ICS Security Courses

FOUNDATIONAL

ICS 310 — **ICS Cybersecurity Foundations™**
Learn the cyber fundamentals to protecting ICS/OT environments.

ESSENTIAL

ICS 410 — **ICS/SCADA Security Essentials™**
Gain the essential skills to keep industrial environments safe from cyber threats.

MANAGEMENT

ICS 418 — **ICS Security Essentials for Leaders™**
Manage the people, processes, and technologies for OT cyber risk programs.

TACTICAL

ICS 456 — **Essentials for NERC Critical Infrastructure Protection™**
Maintain a defensible compliance program up to NERC CIP standards.

ICS 515 — **ICS Visibility, Detection, and Response™**
Monitor threats, perform incident response and enhance network security.

ADVANCED

ICS 612 — **ICS Cybersecurity In-Depth™**
Identify threats in a real-world ICS environment to protect against adversary attacks.

ICS 613 — **ICS/OT Penetration Testing & Assessments™**
Perform safe, hands-on ICS/OT penetration testing & assessments to identify vulnerabilities and improve operational resilience.

ICS Cyber Attacks Normally Require Two Distinct Stages

STAGE 1

Cyber Intrusion Preparation and Execution

PLANNING		Reconnaissance
PREPARATION		Weaponization
		Targeting
CYBER INTRUSION	ATTEMPT	Delivery
		Exploit
	SUCCESS	Install/Modify
MANAGEMENT & ENABLEMENT		C2
SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION		Act

Stage 1 mimics a targeted and structured attack campaign.

Discovery	Movement	Install/Execute	Launch
Capture	Collect	Exfiltrate	Clean/Defend

STAGE 2

ICS Attack Development and Execution

ATTACK DEVELOPMENT & TUNING		Develop
VALIDATION		Test
ICS ATTACK		Deliver
		Install/Modify
		Execute ICS Attack

Enabling Attack	Initiating Attack	Supporting Attack
Trigger	Modify	Hide
Deliver	Inject	Amplify

Stage 2 shows the steps associated with a material attack that requires high confidence.

Based on the Cyber Kill Chain® model from Lockheed Martin

SANS | GIAC CERTIFICATIONS

ICS

POSTER

sans.org/ics

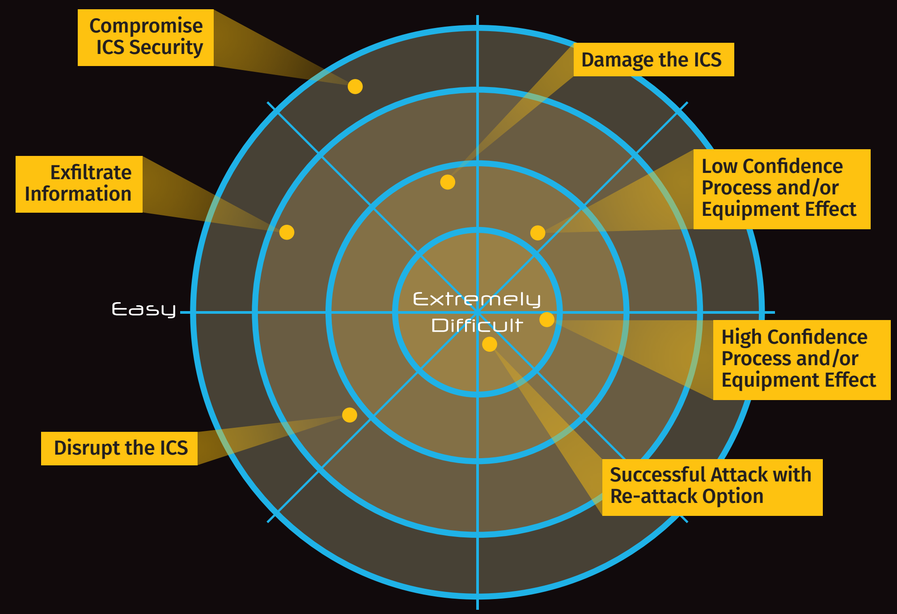
Attacker Objectives

LOSS
- Loss of View
- Loss of Control

DENIAL
- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION
- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments
- Manipulation of Safety

ICS Attack Difficulty



ICS_SCALE_v1.4_04-25

The Sliding Scale of Cybersecurity

ICS410
ICS/SCADA Security Essentials™

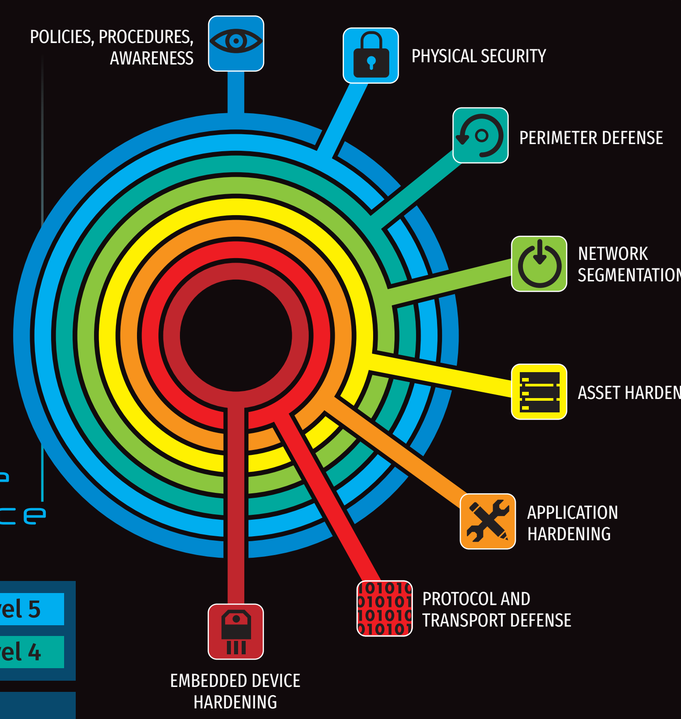
This course builds on foundational ICS cybersecurity principles to provide industrial cybersecurity professionals with the advanced skills necessary to secure OT environments effectively. By focusing on the unique demands of industrial systems, the course equips both IT and OT cybersecurity professionals to address emerging threats, ensuring the safety, security, and resilience of critical infrastructure with minimal operational impact.

ICS515
ICS Visibility, Detection, and Response™

This course teaches how to gain visibility into ICS/OT networks, detect threats, and respond to cyber incidents targeting industrial environments. It empowers students to deconstruct real-world attacks, apply intelligence-driven defense strategies, and enhance network security and reliability.

ARCHITECTURE | **PASSIVE DEFENSE** | **ACTIVE DEFENSE** | **INTELLIGENCE** | **OFFENSE**

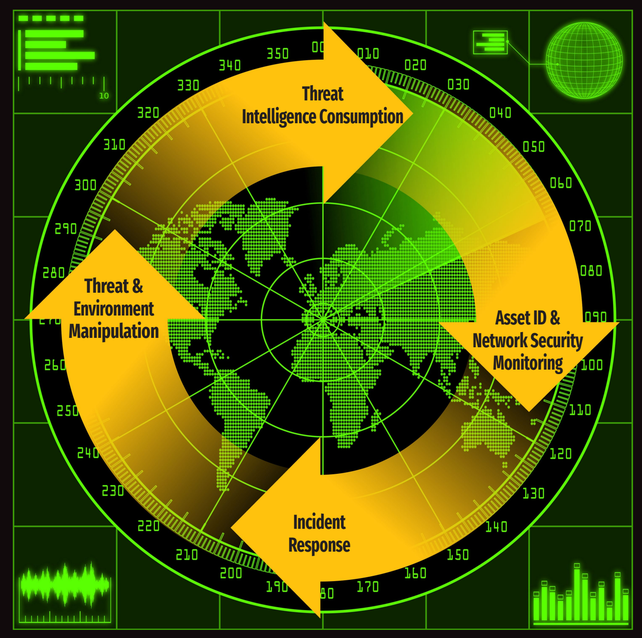
Layers of ICS Defense In Depth



Purdue Reference Model

ENTERPRISE ZONE	Level 5
	Level 4
DMZ	
MANUFACTURING ZONE	Level 3
CELL/AREA ZONE	Level 2
	Level 1
	Level 0

Active Cyber Defense Cycle



The Diamond Model

by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz

NOT RECOMMENDED IN ICS ENVIRONMENTS

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

sans.org/ics
linkedin.com/showcase/sans-ics
ics-community.sans.org/signup
youtube.com/c/SANSICSsecurity
@SANSICS

Poster was created by Rob T. Lee—author of SANS ICS515
ICS_SCALE_v1.4_04-25