Stellar Cyber OT Protocols

Stellar Cyber Open XDR Platform supports your IT and OT environments, enabling security teams to deliver consistent security outcomes across your organization. Stellar Cyber's network-based Security Sensors natively understand the following protocols. Stellar Cyber's DPI understands many other protocols beyond the following SCADA reference.

Protocol	Description
AAON PRISM 2	AAON Prism 2 is a software for control of AAON HVAC, Wattmaster Commlink 5 module over IP.
B&R Automation	B&R Industrial Automation is a manufacturer for the industry. This plugin classifies a plastic molding machinery.
BACnet Application Layer	BACnet is a communication protocol for Building Automation and Control (BAC) networks defined by the standard ISO 16484-5. The BACnet stack defines different layers, and the BACnet Application Layer (bacnet_app) manages access to objects exposed by BACnet devices and operations done on them.
BACnet Network Layer	BACnet is a communication protocol for Building Automation and Control (BAC) networks defined by the standard ISO 16484-5. The BACnet stack defines different layers, the BACnet Network Layer (bacnet_net) contains the network addresses required for routing BACnet messages to BACnet devices.
BACnet Virtual Link Control	BACnet is a communication protocol for Building Automation and Control (BAC) networks defined by the standard ISO 16484-5. The BACnet stack defines different layers, the BACnet Virtual Link Control layer (bacnet_vlc) is used by BACnet devices over IP networks. It formalizes all the services that a BACnet device might require from the link layer but are not readily available from the underlying IP layer.
Bosch Security Conettix	Bosch Conettix is a security alarm product line. This plugin classifies the D6600 when no encryption is configured.
Codesys Protocol (IDE-PLC)	Codesys is an embedded system, and IDE for industrial Programmable Logic Controller (PLC). This plugin classifies the protocol between the IDE and the PLC.
The Common Industrial Protocol	The Common Industrial Protocol (CIP) is an industrial protocol for industrial automation applications.
CSP AB/Ethernet	Proprietary protocol developed by Allen-Bradley, used on programmable logical controllers (PLC).
DeltaV	Traffic is related to DeltaV, a distributed control system used in industrial process control (Emerson Process Management).
Distributed Network Protocol	DNP3 (Distributed Network Protocol) is a set of protocols between components in process automation systems (SCADA).

Protocol	Description
DLMS/COSEM over IP	DLMS/COSEM is a standardized protocol for energy and water smart meters. This plugin classifies DLMS above the UDP or wrapper_dlms (WPDU).
DLMS/COSEM over IP wrapper	TCP/UDP wrapper protocol (WPDU) for transporting over IP the DLMS/COSEM (IEC-62056) protocol for energy and water smart meters.
Dr. Schenk Inspection System	Dr. Schenk Inspection System is a product that inspects and analyzes raw material from a factory production chain. It gathers sensors, actuators, and visualization components all interacting with the Inspection System.
EquipCommand	This layer classifies the EquipCommand protocol from TotalTrax equipment (SX/VX series). It solely handles the non-ciphered part of this protocol.
ESK M3	This plugin classifies the control protocol between the ESK M3 Access Control module for forklifts and the P106 software that manages them.
Ethernet/IP	ENIP (EtherNet/IP) is an industrial network protocol that adapts the Common Industrial Protocol to standard Ethernet.
Experion product	This plugin classifies Experion Control Builder for Server LX.
Fanuc gen	This layer gathers signatures of protocols used by Fanuc equipment. This layer does not cover ALL protocols generated by Fanuc equipment.
General Electric Proficy	Proficy is a General Electric product for industrial environments, allowing monitoring and data management from the SCADA network. This plugin classifies traffic related to the Proficy Gateway service (PR Gateway) and Proficy Licensing server (PR Licensing).
Generic Object Oriented Substation Events	GOOSE (Generic Object Oriented Substation Events) is a controlled model mechanism in which any format of data (status, value) is grouped into a data set and transmitted within 4 milliseconds.
High-Availability Seamless Redundancy	High-Availability Seamless Redundancy provides redundancy for industrial Ethernet networks. This header is used for packet duplication removal. The ixEngine does not run the duplication removal algorithm.
High-Level Data Link Control	High-Level Data Link Control (HDLC) is a data link layer protocol standardized by ISO/IEC 13239:2002. This plugin classifies Frame Type 3 when transported over TCP/IP.
Honeywell Process History Database	Traffic related to Honeywell Process History Database (PHD).
HSR/PRP supervision frame	High-availability seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) provide redundancy for industrial Ethernet networks. This plugin classifies supervision frames.
IEC 60870-5-104	IEC 60870-5-104 protocol (aka IEC 104) is a part of IEC Telecontrol Equipment and Systems Standard IEC 60870-5 that provides a communication profile for sending essential telecontrol messages between two systems in electrical engineering and power system automation.
IEC 61850 Sampled Values	IEC 61850 Sampled Measured Values (SMV or SV) is a protocol used in Electrical substations to share data between Intelligent Electronic Devices (IED) under hard real-time constraints (IEC 61850-9-2).

Protocol	Description
IEEE C37.118 Synchrophasor	IEEE C37.118 Synchrophasor Protocol conveys electrical current measurements in power grid substations.
Inter-Control Center Communications Protocol	IEC 60870-6/TASE.2. Inter-Control Center Communications Protocol (ICCP) provides data exchange over Wide Area Networks (WANs) between utility control centers, utilities, power pools, regional control centers, and Non-Utility Generators.
Intermec SmartSystem Foundation	Intermec (Honeywell subsidiary) SmartSystem is a barcode scanner fleet management software.
Invar Systems AS/RS Control	Invar Systems AS/RS (Automated Storage and Retrieval System) control protocol is part of Invar's integrated warehouse software system (IWS).
iWarehouse	iWarehouse is the fleet and warehouse management system of Raymond Corporation (a subsidiary of Toyota Industries that manufactures and distributes electric lift trucks). This plugin classifies the protocol of the on-board device, named Monitor.
KEYENCE Barcode Reader	This plugin classifies the control protocol of KEYENCE Barcode Reader products, also used by their setup software (AutoID Network Navigator).
Lenel OnGuard client	OnGuard is a product from Lenel for managing the physical security of buildings. This plugin classifies the connection from the client software to the server.
Manufacturing Message Specification (ISO 9506)	ISO 9506 Manufacturing Message Specification (MMS).
Mercury Security	This plugin classifies Mercury Security controller's communication protocol with TLS disabled. Mercury security controllers manage physical access control (doors and card readers) to buildings.
Mettler Toledo Standard Interface Command Set	Standard Interface Command Set (SICS) is a protocol to control Mettler Toledo industrial scales.
Modbus	Modbus is a standard communication protocol in the industry for connecting industrial electronic devices (SCADA). Here, we consider Modbus as the combination of Modbus/TCP (Transport layer for TCP/IP networks) and Modbus (serial communication protocol).
Modbus Remote Terminal Unit	Traffic related to Modbus Remote Terminal Unit (RTU), a distributed control system used in industrial process control. The Modbus RTU communications can be sent to the network using a basic RS485 to TCP adapter.
Moxa Async Server Proprietary Protocol (ASPP)	This plugin classifies ASPP (Async Server Proprietary Protocol) from Moxa (NPort devices) without activation of encryption.
Omron FINS protocol	Omron FINS Protocol is a SCADA protocol to communicate with PLC.
OPC Unified Architecture	OPC is the interoperability standard for secure and reliable data exchange in the industrial automation space and in other industries. This plug-in classifies the OPC Unified Architecture (UA) binary protocol over TCP.
Parallel Redundancy Protocol	Parallel Redundancy Protocol provides redundancy for industrial Ethernet networks. This plugin detects the Redundancy Control Trailer (RCT) to Ethernet frames. The ixEngine does not run the duplication removal algorithm.

Protocol	Description
PC-cubed	PCCC is a Programmable Controller Communication Commands, which is used to control software running in Programmable Logic Controller (PLC). PCCC traffic can be hardware-specific. This plugin addresses traffic generated by Rockwell/Allen-Bradley to talk to SLC5, PLC5E, and MicroLogix PLC for service.
PI AF	OSI PI Analysis Framework SCADA protocol (AF Server, MDB Sync, etc.).
PI Data Archive	OSI PI DataArchive and Server SCADA protocol (ProcessBook, Datalink, etc.).
Process Field Net	PROFINET (an acronym for Process Field Net) is an industry technical standard for data communication over Industrial Ethernet, designed for controlling and collecting data from equipment in industrial systems, with particular strength in delivering data under tight time constraints (1ms or less). The standard is maintained and supported by Profibus & Profinet International, an umbrella organization headquartered in Karlsruhe, Germany.
Rockwell RNA protocol	Rockwell Network Applications (RNA) is a Rockwell implementation of Windows DNA-M and is used for communication between Rockwell FactoryTalk products.
s7 Communication	S7comm (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7-300/400 family. It is used for PLC programming, exchanging data between PLCs, accessing PLC data from SCADA (supervisory control and data acquisition) systems, and diagnostic purposes.
S7 Communication Plus	S7communication Plus is a Siemens proprietary protocol for Siemens' Programmable Logic Controllers (PLC).
Schneider Integrated Object Network	Integrated Object Network (ION) is a proprietary SCADA protocol for Schneider Electrics smart meters.
Seamless Message Protocol	Seamless Message Protocol (SLMP) is for the control of Mitsubishi PLC devices.
Siemens Apogee	This plugin classifies the primary data protocol used by the Siemens Apogee HVAC product line. This device also uses BACnet and other control protocols that are not covered here.
Socomec	Socomec is a manufacturer of industrial power networks. This plugin classifies the monitoring socket of the Silverlight user interface for the PassIP+ gateway to the proprietary ISOM bus. It is used for insulation fault detection.
Toyo PLC protocol	This layer classifies only a limited number of protocols known to be used by Toyo hardware (PLC).
Vnet/IP	Yokogawa's control communication network is approved by international standards (IEC 61784-2 Ed.2.0).
Yokogowa protocol	This layer classifies only a limited number of protocols known to be used by Yokogawa hardware

Learn more about how Stellar Cyber can meet your OT security needs at www.stellarcyber.ai/ot-security/