational alerts. Today's cybercriminals are constantly evolving their techniques to fly under the radar and avoid detection for as long as possible. Composite alerts allow organizations to be confident that they are detecting critical and high severity alerts, while not missing real threats in low-to-medium severity alerts.

Composite alerts can detect:

- Potential cloud-native ransomware attacks
- Potential cryptomining attacks on hosts
- Potential AWS defense evasion
- Potentially compromised AWS keys
- Potentially compromised hosts
- Potentially compromised Google Cloud identities
- Potentially compromised K8s user

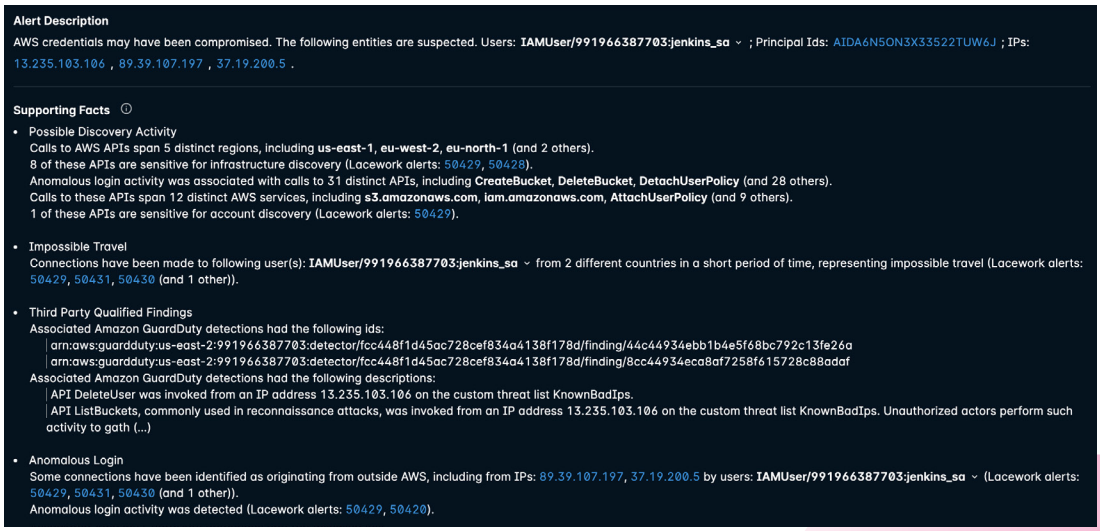

Figure 1: Lacework composite alerts are rare and reliably signal suspicious activity. The Details tab includes all evidence pointing to the cloud threat.

Why Lacework?

"These enriched composite alerts give us greater confidence and reduce our investigation time, allowing us to focus on the threats that could have the greatest impact on our cloud."

INSTRUCTURE YISEHAK LEMMA, CISO

Explore an interactive demo >>

About Lacework

Lacework keeps organizations secure in the cloud, allowing them to innovate faster with confidence. Cloud security requires a fundamentally new approach and the Lacework platform is designed to scale with the volume, variety, and velocity of cloud data across an organization's cloud environment: code, identities, containers, and multicloud infrastructure. Only Lacework provides Security and Development teams with a correlated and prioritized end-to-end view that pinpoints the largest risks and handful of security events that matter most. Learn more at www.lacework.com.