INDUSTRIAL NETWORKS CYBERSECURITY

ADVANCED CYBERSECURITY

CS-3000

The Industrial Control Systems (ICS) and Operational Technology (OT) network security environment is built on devices, protocols, connectivity specifications and requirements that do not exist in the SOHO or Enterprise network environments.

In the Marcraft Industrial Networks Cybersecurity Course students will be introduced to ICS embedded devices including PLCs, RTUs and IEDs. Students will also become acquainted with industrial network protocols including - Modbus, DNP3, BacNet, etc. Other key topics include ICS/Utility network communication methods and the real-time IAC tenets associated with these networks.

CERTIFICATIONS

SANS Institute GICSP Certification

Not Just a Simulation! Hands-on Labs Use the Following Equipment:

- PLCs
- HMI & SCADA Systems
- Data Historians
- Pentesting Software
- Servers, Enterprise Routers, and Switches
- Firewall Appliances

The Marcraft Industrial Network Cybersecurity Certification Course covers these topics:

- Global Security Standards, Practices, & Regulations
- Open & Closed Loop Control Systems
- Dedicated & Distributed Control Systems
- Industrial Sensors
- Final Control Elements/Actuators
- Industrial Process Controllers
- Field Devices & Industrial Networks
- SCADA
- Common Industrial Network Structures
- Industrial Network Communication Media
- Asynchronous Serial Standards
- Remote Access Communication Media
- Industrial Network Protocols
- Utility Collection & Control Networks
- Customer Data Management Systems
- Industrial and Utility Network Security
- Boundary Protection
- Wide Area Network Security
- ICS Risk Assessments
- **AND MUCH MORE!**

Real-World Hands-On Labs!

ALSO AVAILABLE AS AN ADD-ON TO THE CS-1000 CYBERSECURITY ESSENTIALS COURSE

Manufacturing is #1 in Cyber Attacks for the Third Straight Year. What Can Be Done?

A 2024 IBM study found that 85% of incidents could have been mitigated with patching, multi-factor authentication or least-privilege principles.

LAB ACTIVITIES

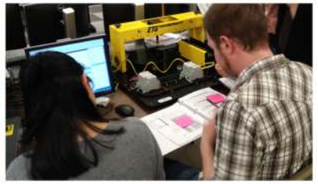
Basic ICS Networking
- Introduction to PLCs, SCADA, and HMI Systems
- Stand-Alone and Multiple Zone PLC Control
- SCADA/HMI Systems
- Data Historian Servers

IT/OT Vulnerabilities
- Exploiting OT Network Vulnerabilities
- Physical MitM Attacks
- IT/OT Reconnaissance
- Exploiting IT/OT Network Vulnerabilities

Cyber Vulnerabilities
- Attacking the Front Door and an Outward-Facing Web Server
- Spear Phishing Attacks
- Installing a Reverse Shell and Exploiting Hashes
- Wireless Perimeter Attacks and WiFi Exploits

Defending the OT Network
- End Point Hardening and DoD Secure Host Compliance
- Network Switch Security
- IT/OT Network Segmentation, VLANs, and Security Routing
- Working with Firewalls and DMZs

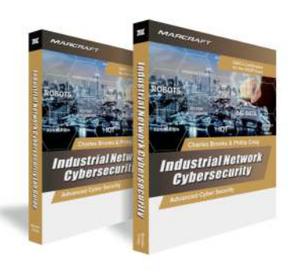
Incident Response and Handling
- Incident Response Handling
- Security Logging and Auditing
- Disaster Recovery (Backup and Restore)

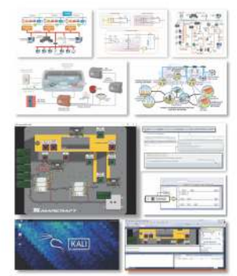


INCLUDES:

CS-3000	Industrial & Utility Cybersecurity Trainer
CS-300SET	2 Sets of the Industrial Network Cybersecurity Textbook & Lab Guide
CS-300IG	Instructors Guide with Digital Media (1 Per Classroom)

Requires 1 PC Workstation Computer





ACCESSORIES:

CS-300SET	Additional Sets of the Industrial Network Cybersecurity Textbook & Lab Guide

"In today's interconnected world, ICS and Operational Technology (OT) cybersecurity has become a critical area of focus. As industries increasingly rely on digital systems to control physical processes, the need to secure these systems has never been more important. OT cybersecurity involves protecting critical infrastructure like power grids, manufacturing plants, and transportation systems from cyber threats. However, hiring skilled professionals in this niche field poses significant challenges. *OT cybersecurity isn't just about IT security; it requires a blend of engineering and security skills.* This specialized skill set makes these professionals unique and in high demand."

SURESH PATEL, A SENIOR CYBERSECURITY ANALYST IN INDUSTRIAL CYBERSECURITY