



Defensible Security Architecture and Engineering

Course Introduction:

In an increasingly complex cyber threat landscape, organizations must ensure that their security infrastructures are not only reactive but also strategically designed to withstand and mitigate both present and future risks. This five-day course on Defensible Security Architecture and Engineering will equip participants with the knowledge and skills needed to design, implement, and maintain robust security architectures. Throughout the course, attendees will gain a thorough understanding of security principles, architectures, and methodologies that integrate both proactive defense mechanisms and resilience strategies into their network infrastructure.

The course will focus on building a strong foundation of security engineering best practices, emphasizing theoretical techniques for securing networks, systems, and applications. Participants will explore a wide range of security tools, frameworks, and technologies used to create an environment where vulnerabilities are minimized, and the system can recover quickly from any breach or disruption. By the end of the training, attendees will have the knowledge to create and assess secure, defensible architectures that are adaptable and scalable to evolving cyber threats.

Course Objectives:

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

- Understand core security principles and apply them to defend enterprise architecture.
- Implement security designs that minimize vulnerabilities across network, systems, and applications.
- Develop and maintain a robust security architecture lifecycle.
- Apply risk management methodologies to security architecture and design.
- Integrate security into the network infrastructure, from firewalls to advanced detection systems.
- Design secure systems using best practices for software development and configuration.
- Leverage cloud security frameworks and methodologies to ensure the safety of cloud applications and services.
- Build secure, compliant, and privacy-respecting architectures for applications and systems.
- Plan and prepare for incident detection, response, and recovery within a defensible architecture.
- Assess and test security measures through penetration testing and other red teaming techniques.

Who Should Attend?

This course is suitable for Security architects and engineers responsible for designing, building, and maintaining secure systems, IT professionals and network engineers seeking to deepen their understanding of security architecture, Systems administrators involved in securing networks, servers, and endpoints, Cloud security specialists and DevSecOps engineers working to secure cloud environments and applications, IT auditors and risk management professionals interested in learning how to evaluate and improve security posture, and Security operations personnel and incident response teams who need to implement and maintain security architecture at scale.

Course Outline:

Day 1: Introduction to Security Architecture and the Defensible Design Framework

- **Course Overview:** Defining security architecture and engineering in modern cybersecurity.
- **Fundamentals of Security Design:** Overview of the principles of a defensible security design.
- **Security Defense-in-Depth:** Exploring multi-layered defense strategies.
- **Frameworks & Standards:** Introduction to key security frameworks (NIST, ISO/IEC 27001, CIS Controls, etc.).
- **The Role of Risk Management:** Identifying and assessing risks to security architecture.
- **Security Architecture Lifecycle:** Phases of developing, deploying, and maintaining secure systems.

Day 2: Building Secure Network Architecture

- **Network Segmentation:** Creating zones of trust and isolating critical assets.
- **Perimeter Defense Strategies:** Firewalls, IDS/IPS, VPNs, and DMZs.
- **Zero Trust Architecture:** Concepts and principles of zero trust and how to implement them.
- **Advanced Network Security Protocols:** Secure communication, encryption standards, and VPN designs.
- **Incident Detection and Response:** Monitoring for security events and reacting to threats within the network.

Day 3: Secure Systems Design and Development

- **Secure Software Development Lifecycle (SDLC):** Integrating security into the development process.
- **Vulnerability Management:** Identifying, assessing, and mitigating vulnerabilities in software and systems.

- **Identity and Access Management (IAM):** Designing secure access control systems and authentication mechanisms.
- **Secure Configuration Management:** Hardening operating systems and applications for minimal attack surfaces.
- **DevSecOps Integration:** Embedding security practices into the DevOps process.

Day 4: Cloud Security and Secure Application Design

- **Cloud Security Challenges:** Security considerations in hybrid, multi-cloud, and on-prem environments.
- **Cloud Security Architecture:** Designing for secure cloud applications and data protection.
- **Application Security Best Practices:** Secure coding, OWASP Top Ten, and web application firewalls.
- **Threat Modeling for Applications:** Conducting threat assessments for software applications and cloud deployments.
- **Data Privacy and Compliance:** Managing regulatory requirements and data protection within cloud systems.

Day 5: Security Operations and Incident Response in Defensible Architectures

- **Building a Security Operations Center (SOC):** Role, design, and functionality of SOC in managing enterprise security.
- **Incident Response Planning:** Developing an effective incident response strategy.
- **Disaster Recovery and Business Continuity:** Planning for system and data recovery after a breach or disaster.
- **Penetration Testing and Red Teaming:** Simulating attacks to identify weaknesses in architecture.
- **Final Review:** Review of key concepts.

Course Methodology:

A variety of methodologies will be used during the course that including:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires

- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course location. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session

المركز العالمي للتدريب والتطوير
International Centre For Training & Development