WHITE PAPER

How Corelight's ICS/OT Collection enhances visibility across diverse networks

INTRODUCTION

Industrial Control Systems (ICS) and Operational Technology (OT) devices aren't always limited to heavy industrial or utility environments. Often, they can be observed communicating on unsuspected segments of traditional enterprise IT networks, potentially exposing organizations to unknown risks. The lack of awareness and understanding of these devices within both enterprise and industrial networks can lead to security blind spots, making them an attractive target for threat actors. Addressing this challenge, Corelight presents the ICS/OT Collection—a solution designed to provide enhanced visibility and security for ICS/OT devices and protocols across diverse environments.

Corelight's ICS/OT Collection capabilities

Corelight's ICS/OT Collection enhances our sensor capabilities by delivering visibility into ICS/OT network communications, expediting incident response, and simplifying inventory management. This collection identifies and logs activity related to ICS/OT protocols, yielding greater visibility and faster incident response times. It empowers security teams to comprehend and defend their environment more thoroughly, whether it's a manufacturing plant's control system or an enterprise network with unexpected ICS devices.

Visibility for diverse environments

FOR ENTERPRISE IT CUSTOMERS

Enterprise networks, which are not traditionally associated with ICS/OT, may unknowingly host these devices and protocols. These could include systems such as HVAC, security cameras, smart lighting, and access control systems, all of which could be exploited by threat actors.

With the ICS/OT Collection, enterprises can discover and comprehend these devices within their network. This newfound visibility aids in inventory management, incident response, and network behavior monitoring for potential risks, offering a crucial layer of defense against unauthorized access and misuse.

FOR FEDERAL AGENCIES

Federal agencies are tasked with a mission-critical responsibility to protect their networks and systems from threats while adhering to regulatory guidance. In this capacity, the ICS/OT Collection from Corelight proves to be an invaluable tool. The Collection enables these agencies to detect, analyze, and understand ICS/OT protocols present in their networks, enhancing their ability to monitor and safeguard against potential cyber threats.

Furthermore, the ICS/OT Collection was developed based on contributions from the Cybersecurity and Infrastructure Security Agency (CISA), leveraging their National Infrastructure Protection Plan (NIPP) and amplifying their expertise to address the unique cybersecurity challenges that federal agencies face.

FOR INDUSTRIES WITH ICS/OT NETWORKS

Industries such as healthcare, transportation, oil and gas, chemical, food and beverage, pharmaceuticals, and telecommunications rely on ICS/OT networks to automate and control critical processes, maintain operational efficiency, and ensure safety. These environments could include a wide variety of systems, ranging from process automation in manufacturing facilities to control systems for public utilities.

Regardless of the specific application, the ICS/OT Collection provides valuable insights that can significantly improve incident response times, contribute to forensics analysis, and enable continuous monitoring of network behavior. This ability to understand and monitor network behavior aids in managing and mitigating potential risks, regardless of the size or scale of the organization. Thus, Corelight's ICS/OT Collection proves to be a vital tool in enhancing the security posture of companies in the industrial and utility sectors.

Uses cases for Corelight's ICS/OT Collection

SECURITY MONITORING AND INCIDENT RESPONSE

The ICS/OT Collection helps security teams maintain constant awareness of the ICS/OT protocols in their network, which is crucial for identifying potential security incidents. For instance, it lets teams detect unusual network behavior, such as a lighting controller talking to a payroll server. The ability to monitor these protocols aids in incident triage and forensics, offering insights that can significantly accelerate the incident response process.

ASSET AND INVENTORY MANAGEMENT

As the saying goes, "You can't protect what you don't know about." With Corelight's ICS/OT Collection, security and network teams can maintain a detailed inventory of ICS/OT devices and the protocols they use. This visibility is crucial for managing and mitigating risks associated with critical infrastructure devices.

NETWORK BEHAVIOR ANALYSIS FOR RISK MANAGEMENT

Many ICS/OT protocols are unauthenticated and unencrypted, which could present significant risks if misused or accessed without authorization. The ICS/OT Collection allows teams to monitor and analyze network behavior for specific risks, providing a proactive risk management approach.

Examples of supported protocols:

- BACnet: Protocol for building automation and control systems
- DNP3: Protocol for utility industry control system communication
- Ethercat: High-speed industrial Ethernet protocol for real-time control
- Ethernet/IP and CIP: Protocols for industrial automation and device integration
- Modbus: Widely used protocol for serial communication between devices
- PROFINET: Ethernet-based protocol for industrial automation and process control
- S7Comm: Siemens' protocol for communication with S7 programmable logic controllers
- TDS: Tabular Data Stream, a protocol used by Microsoft SQL Server for database communication

  Detailed protocol logs are generated for each enabled protocol, and new services are identified in the connection log, providing a detailed view of the network's communication and behavior.

Conclusion

Corelight's ICS/OT Collection offers critical insights into industrial control systems and operational technology, providing enhanced visibility, rapid incident response, and accurate inventory management. These capabilities are crucial for defending against threats in these critical sectors. By leveraging Corelight's ICS/OT Collection, organizations can bolster their defense against cyber threats and contribute to a more resilient industrial landscape.

Learn more about Corelight Collections

Corelight Collections are detection sets included with your Corelight subscription and can be activated depending on your needs. In addition to the ICS/OT Collection, Corelight also offers the following collections:

- Entity Collection
- Encrypted Traffic Collection
- C2 Collection
- Core Collection

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497