

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	 5 hours, 30 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.
	Industrial Control Systems (ICS) Introduction		
	ICS Fundamentals		
	ICS Operation Environment		
	ICS Networking		
	ICS Security Introduction		
	ICS Security Management		
	ICS Security Fundamentals Project		
Skill Path (Track 2)	Contents	Estimated Duration	Goals/Objectives
ICS/SCADA Security Analyst 	SCADA Security Frameworks	 6 hours, 56 mins	The ICS/SCADA Security Analyst skill path provides knowledge needed to defend the systems that control critical infrastructure. Participants would learn about assessing the security of ICS/SCADA systems and protecting them from cyber threats.
	SCADA Security Assessment		
	SCADA Device Identification and Analysis		
	SCADA Vulnerabilities		
	Pentesting SCADA Services and Protocols		
	SCADA Access Controls		
	Remote Access and Field Site Security		
	SCADA Network Security		
	SCADA Intrusion Detection and Incident Response		
	SCADA Preventative Controls		
Labs (Hands-On) (Track 1 and 2)	Contents	Estimated Duration	Goals/Objectives

SCADA Cyber Range	Modbus PLC Introduction	6 hours, 30 mins	
	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		
	ICS/SCADA Pentesting CTF: Lights Out		
Certification Path (Track 1 and 2)	Contents	Estimated Duration	Goals/Objectives
Certified SCADA Security Architect (CSSA)	Introduction to SCADA Security	8 hours, 54 mins	
	ICS Protocols		
	SCADA Security Frameworks		
	SCADA Security Assessment		
	SCADA Device Identification and Analysis		
	SCADA Vulnerabilities		
	Pentesting SCADA Services and Protocols		
	SCADA Access Controls		
	Remote Access and Field Site Security		
	SCADA Network Security		
	SCADA Intrusion Detection and Incident Response		
	SCADA Preventive Controls		
	ICS/SCADA Security Best Practices		
	CSSA Exam Overview		

Career Paths

Cyber Defense Analyst, Threat / Warning Analyst, Vulnerability Assessment Analyst, Network Operations Specialist, Cyber Workforce Developer and Manager, Systems Security Analyst

In-Person Training Module Leading to CEU Certification

Group 1

Occurs Every Friday Succeeding the Online Training

National Wind Institute (NWI)-Reese Technology Center Campus, Building 250

8:00 am to 8:30 am	Registration and Breakfast – Room 106/Conference Room
TRACK 1 Morning –	SCADA – Room 106
8:30 am to 9:00 am	Introduction to the Cyber-Physical Testbed
9:00 am to 10:30 am	Cyber-Physical Security Training on the Real-Time Simulator
10:30 am to 10:45 am	BREAK
10:45 am to 12:00 pm	Distribution Systems SCADA Operations and Security Best Practices
12:00 pm to 12:45 pm	Lunch – Conference Room
TRACK 1 Afternoon – SCADA – Room 106	
1:00 pm to 1:30 pm	Introduction to the Cyber-Physical Testbed
1:30 pm to 2:45 pm	Cyber-Physical Security Training on the Real-Time Simulator
2:45 pm to 3:00 pm	BREAK
3:00 pm to 4:30 pm	Distribution Systems SCADA Operations and Security Best Practices

GLEAMM Microgrid Building

TRACK 2 Morning – Networking and Cyber-Security for Industrial Control Systems	
8:30 am to 9:00 am	Networking Introduction
9:00 am to 10:00 am	Networking / Cyber-Security Concepts
10:00 am to 10:15 am	BREAK
10:15 am to 11:30 am	Hands-on network deployments
11:30 am to 12:00 pm	Hands-on cyber-Security demonstrations
12:00 pm to 12:45 pm	Lunch – NWI Conference Room, Building 250
TRACK 2 Afternoon –	Networking and Cyber-Security for Industrial Control Systems
1:00 pm to 1:30 pm	Networking Introduction
1:30 pm to 2:30 pm	Networking / Cyber-Security Concepts
2:30 pm to 2:45 pm	BREAK
2:45 pm to 4:00 pm	Hands-on network deployments
4:00 pm to 4:30 pm	Hands-on cyber-Security demonstrations

Group 2

Occurs Every Saturday Succeeding the Online Training

National Wind Institute (NWI)-Reese Technology Center Campus, Building 250

8:00 am to 8:30 am	Registration and Breakfast – Room 106/Conference Room
TRACK 1 Morning –	SCADA – Room 106
8:30 am to 9:00 am	Introduction to the Cyber-Physical Testbed
9:00 am to 10:30 am	Cyber-Physical Security Training on the Real-Time Simulator
10:30 am to 10:45 am	BREAK
10:45 am to 12:00 pm	Distribution Systems SCADA Operations and Security Best Practices
12:00 pm to 12:45 pm	Lunch – Conference Room

TRACK 1 Afternoon – SCADA – Room 106

1:00 pm to 1:30 pm	Introduction to the Cyber-Physical Testbed
1:30 pm to 2:45 pm	Cyber-Physical Security Training on the Real-Time Simulator
2:45 pm to 3:00 pm	BREAK
3:00 pm to 4:30 pm	Distribution Systems SCADA Operations and Security Best Practices

GLEAMM Microgrid Building

TRACK 2 Morning – Networking and Cyber-Security for Industrial Control Systems

8:30 am to 9:00 am	Networking Introduction
9:00 am to 10:00 am	Networking / Cyber-Security Concepts
10:00 am to 10:15 am	BREAK
10:15 am to 11:30 am	Hands-on network deployments
11:30 am to 12:00 pm	Hands-on cyber-Security demonstrations
12:00 pm to 12:45 pm	Lunch – NWI Conference Room, Building 250

TRACK 2 Afternoon – Networking and Cyber-Security for Industrial Control Systems

1:00 pm to 1:30 pm	Networking Introduction
1:30 pm to 2:30 pm	Networking / Cyber-Security Concepts
2:30 pm to 2:45 pm	BREAK
2:45 pm to 4:00 pm	Hands-on network deployments
4:00 pm to 4:30 pm	Hands-on cyber-Security demonstrations