LACEWORK.

Eliminating complexity to empower a small team to better secure their Google Cloud

sift

Challenges

· Small security team needed to scale

· Inadequate resource capacity to manage rules-based approach

· Needed to satisfy requirements for upcoming SOC 2 certification

Solutions

· Achieved new levels of team efficiency

· Enabled thorough investigation of the alerts that matter

· Gained breadth of coverage managed by a single pane of glass

Results

· Reduced alert volume to one critical alert per day

· Streamlined investigation time to under five minutes per event

· Accelerated security roadmap by six months

"Using the Lacework platform, we were able to reduce our security budget by 50%. It's all done in a complete package, with a single pane of glass, at the click of a button."

SCOTT KLEVEN, SECURITY PROGRAM LEADER

Security challenge

Sift was concluding a major cloud transformation, having migrated to Google Cloud Platform. They were loading rich, massive Google Cloud logs into their SIEM and were quickly exceeding their existing capacity. Their current approach would require adding SIEM capacity and 10+ people to write and maintain rules and investigate alerts. They would also need to expand their security stack to support an upcoming SOC 2 certification. This approach was not scalable, so they decided to invest in a consolidated solution that could meet their budget, time, capability, and efficiency requirements.

A small security team becomes exceptionally efficient

With a small security team, efficiency must be the primary focus of the Sift team. "With Lacework, we take what would otherwise take a team of five and turn it into something that I can manage on my own in minutes," says Schneider. "I can stay on top of everything that is happening in our environment and am alerted when I need to take action. The amount of work reduced and visibility achieved is game-changing."

Using Lacework, the Sift security team doesn't need to spend valuable time writing rules and can complete thorough investigations of anomalous events in minutes instead of hours. Lacework has unlocked greater efficiency, which has allowed them to accelerate their security roadmap by more than six months. "I don't need to worry about that side of the house, and I can focus my team on new revenue-generating aspects of the business," says Scott Kleven, Security Program Leader.

Solving multiple security needs with a single platform

To support an upcoming SOC 2 certification, the Sift team needed to add file integrity monitoring, vulnerability detection, intrusion detection, and additional compliance reporting capabilities to their technology stack. Lacework improved these capabilities seamlessly, with a single pane of glass for a consistent management experience. Sift's DevOps team appreciated that a single Lacework agent could address various needs, freeing up engineering resources. "Using the Lacework platform, we were able to reduce our security budget by 50%," Kleven explained. "It's allowed us to use our small security team to cover a much broader breadth. It's all done in a complete package, with a single pane of glass, at the click of a button."

Find out more at lacework.com

Sift is a leader in the digital trust and safety industry. Sift reviews online user session behavior and provides a score that indicates the likelihood of a session being fraudulent, ultimately preventing fraud and abuse for their customers. Their AI and machine learning-based engine analyzes over 35 billion transactions per month for global brands.