

Industrial Control System and IT Protocols Support

As of July 2019

Industrial Control System Expertise

Claroty's interdisciplinary team of analysts and researchers are domain experts who continuously track ICS-specific zero-days, global campaigns, and adversaries as well as reverse-engineer malware. Leveraging deep understanding of cybersecurity, OT-specific protocols and industrial control systems – our solutions deliver immediate value by protecting your plants, processes and operations from cyber threats.

Multispectral Data Collection

Leveraging multispectral data collection methods, we provide 100% visibility into OT assets and network communications.

Claroty safely extracts fine-grained details about the assets, communications and the actual OT conversations for both serial and IP-based networks – all the way down to the I/O level. This extreme visibility is achieved using a combination of the data collection capabilities including:

Passive – Continuous, real-time monitoring of OT networks

ABB Bailey • ABB DMS system • ABB HC800 (Infininet) • ABB Spirit • ABB Symphony Plus • Alstom E-Terra • Alstom Alspa • Altus ALnet • BACNET • Beckhoff AMS • B&R INA2000 • NetBIOS Browser (UDP 138) • CAPWAP • CC Link IE - Field • Cisco Discovery Protocol (CDP) • Citect HMI • Cognex Discovery • Control Technologies Inc. (CTI) • Control NS Link • CPHA (Checkpoint High Availability) • Digi4 • Digi5 • Microsoft DCE RPC • Microsoft DCE RPC - ABB DCS Service Manager • Emerson DeltaV • Telnet - DeltaV • DACP • DHCP • DNP3 • Emerson Ovation • Emerson ROC Plus • ETHERNET/IP • Foxboro RTV • Foundation Fieldbus (FF) • Foxboro LLC • FTP – SEL • Siemens FWL LOAD (firmware upload) • GE-ALM • GE Bentley Nevada (BNC3500) • GE-EGD • GE-EGD-CMP • GE PAC8000 (AXE) • GE QuickPanel (TRAPI+HTTP) • GE SDI (MarkVie) • GE SDI Classic (MarkVie) • GE SRTP • Goose (IEC-61850) • HART-IP • HiDiscovery – Hirschmann LLC • Honeywell C200 – Ftebcip • Honeywell Experion - CeeNTComm (C300, EHPM) • Honeywell EpicMo (C300 management) • Honeywell Firewall CF9 • Hot Standby Router Protocol (HSRP) • HTTP • HTTP-XML (specific schemes) • IEC101 • IEC103 • IEC104 • Keyence Host-Link Communication • Keyence KV Studio • Keyence Logger • Kongsberg • Knapp • Lantronix Serial GW • Linux High Availability • LLDP • Microsoft NTLMSSP (Auth protocol) • Microsoft SAMR • Microsoft CIFS (SMB) • Mitsubishi Melsec • Mitsubishi Melsec • MNDP • MMS • Modbus • Modbus ScadaPack • Modbus Modsoft • Modbus Concept • Modbus Eltec • Modbus Execlod • Modbus GE Enervista • Modbus Schneider • Motorola MDLC • NetBios Datagram Service • NetManage • Niagara Tridium (BMS) • Omniflow Flow computer • Omron FINS • OPTO MMP • OSISoft PI • Siemens P2 • PCCC • Portwell • POP3 • ProConoS (TCP 20547) • Profinet DCP • Profinet I/O • Profinet Real-Time • Microsoft RDP • MQTT • Radius • RTCP • RCDP • Redlion Crimson • Rockwell CIP • Rockwell PCCC • Rockwell ENIP • S7Comm Plus • S7Comm Plus • SIP • Skinny • SLMP (CC Link IE Field Basic) • SNMP • SSH • Synchrophasor • Telnet- DeltaV • Telnet- Moxa • Telnet- Omniflow • Telnet- Hirschmann • Telnet- SEL • TFTP • ABB Totalflow • Triconex Tristation • Triconex TSAA • WonderWare Suitelink IOTalk • Yokogawa VNET (VHF) • Yokogawa odeg

Active – Precise, periodic queries of OT assets

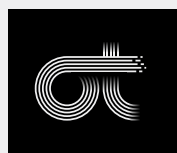
BACnet • Beckhoff • B&R Query/Profile • Cisco Profile • CIP • DNP3 • ENIP Query/Scan • Hirschman Discovery Query/Scan • Hirschman Profile • HTTP Query • IoT Query • Modbus Information Object • MS Net Bios • Net Bios • Profinet – DCP Query/Scan • Ping Sweep • Rockwell Profile • Schneider Unity Query • Siemens Profile • Siprotec 5 • S7comm • SNMP Query/Scan • SNMP Siprotec 5 • Telnet • TCP Port Scan • Windows Profile • WMI • WSD Query/Discovery

App DB – Targeted periodic enrichment of OT asset data

ABB – AC800M • B&RY • Emerson DeltaV • GE Proficy Machine Edition • GE PacsAnalyzer • GE Mark VI • Honeywell – Experion • Honeywell – EHPM • Rockwell – MicroLogix • Rockwell RSLogix 500 /5000 • Rockwell RS System Ferret • Rockwell – Advance • Rockwell – ICSTriplex • Schneider – Modicon, Quantum, Concept, M221, Twido, TSX Micro/Premium • Schneider Triconex – Tristation • Siemens – Step7 • Siemens – Digi4/Digi5 • Siemens – S7 • Yokogawa – CentumVP/CS3000 • Yokogawa – ProsaferS

Broad Support for Industrial Control Systems and ICS / IT Protocols

Claroty has made a multi-million-dollar investment into the most extensive ICS lab in the industry – ensuring your systems continue to have the best protection available now and in the long haul.



Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. The Claroty Platform is an integrated set of cyber security products that provides extreme visibility, unmatched cyber threat detection, secure remote access, and risk assessments for industrial control networks (ICS/OT).

www.claroty.com

contact@claroty.com



CLAROTY

Copyright © 2019 ClarotyLtd. All rights reserved