SANS | GIAC CERTIFICATIONS

Supported by CSA SINGAPORE Cyber Security Agency of Singapore

# OT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for OT Environment**

**This Course Will Help You To:**

- Analyse APT groups, understanding their motivations, targets, and attack methods to better defend critical infrastructure.
- Apply the MITRE ATT&CK framework to map APT and other attacker techniques.
- Integrate Operational Technology (OT) threat intelligence with IT security operations.
- Design secure network architectures using principles like network segmentation, zero trust, and layered defences.
- Conduct OT asset inventories and map connections between IT and OT systems using the Purdue Model and understanding OT-specific systems.
- Assess risks in OT environments, identifying vulnerabilities in industrial protocols and legacy systems commonly targeted by APT groups in critical infrastructure.
- Implement security controls for OT environments, including network separation, data diodes, patch management for operational systems, and secure remote access.

## Course Overview

Industrial Control Systems (ICS) and Operational Technology (OT) environments are facing increasingly sophisticated cyber threats that can disrupt critical operations and impact safety, reliability, and business continuity. Securing these environments requires cybersecurity professionals with a strong understanding of industrial systems, emerging threats, and effective defence strategies.

This course provides participants with the essential knowledge and practical skills to protect ICS/OT environments, from establishing foundational security principles and maintaining operational resilience to gaining network visibility, detecting threats, responding to incidents, and applying intelligence-driven approaches to cyber defence. Participants will develop the capabilities needed to safeguard industrial operations against current and evolving cyber threats while supporting a safer and more resilient operational environment. This course also equips participants with the knowledge and practical skills needed to prepare for GIAC Response and Industrial Defense (GRID).

### SECTION 1: : ICS CONCEPTS, ARCHITECTURE AND GOVERNANCE

This section lays the groundwork for understanding industrial control systems (ICS), exploring how these environments operate, the roles that support them, and how they differ from traditional IT. Building on this foundation, the course introduces established security program frameworks and walks through the practical steps of building a defensible ICS security posture, from policy development to risk measurement to technical defences across networks, systems, and platforms. These concepts are reinforced through a realistic course scenario and hands-on labs that let students build and operate ICS components themselves.

**TOPICS:**
ICS Processes, Roles, and Industries; Controllers and Field Devices; HMIs, Historians, and SCADA Systems; Ethernet and TCP/IP Concepts; IT and ICS Differences; ICS Security Program Frameworks; SANS 5 Critical Controls; Security Policy Development and Implementation; Risk Measurement Approaches; Enforcement Zone Devices; Basic Cryptography for ICS; Wireless Technologies and Defences; Windows, Unix, and Linux Defence Strategies

SANS | GIAC CERTIFICATIONS

Supported by CSA SINGAPORE Cyber Security Agency of Singapore

# OT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for OT Environment**

**This Course Will Help You To:**

- Harden industrial control systems whilst maintaining operational availability against APT persistence techniques.
- Configure OT monitoring tools in industrial protocols and identify APT threats.
- Develop incident response plans for OT environments.
- Investigate OT security incidents using structured techniques and map findings to the MITRE ATT&CK for ICS frameworks.
- Establish procedures to safely restore OT systems after APT incidents.

## SECTION 2: ICS CYBER THREAT INTELLIGENCE

This section introduces the discipline of active defence within industrial control systems, grounded in a real-world case study of an attack on a CHP plant. Students are introduced to cyber threat intelligence and the ICS cyber kill chain, exploring how intelligence is consumed and applied to strengthen an organization's defensive posture, along with the role of open-source intelligence (OSINT) in understanding the ICS threat landscape. These concepts are reinforced through hands-on labs applying structured analytical techniques, mapping the ICS information attack space, and using tools like Maltego and Shodan to visualize exposure.

**TOPICS:**
ICS Active Defence; Cyber Threat Intelligence; ICS Cyber Kill Chain; Threat Intelligence Consumption; ICS OSINT

## SECTION 3: VISIBILITY AND ASSET IDENTIFICATION

This section addresses the challenge of gaining true visibility into ICS environments, beginning with a real-world case study of a sophisticated intrusion into critical infrastructure. Students learn approaches to building asset inventories and collection management frameworks, along with the network visibility techniques and discovery protocols needed to understand what's actually running in an ICS environment. The course also examines how preventive controls degrade over time and the frameworks used to guide patching decisions, before moving into the analysis of ICS protocols using tools like Wireshark. These concepts are reinforced through hands-on labs covering ICS traffic analysis, protocol analysis, and network mapping.

**TOPICS:**
Asset Inventories and Collection Management Frameworks; ICS Network Visibility and Discovery Protocols; Prevention Atrophy and Patching Decision Frameworks; ICS Protocol Analysis

SANS | GIAC CERTIFICATIONS

Supported by CSA SINGAPORE Cyber Security Agency of Singapore

# OT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for OT Environment**

## SECTION 4: ICS THREAT DETECTION

This section focuses on building detection capabilities across ICS environments, examining how threat hunting and detection strategies apply to industrial systems and grounding the discussion in a real-world case study of a major attack on critical infrastructure. Students explore common points of compromise, including supervisory servers and HMI and UI vulnerabilities, alongside the tools and approaches used to monitor ICS networks and endpoints, such as network security monitoring and SIEM platforms. These concepts are reinforced through hands-on labs covering the detection and investigation of multi-stage intrusions, traffic analysis of control manipulation, and verification of system logic and field-level integrity.

**TOPICS:**
ICS Threat Hunting; Threat Detection Strategies; Supervisory Server Attacks; HMI and UI Vulnerabilities; ICS Network Security Monitoring; Endpoint Protection and SIEMs

## SECTION 5: ICS INCIDENT RESPONSE AND THREAT AND ENVIRONMENT MANIPULATION

This section covers the fundamentals of digital forensics and incident response as applied to ICS environments, beginning with how to prepare an ICS incident response team and grounding the discussion in a real-world case study of malware designed to target safety instrumented systems. Students examine the forensic data sources available across ICS networks and gain hands-on experience with acquisition in operational environments, PLC logic and protocol analysis for root cause investigation, HMI memory forensics, and process triage. The section then turns to the offensive side of the equation, exploring the goals behind threat manipulation, the considerations involved in manipulating an ICS environment, and the process of triaging and analyzing malware, reinforced through a lab in logic analysis for root cause determination.

**TOPICS:**
ICS Digital Forensics and Incident Response; ICS Incident Response Team Preparation; Forensic Data Sources in ICS Networks; ICS Threat Manipulation Goals; Environment Manipulation Considerations; Threat Analysis and Malware Triaging

SANS | GIAC CERTIFICATIONS

Supported by CSA SINGAPORE Cyber Security Agency of Singapore

# OT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for OT Environment**

**SECTION 6: GRID NETWARS**

This capstone exercise challenges students to apply everything they've learned across a realistic, multi-stage incident that spans both IT and OT environments. Participants work through the full arc of a real-world attack, from initial incident response as the adversary pivots from the enterprise network into the OT environment, through the challenges of adversarial access and reconnaissance, to deep analysis of logs, packet captures, and other digital artefacts to understand how the adversary caused system outages. The exercise culminates in recovery efforts, requiring participants to apply their knowledge to restore the integrity of the system and process to normalcy.

**TOPICS:**
IT/OT Incident Response; Adversary Pivoting from Enterprise to OT; Adversarial Access and Reconnaissance; OT/ICS Log and PCAP Analysis; System Outage Root Cause Analysis; Recovery and System Integrity Restoration

## GRID
**Response and Industrial Defense**
**giac.org/grid**

### GIAC Response and Industrial Defense

The GRID certification validates a practitioner's command of Active Defense strategies for protecting Industrial Control System (ICS) networks and systems, including how !CS-specific attacks inform mitigation strategies and how to apply network security monitoring, digital forensics, and incident response in an industrial context.

- Active Defense Concepts and ICS-Specific Attacks
- Network Security Monitoring and ICS Protocol Analysis
- Digital Forensics and Incident Response for Industrial Environments

**Strengthen detection. Accelerate response. Build resilience.**
Contact **Singapore@sans.org** for registration, eligibility and GIAC certification details

**Sign up today**