- **1: ICS Overview**
  - Global Industrial Cybersecurity Professional (GICSP) Overview
  - Overview of ICS

- Processes & Roles

- Industries

  - Purdue Levels 0 and 1

- Controllers and Field Devices

- Programming Controllers

- Exercise: Programming a PLC

  - Purdue Levels 2 and 3

- HMIs, Historians, Alarm Servers

- Specialized Applications and Master Servers

  - DCS and SCADA

- Differences in Location and Latency

- Exercise: Programming an HMI

  - IT & ICS Differences

- ICS Life Cycle Challenges

  - Physical and Cyber Security
  - Secure ICS Network Architectures

- ICS410 Reference Model

- Design Example

- Exercise: Architecting a Secure DCS

ICS410.2: Field Devices & Controllers

- ICS Attack Surface

    - Threat Actors and Reasons for Attack
    - Attack Surface and Inputs
    - Vulnerabilities
    - Threat/Attack Models
- Purdue Level 0 and 1
    - Purdue Level 0 and 1 Attacks
    - Control Things Platform
    - Exercise: Finding Passwords in EEPROM Dumps
    - Purdue Level 0 and 1 Technologies
    - Purdue Level 0 and 1 Communications
    - Fieldbus Protocol Families
    - Exercise: Exploring Fieldbus Protocols
    - Purdue Level 0 and 1 Defenses
- Ethernet and TCP/IP
    - Ethernet Concepts
    - TCP/IP Concepts
    - Exercise: Network Capture Analysis
    - ICS Protocols over TCP/IP
    - Wireshark and ICS Protocols
    - Attacks on Networks
    - Exercise: Enumerating Modbus TCP

ICS410.3: Supervisory Systems

- Enforcement Zone Devices
    - Firewalls and NextGen Firewalls
    - Data Diodes and Unidirectional Gateways
- Understanding Basic Cryptography
    - Crypto Keys
    - Symmetric and Asymmetric Encryption
    - Hashing and HMACs
    - Digital Signatures
- Wireless Technologies
    - Satellite and Cellular
    - Mesh Networks and Microwave
    - Bluetooth and Wi-Fi
- Wireless Attacks and Defenses
    - 3 Eternal Risks of Wireless
    - Sniffing, DoS, Masquerading, Rogue AP
- Exercise: Network Forensics of an Attack
- Purdue Level 2 and 3 Attacks
    - Historians and Databases
    - Exercise: Bypassing Auth with SQL Injection
    - HMI and UI Attacks

- Web-based Attacks
- Password Defenses
- Exercise: Password Fuzzing

ICS410.4: Workstations and Servers

Workstations and Servers

-
- Patching ICS Systems
  - Patch Decision Tree
  - Vendors, CERTS, and Security Bulletins
- Defending Microsoft Windows
  - Windows Services
  - Windows Security Policies and GPOs
  - Exercise: Baselining with PowerShell
- Defending Unix and Linux
  - Differences with Windows
  - Daemons, SystemV, and SystemD
  - Lynis and Bastille
- Endpoint Security Software
  - Antivirus and Whitelisting
  - Application Sandboxing and Containers
  - Exercise: Configuring Host-Based Firewalls
- Event Logging and Analysis
  - Windows Event Logs and Audit Policies
  - Syslog and Logrotate
  - Exercise: Windows Event Logs
- Remote Access Attacks
  - Attacks on Remote Access
  - Honeypots
  - Exercise: Finding Remote Access

ICS410.5: ICS Security Governance

ICS Security Governance

- Building an ICS Cyber Security Program
  - Starting the Process
  - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
  - Using the NIST CSF
- Creating ICS Cyber Security Policy
  - Policies, Standards, Guidance, and Procedures

    - Culture and Enforcement
    - Examples and Sources
- Disaster Recovery
    - DR and BCP Programs
    - Modification for Cyber Security Incidents
- Measuring Cyber Security Risk
    - Quantitative vs Qualitative
    - Traditional Models
    - Minimizing Subjectivity
- Incident Response
    - Six Step Process
- Exercise: Incident Response Tabletop Exercise
- Final Thoughts and Next Steps
    - Other ICS Courses by SANS
    - Other SANS Curriculums and Courses
    - Netwars