# Advanced Cybersecurity in Laboratory Systems Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Biotechnology and Pharmaceutical Development | **Duration** | 10 Days |
| **Base Fee** | $4,000 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

Laboratory systems, including LIMS (Laboratory Information Management Systems), Chromatography Data Systems (CDS), and integrated IoT/OT devices, are the new high-value targets for sophisticated cyber threats. The convergence of Operational Technology (OT) with traditional IT networks in modern laboratories presents a unique and expanding attack surface. Advanced Cybersecurity in Laboratory Systems Training Course moves beyond basic security protocols to delve into threat modeling specific to the regulatory and operational environment of a lab. We focus on securing GXP compliant systems, protecting sensitive Intellectual Property (IP), and ensuring data integrity against increasingly automated and stealthy attacks. Graduates will master the Zero Trust Architecture (ZTA) principles and apply cutting-edge techniques in incident response to secure critical scientific data and maintain business continuity.

The field of Cybersecurity in Laboratory Systems is evolving at an unprecedented pace, primarily due to the rapid integration of Operational Technology (OT), Internet of Things (IoT), and Cloud Computing into traditional laboratory environments. This convergence introduces complex cyber-physical risks that threaten the integrity of scientific research, development, and patient safety. Traditional IT security measures are often inadequate for the specialized and often proprietary systems found in research, clinical, and industrial labs, which include everything from high-tech analyzers to automated robotics. A single security failure can compromise critical research data, lead to regulatory non-compliance, and halt essential operational workflows.

## Programme Curriculum

**Advanced Cybersecurity in Laboratory Systems Training Course**

**Introduction**

Laboratory systems, including LIMS (Laboratory Information Management Systems), Chromatography Data Systems (CDS), and integrated IoT/OT devices, are the new high-value targets for sophisticated cyber threats. The convergence of Operational Technology (OT) with traditional IT networks in modern laboratories presents a unique and expanding attack surface. Advanced Cybersecurity in Laboratory Systems Training Course moves beyond basic security protocols to delve into threat modeling specific to the regulatory and operational environment of a lab. We focus on securing GXP compliant systems, protecting sensitive Intellectual Property (IP), and ensuring data integrity against increasingly automated and stealthy attacks. Graduates will master the Zero Trust Architecture (ZTA) principles and apply cutting-edge techniques in incident response to secure critical scientific data and maintain business continuity.

The field of Cybersecurity in Laboratory Systems is evolving at an unprecedented pace, primarily due to the rapid integration of Operational Technology (OT), Internet of Things (IoT), and Cloud Computing into traditional laboratory environments. This convergence introduces complex cyber-physical risks that threaten the integrity of scientific research, development, and patient safety. Traditional IT security measures are often inadequate for the specialized and often proprietary systems found in research, clinical, and industrial labs, which include everything from high-tech analyzers to automated robotics. A single security failure can compromise critical research data, lead to regulatory non-compliance, and halt essential operational workflows.

**Course Duration**

10 days

**Course Objectives**

1. Master the unique security challenges of Operational Technology (OT) and Industrial Control Systems (ICS) within the laboratory environment.
2. Design and deploy a Zero Trust Architecture (ZTA) specifically for segregated lab networks and instruments.
3. Conduct advanced Threat Modeling for complex cyber-physical laboratory systems
4. Implement security controls to ensure ALCOA+ principles and compliance with regulations like FDA 21 CFR Part 11.
5. Apply Digital Forensics and Triage techniques specific to compromised lab instrumentation and data files.
6. Evaluate and mitigate Supply Chain Risks associated with lab software, consumables, and instrument firmware.
7. Secure lab data and applications migrated to Cloud platforms
8. Develop targeted Vulnerability Management programs for legacy, unpatchable, or embedded lab devices.
9. Develop and execute tailored Cyber Incident Response Plans (CIRP) for operational downtime in clinical/research labs.
10. Utilize the MITRE ATT&CK for ICS framework to analyze and defend against attacks on lab control systems.
11. Enforce Secure Configuration Baselines for various operating systems and specialized lab applications.
12. Integrate AI/ML tools for Threat Detection and Anomaly Detection in high-volume lab network traffic.
13. Secure Genomic Data and Bioinformatics Pipelines from manipulation and unauthorized access.

**Target Audience**

1. Laboratory IT/OT Professionals.

2. Information Security Analysts/Engineers.
3. Quality Assurance (QA)/Compliance Officers.
4. Laboratory Managers/Directors.
5. Biomedical/Clinical Engineers.
6. Validation/Qualification Specialists.
7. IT/OT Auditors.
8. R&D Scientists/Engineers.

**Course Modules**

**1. The Evolving Laboratory Threat Landscape**

- Understanding the IT/OT Convergence and its unique risks.
- Analysis of Advanced Persistent Threats (APTs) targeting research data.
- FDA, EMA, HIPAA in the context of cyberattacks.
- Focus on Ransomware and its impact on LIMS/CDS systems.
- Confidentiality, Integrity, Availability (CIA) triad in a lab context.
- Case Study: Analysis of a pharmaceutical company?ÇÖs delay in drug filing due to a targeted ransomware attack on its R&D lab?ÇÖs CDS infrastructure.

**2. Regulatory Compliance & Data Integrity**

- Deep dive into FDA 21 CFR Part 11 on electronic records and signatures.
- Implementing ALCOA+ principles through technical security controls.
- Mapping security policies to GXP requirements.
- Audit trails, system validation, and security documentation best practices.
- Securing Quality Management Systems and validated data repositories.
- Case Study: Reviewing an FDA warning letter where non-compliance was traced back to inadequate access controls and unsecure audit logs on a critical lab instrument.

**3. Securing Laboratory Operational Technology (OT)**

- Architecture of lab ICS/SCADA systems and their vulnerabilities.
- Network segmentation and firewall rule design for OT environments.
- Protocol analysis and securing non-IP communications.
- Patch management strategies for legacy lab equipment and embedded systems.
- Physical security controls for data centers and restricted lab access points.
- Case Study: Simulating an unauthorized remote control attack on an automated robotic system via a compromised human-machine interface (HMI).

**4. Advanced Network Security & Micro-segmentation**

- Implementing Zero Trust Architecture (ZTA) for lab networks.
- Strategies for Micro-segmentation of individual instrument islands.
- Secure remote access for engineers and vendors.
- Deep packet inspection and protocol filtering on the lab network.
- Wireless network security for portable lab devices
- Case Study: Designing and testing a micro-segmentation strategy to isolate an unpatchable NMR machine from the rest of the corporate network.

**5. Identity and Access Management (IAM) for Labs**

- Implementing Multi-Factor Authentication (MFA) across all critical systems.
- Managing Privileged Access Management (PAM) for instrument administrators.
- Role-Based Access Control (RBAC) specific to scientific and technical roles.
- Securing service accounts used for system-to-system communication.
- Integrating lab systems with enterprise Directory Services
- Case Study: Analyzing a breach where an attacker leveraged a compromised generic service account to exfiltrate data from a central LIMS.

**6. Vulnerability Management & Penetration Testing**

- Developing a risk-based Vulnerability Management (VM) program for lab assets.
- Penetration Testing methodologies for specialized lab applications
- Secure Code Review for in-house developed bioinformatics scripts.
- Managing exceptions for unpatchable/EOL instruments.
- Utilizing automated tools for Continuous Monitoring of configuration drift.
- Case Study: Conducting a mock penetration test on a web-based electronic lab notebook (ELN) system to discover common injection and cross-site scripting flaws.

**7. Cloud Security for Scientific Data**

- Securing SaaS LIMS and cloud-based data repositories.
- Implementing Cloud Security Posture Management best practices.
- Data sovereignty and international regulatory considerations.
- Secure API integrations between on-premise instruments and cloud analytics platforms.
- Encryption strategies for Data-at-Rest and Data-in-Transit in the cloud.
- Case Study: Evaluating the security gaps in a life sciences organization?ÇÖs deployment of a public cloud for storing large-scale genomic sequencing data.

**8. Digital Forensics and Incident Response (DFIR)**

- Establishing a Cyber Incident Response Plan (CIRP) specific to lab downtime.
- Triage and containment strategies for infected lab instruments.
- Data collection and preservation for forensic analysis of non-standard file types.
- Legal and regulatory implications of a lab data breach.
- Coordination with legal, public relations, and operational teams during a crisis.
- Case Study: Responding to a simulated zero-day exploit that renders a high-value mass spectrometer inoperable, focusing on data preservation and operational recovery.

**9. Threat Intelligence and Threat Hunting**

- Sources and methods for gathering Threat Intelligence relevant to the life sciences sector.
- Using the MITRE ATT&CK for ICS framework to map adversarial tactics.
- Proactive Threat Hunting techniques in log data and network traffic.
- Developing custom Indicators of Compromise (IOCs) for lab-specific malware.
- Integrating SIEM/SOAR platforms with OT system logs.
- Case Study: Applying a recent threat report on a nation-state actor targeting vaccine research to an internal lab environment to hunt for dormant indicators.

**10. Bioinformatics and Genomic Data Security**

- Security challenges in Bioinformatics Pipelines and analysis tools.

- Protecting Personally Identifiable Information (PII) within genomic datasets.
- Anonymization and pseudonymization techniques for patient data.
- Securing data transfer protocols and API endpoints in collaborative research.
- Integrity checks and controls for the entire data lifecycle.
- Case Study: Investigating a potential data corruption event in a gene sequencing pipeline where malicious input data could alter the final research results.

**11. Endpoint Detection and Response (EDR) for Lab Systems**

- Deployment and tuning of EDR solutions on specialized lab workstations.
- Managing whitelisting/application control for validated software.
- Monitoring and securing removable media
- Advanced Malware Analysis and reverse engineering of lab-specific threats.
- Hardening operating systems and reducing the attack surface.
- Case Study: Analyzing a piece of malware found on a PCR machine control PC that was designed to subtly alter temperature settings over time.

**12. Supply Chain Risk Management (SCRM)**

- Conducting vendor security assessments for instrument manufacturers and software providers.
- Vetting third-party remote access and maintenance tools.
- Managing the security of software-defined instruments and firmware updates.
- Implementing controls against Software Bill of Materials (SBOM) vulnerabilities.
- Contractual requirements for security and breach notification in vendor agreements.
- Case Study: A laboratory discovers that a recent instrument firmware update introduced an undocumented backdoor, requiring a full supply chain risk audit.

**13. Security Architecture Review and Design**

- Principles of Secure-by-Design for new laboratory facilities and system rollouts.
- Reviewing and improving existing network architecture diagrams for security.
- Implementing hardware security modules (HSMs) for cryptographic keys.
- Designing and testing effective backup and disaster recovery strategies.
- Developing security metrics and KPIs for lab system performance.
- Case Study: Overhauling the security architecture for a new high-containment BSL-3 laboratory to meet both high-security and high-availability demands.

**14. AI and Machine Learning in Lab Security**

- Leveraging AI/ML for Anomaly Detection in instrument performance data.
- Using machine learning for automated threat prioritization.
- Implementing Security Orchestration, Automation, and Response in a lab environment.
- Securing AI/ML models and the data used to train them.
- Ethical considerations and bias in automated security decision-making.
- Case Study: Developing an AI model to detect deviations in a gas chromatograph's baseline data that could indicate a hidden data manipulation attempt.

**15. Capstone: Real-World Cyber Range Exercise**

- Full-scale simulation of a Targeted Lab Attack in a live cyber range environment.
- Executing the Incident Response plan under pressure.

- Red Team/Blue Team exercises focused on OT protocol exploitation.
- Presenting post-incident forensic findings and remediation recommendations to a simulated executive team.
- Developing an Executive-Level Risk Briefing based on the exercise outcomes.
- Case Study: Participants execute a multi-stage attack scenario, from initial network compromise to altering a final test result file, and then defend against it.

**Training Methodology**

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.com 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 |
|---|---|---|---|
| **07 Sep 2026** | 18 Sep 2026 | Online | $4,000 |
| **14 Sep 2026** | 25 Sep 2026 | Online | $4,000 |
| **21 Sep 2026** | 02 Oct 2026 | Online | $4,000 |
| **28 Sep 2026** | 09 Oct 2026 | Online | $4,000 |
| **05 Oct 2026** | 16 Oct 2026 | Online | $4,000 |
| **12 Oct 2026** | 23 Oct 2026 | Online | $4,000 |
| **19 Oct 2026** | 30 Oct 2026 | Online | $4,000 |
| **26 Oct 2026** | 06 Nov 2026 | Online | $4,000 |

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

**Register Online Now**

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