Faysal Aziz

Foundations of Modern Cybersecurity

Intelligence, Review, and AI-Aware Defense

FA-0212 · one-day

DevOps, Cloud & Infrastructure · Cybersecurity

Introduction

Introduction

Cybersecurity today is defined by constant change — driven by cloud adoption, sophisticated cyber-attack strategies, and the rapid emergence of artificial intelligence. Organizations must understand not only defensive techniques but also the intelligence that guides security decisions and the technologies that enable both attackers and defenders. This one-day theoretical course brings together key concepts such as code and configuration review, open source intelligence (OSINT), cloud security best practices, and AI-enhanced approaches to testing and defense.

It is designed to build a balanced mental framework so you can understand where vulnerabilities come from, how they are discovered, and how emerging technologies influence both threats and protections. Rather than focusing on tools or hands-on labs, this course emphasizes strategic principles, current practices, risk perspectives, and ethical considerations that are essential for anyone stepping into cybersecurity today.

Learning outcomes

By the end of this course, participants will be able to:

- Define and explain core cybersecurity principles, including risk management, confidentiality/integrity/availability (CIA), and defense in depth.
- Understand the purpose and limits of code review and source code analysis as part of secure software development.

- Describe how OSINT contributes to security assessment and defensive planning.
- Explain cloud security configuration best practices and why misconfigurations are a major risk factor.
- Articulate the concepts of intelligence-led and AI-assisted penetration testing — including their benefits and ethical considerations.
- Recognize how artificial intelligence affects the cybersecurity landscape, from threat detection to automated exploitation.
- Discuss ethical, legal, and governance issues associated with modern security practices.

Prerequisites

Participants should have:

- A basic understanding of computer systems and networking.
- Familiarity with general cybersecurity terminology (e.g., malware, firewall, vulnerability).
- Curiosity about how defensive and offensive techniques interact.

Training outline

1. 1. Foundations of Cybersecurity

Core principles

- Confidentiality, Integrity, Availability (CIA triad)
- Authentication and authorization
- Defense-in-Depth and Least Privilege
- Risk management frameworks (qualitative vs quantitative)

Threat landscape overview

- Common threat actors and motivations
- Attack vectors and exploit categories

2. 2. Code Review and Source Code Security

Purpose of code review in security

- Identifying logic flaws and insecure patterns
- Relationship to secure SDLC (Software Development Life Cycle)

Types of code analysis

- Manual review and peer inspection

- Automated static analysis

Limitations of code review

- False positives and negatives
- Context and domain specificity

3. 3. Open Source Intelligence (OSINT) in Cybersecurity

OSINT defined

- Sources of openly available information
- How attackers use OSINT for reconnaissance

Defensive use cases

- Threat profiling and attack surface discovery
- Monitoring exposed sensitive data

- Ethical and legal boundaries for OSINT

4. 4. Cloud Security Configuration Best Practices

Characteristics of cloud environments

- Shared responsibility model
- Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)

Common misconfigurations and risks

- Storage permissions, network access rules, identity and access management (IAM)

Principles of secure cloud configuration

- Zero Trust fundamentals
- Logging, monitoring, and alerting for cloud assets

5. 5. Intelligence-Led Penetration Testing

What is intelligence-led testing?

- Integrating threat intelligence into assessment planning
- Prioritizing tests based on real-world adversary behaviour

Lifecycle of an intelligence-led assessment

- Reconnaissance, targeting, exploitation strategy
- Post-exploit analysis and reporting focus

- Distinguishing ethical penetration testing from malicious hacking

6. 6. AI-Assisted Penetration Testing and AI in Security

The role of AI/ML in modern offensive and defensive security

- Pattern recognition for threat hunting
- Automated vulnerability suggestion and exploit generation (theoretical)

What "AI-assisted" means in a pen test context

- Augmenting human analysis vs full automation
- Limitations and risks of AI-generated outputs

Defensive AI systems

- Behavioral anomaly detection
- Automated response systems

Ethical and governance issues

- Bias, explainability, accountability in security-oriented AI

7. 7. Risk, Compliance, and Security Governance

The role of policies and standards

- ISO/IEC 27001, NIST frameworks

Legal and regulatory considerations

- Data protection and breach reporting laws

Ethical dimensions of cybersecurity work

- Responsible disclosure
- Balancing security with privacy

8. 8. Integration and Strategic Thinking

How all components fit together

- From secure design to testing to continuous monitoring

Emerging trends and future challenges

- AI-driven defenses and attacks
- Cloud native security evolution

- Questions and group discussion

© 2026 Faysal Aziz · Kuala Lumpur