Training Course on Operational Technology and Industrial Control Systems Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected world, the convergence of Information Technology (IT) and Operational Technology (OT) has introduced unprecedented cyber risks to critical infrastructure. Industrial Control Systems (ICS), which underpin sectors like energy, manufacturing, and transportation, are increasingly vulnerable to sophisticated cyberattacks. This necessitates a specialized approach to cybersecurity, particularly in the realm of digital forensics. Training Course on Operational Technology and Industrial Control Systems Forensics is designed to equip professionals with the advanced knowledge and practical skills required to conduct effective forensic investigations in complex OT/ICS environments, ensuring the resilience and security of vital industrial operations.

Understanding the unique characteristics of OT/ICS, from legacy systems to real-time process demands, is paramount for successful incident response and forensic analysis. Unlike traditional IT forensics, OT/ICS forensics requires a deep appreciation for safety, availability, and the potential physical consequences of cyber incidents. This course delves into the methodologies, tools, and best practices essential for identifying, containing, eradicating, and recovering from cyberattacks on industrial control systems, ultimately strengthening an organization's overall cybersecurity posture and minimizing operational disruptions.

Programme Curriculum

Training Course on Operational Technology and Industrial Control Systems Forensics

Introduction

In today's interconnected world, the convergence of Information Technology (IT) and Operational Technology (OT) has introduced unprecedented cyber risks to critical infrastructure. Industrial Control Systems (ICS), which underpin sectors like energy, manufacturing, and transportation, are increasingly vulnerable to sophisticated cyberattacks. This necessitates a specialized approach to cybersecurity, particularly in the realm of digital forensics. Training Course on Operational

Technology and Industrial Control Systems Forensics is designed to equip professionals with the advanced knowledge and practical skills required to conduct effective forensic investigations in complex OT/ICS environments, ensuring the resilience and security of vital industrial operations.

Understanding the unique characteristics of OT/ICS, from legacy systems to real-time process demands, is paramount for successful incident response and forensic analysis. Unlike traditional IT forensics, OT/ICS forensics requires a deep appreciation for safety, availability, and the potential physical consequences of cyber incidents. This course delves into the methodologies, tools, and best practices essential for identifying, containing, eradicating, and recovering from cyberattacks on industrial control systems, ultimately strengthening an organization's overall cybersecurity posture and minimizing operational disruptions.

Course Duration

10 days

Course Objectives

This comprehensive training aims to empower participants with the ability to:

1. Understand the unique architecture and components of Operational Technology (OT) and Industrial Control Systems (ICS).
2. Differentiate between IT forensics and OT/ICS forensics methodologies and challenges.
3. Identify common threat vectors, vulnerabilities, and attack scenarios targeting industrial environments.
4. Master techniques for incident response and digital evidence collection in live OT/ICS systems.
5. Perform forensic imaging and data acquisition from diverse industrial devices (PLCs, RTUs, HMIs).
6. Analyze proprietary industrial protocols and network traffic for malicious activity.
7. Utilize specialized OT/ICS forensic tools and techniques for evidence examination.
8. Conduct malware analysis and reverse engineering specific to industrial control systems.
9. Develop effective containment strategies and eradication plans for OT/ICS incidents.
10. Implement robust recovery procedures and post-incident activities to restore operational integrity.
11. Apply relevant legal and regulatory frameworks governing OT/ICS cybersecurity and data handling.
12. Build comprehensive forensic reports and present findings to technical and non-technical stakeholders.
13. Contribute to an organization's proactive threat hunting and resilience building in industrial environments.

Organizational Benefits

- Strengthens defense against evolving cyber threats targeting critical infrastructure.
- Enables rapid incident response and recovery, minimizing operational disruptions and associated costs.
- Ensures adherence to industry regulations and standards, reducing legal and reputational risks.
- Safeguards essential industrial processes, intellectual property, and sensitive operational data.
- Equips internal teams with specialized expertise, reducing reliance on external consultants during incidents.
- Fosters a culture of proactive threat hunting and vulnerability management.

- Develops structured and efficient incident response plans tailored to OT/ICS environments.
- Contributes to the overall resilience and continuity of critical industrial operations.

Target Audience

1. Industrial Cybersecurity Analysts
2. OT Security Engineers
3. Incident Response Teams (IT and OT)
4. Digital Forensics Investigators
5. Control Systems Engineers and Technicians
6. Critical Infrastructure Operators
7. Security Operations Center (SOC) Analysts
8. IT/OT Managers and Decision-Makers

Course Outline

Module 1: Introduction to OT/ICS and Cyber-Physical Systems

- Defining Operational Technology (OT) and Industrial Control Systems (ICS).
- Key differences between IT and OT environments.
- Understanding SCADA, DCS, PLCs, RTUs, and HMIs.
- The convergence of IT/OT and its security implications.
- Cyber-Physical Systems (CPS) and their criticality.
- *Case Study:* Stuxnet Attack – Analyzing the initial compromise and its impact on Iranian centrifuges.

Module 2: The OT/ICS Threat Landscape

- Common threat actors, motivations, and attack methodologies.
- Notable ICS cybersecurity incidents and their consequences.
- Vulnerabilities specific to industrial protocols and legacy systems.
- Ransomware, wiper malware, and advanced persistent threats (APTs) in OT.
- Supply chain risks in industrial environments.
- *Case Study:* Colonial Pipeline Ransomware Attack – Examining the disruption, impact, and response to a critical infrastructure incident.

Module 3: Foundations of Digital Forensics for OT/ICS

- Digital Forensics Incident Response (DFIR) lifecycle in OT.
- Legal considerations and chain of custody for industrial evidence.
- Forensic readiness and preparedness for OT environments.
- Data integrity, preservation, and anti-forensics in ICS.
- Developing an OT/ICS incident response plan.
- *Case Study:* Ukraine Power Grid Attacks (2015/2016) – Analyzing the synchronized cyber-attacks and the forensic challenges.

Module 4: Incident Response in OT/ICS Environments

- Phases of incident response: preparation, identification, containment, eradication, recovery, post-incident.
- Establishing an OT/ICS incident response team.
- Communication protocols during an industrial cyber incident.
- Leveraging threat intelligence for proactive defense.
- Forensic triage and prioritization in live OT systems.

- *Case Study:* Triton (TRISIS/HatMan) Malware Attack – Investigating an attack designed to manipulate safety instrumented systems.

Module 5: Evidence Collection from OT/ICS Devices

- Challenges of volatile and non-volatile data acquisition in OT.
- Techniques for imaging PLCs, RTUs, and industrial workstations.
- Memory forensics in Windows and Linux-based ICS systems.
- Forensic acquisition from proprietary and embedded devices.
- Best practices for remote and on-site evidence collection.
- *Case Study:* Maroochy Water Breach – Discussing the historical example of remote access and system manipulation.

Module 6: Network Forensics for Industrial Control Systems

- Understanding industrial network architectures (Purdue Model, ISA/IEC 62443).
- Capturing and analyzing industrial network traffic (SCADA, Modbus, DNP3, EtherNet/IP).
- Identifying anomalous network behavior and intrusions.
- Deep packet inspection of proprietary and standard industrial protocols.
- Tools and techniques for network forensics in OT (Wireshark, Zeek).
- *Case Study:* CrashOverride/Industroyer Attack – Analyzing network-based attacks on power substations.

Module 7: Host Forensics on Industrial Workstations

- Forensic analysis of Windows and Linux operating systems in OT.
- Examining file systems, registry, event logs, and memory.
- Identifying persistence mechanisms and malware artifacts.
- Analyzing application logs and configuration files relevant to ICS.
- Extracting evidence from Human-Machine Interfaces (HMIs).
- *Case Study:* NotPetya Ransomware Impact on Industrial Entities – Focusing on the widespread impact on IT/OT convergence points.

Module 8: Programmable Logic Controller (PLC) Forensics

- Understanding PLC programming languages and execution.
- Acquisition of PLC logic, firmware, and configuration.
- Analyzing changes in PLC programs and data tables.
- Identifying unauthorized code injection and manipulation.
- Vendor-specific tools and techniques for PLC forensics.
- *Case Study:* German Steel Mill Attack – Exploring the manipulation of industrial control systems to cause physical damage.

Module 9: Malware Analysis in OT/ICS Context

- Characteristics of malware targeting industrial systems.
- Static and dynamic analysis techniques for OT malware.
- Reverse engineering industrial malware components.
- Sandbox environments for safe analysis of OT threats.
- Attribution and threat intelligence from malware analysis.
- *Case Study:* Havex Malware – Examining an attack specifically targeting SCADA systems for reconnaissance.

Module 10: Data Analysis and Correlation for OT/ICS Incidents

- Correlating event logs from diverse OT/IT sources.
- Utilizing Security Information and Event Management (SIEM) for OT data.
- Time-lining events and reconstructing attack narratives.
- Automated tools and scripts for large-scale data analysis.
- Identifying indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).
- *Case Study:* Saudi Aramco Attack (Shamoon) – Analyzing a data-wiping attack and its impact on operational IT.

Module 11: Cloud and IIoT Forensics in OT Environments

- Forensic challenges of Industrial Internet of Things (IIoT) devices.
- Cloud-based OT systems and their forensic implications.
- Data acquisition from IIoT sensors and gateways.
- Analyzing cloud logs and platform-specific evidence.
- Securing the IIoT attack surface.
- *Case Study:* Recent attacks on smart factory environments leveraging IIoT vulnerabilities.

Module 12: Legal, Regulatory, and Ethical Considerations

- Overview of critical infrastructure regulations (e.g., NERC CIP, ISA/IEC 62443).
- Data privacy and legal implications in forensic investigations.
- Ethical hacking and responsible disclosure in OT.
- Expert witness testimony and presenting forensic findings in court.
- International cooperation in cross-border cyber incidents.
- *Case Study:* Legal ramifications and compliance failures in a significant industrial cyber breach.

Module 13: Reporting and Presenting Forensic Findings

- Structure and content of comprehensive forensic reports.
- Tailoring reports for technical and non-technical audiences.
- Effective visualization of complex forensic data.
- Presenting findings to management, legal teams, and law enforcement.
- Recommendations for remediation and future prevention.
- *Case Study:* Review of a well-structured and impactful forensic report from a past ICS incident.

Module 14: Advanced OT/ICS Forensics Techniques

- Automated forensic collection and analysis in large-scale environments.
- Digital Twins and their role in forensic simulations.
- AI and Machine Learning applications in anomaly detection and forensics.
- Proactive threat hunting methodologies in OT.
- Integration of IT and OT forensic capabilities.
- *Case Study:* Research and development of a novel forensic technique applied to an ICS testbed.

Module 15: Building a Resilient OT/ICS Forensic Program

- Developing an organizational strategy for OT/ICS forensics.
- Budgeting and resource allocation for forensic capabilities.
- Training and continuous professional development for forensic teams.
- Collaboration with external forensic experts and law enforcement.
- Continuous improvement and lessons learned from incidents.

- *Case Study:* A successful example of an organization building and maturing its internal OT/ICS forensic capabilities.

Training Methodology

This course employs a highly interactive and practical training methodology, combining theoretical instruction with extensive hands-on labs and real-world case studies.

- **Instructor-Led Sessions:** Expert-led presentations and discussions to cover core concepts.
- **Hands-on Labs:** Practical exercises using simulated OT/ICS environments, real industrial hardware (where feasible), and industry-standard forensic tools. Participants will gain direct experience in evidence acquisition, analysis, and reporting.
- **Case Study Analysis:** In-depth examination of historical and recent OT/ICS cyber incidents to understand attack vectors, impact, and response strategies.
- **Group Discussions and Workshops:** Collaborative problem-solving and sharing of best practices among participants.
- **Upcoming Scheduled Sessions**

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com