Industry:
Financial

Use cases

- Expand visibility
- Improve detection coverage & accuracy
- Accelerate incident response

corelight

Case study

Global financial firm mitigates multi-platform identity attack in under two hours

ABOUT THE COMPANY

A global financial services and proprietary trading firm that handles massive volumes of high-speed transactions and sensitive financial data daily sees protecting its corporate identity and digital assets from sophisticated and evasive threats as a top security priority.

THE CHALLENGE: A SOPHISTICATED IDENTITY SPOOFING ATTACK

The firm's security team uncovered a sophisticated attack targeting their employees and business partners via suspicious emails and automated security alerts from Google Workspace. Threat actors were creating unauthorized Google Workspace accounts using legitimate corporate email addresses. This attack method is a growing one, where many new evasive attacks use living-off-the-land (LotL) tactics that take advantage of existing authorized tools in the environment. The goal was not to send emails, but to establish a trusted identity that could then be used to create rogue Slack workspaces.

These fraudulent workspaces were used to send direct messages containing phishing links and malicious attachments, which appeared to come from legitimate employees. The attack successfully bypassed traditional security controls by exploiting employees' implicit trust in sender identities using the corporate domain within these major SaaS platforms. The low-level alerts from Google Workspace highlighted suspicious activity, but in isolation, they left the team blind to the broader scope of the attack.

THE SOLUTION: HIGH-FIDELITY EVIDENCE FOR A COMPLEX THREAT

The security team needed a single source of truth to connect the dots between the siloed alerts. They turned to Corelight's network evidence to see the full story. Corelight's detailed logs connected suspicious activity across both Google and Slack into a single, coherent timeline. By analyzing information from the DNS requests, TLS certificates, and connection logs, the team could trace the creation of the fake Google accounts and the subsequent API calls to Slack. This enabled them to correlate suspicious activity across Google and Slack, and quickly determine which employees and domains were affected.

Corelight provided the high-fidelity forensic-grade evidence needed to distinguish legitimate from malicious activity, even when it originated from trusted services like Google and Slack.

THE RESULT: FULL MITIGATION IN LESS THAN TWO HOURS

With the clear evidence from Corelight, the security team fully mitigated the threat in less than two hours. They took control of their domain within Google Workspace, seized the fraudulent accounts, and worked with Slack to shut down the rogue workspaces.

The rapid incident response highlighted the critical need for deep network visibility to combat modern, evasive, LotL, and identity-based threats. By leveraging Corelight Sensors, the firm transformed a series of confusing, isolated alerts into a clear and actionable response, protecting its brand, securing its employees, and turning a potentially devastating security incident into a well-managed, rapid response.

WHY CORELIGHT

Other tools generated alerts, but they were fragmented and siloed inside individual SaaS platforms. Corelight provided:

- **Cross-platform visibility:** Connected Google Workspace activity with Slack API calls to reveal the true scope of the attack.
- **High-fidelity evidence:** DNS, TLS, and connection logs showed exactly how fake accounts were created and abused.
- **Single source of truth:** Transformed confusing, isolated alerts into one coherent timeline of attacker activity.
- **Faster response:** Enabled the team to identify all impacted employees and shut down rogue accounts in under two hours.

corelight

To learn more about combating evasive attacks, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497