# SerialGuard & AnalytICS Engine

Serial Communications Protection and Monitoring for Critical Industrial Control Systems

MOSAICS Industry Day Nov 04, 2020



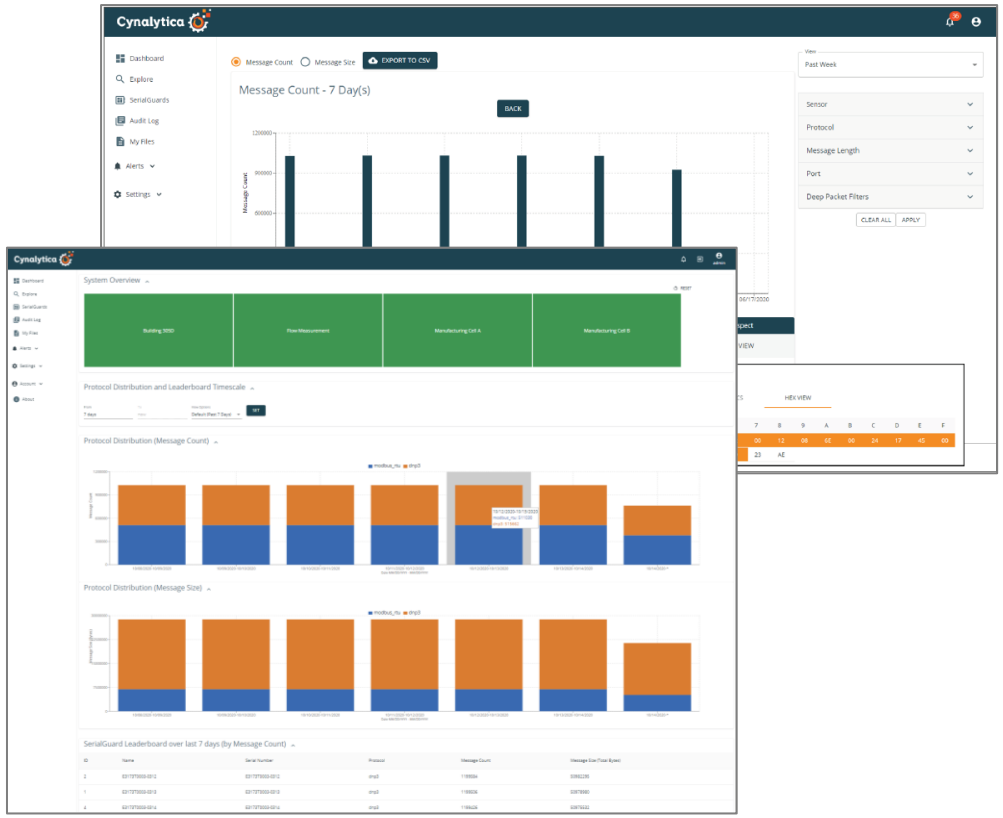
© 2020 Cynalytica, Inc.

MOSAICS 2020 INDUSTRY DAY

Cynalytica

# SerialGuard and AnalytICS Engine

## Intrusion Detection and Data Visibility for Legacy Serial Communications

MOSAICS

2020 INDUSTRY DAY

Cynalytica

# USD STP&E: Resilient Systems

The STP&E Resilient Systems (RS) Directorate focuses on policy and practice to ensure DoD systems are resilient to advanced cyber threats."

Objectives include:

a) Lead program protection planning and system security engineering policy and practices to mitigate the compromise and exploitation of advanced warfighting capabilities
b) Mitigate malicious and non-malicious activity to mission-critical hardware and software in DoD weapon systems
c) Safeguard DoD-controlled technical information from exploitation through cost-effective countermeasures

**USD STP&E Resilient Systems Directorate, 2020**

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

# Secure Visibility into Legacy ICS

1. Visibility and Data Integrity Solution for Legacy Serial Communications
   a) Passive and Fail-Safe SerialGuard encrypts captured serial traffic to AnalytICS Engine for storage and analysis
   b) Deep Packet Inspection (DPI) on various ICS protocols (Modbus RTU, DNP3, IEC-101, BACnet MS/TP)

2. Alerting of Anomalous/Malicious Serial Communications
   Reduces time to detection and response, **increasing resiliency**

3. SIEM/SCADA Integrations
   Stream DPI information, alerts, and audit information to existing SIEMs in near real-time via SYSLOG/JSON/XML and more

MOSAICS

2020 INDUSTRY DAY

Cynalytica

# Level 0/1 Intrusion Detection Enhances Resiliency

1. Passive and Fail-Safe SerialGuard
    a) Cannot use SerialGuard to write data on serial bus
    b) Serial communications remains in the event of SerialGuard power failure
    c) Protocol-Agnostic, supports any RS-232/485/422 traffic

2. AnalytICS Engine
    a) Data Analytics Platform for SerialGuard data
    b) DPI and Alerting for Industrial Automation protocols such as Modbus RTU, DNP3, IEC-101, BACnet and more

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

# Platform Integrates with MOSAICS Workflows

1. SerialGuard provides serial data capture, securely
   a) Encrypts captured traffic in transit to AnalytICS Engine
   b) No longer the need to rely on potentially falsified information from Level 1 devices (PLCs, RTUs, etc)

2. AnalytICS Engine provides data analytics and alerting for serial communications
   Identify malicious/anomalous serial network traffic in near real-time to validate SCADA datapoints.

3. Seamlessly integrate into other MOSAICS technologies via AnalytICS Engine's Integrations capaiblites
   Stream datapoints from AnalytICS Engine via SYSLOG, JSON, XML, and more

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

# TRL & Contract Paths

1. TRL 8 (SerialGuard & AnalytICS Engine)
    a) Actual system completed and qualified through test and demonstration. Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development.
2. Second Generation of SerialGuard w/AnalytICS Engine Q1 2021
    a) High-speed communication protocols
    b) Wireless Back-haul capabilities

3. Current Contract
    a) Sandia National Laboratories PO
    b) Commercial Availability

# Product Validation in Energy Environments

1. Electric Power Research Institute (EPRI)
    a) EPRI's Cyber Security Research Laboratory (CSRL) in Knoxville, Tennessee
    b) SerialGuards and AnalytICS Engine connected to various Electrical Relays and Real Time Automation Controllers (RTACs)
    c) Identified various scripted communication anomalies, cabling issues, malicious commands, and behavioral changes in CSRL environment.

2. ONE Gas
    a) Approval to operate in ONG environment (OK, KS, TX)
    b) Instrumented SerialGuard and AnalytICS Engine into ONEGas environment.

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

# Demonstration

1. Baselining and troubleshooting serial communications
2. Asset management
3. Alerting anomalous and malicious serial communications

Presenter:
Joseph Bessette
joseph@cynalytica.com
(540)-538-5191

POC Information:
www.cynalytica.com
sales@cynalytica.com

# THANK YOU

joseph@cynalytica.com



Cynalytica