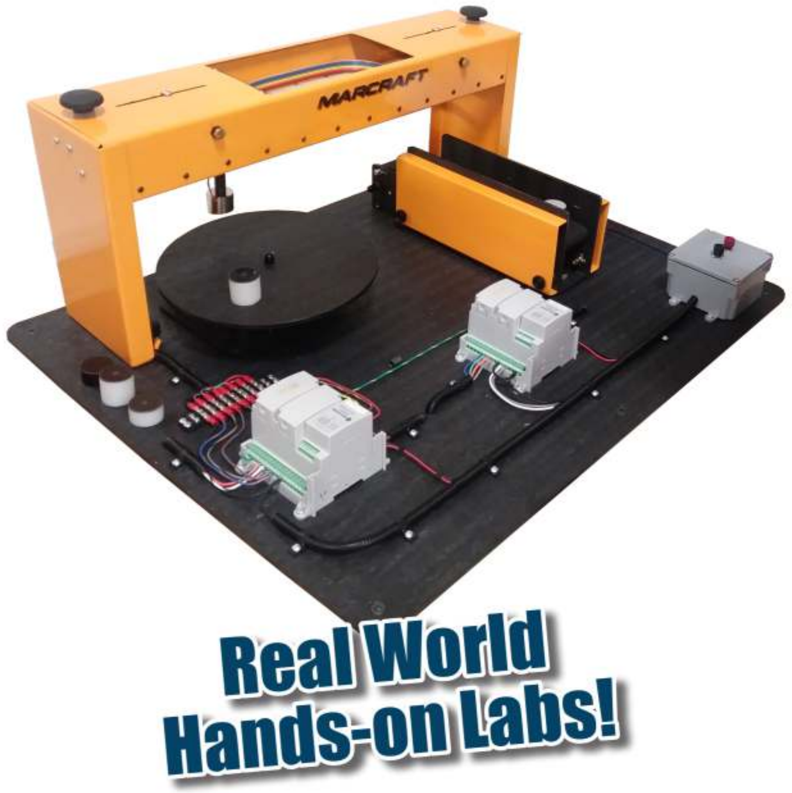
INDUSTRIAL NETWORKS CYBERSECURITY

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

GICSP CERTIFICATION — 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!**

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

> "… Industrial Control Systems (ICS), which constitute the "soft underbelly" of the American economy and defense, can enable a "Cyber Pearl Harbor" to occur without having the capability of even knowing the impacts were cyber-induced..."
>
> STANFORD UNIVERSITY CENTER FOR INTERNATIONAL SECURITY AND COOPERATION

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

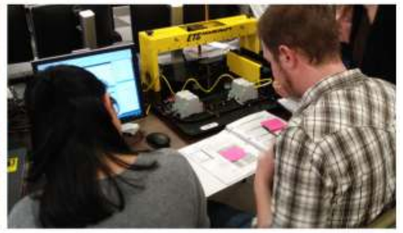
- Attacking the Front Door and an Outward Facing Web Server
- Spear Phishing Attacks
- Installing a Reverse Shell and Exploiting Hashes
- Wireless Perimeter Attacks and WiFi Exploits

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

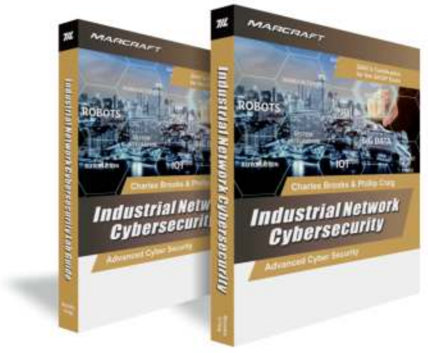
Incident Response and Handling

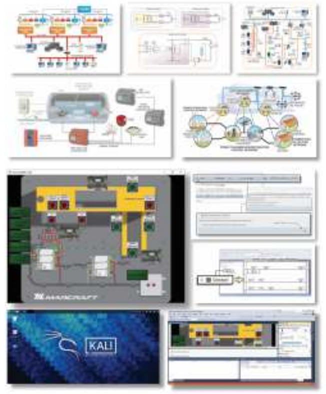
- Incident Response Handling
- Security Logging and Auditing
- Disaster Recovery (Backup and Restore)



INCLUDES:

CS-3000	Industrial Security System Equipment Package which includes 1 Industrial & Utility Cybersecurity Trainer (Requires Dedicated PC Workstation Computers)
CS-300IG	Instructors Guide with PowerPoint Presentation USB Drive (1 Per Classroom)





ACCESSORIES:

CS-300SET	Industrial Security System Text & Lab Book