

Comprehensive Passive OT/ICS Network Security

vSOCBox NDR delivers non-intrusive, real-time Network Traffic Analysis (NTA) and Network Detection & Response (NDR) for Critical Infrastructure and Industrial Environments. Operating via agentless, passive SPAN/TAP monitoring, vSOCBox provides deep operational visibility, asset discovery, threat detection, and forensic analysis without impacting sensitive PLCs, HMIs, or controllers.

100%

AGENTLESS & PASSIVE

Dozens

ICS PROTOCOLS PARSED

ATT&CK

MITRE ICS MAPPED

ML & AI

ANOMALY DETECTION

CORE OT SECURITY CAPABILITIES

Capability	Description & Operational Value
Passive OT Monitoring	Zero operational risk—no agents installed on sensitive PLCs, HMIs, or industrial controllers.
Deep Packet Inspection (DPI)	Natively decodes industrial and enterprise protocols down to command and register levels.
Network Traffic Analysis (NTA)	Provides complete visibility across cross-segment IT and OT network communications.
Asset Discovery & Inventory	Automatically discovers OT assets from network traffic and maps to user-defined inventories.
Device Fingerprinting	Advanced JA4/JA3 TLS fingerprinting and MAC OUI identification for exact device profiles.
ICS Best Guess Detection	Identifies proprietary or unknown industrial traffic via port heuristics and behavioral patterns.
MITRE ATT&CK Mapping	Real-time correlation against ATT&CK Enterprise and ATT&CK for ICS threat frameworks.
Forensics & Full PCAP Support	Stores raw packet captures, Zeek logs, and Suricata alerts for in-depth incident investigation.
Malware & File Analysis	Extracts files in real-time for Anti-Virus, YARA, capa, and cryptographic hash analysis.
Machine Learning Anomalies	Random Cut Forest (RCF) ML algorithms detect subtle shifts in traffic volume, actions, and protocols.

Network Threat Detection

- Unauthorized cross-segment communications
- New or unknown device discovery alerts
- External / Internet-bound connection attempts
- Plaintext credential exposure in OT traffic
- Suspicious file transfers & large data exfiltration
- Beaconing behavior & Command-and-Control (C2)
- Lateral movement indicators across zones

Industrial Protocol Support

Native deep packet inspection for leading automation standards:

- Modbus/TCP
- DNP3
- BACnet
- OPC UA
- PROFINET
- EtherNet/IP (CIP)
- Siemens S7
- IEC-60870-5-104
- IEC-61850 MMS
- MQTT
- BSAP (Bristol)
- ANSI C12.22
- IEEE C37.118

OT/ICS-Specific Threat Detection

- Unusual PLC programming & logic changes
- Controller configuration updates & restarts
- Unauthorized Engineering Workstation access
- Industrial protocol misuse & malformed packets
- Unexpected write operations & force commands
- Unsafe operational commands & parameter limits
- Abnormal changes in controller communication cycles

IT & Infrastructure Protocols

- LLDP
- ARP
- VLAN
- STP
- IPv4/IPv6
- DNS
- DHCP
- HTTP/S
- FTP
- SMB
- LDAP
- Kerberos
- SSH
- SNMP
- RDP
- TLS/QUIC

Discovered Asset Categories

Automatically classifies critical industrial endpoints:

- PLCs & RTUs
 - HMIs & Operator Stations
 - Engineering Workstations
- Historians & Servers
 - Industrial Switches
 - Remote I/O & Sensors

ATT&CK for ICS Framework

Maps threat vectors directly to MITRE ACID analytics:

- Initial Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Inhibit Response
- Impair Process Control
- Impact

ICS Best Guess Detection

When proprietary or unparsed protocols are encountered, vSOCBox leverages port heuristics, vendor signatures, and behavioral patterns to accurately identify traffic without requiring custom decoders.

BUILT-IN OPERATIONAL DASHBOARDS & ANALYTICS

- ICS Security Overview
- Modbus / DNP3 / BACnet
- OPC UA & EtherNet/IP
- PROFINET & IEC-104
- MQTT & Best Guess ICS
- ATT&CK for ICS Dashboard
- Asset Inventory & Fingerprinting
- External & Cross-Segment Traffic
- File Transfers & Security Notices

SUPPORTED MANUFACTURING & INFRASTRUCTURE SECTORS

- Discrete Manufacturing
 - Automotive & Semiconductor
 - Oil & Gas / Petrochemical
 - Power Generation & Utilities
- Water & Wastewater
 - Pharmaceuticals & Food/Bev
 - Mining, Metals & Steel
 - Cement, Paper & Pulp
- Electronics Manufacturing
 - Building Automation Systems
 - Transportation & Logistics
 - Renewable Energy Sites