ICS/OT Detection and Response

Kai Thomsen, Director, Incident Response Services

Definition reminders

- **Unintentional Insider Threat:** somebody made a mistake that had cybersecurity consequences
- **Malicious Insider:** someone with the intent of causing degradation, disruption, or even destruction

Mentimeter Question: Incident Response

How does your organization deal with OT cybersecurity related cybersecurity incidents?

- We have a dedicated OT incident response plan
- We have an IT incident response plan
- We do not have an incident response plan yet

To vote, go to **www.menti.com** and use the code **2304 2950.**

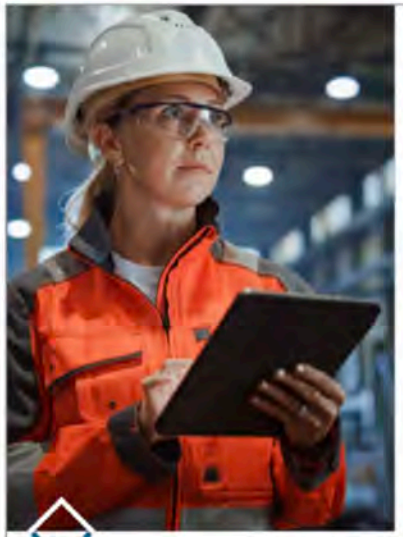
What do OT Incidents look like?

- Remember: the objective is physical impact!
- It starts in an IT environment. But that might not be yours (think MSSPs, partners, OEMs, etc.)
- As the objective is physical impact, the effect might look like a malfunction
- Without proper network-based OT security monitoring, discerning a malfunction from an attack is challenging
- During IR, priority is to maintain Safety & Reliability of operations

Case Study – ICS SW Bug Looks Like Attack

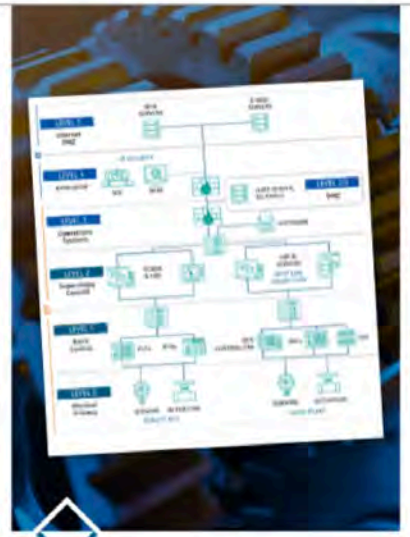
- A renewable energy provider experienced a sudden voltage drop at the intertie
- Their equipment was the same targeted by ELECTRUM/SANDWORM in Ukraine in 2015
- There was no ICS network security monitoring
- Incident responders immediately rolled out monitoring, identified the origin system sending commands
- Root cause turned out as a software bug triggered by an edge case configuration
- Remember that attacks can look like bugs and vice versa!

The Five Critical Controls for ICS/OT



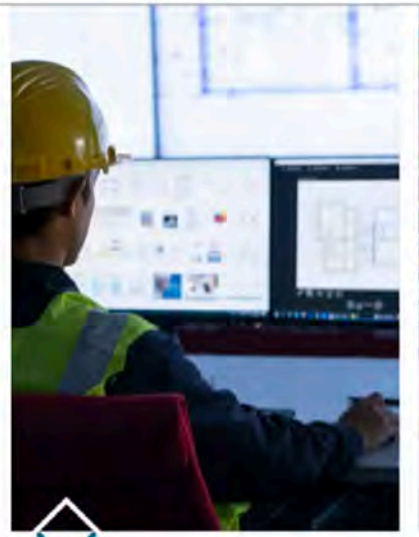
ICS INCIDENT RESPONSE

Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment



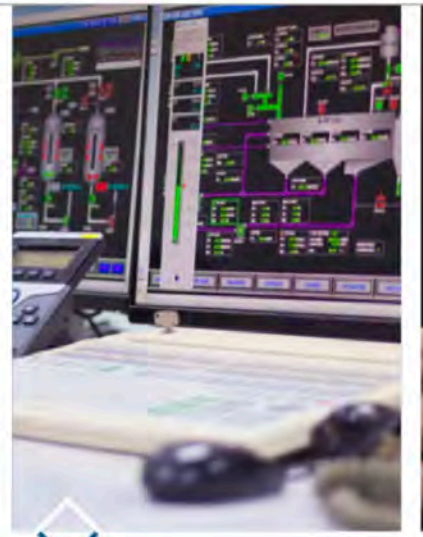
DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement



ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

RISK-BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Mentimeter Question: OT Cybersecurity Controls

What cybersecurity controls are implemented in your OT environment?

- We have ICS protocol aware network security monitoring
- We have firewalls at the perimeter between IT and OT
- VPN and other remote access solutions to our OT environment require Multi Factor Authentication
- We do not have any of these controls implemented yet

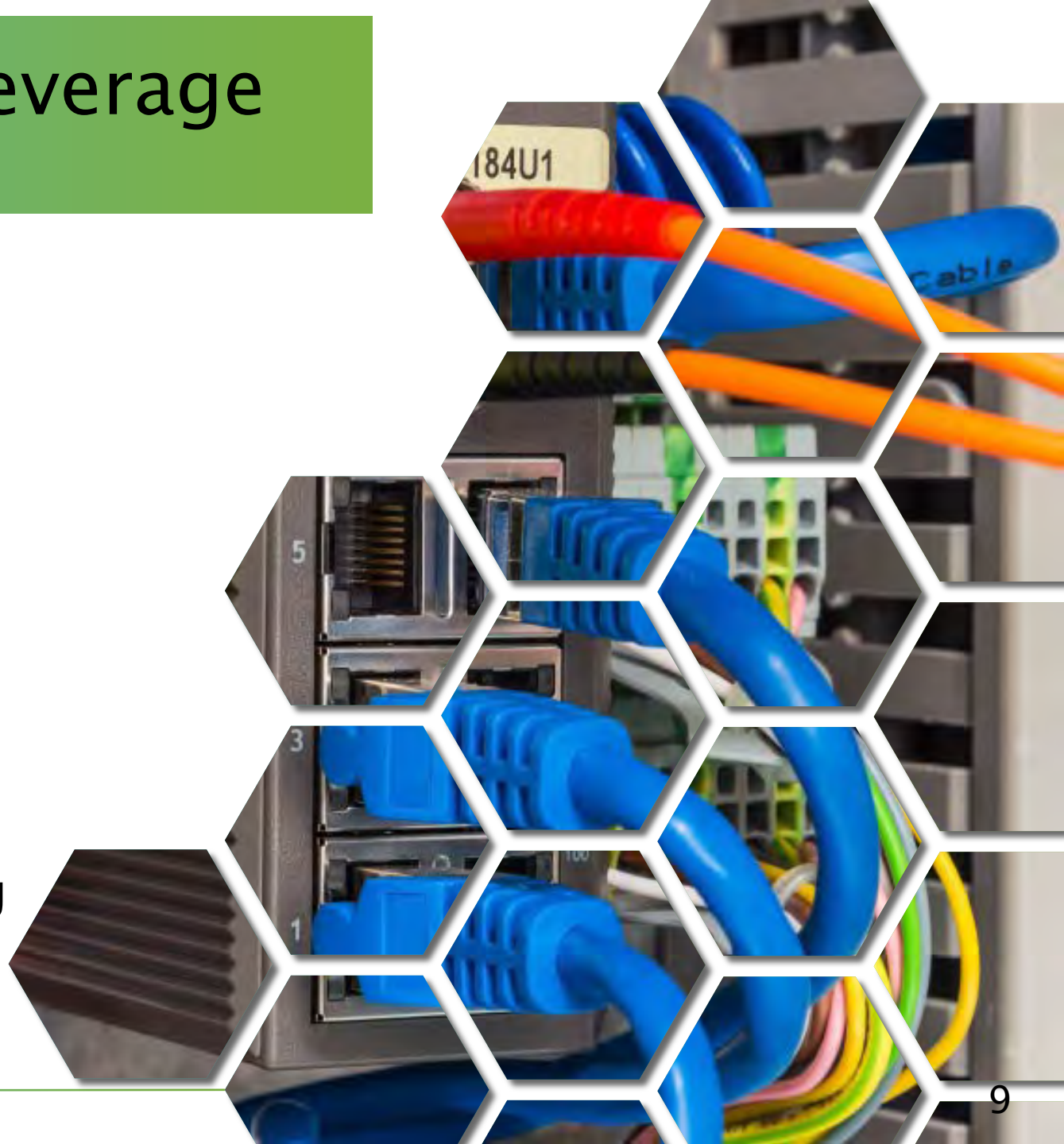
To vote, go to **www.menti.com** and use the code **2304 2950.**

Case Study: Water insider attack

- IT Sec team announced changes
- These were opposed by the OT team
- Once implemented, OT systems suddenly started to malfunction
- Root cause were not the changes, but deliberate tampering by disgruntled employees

Case Study: food and beverage unintentional insider

- During a plant commissioning, a beverage tank suddenly had it's drain valve opened, resulting in loss of product
- Company assumed an attack, possibly by an insider and activated their OT IR retainer
- Process logs were not helpful
- OT network monitoring identified the source of the "Open Valve" command
- Further analysis unveiled a logic error in the code of the packaging system as root cause



Case study: negligence leads to ransomware incident

- A critical OT system on a solid waste disposal system of a large municipality stopped operating
- The HMI was displaying a ransom note
- Forensic analysis and employee interviews identified an unauthorized remote access solution installed by the MSSP for remote maintenance as the initial access vector for the external adversary

Insiders Used as Agents

- Russia has been leveraging “single use agents” to conduct physical attacks against critical infrastructure
- Increasing availability of easy-to-use software to conduct generic attacks against OT systems, we need to prepare for similar approaches in cyber

Mentimeter Question: Exercises

What level of exercising for IT/OT cybersecurity is your organization doing?

- We have not yet started running tabletop exercises
- We have done a first tabletop exercise
- We are running IT focused tabletop exercises regularly
- We are running OT focused tabletop exercises

Exercises – Pre-requisites

- Consider that most networks are like M&M's, hard perimeter, but no significant protections on the inside
- Insider Threats are *inside your network*, thus will likely not be detected or blocked by your security controls
- Dealing with an insider threat is a multi team effort and your IR/cybersecurity team should not be in charge

Types of Exercises I – ROC and Standard TTX

- A Rehearsal of Concept (ROC) takes a very short scenario and goes through the Incident Response Plan step by step, asking “what if” questions
  - Example: what if the Intertie HMI became unresponsive and showed a ransom note?
- A Standard Tabletop Exercise (TTX) uses pre-defined scenarios to test and drill a team’s ability to execute the Incident Response Plan. Focus is on ability to organize, plan, and communicate
  - Example: pre-defined adversary, e.g. ELECTRUM targeting a substation of a nuclear power plant

Types of Exercises II – Custom TTX

- A Custom TTX is tailored towards the technology, operations, and other aspects of an organization. It takes a long time to implement, but can be highly realistic
- Will often involve multiple teams
  - Example: insider conducting sabotage against secondary systems at a facility, resulting in system lockouts, physical security systems shutting down parts of the facility, and failure of critical systems like AC

Types of Exercises III – Executive TTX

- An Executive TTX involves the highest leadership levels at a site or an organization
- It is tailored towards their requirements and expectations with a focus on planning, communication, and strategy
- Might involve or simulate multiple execution teams
  - Example: insider conducting sabotage against secondary systems at a facility, what is our course of action? How do we deal with/involve third parties, law enforcement, media, the public? How effective is our internal crisis management organization?

Developing an Exercise Mindset

- Start small, i.e. with an ROC (Crawl > Walk > Run)
- In some cultures, getting leadership buy in might require you to run an Executive TTX first
- Once rolling, run ROCs and Standard TTXs on a regular basis to better train your teams
- Make sure to always conduct a hotwash, lessons learned, and execution plan for improvement after each exercise

kthomsen@dragos.com