ICSForge

OT/ICS Security Coverage Validation Platform

ICSForge™ is an open-source OT/ICS Security Coverage Validation Platform.

It aims to solve a real problem “How do I safely validate OT security countermeasures from functionality, visibility and detection coverage perspective by using industrial-looking traffic?”

The goal is simple: make it easier to answer “Are we actually seeing, detecting, and controlling what we think we are?”

ICSForge™ is an open-source OT/ICS Security Coverage Validation Platform.

OT defenders have no practical way to validate whether their sensors, firewalls, and segmentation controls actually detect and/or protect against real ICS attack techniques.

ICSForge lets them prove it -not claim it, prove it- with a sender/receiver correlation loop across 10 protocols and 68 ATT&CK for ICS techniques with 500+ different scenarios.

Motivation and Problem Statement

If we take a look to the recent Dragos 2026 Year in Review report (https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review);
Based on previous incidents that have been studied on that report:
- 81% of reports showed poor IT/OT segmentation, 53% had exposed internet-facing assets.
- 46% of architecture reviews and 88% of tabletops showed deficient detection.

Modern OT environments increasingly deploy security controls such as:
- OT-aware firewalls and segmentation gateways
- Network Security Monitoring (NSM) sensors
- IDS/NDR platforms
- SIEM pipelines consuming OT telemetry

Despite this investment, many organizations cannot confidently answer basic operational questions:
- What OT/ICS traffic is actually visible to our sensors?
- Are detection rules triggering when they should?
- Are segmentation and firewall policies enforced as designed?
- Can SOC analysts distinguish expected OT behavior from suspicious or policy-violating activity?

ICSForge was created to address this gap by enabling repeatable, protocol-aware validation of OT network visibility and detection coverage using controlled, inspectable traffic generation.

Detailed project outline is here: https://www.icsforge.nl

Source code can be found here: https://github.com/ICSForge/ICSForge

ICSForge Demo Lab (Flying IT/OT Lab)

ICSForge Demo Lab is a cabin-size mobile IT/OT lab and it has three zones:
IT Zone, DMZ and OT Zone.

IT distribution switch and ICSForge Sender (with display) are in IT Zone.
IT/OT firewall is separating IT and OT zone, and network security monitoring sensor is in DMZ.
SCADA server, touchscreen HMI, CO_2 Tank, OT distribution switch and ICSForge Receiver (with display) are in OT Zone.

ICSFORGE PROJECT DETAILS

ICSForge™

OT/ICS Cybersecurity Coverage Validation Platform

ICSForge™ is an open-source **OT/ICS security coverage validation platform** designed to help defenders, SOC teams, and OT security engineers validate detection, visibility, and readiness against real-world industrial attack techniques.

ICSForge focuses on what can actually be observed on the network and generates realistic OT traffic and PCAPs in **10 industrial protocols (Modbus/TCP, DNP3, S7comm, IEC-104, OPC UA, EtherNet/IP, BACnet/IP, MQTT, IEC 61850 GOOSE, PROFINET DCP)** which are aligned with **68 of 83 unique techniques in MITRE ATT&CK for ICS v18 (82% coverage)** — without exploiting real systems or causing unsafe process impact — to help asset owners and defenders assess the quality of existing security countermeasures such as firewalls, OT NSM sensors and ACLs and identify hidden gaps.

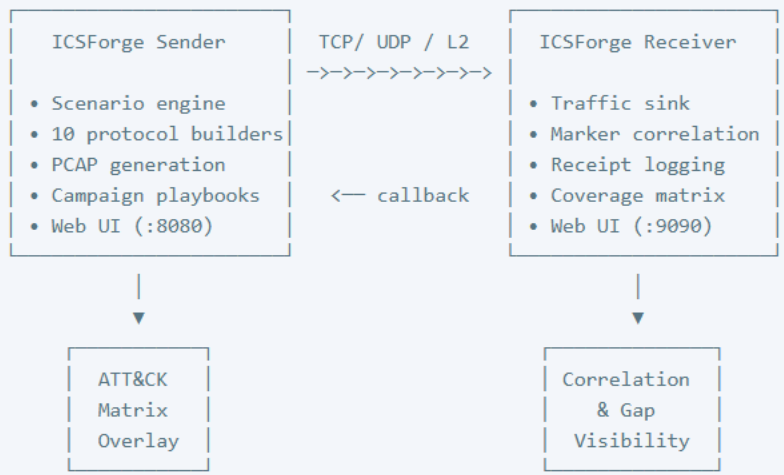
ICSForge is developed with a **defender-first** and **safe-by-design** approach around a **Sender-Receiver architecture** and interacting with the designated sender and receiver, without the need of touching other OT devices. By default, live traffic sends are restricted to RFC 1918 / loopback addresses, and PCAP replay is restricted to private ranges unless explicitly unlocked via Tools → Send Policy.

> Most ICS security tools promise coverage - ICSForge lets you **prove it**.

Key Numbers (v0.61.0)

Metric	Value
Protocols	10 industrial protocols (Modbus/TCP, DNP3, S7comm, IEC-104, OPC UA, EtherNet/IP, BACnet/IP, MQTT, IEC 61850 GOOSE, PROFINET DCP)
Runnable Scenarios	536 standalone + 11 named attack chains = 547 total
ATT&CK for ICS Techniques Implemented	68 unique technique IDs in scenario steps
ATT&CK for ICS Matrix	83 unique technique IDs (94 total entries — 11 appear under multiple tactics)
ATT&CK for ICS Matrix Coverage	82% (68 out of 83 technique) — 35 of 68 techniques at 10/10 protocols
Detection Rules	Auto-generated Suricata + Sigma rules per scenario

Architecture



Quick Start

Install

```
git clone https://github.com/ICSforge/ICSforge.git
cd ICSforge
python3 -m venv .venv
source .venv/bin/activate
python -m pip install --upgrade pip
pip install -e .
chmod +x icsforge.sh
```

Web UI

```
sudo ./icsforge.sh web                                  # Sender dashboard on :8080
sudo ./icsforge.sh receiver                             # Receiver dashboard on :9090
sudo ./icsforge.sh receiver --l2-iface eth0 # Receiver with Profinet Listener
```

> **Token:** Generated automatically on first sender setup and shown in the setup UI. Copy it to the receiver launch command. Required for receipt integrity.

Or with Docker

```
docker compose up
# Sender UI:   http://localhost:8080
# Receiver UI: http://localhost:9090
```

Protocol Coverage

Protocol	Port	Styles	Techniques (of 68)
OPC UA	TCP/4840	30	59/68
DNP3	TCP/20000	22	57/68
S7comm (Siemens)	TCP/102	36	56/68
EtherNet/IP (Allen-Bradley)	TCP/44818	24	55/68
Modbus/TCP	TCP/502	29	54/68
BACnet/IP	UDP/47808	16	54/68
MQTT	TCP/1883	17	52/68
IEC-104	TCP/2404	20	51/68
PROFINET DCP	L2/EtherType 0x8892	8	44/68
IEC 61850 GOOSE	L2/EtherType 0x88B8	5	42/68

IEC 61850 GOOSE and **PROFINET DCP** are Layer 2 protocols — they require a raw socket interface (`--l2-iface eth0`) for live sends. PCAP and offline generation work without a network interface.

Techniques at Full Coverage (10/10 protocols)

T0800, T0801, T0802, T0803, T0804, T0806, T0811, T0813, T0814, T0815, T0819, T0821, T0822, T0826, T0827, T0828, T0829, T0830, T0831, T0832, T0835, T0836, T0840, T0843, T0846, T0848, T0855, T0856, T0858, T0859, T0861, T0866, T0868, T0869, T0877, T0881, T0882, T0885, T0886, T0888, T0889, T0891 — **35 techniques** fully covered across all 10 protocols.

Scenarios

Scenarios are defined in `icsforge/scenarios/scenarios.yml`.

Naming convention: `T08XX__<description>__<protocol>[_variant]`

Types:

Type	Count	Description
Standalone scenarios	536	Single-technique, single-protocol runs
Named attack chains	11	Multi-step sequences modelling real campaigns

Named attack chains include:

- **Industroyer2** — Ukraine 2022 power grid attack (IEC-104 + S7comm)
- **SIS Targeting (TRITON-inspired)** — Safety system targeting (SIS), Modbus + S7comm surrogate
- **Stuxnet-style** — Siemens PLC programme manipulation
- **Water Treatment** — Oldsmar-style setpoint tampering (Modbus + IEC-104)
- **OPC UA Espionage** — Silent data exfiltration via OPC UA sessions
- **EtherNet/IP Manufacturing** — Allen-Bradley CIP manipulation
- **AitM + Sensor Spoof** — Adversary-in-the-Middle combined with DNP3 measurement injection
- **Firmware Persistence** — S7comm firmware implant and persistence
- **Full ICS Kill Chain** — Recon to impact (S7comm + Modbus)
- **Loss of Availability** — Multi-protocol concurrent DoS (DNP3 + IEC-104 + Modbus)
- **Default Creds → Impact** — Lateral pivot to programme modification

---

What Techniques Are Covered

ICSForge implements 68 of 83 ATT&CK for ICS techniques at the network-observable level. The remaining 15 are correctly classified as host-only, require physical access, or generate no network-observable packets — they are documented in `icsforge/data/technique_support.json` with explicit rationale per technique, and also exposed via `/api/technique_support`.

ATT&CK matrix counts explained:

- 83 unique technique IDs in the matrix
- 94 total matrix entries — 11 techniques appear under multiple tactics (e.g. T0856 Spoof Reporting Message appears under both Evasion and Impair Process Control, which is correct ATT&CK for ICS design)
- The `/api/matrix_status` response includes a `matrix_info` block that makes this distinction explicit

SENDER WEB UI

OT/ICS CYBERSECURITY COVERAGE VALIDATION PLATFORM
ATT&CK FOR ICS · EXECUTED → DELIVERED → DETECTED

OPEN SENDER →

ATT&CK MATRIX

ICSForge helps you to validate cybersecurity detection coverage across OT/ICS environments by generating realistic industrial network traffic aligned to ATT&CK for ICS v18. Fire live packets or generate PCAPs — then prove **Executed → Delivered → Detected** coverage across your OT environment.

Safe by design: destination validation, cooperative receiver, no destructive payloads.

536	68	10	4
SCENARIOS	TECHNIQUES	PROTOCOLS	INDUSTRY PROFILES

QUICK START

1. Start a receiver on a safe destination IP in your OT environment (or use loopback for a local demo).
2. Open Sender → pick a scenario or attack chain → set receiver destination → Run Live.
3. Use Campaign Playbooks to sequence multi-scenario attacks with dwell timers as a single run_id.
4. Open the ATT&CK Matrix to browse coverage — click any runnable tile to fire traffic and overlay results. Export a Coverage Report when done.

SCENARIO PACK

scenarios
547 scenarios · 10 protocols · 68 techniques

`bacnet` `dnp3` `enip` `iec104` `iec61850` `modbus` `mqtt` `opcua` `profinet_dcp` `s7comm`

TOP TECHNIQUES BY COVERAGE

ID	TECHNIQUE	PROTOCOLS	SCENARIOS
T0855	Unauthorized Command Message	10/10	38
T0889	Modify Program	10/10	38
T0848	Rogue Master	10/10	35
T0831	Manipulation of Control	10/10	31
T0888	Remote System Information Discovery	10/10	29
T0861	Point & Tag Identification	10/10	29

BROWSE SCENARIOS

Filter by ID, technique, or keyword…

SCENARIO ID	TITLE
CHAIN__aitm_sensor_spoof__opcua_dnp3	CHAIN – AitM + Sensor Spoofing via OPC UA + DNP3 (T0830+T0856+T0832)
CHAIN__default_creds_to_ics_impact__multi	CHAIN – Default Creds → Lateral Pivot → Program Modification → Impact
CHAIN__enip_manufacturing_attack	CHAIN – EtherNet/IP manufacturing line attack

OT/ICS CYBERSECURITY COVERAGE VALIDATION PLATFORM

ATT&CK FOR ICS · EXECUTED → DELIVERED → DETECTED

OPEN SENDER →

ATT&CK MATRIX

ICSForge helps you to validate cybersecurity detection coverage across OT/ICS environments by generating realistic industrial network traffic aligned to ATT&CK for ICS v18. Fire live packets or generate PCAPs — then prove **Executed → Delivered → Detected** coverage across your OT environment.

Safe by design: destination validation, cooperative receiver, no destructive payloads.

536	68	10	4
SCENARIOS	TECHNIQUES	PROTOCOLS	INDUSTRY PROFILES

QUICK START

1. Start a receiver on a safe destination IP in your OT environment (or use loopback for a local demo).
2. Open Sender → pick a scenario or attack chain → set receiver destination → Run Live.
3. Use Campaign Playbooks to sequence multi-scenario attacks with dwell timers as a single run_id.
4. Open the ATT&CK Matrix to browse coverage — click any runnable tile to fire traffic and overlay results. Export a Coverage Report when done.

SCENARIO PACK

scenarios
547 scenarios · 10 protocols · 68 techniques

`bacnet` `dnp3` `enip` `iec104` `iec61850` `modbus` `mqtt` `opcua` `profinet_dcp` `s7comm`

TOP TECHNIQUES BY COVERAGE

ID	TECHNIQUE	PROTOCOLS	SCENARIOS
T0855	Unauthorized Command Message	10/10	38
T0889	Modify Program	10/10	38
T0848	Rogue Master	10/10	35
T0831	Manipulation of Control	10/10	31
T0888	Remote System Information Discovery	10/10	29
T0861	Point & Tag Identification	10/10	29

BROWSE SCENARIOS

Filter by ID, technique, or keyword…

SCENARIO ID	TITLE
CHAIN__aitm_sensor_spoof__opcua_dnp3	CHAIN – AitM + Sensor Spoofing via OPC UA + DNP3 (T0830+T0856+T0832)
CHAIN__default_creds_to_ics_impact__multi	CHAIN – Default Creds → Lateral Pivot → Program Modification → Impact
CHAIN__enip_manufacturing_attack	CHAIN – EtherNet/IP manufacturing line attack

NETWORK SETTINGS

SENDER IP (SRC)	RECEIVER IP (DST)	RECEIVER PORT	SENDER CALLBACK URL (OPTIONAL OVERRIDE)	CALLBACK TOKEN (OPTIONAL)
127.0.0.1	192.168.213.128	9090	http://sender-ip:8080/api/receiver/callback	NZ-550EXrQLLNMc1vMuUF9j7

PULL MODE SENDER-INITIATES | SAVE & CONNECT | Receiver: 192.168.213.128

ATTACK CHAINS — ONE-CLICK NAMED SCENARIOS

EtherNet/IP MFG
Allen-Bradley · CIP manipulation
T0836 T0848 T0868 T0881

OPC UA Espionage
Silent exfil via OPC UA sessions
T0801 T0822 T0861 T0879

Industroyer2
Ukraine 2022 · IEC-104 + S7comm
T0813 T0815 T0848 T0855

Stuxnet-style
Siemens PLC · Program manipulation
T0848 T0843 T0845 T0858

SIS Targeting (TRITON-inspired)
Modbus+S7comm surrogate · SIS disable pattern
T0829 T0832 T0882 T0880

Water Treatment
Oldsmar-style · Setpoint tampering
T0806 T0829 T0831 T0861

MULTI-PROTOCOL CHAINS

CHAIN - AitM + Sensor Spoofing via OPC UA + DNP3 (T0830+T0856+T0832)
dnp3 · opcua
T0830 T0832 T0856 T0882

CHAIN - Default Creds → Lateral Pivot → Program Modification → Impact
enip · iec104 · modbus · opcua · s7comm
T0812 T0831 T0855 T0806

CHAIN - Firmware Persistence via S7comm (T0889+T0839+T0857+T
s7comm
T0839 T0857 T0858 T0888

CHAIN - Full ICS Kill Chain — Recon to Impact (S7comm-centric)
modbus · s7comm
T0812 T0813 T0835 T0838

CHAIN - Loss of Availability — Multi-protocol concurrent DoS (T0826+T0814+T0813)
dnp3 · iec104 · modbus · s7comm
T0813 T0814 T0826

SCENARIO

INDUSTRY PROFILE: All sectors

SEARCH: Filter by name, technique ID, or protocol…

LATERAL MOVEMENT

- T0812 – Default Credentials — Modbus FC43 device…
- T0812 – MQTT anonymous broker access
- T0812 – Default Credentials — OPC UA anonymous/d…
- T0812 – Default Credentials — S7comm blank/defau…
- T0843 – BACnet/IP AtomicWriteFile program upload

Sends Modbus FC43 Read Device Identification then follows with FC16 writes using the default unit ID, probing for open write access characteristic of default-configured PLC field devices.

LIVE PAYLOAD PREVIEW

Actual PDU bytes from the real protocol builder — what hits the wire.

← PREV | Step 1 / 2 | NEXT →

modbus | style: default_creds_probe | TCP :502 | 65 bytes | T0812

```
0000  45 39 00 00 00 3b 1b 2b 0e 01 00 49 43 53 46 4f   E9...;.+...ICSFO
0010  52 47 45 3a 49 43 53 46 4f 52 47 45 3a 50 52 45   RGE:ICSFORGE:PRE
0020  56 49 45 57 3a 54 30 38 31 32 5f 5f 64 65 66 61   VIEW:T0812__defa
0030  75 6c 74 5f 63 72 65 64 73 3a 54 30 38 31 32 3a   ult_creds:T0812:
0040  3a                                                :
```

SCENARIO SUMMARY

2 steps · 8 total packets modbus

Scenario fired
T0812__default_creds__modbus_device_id · 8 packets

T0891 – Hardcoded Credentials — BACnet unauthent…
T0891 – Hardcoded Credentials — DNP3 authenticat…
T0891 – Hardcoded Credentials — EtherNet/IP defa…
T0891 – Hardcoded Credentials — IEC-104 no authe…
T0891 – Hardcoded Credentials — IEC 61850 GOOSE

Uses the hardcoded default credential (empty password) in Allen-Bradley PLCs and I/O modules to establish a CIP session. Many ControlLogix and MicroLogix devices ship with authentication disabled or with a blank password. The attacker uses this hardcoded credential to gain full read/write access to the controller.

```
0020  4f 52 47 45 3a 49 43 53 46 4f 52 47 45 3a 50 52   ORGE:ICSFORGE:PR
0030  45 56 49 45 57 3a 54 30 38 39 31 5f 5f 68 61 72   EVIEW:T0891__har
0040  64 63 6f 64 65 64 5f 63 72 65 3a 54 30 38 39 31   dcoded_cre:T0891
0050  3a 3a                                            ::
```

CONFIGURATION

DESTINATION IP: 192.168.213.128
TIMEOUT (S): 2.0
SOURCE IP (PCAP): 127.0.0.1
INTERFACE (L2, OPTIONAL): eth0

PROTOCOL PARAMETERS (ENIP)
SLOT NUMBER: CIP route slot

BUILD PCAP

✓ CONFIRM: DESTINATION IS A SAFE HOST (RECEIVER) IN YOUR ENVIRONMENT

STEALTH MODE — REAL TRAFFIC, NO SYNTHETIC TAGS

▶ RUN LIVE | ⬇ PCAP ONLY | × CLEAR

✅ hardcoded_creds · enip — 8 packets sent 3:27:43 PM

SCENARIO SUMMARY

2 steps · 8 total packets enip

enip T0891 default_auth ×3 0.5s
enip T0891 write_tag ×5 1s

STEP PLAN

✓ enip T0891 default_auth ×3
✓ enip T0891 write_tag ×5

```
[LIVE] T0891__hardcoded_creds__enip → 192.168.213.128
[OK] run_id=2026-04-14-XRAY-05  sent=8
  events → /home/kali/Desktop/ICSForge-v0.61.0/out/events/2026-04-14-XRAY-05.jsonl
```

LIVE ATTACK TIMELINE

T0891__hardcoded_cre

enip default_auth T0891 ×3 confirmed
enip write_tag T0891 ×5 confirmed

2 delivered · 2 confirmed by receiver 9.2s

LIVE RECEIVER FEED

8	1	1	1
PACKETS	RUNS	TECHNIQUES	PROTOCOLS

T0891 8

INDUSTRY PROFILE

All sectors — show everything

🎯 Campaign Playbooks

Multi-scenario sequenced campaigns with configurable dwell timers between steps.

🎯 **Full ICS Kill Chain**

Comprehensive 9-scenario campaign covering the complete OT attack lifecycle: reconnaissance → creden…

9 scenarios ~3 minutes

⚙ **Stuxnet-Style Campaign**

Reproduces the Stuxnet attack sequence: PROFINET device discovery, S7comm fingerprinting, program up…

5 scenarios ~90 seconds

📡 **AitM + Sensor Spoofing**

Adversary-in-the-Middle attack against OPC UA historian followed by spoofed sensor values injected i…

5 scenarios ~75 seconds

🔑 **OT Credential Harvest**

Multi-protocol default credential probe across Modbus, S7comm, OPC UA, and EtherNet/IP followed by l…

5 scenarios ~60 seconds

☢ **Safety System Attack (Triton-style)**

Targets safety instrumented systems: reads SIS state, manipulates protection relays, disables safety…

5 scenarios ~90 seconds

• 🎯 FULL ICS KILL CHAIN — Campaign Playbook

Comprehensive 9-scenario campaign covering the complete OT attack lifecycle: reconnaissance → credential access → collection → C2 → impact. Based on combined TTPs from Stuxnet, Industroyer, and Triton.

Destination IP: 192.168.213.128

Interface (PROFINET L2, optional): eth0

Steps

1	Phase 1 · Recon: EtherNet/IP device sweep	
2	Phase 1 · Recon: S7comm SZL fingerprint	+8s
3	Phase 2 · Initial Access: Default credentials	+10s
4	Phase 3 · Collection: Process state monitoring	+12s
5	Phase 3 · Collection: Full I/O image read	+10s
6	Phase 4 · C2: Covert beacon via Modbus registers	+15s
7	Phase 5 · Inhibit: Alarm threshold manipulation	+12s

RUN CAMPAIGN ABORT Running…

• LIVE PROGRESS — run_id: 2026-04-14-E

✓	Phase 1 · Recon: EtherNet/IP device sweep	
✓	Phase 1 · Recon: S7comm SZL fingerprint	+8s
✓	Phase 2 · Initial Access: Default credentials	+10s
▶	Phase 3 · Collection: Process state monitoring	+12s
5	Phase 3 · Collection: Full I/O image read	+10s
6	Phase 4 · C2: Covert beacon via Modbus registers	+15s
7	Phase 5 · Inhibit: Alarm threshold manipulation	+12s
8	Phase 6 · Impact: PLC program modification	+15s
9	Phase 6 · Impact: CPU STOP + program reload	+10s

Event Stream

```
12:33:52 Step 2/9: Phase 1 · Recon: S7comm SZL fingerprint
12:33:54   ✓ 12 packet(s)
12:33:54   ⏱ waiting 10s…
```

ATT&CK for ICS v18.1 — Interactive Matrix

RUNNABLE = live network traffic | PRECURSOR = observable approximation | – = host-only / not implemented

Receiver IP (e.g. 10.0.0.50) | SAVE IP | ALL | RUNNABLE | PRECURSOR | GAP

Overlay: (no overlay) | LOAD RUNS | APPLY | CLEAR

■ Executed ■ Detected ■ Gap

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
T0817 Drive-by Compromise	T0807 Command-Line Interface	T0839 Module Firmware	T0874 Hooking	T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	T0812 Default Credentials	T0801 Monitor Process State	T0869 Standard Application Layer Protocol	T0800 Activate Firmware Update Mode	T0806 Brute Force I/O	T0813 Denial of Control
T0819 Exploit Public-Facing Application	T0821 Modify Controller Tasking	T0857 System Firmware	T0890 Exploitation for Privilege Escalation	T0849 Masquerading	T0842 Network Sniffing	T0843 Program Download	T0802 Automated Collection	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0815 Denial of View
T0822 External Remote Services	T0823 Graphical User Interface	T0859 Valid Accounts		T0851 Rootkit	T0846 Remote System Discovery	T0859 Valid Accounts	T0811 Data from Information Repositories	T0885 Commonly Used Port	T0804 Block Reporting Message	T0839 Module Firmware	T0826 Loss of Availability
T0847 Replication Through Removable Media	T0834 Native API	T0873 Project File Infection		T0856 Spoof Reporting Message	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0830 Adversary-in-the-Middle		T0805 Block Serial COM	T0855 Unauthorized Command Message	T0827 Loss of Control
T0848 Rogue Master	T0853 Scripting	T0889 Modify Program		T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0867 Lateral Tool Transfer	T0845 Program Upload		T0809 Data Destruction	T0856 Spoof Reporting Message	T0828 Loss of Productivity and Revenue
T0860 Wireless Compromise	T0858 Change Operating Mode	T0891 Hardcoded Credentials		T0872 Indicator Removal on Host		T0886 Remote Services	T0852 Screen Capture		T0814 Denial of Service		T0829 Loss of View
T0862 Supply Chain Compromise	T0863 User Execution			T0894 System Binary Proxy Execution		T0891 Hardcoded Credentials	T0861 Point & Tag Identification		T0816 Device Restart/ Shutdown		T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0871 Execution through API						T0868 Detect Operating Mode		T0835 Manipulate I/O Image		T0832 Manipulation of View
T0865 Spearphishing Attachment	T0874 Hooking						T0877 I/O Image		T0838 Modify Alarm Settings		T0837 Loss of Protection
T0866 Exploitation of Remote Services	T0895 Autorun Image						T0887 Wireless Sniffing		T0851 Rootkit		T0879 Damage to Property
T0883 Internet Accessible Device							T0893 Data from Local System		T0857 System Firmware		T0880 Loss of Safety
T0886 Remote Services									T0878 Alarm Suppression		T0882 Theft of Operational Information
									T0881 Service Stop		
									T0892 Change Credential		

ATT&CK for ICS v18.1 — Interactive Matrix

RUNNABLE = live network traffic | PRECURSOR = observable approximation | – = host-only / not implemented

Receiver IP (e.g. 10.0.0.50) | SAVE IP | ALL | RUNNABLE | PRECURSOR | GAP

Overlay: ★ All runs (aggregate) | LOAD RUNS | APPLY | CLEAR

■ Executed ■ Detected ■ Gap

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
T0817 Drive-by Compromise	T0807 Command-Line Interface	T0839 Module Firmware	T0874 Hooking	T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	T0812 Default Credentials	T0801 Monitor Process State	T0869 Standard Application Layer Protocol	T0800 Activate Firmware Update Mode	T0806 Brute Force I/O	T0813 Denial of Control
T0819 Exploit Public-Facing Application	T0821 Modify Controller Tasking	T0857 System Firmware	T0890 Exploitation for Privilege Escalation	T0849 Masquerading	T0842 Network Sniffing	T0843 Program Download	T0802 Automated Collection	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0815 Denial of View
T0822 External Remote Services	T0823 Graphical User Interface	T0859 Valid Accounts		T0851 Rootkit	T0846 Remote System Discovery	T0859 Valid Accounts	T0811 Data from Information Repositories	T0885 Commonly Used Port	T0804 Block Reporting Message	T0839 Module Firmware	T0826 Loss of Availability
T0847 Replication Through Removable Media	T0834 Native API	T0873 Project File Infection		T0856 Spoof Reporting Message	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0830 Adversary-in-the-Middle		T0805 Block Serial COM	T0855 Unauthorized Command Message	T0827 Loss of Control
T0848 Rogue Master	T0853 Scripting	T0889 Modify Program		T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0867 Lateral Tool Transfer	T0845 Program Upload		T0809 Data Destruction	T0856 Spoof Reporting Message	T0828 Loss of Productivity and Revenue
T0860 Wireless Compromise	T0858 Change Operating Mode	T0891 Hardcoded Credentials		T0872 Indicator Removal on Host		T0886 Remote Services	T0852 Screen Capture		T0814 Denial of Service		T0829 Loss of View
T0862 Supply Chain Compromise	T0863 User Execution			T0894 System Binary Proxy Execution		T0891 Hardcoded Credentials	T0861 Point & Tag Identification		T0816 Device Restart/ Shutdown		T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0871 Execution through API						T0868 Detect Operating Mode		T0835 Manipulate I/O Image		T0832 Manipulation of View
T0865 Spearphishing Attachment	T0874 Hooking						T0877 I/O Image		T0838 Modify Alarm Settings		T0837 Loss of Protection
T0866 Exploitation of Remote Services	T0895 Autorun Image						T0887 Wireless Sniffing		T0851 Rootkit		T0879 Damage to Property
T0883 Internet Accessible Device							T0893 Data from Local System		T0857 System Firmware		T0880 Loss of Safety
T0886 Remote Services									T0878 Alarm Suppression		T0882 Theft of Operational Information
									T0881 Service Stop		
									T0892 Change Credential		

Overlay applied
all runs

• COVERAGE REPORT

Build an ATT&CK for ICS heatmap. Fill in what was tested, what was detected, and where gaps were found. Export as a self-contained HTML report.

Run Reference

Select a previous run

★ All runs combined (50 runs) LOAD

or paste run ID manually

Loaded 45 unique technique(s) across 50 runs

Technique Coverage

Executed — fired by ICSForge

```
T0800
T0801
T0802
T0803
T0809
```

Detected — confirmed by NSM / SIEM

```
T0880

T0885
T0886
T0888
T0889
```

Gaps Found — executed but not detected (blind spots)

```
T0882
T0883
```

Protocol Coverage Gaps

Flag specific protocols that are not firewalled, monitored, or have known blind spots. These appear as a dedicated table in the report.

EtherNet/IP (4481 | Not firewalled | ×

ICSForge Coverage Report

Assessment Date: 2026-04-14 · **Generated:** 2026-04-14 10:37 UTC
Run ID: — · **Matrix:** ATT&CK for ICS v18.1
Organization: Test Inc. · **Analyst:** John Kurnaz
Notes: First Assessment

94	45	43	2	47%
MATRIX TECHNIQUES	EXECUTED	DETECTED	GAPS FOUND	MATRIX COVERAGE

95%	2
DETECTION RATE	PROTOCOL GAPS

ATT&CK FOR ICS HEATMAP

Detected · Executed / Not Detected · Gap Found (blind spot) · Not Tested

TOOLS

Convenience UI for key workflows. Sender mode includes offline artifacts and replay. Receiver mode is read-only and minimal.

HEALTH & SELF-TEST

Quick sanity checks for demo readiness.

HEALTH

OUTPUT

```
{
  "capabilities": {
    "af_packet": true,
    "pcap_write": true,
    "profinet_live": true
```

INTERFACES

Discover local network interfaces (useful for replay and live send).

REFRESH

eth0

OFFLINE GENERATE

Generate ground-truth JSONL and optional PCAP from `icsforge/scenarios/scenarios.yml` without live sending.

SCENARIO

filter scenarios (e.g. T0855 / modbus)

T0878__alarm_suppression__iec104_inhibit

Choose a scenario

OUTDIR: out

DST IP (FOR ARTIFACTS): 198.51.100.42

SRC IP (FOR ARTIFACTS): 127.0.0.1

✓ BUILD PCAP GENERATE

⬇ DOWNLOAD PCAP — T0878__ALARM_SUPPRESSION__2026-04-14__OSCAR.PCAP

RESULT

```
✓ Events: /home/kali/Desktop/ICSForge-v0.61.0/out/events/
T0878__alarm_suppression__2026-04-14__OSCAR.jsonl
✓ PCAP:   /home/kali/Desktop/ICSForge-v0.61.0/out/pcaps/
T0878__alarm_suppression__2026-04-14__OSCAR.pcap
```

PCAP REPLAY

Replay a PCAP toward a destination IP (requires sudo/root for raw send on many systems).

⚠ Replay accepts any destination IP including addresses outside RFC 1918. Only replay PCAPs to devices you own and have explicit permission to test.

PCAP PATH (SERVER-SIDE) OR UPLOAD BELOW

/home/kali/Desktop/ICSForge-v0.61.0/out/pcaps/uploads/T0846__network_scanning_

Upload PCAP: Browse... T0846__network_scann...6-04-14__QUEBEC.pcap UPLOAD

✓ T0846__network_scanning__2026-04-14__QUEBEC.pcap

REPLAY

RESULT

```
Sent: 40 packets
L2 frames (PROFINET/GOOSE) are skipped — require raw socket
interface.

{
  "ok": true,
  "sent": 40
}
```

RECEIVER WEB UI

RECEIVER

Passive proof-of-delivery sink · no responses · no PLC writes

● Last: 2026-04-14 10:41:28 PASSIVE ⟳ RESET

1029	53	42	8
PACKETS RECEIVED	ACTIVE RUNS	TECHNIQUES SEEN	PROTOCOLS SEEN

⬡ L2 listeners active (PROFINET DCP + GOOSE) on interface: eth0

SENDER CALLBACK SETTINGS

Configure where this receiver should send live receipt confirmations.

SENDER CALLBACK URL: http://sender-ip:8080/api/receiver/callback

CALLBACK TOKEN (OPTIONAL): NZ-550EXrQLLNMc1vMuUF9j7oRyOkcWc

SAVE CALLBACK | TEST CALLBACK

LIVE RECEIPTS

RUN ID: e.g. 2026-03-05-BRAVO-0 | TECHNIQUE: e.g. T0855 | PROTOCOL: e.g. modbus | APPLY

TIME	PROTO	SOURCE	TECHNIQUE	RUN ID	BYTES
2026-04-14 10:41:28	iec104	192.168.213.128:59668	T0889	2026-04-14 JULIET-80	106
2026-04-14 10:41:27	iec104	192.168.213.128:59660	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:26	iec104	192.168.213.128:59644	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:25	iec104	192.168.213.128:59632	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:24	iec104	192.168.213.128:37430	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:23	iec104	192.168.213.128:37426	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:22	iec104	192.168.213.128:37424	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:21	iec104	192.168.213.128:37416	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:20	iec104	192.168.213.128:37402	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:19	iec104	192.168.213.128:37392	T0889	2026-04-14 JULIET-80	110

RUN DETAILS

Click a run_id in the table to inspect.

2026-04-14-JULIET-80 DELIVERED

Packets: **11**
First: 2026-04-14 10:41:18
Last: 2026-04-14 10:41:28

Techniques observed:

T0889

Evidence stored in receipts.jsonl with correlation marker.

RECEIVER

Passive proof-of-delivery sink · no responses · no PLC writes

Last: 2026-04-14 10:41:28 PASSIVE ⟳ RESET

1029	53	42	8
PACKETS RECEIVED	ACTIVE RUNS	TECHNIQUES SEEN	PROTOCOLS SEEN

⬡ L2 listeners active (PROFINET DCP + GOOSE) on interface: eth0

SENDER CALLBACK SETTINGS

Configure where this receiver should send live receipt confirmations.

SENDER CALLBACK URL: http://sender-ip:8080/api/receiver/callback

CALLBACK TOKEN (OPTIONAL): NZ-550EXrQLLNMc1vMuUF9j7oRyOkcWc

SAVE CALLBACK | TEST CALLBACK

LIVE RECEIPTS

RUN ID: e.g. 2026-03-05-BRAVO-0 | TECHNIQUE: e.g. T0855 | PROTOCOL: e.g. modbus | APPLY

TIME	PROTO	SOURCE	TECHNIQUE	RUN ID	BYTES
2026-04-14 10:41:28	iec104	192.168.213.128:59668	T0889	2026-04-14 JULIET-80	106
2026-04-14 10:41:27	iec104	192.168.213.128:59660	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:26	iec104	192.168.213.128:59644	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:25	iec104	192.168.213.128:59632	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:24	iec104	192.168.213.128:37430	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:23	iec104	192.168.213.128:37426	T0889	2026-04-14 JULIET-80	108
2026-04-14 10:41:22	iec104	192.168.213.128:37424	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:21	iec104	192.168.213.128:37416	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:20	iec104	192.168.213.128:37402	T0889	2026-04-14 JULIET-80	110
2026-04-14 10:41:19	iec104	192.168.213.128:37392	T0889	2026-04-14 JULIET-80	110

RUN DETAILS

Click a run_id in the table to inspect.

2026-04-14-JULIET-80 DELIVERED

Packets: 11
First: 2026-04-14 10:41:18
Last: 2026-04-14 10:41:28

Techniques observed:

T0889

Evidence stored in receipts.jsonl with correlation marker.

ATT&CK for ICS v18.1 — Interactive Matrix

RUNNABLE = live network traffic | PRECURSOR = observable approximation | – = host-only / not implemented

ALL | RUNNABLE | PRECURSOR | GAP

Overlay: (no overlay) | LOAD RUNS | APPLY | CLEAR

■ Executed ■ Detected ■ Gap

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
T0817 Drive-by Compromise	T0807 Command-Line Interface	T0839 Module Firmware	T0874 Hooking	T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	T0812 Default Credentials	T0801 Monitor Process State	T0869 Standard Application Layer Protocol	T0800 Activate Firmware Update Mode	T0806 Brute Force I/O	T0813 Denial of Control
T0819 Exploit Public-Facing Application	T0821 Modify Controller Tasking	T0857 System Firmware	T0890 Exploitation for Privilege Escalation	T0849 Masquerading	T0842 Network Sniffing	T0843 Program Download	T0802 Automated Collection	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0815 Denial of View
T0822 External Remote Services	T0823 Graphical User Interface	T0859 Valid Accounts		T0851 Rootkit	T0846 Remote System Discovery	T0859 Valid Accounts	T0811 Data from Information Repositories	T0885 Commonly Used Port	T0804 Block Reporting Message	T0839 Module Firmware	T0826 Loss of Availability
T0847 Replication Through Removable Media	T0834 Native API	T0873 Project File Infection		T0856 Spoof Reporting Message	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0830 Adversary-in-the-Middle		T0805 Block Serial COM	T0855 Unauthorized Command Message	T0827 Loss of Control
T0848 Rogue Master	T0853 Scripting	T0889 Modify Program		T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0867 Lateral Tool Transfer	T0845 Program Upload		T0809 Data Destruction	T0856 Spoof Reporting Message	T0828 Loss of Productivity and Revenue
T0860 Wireless Compromise	T0858 Change Operating Mode	T0891 Hardcoded Credentials		T0872 Indicator Removal on Host		T0886 Remote Services	T0852 Screen Capture		T0814 Denial of Service		T0829 Loss of View
T0862 Supply Chain Compromise	T0863 User Execution			T0894 System Binary Proxy Execution		T0891 Hardcoded Credentials	T0861 Point & Tag Identification		T0816 Device Restart/ Shutdown		T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0871 Execution through API						T0868 Detect Operating Mode		T0835 Manipulate I/O Image		T0832 Manipulation of View
T0865 Spearphishing Attachment	T0874 Hooking						T0877 I/O Image		T0838 Modify Alarm Settings		T0837 Loss of Protection
T0866 Exploitation of Remote Services	T0895 Autorun Image						T0887 Wireless Sniffing		T0851 Rootkit		T0879 Damage to Property
T0883 Internet Accessible Device							T0893 Data from Local System		T0857 System Firmware		T0880 Loss of Safety
T0886 Remote Services									T0878 Alarm Suppression		T0882 Theft of Operational Information
									T0881 Service Stop		
									T0892 Change Credential		

ATT&CK for ICS v18.1 — Interactive Matrix

RUNNABLE = live network traffic | PRECURSOR = observable approximation | – = host-only / not implemented

ALL | RUNNABLE | PRECURSOR | GAP

Overlay: ★ All runs (aggregate) | LOAD RUNS | APPLY | CLEAR

■ Executed ■ Detected ■ Gap

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
T0817 Drive-by Compromise	T0807 Command-Line Interface	T0839 Module Firmware	T0874 Hooking	T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	T0812 Default Credentials	T0801 Monitor Process State	T0869 Standard Application Layer Protocol	T0800 Activate Firmware Update Mode	T0806 Brute Force I/O	T0813 Denial of Control
T0819 Exploit Public-Facing Application	T0821 Modify Controller Tasking	T0857 System Firmware	T0890 Exploitation for Privilege Escalation	T0849 Masquerading	T0842 Network Sniffing	T0843 Program Download	T0802 Automated Collection	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0815 Denial of View
T0822 External Remote Services	T0823 Graphical User Interface	T0859 Valid Accounts		T0851 Rootkit	T0846 Remote System Discovery	T0859 Valid Accounts	T0811 Data from Information Repositories	T0885 Commonly Used Port	T0804 Block Reporting Message	T0839 Module Firmware	T0826 Loss of Availability
T0847 Replication Through Removable Media	T0834 Native API	T0873 Project File Infection		T0856 Spoof Reporting Message	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0830 Adversary-in-the-Middle		T0805 Block Serial COM	T0855 Unauthorized Command Message	T0827 Loss of Control
T0848 Rogue Master	T0853 Scripting	T0889 Modify Program		T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0867 Lateral Tool Transfer	T0845 Program Upload		T0809 Data Destruction	T0856 Spoof Reporting Message	T0828 Loss of Productivity and Revenue
T0860 Wireless Compromise	T0858 Change Operating Mode	T0891 Hardcoded Credentials		T0872 Indicator Removal on Host		T0886 Remote Services	T0852 Screen Capture		T0814 Denial of Service		T0829 Loss of View
T0862 Supply Chain Compromise	T0863 User Execution			T0894 System Binary Proxy Execution		T0891 Hardcoded Credentials	T0861 Point & Tag Identification		T0816 Device Restart/ Shutdown		T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0871 Execution through API						T0868 Detect Operating Mode		T0835 Manipulate I/O Image		T0832 Manipulation of View
T0865 Spearphishing Attachment	T0874 Hooking						T0877 I/O Image		T0838 Modify Alarm Settings		T0837 Loss of Protection
T0866 Exploitation of Remote Services	T0895 Autorun Image						T0887 Wireless Sniffing		T0851 Rootkit		T0879 Damage to Property
T0883 Internet Accessible Device							T0893 Data from Local System		T0857 System Firmware		T0880 Loss of Safety
T0886 Remote Services									T0878 Alarm Suppression		T0882 Theft of Operational Information
									T0881 Service Stop		
									T0892 Change Credential		

ATT&CK for ICS v18.1 — Interactive Matrix

RUNNABLE = live network traffic PRECURSOR = observable approximation – = host-only / not implemented

ALL | RUNNABLE | PRECURSOR | GAP

Overlay: (no overlay — select a run) LOAD RUNS APPLY CLEAR

■ Executed ■ Detected ■ Gap

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
T0817 Drive-by Compromise	T0807 Command-Line Interface	T0839 Module Firmware	T0874 Hooking	T0820 Exploitation for Evasion	T0840 Network Connection Enumeration	T0812 Default Credentials	T0801 Monitor Process State	T0869 Standard Application Layer Protocol	T0800 Activate Firmware Update Mode	T0806 Brute Force I/O	T0813 Denial of Control
T0819 Exploit Public-Facing Application	T0821 Modify Controller Tasking	T0857 System Firmware	T0890 Exploitation for Privilege Escalation	T0849 Masquerading	T0842 Network Sniffing	T0843 Program Download	T0802 Automated Collection	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0815 Denial of View
T0822 External Remote Services	T0823 Graphical User Interface	T0859 Valid Accounts		T0851 Rootkit	T0846 Remote System Discovery	T0859 Valid Accounts	T0811 Data from Information Repositories	T0885 Commonly Used Port	T0804 Block Reporting Message	T0839 Module Firmware	T0826 Loss of Availability
T0847 Replication Through Removable Media	T0834 Native API	T0873 Project File Infection		T0856 Spoof Reporting Message	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0830 Adversary-in-the-Middle		T0805 Block Serial COM	T0855 Unauthorized Command Message	T0827 Loss of Control
T0848 Rogue Master	T0853 Scripting	T0889 Modify Program		T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0867 Lateral Tool Transfer	T0845 Program Upload		T0809 Data Destruction	T0856 Spoof Reporting Message	T0828 Loss of Productivity and Revenue
T0860 Wireless Compromise	T0858 Change Operating Mode	T0891 Hardcoded Credentials		T0872 Indicator Removal on Host		T0886 Remote Services	T0852 Screen Capture		T0814 Denial of Service		T0829 Loss of View
T0862 Supply Chain Compromise	T0863 User Execution			T0894 System Binary Proxy Execution		T0891 Hardcoded Credentials	T0861 Point & Tag Identification		T0816 Device Restart/ Shutdown		T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0871 Execution through API						T0868 Detect Operating Mode		T0835 Manipulate I/O Image		T0832 Manipulation of View
T0865 Spearphishing Attachment	T0874 Hooking						T0877 I/O Image		T0838 Modify Alarm Settings		T0837 Loss of Protection
T0866 Exploitation of Remote Services	T0895 Autorun Image						T0887 Wireless Sniffing		T0851 Rootkit		T0879 Damage to Property
T0883 Internet Accessible Device							T0893 Data from Local System		T0857 System Firmware		T0880 Loss of Safety
T0886 Remote Services									T0878 Alarm Suppression		T0882 Theft of Operational Information
									T0881 Service Stop		
									T0892 Change Credential		

TOOLS

Convenience UI for key workflows. Sender mode includes offline artifacts and replay. Receiver mode is read-only and minimal.

HEALTH & SELF-TEST

Quick sanity checks for demo readiness.

HEALTH

OUTPUT


```
{
  "capabilities": {
    "af_packet": true,
    "pcap_write": true,
    "profinet_live": true,
    "tcp_send": true
  },
  "ok": true,
  "receiver": null,
  "receiver_error": null,
  "receiver_ok": null,
  "repo_root": "/home/kali/Desktop/ICSForge-v0.61.0",
  "scenario_pack_count": 1,
  "scenario_packs": [
    "/home/kali/Desktop/ICSForge-v0.61.0/icsforge/scenarios/scenarios.yml"
  ],
  "timestamp": "2026-04-14T10:42:52.859200+00:00Z",
  "version": "0.61.0"
}
```


INTERFACES

Discover local network interfaces (useful for replay and live send).

REFRESH

eth0

EXAMPLE DETECTIONS IN OT NSM SENSOR

Defender for IoT | Alerts

Search

Discover

Overview
Device map
Device inventory
Alerts

Analyze

Event timeline
Data mining
Risk assessment
Trends & statistics
Attack vector

Manage

System settings
Custom alert rules
Users
Forwarding

Support

Support

Refresh | Edit Columns | Export to CSV | Change Status | Export to PDF | Learn

Search

Status == **New** | Last detection == **Last day** | Source Device == **192.168.178.10** | Destination Device == **192.168.178.30** | Add filter | Reset filters

Showing 324 of 616 alerts

Group by: Severity

Severity	Name	Engine	Last detection	Status	Source Device	Destination Device
Critical (1)						
Critical	Unauthorized PLC Programming	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major (321)						
Major	Unpermitted Usage of Modbus Function Code	Policy Violation	4 hours ago	New	192.168.178.10	192.168.178.30
Major	Unpermitted Usage of ASDU Types	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized Siemens S7 Execution of User Defi	Policy Violation	4 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized Siemens S7 Execution of Control Fu	Policy Violation	4 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized PLC Program Upload	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized HTTP Activity	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized BACNet Route	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	Unauthorized BACNet Object Access	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	New Activity Detected - EtherNet/IP Protocol Cor	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	MQIsdp New Topic Subscription Detected	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	MQIsdp New Publish Detected	Policy Violation	5 hours ago	New	192.168.178.10	192.168.178.30
Major	Modbus Address Range Violation	Policy Violation	4 hours ago	New	192.168.178.10	192.168.178.30
Major	Modbus Address Range Violation	Policy Violation	4 hours ago	New	192.168.178.10	192.168.178.30

https://www.icsforge.nl