corelight

Case study

Top government agency uses network detection & response

to improve visibility across diverse & ever-changing environments

The agency builds the foundation for a new SOC to gain the upper hand in national security.

BACKGROUND: NO ORDINARY EXERCISE

In the high-stakes world of national security, it's a never-ending battle to keep up with attackers' latest tools and techniques. This is particularly crucial at the highest levels of the Federal government and its partners, where agencies are tasked with domestic and international security that affects the lives of billions of people daily.

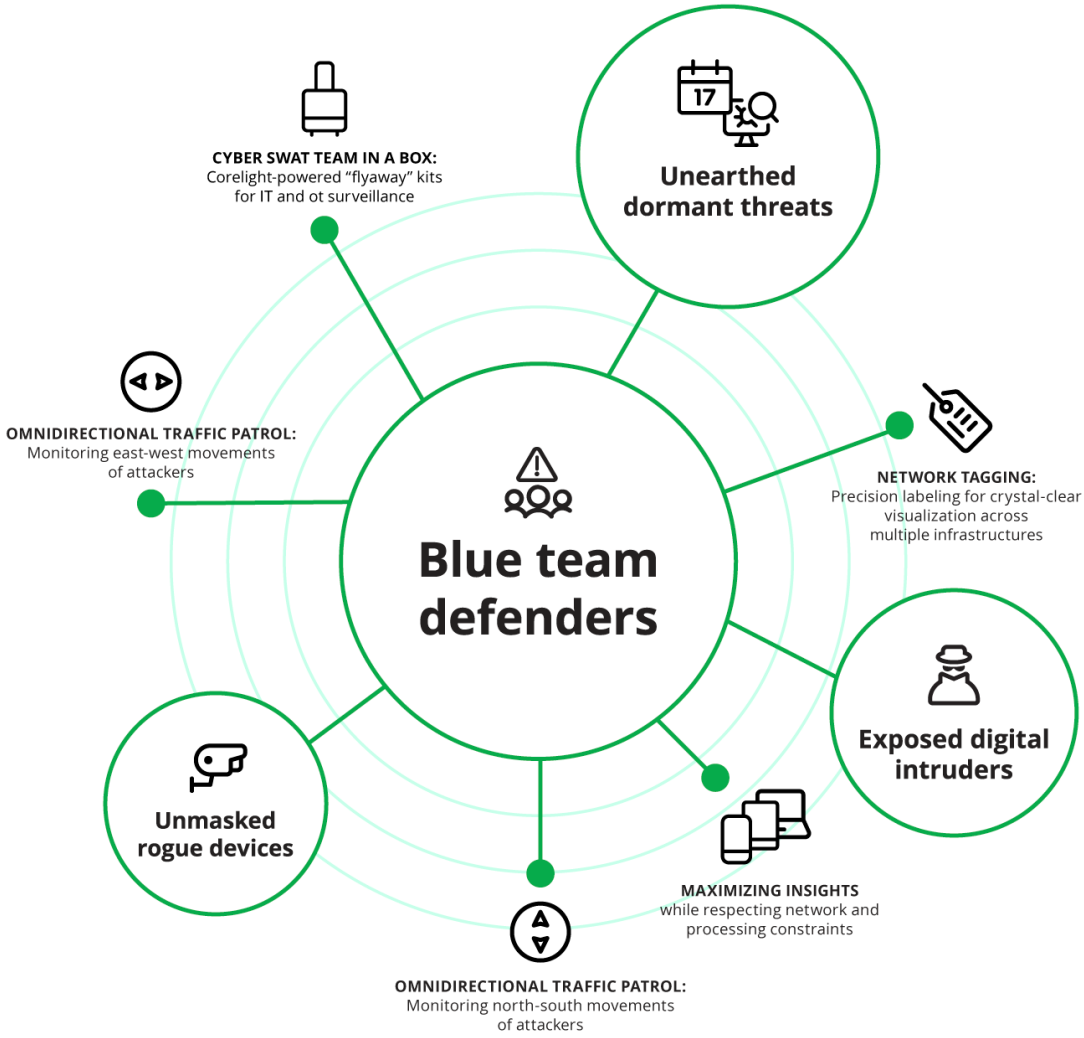
In an effort to safeguard some of the nation's most sensitive information and environments, one top U.S. security agency (the "Agency") rapidly assesses and secures unfamiliar locations under intense time pressure. The Agency works across diverse environments—most of which the agency does not control, did not set up the IT infrastructure for, nor has a baseline of network traffic to understand what is "out of the ordinary." Their mission: to identify and neutralize potential threats in highly sensitive situations.

To train the Agency's team to better understand the modern threat landscape and improve protection against physical and digital attacks, a premier national research organization invited them to participate in a hands-on "red team, blue team" security exercise at their facility. The facility's infrastructure was anything but ordinary—it was a complex ecosystem of advanced IT systems seamlessly integrated with critical operational technology (OT) components.

> **"Corelight is one of the most knowledgeable and supportive teams I've ever worked with."**
>
> - Agency lead

Whether an exercise or a real world example like that of the Volt Typhoon, critical infrastructure continues to be the target of attackers who use "living-off-the-land" techniques to infiltrate and disrupt. Industry reports show these types of industrial facilities are increasingly vulnerable to cyber threats:

- In 2023, Researchers at Georgia Tech found that 78% of the discovered attack paths were found to be exploitable using only publicly available tools and techniques.
- In 2023, 53% of vulnerabilities analyzed by Dragos could cause both loss of view and control of industrial processes, a 3% increase from 2022.
- About 34% of security vulnerabilities impacting industrial control systems (ICSs) that were reported in the first half of 2023 have no patch or remediation, registering a significant increase from 13% the previous year. (2023 report by SynSaber)



Using a comprehensive approach to threat detection with Corelight Network Detection & Response (NDR), the Blue Team was able to map the entire IT/OT environment in a security exercise, revealing several critical findings on the network.

CHALLENGES

The Agency faced several challenges in defending these types of environments:

- Monitoring diverse and complex network environments that they do not typically control nor set up, including an increasing number of OT systems found on IT networks (best practices recommend having these environments separated)
- Identifying potential threats in high-pressure situations where time to detection is critical
- Identifying regular vs anomalous traffic in an unfamiliar environment without full network ownership
- Managing a high turnover rate in their security team. This requires easy-to-implement and maintain solutions that are clear enough for new team members to pick up quickly where previous teams left off
- Transforming raw network data into relevant insights, beyond basic NetFlow but short of full packet capture
- Bridging the gap between IT and OT security with a team of generalists

> **"For once, we weren't chasing shadows. We saw the attack unfold in real-time, "This exercise is a game-changer—it's given us a playbook for future threats."**
>
> - Agency lead

THE EXERCISE: LEARNING NETWORK PROTECTION & ELITE DEFENSE

The security exercise was designed to teach the Agency how to identify and remediate attacks from highly sophisticated adversaries. The research facility played the role of the "Red Team," simulating advanced attackers targeting industrial control systems (ICS) and OT. The Agency's team—cast as the "Blue Team" defenders—deployed their mobile security operations center (SOC). The Blue Team's mission was to uncover hidden threats lurking within both IT and OT environments, aiming to stay ahead of the simulated attackers.

> **"Corelight just works out of the box. Plug it in and it starts to work quickly."**
>
> - Agency lead

As part of the exercise, the research facility set up both real and simulated OT and IT environments across various parts of the organization and corporate network—including electric power plants, building automation, and HVAC systems. The exercise was modeled after a real-world attack and, like many breaches, began with a simple phishing email. Once clicked, the Red Team gained access to parts of the corporate network, made lateral movements, and eventually breached the OT side and building-automation systems.

The Blue Team monitored IT and OT networks, tracing the Red Team's movements through physical effects on the network. The research facility created a virtual "mini town" to visualize events across environments, allowing them to "see" trouble spots and quickly move in to remediate. The Red Team was able to manipulate the OT systems, even starting a physical fire in one part of the town. The Blue team was able to see fires start and smoke generated as soon as they started.

The Blue Team defenders leveraged a comprehensive approach to threat detection:

- Cyber SWAT team in a box: lightning-fast deployment of Corelight-powered "flyaway" kits for IT and OT surveillance
- Omnidirectional traffic patrol: monitoring both north-south and east-west movements of attackers through the network
- Network tagging: precision labeling for crystal-clear visualization across multiple infrastructures
- Maximizing insights while respecting network and processing constraints

RESULTS: GREATER VISIBILITY & A PLAYBOOK FOR A MORE SECURE FUTURE

OT systems present unique challenges, as they control everything from building management to HVAC and IoT devices. Unlike traditional IT infrastructure, many of these components can't be secured with standard endpoint protection. Instead, they require close monitoring of network behavior for anomalies.

Using Corelight NDR in this exercise, the Agency was able to map the entire environment, revealing several critical findings on the network:

- Exposed digital intruders: caught bad actors that might have otherwise been missed by OT blind spots. It was able to identify and fight physical fires set up by the Red Team
- Unmasked rogue devices: spotted security cameras gone wild, operating beyond their expected boundaries
- Unearthed dormant threats, powering digital forensics with insights from historical data that spanned across months and not days

"For once, we weren't chasing shadows. We saw the attack unfold in real-time," continued the Agency lead. "This exercise is a game-changer—it's given us a playbook for future threats."

KEY BENEFITS

- X-ray vision for networks: seamless visibility across IT and OT landscapes
- Threat hunter's edge: uncovering dangers lurking in overlooked OT corners
- Time machine analytics: rewinding the clock on attacks for full-scope insights
- Plug-and-protect deployment: battle-ready kits for instant fortification
- Adaptability: thriving in any network ecosystem
- Future-proof management: streamlined upkeep with Corelight's intuitive interface and Fleet Manager

LET THERE BE CORELIGHT

"Corelight just works out of the box. Plug it in and it starts to work very quickly," noted an Agency lead on the project. "Corelight is one of the most knowledgeable and supportive teams I've ever worked with," the Agency lead continued. "The solution worked perfectly, exactly as we'd hoped it would."

Corelight provided visibility into all network traffic, revealing potentially malicious activities. When the Agency faced challenges, Corelight offered significant assistance in identifying and solving problems. Its NDR solution can parse more than three (3) dozen protocols to be used across a variety of ICS and OT environments.

Flexibility is at the core of the Corelight solution. One example is the SPICY framework, a parser generator that facilitates the creation of robust C++ parsers for network protocols, file formats, and more. This framework allows customers to write their own protocols for unique use cases and run them on Corelight, enhancing its adaptability to diverse environments.

CONCLUSION: YOU CAN'T PROTECT WHAT YOU CAN'T SEE

In today's interconnected world, the line between office networks and industrial systems is blurring. This exercise illuminated vulnerabilities in facilities, exposing weaknesses not only in corporate networks but also in unexpected places like security cameras and HVAC systems.

Corelight's NDR solution helped quickly identify and remediate potential cyber threats in both traditional IT and often-overlooked operational technology. It served as the Agency's eyes and ears on the network, providing unprecedented visibility across diverse environments. Through this exercise, the Agency gained valuable insights about the modern security landscape, helping them build the future SOC that the agency will deploy to secure sensitive situations.

The bottom line? In cybersecurity, you can't protect what you can't see. As the field evolves, visibility and network detection are critical in helping defenders identify threats early on, allowing us all to sleep a little easier at night.

corelight

To learn more, request a demo at **https://corelight.com/contact**

info@corelight.com | 888-547-9497