Industry:
High Tech

Use cases

- Accelerate incident response
- Improve detection coverage & accuracy

corelight

Case study

Global gaming giant thwarts $10M ransomware attack with network evidence

BACKGROUND: PROTECTING A GLOBAL ENTERTAINMENT LEADER

A global game developer with more than $1 billion in revenue and millions of daily players operates a massive, complex digital infrastructure. Protecting its intellectual property and ensuring player trust is paramount to its business.

CHALLENGE: THE $10 MILLION RANSOMWARE DEMAND

The company received a ransomware email demanding $10 million, with attackers claiming to have stolen a significant amount of sensitive source code and other critical IP. The executive team was faced with a high-stakes decision: pay the ransom or risk the public release of potentially damaging data. Their existing security tools, while extensive, could not provide the definitive source of truth needed to quickly verify the attackers' claims and scope the full extent of the breach.

> "Corelight was tremendously valuable during the ransomware attack."
>
> - Security team member

SOLUTION: UNCOVERING THE TRUTH WITH HIGH-FIDELITY NETWORK EVIDENCE

The security team turned to Corelight's Open NDR Platform. The rich, comprehensive network evidence generated by Corelight's Zeek and Suricata engines was instrumental in the investigation. No matter how stealthy attackers are, they cannot avoid the network and inevitably leave 'footprints' of their activity. The problem is that most traditional security tools lack the necessary visibility to see this evidence. Unlike alerts from other tools that lacked context, Corelight provided a complete historical record of the attackers' activities, allowing the team to trace their every move with certainty.

Corelight's evidence allowed the team to rapidly build a timeline of the attack. They witnessed evidence of intruders moving laterally across the network via SMB traversal, attempting to reach the company's 'crown jewels'—the game build servers. They saw the attackers' attempts to smuggle data out to a cloud storage location. This granular visibility gave them irrefutable proof of what was—and was not—compromised.

In addition, the investigation also highlighted how network evidence is invaluable not just for tracking threats, but for identifying network hygiene issues that leave the door open for attackers. For example, the team observed the attackers use plaintext passwords to access servers and internal Docker registries, revealing a critical internal security gap.

RESULTS: A CONFIDENT REJECTION AND A CLOSED INVESTIGATION

Within hours, the investigation yielded a clear and powerful conclusion: the attackers had lied. The data they exfiltrated was limited and non-critical. Armed with this definitive network evidence, the leadership team confidently rejected the ransom demand.

- Saved $10,000,000 by confidently rejecting the ransom demand
- Accelerated incident response by providing the authoritative source of truth for network activity, enhanced with real-time context to scope the attack in hours, not weeks
- Provided executive assurance with indisputable evidence, transforming a high-stakes crisis into a decisive security win
- Strengthened security posture by uncovering weak points like plaintext password usage, which were immediately remediated

WHY CORELIGHT: CERTAINTY IN A CRISIS

In a high-pressure situation where “I think” isn’t good enough, Corelight delivered the certainty of “I know.” The platform’s ability to provide complete, queryable network evidence enabled the security team to move beyond alerts and truly understand the scope and impact of the attack. This clarity was the key to making a confident, evidence-based decision that saved the company millions and protected its reputation.

corelight

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

https://corelight.com/contact

info@corelight.com | 888-547-9497