corelight
NETWORK DETECTION & RESPONSE

NDR FOR PUBLIC SECTOR

STATE | LOCAL | EDUCATION | CRITICAL INFRASTRUCTURE

With complex networks and limited security resources, public sector organizations need smarter detection. Corelight turns network activity into meaningful insights, empowering SOC teams to uncover threats quickly, respond decisively, and optimize data costs.

BENEFITS OF **CORELIGHT NDR**

VISIBILITY

- Uncover threats before impact with real-time traffic monitoring of IT and OT networks, including control centers, substations, and supply chains
- Strengthen ransomware defense to see early signs of reconnaissance and scanning, and capture evidence of data access / movement
- Comprehensively **inventory** devices, services, credentials, and certificates on the network
- Safeguard operations by spotting lateral movement to stop threats before critical systems are affected

DETECTIONS

- Protect command integrity by detecting anomalies in OT protocols including Bacnet, Modbus, DNP3, and more
- Lower operational disruption risks: see irregularities in vulnerable systems using behavioral analytics
- Automate broad file-based malware detection and identify payloads like BlackEnergy using YARA rules

RESPONSE

- Triage up to 50% faster and accelerate IR to help ensure uptime and continuous operations
- Interrupt exfiltration and unauthorized transfer attempts to safeguard sensitive data
- Identify attack origin, scope, and spread to rapidly contain incidents, including phishing

FORENSICS + OPERATIONS

- Support NERC CIP standards efforts and maintain detailed logs for investigations and root cause analysis
- Improve future defensive strategies by retrospectively identifying APT behaviors on the network
- Enhance system insight by optimizing logs for high-priority traffic flows to reduce SOC noise and enhance focus on key activities

BUILT FOR PUBLIC SECTOR NETWORK NEEDS

- Compliant & Secure: Aligned with sensitive cybersecurity frameworks and data protection standards
- Flexible Deployment: On-prem or cloud-ready to fit your infrastructure and budget
- Compatible with Existing Tools: Integrates easily with Splunk, Elastic, Microsoft Sentinel, and other SIEMs
- Open Ecosystem: Backed by open standards, avoiding vendor lock-in

CORELIGHT'S **OPEN NDR PLATFORM**

corelight

Close cases faster, with more accuracy and greater efficiency

Strengthen infrastructure security with a system designed to help you detect and quickly neutralize adversaries. Our 4:1 Open NDR Platform combines a full detection suite with IDS, PCAP, NetFlow and NSM and creates a standardized dataset across alerts, logs, files, and packets. Powered by open-source technologies including Zeek®, Suricata®, and YARA, it seamlessly connects alerts to evidence for rapid response, forensics, and reporting. The platform streams logs in real time to your SIEM, offering native integration with existing tools across your security stack. Deployable in a range of environments and scalable from 1 Mbps to 1 Tbps per sensor, it offers central control and management of hundreds of sensors from one dashboard. Streamline operations with this fully integrated solution. **Learn more.**

COMPREHENSIVE VISIBILITY

- Unify visibility and aggregate industrial telemetry across hybrid environments
- Monitor OT/IT convergence points for APTs and lateral movement
- Expand visibility to unmonitored assets and third party data
- Inventory assets in use with Corelight's **Entity Collection**
- Establish baseline network activity to detect security events

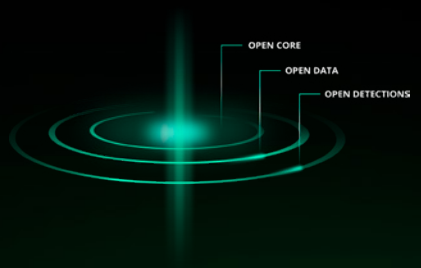
EXPANDED DETECTION COVERAGE

Lateral Movement	PLC-to-PLC scanning, abnormal function calls
Command Injection	Unauthorized Modbus writes, unexpected register changes
Replay Attacks	Timed ICS command sequences replays Reconnaissance
Reconaissance	Port sweeps, unauthorized device enumeration
Protocol Anomalies	Invalid function codes, malformed packets
IT/OT Bridge Detection	Traffic from IT-originating hosts in ICS VLANs

- Parses 10+ industrial protocols including BACnet, DNP3, EtherCAT, CIP/ENIP, Modbus/TCP, PROFINET, and S7Comm. Corelight's **ICS/OT Collection**
- Enhance NERC CIP programs with perimeter monitoring and real-time detection and response
- Improve malware detection rates by up to 35% with YARA file analysis
- Uncover unauthorized access points and expired certificates
- Extract insights from encrypted traffic analysis
- Create custom detections to identify unauthorized access to sensitive data

FASTER INCIDENT RESPONSE

- Lower MTTR with AI-assisted workflows, automation, and guided triage
- Automatically capture evidence from suspicious flows and extend forensic windows with Smart PCAP
- Discover the entire kill chain with fast, chainable searches
- Increase close rates and validate containment



INCLUDES:

- Detections
- SIgnature-based
- Behavioral
- Anomaly
- AI/ML

Static file analysis • Threat intelligence

Integrated visuals and context

Deep integrations with cloud control plane data

Coverage for 80+ MITRE ATT&CK® network TTPs

Deploy as physical or virtual appliances, cloud sensors, or with air gapped support

Integration-ready with SIEMs, SOAR, and XDR tools

CORELIGHT'S **OPEN NDR PLATFORM**

corelight

STREAMLINED OPERATIONS

- Enhance resilience and improve reporting for NIS2, CEER, etc.
- Quickly and precisely generate detailed audit reports
- Ensure reliability with continuously monitored and updated software
- Access technical support provided by industry-leading Corelight experts
- Benefit from an open platform to accelerate innovation and avoid vendor lock-in
- Available rggedized hardware for on-site ICS environments

PROVEN IN THE PUBLIC SECTOR

Corelight protects some of the largest government agencies, research universities nationwide—helping them detect ransomware, insider threats, and lateral movement before damage occurs.

STRENGTHENING CYBERSECURITY FOR THE PUBLIC SECTOR

SAFEGUARDING SYSTEMS RELIED ON BY
61+M
CITIZENS AND STUDENTS

DEFENDING
$27B+
IN R1 UNIVERSITY RESEARCH ACTIVITY

PROTECTING
532M+
ANNUAL TRANSIT RIDES

OPERATING ACROSS
22
U.S. STATES

ACADEMIC MEDICINE, HIGHER ED, K-12, LOCAL GOVERNMENT, STATE AGENCIES AND UTILITIES, TRANSPORTATION

"**If you have intelligence from the platform along with skilled people who know how to use it,** you at least have a fighting chance against the evolving threat landscape."

— Mike Manrod, Chief Information Security Officer (CISO), Grand Canyon Education

ENHANCE VISIBILITY AND SECURITY FOR **ICS/OT** DEVICES AND PROTOCOLS

Corelight's turnkey **ICS/OT Collection** enhances the Open NDR Platform by monitoring the most common ICS and OT protocols, empowering security teams to defend against threats across diverse environments.

- Log protocols like BACnet, DNP3, Ethercat, and Modbus
- Identify new services in the connection log in real-time
- Based on contributions from DHS CISA

WORLD-CLASS SUPPORT

Our support team continually delights customers with their unparalleled knowledge and fast response times.

A Leader in 2025 Gartner® Magic Quadrant™ for Network Detection and Response

Gartner, Magic Quadrant for Network Detection and Response, 29 May 2025, Thomas Lintemuth, et. al

DEFENDING THE WORLD'S **MOST SENSITIVE NETWORKS**

Learn more about Corelight
Speak to an expert: 1-888-547-9497
info@corelight.com

corelight