Training Course on Investigating Cyber-Physical System Attacks

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Cyber-Physical Systems (CPS) are the backbone of modern critical infrastructure, seamlessly integrating computational algorithms with physical processes. From smart grids and autonomous vehicles to advanced manufacturing and healthcare, these interconnected systems underpin our daily lives. However, their increasing complexity and interconnectedness also present a burgeoning attack surface for sophisticated **cyber threats**. The convergence of IT and OT (Operational Technology) demands a specialized understanding of how cyberattacks can manifest in the physical world, leading to potentially catastrophic consequences like system failures, environmental damage, or even loss of life. Training Course on Investigating Cyber-Physical System Attacks is meticulously designed to equip professionals with the essential knowledge and practical skills to proactively defend, meticulously investigate, and effectively respond to **Cyber-Physical System attacks**.

As the digital and physical realms continue to converge, the urgency for skilled **cybersecurity professionals** capable of navigating this intricate landscape intensifies. Traditional cybersecurity approaches often fall short in addressing the unique vulnerabilities and operational characteristics of CPS. This course delves into the methodologies and tools necessary to conduct thorough **digital forensics** and **incident response** in CPS environments, emphasizing the critical interplay between cyber intrusion and physical impact. Participants will gain hands-on experience in identifying attack vectors, analyzing compromised systems, and implementing robust mitigation strategies to safeguard these vital infrastructures against evolving and complex **Advanced Persistent Threats (APTs)** and **ransomware attacks**.

Programme Curriculum

Training Course on Investigating Cyber-Physical System Attacks

Introduction

Cyber-Physical Systems (CPS) are the backbone of modern critical infrastructure, seamlessly integrating computational algorithms with physical processes. From smart grids and autonomous vehicles to advanced manufacturing and healthcare, these interconnected systems underpin our daily lives. However, their increasing complexity and interconnectedness also present a burgeoning attack surface for sophisticated **cyber threats**. The convergence of IT and OT (Operational Technology) demands a specialized understanding of how cyberattacks can manifest in the physical world, leading to potentially catastrophic consequences like system failures, environmental damage, or even loss of life. Training Course on Investigating Cyber-Physical System Attacks is meticulously designed to equip professionals with the essential knowledge and practical skills to proactively defend, meticulously investigate, and effectively respond to **Cyber-Physical System attacks**.

As the digital and physical realms continue to converge, the urgency for skilled **cybersecurity professionals** capable of navigating this intricate landscape intensifies. Traditional cybersecurity approaches often fall short in addressing the unique vulnerabilities and operational characteristics of CPS. This course delves into the methodologies and tools necessary to conduct thorough **digital forensics** and **incident response** in CPS environments, emphasizing the critical interplay between cyber intrusion and physical impact. Participants will gain hands-on experience in identifying attack vectors, analyzing compromised systems, and implementing robust mitigation strategies to safeguard these vital infrastructures against evolving and complex **Advanced Persistent Threats (APTs)** and **ransomware attacks**.

Course Duration

5 days

Course Objectives

1. Grasp the fundamental components, interdependencies, and communication protocols within diverse Cyber-Physical Systems.
2. Pinpoint common vulnerabilities and exposure points across various industrial control systems (ICS), SCADA, and IoT devices.
3. Characterize the latest **AI-powered cyberattacks**, **ransomware**, and **supply chain risks** targeting CPS.
4. Apply specialized **forensic techniques** to collect, preserve, and analyze evidence from compromised operational technology environments.
5. Develop and implement robust **incident response plans** tailored for CPS security breaches, minimizing physical impact.
6. Leverage **cyber threat intelligence** to anticipate and mitigate novel attack methodologies against critical infrastructure.
7. Employ **machine learning** and **AI for threat detection** to identify anomalous behaviors indicative of CPS attacks.
8. Proactively identify, assess, and remediate **vulnerabilities** in CPS components and networks.
9. Apply best practices for **ICS cybersecurity**, including network segmentation and secure configurations.
10. Understand the characteristics and impact of **malware** specifically designed to target and disrupt Cyber-Physical Systems.
11. Design and implement **resilient CPS architectures** to withstand and recover from sophisticated cyberattacks.
12. Navigate and adhere to relevant **cybersecurity regulations** and standards for critical infrastructure protection.

13. Gain practical experience through **hands-on labs** and **attack simulations** to hone investigation and response skills.

Organizational Benefits

- Minimize downtime and protect critical services from **cyber-physical disruptions**.
- Mitigate the economic impact of **data breaches**, system failures, and regulatory fines.
- Build a proactive and robust defense against sophisticated and evolving **cyber threats**.
- Ensure adherence to industry regulations and effectively manage **cyber risk** within CPS environments.
- Develop a highly skilled team capable of rapid and effective **incident handling** and recovery.
- Safeguard critical infrastructure, preventing attacks that could lead to physical harm or fatalities.
- Maintain public trust and organizational credibility by demonstrating strong **cybersecurity governance**.

Target Audience

1. Cybersecurity Analysts
2. Industrial Control System (ICS) Engineers
3. Security Operations Center (SOC) Personnel
4. IT/OT Convergence Teams
5. Incident Response Teams.
6. Forensic Investigators
7. Risk Management Professionals.
8. System Architects and Engineers

Course Outline

Module 1: Introduction to Cyber-Physical Systems and Their Security Landscape

- Understanding CPS Fundamentals
- Convergence of IT and OT
- CPS Attack Vectors and Threat Actors
- Impact of CPS Attacks:
- Legal and Regulatory Frameworks
- **Case Study: Stuxnet (2010):** Analysis of the sophisticated malware attack on Iran's nuclear program, demonstrating the physical impact of a cyberattack on centrifuges.

Module 2: CPS Architecture and Vulnerability Assessment

- Common CPS Architectures
- Component-Level Vulnerabilities.
- Network Protocols in CPS.
- Vulnerability Scanning and Penetration Testing for OT
- Risk Assessment Frameworks for CPS
- **Case Study: Colonial Pipeline Ransomware Attack (2021):** Investigating how a ransomware attack on IT systems forced the shutdown of operational pipelines, highlighting IT/OT convergence risks.

Module 3: Digital Forensics in Cyber-Physical Environments

- Principles of Digital Forensics

- Challenges of Forensics in OT
- Evidence Collection from ICS/SCADA Systems
- Network Forensics for Industrial Networks.
- Memory and Disk Forensics in CPS.
- **Case Study: Ukraine Power Grid Attack (2015 & 2016):** Forensic analysis of the BlackEnergy and Industroyer malware attacks, detailing how attackers gained access and manipulated ICS components to cause power outages.

Module 4: Incident Response and Threat Hunting for CPS

- CPS Incident Response Lifecycle
- Containment, Eradication, and Recovery.
- Threat Hunting in OT Networks
- Playbooks for CPS Incidents
- Communication and Coordination During Incidents
- **Case Study: Saudi Aramco Shamoon Attack (2012):** Examining the destructive malware attack that wiped data on tens of thousands of workstations, showcasing the importance of rapid containment and recovery.

Module 5: Malware Analysis and Reverse Engineering for CPS

- Introduction to Malware Analysis
- Static and Dynamic Analysis Techniques
- Malware Families Targeting CPS.
- Reverse Engineering Industrial Protocols
- Indicators of Compromise (IOCs) and Detection Signatures
- **Case Study: TRITON/TRISIS Attack (2017):** Analysis of the malware designed to target Schneider Electric's Triconex safety instrumented systems, demonstrating the potential for physical destruction.

Module 6: Security Monitoring and SIEM for CPS

- Log Management and Correlation in OT.
- Security Information and Event Management (SIEM) for CPS
- Behavioral Analytics and Anomaly Detection.
- Threat Detection and Alerting
- Integrating IT and OT Security Monitoring.
- **Case Study: Maroochy Shire Council Sewage Spill (2000):** A precursor to modern CPS attacks, where a disgruntled former employee remotely accessed and controlled the sewage system, highlighting the need for robust access control and monitoring.

Module 7: Advanced Topics in CPS Security

- Supply Chain Security for CPS
- Cloud Security in CPS Context
- Artificial Intelligence and Machine Learning in CPS Security.
- Quantum Computing and CPS Security
- Homeland Security and Critical Infrastructure Protection
- **Case Study: Water Treatment Plant Intrusion (Florida, 2021):** An incident where an attacker attempted to increase sodium hydroxide levels, illustrating the real-world safety implications and the need for multi-layered defense.

Module 8: Practical Application and Capstone Project

- Hands-on Lab: Setting up a Mini-CPS Environment
- Attack Simulation and Penetration Testing Lab.
- Forensic Investigation Workshop
- Incident Response Tabletop Exercise
- Capstone Project
- **Case Study: Real-world Industry Examples (Varied):** Discussing several recent, publicly reported, but unnamed, incidents across different critical infrastructure sectors, focusing on lessons learned and best practices.

Training Methodology

This course employs a **blended learning approach** to maximize engagement and knowledge retention for technical professionals.

- **Instructor-Led Sessions:** Interactive lectures, discussions, and Q&A sessions led by industry experts.
- **Hands-on Labs:** Extensive practical exercises using realistic simulated Cyber-Physical System environments and specialized cybersecurity tools. This will involve virtualized ICS/SCADA systems, network traffic analysis tools, and forensic workstations.
- **Case Study Analysis:** In-depth examination of real-world CPS attack incidents to understand attack methodologies, impact, and response strategies.
- **Group Activities and Discussions:** Collaborative problem-solving, peer learning, and knowledge sharing among participants.
- **Attack Simulations and Tabletop Exercises:** Experiential learning through controlled attack scenarios to practice incident response and decision-making under pressure.
- **Demonstrations:** Live demonstrations of attack techniques, forensic procedures, and security tool usage.
- **Capstone Project:** A culminating project that integrates all learned concepts, providing a practical application of skills.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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