2021

Managed Service Platform (MSP)

OT OptICS™

The Industry's **First** AI-Driven Monitoring and Intrusion Detection System for Level 0/1 Serial-Connected Industrial Control Systems (ICS)

Cynalytica

Cynalytica

Protecting Legacy Cyber-Physical Systems

An industry first in AI-driven intrusion detection, OT OptICS combines machine learning with Cynalytica's SerialGuard AnalytICS Platform to enhance anomaly detection of serial-connected ICS. Based on Idaho National Laboratory's award-winning technology, Autonomic Intelligent Cyber Sensor (AICS), OT OptICS understands and learns serial traffic behavior to provide cyber-physical systems with unparalleled protection. Unlike other AI-driven OT cybersecurity platforms, OT OptICS autonomously monitors Level 0/1 serial communications that control industrial physical processes. This allows it to detect lower-level compromises and misconfigurations that can cause physical damage and downtime.

Automated Serial Network Monitoring and Intrusion Detection

- Reduces downtime through automated network health monitoring and surveillance
- Validates the data integrity of serial-connected Industrial Control Systems
- Enhances visibility and situational awareness of legacy cyber-physical systems
- Automates and centralizes serial data collection and analysis
- Reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to cyber threats
- Seamlessly integrates with third-party SIEMs/SOCs

OT OptICS is available as a Managed Service Platform (MSP), helping you reduce costly risk to critical systems without the costs and implementation effort of building out a sophisticated legacy infrastructure team.

OT OptICS

Managed Service Platform (MSP)

Get the Support You Need with Continuous Monitoring Services

Cynalytica offers OT OptICS as a Managed Service Platform so you can get the most from our technology with minimal effort. Whether you're looking for better ways to improve your cybersecurity posture or need a quick and easy route to implementation, OT OptICS provides you with the technology, security expertise and industry know-how to deliver cost-effective results.

OT OptICS Managed Service Platform

- 24/7 SerialGuard monitoring
- AnalytICS Engine application hosting
- AnalytICS Engine integration
- System administration
- Network engineering support
- Management, maintenance and application support
- Professional services
  - Analytics
  - Audits
  - Compliance reporting
  - Troubleshooting and diagnostics

Managed Service Platform Benefits

- Quick and easy implementation
- Reduced labor and training costs
- Rapid incident response and investigation
- Regulatory compliance
- Out-of-hours support
- Improved cybersecurity posture

Enhanced Operational Health Monitoring and Intrusion Detection

OT OptICS combines machine learning with the SerialGuard AnalytICS Platform to enhance operational health monitoring, detect network intrusions and accelerate incident response times without the need for human rulesets. This unified platform can understand network behavior changes and automatically searches for anomalies — providing operators with an intelligent intrusion detection system and scalable tool that enables remote monitoring and analysis of serial-connected inventory.

LEVEL 3

OPERATIONAL

IT SECURITY

SIEMS

AnalytICS Engine User Platform

Integrations

IT NETWORK

AIRGAP/
FIREWALL

OT OptICS

LEVEL 2

ENGINEERING/
SCADA/HMI

OT NETWORK

TCP/IP Protocol

LEVEL 1

PLC/RTU

Message ID	Size	Port	Protocol
104690	15	1	modbus_rtu
104691	12	2	modbus_rtu

SerialGuard™

Secure Data
Transfer

1010101010101010101010
1010101010101010101010101010
1010101010101010101010101010

Serial Protocol

LEVEL 0

FIELD
DEVICES

SerialGuard AnalytICS Platform

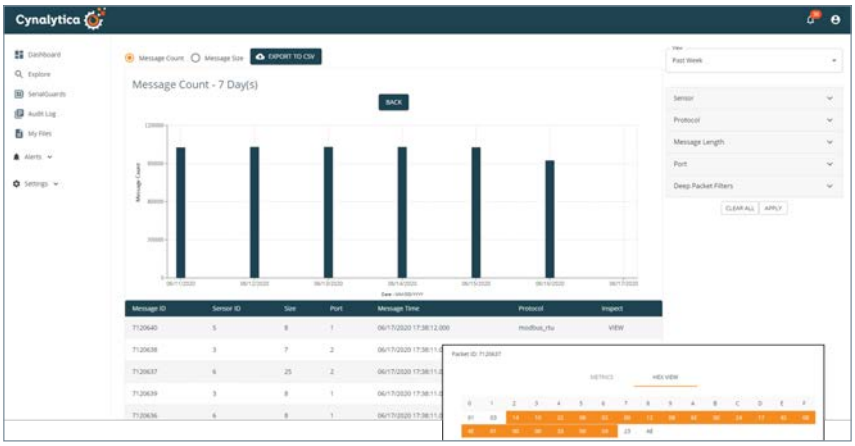
SerialGuard
Passive Serial Packet Sniffer

- Passive
- Fail-safe
- Full/half duplex serial monitoring
- RS-232/485/422 protocol monitoring
- Protocol agnostic support
- Deep packet inspection

OT OptICS uses serial data captured by our SerialGuard sensor to bring real-time intrusion detection to legacy ICS. SerialGuard is a passive hardware sensor that installs seamlessly into supervisory control and data acquisition (SCADA) and other legacy control systems. The SerialGuard sensor provides Level 0/1 security monitoring for legacy ICS that utilize insecure RS-232, RS-485 and RS-422 serial communications. The sensor sits in-line between field devices and controllers, passively capturing real-time Level 0/1 serial data. It then encapsulates the captured data into encrypted TCP data packets before securely transmitting them to our AnalytICS Engine for inspection.

AnalytICS Engine with OT OptICS

AnalytICS Engine, SerialGuard's supporting platform, operates as an Endpoint Protection (EPP), Endpoint Detection and Response (EPR), Intrusion Detection System (IDS) and data validation tool. The software securely aggregates the serial data into easy-to-read visualizations, enabling users to create a baseline for normal operations, analyze trends and create alerts on serial traffic behavior. Combined with new machine learning capabilities, this platform provides automated anomaly detection and alerts using real-time serial data.



- Automates anomaly detection
- Enables rule-based alerts
- Performs deep packet inspections
- Integrates with third-party SIEMs
- Manages SerialGuard sensors remotely
- Features easy-to-read data visualization

Our platform provides a scalable enterprise management tool that incorporates serial communications data from SerialGuard sensors to improve the visibility of serial-based network traffic in ICS. AnalytICS Engine also seamlessly integrates with third-party SIEMs to provide ICS/SCADA operators with maximum visibility across their IT/OT networks.

Cynalytica

ABOUT CYNALYTICA

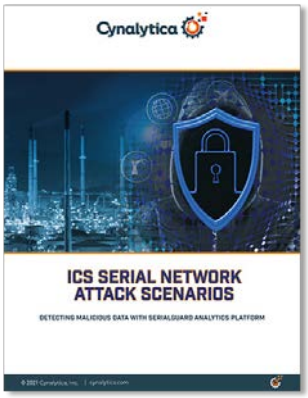
Cynalytica, Inc.® combines a diverse set of industry expertise with decades of applied research and development experience to deliver pioneering cybersecurity and machine analytics technologies that protect critical national infrastructure, securely enable Industry 4.0 and help industries accelerate their digital transformation objectives. The company employs innovative and novel techniques in machine learning, data analytics and high-performance computing, combined with manufacturing capabilities, to provide revolutionary threat detection solutions and analytics for ICS and infrastructures.

See the SerialGuard AnalytICS Platform in Action

Detecting Malicious Data and Advanced Attacks
(False Feedback Attacks & Other Malicious Data)

Serial Communications Asset and Configuration Change Management

Troubleshooting & Diagnostics



ICS Serial Network Attack Scenarios

WWW.CYNALYTICA.COM