# Training Course Geospatial Cybersecurity and Threat Intelligence

Professional Development Training Course Outline

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

## Course Introduction

In an increasingly interconnected world, the convergence of **geospatial technologies** and **cybersecurity** has become paramount. Organizations across critical infrastructure, defense, smart cities, and commercial sectors heavily rely on **Geographic Information Systems (GIS)**, **satellite imagery**, and **location-based services**. This reliance, while offering unprecedented analytical capabilities and situational awareness, simultaneously exposes these systems to sophisticated **cyber threats**. Protecting sensitive **spatial data**, ensuring the integrity of **geospatial platforms**, and developing robust **threat intelligence** capabilities are no longer optional, but essential for national security, economic stability, and public safety.

Training Course Geospatial Cybersecurity and Threat Intelligence addresses the urgent need for professionals to understand and mitigate the unique **cyber risks** associated with geospatial assets. Participants will gain in-depth knowledge of **geospatial vulnerabilities**, learn to implement **defensive strategies**, and develop expertise in **geospatial threat intelligence**. Through practical **hands-on exercises** and real-world **case studies**, attendees will acquire the skills necessary to safeguard critical **location intelligence**, ensuring the resilience and security of their organizations' most valuable spatial data and systems against evolving **cyber warfare** and **advanced persistent threats (APTs)**.

## Programme Curriculum

**Training Course Geospatial Cybersecurity and Threat Intelligence**

**Introduction**

In an increasingly interconnected world, the convergence of **geospatial technologies** and **cybersecurity** has become paramount. Organizations across critical infrastructure, defense, smart cities, and commercial sectors heavily rely on **Geographic Information Systems (GIS)**, **satellite**

**imagery**, and **location-based services**. This reliance, while offering unprecedented analytical capabilities and situational awareness, simultaneously exposes these systems to sophisticated **cyber threats**. Protecting sensitive **spatial data**, ensuring the integrity of **geospatial platforms**, and developing robust **threat intelligence** capabilities are no longer optional, but essential for national security, economic stability, and public safety.

Training Course Geospatial Cybersecurity and Threat Intelligence addresses the urgent need for professionals to understand and mitigate the unique **cyber risks** associated with geospatial assets. Participants will gain in-depth knowledge of **geospatial vulnerabilities**, learn to implement **defensive strategies**, and develop expertise in **geospatial threat intelligence**. Through practical **hands-on exercises** and real-world **case studies**, attendees will acquire the skills necessary to safeguard critical **location intelligence**, ensuring the resilience and security of their organizations' most valuable spatial data and systems against evolving **cyber warfare** and **advanced persistent threats (APTs)**.

**Course Duration**

10 days

**Course Objectives**

1. Master Geospatial Cyber Threat Intelligence (GCTI) methodologies for proactive defense.
2. Identify and analyze Zero-Day vulnerabilities specific to GIS and remote sensing systems.
3. Implement secure coding practices for geospatial application development.
4. Develop effective incident response plans tailored for geospatial data breaches.
5. Understand and mitigate supply chain risks in geospatial technology ecosystems.
6. Apply Machine Learning (ML) and Artificial Intelligence (AI) for geospatial anomaly detection.
7. Secure cloud-based geospatial platforms and big data analytics.
8. Analyze nation-state cyber threats targeting critical geospatial infrastructure.
9. Implement blockchain for geospatial data integrity and provenance.
10. Conduct geospatial penetration testing and vulnerability assessments.
11. Develop strategies for securing IoT devices integrated with geospatial networks.
12. Ensure regulatory compliance (e.g., GDPR, CCPA) for sensitive location data.
13. Build cyber-physical security resilience for space-based assets and GNSS systems.

**Organizational Benefits**

- Safeguard sensitive geospatial data from breaches, manipulation, and unauthorized access, ensuring data integrity and confidentiality.
- Proactively identify and mitigate unique vulnerabilities within geospatial systems, minimizing potential attack surfaces.
- Develop robust capabilities for identifying and responding to advanced persistent threats (APTs) and targeted attacks against location intelligence.
- Ensure adherence to global data privacy regulations and industry standards, reducing legal and reputational risks.
- Protect vital national assets dependent on geospatial technologies, contributing to national security and public safety.
- Implement intelligence-driven security measures, allowing for more efficient allocation of cybersecurity resources.
- Cultivate in-house expertise in a specialized and high-demand field, gaining a strategic edge in the market.

- Minimize downtime and operational disruptions caused by cyber incidents affecting geospatial systems, ensuring uninterrupted services.

**Target Audience**

1. GIS Professionals & Analysts
2. Cybersecurity Analysts & Engineers.
3. IT Managers & Architects
4. Defense & Intelligence Personnel.
5. Critical Infrastructure Operators
6. Smart City Developers & Planners.
7. Software Developers.
8. Data Scientists & Researchers.

**Course Outline**

**Module 1: Introduction to Geospatial Systems & Cybersecurity Landscape**

- Understanding core GIS concepts, components, and applications.
- Overview of the evolving geospatial technology stack
- Introduction to fundamental cybersecurity principles and concepts.
- Defining the unique attack surface of geospatial systems.
- **Case Study:** The compromise of a municipal GIS database revealing sensitive infrastructure layouts.

**Module 2: Geospatial Data Vulnerabilities and Threats**

- Common vulnerabilities in spatial databases, web mapping services (WMS/WFS), and geospatial APIs.
- Threat vectors: data manipulation, spoofing, jamming, data exfiltration, and denial of service (DoS).
- Analysis of real-world geospatial cyber incidents and their impact.
- Understanding the intelligence value of geospatial data for adversaries.
- **Case Study:** GPS spoofing attacks on maritime navigation systems and their economic consequences.

**Module 3: Geospatial Threat Intelligence Fundamentals**

- Introduction to Cyber Threat Intelligence (CTI) and its application to geospatial domain.
- Intelligence cycle: planning, collection, processing, analysis, dissemination.
- Sources of geospatial threat intelligence (OSINT, HUMINT, SIGINT, FININT).
- Developing Threat Intelligence Platforms (TIPs) for spatial data.
- **Case Study:** Using open-source satellite imagery and social media to track and analyze disinformation campaigns targeting critical infrastructure.

**Module 4: Secure Geospatial Architecture Design**

- Principles of "Security by Design" for GIS and geospatial applications.
- Network segmentation and zoning for geospatial infrastructure.
- Implementing secure APIs and authentication mechanisms for spatial services.
- Choosing secure cloud environments for geospatial data storage and processing.
- **Case Study:** Designing a secure architecture for a national land registry system to prevent data tampering.

**Module 5: Geospatial Data Privacy and Compliance**

- Understanding data privacy regulations (GDPR, CCPA, PII) in the context of location data.
- Techniques for anonymization, pseudonymization, and differential privacy for spatial datasets.
- Ethical considerations in collecting, processing, and sharing geospatial information.
- Implementing privacy-by-design principles in geospatial projects.
- **Case Study:** A privacy breach involving location data from a popular fitness tracking app and lessons learned.

**Module 6: Access Control and Identity Management for GIS**

- Implementing Role-Based Access Control (RBAC) for geospatial data and tools.
- Multi-Factor Authentication (MFA) strategies for GIS user accounts.
- Managing privileges and least privilege principles in geospatial environments.
- Auditing and monitoring user access to sensitive spatial data.
- **Case Study:** Preventing insider threats in a defense geospatial intelligence unit through stringent access controls.

**Module 7: Secure Geospatial Software Development**

- Common vulnerabilities in geospatial programming
- Best practices for secure coding in Python, JavaScript, and other GIS-related languages.
- Automated security testing (SAST, DAST) for geospatial applications.
- Integrating security into the Geospatial Software Development Lifecycle (GSDLC).
- **Case Study:** Analyzing and remediating vulnerabilities found in an open-source mapping library.

**Module 8: Encryption and Data Integrity in Geospatial Systems**

- Encryption techniques for geospatial data at rest and in transit.
- Implementing Transport Layer Security (TLS) for web mapping services.
- Ensuring data integrity using hashing, digital signatures, and blockchain technologies.
- Secure storage solutions for large-scale geospatial datasets.
- **Case Study:** Using blockchain to ensure the immutability and provenance of land records in a smart city initiative.

**Module 9: Geospatial Incident Response and Recovery**

- Developing an incident response plan specific to geospatial cyber incidents.
- Containment, eradication, and recovery strategies for spatial data breaches.
- Forensic analysis of geospatial systems after an attack.
- Business continuity and disaster recovery planning for critical GIS operations.
- **Case Study:** Responding to a ransomware attack on a utility company's SCADA and geospatial control systems.

**Module 10: Advanced Geospatial Threat Analysis Techniques**

- Applying MITRE ATT&CK framework to geospatial attack scenarios.
- Hunting for advanced persistent threats (APTs) targeting spatial infrastructure.
- Using Big Data analytics and Machine Learning for anomaly detection in geospatial logs.
- Threat modeling for complex geospatial systems.

- **Case Study:** Deconstructing a sophisticated cyber attack campaign by a nation-state actor against a national mapping agency.

**Module 11: Securing Space-Based Assets and GNSS Systems**

- Understanding vulnerabilities in satellite communications and ground stations.
- Mitigating risks associated with GNSS (GPS, GLONASS, Galileo) spoofing and jamming.
- Cybersecurity challenges of Low Earth Orbit (LEO) satellite constellations.
- Protecting space-based critical infrastructure from cyber warfare.
- **Case Study:** Analysis of a suspected state-sponsored attack attempting to disrupt satellite navigation for military operations.

**Module 12: Cyber-Physical Security for Critical Geospatial Infrastructure**

- Integration of cybersecurity with physical security for critical infrastructure
- Securing SCADA and Industrial Control Systems (ICS) that leverage geospatial data.
- Addressing vulnerabilities at the IT/OT convergence points in geospatial contexts.
- Risk assessment for interdependent cyber-physical geospatial systems.
- **Case Study:** The Stuxnet attack's implications for geospatial systems controlling industrial processes.

**Module 13: Legal, Ethical, and Policy Aspects of Geospatial Cybersecurity**

- International laws and regulations pertaining to geospatial data and cyber warfare.
- Ethical considerations in the use of geospatial intelligence for surveillance and tracking.
- Developing organizational policies and frameworks for geospatial security.
- The role of public-private partnerships in securing geospatial assets.
- **Case Study:** Debates surrounding the ethical use of drone imagery and facial recognition in public spaces.

**Module 14: Emerging Technologies and Future Trends**

- The impact of Artificial Intelligence (AI) and Machine Learning (ML) on geospatial security (both defensive and offensive).
- Quantum computing's implications for geospatial encryption.
- The rise of IoT and Edge Computing in geospatial environments and their security challenges.
- Blockchain and Distributed Ledger Technologies (DLT) for secure geospatial data sharing.
- **Case Study:** Exploring the potential for AI-driven geospatial analytics to predict and prevent cyber-physical attacks.

**Module 15: Practical Geospatial Security Assessment & Capstone Project**

- Conducting a mock geospatial vulnerability assessment and penetration test.
- Utilizing open-source tools for geospatial security analysis.
- Developing a comprehensive geospatial security strategy for a hypothetical organization.
- Presentation of individual or group capstone projects addressing real-world geospatial security challenges.
- **Case Study:** A hands-on exercise to identify and exploit a simulated vulnerability in a web-based GIS application, followed by mitigation strategies.

**Training Methodology**

- Interactive Lectures

- Software Demonstrations
- Practical Labs.
- Case Studies Analysis.
- Group Discussions
- Project-Based Learning.
- Expert-Led Mentorship.

**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** | 04 Dec 2026 | Online | $2,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $3,000 |

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **23 Nov 2026** | 04 Dec 2026 | Physical | $6,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $6,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $12,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $9,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $12,000 |
| **23 Nov 2026** | 04 Dec 2026 | Physical | $12,000 |

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

**Register Online Now**

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