6. ICS Incident Response (IR) Objectives

Successful ICS IR requires a clear understanding of roles, responsibilities, physical safety, the engineering process, network visibility, industrial protocols, and forensics capabilities. It also requires having a defensible cyber position. Adapt traditional IR steps to suit industrial control environments. Consider:

- Acquiring forensics data from key ICS assets
- Quickly triaging to understand the threat
- Executing the Defensible Cyber Position
- Containing threats while running operations
- Eradicating when its safe for operations
- Any reliance on external vendors and IT
- Applying lessons learned to the ICS IR Plan
- Exercising ICS IR tabletops regularly
- Legacy devices – connectivity and isolation

7. ICS IR Roles and Testing the Plan

Test the ICS IR Plan to validate controls and processes, and communicate roles across multiple teams – Safety, Compliance, Engineering, Operations, Networks, Legal, etc. Assign key roles for IR action:

Incident Response Director - Interfaces with leadership on IR updates, resources, impacts, business, and safety options.

Lead Responder - Guides IR personnel, quick triage, timeline analysis; advises Incident Response Director on available actions to reduce impact to safety and operations.

Incident Handlers - Cybersecurity, ICS field, and technical personnel required to perform evidence acquisition and scope threat, and to make system and asset changes.

Fire & Security, Safety & Law Enforcement – Teams prepared for physical first aid, emergency response, evacuation strategy for the site, and effects beyond the site.

8. ICS IR Jump Bag

Use these tools to, acquire forensics data from critical ICS assets and conduct triage to understand the threat(s) and operational impacts. Present response options to facility owners and stakeholders that will inform business and safety decisions to minimize loss. Essential ICS Incident Response Jump Bag items are:

- Data acquisition tools (prioritize memory)
- Laptops with Security Onion, REMnux, SIFT
- Malware analysis tools (static, automated)
- Baseline images of critical ICS assets
- Hashes of field device logic/config files
- Log, packet analysis, and timeline tools
- Approved digital camera (no photo metadata)
- Hardcopy ICS IR playbooks, network diagrams
- Network/converter cables (USB <-> Serial)
- Contacts: safety, engineering, integrators
- Out of band communications, handheld radios
- Forensically clean USBs, external drives
- Safety Personal Protective Equipment
- Site physical safety training certificates

Store equipment in rolling protective cases at critical sites or deploy the jump bag with the ICS IR team as they travel to sites to conduct incident response.

9. ICS IR – In Practice

Use indicator "hits" to scope infection. Compare hashes of production/baselined configs to detect field device tampering. Conduct static/automated malware analysis to determine technical impacts. Deploy countermeasures while maintaining safety; fighting through attacks by enabling a cyber defensible position, firewall changes, network isolation. Shift ICS to manual mode, block C2 connections. Disable remote access – contain/eradicate. Recover and apply lessons learned. Correct gaps in evidence acquisition and security controls, and add NSM capabilities, etc. Threats could be malware or human adversaries.

Industrial Network Security Monitoring & Incident Response Cheat Sheet

SANS ICS
ics.sans.org

By Dean Parsons
dparsons@sans.org

This tri-fold cheat sheet provides guidance for Industrial Control System (ICS) Network Security Monitoring (NSM), and Incident Response (IR) for control system environments.

Unlike IT incidents, ICS incidents need to consider potential loss or damage of physical property or engineering assets, as well as safety risks to people and the environment. ICS IR will be a joint effort with security incident responders, engineers, operators, and network architects.

How to Use This Cheat Sheet

This cheat sheet is split into two main sections covering the setup, deployment, and use of ICS NSM. It informs actions for ICS IR while supporting the safety of operations.

1. **ICS Network Security Monitoring:** Setup, Collection, Detection, Analysis, ICS NSM in Practice.
2. **ICS Cyber Security Incident Response:** ICS IR Objectives, Roles/Responsibilities, ICS IR Jump Bag, ICS IR Practice and considerations beyond IT.

1. Network Security Monitoring – Setup

NSM is a human driven, proactive, repeatable process of Collection, Detection, and Analysis. NSM excels in ICS environments because they are more static and host fewer users than IT environments. Below are two methods to ensure NSM Collection is established. Having an ICS asset inventory prior to NSM is ideal.

Network TAP - **Hardware device in-line in the ICS network that copies network traffic. Typically requires a network outage to install. Always ensure it fails open and allows traffic to flow through in the event of device failure, otherwise it could interrupt legitimate control operations.**

Network SPAN - **May be available on existing managed switches. No network outage required to implement. May miss or drop mirrored packets if switch is overloaded. Phase VLANs, network segments, into the SPAN configuration one or two at a time to ensure switch CPU and memory can manage the load.**

Commands differ across switch manufacturers. Pseudo command to create a local SPAN session 1 for monitoring bi-directional traffic from port 1 to port 2, and show change is applied:

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

# monitor session 1 destination interface
gigabitethernet1/2

# show monitor all
```

You can collect network data with a Security Onion laptop using Wireshark, tcpdump, etc. Beyond just security events, ICS NSM can uncover fixes for networking and engineering misconfigurations.

2. Network Security Monitoring – Collection

Collection – Align with the Purdue architecture to establish enforcement boundaries, naturally creating chokepoints for NSM data collection and doubling as control points for contamination. Collect ICS traffic at least at Purdue Levels 0-3. Use fully managed switches to passively collect data via SPAN, or TAP. Capture at least 5-tuple IPFIX data, but full packet capture is ideal.

5-tuple IPFIX capture – **Only src and dst IP, src and dst port, and protocol.**

Full Packet Capture - **Entire packet content. 5-tuple IPFIX and full payload. Can extract files, malware samples, etc. Consumes significantly more storage than IPFIX alone.**

3. Network Security Monitoring – Detection

Detection – Leverage threat intel from your ICS sector, tcpreplay, an IDS with ICS rulesets, and use these pseudocode rules to start network detection.

Replay packet capture files against a Network IDS:

```
sudo tcpreplay --intf1=<nic_for_ids> --
mbps=500 potentially_evil.pcap
```

Alert on communications to PLC that is not HMI:

```
alert tcp !$Modbus_HMI any -> $Modbus_PLC
any (msg: "TCP comms to PLC but not HMI";)
```

Alert on possible recon scan or mapping attack:

```
alert tcp any any -> any 502 (msg: "Scan or
usage of ModbusTCP on network without it";)
```

Alert on possible connection to known evil C2:

```
alert tcp any any -> <evil_C2_ip> any (msg:
"Connection attempt to known evil C2 IP";)
```

4. Network Security Monitoring – Analysis

Analysis - Using "hits" from Detection, Analysis helps determine when ICS IR is needed. Start with no-cost tools to extract suspicious files from network captures. File hashes can be searched across malware databases or files can be executed in isolated malware analysis sandboxes to determine threat behaviors for quick defense countermeasures.

Wireshark – Has many ICS protocol dissectors built-in. Extract files: File -> Export Objects -> <type> -> Save

NetworkMiner – Categorizes and extracts data for quick analysis – images, files, web sessions, SSL keys, passwords, etc.

5. ICS NSM – In Practice

Phase in NSM Collection around critical and most vulnerable ICS assets first; historians, field devices, HMIs, engineering workstations, etc., one segment at a time. Sift through collected data for indicators of compromise starting with IP addresses.

Analyze network 5-tuple data first for:
- **Matches of known malicious Ips**
- **Top talking IP addresses**
- **Devices talking that did not previously**
- **Network oddities - spikes in traffic etc.**

Analyze deep packet network data for:
- **Abnormal ICS protocol patterns/commands**
- **Signs of unexpected encryption**
- **Outbound Internet or odd DNS requests**
- **Newly registered devices on the network**

Repeat NSM Collection, Detection, Analysis steps. High-confidence indicators of compromise matches and anomalies will trigger ICS incident response.