Building an Effective ICS/OT Security Monitoring and Defense Program

Kai Thomsen, Dragos Inc
whoami

- Director, International Incident Response Services at Dragos Inc.

- 22+ years of DFIR experience in IT, ICS/OT, and I have done a little IR around vehicles 😊

- Certified SANS Instructor in the ICS curriculum
Safeguarding Civilization

Built For Practitioners, By Practitioners
The largest & most experienced team of ICS security specialists make the best technology.

500+ EMPLOYEES
300+ CUSTOMERS
20 COUNTRIES
11 INDUSTRY VERTICALS

HQ | Hanover, MD
REGIONAL | US & Canada, Australia-New Zealand, Gulf Coast, UK/Europe

- ELECTRIC
- OIL & GAS
- MANUFACTURING
- BLDG AUTO SYS
- CHEMICAL
- GOVERNMENT
- WATER
- FOOD & BEV
- MINING
- TRANSPORTATION
- PHARMACEUTICAL
Agenda

• Short ICS/OT Intro
• IT <-> ICS Differences
• Examples of ICS/OT Cyber Attacks
• ICS IR Case Study
• Active Cyber Defense Cycle
  • Threat Intelligence
  • Visibility
  • Detection
  • Incident Response
  • Threat & Environment Manipulation
• Collection Management Frameworks
• Threat Hunting
Intro into ICS/OT
Some Common Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT</td>
<td>Operational Technology</td>
<td>IT Systems that control industrial or physical processes</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
<td>Specialized computing equipment that directly manipulate and/or control</td>
</tr>
<tr>
<td>IACS</td>
<td>Industrial Automation and Control Systems</td>
<td>Same as above, this term is more commonly used in Oil &amp; Gas and Offshore</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
<td>A computer that is ruggedized and adapted for industrial control.</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
<td>More advanced version of a PLC that interfaces with DCS or SCADA systems</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
<td>Controllers for power system equipment in the electric industry</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
<td>Combination of OT and ICS to enable realtime control industrial processes</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
<td>Even larger scale visualization and control of industrial processes, not realtime</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
<td>Your fancy operations UX</td>
</tr>
<tr>
<td>EWS</td>
<td>Engineering Workstation</td>
<td>The computers used to program, configure, and update control systems</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System</td>
<td>Dedicated controllers to maintain safety of industrial processes</td>
</tr>
</tbody>
</table>
What is OT/ICS?
IT + Physics
The Mission is Different

Priorities are:
1. Safety & Reliability of Operations
2. Business
3. Everything else
Safety & Reliability

In ICS environments we are dealing with hard real-time requirements, proprietary systems that often must not be rebooted during plant operation and equipment lifecycles of 10-30+ years. Interaction with these environments requires understanding the procedures, regulations, and risks involved. Physical impact can often lead to huge financial losses, environmental damage or even danger to loss of limb or life.
The Purdue Model

- The Purdue Model (PERA, Purdue Enterprise Reference Architecture) is a reference architecture that can model the enterprise in multiple layers and in multiple stages of the architectural life cycle.
- This was not (strictly) built with security in mind, but is a good model to understand zoning and different requirements.
- Oftentimes, especially in manufacturing, this is rather conceptual and zoning recommendations are not strictly followed.
What this Means for ICS/OT Security

**UNDERSTAND OT**
ICS incident responders must be able to effectively communicate with OT teams. Ultimately only OT staff should be directly interacting with ICS equipment under guidance of experienced ICS incident responders. Adversaries are aiming for physical impact. Incident responders must ensure they don’t cause it unintentionally.

**SAFETY PROCEDURES**
For certain ICS environments, mandatory safety trainings & certifications are required to be allowed to enter. ICS incident responders must meet these requirements and know how to take care of themselves and their peers.

**PROPRIETARY HARD-AND SOFTWARE**
In ICS it’s not only about Windows systems. ICS equipment, software, and network protocols are highly proprietary. To understand the potential impact of an intrusion to the plant process, incident responders need to have deep knowledge about ICS equipment and protocols.
Working in Live Environments

- In many scenarios, ICS incident responders will be engaging in live environments.
- Plant operators may choose to defer shutdown procedures to scheduled windows or determine the risk of an intrusion is lower than the operational impact of shutdown.
- Even if a plant is shut down, various systems are still running to ensure a safe state. Causing these systems to malfunction during an investigation might lead to hazardous situations.
Short Interlude
Read this book!

- We live in - very - volatile times
- Given our current posture, we will hardly be able to avert serious incidents
- Organizations, companies, and individuals need to learn to adapt to living through „right of boom“
Current Challenges in ICS/OT

Cultural:
• Many CISOs do not understand IT <> ICS/OT differences
• IT Security requirements clash with Safety regs and regulations
• IT and OT staff often do not understand each other
• „Our OT environment is air-gapped“
  • What they believe this means: there is no connection between Internet and OT
  • What it actually means: you cannot reach OT directly from the Internet

Technical/Procedural:
• Standards are 90% prevention focused, detection & response capabilities are afterthoughts at best
• Lack of ICS/OT aware visibility
• No dedicated ICS/OT Incident Response Plan
• Plans don’t get exercised
Examples of ICS Cyber Attacks
June 2010: A malware called “Stuxnet” affects the uranium enrichment facility in Natanz, Iran, damaging ~2300 centrifuges. In 2015, the New York Times publishes a comprehensive article, attributing the attack to the USA and Israel, conducted under the code name “Operation Olympic Games”

December 2015: a cyber attack against 3 electric power distribution substations in central Ukraine leaves ~225000 people without electricity for ~9 hours. The damage to the SCADA systems took about 9 months to fix

December 2016: a cyber attack against an electric power distribution substation north of Kiev leaves a few thousand people without power for less than an hour. The intended impact of the attack was much worse. Due to errors by the attacker, the impact was low
August 2017: a refinery in Saudi Arabia, belonging to Petro Rabigh, goes into emergency shutdown. Incident responders discover a malware installed on a Safety System in the refinery that Dragos names TRISIS. The attackers had also manipulated a highly volatile petrochemical process. This would have resulted in a large explosion, potentially causing a huge number of fatalities, if not for one small programming error by the attacker.

Source: https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/
Hybrid Warfare
Because there is no Cyberwar

Satellite cyber attack paralyzes 11GW of German wind turbines

The communication channels affected are also used by photovoltaic systems.

MARCH 1, 2022 MARIAN WILLUHN

In the event of a communication breakdown, solar and wind power plants automatically switch to a kind of “autopilot.”

Ukraine Thwarts Cyberattack on Electric Grid, Officials Say

The attack, which was set for last Friday, used software similar to the ‘Industroyer’ code used in a 2016 hack of Kyiv’s grid, experts noted.

Downtown Mariupol, Russia has launched devastating assaults on Ukraine, but major cyber disruptions widely anticipated by analysts haven't materialized.
The 5 Critical Controls
Because you need to focus

1. Defensible Architecture
2. ICS/OT Aware Monitoring
3. ICS Incident Response Plan
4. Key Vulnerability Management
5. Multi-Factor Remote Access Authentication
The 5 Critical Controls

Because you need to focus

1. Defensible Architecture
2. ICS/OT Aware Monitoring
3. ICS Incident Response Plan
4. Key Vulnerability Management
5. Multi-Factor Remote Access Authentication

We will focus on these
Case Study: The Ghost in the Machine
Scenario

- In February 2021, dead of the night, somewhere in the Middle of Nowhere (TM), in North America, the gas turbines at a peak power generation site, turn on and idle
- The SCADA operations had not issued a START command
- There was no need for peak electric power generation
- The local operations team had not issued a START command
- The operator activated their ICS Incident Response Retainer and Dragos responders arrived at the site within 8 hours
- There was no OT (or IT) monitoring solution in place
- The firewall had not recorded any incoming connections
- No one from the local operations crew had entered the control shed next to the turbine & generator hall
How would you investigate?
Who said you can just dive right in?
Remember

Safety & Reliability come first!

You will go exactly nowhere without proper PPE

Arc Flash Hazards

Arc flash is a hazard that is inherent to almost every sector of the power generation industry. Past facts about Arc Flash:

- An Arc Flash is an energy discharge that burns肌肤 when an arc fault occurs in an electric circuit
- Electrical arcs produce arcs of the highest temperature known to occur on earth
- Burns from arc flashes can be severe and sometimes fatal
- Arc flashes are often reported incorrectly as faiilt injuries due to the flash causing workers to fall from power lines and other elevated equipment

Without these hazards we would simply allow anyone outside of the power generation industry to work in the field. These jobs go with the territory. Authorities responsible for safety have been complaining about these dangers. Working proper PPE is vital. Flame resistant clothing with full body coverage will keep workers protected and reduce the impact of injuries caused by an arc flash incident. Check out the NSA for additional information about arc flash and the proper arc flash PPE.

Working as we typically do in wet weather, solar substrates, or in a hazardous environment can all exacerbate the risk of an arc flash incident, even when equipment is considered no-energy class. Insulating and glove work on any equipment may have impractical factors that could lead to potential arc flash incidents. Providing accessible and comfortable PPE options is essential for protecting workers in these unique environments.

Click here for more information on why proper arc flash PPE is so important. Individual workers to improve in non-chalant ways.

Arc Flash PPE

Personal protective equipment is the last line of defense for workers in any industry with industrial risks like arc flash hazards. Assuming that substitutions, replacements, and provide are always correlated while working on them, wearing proper arc flash PPE can prevent an arc flash incident from causing potentially serious and fatal injuries.

Natural safety apparel is covered clothing and arc flash PPE is by far the best and most cost-effective. This means the PPE should be adapted to the needs of the industry and should not be used as a full-body arc flash PPE, which includes arc flash suits and headgear. Coverall and gloves is a practical solution to the arc flash incident. The same is true for full body arc flash PPE, which includes arc flash suits and headgear. Coverall and gloves is a practical solution to the arc flash incident. The same is true for full body arc flash PPE, which includes arc flash suits and headgear. Coverall and gloves is a practical solution to the arc flash incident. The same is true for full body arc flash PPE, which includes arc flash suits and headgear.

Electric Shock Hazard

Power generation equipment's electrical systems to create the source of power, which powers workers comfortable. The risk of electric shock. Auto PPE is essential before the matter the safe, PPE has many significant risks involved in not high-voltage equipment, power generation workers are advised to choose PPE that will account for protection against electrical shock.

When in doubt, always wear PPE! Equipment in certain parts that may be dangerous should be handled with caution and the proper PPE should be worn. PPE should be worn even if the worker is too far away from the hazard to ensure that equipment is not damaged. Arc flashes and electric shocks can affect workers without direct contact. PPE such as gloves or only approved test during these tests.

Rubber Voltage Gloves

For insulated voltage gloves are on the proper PPE to be worn when working on power generation safety equipment or any energized equipment in the power generation industry. The electrical gloves are safe for use in the field. These gloves are not only made of rubber but also of various materials that can be dressed or insulated. The voltage protection provided by the voltage electric shock protection and prevent contamination and punctures that can compromise the electrical safety glove.

Insulated Tool Kit

Any work on energized equipment or systems in power generation facilities that require the use of tools can potentially expose workers to an arc flash incident and electrical shock. Using insulated tools can contribute to the shock and burn injuries caused by these hazards. Implementing insulated tools is a smart choice to cut potential deadly hazards caused by hand tools.

Heat/Cold Stress

Power generation facilities and outdoor equipment can put workers at risk for extreme temperature-related hazards. PPE is often the first line of defense in the event there is an arc flash or flash fire incident, whereas wearing the proper garments can prevent heat and cold stress.

Source: https://www.thinknsa.com/power-generation-safety-ppe
What questions would you ask?
The Knowns

- Neither the SCADA control center nor the local team issued a START command for the gas turbines.
- At the time the turbines were started (and a few days before) there were no incoming connections logged by the local firewall.
- CCTV footage did not reveal anyone walking up to the door of the control shed.
- Initial forensic triage of the HMI that controls the turbines did not reveal any unauthorized access. Actually no access at all.
- But right around the startup of the turbines, some applications were launched, including the one that starts the turbines.
The Unknowns

• Are there other remote connections into the local network?
• Might there be another way into the control shed not monitored by CCTV?
• Might malware have been planted on the HMI some time ago
• There might be an insider threat
• There might be a root cause entirely unrelated to „cyber“
The Unknown Unknowns

Your guess is as good as mine 😏

Remember: every investigation requires the right combination of thoroughness, process, and an open mind.
• While examining the control shed, the responder notes it is very cold in there

• Moisture has condensed on the HMI
Hypothesis: moisture might have caused „ghost input“ on the HMI’s touch screen
How do you verify this hypothesis?
Meet an unexpected built-in Windows forensics tool

- Usually you are not allowed to install any software on ICS/OT systems
- Sometimes even running forensics tools from removable media is an issue, depending on regulations
- No forensic tool can help you determine a broken touch panel
Investigation Result

• It was determined a faulty touch screen on the HMI registered ghost input due to overpressure.

• In ICS/OT Root Cause Analysis, it is important to understand the industrial processes involved, potential environmental effects, and overall context.

• Remember:

ICS/OT = IT + Physics
Active Cyber Defense Cycle

- Threat Intelligence Consumption
- Visibility
- Threat Detection
- Incident Response
- Threat & Environment Manipulation
Threat Intelligence Consumption
The ICS Cyber Kill Chain

- High confidence attacks with the aim of process manipulation or physical damage require deep ICS knowledge
- This results in significantly longer dwell time of the adversary in a target environment
- An adversary might inadvertently disrupt the ICS during their „research“
- All of this presents more opportunities to detect the adversary „left of boom“
ICS TI Reports

- Consume reports focused on your
  - Industrial vertical(s)
  - Region
- Favor TTPs over IOCs
- Ensure you provide actionable intelligence internally, i.e. recommendations & guidance
- Understand your organization’s
  - Threat Landscape
  - Information Attack Surface
- ICS/OT Threat Intel providers
  - ISACs
  - CERTs
  - Commercial

AA-2022-43: Broad MFA Exploitation Campaign by Unknown Adversary
05 October 2022

ICS Impact

Dragos investigated the source of anomalous, unsolicited Multi-Factor Authentication (MFA) requests received via mobile devices belonging to a small number of Dragos employees. Dragos identified the source as an IP address of a cloud host of an otherwise legitimate developer whose credentials were most likely stolen and used in an automated, “low and slow” MFA exploitation campaign. The adversary broadly targeted thousands of organizations (many with ICS and OT environments) that employ internet-facing Single Sign-On (SSO) infrastructure from multiple vendors. The SSO appliances from different vendors appeared to integrate with Microsoft Office 365/Azure Active Directory (AD) authentication.

Internet telemetry indicates that multiple organizations that employed internet-facing servers running Microsoft’s Active Directory Federated Services (AD FS) showed significant network flow. Notable targets of significant flow with the adversary IP address are AD FS servers associated with a major Fortune 500 manufacturer of industrial products. While the traffic volume could be explained by the adversary’s generation of an unusual amount of multi-factor (MFA) requests to the staff of those organizations, Dragos cannot at this time rule out a compromise.

Dragos is releasing this advisory alert with adversary indicators and recommendations to highlight the importance of ICS cybersecurity controls against a capable adversary. Left unmitigated, successful MFA exploitation with subsequent access by a capable adversary can facilitate the adversary’s objectives on enterprise or more impactful OT/ICS networks. Industrial control systems (ICS) and operational technology (OT) network owners should architect ICS and OT networks to minimize adversary impacts even in the face of MFA control evasion and perimeter device compromise.

<table>
<thead>
<tr>
<th>Threat Analysis</th>
<th>Analyst Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>Information Technology (IT)/Operational Technology (OT) Security professionals and managers</td>
</tr>
<tr>
<td>Targeted Sector/Industry</td>
<td>All</td>
</tr>
<tr>
<td>Targeted Region</td>
<td>Western Europe, Middle East, South Africa, North and South America, Japan, Australia, Hong Kong</td>
</tr>
<tr>
<td>Threat Group</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat Intelligence Score</td>
<td>A limited threat, risk, or vulnerability requiring an applicability assessment before taking action</td>
</tr>
<tr>
<td>ICS Cyber Kill Chain Stage</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
"Actionable Threat Intel"

- Good Threat Intelligence provides immediate value to defenders

- Common questions it should answer
  - What do I need to focus on?
  - What adversaries might be targeting my organization and what are their TTPs?
  - What TTPs are they using along the Kill Chain?
Current Threat Landscape

ICS Curious (ICS CKC Stage 1)
- Ch
- Co
- Ra
- Va
- Pv
- Ta
- Ma
- Pi
- St
- Ra

ICS Capable (ICS CKC Stage 2)
- Wa
- Hx
- Dy
- Er
- AL

ICS Elves (ICS CKC Stage 2 – Act)
- EL
- Ko
- Xt
- Ka
- Cv
OT = IT + Physics, remember?
OT = IT + Physics, remember?

Physics
Visibility

• You cannot defend what you don’t know you have

• Visibility & monitoring solutions in industrial environments need to be aware of ICS protocols & context

• Whatever solution you choose, ensure it has sufficient protocol coverage for your ICS environment

• You will need to at least conceptually map industrial process to network
# How to Create an Asset Inventory

<table>
<thead>
<tr>
<th>Passive Traffic Analysis</th>
<th>Active Scanning/Querying</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Walkthrough</td>
<td>Configuration Analysis</td>
</tr>
</tbody>
</table>
How to Create an Asset Inventory

- Passive Traffic Analysis
- Active Scanning/Querying
- Site Walkthrough
- Configuration Analysis

- Lowest risk/best results in combination
- High risk of interfering with normal operations
- Requires a high amount of subject matter expertise over various technology stacks, but good way to supplement other approaches
PRIORITIZE WHAT MATTERS MOST

RECOMMENDATION: CROWN JEWELS ANALYSIS

CRITICAL SYSTEM OR SUBSYSTEM
- Refinery
- Boiler House

CRITICAL FUNCTION OR SUB-FUNCTION
- Instrument Air, Pressure Control System, Dew Point
- Compressors, Pressure Control Station, Air Dryers

CRITICAL COMPONENTS
- Vibration Monitor, DCS, Dryer PLC, Dew Point Analyzer

CONTROLLERS
- Vibration Monitor, PLC, DCS, Analyzer, Remote Access, Firewall(s)
Threat Detection
## Threat Detection
### The 4 Types of Detection

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modeling</td>
<td>Threat Behaviors</td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td>Indicators</td>
</tr>
</tbody>
</table>
Threat Detection
Configuration Analysis

- Aka Whitelisting
- Great for investigations when baselines exist, especially for any host systems
- Usually generates too many (false) alerts for initial detection
Threat Detection Modeling

- Aka „Machine Learning“ or (even worse) „AI Based Detection“
- Statistical/Threshold Based Modeling to allow for some variance until an event is triggered
- Great for enhancing analysis and investigations, not only on network activity, but also for alerting on variance in industrial processes that cross a threshold
- Mostly not effective for initial detection as the vendor’s model is certainly not based on your ICS environment
## Threat Detection

### Indicators

- Indicators of Compromise (IOCs) are the most common method for detection.

- We are dealing with highly sophisticated adversaries in ICS/OT, they do use different infrastructure for different targets, thus often (even more) ineffective for initial detection than in IT.

- IOCs gathered during DFIR investigations are *highly effective* for scoping the extent of a breach, especially when enhanced/extended through Threat Intel consumption.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modeling</td>
<td>Threat Behaviors</td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td>Indicators</td>
</tr>
</tbody>
</table>
**Threat Detection**

**Threat Behaviors**

- Threat Behaviors aka TTPs are the most effective for detecting potentially malicious behavior.

- It is hard for humans (think training, habits, budgets) to change behavior. Adversaries are humans, too 😊

- Sometimes difficult to encode into detections in your (often IOC biased) defense toolkit.

- If you are good at detecting typical adversary behavior, you will detect activity even if they are using 0-days.
# Mitre ICS Att&ck Matrix

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impact Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Blunt Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Malware Firmware</td>
<td>Indicator Removal on Host</td>
<td>I/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Change Program State</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Execution through API</td>
<td>Program Download</td>
<td>Masquerading</td>
<td>Network Connection Enumeration</td>
<td>External Remote Services</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Masquerading</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File Infection</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td>Block Reporting Message</td>
<td>Modify Control Logic</td>
<td>Loss of Availability</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Roodit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td>Block Serial COM</td>
<td>Modify Paramater</td>
<td>Loss of Control</td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Spoof Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td>Data Destruction</td>
<td>Module Firmware</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Project File Infection</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td>Point &amp; Tag Identification</td>
<td>Program Upload</td>
<td>Role Identification</td>
<td>Screen Capture</td>
<td>Threat of Operational Information</td>
<td></td>
</tr>
</tbody>
</table>

Source: https://collaborate.mitre.org/attackics/index.php/Main_Page
### Mapping Threat Groups & ICS Att&ck

**XENOTIME**

<table>
<thead>
<tr>
<th>INITIAL ACCESS</th>
<th>EXECUTION</th>
<th>PERSISTENCE</th>
<th>PRIVILEGE ESCALATION</th>
<th>EVASION</th>
<th>DISCOVERY</th>
<th>LATERAL MOVEMENT</th>
<th>COLLECTION</th>
<th>COMMAND AND CONTROL</th>
<th>SENTRY RESPONSE FUNCTION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Operating Mode</td>
<td>Modify Program</td>
<td>Exploitation for Privilege Escalation</td>
<td>Change Operating Mode</td>
<td>Network Connection Discovery</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Driver-by Compromise</td>
<td>Command Line Interface</td>
<td>Module Firmware</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Network Sniffing</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Modify Parameter</td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Execution through API</td>
<td>Project File Infection</td>
<td>Indication Removal on Host</td>
<td>Malware/Exfiltration</td>
<td>Remote System Discovery</td>
<td>Program Organization Unit</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Export Public Facing Application</td>
<td>Graphical User Interface</td>
<td>System Firmware</td>
<td>Masking</td>
<td>Exploitation of Remote Services</td>
<td>Remote System Information Discovery</td>
<td>Lateral Tool Transfer</td>
<td>I/O Image</td>
<td>Block Reporting Message</td>
<td>Unauthenticated Command Message</td>
<td>Loss of Control</td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Native API</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Denial of Service</td>
<td>Device Restart/Shutdown</td>
<td>Loss of Protection</td>
<td></td>
</tr>
<tr>
<td>Remote Services</td>
<td>Scoping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device Restart/Shutdown</td>
<td>Manipulate I/O Image</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Alarm Settings</td>
<td>Network Sniffing</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Rogue Master</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rootkit</td>
<td>Manipulate of Control</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Interpreting Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rootkit</td>
<td>Manipulate of View</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Service Stop</td>
<td>Theft of Operational Information</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System Firmware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**XENOTIME**
# XENOTIME in Depth

Detect more than one technique per Kill Chain Phase

<table>
<thead>
<tr>
<th>INITIAL ACCESS</th>
<th>EXECUTION</th>
<th>PERSISTENCE</th>
<th>PRIVILEGE ESCALATION</th>
<th>EVASION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Operating Mode</td>
<td>Modify Program</td>
<td>Exploitation for Privilege Escalation</td>
<td>Change Operating Mode</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Execution through API</td>
<td>Project File Infection</td>
<td>Indicator Removal on Host</td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>System Firmware</td>
<td>Masquerading</td>
<td></td>
</tr>
<tr>
<td>Exploitation of Remote Services</td>
<td>Hooking</td>
<td>Valid Accounts</td>
<td>Rootkit</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Modify Controller Tasking</td>
<td></td>
<td></td>
<td>Spoof Reporting Message</td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Native API</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Services</td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue Master</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spear phishing Attachment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
XENOTIME in Breadth

Detections over multiple Kill Chain phases

<table>
<thead>
<tr>
<th>DISCOVERY</th>
<th>LATERAL MOVEMENT</th>
<th>COLLECTION</th>
<th>COMMAND AND CONTROL</th>
<th>INHIBIT RESPONSE FUNCTION</th>
<th>IMPAIR PROCESS CONTROL</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Connection Enumeration</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Network Sniffing</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Modify Parameter</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Remote System Discovery</td>
<td>Program Organization Units</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Module Firmware</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Remote System Information Discovery</td>
<td>Lateral Tool Transfer</td>
<td>I/O Image</td>
<td>Block Reporting Message</td>
<td>Spoof Reporting Message</td>
<td>Block Serial COM</td>
<td>Loss of Availability</td>
</tr>
<tr>
<td>Wireless Sniffing</td>
<td>Program Download</td>
<td>Man in the Middle</td>
<td>Block Serial COM</td>
<td>Unauthorized Command Message</td>
<td>Unauthorized Command Message</td>
<td>Loss of Control</td>
</tr>
<tr>
<td>Remote Services</td>
<td>Monitor Process State</td>
<td>Data Destruction</td>
<td>Denial of Service</td>
<td>Device Restart/Shutdown</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Point &amp; Tag Identification</td>
<td>Screen Capture</td>
<td>Manipulate I/O Image</td>
<td>Rootkit</td>
<td>Loss of Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wireless Sniffing</td>
<td>Modify Alarm Settings</td>
<td>Service Stop</td>
<td>Theft of Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rootkit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System Firmware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Coverage and Gap Analysis

**Red and Yellow = Your Security Monitoring Program Roadmap**

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Attack Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>L/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Change Program State</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Execution through API</td>
<td>Program Download</td>
<td>Masquerading</td>
<td>Network Connection Enumeration</td>
<td>External Remote Services</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Masquerading</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td>Block Reporting Message</td>
<td>Modify Control Logic</td>
<td>Loss of Availability</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td>Block Serial Comm Port</td>
<td>Modify Parameter</td>
<td>Loss of Control</td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Sniff Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td>Data Destruction</td>
<td>Module Firmware</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
</tr>
<tr>
<td>Application Through Removable Media</td>
<td>Project File</td>
<td>Utilize/Change Operating Mode</td>
<td>Social Engineering Enumeration</td>
<td>Monitor Process State</td>
<td>Denial of Service</td>
<td>Program Download</td>
<td>Loss of Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spear Phishing Attachment</td>
<td>Scripting</td>
<td>Point &amp; Tag Identification</td>
<td>Device Restart/Shutdown</td>
<td>Rogue Master Device</td>
<td>Loss of View</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>User Execution</td>
<td>Program Upload</td>
<td>Exploitation for Denial of Service</td>
<td>Service Stop</td>
<td>Manipulation of Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td>Role Identification</td>
<td>Manipulate I/O</td>
<td>Spoofer Reporting Message</td>
<td>Manipulation of View</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Screen Capture</td>
<td>Unauthorized Command Message</td>
<td>Theft of Operational Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Modify Control Logic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Program Download</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rootkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System Firmware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Utilize/Change Operating Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IT/OT SOC Workflow Recommendations
Remember the 2 stages of the ICS Cyber Kill Chain. It starts in IT!
Incident Response
Different Mission, Different Requirements
And a lot of different challenges...

Considerations
• Regulations
• Compliance
• Laws
• Safety & Reliability
• Unions
• Governments
• Vendors
• Legacy/Unique Systems
• Data Collection
PICERL Differences

Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned
PICERL Differences

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Industrial Incident Responders need prepare a lot more than IT IR.
Preparation

Things to consider

• PPE. If you’re not wearing the proper gear, no entry
• Safety Certifications. Think NERC CIP, BOSIET, etc.
• Connectors, cables, and SW tools to connect to old/legacy equipment
• Out-of-band comms. Some plants are large and don’t have good mobile phone coverage. Verify the comms meet the local safety requirements!
• How to obtain forensic data from ICS systems
• Where to analyze the data. Are you allowed to remove data from the plant? The country?
PICERL Differences

**Preparation**
Industrial Incident Responders need prepare a lot more than IT IR

**Identification**
Identification ideally performed by OT SOC, but often IR does this

**Containment**

**Eradication**

**Recovery**

**Lessons Learned**
Forensic Data Sets
You need to map cyber to physical process

This is new territory for you enterprise folks
PICERL Differences

Preparation
Industrial Incident Responders need prepare a lot more than IT IR

Identification
Identification ideally performed by OT SOC, but often IR does this

Containment
IR advises, but OT Operations team performs containment, eradication, and recovery

Eradication

Recovery

Lessons Learned
PICERL Differences

**Preparation**
Industrial Incident Responders need prepare a lot more than IT IR

**Identification**
Identification ideally performed by OT SOC, but often IR does this

**Containment**
IR advises, but OT Operations team performs containment, eradication, and recovery

**Eradication**

**Recovery**

**Lessons Learned**
IR supports lessons learned, implementation is a cross team effort
Collection Management Frameworks
Collection Management Framework (CMF)

What:
• A “Collection Management Framework” is a process for identifying and documenting data sources which could answer important business-related questions or investigations

Why:
• Locating resources preemptively reduces a team’s response time to an incident
• Conducting a CMF will identify gaps in visibility and enable defenders to fill them before the data is needed
Process

The 5 Steps of a CMF

1. Develop requirements
2. Develop a collection plan
3. Enhance the collection plan
4. Test the plan
5. Update the plan
Develop Requirements

What:
- Achieving business objectives requires information. “Requirements” are questions which seek that necessary information.

Why:
- A list of requirements (questions) enables defenders to search for data sources and decide which are relevant, which exist, and which do not.

How:
- Initial requirements for a CMF generally address the safety of mission-critical systems.
- Other requirements can be drawn from activities like table-top exercises, Crown Jewels Analysis, vulnerability analysis, etc.

Example
What were the most critical items in our last vulnerability scan of Refinery A?

How could an adversary exploit these?

What activity-groups target our industry?
Develop a Collection Plan

What:
The Collection Plan is the product – it can take whatever form is useful to the analyst. A Collection Plan for incident responders may be an excel sheet of assets and log repositories while one about vulnerability analysis might be a list of links to documents such as an asset inventory and system update policies.

How:
Break down requirements into specific questions which can be answered by data sources. Identify if the data sources exist and add them to a CP.

Example
An activity group which targets your industry has started a new spear phishing campaign. How could you tell if an employee clicked a malicious link?

- Firewall logs
- DNS logs
- IDS alerts…
Enhance the Collection Plan

What:
In this phase, an organization should enhance existing data sources (e.g. retention period of logs), create data sources where they do not exist but should, and create new policies and procedures to streamline access to data sources.

Why:
As the team investigates its data sources, it will recognize gaps and points of tension which will unacceptably inhibit responses.

Example

- Windows logs on the IT network are forwarded to a central server, but not on the OT network – fix it!
- The current procedure means it takes an analyst at least a day to retrieve firewall logs – consider making an emergency procedure to shorten that time, at a minimum.
Test the Plan

What:
• Implement the collection plan and observe for strengths and weaknesses.

Why:
• Changing the way assets log or various policies and procedures may create new issues.

How:
• Develop and act on training scenarios requiring the use of the collection plans

Example
A system may have greater logging capacity than was previously utilized. Turning on these new logs may reduce retention of all logs below an acceptable level, requiring further tuning.
Update the Plan

What:
• In addition to making any changes made apparent by testing, the entire system must be continually assessed and modified.

Why:
• Over time, requirements will change, and data sources will cease to exist or new ones will be added. Without editing, it will not provide useful or accurate information.

Example
Your company has sold off a business line whose infrastructure included your Windows logging hub. Build a new hub and update the CMF accordingly.
## Example CMF

<table>
<thead>
<tr>
<th>Site</th>
<th>Segment / Level</th>
<th>Asset</th>
<th>Data Type</th>
<th>Kill Chain Phases</th>
<th>Data Storage Location</th>
<th>Data Retention</th>
<th>Follow-On Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>DMZ</td>
<td>VPI</td>
<td>Access Logs</td>
<td>Reconnaissance, Command and Control, Delivery</td>
<td>Enterprise SEM</td>
<td>2 Years</td>
<td>Local Firewall Logs</td>
</tr>
<tr>
<td>DMZ</td>
<td>Firewall Logs</td>
<td>VPI</td>
<td>Access Logs</td>
<td>Reconnaissance, Command and Control, Delivery</td>
<td>Enterprise SEM</td>
<td>180 Days</td>
<td>Firewall Ruleset</td>
</tr>
<tr>
<td>DMZ</td>
<td>Jump Host</td>
<td>VPI</td>
<td>Windows Event Logs</td>
<td>Reconnaissance, Command and Control, Delivery</td>
<td>Enterprise SEM</td>
<td>1 Year</td>
<td>Registry</td>
</tr>
<tr>
<td>Alpha Facility</td>
<td>Supervisory Network Alpha</td>
<td>Hierarchy</td>
<td>Windows Event Logs</td>
<td>Exploitation, Installation, Actions on Objectives</td>
<td>Log Server</td>
<td>60 Days</td>
<td>Hierarchy Logs, Registry</td>
</tr>
<tr>
<td>Alpha Facility</td>
<td>Supervisory Network Alpha</td>
<td>Dragons</td>
<td>Windows Event Logs</td>
<td>Exploitation, Installation, Actions on Objectives</td>
<td>Log Server</td>
<td>60 Days</td>
<td>Known Good Baseline Comparison</td>
</tr>
<tr>
<td>Alpha Facility</td>
<td>Supervisory Network Alpha</td>
<td>EWS</td>
<td>Windows Event Logs</td>
<td>Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives</td>
<td>Log Server</td>
<td>30 Days</td>
<td>Registry, Memory, MFT</td>
</tr>
<tr>
<td>Alpha Facility</td>
<td>Control Network Alpha</td>
<td>RTUs</td>
<td>Sylog</td>
<td>Installation, Actions on Objectives</td>
<td>Log Server</td>
<td>90 Days</td>
<td>Controller Logic</td>
</tr>
<tr>
<td>Alpha Facility</td>
<td>Control Network Alpha</td>
<td>HMIs</td>
<td>Windows Event Logs</td>
<td>Installation, Actions on Objectives</td>
<td>Local Host</td>
<td>15 Days</td>
<td>Memory, MFT</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Supervisory Network Bravo</td>
<td>Hierarchy</td>
<td>Windows Event Logs</td>
<td>Exploitation, Installation, Actions on Objectives</td>
<td>Log Server</td>
<td>60 Days</td>
<td>Hierarchy Logs, Registry</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Supervisory Network Bravo</td>
<td>EWS</td>
<td>Windows Event Logs</td>
<td>Exploitation, Installation, Actions on Objectives</td>
<td>Local Host</td>
<td>4 Years</td>
<td>Registry, Memory, MFT</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Supervisory Network Bravo</td>
<td>Short IDS</td>
<td>Alerts</td>
<td>Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives</td>
<td>Log Server</td>
<td>90 Days</td>
<td>Controller Logic</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Control Network Bravo</td>
<td>RTUs</td>
<td>Security Events</td>
<td>Installation, Actions on Objectives</td>
<td>Log Server</td>
<td>1 Year</td>
<td>Controller Logic</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Control Network Bravo</td>
<td>HMIs</td>
<td>Windows Event Logs</td>
<td>Installation, Exploitation, Actions on Objectives</td>
<td>Local Host</td>
<td>7 Days</td>
<td>Registry, Memory, MFT</td>
</tr>
<tr>
<td>Bravo Facility</td>
<td>Control Network Bravo</td>
<td>Short IDS</td>
<td>Alerts</td>
<td>Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives</td>
<td>Log Server</td>
<td>90 Days</td>
<td>RegServer</td>
</tr>
<tr>
<td>Charlie Facility</td>
<td>Supervisory Network Charlie</td>
<td>Hierarchy</td>
<td>Windows Event Logs</td>
<td>Exploitation, Installation, Actions on Objectives</td>
<td>Local Host</td>
<td>15 Days</td>
<td>Hierarchy Logs, Registry</td>
</tr>
<tr>
<td>Charlie Facility</td>
<td>Supervisory Network Charlie</td>
<td>EWS</td>
<td>Windows Event Logs</td>
<td>Installation, Actions on Objectives</td>
<td>Local Host</td>
<td>10 Years</td>
<td>Registry, Memory, MFT</td>
</tr>
<tr>
<td>Charlie Facility</td>
<td>Supervisory Network Charlie</td>
<td>Short IDS</td>
<td>Alerts</td>
<td>Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives</td>
<td>Log Server</td>
<td>90 Days</td>
<td>Controller Logic</td>
</tr>
<tr>
<td>Charlie Facility</td>
<td>Control Network Charlie</td>
<td>RTUs</td>
<td>Security Events</td>
<td>Installation, Actions on Objectives</td>
<td>Local Host</td>
<td>7 Days</td>
<td>Controller Logic</td>
</tr>
<tr>
<td>Charlie Facility</td>
<td>Control Network Charlie</td>
<td>HMIs</td>
<td>Windows Event Logs</td>
<td>Installation, Exploitation, Actions on Objectives</td>
<td>Local Host</td>
<td>7 Days</td>
<td>Registry, Memory, MFT</td>
</tr>
</tbody>
</table>
Threat & Environment Manipulation
Environment
How to Prepare

• Think in scenarios, e.g. ransomware, worms, attacks against crown jewels

• Prepare for segmentation ahead of time, i.e. logical network separation through firewall rules

• Ask yourself, how long the process can sustain separation

• Have a plan & exercise it
Threat
Understand the Threat

• Leverage good Threat Intel
  • Who are you dealing with?
  • What might be their objectives
• Understand their TTPs and tools
• Identify weaknesses in your environment and their TTPs and tools
• Leverage your knowledge for defense, buying your team time to eradicate and recover
Consequence Driven Threat Hunting
Risk = (Threat * Vulnerability) * Consequence
Threat Hunt Model

- Take actionable information and proactively do actions with it = Threat Hunting
Threat Hunt Model

- Hyp: adversary has compromised EWS in DeltaV DCS of Fanta Coloring Plant and is using DNSTUNNEL for C2
Threat Hunt Model

- **Location:** DeltaV DCS of Fanta Color Plant
- **Logs:** DNS records on hosts, passive DNS, DNS Server Logs, hosts files, resolv.conf, Zeek, Windows Event Logs, Proxy logs, FEYE HX/PX logs, FW logs, netflow/IPFIX, syslog, DeltaV logs, Windows registry, DHCP config/logs
Threat Hunt Model

- Collection Management Framework
- Logs:
  - passive DNS (Level 4 DMZ)
  - DNS Server Logs (Level 2 DCS)
  - hosts files (on host)
  - resolv.conf (on host)
  - Zeek (not available)
  - Windows Event Logs (CMF 30 days)
  - Proxy logs (Level 4 DMZ, but no DNS)
  - FEYE HX/PX logs
  - FW logs (Level 2-4)
  - netflow/IPvIX
  - Syslog (depends on plant and location)
  - DeltaV logs (local, 90 days)
  - Windows registry (local)
  - DHCP config/logs (local)

- Is the plant compliant with the BASF data model? (yes/no)
Threat Hunt Model

- Viability
- Fit to Purpose
- Scope modifications

- Logs:
  - passive DNS (Level 4 DMZ)
  - DNS Server Logs (Level 2 DCS)
  - hosts files (on-host)
  - resolv.conf (on-host)
  - Zeek (not available)
  - Windows Event Logs (CMF 30 days)
  - Proxy logs (Level 4 DMZ, but no DNS)
  - FEYE HX/PIX logs
  - FW logs (Level 2-4)
  - netflow/PEFIX
  - Syslog (depends on plant and location)
  - DeltaV logs (local, 90 days)
  - Windows registry (local)
  - DHCP config/logs (local)
Threat Hunt Model

- Carry out Hunt
- Additional Hypotheses
- Generate Report
- Logs:
  - passive DNS (Level 4 DMZ)? Maybe DNS tied to AD, ask AD ops team, DNS queries are in SIEM, but not replies
  - Proxy logs (Level 4 DMZ, but no DNS), in SIEM
  - FEYE HX/PX logs, Alerts in SIEM, events local
  - FW logs (Level 2-4), SIEM
Threat Hunt Model

- Feedback
  - What worked?
  - What can be improved?

- Internal:
  - What are collection gaps?
  - What are policy and procedure gaps?
  - How would we have done if we were patient 0?

- External:
  - Process improvements
  - Resource improvements
  - Provide additional findings back to source
  - What information was useful?
Case Study: Applied Threat Hunt Model
De-Salting Unit

- FIC - Flow Indicated Control
- TT – Temperature Transmitter
- PT – Pressure Transmitter
- DPC – Dual Zone Pressure Controller
- LC – Level Controller

Source: https://www.slideshare.net/OctoVeranClive/petroleum-intricacy-4/10

* This is not paid marketing for BGR Energy and we have not worked in collaboration with BGR Energy to produce this webinar. This does not represent BGR Energy views.
Purpose

- Gain visibility and understanding into critical process assets in desalination
Scope: Phase 1

- 1 Refinery in San Antonio, Texas
  - Desalination Process
    - ABB Freelance DCS
      - Freelance Operation Center
      - All AC 900F Controllers
      - All AC 800F Controllers
      - All AC 700F Controllers
        - Profibus, Modbus (RTU and TCP)
ABB: Freelance DCS

- Modernized Control System
- Variety of implementations
- Integrations with many other applications
- Hundreds of IOs and field devices
- Controllers:
  - AC 700F, AC 800F, AC 900F
  - Remote IO: S700, S800, S900
- Freelance Operations
- Freelance Engineering
Scope: Phase 2: Hypotheses

- Hypotheses
  - Attackers are leveraging Freelance Operation Center login information to do reconnaissance on desalination process.
  - Attackers are sending malicious commands to AC 900F and AC 700F controllers to manipulate desalination process.
Equip: Phase 1: CMF

- Freelance Operations center
  - Asset Management
  - Process information
  - User logging + Timestamps
  - System Changes
- Freelance Engineering
  - Database
  - Project configurations
- Network Traffic to Controllers
- Historian Assets
# Collection Management Framework

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Desalination Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Logs</td>
<td>2 Days</td>
</tr>
<tr>
<td>Freelance Operations</td>
<td>30 Days</td>
</tr>
<tr>
<td>FreeLance Engineering</td>
<td>30 Days</td>
</tr>
<tr>
<td>Full Network Capture</td>
<td>7 Days</td>
</tr>
<tr>
<td>Process Historian</td>
<td>60 Days</td>
</tr>
<tr>
<td>Controllers</td>
<td>None Available</td>
</tr>
</tbody>
</table>
Equip: Phase 2: Resource Allocation

- Team members
  - Senior
  - Junior
- Tools
  - Approved
  - Custom vs General
- Time
Plan Review

- Stakeholder awareness
- Potential issues with achieving purpose success
- Any alterations
Execute

- Use hypotheses to structure hunts with relevant data sources
- Discussions with Subject Matter Experts on what is “normal”
- Hunt to find what does not fit the expected normal
- Observables of known adversary behavior
Hypothesis #1

• Attackers are leveraging Freelance Operation Center login information to do reconnaissance on desalination process.

• Data Source
  • Freelance Operation Center
    • Weird logons
    • Unknown users
    • Timestamps during non-working hours
    • Un-successful logon attempts in high frequency and volume

• Data Source
  • Network Capture
    • Timestamps during non-working hours
    • Unknown addressing space
    • Scanning activity
    • Exfiltration of data
Hypothesis #2

- Attackers are sending malicious commands to AC 900F and AC 700F controllers to manipulate desalination process.

**Freelance Operation Center**
- Trend Analysis
- Normal operations as baseline
- Event logs
- User Authentication

**Network Capture**
- Controller Command Responses
- Controller Status

**Freelance Engineering**
- Understanding of PLC configuration files
- Stateful analysis

**Process Historian**
- Alarm Events
- Trend Analysis
Execute: Report

- Summary of all findings
- Hypothesis confirmation or falsification
- Better understanding of environment
- Establish baseline of operations for follow on hunts with new scopes
Feedback

- **Purpose**: How was the report received?
- **Scope**: Too broad or narrow? Follow on hunts?
- **Equip**: Data sources? Team Experience?
- **Plan Review**: Any blatant issues missed?
- **Execute**: Did we prove or disprove hypothesis with confidence?
• A Hunt activity should (ideally) always start with good hypotheses generation, otherwise, hunters would be groping in the dark, looking for "something" without a clear target and scope.

• There is a substantial difference between
  • Hunting in one's own network
  • Hunting for threats in someone else's environment and/or from the outside.
Threat Hunting - Hypotheses

• Generating good Hypotheses
  • From Observation
    • E.g. how did previous intrusion look like?
  • With Testability in mind
    • Need to come up with hypotheses that we know we can test (validate/invalidate) given the data we have.
    • Once all the previous research has been completed, hunters should generate (or discard) hypotheses based on what technical data/telemetry is at their disposal: a hypothesis for which the data to prove/disprove it is not (or mostly not) available, it is not a good hypothesis.
Threat Hunting - Hypotheses

- One more thing to consider before structuring the activity, it's what type of "approach" one is going for:
  - Victim Centric
  - Technology Centric
  - Adversary Centric
  - Socio-Political Centric
  - etc.
That's all folks! And remember: defense is doable!

Thank you for your time! Questions?
Twitter: @kaithomsen
Email: kthomsen@dragos.com