Industry:
Transportation/
High Tech

Use cases
- Accelerate incident response
- Expand visibility

corelight

Case study

Autonomous vehicle pioneer verifies Log4j exposure and uncovers internal risks with network evidence

Background: Engineering the future of mobility

Developing self-driving technology requires more than just sensors on the road; it requires a complex, high-performance engine behind the scenes. This leader in the autonomous vehicle space manages a sprawling hybrid environment that bridges on-premise data centers with Google Cloud Platform (GCP). This infrastructure generates massive volumes of network traffic—data that is essential to their innovation but creates a vast surface area to secure.

Challenge: Proving a negative and finding hidden threats

When the Log4j vulnerability hit, the question wasn't just "are we safe?" but "can we prove it?" Like many organizations, the security team needed a definitive source of truth to verify exposure. Guesswork implies risk, and in this industry, precision is everything.

Simultaneously, the team was on a mission to hunt for the quiet risks—such as unencrypted credentials—that allow attackers to move laterally undetected. Without high-fidelity network evidence, both verifying Log4j and hunting for hidden threats were slow, inconclusive processes. They were essentially driving in the dark.

> **"I am happy with our partnership & would give an 'A' at this point… Love the proactive approach & the way [Corelight delivers] new features."**
>
> - Security engineer

Solution: A single source of truth for on-prem and cloud

To turn the lights on, the company deployed Corelight's Open NDR Platform. They placed hardware sensors in their physical data centers and software sensors in GCP, establishing a consistent, rich stream of data across their entire hybrid map.

The team then forwarded Corelight's Zeek® logs to their CrowdStrike LogScale instance. This created a centralized command center for deep analysis, giving them the visibility required to turn raw traffic into actionable intelligence.

Results: Confident response and proactive risk reduction

With comprehensive network evidence at their fingertips, the security team stopped hoping for the best and started verifying reality.

- **Rapid incident verification:** The team utilized Corelight as their primary verification tool to identify specific instances of Log4j activity. This allowed them to confirm the full scope of their exposure and respond with the speed and confidence the situation demanded.
- **Hidden risk discovery:** Proactive threat hunts using Corelight data revealed instances of unencrypted credentials passing over HTTP. This insight allowed them to close a critical security gap before it could be exploited.
- **Established as a foundational tool:** Corelight evolved from a tactical solution to a cornerstone of their security program, providing the essential evidence needed for investigations across a complex hybrid landscape.

Why Corelight: Trustworthy data at scale

The security team chose Corelight to replace an unmanaged, open-source Zeek deployment. They needed enterprise-grade muscle that could scale across a hybrid environment without adding management overhead. Corelight provided the rich, actionable network evidence and seamless integration necessary to tackle both emerging threats and latent risks with authority.

corelight

To see how Corelight helps transportation and high-tech security teams accelerate incident response and expand visibility, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497