Cynalytica

SerialGuard™ + AnalytICS Engine

Securely Enabling Industry 4.0 – Bringing True Visibility to Legacy Critical Infrastructure

Serial Communication's Enduring Prevalance

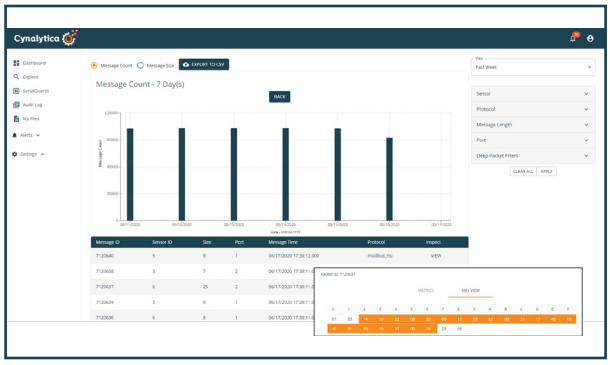
- Per Industry Estimates, 30-60% of Industrial Control Systems (ICS) communications occur over Serial.
- Current serial device monitoring is inadequate and leaves the operator dependent on unverifiable operations data.
  - A compromised logic controller can provide monitoring systems falsified communications data.
- Serial communications will remain a crucial segment of critical infrastructure for at least 10 - 20 more years.

IT/OT Convergence Expands ICS Attack Surface

- ICS owners and operators pursue Industry 4.0 operational efficiencies by connecting previously siloed OT systems to their corporate IT networks.
- Increased connectivity broadens the ICS attack surface, reducing the sophistication required to target ICS.
- Bad actors from script kiddies to nation states have stepped up targeting ICS, increasing risk of cyber-physical damage to critical infrastructure.

SerialGuard™

- Hardware device that taps serial data completely passively - cannot physically write to the serial line and does not introduce latency.
- Fail-Safe operation - if the device loses power, the ICS network will maintain normal operation.
- Installed at lowest layer of ICS - between field device and logic controller - to ensure data integrity.



AnalytICS Engine

- Remotely manages and collects encrypted serial data from SerialGuard™ on separate subnetwork.
- Stores serial data and performs deep packet inspection, creating summary metrics and visualizations for system level analysis and threat hunting.
- Alert monitoring seamlessly integrates with 3rd party SIEMs for unified IT/OT threat detection.

Creation of Value Across the Enterprise

EXECUTIVES

Risk Mitigation and Financial Savings

- Industrial health monitoring -- identify nonoptimal operation early as catalyst to preventative maintenance.
- Detection of cyber-physical attacks to avoid: asset damage, loss of life, injury and legal liability.
- Extension of Asset Useful Life -- reduce capital outlays & avoid equipment overhauls.

MANAGERS

Painless Implementation & Maintenance

- Avoid network downtime by detecting anomalous serial communications early in attack kill chain.
- Plug-and-Play hardware installation and streamlined, remote software configuration.
- Improves cybersecurity compliance posture -- brings NERC/CIP-level of network monitoring. required of IP-based networks to serial communications.

OPERATORS

Ease of Operation & Management

- Reduces time to resolve cyber-physical incidents through early detection via alert monitoring.
- Automates process of identifying misconfigurations and physical issues via user-defined rules.
- Integration with third-party SIEMs for single-pane-of-glass IT/OT Management.