ThreatGEN® Red vs. Blue

ICS 101: Introduction to Internediate OT/ICS Cybersecurity

Industrial security should be ingrained in your company's culture, equivalent to safety. Cyber incident preparedness begins with people. This class starts from a strategic perspective, helping students "get their head around" the big picture. It introduces beginner to intermediate topics such as OT/ICS vulnerabilities, "*hacker*" methodologies, and security controls at a comfortable and easy to follow pace. These topics are then exercised and reinforced using ThreatGEN® Red vs. Blue cybersecurity training game and other hands-on simulations.

This course will help students gain an understanding of the overall cyber risk management program and strategy, as well as OT/ICS vulnerabilities, basic adversary methods, and the security controls and strategies to defend against them.

What you will get out of this class

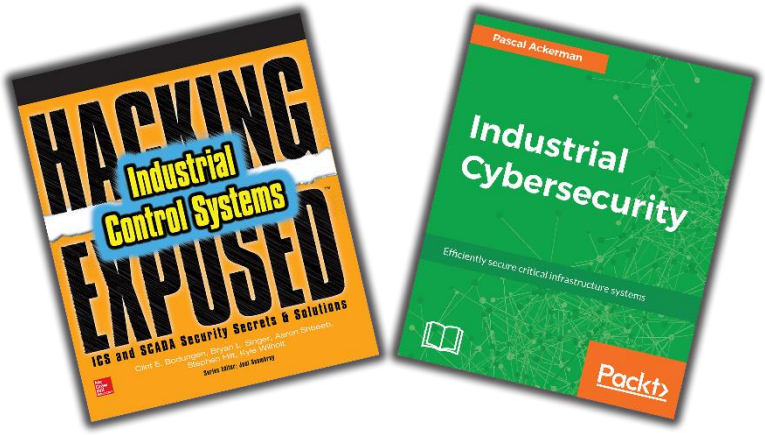
- Gain a comprehensive, "*big picture*" understanding of how all the cybersecurity pieces work together
- An introductory overview of the concepts, function, and components of industrial control systems, equipment, and technology
- Learn vulnerabilities and attack vectors specific to ICS
- Learn about the methods and strategies hackers use to attack industrial control systems as well as traditional IT systems (**Introductory level. This is not a technical hands-on, "hacking" course**)
- Learn and apply practical industrial cybersecurity and risk management concepts
- Learn how to deploy efficient and cost-effective mitigation strategies and security controls
- Learn how to build a complete ICS cyber security program
- Apply what you've learned against a live adversary using the cutting-edge, turn-based computer training simulation/game, ThreatGEN Red vs. Blue
- Learn how to respond to, adapt, and defend against active attacks (**Introductory level, this is not an incident response or threat hunting class**)
- Participate as the blue team and the red team, regardless of experience or technical skill level
- Taught by world-renown 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 gaining a better understanding over the overall cybersecurity "big picture"
- Cybersecurity managers
- Upper management concerned with IT/OT cybersecurity
- Plant managers and asset owners
- IT cybersecurity staff tasked with ICS/OT cybersecurity
- Engineers tasked with ICS/OT cybersecurity
- End users looking for a more effective (and entertaining) cybersecurity awareness training

Outline

1) What is OT Cybersecurity
    a. Cybersecurity is [Cyber] Risk Management
    b. What is OT (30,000 ft. View)
    c. IT Risk vs. OT Risk
    d. When the Solution Becomes Part of the Problem
2) OT Primer
    a. What is OT
    b. OT/ICS vs. IOT
    c. OT Equipment (Devices)
    d. Communication Architecture
    e. Communication Protocols
3) OT Threat Landscape
    a. What's the Risk [to OT]?
    b. The Evolving Threat



June 17th, 2020 version

i. Threat Intelligence vs. Threat Information
ii. Brief History of OT Threats
iii. What to Look For
iv. Who/What Are the Threats?
v. Taxonomy of Potential Threat Sources
vi. Threat Source Capabilities, Motivations, and Objectives

4) OT Cybersecurity/Risk Management Program at a Glance
   a. You Have Questions and you need help…
   b. Your OT Cybersecurity Program
      i. The Trilogy: IT, OT/ICS, Management
      ii. Personnel & Skills
      iii. Governance
      iv. Budget
5) OT Cybersecurity/Risk Management Strategy
   a. Layered Defense is a Great Concept, but…
   b. The Consequence Driven, Risk Modeling Approach
   c. Mitigate Risk vs. Remediating Vulnerability
   d. Cybersecurity Controls vs. Policy
   e. Other OT Consequence Driven Cyber Risk Management Models
      i. RIPE
      ii. Bowtie
6) The Risk Assessment Process
   a. Key Terms
      i. Include Black box, gray box, white box, etc.
   b. The Consequence Driven, Risk Modeling Process
      i. OT Risk Review
   c. System Identification, Classification & Characterization
   d. ATT&CK
7) Vulnerabilities Primer
   a. Key terms
   b. What are Vulnerabilities
   c. Types of Vulnerabilities
8) ICS Specific Vulnerabilities
   a. Industrial Protocol and Communications Vulnerabilities
   b. ICS Workstation/Server Vulnerabilities
   c. OT Equipment/Device Vulnerabilities
   d. Top Issues Found in OT Assessments
9) OT Attack Surface
   a. Key Terms
   b. Anatomy of an Attack
   c. Basic Strategies & Methods
   d. OT Specific Attack/Exploit Strategies
   e. OT/ICS Cyber Kill Chain
   f. Common OT Attack Vectors
10) Cybersecurity Basics: “Blocking and Tackling”
   a. Key Terms
   b. Cyber Security Policies and Procedures
   c. Configuration and System Hardening
   d. Network Security
   e. Physical Security
   f. MoC Program
   g. Anti/Virus and Patch Management
   h. Data Backups
   i. Documentation Maintenance
      i. Internal (configuration management, network diagrams, etc.)
      ii. Industry standards monitoring
      iii. Change Management (MoC)
11) Architecture
   a. Key Terms
   b. Segmentation
   c. The Purdue Model
12) Threat Monitoring
   a. Key Terms
   b. The Big Questions: Do I need it? When do I need it?
   c. Passive vs. “Active”
   d. Available Technology
   e. Event Monitoring
   f. SOC vs. MSSP
   g. Considerations for Building a SOC
13) Incident Response
   a. Key Terms
   b. CERT Program
   c. DHS “ICS-CERT” NCICC Outreach
   d. Local FBI Outreach
   e. Incident Response (IR) Plan
   f. Disaster Recovery & Business Continuity

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.