**Day 2 - Operational Technology (OT) Security (18.6.)**

**1. SCADA & ICS Fundamentals**

**Topics**

* Overview of **OT systems**: SCADA, ICS, PLCs, RTUs
* Key components in industrial control environments
* Protocols used in OT: Modbus, DNP3, OPC, BACnet
* Common architecture patterns in manufacturing and critical infrastructure
* Real-world examples: Power grid, water treatment, factory automation

**Required Infrastructure & Components**

* Virtual ICS simulation lab or prebuilt OT network topology diagram
* Protocol analyzer tools (e.g., Wireshark with Modbus filters)
* Documentation for common ICS components
* MITRE ATT&CK for ICS Navigator

**To-Dos & Steps**

1. Compare SCADA vs. traditional IT environments
2. Identify key OT components and their interconnections
3. Analyze communication patterns in Modbus/DNP3
4. Map typical OT attack surfaces (engineering workstations, HMI, PLCs)
5. Reflect on safety-critical constraints (availability > confidentiality)

**Webinars**:

* SANS ICS Security Essentials Webinar [Why ICS/OT Need Specialized Cyber Training | SANS ICS Security](https://www.youtube.com/c/SANSICSsecurity) – 00:07
* CISA Webinar on Industrial Control Systems Cybersecurity[CISA Cybersecurity Resources for Agriculture Infrastructure](https://www.youtube.com/watch?v=H-tZqYXK414) – 00:35

**YouTube**:

* [SCADA Explained | RealPars](https://www.youtube.com/watch?v=nlFM1q9QPJw) – 00:08
* [Introduction to SCADA Systems | Edureka](https://www.youtube.com/watch?v=YC8Qwr7mQbY) – 00:17
* [PLC, SCADA, and RTU explained | AutomationDirect](https://www.youtube.com/watch?v=gC4MEhx3NnM) – 00:03

[What is an RTU? Remote Terminal Unit](https://www.youtube.com/watch?v=t14aSlX4xK8&t=125s) – 00:09

**Reading Material**:

* MITRE ATT&CK for ICS Overview[Matrix - ICS | MITRE ATT&CK®](https://attack.mitre.org/matrices/ics/)
* ISA/IEC 62443 Standards Overview[Message from Keyfactor](https://www.keyfactor.com/education-center/mastering-iec-62443-a-guide-to-securing-industrial-automation-and-control-systems/?utm_content=dsa&gad_source=1&gad_campaignid=17374843093&gbraid=0AAAAADoanaPmB-KREKpiqt51Ns3UWnN5Q&gclid=EAIaIQobChMIjLyRs7bajQMVbMpEBx1PtwqIEAAYASAAEgIQxvD_BwE)
* Introduction to Modbus Protocol (Modbus Organization) [An Introduction to the Modbus Protocol](https://www.youtube.com/watch?v=zuspWMx4o7A) – 00:14
* ICS-CERT Recommended Practices [Guide to Industrial Control Systems (ICS) Security](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf)

**2. OT vs. IT Threat Landscape**

**Topics**

* Differences in priorities: IT = CIA, OT = AIC (Availability first)
* Attack vectors in OT: physical access, firmware, insecure protocols
* Case studies: Stuxnet, Triton, BlackEnergy
* Threat actors and motivations (nation states, hacktivists, insiders)
* Challenges in patching, visibility, and segmentation

**Required Infrastructure & Components**

* Timeline of major ICS cyber incidents
* Threat actor profiles and OT-specific TTPs
* Example attack flow diagrams (from MITRE or Dragos reports)
* Optional: OT honeypot logs or ICS packet captures

**To-Dos & Steps**

1. Analyze one ICS breach case and reconstruct attack steps
2. Identify gaps between IT detection tools and OT visibility
3. Discuss risks of IT/OT convergence
4. Propose segmentation models to separate OT from IT networks
5. Review standard OT hardening practices (disable USB, physical lockdowns)

**Webinars**:

* Dragos Webinar: State of Industrial Cybersecurity [Endlich gibt es ein CRM, mit dem dein Team richtig gerne arbeitet | monday sales CRM](https://www.youtube.com/watch?v=ZkbLe5Q7BwY) – 01:02
* SANS ICS Security Summit: [Key Threats Facing OT](https://www.dragos.com/resources/video/armor-for-ot-security-leaders-sans-ics-security-summit-2021/) – 00:29

**YouTube**:

* [What is OT Security? ICS/SCADA Cybersecurity Explained | Claroty](https://www.youtube.com/watch?v=xWlB5PFoGag&t=347s) – 00:07
* [Stuxnet Explained | RealPars](https://www.youtube.com/watch?v=EOPLN-MVKY4) – 00:18
* [BlackEnergy Malware Attack Explained | CyberX Labs](https://www.youtube.com/watch?v=9TkbYXey3Vs) – 00:14

**Reading Material**:

* Dragos Threat Report: ICS Cybersecurity Year in Review[2025 OT Cybersecurity Report | Dragos](https://www.dragos.com/ot-cybersecurity-year-in-review/)
* CISA: Lessons Learned from Recent ICS Cyber Incidents [Real World Case Studies | CISA](https://www.cisa.gov/real-world-case-studies)
* SANS Strategy Guide ICS [SANS Strategy Guide: ICS Is the Business | SANS Institute](https://www.sans.org/mlp/ics-business-guide/)

**3. Purdue Model for ICS Security**

**Topics**

* The **Purdue Enterprise Reference Architecture (PERA)**
* Layered model: Level 0–5
* Security zones and conduits
* Zoning and segmentation best practices
* Mapping detection and defense controls to each layer

**Required Infrastructure & Components**

* Purdue Model diagram templates
* ICS reference architecture examples (e.g., ISA-99/IEC 62443)
* Annotated defense-in-depth example
* Access control and logging models for OT environments

**To-Dos & Steps**

1. Build a layered ICS architecture using the Purdue Model
2. Define security controls for each level (e.g., firewall between L3 and L2)
3. Identify weakest links in a sample design
4. Simulate lateral movement from IT into OT in a diagram
5. Develop a simple OT zoning policy with controls per segment

**Webinars**:

* Nozomi Networks: Purdue Model for ICS Explained [Nozomi Networks](https://www.ikarussecurity.com/wp-content/downloads/Nozomi-Networks-NIS-Compliance-Mapping-Guide.pdf) – 10 pages
* ISA Webinar: ICS/OT Architecture and the Purdue Model [Excerpt #2: Industrial Cybersecurity Case Studies and Best Practices](https://gca.isa.org/blog/excerpt-2-industrial-cybersecurity-case-studies-and-best-practices)

**YouTube**:

* [Purdue Model for ICS Security | RealPars](https://www.youtube.com/watch?v=c81YnS-Syik) – 00:09
* [ICS Purdue Model Explained | Control Systems Cybersecurity](https://www.youtube.com/watch?v=dMzTEVz4Ih4) – 00:14

**Reading Material**:

* [ISA-95 and Purdue Model Relationship](https://itotinsider.substack.com/p/isa-95-and-the-purdue-model-explained) – 00:04
* [ISA-62443 and the Purdue Model](https://www.paloaltonetworks.ca/cyberpedia/what-is-the-purdue-model-for-ics-security) – 00:05
* [Defense-in-Depth Strategies for ICS (CISA)](https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf) – page 1-43

**4. MITRE ATT&CK for ICS**

**Topics**

* Overview of MITRE ATT&CK for ICS vs. Enterprise
* Key tactics & techniques used in OT-focused attacks
* Mapping detections and controls to ICS kill chain
* Integrating ATT&CK into OT monitoring strategy
* Detection gaps in legacy systems

**Required Infrastructure & Components**

* MITRE ATT&CK Navigator (ICS matrix)
* Real-world ICS technique mappings
* Threat hunting playbook template for ICS
* Access to simulated attack paths (e.g., TryHackMe ICS lab)

**To-Dos & Steps**

1. Navigate and explore MITRE ATT&CK for ICS
2. Map attack techniques from a selected case study
3. Highlight which phases lack detection today
4. Build a threat hunting hypothesis based on ICS technique
5. Review how to adapt IT SOC tools to OT telemetry

**Webinars**:

* [MITRE ATT&CK for ICS Introduction](https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics)
* [Dragos Webinar: How to Use MITRE ATT&CK for ICS in Your Security Program](https://www.youtube.com/watch?v=NARspb8QfFE) – 00:44

**YouTube**:

* [MITRE ATT&CK for ICS Overview Video](https://www.youtube.com/watch?v=EgKOMgU_to8) – 01:04
* [Threat Detection for ICS Networks | Recorded Future](https://www.youtube.com/watch?v=IAWzWHkc3vQ) – 00:35

**Reading Material**:

* [MITRE ATT&CK for ICS Full Matrix](https://attack.mitre.org/matrices/ics/)
* ICS Threat Hunting and Detection Mappings (MITRE)[ICS Threat Hunting using MITRE ATT&CK and Elastic Security - Yashraj Kalpesh Solanki](https://www.youtube.com/watch?v=1VZjTKyRj9c) – 00:30
* Dragos: ICS Threat Detection and Response Best Practices[Dragos ICS Threat Detection & Response Platform Demo | Dragos](https://www.dragos.com/resources/video/dragos-ics-threat-detection-response-platform-demo/) – 00:19

**Afternoon Lab: TryHackMe – ICS & SCADA Room (Community)**

*Alternative: Hack The Box – ICS Labs*

* Hands-on walkthrough of OT-specific vulnerabilities and misconfigurations
* Analyze Modbus or BACnet traffic
* Simulate adversary access to HMI or PLCs
* Propose real-time detection and containment steps
* [TryHackMe: ICS & SCADA Room](https://tryhackme.com/)
* **Alternative**:
  + [Hack The Box: ICS Labs](https://www.hackthebox.com/)

**🎯 End-of-Day Goal**

Participants should be able to:

* Understand how ICS/SCADA environments differ from IT systems
* Analyze real-world OT attack scenarios and adversary techniques
* Apply the Purdue Model to design secure ICS architectures
* Use MITRE ATT&CK for ICS to identify threat detection and prevention strategies
* Complete a practical OT lab challenge in a controlled environment