SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

ICS Cybersecurity FIELD MANUAL

Vol. 2

Author:

Dean Parsons
B.SC., GICSP, GRID, CISSP, GSLC, GCIA

Certified SANS Instructor |
CEO ICS Defense Force Inc. &
ICS Cybersecurity Leader

Contents

What to expect from these ICS security field manuals

If you are new to industrial control system (ICS) security, the SANS ICS Cybersecurity Field Manuals will get you up to speed quickly with long-lasting reference materials, free resources, and a training path in control system security for you and your teams. The manuals consist of several sections and volumes, each focusing on a different aspect of ICS cyber defense.

Introduction to Volume 2

The consequences of modern ICS cyber-attacks can include but are not limited to widespread power grid blackouts, failure or physical destruction of critical engineering equipment, massive business financial losses, paralysis of smart city emergency infrastructure in large municipalities, human injury or death, and possibly devastating environmental impacts. ICS intrusions will continue to occur and likely increase in their severity and range of consequences across multiple critical infrastructure sectors. However, managing control system cyber risk and effectively applying tactical ICS defenses is achievable!

Volume 2 of the ICS Cybersecurity Field Manual provides insight into the active cyber defense cycle, presents effective ways to establish an ICS asset inventory and obtain network visibility to apply network security monitoring (NSM) through data collection, network traffic analysis, and network threat detection. It also serves as a resource for budget-constrained ICS security programs to leverage no-cost or low-cost tools as they start their journey to mature efforts to protect control systems and critical infrastructure.

ICS418 ICS Security Leadership Simulation Game - Industrial Cyber42

SANS has extended the Cyber42 Leadership Simulation Game to the ICS418 course as Industrial Cyber42 (https://www.sans.org/blog/cyber42). Students participate in various ICS risk-based and management decision scenarios to protect a control system using their risk management skills. The object of the game is to finish with the highest safety culture score.

Sliding scale of cybersecurity

The Sliding Scale of Cybersecurity can be used to categorize the security maturity, actions, and investments that build a cybersecurity program.[1] The scale has five progressive categories: Architecture, Passive Defense, Active Defense, Intelligence, and Offense. Each category builds on the previous one to make the upcoming categories stronger. Architecture is a foundational and affordable starting point to which there is high return on investment, and from which all following categories of the scale will benefit. Each category in the scale is described below.

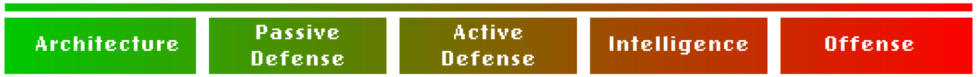


Figure 1: Sliding Scale of Cybersecurity

1. **Architecture**. The planning, establishment, and maintenance of systems with security and reliability as the priority, including the supply chain, patching, and network architecture.
2. **Passive Defense**. Systems added to Architecture that do not require consistent human interaction and provide reliable defense or insight into a subset of less-advanced threats.
3. **Active Defense**. The process of human analysis consistently involved in proactive defense. It involves using ICS-specific tools, monitoring for, actively responding to, and learning from adversaries internal to the control networks.
4. **Intelligence**. Collecting data, exploiting collected data and processing it into information, obtaining or adding context, and producing actionable threat intelligence to inform proactive defense.
5. **Offense**. Partaking in legal countermeasures and self-defense actions against the adversary.

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course teaches students all steps of the Active Cyber Defense Cycle through hands-on technical labs and real-world industrial attack scenarios and related lessons learned.

[1] For more information, see the SANS White Paper, The Sliding Scale of Cybersecurity, available here: www.sans.org/white-papers/36240/

Defining network visibility and active ICS defense

ICS security managers must support their teams to lead them to success. This means positioning team members and technologies, at a minimum, in an Active Defense position within the Sliding Scale of Cybersecurity. Active cyber defense for control systems involves trained ICS analysts leveraging technology and ICS-specific knowledge and protocols to monitor, respond to, and learn from threats targeting control networks. In parallel, ICS defenders and risk managers must work with engineering teams to define incident response processes, outcomes, and recovery steps, as safety is prioritized above all else.

ICS security managers must map existing technical ICS security controls to the sliding scale. They can start maturing their Industrial Control System and Operational Technology cybersecurity program with the Architecture and Passive Defense categories, then move to the Active Defense category by documenting a control system asset inventory as a best practice.

Tactical ICS security team members must ensure that the tools deployed in control system environments are "ICS-aware" – that is, they are specifically designed or adapted to suit ICS for both endpoint and network defense. For example, network intrusion detection systems (IDS) must be capable of deep packet inspection and perform complete ICS protocol packet dissection.

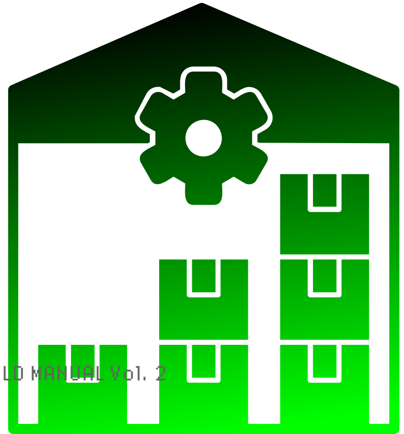
Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course includes an ICS attack history walkthrough for new and existing ICS/OT security managers, with a focus on lessons learned to improve ICS risk management and reporting to the board.

Establishing an ICS asset inventory

It is difficult to protect a control environment and keep engineering operations resilient without knowing which engineering assets are in production and which assets are deemed critical. An established ICS asset inventory of operational technology and engineering assets will improve the ICS security program's vulnerability management, network security monitoring, and incident response scenarios. The common methodologies to establish and maintain an inventory are physical inspection, configuration analysis, active scanning, and passive network traffic analysis. These methods can refine an existing asset inventory or be used to build and maintain an inventory.

- **Physical Inspection**: This involves physically walking through industrial facilities, documenting the hardware seen in racks and network cabinets, inspecting the software and protocols used, and taking other proactive steps. Physical inspection is time-consuming and expensive if it involves traveling to remote sites. Some potential physical risk exists, so personal protective equipment will be required at sites.



- **Configuration Analysis**: A review of configuration settings may require access to many controls system and network devices. Switch and firewall configurations can reveal IP address and MAC address pairings through Address Resolution Protocol (ARP) tables to indicate devices allowed or denied access to the network. Traffic and port information at a quintuple level could reveal general protocols in use. Collection and interpretation of configuration settings from ICS systems (programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices) can also be used to generate a holistic inventory of hardware, software, and firmware installed on these devices.

- **Active Scanning**: This is intrusive to ICS operations and an unnatural representation of network communications. However, this method of asset identification is very fast and can provide detailed information about devices, services, etc. It should be tested in a development environment prior to scanning any production environment.
- **Passive Network Traffic Analysis**: Nonintrusive to industrial operations, this analysis can provide an accurate representation of natural control system network communications. It can provide a visual network diagram that can be printed and used for engineering troubleshooting and ICS incident response. Where feasible and for best results, it is beneficial (though not always possible) to capture and analyze network traffic during different modes of operation (startup, normal operations, and emergency modes).

Each asset inventory method poses different risks to operations and takes different times to complete. Tactical ICS defenders and engineering staff must work together to weigh the risk versus time and related returns on investment for each method. Methods can be combined based on the ICS security program maturity and budget. For example, performing physical inspection and augmenting it with passive control system network traffic capture and analysis can be highly effective in a maturing program.

We can see several benefits when combining asset inventory methods. In the above example, physical inspection takes advantage of face-to-face security awareness discussions on-site with engineering, safety, and operational teams. This goes a long way when the teams need to perform ICS incident response in the field but rely on engineering staff to help with forensic data acquisition, log collection and/or engineering network changes during containment, or threat eradication, for example. Passive control system network traffic captures are safer and quicker and can create or verify an existing inventory. They provide network data to analyze when performing threat hunting or threat detection exercises.

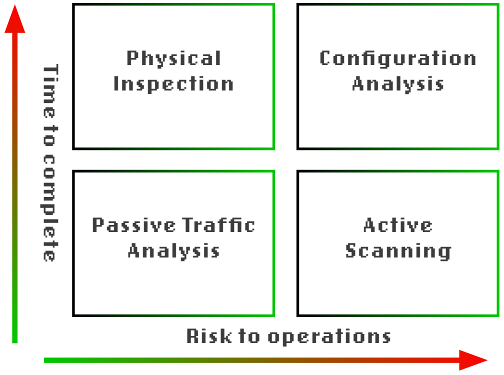


Figure 2: Asset Inventory Method Analysis

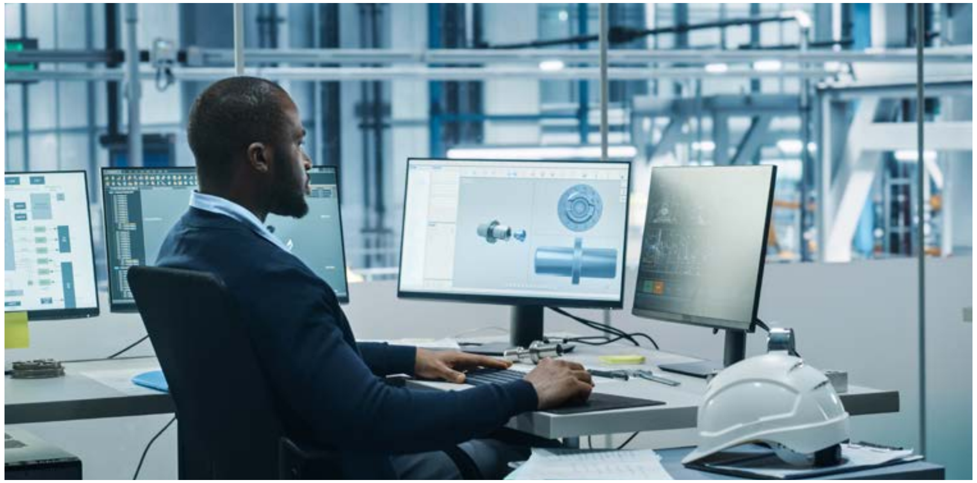
A PRACTICAL EXAMPLE TO AN ICS ASSET INVENTORY

The steps below are an example of a practical approach to an ICS asset inventory that combines both physical and passive network traffic capture.

1. Start by reviewing any already-created network diagrams and engineering documentation such as “as-built documents.”
2. Use an encrypted laptop with at least a basic spreadsheet application to start cataloging and storing ICS asset information during a physical site walk-through, as seen below in Table 1: Sample Asset Inventory Attributes.
3. Augment physical inspection with passive network packet captures on critical network segments that host critical ICS assets by using either a SPAN or mirrored port configuration off a fully managed switch or hardware TAP.
4. Ensure field device configurations are backed up during an incident and securely stored for later comparison to detect whether an unauthorized change occurred and reload trusted configurations and project files (controller logic), if needed.
5. At a minimum, record attributes from the commonly targeted critical assets such as data historians, human machine interfaces (HMIs), PLCs, RTUs, engineering workstations, core network devices, and active safety instrumented systems.

Table 1: Sample Asset Inventory Attributes

Sample Asset Inventory Attributes
Site location
Facility type
Asset type and ID tag
Asset location room, cabinet, rack
Description of asset function for operations
Impact to operations if assets are unavailable
IP and MAC address
Network protocols used
Model, manufacturer, serial number
Firmware version for controllers and related modules, chassis information
Applications installed on critical assets with versions
Assets deemed critical – data historians, HMIs, primary controllers, control system network switches
Project files and configuration (last change date, secure storage location, etc.)
Dependencies – systems, networks, other assets, etc.
Primary and secondary contact for asset



Native tools, discovery protocols, and several packet filters on passively collected traffic captures can be used to safely discover host information and engineering system commands to understand normal control operations.

For example, Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 discovery protocol and can be used to identify network assets and their capabilities.

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

```
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> | sort | uniq
```

ARP is a tool available in common operating systems to reveal ARP cache to show IP and MAC addresses pairings. You can find asset IP and MAC addresses from ARP tables:

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

Device network status can reveal connections and their related IP addresses on an asset:

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

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course provides students with an industrial-grade lab kit, walks them through its operation, and explores attack vectors and defenses of power generation, transmission, and distrubution systems. Students keep the kit for further learning after the course is finished. The course material applies to all ICS critical infrastructure sectors.

MAINTAINING AN ICS ASSET INVENTORY

To maintain a long-term inventory, best practice is that it be in an established digital, searchable, scalable, and secure database. Having a formal inventory in such a database, combined with sector-specific threat intelligence, provides a quick view of the risk surface of vulnerable or targeted assets. It also helps with engineering device lifecycle management, that is, system restarts and recovery procedures that can incorporate identifying system dependencies for streamlined restoration.

The asset inventory is incredibly valuable to engineering asset owners and a target of adversaries. The ICS asset inventory can be safeguarded by storing it in a digital database that is secure, searchable, and scalable.

- **Secure**: Use standard data protection and security practices, including authentication and network segmentation, to protect this sensitive data.
- **Searchable**: Index all fields to enable quick searching across inventories for all sites.
- **Scalable**: Ensure that site inventories can be updated or expanded and backed up regularly.

It is important to securely store field device configuration and production logic (project files) for engineering recovery purposes. In addition, these files should be hashed for easy comparison to detect changes in production and known trusted backup files. The files can be used for the restoration of engineering systems to a trusted restore point in recovery actions.

Industrial control network protocols

ICS security defenders must know and understand the protocols and engineering commands in use at their networks, how they are used, and which ones are used under different facility operating conditions. This requires obtaining and protecting network traffic flow to and from critical devices such as but not limited to, PLCs, HMIs, OPC servers, data historians, RTUs, and safety instrumented systems.

Several tools can be used to obtain and analyze commands on the network in the various ICS protocols. To start, a budget-constrained facility can use common tools such as tshark or Wireshark until such time when a more scalable solution can be deployed.

There are many industrial protocols. Below are several tshark and Wireshark filters to concentrate on when analyzing commands in industrial networks to help with engineering troubleshooting as well as security initiatives across multiple ICS 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 and from HMIs and intelligent electronic devices across several industrial sectors, including the electricity sector and many others.

Career Development Opportunity - ICS456

The SANS ICS456: Essentials for NERC Critical Infrastructure Protection course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and regional entities, provides multiple approaches for identifying and categorizing bulk electric system (BES) Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

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

Application: The BACnet protocol enables communications for building automation and controls for heating ventilation air conditioning systems.

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

Application: OPC can be implemented in several ways to determine the ports used. Observing Distributed Computing Environment/Remote Procedure Call (DCE/RPC) traffic can help identify if OPC is in use. OPC is used to enable communications from different vendor devices in a vendor-neutral way.

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

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

Distributed Network Protocol Version 3 (DNP3)
Port: TCP 20000
tshark/Wireshark filter "dnp3"

Application: DNP3 is commonly seen in water and electricity sectors and occasionally in gas pipeline operations. It is used for communications between control centers and field devices such as RTUs or intelligent electronic devices.

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

Application: The IEC 60870-5-104 protocol is commonly used in the electricity sector to monitor power systems. It can restart devices and modify set points in the field, such as directly interacting with RTUs.

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

Application: IEC 61850 is a communications protocol commonly used for communications with intelligent electronic devices at electricity substations.

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course leverages native protocols in control networks to help safely identify assets, perform threat detection, and understand threats that may be "living off the land."

Defining network security monitoring for ICS

NSM is a human-driven, proactive, and repeatable process of collection, detection, and analysis. While not specific to ICS, NSM excels in control system networks because the environment is usually more static and has far fewer users than in traditional information technology environments. ICS NSM is most effective with an established ICS asset inventory and deep knowledge of ICS protocols for proactive threat detection methods that drive industrial incident response to reduce impacts to operations and the safety of people, the environment, and physical engineering devices.

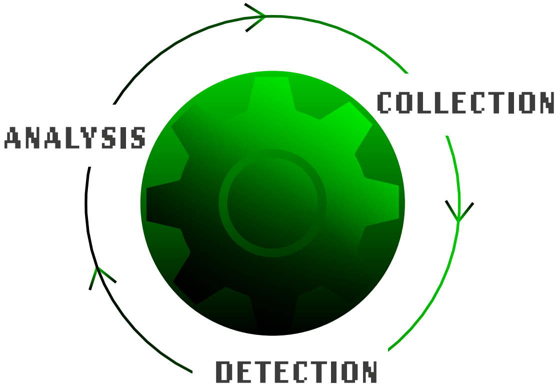


Figure 3: ICS Network Security Monitoring Process

ICS NETWORK SECURITY MONITORING – COLLECTION

A properly segmented ICS network following the SCADA reference architecture from the SANS ICS410 course has enforcement boundaries that naturally create chokepoints for network traffic collection.[2] A properly segmented ICS network also provides control points for containment in industrial incident response. ICS NSM collection should be conducted at levels 0-3 of the Purdue Model for ICS Security at a minimum for full packet captures. This includes the communications to and from the HMIs, PLCs, RTUs, and other intelligent electronic devices. Common network collection points could be on edge or internal zone industrial firewalls or on core control network switches. Fully managed network switches can be used to passively collect data via SPAN configuration. Alternatively, a dedicated hardware TAP device may also be used for network traffic collection. The two main types TAP devices for network-based collections are described below.

[2] Information on SANS ICS410 is available at www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

5-tuple Capture: This consists of five attributes in a TCP/IP network connection:

1. Source IP address
2. Destination IP address
3. Source port
4. Destination port
5. Protocol observed

Full-Packet Capture: This includes the 5-tuple data as well as the full-packet payload of network communications. For example, the query and response data used in ModbusTCP has the industrial commands, function codes, and other artifacts available for security defenders and engineering staff to analyze using this approach. Even files transferred across a network will be present in the packet stream. Full-packet capture can consume significantly more storage space than just capturing 5-tuple data, but it has far more value. Full-packet capture can drive proactive threat detection, inform ICS incident response processes and threat analysis, and assist with networking and engineering troubleshooting.

ICS ASPECT – COLLECTION

Collect the 5-tuple data at a minimum at north/south firewalls at the perimeter of the ICS network(s) to help identify malicious remote connections, network pivoting from IT network into the ICS networks through trusted connections, and adversary command and control (C2) connections.

Collect full-packet captures inside the control network from the ICS DMZ down to Level 1 or 0 of the Purdue model as east/west traffic to ensure industrial protocol commands and data streams are captured for analysis, baselining, and threat detection.

Beyond security events, ICS NSM, also known as ICS network visibility, can uncover general networking and engineering system misconfigurations or errors which improve overall industrial network efficiency, safety, and resilience.

ICS NETWORK SECURITY MONITORING – DETECTION

Network detection is about discovering potentially malicious and/or abnormal activity. These activities include unusual inbound or outbound connections, network events linked to known indicators of compromise (such as IP addresses), and other network anomalies observed through the NSM collection phase that do not align with what is expected on the network from an engineering perspective.

To start network detection in ICS on a limited budget, facilities can leverage sector-specific ICS threat intelligence using freely available tools such as tcpreplay, Snort, Zeek, and Suricata with built-in or added ICS rulesets/dissectors. Known IP addresses associated with attack campaigns can be used in a search across network 5-tuple or full-packet captures. The pseudo rules and logic detailed below can be expanded or changed to suit an organization's control network, tools deployed, and general setup.

ICS ASPECT – DETECTION

An IDS is preferred for threat detection in ICS environments over an intrusion prevention system (IPS). IDS is also preferred to prioritize safety – that is, to reduce false positive detections that could cause legitimate control commands to be blocked if detected by an IPS and that may cause operational and safety disruptions. The NSM Detection phase is primarily about understanding what is "normal" for the industrial operations to be better at spotting "abnormal" activity. For example, with engineering knowledge and through analysis of normal operations, expected function codes, other operations and elements, and anonymous activity can be discovered. Using these tools and filters are a great start when developing an ICS NSM program.

Pseudo rules and Logic:

Replay packet captures against a listening network IDS such as Snort to alert to known threats:

```
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 using ModbusTCP on a network that does not use it:

```
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”;)
```

ICS NETWORK SECURITY MONITORING – ANALYSIS

A triggered detection rule, such as a match on a malicious IP address from ongoing attack campaign, will lead to the NSM Analysis phase. It is important to know which assets on the network are critical for safety and operations. This makes it easier to identify anomalous network connections around critical assets to determine when ICS incident response should be performed. The tshark or Wireshark filters discussed below can be expanded or changed to suit the hunt for malicious network activity.

ICS ASPECT – ANALYSIS

ICS environments have far less connectivity to the Internet and use far fewer encrypted communications than in traditional IT environments. ICS attacks can abuse legitimate engineering software and native industrial control protocols.

Information, assets, protocols, files, and commands from the control network can be discovered and analyzed by the tools and filters below.

Wireshark:

```
Wireshark > Statistics > Endpoints
```

Provides statistics about logical addresses on the network, including the asset IP and MAC addresses. Displays number of packets, total bytes, bytes received and transmitted, and attempts to perform DNS name resolution, which can help with asset identification. Each IP address and associated ports should be recorded and analyzed to identify all active assets for legitimate operation.

Wireshark:

```
Wireshark > Statistics >
Conversations
```

Provides statistics about conversations in the traffic between devices, displayed as IP addresses. Information such as the start, stop, and duration of the conversations is notable. The devices communicating, protocols in use, and their communication pattern should be noted. A single device having conversations with multiple devices could indicate an HMI.

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 in an overall capture. The list should be recorded to determine which protocols are needed and expected for operations. Legitimate protocols could be abused in attack scenarios, so it is important to record and analyze protocol patterns and source and investigate and validate devices sending commands to field devices.

Wireshark:

```
Wireshark > Export Objects >
<type> > Save
```

Can be used to extract files from a packet capture. 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 to develop defensive countermeasures.

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course walks through each phase of the Active Cyber Defense Cycle with indepth hands-on techincal labs to conduct threat detection in control systems.

General network statistics about logical addresses on the network:

```
tshark -qz ip_hosts,tree -r <ICS-Network_file.pcap>
```

Asset names from NetBIOS communications:

```
tshark -Y nbns -T fields -e nbns.name -r <ICS-Network_file.pcap> | sort |
uniq
```

Asset names from DNS that could be assets performing Internet checks:

```
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 -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 -Y ssl -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 -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 -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 -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 -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 -Y bacnet -T fields -e ip.src -e ip.dst -e bacnet.control  -e _ws.col.
Info -r <ICS-Network_file.pcap> | sort | uniq
```

Possible HTTP downloads, including filename and uniform resource identifier (URI):

```
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 -r <ICS-Network_file.pcap> --export-objects http,<OutputDir> | sort |
uniq
```

Export data for analysis – SMB file transfers, including filename and file data:

```
tshark -r <ICS-Network_file.pcap>  --export-objects smb,<OutputDir>
```

Files transferred via server message block (SMB) with remote hostname, account name, file(s) accessed:

```
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>
```

ICS security defenders must know what is normal in the ICS environment, which network protocols are expected in different control system states, and what commands inside ICS protocols can read and change physical outputs in the field.

Set-up of ICS network security monitoring

Two main approaches can be used to ensure NSM collection is established, as follows:

1. Network hardware TAPs
2. Network SPAN configuration

Each approach has pros and cons which should be considered by ICS security and engineering teams before deployment.

Network TAP: This is a purpose-built hardware device installed in-line in a network that copies all network traffic. Its installation requires a network outage and should always be configured to allow traffic to flow through the device in the event of a failure, otherwise it could impede legitimate control network communication. TAP installations in industrial control environments are usually added as a task as part of an engineering maintenance window when operations are scheduled to be down. Figure 4 shows a TAP configuration.

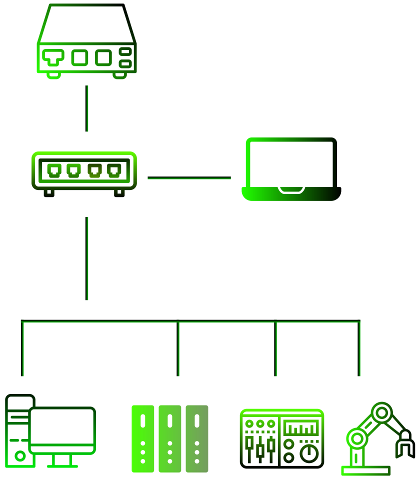


Figure 4: TAP Configuration Example

Network SPAN: Also known as port mirroring, a SPAN configuration may be available on already-deployed fully managed switches in more modern control networks. No network outage is required to implement a SPAN configuration. SPAN configurations can also be phased in based on existing network segments and Virtual LAN configurations to reduce risk during implementation – that is, to ensure that switch CPU and memory can handle the SPAN configuration and traffic load as it copies inbound and outbound packets to its configured mirror port. Figure 5 shows a SPAN configuration.

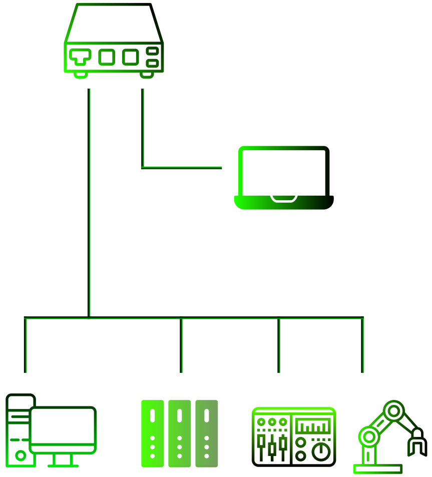


Figure 5: SPAN Configuration Example

TAP vs. SPAN: The decision on which method is best to use for NSM collection in ICS may depend on budget, engineering maintenance schedules, existing technology, and existing and upgradable network architecture. The pros and cons of a hardware TAP and SPAN configuration are illustrated in the table below.

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course walks through each phase of the Active Cyber Defense Cycle with indepth hands-on techincal labs to perform ICS network monitoring and prepare for incident response.

Table 2: TAP and SPAN Pros and Cons

NSM Collection Method	Pros	Cons
TAP Hardware	Capture also includes network errors – malformed packets, etc. Dedicated hardware – TAP is more challenging to compromise than a switch SPAN configuration	ICS network outage required Additional hardware required
SPAN Configuration	Deploys on existing fully managed switches using a 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 fully managed 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. The minor port is port 2, where bi-directional traffic is copied, thus creating the network collection needed to perform effective detection. To be most effective, data should first be collected from critical segments that see control system traffic and engineering commands around critical assets. Once a threat is found, it will lead to ICS incident response.

```
# monitor session 1 source interface gigabitethernet1/1 both

# monitor session 1 destination interface gigabitethernet1/2

# show monitor all
```

ICS network security monitoring in practice

ICS Network Security Monitoring Collection Platform

ICS NSM collection should first be implemented in phases around the most critical and vulnerable ICS/OT assets in the most important IP-connected engineering networks. Collection should be scaled one network segment at a time.

Collected data should be sifted for indicators of compromise starting with IP addresses. Sector-specific threat intel can be used 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, the no-cost Linux Security Onion distribution on a laptop with external storage and built-in tools such as tcpdump or Wireshark, can be used to start ICS NSM collection with a network card in promiscuous mode. For detection and analysis, Wireshark, which has several built-in packet dissectors for common industrial protocols, is extremely helpful in determining the assets, protocols in use, and communication patterns in an industrial environment.

Career Development Opportunity - ICS515

SANS ICS515: ICS Visibility, Detection, and Response is a technical course for ICS incident response team leaders, ICS/OT and engineering staff, IT security professionals, and Security Operations Center leaders and analysts. Students execute every step of the active cyber defense cycle and complete the course with an ICS-specific challenge on the final day.

Passive ICS Network Traffic Capture Window

Passive control network capture times could be as short as several hours for point-in-time assessments or threat hunts. This depends on the collection objective, storage, size of the control environment, and current engineering operating states. Point-in-time assessment for full-packet captures is commonly between 1 and 24 hours.

Control System Network Capture Considerations

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 occur during the industrial process start-up and normal operations.

The NSM collection, detection, and analysis phases should be started and repeated while the above methods are applied across the three phases to prioritize the safety and reliability of ICS operations. Deeper engineering knowledge is required for more specific ICS protection. High confidence indicator of compromise matches and the discovery of anomalous network patterns will call industrial incident response steps into action.

STAGE 1: ICS THREAT DETECTION CONCEPTS FOR 5-TUPLE

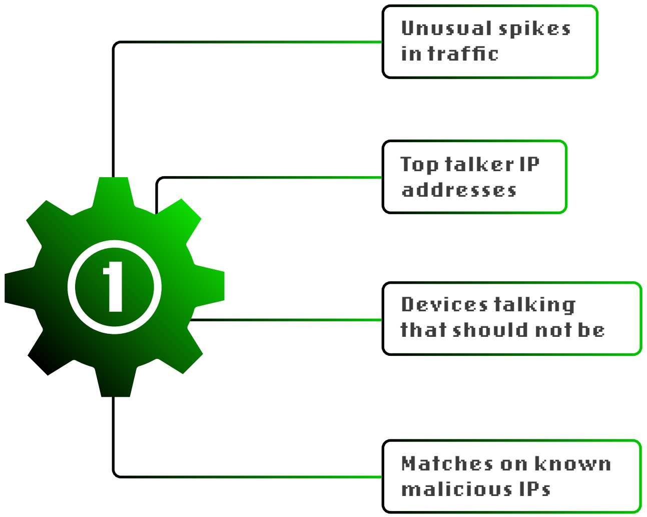

1
Unusual spikes in traffic
Top talker IP addresses
Devices talking that should not be
Matches on known malicious IPs

Figure 6: Stage 1- ICS Threat Detection Concepts for 5-Tuple

STAGE 2: ICS THREAT DETECTION CONCEPTS FOR FULL-CAPTURE PACKET ANALYSIS

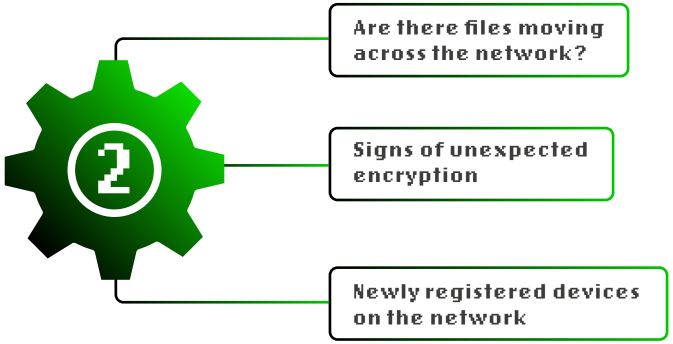

2
Are there files moving across the network?
Signs of unexpected encryption
Newly registered devices on the network

Figure 7: Stage 2- ICS Threat Detection Concepts for Full-Capture Packet Analysis

STAGE 3: ICS THREAT DETECTION BASED ON ICS BEHAVIOR

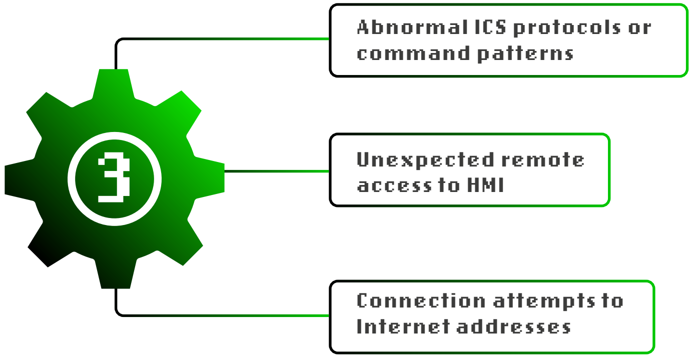

3
Abnormal ICS protocols or command patterns
Unexpected remote access to HMI
Connection attempts to Internet addresses

Figure 8: Stage 3 - ICS Threat Detection Based on ICS Behavior

Compatible tools for ICS network security monitoring

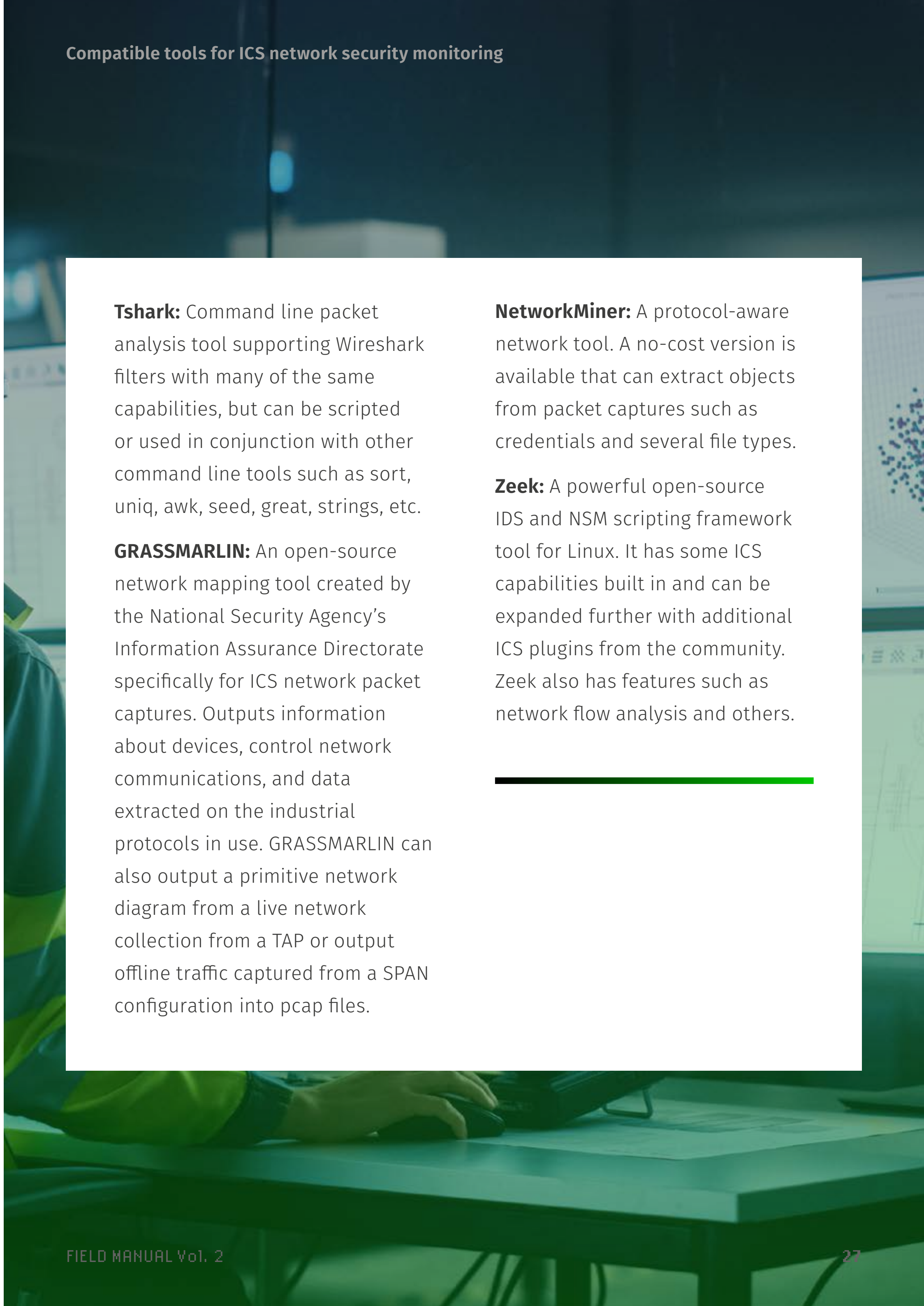
Many low-cost or no-cost open-source tools are available to help organizations start their ICS security program journey and to mature and deploy ICS NSM capabilities. Specific ICS-trained defenders can leverage several tools that have built-in or ICS-specific features or plugins – a good place to start when there is a limited budget.

Security Onion: Open-source Linux platform designed for intrusion detection, network security monitoring, and event log management and analysis, with many supporting tools built in.

Snort: IDS with many ICS-specific pre-processes built in to help detect ICS vulnerabilities and attack traffic in control networks. Newly created ICS plugins are often 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 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, but can be scripted or used in conjunction with other command line tools such as sort, uniq, awk, seed, great, strings, etc.

GRASSMARLIN: An open-source network mapping tool created by the National Security Agency's Information Assurance Directorate specifically for ICS network packet captures. Outputs information about devices, control network communications, and data extracted on the industrial protocols in use. GRASSMARLIN can also output a primitive network diagram from a live network collection from a TAP or output 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: A powerful open-source IDS and NSM scripting framework 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.

The active cyber defense cycle

The repeatable active cyber defense cycle guides a team through proactive monitoring as a best practice in today's ICS threat landscape. The cycle has five phases, as shown in Figure 9.

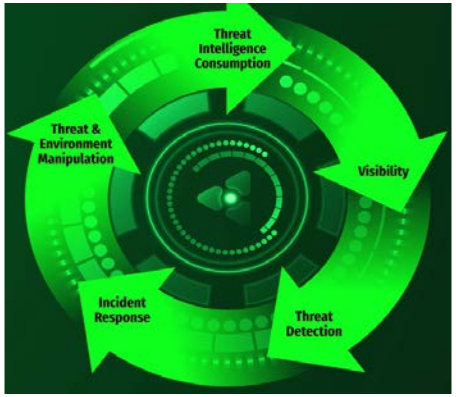

Threat Intelligence Consumption
Threat & Environment Manipulation
Visibility
Incident Response
Threat Detection

Figure 9: The Active Cyber Defense Cycle
https://www.sans.org/white-papers/36240/

1. **Threat Intelligence Consumption:** Cyber threat intel is refined information with context on cyber threats and threat groups that defenders can leverage to detect, scope, or prevent the same or similar attacks previously observed.

2. **Visibility:** Increasing visibility can enhance technical and situational awareness of control system traffic and security. This means having a formal asset inventory and at least a passive view of the ICS network, and using technology that can dissect and properly interpret specific industrial protocols in network traffic streams.

3. **Threat Detection:** Detecting threats requires the capability to leverage technology that sifts through data for malicious signs of attack attempts or intruder entry.

4. **Incident Response:** Successful incident response requires being prepared to execute quick triage and adapt incident response steps specific to control systems while maintaining safety.

5. **Threat and Environment Manipulation:** To make the environment less habitable for threat actors, defenders need to know how to change the threat during the attack or change the control system. A threat is defined as a malware capability introduced by a threat actor or as human threat actors using legitimate operational software or protocols with malicious intent to cause negative impacts.

Career Development Opportunity - ICS515

The SANS ICS515: ICS Visibility, Detection, and Response course and the related GIAC Response and Industrial Defense (GRID) certification are a must-have for ICS/SCADA/OT and IT professionals who want to demonstrate their knowledge of active cyber defense strategies specific to industrial control system networks and environments. It is common for professionals working or looking to work or consult in these areas to earn their GRID certification.

NSM excels in control system environments due to the more static nature of ICS networks compared with IT enterprise networks. The active cyber defense cycle makes clear the benefits of ICS NSM in today's threat landscape. It leverages ICS NSM by increasing knowledge of the control system, collecting data, analyzing data for threats, and executing ICS-specific incident response. However, the active cyber defense cycle and ICS NSM – what can be called the "network visibility" of control environments – are not only about security. They also directly support engineering tasks such as communication, command, and integration troubleshooting, all of which support safety for facilities and their workers.

ICS NSM is especially important in the case of adversaries living off the land, where it is unlikely that antivirus agents, even allowing for listing features designed specifically for ICS, would detect the abuse of legitimate control system functions, including the abuse of legitimate ICS/OT network protocols and engineering software.

Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course empowers new and established ICS security managers from all areas to understand the differences between IT and ICS/OT, prioritize safety, build and maintain strong relationships, build teams, and effectively manage ICS/OT cyber risk.

Epilogue to Volume 2

Adversaries continue to evolve their attack tradecraft using traditional IT malware and extending the attack range with knowledge of how to abuse ICS systems. This “living off the land” attack approach has them abusing native commands and software. In their wake, adversaries leave serious financial, brand, and operational impacts, with potential catastrophic consequences for operating environments, the safety of people, cities, regions, and countries who run and rely on them.

ICS security managers looking to improve ICS risk management and the resilience of their ICS security program must first establish an official asset inventory with the methodologies described in this manual. They must then leverage and mature the program to an active defense position. The objective is to ensure that security controls are in place specifically for industrial control systems, with ICS network and engineering device visibility. Security team members must possess the ICS-knowledge required for rapid ICS incident triage and the recovery of engineering devices to trusted restore points.

ICS security defenders looking to improve tactical ICS security must obtain and continue to grow their knowledge of cybersecurity and engineering operations (including protocols and commands), while prioritizing safety and administrating modern security tools specifically designed or tuned for ICS environments. A main focus should be on performing the repeatable steps of the active cyber defense cycle while leveraging ICS network visibility, packet captures and analysis, and hunt for threats proactively in the network.

ICS facilities owners and operators will do well to consider these top takeaways to kick-start or mature their ICS cybersecurity program:

- Continue to prioritize safety as #1
- Embrace ICS and IT security differences
- Establish a secure and searchable ICS asset Inventory
- Enable ICS network security monitoring
- Deploy the Active Cyber Defense Cycle for technical teams
- Align priorities against the Sliding Scale of Cyber Security

Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers two-day course prepares new and experienced managers and leaders responsible for ICS/OT security. Students complete many in-class leadership drills and real-world management-level ICS security scenarios in an online leadership simulation game across both days.

SANS ICS Curriculum

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of industrial control systems. The initiative equips security professionals and control system engineers with the security awareness, work-specific knowledge, and hands-on technical skills they need to secure automation and control system technology.

ICS410: ICS/SCADA Security Essentials

This course provides an understanding of ICS components, purposes, deployments, significant drivers, and constraints. It includes hands-on lab learning experiences to control system attack surfaces, methods, and tools.

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

ICS515: ICS Visibility, Detection, and Response

This course will help you deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/

Career Development Opportunity - ICS GIAC Certifications

- ICS attackers are honing their skills and plotting their attacks. We can up our defensive skills to counter them and protect critical infrastructure that supports our modern way of life.

- ICS GIAC certified professionals have demonstrated they have the skills to help protect critical infrastructure from a technical and/ or strategic level.

ICS456: Essentials for NERC Critical Infrastructure Protection

This course empowers students with knowledge of the “what” and the “how” of NERC’s Critical Infrastructure Standards. It provides multiple approaches to identify and categorize BES Cyber Systems and helps determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies with a balanced practitioner approach to both cybersecurity benefits and regulatory compliance.

https://www.sans.org/cyber-security-courses/essentials-for-nerc-critical-infrastructure-protection/

ICS612: ICS Cybersecurity In-depth

This course provides advanced coverage of security concepts primarily driven by applied learning with hands-on labs. The in-classroom environment simulates a real-world factory, and the labs move students through a variety of exercises that demonstrate how an attacker can compromise an ICS environment and how defenders can better secure and manage that environment.

https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth/

ICS418: ICS Security Essentials for Managers

This course fills the identified gap among leaders working across critical infrastructure and operational technology environments. It equips ICS managers with the experience and tools to address business and industry pressures. It positions ICS leaders to manage cyber threats and defenses while also addressing the safety and reliability of ICS operations. Both new and established ICS security managers will leave the course with a firm understanding of the drivers and constraints that exist in cyber-physical environments, as well as a nuanced understanding of how to manage the people, processes, and technologies in their organizations.

https://www.sans.org/cyber-security-courses/ics-security-essentials-managers/