5. Spreadsheet, Laptop Stand, Network Diagrams

Start by reviewing network diagrams. Use an encrypted laptop with at least a basic spreadsheet application to start storing your ICS asset information. At a minimum, capture these attributes for commonly targeted assets such as Data Historians, HMI, PLCs, Engineering Workstations, core network devices and Safety Instrumented Systems (SIS):

- Site Name, 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
- Model/manufacturer, serial number
- Firmware version
- Applications installed and versions

6. Follow Up with Traffic Analysis

Maintenance windows and safety risks can prevent physical inspection of some assets. Augment the physical inspection inventory with passive network traffic capture (will require coordination and approval from operations staff and a configured SPAN with a network security monitoring platform such as Security Onion). Common capture times range from 2-24 hours. Identify critical assets through packet analysis and by observing ICS protocol traffic patterns. Use features in free tools like Wireshark to help:

```
Wireshark > Statistics > Endpoints
Wireshark > Statistics > Protocol Hierarchy
Wireshark > Statistics > Conversations
```

7. Storing Asset Inventory Back at the Office

The inventory is incredibly valuable. When back at the office store inventory updates in a database that is:

Scalable - 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 searches across inventories gathered when used in conjunction with threat intelligence or vulnerability information.

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

Asset Inventory for ICS Defense

Use threat intel to drive searches across an established inventory database for vulnerabilities and targeted assets for proactive defense changes. Targeted assets:

Data Historian – This is a database that stores operational process records. Can be abused to pivot from a compromised asset in IT to one in the ICS network(s).

Engineering Workstation - The EW has access to software to program and change PLCs 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 review and control the process.

Programmable Logic Controllers – PLCs connect the physical hardware in the real world and run logic code to read the state or change the state of the engineered process.

ICS Site Visit Plan v0.1

SANS ICS
ics.sans.org

By Dean Parsons
dparsons@sans.org

This tri-fold cheat sheet will help maximize efforts to identify critical assets during on-site Industrial Control System (ICS) visits, promote ICS security awareness, and facilitate a smooth ICS cyber incident response process.

Use this guide to plan ICS site visits, prepare for cybersecurity and safety discussions, ethical hacks of the physical security perimeter, and to establish an ICS asset inventory that can be put it into action for proactive defense.

How to Use This Sheet

Consider these seven points to ensure that industrial control system security supports the safety and reliability of operations as you plan to visit site(s).

1. OSINT for ICS Defenders
2. Coordinate with Safety & Security
3. Ethically Hacking the Physical Perimeter
4. Plant Floor Cybersecurity Discussions
5. Spreadsheet App, Laptop Stand, Network Diagrams
6. Follow Up with Traffic Analysis
7. Storing Asset Inventory Back at the Office

1. OSINT for ICS Defenders

While often overlooked, an open-source intelligence (OSINT) exercise provides a starting point to understand an organization’s information attack space, does not introduce disruption or risk to industrial operations and is not detectable by ICS defenders.

An OSINT exercise can reveal an organization’s Internet-connected devices, remote access services, open ports, and protocols in use. This information can be pieced together to help adversaries build an attack against a target ranging from a spear phishing attack to the creation or use of an exploit targeting a vulnerability.

ICS defenders should at least know what information is publicly available about their organization through common search engines such as Google. They should also know which Internet-connected devices are deployed from search results from Shodan or similar tools. It is practical to assume that adversaries already know whatever was found from an OSINT exercise. Common Shodan website filters:

```
Search organization IP range: net:x.x.x.x/y
Search by organization name: org:”name”
Search by IP Address: x.x.x.x
Search by city: city:”name of city”
Search by webpage title: title:”text here”
Search for common remote access: port:"3389"
Common ICS Port: BacNET port:"47808"
Common ICS Port: Modbus port:”502"
Common ICS Port: EtherNet/IP port:”44818"
```

Ensure that Internet-connected assets are removed where feasible and that remote access has secure multi-factor authentication with monitoring and auditing in place. Verify with the key stakeholders and applicable on-site teams before changing anything.

2. Coordinate with Safety & Security Teams

Establish and maintain relationships with fire & safety, physical security, and engineering teams before arriving to the site. These teams know just about everything about the facilities – the location of physical assets, how to navigate the site, network designs, and critical assets. Your team may have to rely on these teams to help you throughout the ICS incident response process going forward.

Site safety is always going to be top of mind, even above cybersecurity. Follow the lead of the safety team and the safety protocols to ensure that you and your team remain physically safe. This also means wearing your personal protective equipment (PPE). Most sites require that you have completed safety training and show certificates of completion before entering a site.

3. Ethically Hack the Physical Security Perimeter

When arriving at the site, there’s always an opportunity to audit physical security controls.

This can be done by observing authentication processes, starting with the front gate. Wait to show a badge until it is requested, document tailgating observations, and look for unlocked doors, doors being propped open, fences with gaps, etc., all while keeping safety as the highest priority.

Conduct passive wireless sweeps looking for rogue access points and/or unsecured wireless settings.

Always seek documented approvals with management for ethical hacking exercises of this nature before attempting them.

4. Plant Floor Cybersecurity Discussions

There is a great benefit in organizing direct discussions in regard to ICS security and safety to occur on the plant floor or in the facility as this allows for direct observations and provides operational context for the environment in which the digital assets are located. However, some operating environments may have prohibitive noise, safety or access limitations that require the discussions to happen elsewhere. Include the process engineers, field technicians, programmers, operators, and managers.

Cybersecurity staff need to know how the physical processes and plant operate, and which systems are critical to operations and safety.

Walk the teams through industry case studies such as CRASHOVERRIDE, TRISIS, HAVEX, STUXNET, etc..

Start a discussion around what an impactful event would be for your environment and how it could be achieved. The individuals who operate your facilities, certainly have thoughts and experiences on how it has or could fail.

Leverage the physical engineering safety culture by drawing parallels between physical safety and cyber “safety” events and highlight the cyber defense safeguards that are in place to ensure the safety and reliability of engineering operations.

Reword cyber ‘security ’to cyber ‘safety’ in security awareness memos.