Critical Infrastructure Security Training Programs for Industry Professionals and University Students

Online Training Module Leading to Professional Certification

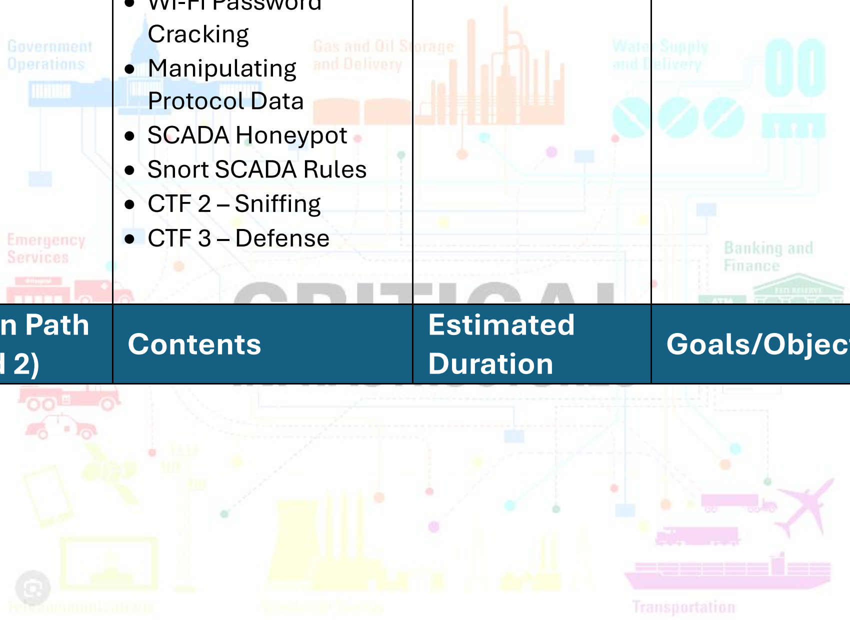
Skill Path (Track 1)	Contents	Estimated Duration	Goals/Objectives
ICS/SCADA Security Fundamentals	• ICS SCADA Security Fundamentals Skill Assessment • Industrial Control Systems (ICS) Introduction • ICS Fundamentals • ICS Operation Environment • ICS Networking • ICS Security Introduction • ICS Security Management • ICS Security Fundamentals Project	**5 hours, 14 mins**	The ICS/SCADA Security Analyst skill path provides fundamental knowledge about SCADA systems and security, including protocols, access controls, physical security, cybersecurity tools and more.
Skill Path (Track 2)	**Contents**	**Estimated Duration**	**Goals/Objectives**
OT/ICS Certified Security Professional	**ICS and SCADA Overview –** • Types of ICS, • ICS Components, • Strenght and Weaknesses, • Process Control Networks and Devices, • IT vs ICS, Modbus, DNP3 and HART Protocols, • Other ICS Protocols, • Open vs Proprietary Protocols, • OLE for Process Control, • ICS Incidents, • Threats to SCADA, Security	**12 hours, 35 mins**	The OT/ICS provides learners with the best practices for securing Operational Technologies, including industrial control systems and SCADA networks. This learning path reveals how to defend against both internal and external attackers to provide comprehensive security for critical infrastructure automation systems.

	Frameworks and Strategy, • Policies, Standards, Procedures and Guildlines, • Developing a SCADA Security Policy, • ICS Security Standards Bodies. **ICS Security Controls –** • Risk Management Process, • ICS Security Objectives, • Security Assessments, • SCADA Security Testing Methodology, • Vulnerability Assessment and Pentesting, • DNS and SNMP Recon, • Host and Port Scanning, • Sniffing Network Traffic, • Device Functionality Analysis, • Common Vulnerabilities, • Vulnerability Scanning, • Server OS Testing, • Authentication and Remote Access, • Attacking Standard Services, • Attacking ICS Protocols, **Pentesting ICS** • Wireless Communication Attacks, • Categorization of System Control, • Physical Safety and Security,		

	- Identification, Authentication and Authorization, - Access Control Models, - Remote Access Security, - Remote Access Technologies, - Field Site Security, - Secure Network Design, - Firewalls, - Logical Security Zones **ICS Security Controls** - IDS/IPS, - Snort, - Log Monitoring and Management, - Incident Response, - Anti-Malware, - Patch Management, - Application Whitelisting, - Active Directory and Group Policy, - SCADA Best Practices: Prevention, - SCADA Best Practices: Detection, - SCADA Best Practices: Correction		

Labs (Hands-On) (Track 1 and 2)	Contents	Estimated Duration	Goals/Objectives

SCADA Cyber Range	• Modbus PLC Introduction • SNMP Reconnaissance • Datasheet Analysis • Scanning ICS/SCADA Networks • CTF1 – Reconnaissance • Attacking the Infrastructure • Firewall Rules for SCADA • Exploiting OS-level Vulnerabilities • Extracting Network Keys • Wi-Fi Password Cracking • Manipulating Protocol Data • SCADA Honeypot • Snort SCADA Rules • CTF 2 – Sniffing • CTF 3 – Defense	**15 hours**	
Certification Path (Track 1 and 2)	**Contents**	**Estimated Duration**	**Goals/Objectives**



CompTIA Security+ (SY0-701, 2024)	• Security Basics • Cryptography • Threats • Attacks • Identity and Access Management • Organization Security • Network Security Devices • Security Operations • Virtualization • Mobile Security • Vulnerability Management • Incident Response • Data Protection • Governance • Security+ 701 practice exam (2024)	**9 hours, 53 mins**	
Career Paths	Cyber Defense Analyst, Threat / Warning Analyst, Vulnerability Assessment Analyst, Network Operations Specialist, Cyber Workforce Developer and Manager, Systems Security Analyst, Cyber Security Analyst/Associate		