Industrial Network Security Monitoring

This poster offers guidance on setting up and performing Network Security Monitoring (NSM) with freely available, no-cost tools to carry out active cyber defense in industrial control system (ICS) environments. Several traditional concepts are adapted to provide an "ICS aspect" to further cybersecurity efforts in control networks.

NETWORK SECURITY MONITORING

NSM (Network Security Monitoring) is a human driven proactive repeatable process of Collection, Detection, and Analysis. While not specific to ICS (Industrial Control Systems), NSM excels in control system networks as the environment is usually more static and has less users than in traditional IT (Information Technology) environments. NSM is most effective with an established ICS asset inventory and is an active approach in detecting threats in early phases of an attack.

ICS ASSET INVENTORY

Having an established ICS asset inventory of operational technology devices and engineering assets will drastically improve industrial network security monitoring efforts and assist in ICS Incident Response scenarios.

Common methodologies to establish the inventory are below and can be combined for improved accuracy. For example, Physical Inspection will take advantage of face-to-face security awareness and educational discussion on-site with engineering and operational teams. Augmented with Passive Network Captures can create and verify an inventory while having network traffic to sift through for threat detection.

Asset identification information is available from several network devices such as routers, switches, and firewalls. Beyond the network layer, asset information can be discovered by extracting data directly from endpoints themselves such as the Data historians, HMI etc.

Physical Inspection—Getting physically to industrial facilities, documenting the hardware seen in racks, cabinets, on plant floor, software and protocols used, etc. Time consuming, accurate, can be expensive if traveling to remote sites. There is some potential physical risk, so PPE (Personal Protective Equipment) is required on sites.

Passive Network Packet Capture—Nonintrusive to ICS operations, accurate representation of natural network comms. Can be quick. Can output a visual network diagram that can be printed and used for engineering troubleshooting and ICS Incident Response.

Active Scanning—Intrusive to ICS operations, unnatural representation of network comms., but very fast and very detailed information about devices, services, etc. Should be tested in a development environment prior to scanning any production environment.

Configuration Analysis—Many control system and network devices may have to be accessed to review configuration settings. Switch and firewall configurations can reveal IP address and MAC address pairings through ARP tables to indicate devices allowed or denied access on the network. Traffic and port information at a 5-tuple level could reveal general protocols in use.

A practical approach—Start by reviewing any already created network diagrams. Use an encrypted laptop with at least a basic spreadsheet application to start cataloging and storing ICS asset information during a physical site walkthrough. At a minimum, record the following attributes from the commonly targeted critical assets such as Data Historians, HMI, PLCs, Engineering Workstations, core network devices, and active Safety Instrumented Systems (SIS) used.

- Site Name
- Site location
- Facility type
- Asset type and ID tag
- Asset location: room, cabinet, rack
- Description of asset function
- Impact to operations if unavailable
- IP and MAC address
- Operating ICS protocols used
- Model/manufacturer, serial number
- Firmware version
- Applications installed and versions

Augment physical inspection with passive network packet captures on critical network segments that have critical ICS assets by using either a SPAN configuration off a fully managed switch or utilize a hardware TAP.

Common host and network commands to discover data to help build the ICS asset inventory with built-in operating system and network tools and capabilities. LLDP (Link Layer Discovery Protocol), is a Layer 2 discovery protocol which is vendor-neutral and can be used to identify network assets and their capabilities. tshark filters can be used to reveal asset information from a packet capture using the lldp filter. ARP (Address Resolution Protocol), the 'arp' tool is a simple tool available in common operating systems to reveal ARP cache to show IP and MAC addresses pairing in which that device knows about on the network. Start with the top critical ICS assets first.

Discover LLDP compatible systems, their names and and network capabilities:

```
tshark: tshark -Y lldp -T fields -e lldp.tlv.system.name -e
lldp.tlv.system.desc -e lldp.tlv.system_cap -r <ICS-Network_
file.pcap>
```

Discovery asset IP and MAC addresses from ARP tables:

```
Linux: arp -an
Windows: arp /a
Switches, Firewalls: show arp
```

Discover connections and their related IP addresses on an asset:

```
Linux: netstat -an
Windows: netstat /an
```

Managing the ICS Asset Inventory
The asset inventory is incredibly valuable for the organization, but also for attackers. Safeguard ICS asset inventory by storing it in a database that is:

Scalable—Databases can help ensure that site inventories can be updated or expanded, and back them up regularly.

Searchable—All fields should be indexed to enable quick searching across inventories for all sites.

Secure—Standard data protection and security practices, including authentication and network segmentation, should be used to protect this sensitive data.

A practical approach—Use threat intelligence to drive searches across an established inventory database to understand which ICS assets have identified vulnerabilities. Identify vulnerable industrial assets for proactive defense changes starting with the most critical assets first. Combine asset inventory knowledge with ICS Network Security Monitoring to monitor for traffic anomalies that may lead to NSM Detection and NSM Analysis phases.

CRITICAL ICS ASSETS

Critical industrial assets can be targeted with malware. Also, human adversaries can target the control system to cause negative impacts on the process through directly interacting with the control environment using legitimate operational software with malicious intent. Several critical ICS assets are below. At a minimum, access control, network traffic and system integrity should be protected and regularly monitored for these assets.

Data Historian—This is a database that stores operational process records. Can be abused to act as a pivot point from a compromised asset in IT to an asset in the ICS network.

Engineering Workstation—The engineering workstation has software to program and change PLC and other field device settings/configurations.

Human Machine Interface—The HMI is a visual interface between the physical process and operators that is used to monitor, control, and change most any part of the industrial process.

Programmable Logic Controllers—PLCs connect the physical hardware, run logic code to read the state, change the state or a process, and interfaces with devices that make physical changes in the real-world.

INDUSTRIAL CONTROL NETWORK PROTOCOLS

Use common tshark/Wireshark filters to focus on industrial control network communications to aid in engineering troubleshooting and security initiatives. There are many industrial protocols, the following are just some of the most common protocols in use in their related sectors.

```
ModbusTCP
Port: TCP 502
tshark/Wireshark filter "mbtcp"
```

Application: The TCP version of the serial protocol Modbus is an open industrial protocol standard, the de facto standard, commonly used to communicate with IP-connected field devices to/from HMIs and intelligent electronic devices across several industrial sectors, including the electricity sector.

```
BACnet (Building Automation Controls)
Port: UDP 47808
tshark/Wireshark filter "bacnet"
```

Application: The Building Automation Controls protocol enables communications for building automation and controls for Heating Ventilation Air Conditioning (HVAC) systems.

```
OPC (Open Platform Communications)
Port: <several>, sometimes TCP 135 and DCE/RPC ports
tshark/Wireshark filter "opcua" or "dcerpc"
```

Application: Open Platform Communications can be implemented in several ways, which determines the ports that will be utilized when the communications are deployed. Observing Distributed Computing Environment/Remote Procedure Call (DCE/RPC) traffic can help identify OPC in use. OPC is used to enable communications from different vendor devices in a vendor-natural way.

```
EtherNetIP/CIP
Port: UDP 2222, TCP 44818
tshark/Wireshark filter "enip"
```

Application: EtherNetIP/CIP is commonly observed in manufacturing facilities, using both UDP and TCP. UDP is used for I/O data transfers, while TCP is used for set points to be set or read.

```
DNP3
Port: TCP 20000
tshark/Wireshark filter "dnp3"
```

Application: Distributed Network Protocol version 3 is commonly observed in water and electricity power utilities, and occasionally in gas pipeline operations. It is used for communications between control centers and field devices such as Remote Terminal Units (RTUs) or Intelligent Electronic Devices (IEDs).

```
IEC 60870-5-104
Port: TCP 2404, 2405
tshark/Wireshark filter "iec60870_104"
```

Application: The IEC 60870-5-104 Protocol is commonly observed in the electricity sector to monitor power systems and has the capabilities to restart devices and modify set points in the field.

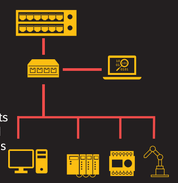
```
IEC 61850
Port:102
tshark/Wireshark filter "goose"
```

Application: IEC 61850 is a communications protocol commonly used for communications with Intelligent Electronic Devices (IEDs) at electric substations.

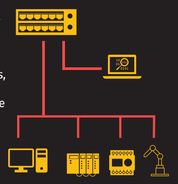
NETWORK SECURITY MONITORING – SETUP

There are two main methods to ensure that NSM Collection is established and serves as a critical step to improve any modern ICS security program: Network TAP and Network SPAN.

Network TAP—A purpose-built hardware device installed in-line in a network that copies network traffic. It typically requires a network outage to install. Always ensure that it is configured to fail open, allowing traffic to flow through the device in the event of a failure. Otherwise, it will drop or block legitimate control network communication. TAP installations in industrial control environments are usually added as a task as part of a scheduled operational maintenance window when operations are scheduled to be down.



Network SPAN—Also known as port mirroring, this may be available on already-deployed managed switches in a control network. No network outage is required to implement it. SPAN configurations can be phased in. Phase VLANs, network segments, into the SPAN configuration one or two at a time to ensure the switch CPU and memory can manage the SPAN load copying packets to a mirror port.



TAP vs. SPAN—The decision as to which method to use for NSM collection may depend on budget, maintenance windows, existing technology, and production network architecture.

NSM Collection Method	Pros	Cons
TAP Hardware	• Capture also includes network errors—malformed packets, etc. • Dedicated hardwar—TAP more challenging to compromise than a switch SPAN configuration	• ICS network outage required • Additional hardware required
SPAN Configuration	• Deploys on existing fully managed switches in phased-in approach • No ICS network outage required	• May miss or drop mirrored packets if switch is overloaded • May not capture network error communications

SPAN Configuration Example—Commands differ across switch manufacturers. The example below shows pseudo commands for setting up a SPAN configuration on a switch to create a local SPAN *session 1* to monitor *bi-directional traffic* from *port 1* to *port 2*, and to verify that the change is applied:

```
# monitor session 1 source interface gigabitethernet1/1 both
# monitor session 1 destination interface gigabitethernet1/2
# show monitor all
```

NETWORK SECURITY MONITORING – ICS-COMPATIBLE TOOLS

Many no-cost, open-source tools are available to assist organizations as they mature their ICS security program and ICS NSM capabilities. Several tools have built-in or ICS-specific features or plugin modules.

Security Onion—A no-cost, open-source Linux platform designed for intrusion detection, network security monitoring, and event log management with many supporting tools built in.

Snort—Intrusion Detection System (IDS) with many ICS-specific preprocesses built in to help detect ICS vulnerabilities and attack traffic in control networks. ICS plugins available.

Tcpreplay—Command-line network tool to play packet capture files (pcap) against a network interface card. Used in conjunction with Snort, or similar IDS systems, to sift through network communication for known malicious activity and to test custom ICS network threat signatures.

Wireshark—Graphical user interface packet analysis tool with built-in dissectors for many common industrial protocols. Also has capabilities to extract file objects from packet captures.

Tshark—Command-line packet analysis tool supporting Wireshark filters with many of the same capabilities.

GRASSMARLIN—An open-source network mapping tool created by the National Security Agency's Information Assurance Directorate specifically for ICS network packet captures. It will output information about devices, control network communications, and data extracted about the industrial protocols in use. GRASSMARLIN can also output a primitive network diagram from a live network collection from a tap, or offline traffic captured from a SPAN configuration into pcap files.

NetworkMiner—A protocol-aware network tool. A no-cost version is available that can extract objects from packet captures such as credentials and several file types.

Zeek—An open-source IDS and NSM tool for Linux. It has some ICS capabilities built in and can be expanded further with additional ICS plugins from the community. Zeek also has features such as network flow analysis and others.

SANS | GIAC CERTIFICATIONS

COLLECT

NETWORK SECURITY MONITORING – COLLECTION

A properly segmented ICS network following the Purdue network architecture model has enforcement boundaries, naturally creating chokepoints for network data collection. It also doubles as control points for containment in industrial incident response. Collect ICS traffic at Purdue Levels 0-3 at a minimum—communications to and from the HMIs, PLCs, RTUs, and other IEDs in critical network segments. Common network collection points would be on internal edge or zone industrial firewalls, or core control network switches. Use fully managed network switches to passively collect data via SPAN, or from hardware TAP devices that would be installed in-line.

ICS ASPECT – COLLECTION: Collect the 5-tuple data at a minimum, where full-packet collection would be ideal to ensure that industrial protocol communications and data are also captured. Beyond just security events, ICS NSM can uncover general networking and engineering system misconfigurations to improve overall industrial network efficiency and resilience.

The 5-tuple Capture: Consists of the source and destination IP addresses, source and destination ports, and protocols observed.

Full-Packet Capture: Consists of the entire packet—including the 5-tuple data as well as the full packet payload, such as the query and response data, industrial commands, function codes, and other artifacts. Even files in the packet payload may be extracted for analysis during incident response cases, such as malware samples. Full-packet capture does consume significantly more storage space than just capturing 5-tuple data.

Response: Trans: 6;	Unit: 255,	Func: 4:	Read Input Registers
Query: Trans: 10;	Unit: 255;	Func: 4:	Read Input Registers
Query: Trans: 1435;	Unit: 255;	Func: 15:	Write Multiple Coils
Query: Trans: 12062;	Unit: 255;	Func: 15:	Write Multiple Coils
Response: Trans: 12062;	Unit: 255;	Func: 15:	Write Multiple Coils
Query: Trans: 20308;	Unit: 255;	Func: 1:	Read Coils
Response: Trans: 20308;	Unit: 255;	Func: 1:	Read Coils

ICSPS_INSM_0525

This poster was created by Dean C. Parsons.

COLLECT DETECT ANALYZE

DETECT

NETWORK SECURITY MONITORING – DETECTION

Network detection is about discovering potentially malicious and/or abnormal activity, including detecting unusual inbound or outbound connections, network events linked to known IP addresses to threat campaigns, and other network anomalies.

Leverage threat intel from the applicable ICS sector and tools such as tcpreplay and Snort, with built-in ICS rulesets, and pseudocode rules below, to start network detection specific to a control environment. Known IP addresses associated with attack campaigns can be used to search across network flow data or packet captures from intrusion detection systems monitoring network communications. Expand and change pseudo rules and logic to suit the organizations' control network and setup.

ICS ASPECT - DETECTION: An Intrusion Detection System (IDS) is preferred for threat detection in ICS environments over an Intrusion Prevention System (IPS). IDS systems are used to prioritize safety, that is, to reduce false positives that could cause legitimate control commands causing operational disruptions. The Detection phase of NSM is primarily about understanding what is "normal" for the industrial operations to be better at spotting "abnormal" activity. These tools and filters can get a program started.

Replay packet captures against a listening network IDS such as Snort:
```
sudo tcpreplay --intf1=<nic_for_snort > --mbps=topspeed <ICS-Network_file.pcap>
```

Alert on communications to PLC that is not HMI:
```
alert tcp !$Modbus_HMI any -> $Modbus_PLC any (msg:"TCP comms to PLC which is not the HMI";)
```

Alert on possible recon scan or mapping if ModbusTCP is not normally used:
```
alert tcp any any -> any 502 (msg:"Scan or usage of ModbusTCP on network without it";)
```

Alert on possible TCP connection to known malicious command and control server:
```
alert tcp any any -> <evil_C2_ip> any (msg:"Connection attempt to known evil C2 IP address";)
```

ANALYZE

NETWORK SECURITY MONITORING – ANALYSIS

Use triggered signatures, which match on malicious activity such as IP addresses from attack campaigns. From the Detection phase on these triggers, pivot to the Analysis phase. With an understanding of which assets on the network are critical for safety and operations, work to identify anomalous network connections around them to help determine when ICS Incident Response is needed. Expand or change the tshark or Wireshark filters below to suit the hunt for malicious network activity.

ICS ASPECT - ANALYSIS: ICS environments have far less connectivity to the Internet and use much less encrypted communications inside control networks than in traditional IT environments. In addition, ICS attack techniques can abuse legitimate native industrial control protocols. These types of network communications should be flagged for analysis to rule out suspicious activity. Discover and analyze information, assets, protocols, files, and commands from the control network by using these tools and filters. Furthermore, file transfers to or from critical assets such as the HMI, Data Historian, or engineering workstations are critical to flag for analysis.

Wireshark: Wireshark > Statistics > Endpoints
Provides statistics about logical addresses on the network, including asset IP address and MAC address. Displays number of packets, total bytes, bytes received and transmitted, and attempts to perform DNS name resolution, which can help with asset identification. Record the expected and potentially anomalous polling rate and direction of traffic between the HMI and field devices (varies by vendor equipment and protocol). Record and analyze each IP address and associated ports to identify all active assets.

Wireshark: Wireshark > Statistics > Conversations
Provides statistics about conversations in the traffic between endpoints, displayed as IP addresses. Information such as the start, stop, and duration of the conversations is notable. Record the devices that are communicating and note their communication patterns. A single device having conversations with multiple devices could indicate the HMI in the network.

Wireshark: Wireshark > Statistics > Protocol Hierarchy
Provides statistics about observed protocols on the network. Protocols are displayed in a tree layout with bar graphs indicating the percent of the protocol seen as a share of the overall protocols in the capture. Record the list to determine which protocols are expected and further analyze protocols that are unexpected. Note, however, that legitimate protocols could be abused in attack scenarios, so it is important to record and analyze protocol patterns and source devices sending commands, in particular to field devices.

Wireshark: Wireshark > Export Objects > <type> > Save
Extract files from a packet capture using this feature. File hashes can be obtained then searched against threat intelligence or malware databases. Or, files can be executed in an isolated malware analysis sandbox to determine threat behaviors in order to develop defensive countermeasures.

General statistics about logical addresses on the network:
```
tshark: tshark -qz ip_hosts,tree -r <ICS-Network_file.pcap>
```

Asset names from NetBIOS communications:
```
tshark: tshark -Y nbns -T fields -e nbns.name -r <ICS-Network_file.pcap>
```

Asset names from DNS that could be assets performing Internet checks:
```
tshark: tshark -T fields -e ip.src -e dns.qry.name -Y "dns.flags.response eq 0" -r <ICS-Network_file.pcap> | sort | uniq
```

Traffic going to external addresses by internal source IP to external IP:
```
tshark: tshark -T fields -e ip.src -e ip.dst -r <ICS-Network_file.pcap> "not ip.dst in {192.168.0.0/16 172.16.0.0/12 10.0.0.0/8}" | sort | uniq
```

Encrypted communications, less common in ICS, which could be covert channels:
```
tshark: tshark -Y tls -T fields -e ip.src -e ip.dst -e tcp.port -e _ws.col.Info -r <ICS-Network_file.pcap> | sort | uniq
```

Protocols in use on the control network:
```
tshark: tshark -T fields -e frame.protocols -r <ICS-Network_file.pcap> | sort | uniq | cut -d : -f 2-20
```

IP addresses of devices having ModbusTCP conversations:
```
tshark: tshark -Y "mbtcp" -T fields -e ip.dst -e ip.src -r <ICS-Network_file.pcap> | sort | uniq
```

All ModbusTCP Function Codes in use on the control network:
```
tshark: tshark -Y mbtcp -T fields -e _ws.col.Info -r <ICS-Network_file.pcap> | sort | uniq | cut -d ":" -f 5,6 | sort | uniq
```

All DNP3 Function Codes in use and IP addresses using them:
```
tshark: tshark -n -Y dnp3 -T fields -e ip.src -e ip.dst -e dnp3.al.func -e _ws.col.Info -r <ICS-Network_file.pcap> | sort | uniq
```

IP addresses of devices using BACnet and BACnet control commands:
```
tshark: tshark -Y bacnet -T fields -e ip.src -e ip.dst -e bacnet.control -e _ws.col.Info -r <ICS-Network_file.pcap> | sort | uniq
```

Discover and analyze possible HTTP downloads, including filename and URI:
```
tshark: tshark -n -T fields -e http.request.method -e http.host -e http.request.uri -r <ICS-Network_file.pcap> | sort | uniq
```

Export data for analysis—HTTP downloads, including filename and URI:
```
tshark: tshark -r <ICS-Network_file.pcap> --export-objects http,<OutputDir> | sort | uniq
```

Export data for analysis—SMB file transfers, including filename and file data:
```
tshark: tshark --export-objects smb,<OutputDir> -r <ICS-Network_file.pcap>
```

Discover files transferred via SMB with remote hostname, account name, file(s) accessed:
```
tshark: tshark -n -Y 'frame.number == 189' -T fields -e smb2.filename -e smb2.tree -e smb2.acct -e smb2.host -r <ICS-Network_file.pcap>
```

NETWORK SECURITY MONITORING – IN PRACTICE

NSM Collection Platform

First, phase in NSM Collection around the most critical and vulnerable ICS assets. Start with the most important IP-connected engineering operation or facility and deploy one network segment at a time.

Sift through collected data for indicators of compromise starting with IP addresses. Use threat intel to drive searches across an established inventory database to identify vulnerabilities in targeted assets that could be flagged for proactive defense changes.

Control network traffic can be collected by purpose-built ICS NSM technology. Alternatively, even the no-cost Linux Security Onion distribution on a laptop with external storage, using built-in tools such as tcpdump or Wireshark, can be used to start ICS NSM Collection. For Detection and Analysis, Wireshark, which has several built-in packet dissectors for common industrial protocols, can be helpful in determining the assets, protocols in use, and communication patterns in an industrial environment. The tools discussed here can also be used to extract objects for further analysis to assist with ICS Incident Response efforts.

Passive ICS Network Traffic Capture Window

Passive control network capture times could be as short as several hours for point-in-time assessments. This would depend on the objective, storage, and size of the control environment. Point-in-time assessment for full-packet captures is commonly between 1 and 24 hours.

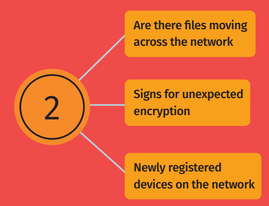
Control System Network Capture Considerations

Note that the control system could be in several operational states, which can affect network collection output. If the system is in a safe-shutdown, maintenance, or emergency procedure, devices that do not normally communicate will be visible, and the more active devices may be invisible. The most effective captures will be during the industrial process start-up and during normal operations.

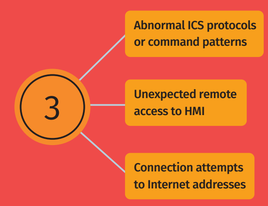
ICS Threat Detection Concepts for 5-TUPLE

Start and repeat the NSM Collection, Detection, and Analysis phases while applying these tips to prioritize the safety and reliability of ICS operations. Add additional engineering knowledge for more specific industrial control system protection. High confidence Indicator of Compromise matches and the discovery of anomalous network patterns will call industrial incident response steps into action.

ICS Threat Detection Concepts for Deep Packet Analysis



ICS Threat Detection Based on ICS Behavior



SANS ICS CURRICULUM

ICS310: ICS Cybersecurity Foundations™

ICS410: ICS/SCADA Security Essentials™
Global Industrial Cyber Security Professional (GICSP)

ICS418: ICS Security Essentials for Leaders™

ICS456: Essentials for NERC Critical Infrastructure Protection™
GIAC Critical Infrastructure Protection (GCIP)

ICS515: ICS Visibility, Detection, and Response™
GIAC Response and Industrial Defense (GRID)

ICS612: ICS Cybersecurity In-Depth™

ICS613: ICS/OT Penetration Testing & Assessments™

SANS ICS RESOURCES

sans.org/ics

ics-community.sans.org/signup

@SANSICS

ControlThings.io
Free and open-source tools for ICS