Cynalytica

AnalytICS Engine

Builds a Complete Picture

NEW High Performance & Scalable Analytical Platform for Serial-Based Network Traffic in Industrial Control Systems

AnalytICS Engine, SerialGuard's supporting platform, operates as an intrusion detection system (IDS). It offers operators the ability to securely capture, baseline and analyze trends in serial communications through encrypted communications. The platform can be deployed on-premise or as a service and provides operators with an easy-to-use set of intuitive tools to monitor communications. Rulesets are flexible, ranging in complexity with the operators' needs that can flag anomalous activities on individual devices or across the network. Our platform provides a scalable enterprise management tool incorporating serial communications data from SerialGuard sensors to provide optimum visibility of serial-based network traffic in Industrial Control Systems. The platform also seamlessly integrates with third party SIEMs to provide ICS/SCADA operators maximum visibility across their IT/OT networks.

Optimizes Visibility for Informed Decision Making

AnalytICS Engine acts as SerialGuard's companion software to enhance visibility of serial-based communications in industrial control environments. The platform remotely configures and manages all deployed SerialGuard devices within the field and enables greater insights through its powerful suite of data visualization and analytic tools. Its software understands specific serial messages, performs thorough deep packet inspections, and enables operators to create rule-based anomaly alerts to help them take action at the right time.

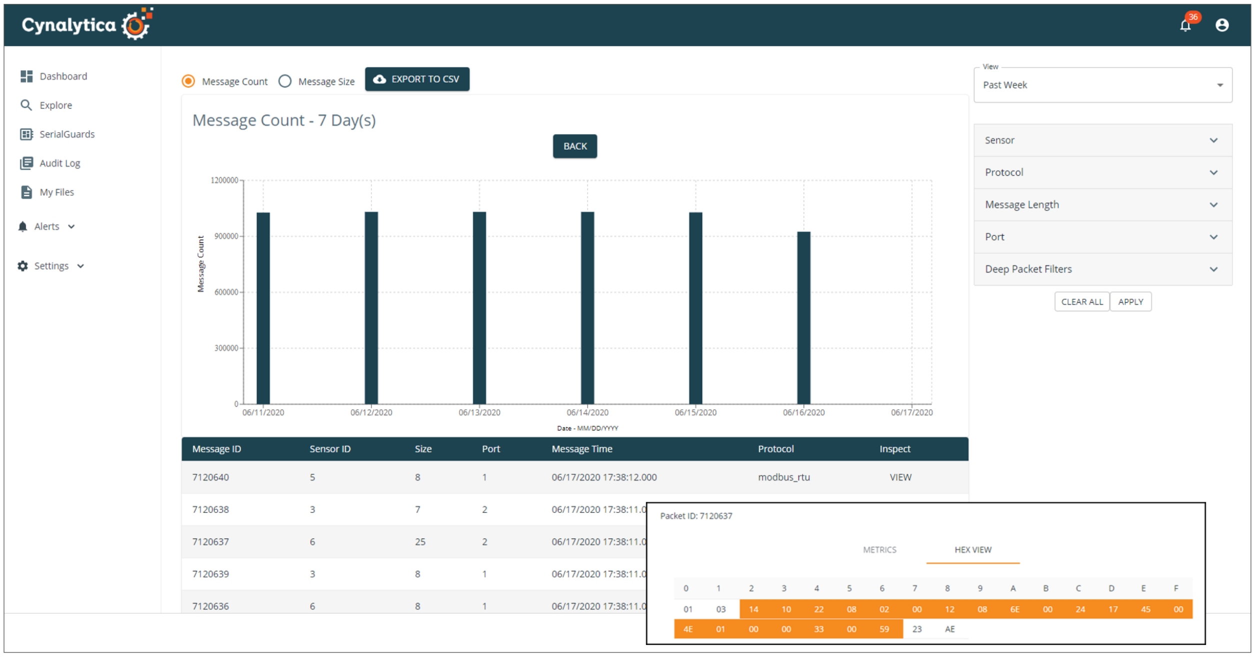
Benefits

- Anomaly alerts significantly reduces Mean Time to Detect (MTTD) cybersecurity threats.
- Increases detections of malicious activities.
- Saves Time - configures and manages SerialGuard devices from a centralized location.
- Organizes data into an easy-to-read format for efficient ICS health monitoring.
- Gives a deeper insight into serial-based ICS traffic behavior.
- Helps ICS security teams make quick, informed decisions.

Management Features

AnalytICS Engine comes with built-in properties that perform device and data management tasks including:

- Remote configuration and management of SerialGuard devices.
- Encryption and authentication with role-based access control.
- Serial traffic alert monitoring.
- Industrial system health monitoring.
- Asset and cluster management.
- Data historian and audit trails.
- Protocol Agnostic Support.
- Integration with commercial SIEMs.
- Native support for Syslog and JSON.
- Data Export to CSV.
- Large data storage.



● Message Count ○ Message Size

View: Past Week

Message Count - 7 Day(s)

Message ID	Sensor ID	Size	Port	Message Time	Protocol	Inspect
7120640	5	8	1	06/17/2020 17:38:12.000	modbus_rtu	VIEW
7120638	3	7	2	06/17/2020 17:38:11.0		
7120637	6	25	2	06/17/2020 17:38:11.0		
7120639	3	8	1	06/17/2020 17:38:11.0		
7120636	6	8	1	06/17/2020 17:38:11.0		

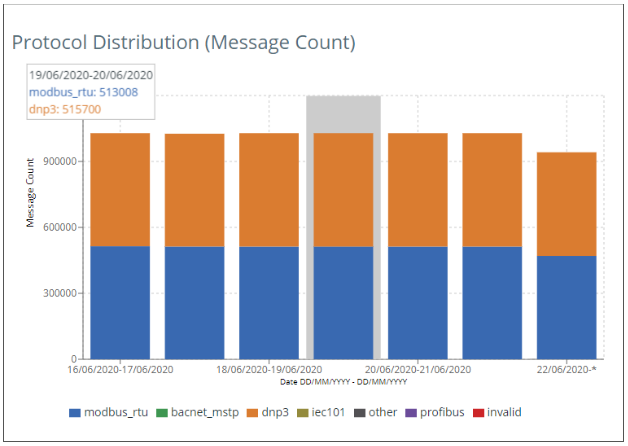
Packet ID: 7120637

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01	03	14	10	22	08	02	00	12	08	6E	00	24	17	45	00
4E	01	00	00	33	00	59	23	AE							

Powerful Data Visualization & Analytical Tools

The platform's powerful suite of data visualization and analytic tools help users understand the serial data sets and identify patterns with ease. Built-in capabilities include:

- ✓ **Visualization and statistical characterization of key serial traffic parameters, such as:**
  - Protocol Density
  - Protocol Distribution
  - Message Size
  - Message Count
- ✓ **Deep Packet Inspection of serial communications**
- ✓ **Rule-based anomaly detection**



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 help 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 industrial control systems and infrastructures.