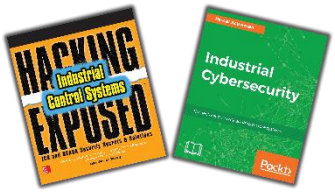
ThreatGEN® Red vs. Blue

ICS 201: Industrial Cybersecurity Vulnerability & Risk Assessment

This course builds upon the knowledge gained in ICS 101 by applying technical cyber risk and vulnerability assessment skills. Through a combination of lecture and hands-on labs, students will learn how to perform standards-based gap assessments and technical ICS vulnerability assessments using industry standard tools and applications. In addition to standard methodologies, they will also learn "ICS safe" methods. Then, they will tie it all together with consequence-driven risk calculation methods.



bonus content:

This course includes content from **Clint Bodungen's upcoming book, "Complete Industrial Cybersecurity Program Management, A Practical Guide to ICS/OT Cyber Risk Management"** Students will learn how to use VBA and PowerShell scripts (in a way that students of all levels can follow and utilize) to automate vulnerability assessment data analysis and maximize the value of vulnerability scanning tool reports.

What you will get out of this class

- Learn to perform security standards-based gap assessments
- Learn and apply consequence-driven risk assessment concepts
- Learn to perform ICS vulnerability assessments in technical hands-on labs
- Learn to perform ICS vulnerability assessments that are safe for ICS environments
- Learn to use VBA and PowerShell scripts to analyze vulnerability assessment data
- Learn to maximize the value of vulnerability scanning tool reports
- Taught by industry-leading, world-class ICS cybersecurity experts with years of real-world experience

Intended Audience

- Anyone interested in gaining beginner to intermediate knowledge of ICS/OT cybersecurity
- Anyone interested in or tasked with ICS/OT risk assessment and management
- Anyone interested in learning more about technical ICS/OT vulnerability assessment
- Cybersecurity managers
- Plant managers and asset owners
- IT cybersecurity staff tasked with ICS/OT cybersecurity
- Engineers tasked with ICS/OT cybersecurity

Outline

1) Overview of Assessments
    a. Types of Assessments
    b. Why and When to Perform an Assessment
2) Vulnerability Assessment Tools
3) Common Vulnerability Assessment Techniques Review/Overview
4) OT/ICS Assessments vs IT Assessments
    a. Why you can't treat ot like IT
    b. What can happen?
5) OT Vulnerability Assessment: Non-Technical Assessments
    a. Key Terms
    b. Site Walk Throughs
    c. Document Review (configs and diagrams)
    d. Standards/Policy Gap Assessment
        i. Using CSET and GRC Tools
    e. Vulnerability Mapping
6) OT Vulnerability Assessment: Technical Assessments
    a. Key Terms
    b. Passive Process
    c. Safe "Scanning" for OT
    d. "Native" Discovery (assets and "scanning")
    e. Maximizing the Value of Vulnerability Assessment Reports with VBA and PowerShell Scripting
7) Putting it All Together: Analysis, Quantification, Scoring & Prioritization
    a. Key Terms
    b. Accounting for "Threat Assessment"
    c. Analysis and Scoring Methods
    d. Prioritizing Risks and Controls
    e. Maximizing the Value of Vulnerability Assessment Reports
    f. Remediation/Mitigation Execution Plan
        1. ii. Building a Remediation/Mitigation POA&M (Plan of Actions and Milestones)
8) Hands-on Lab

THREATGEN

140900 SW FRWY #330, SUGAR LAND, TX 77478 |HTTPS://THREATGEN.COM | INFO@THREATGEN.COM | +1 (833) 339-6753

FOUNDED IN SUGAR LAND, TEXAS IN 2017, THREATGEN DELIVERS A SOLUTION TO BRIDGE "THE ICS CYBERSECURITY SKILLS GAP" UTILIZING ITS RED VS. BLUE ACADEMY AND THREATGEN OT SECURITY SERVICES. THE RED VS. BLUE ACADEMY USES CUTTING-EDGE COMPUTER GAMIFICATION IN THREATGEN® RED VS. BLUE TO PROVIDE AN EXCITING & MODERNIZED APPROACH TO INDUSTRIAL CYBERSECURITY TRAINING, BOTH PRACTICAL AND COST EFFECTIVE! THREATGEN OT SECURITY SERVICES ARE DELIVERED WORLDWIDE BY WORLD-RENOWNED OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY EXPERTS (WE LITERALLY WROTE THE BOOKS INDUSTRY USES) USING STRATEGICALLY CHOSEN PARTNERSHIPS TO CREATE A HOLISTIC SERVICE OFFERING.

June 17th, 2020 version