Implementing Zero Trust Architecture in Corporate Networks Training Course



26 - 30 Oct 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #NO8987_279100

Course Introduction / Overview:

The traditional perimeter-based security model is no longer sufficient to protect against modern cyber threats. This course provides a comprehensive exploration of the Zero Trust security model, a paradigm shift that assumes no implicit trust for any user or device, regardless of their location. We will delve into the core principles of "never trust, always verify," continuous authentication, and least-privilege access. This training moves beyond theoretical concepts, focusing on the practical implementation of a Zero Trust Architecture (ZTA). Drawing on foundational concepts outlined in publications like the NIST Special Publication 800-207, the course offers a structured approach to designing and deploying a robust ZTA. As noted by cybersecurity visionary John Kindervag, the creator of the Zero Trust model, the goal is to stop data breaches by eliminating the concept of trust from an organization's network architecture. BIG BEN Training Center has designed this program to equip professionals with the skills to build a resilient, identity-centric security posture, effectively safeguarding critical assets in today's complex and distributed corporate networks. This is not just a course on security tools; it is a strategic guide to re-architecting your defense-in-depth strategy for the modern era.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs).
- IT Security Managers and Architects.
- Network Engineers and Administrators.
- Cybersecurity Analysts and Consultants.
- Cloud Security Engineers.
- IT Directors and VPs of Infrastructure.
- Systems Administrators.
- Compliance and Risk Management Officers.
- Solutions Architects.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Government and Public Sector Agencies.
- Technology and Telecommunications.
- Retail and E-commerce.
- Energy and Utilities.
- Manufacturing and Industrial Control Systems.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT).
- Cybersecurity and Information Security.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Cloud Infrastructure and Operations.
- Risk Management and Compliance.
- Internal Audit.
- Application Development and DevOps.

Course Offerings:

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

- Articulate the core principles and business drivers behind a Zero Trust security model.
- Develop a strategic roadmap for a phased Zero Trust Architecture implementation.
- Design and implement micro-segmentation policies to isolate critical assets.
- Evaluate and integrate Identity and Access Management (IAM) solutions within a ZTA.
- Implement strong multi-factor authentication (MFA) and continuous verification protocols.
- Assess device health and compliance as a prerequisite for network access.
- Secure application workloads and data flows using Zero Trust principles.
- Leverage automation and analytics for continuous monitoring and threat detection.
- Align Zero Trust initiatives with regulatory compliance and governance frameworks.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive. This course moves beyond traditional lectures to foster a deep, applicable understanding of Zero Trust Architecture. Participants will engage in detailed case study analyses of real-world ZTA implementations, dissecting both successes and failures to draw actionable insights. A significant portion of the course is dedicated to collaborative group workshops where attendees will work together to design a Zero Trust roadmap for a hypothetical corporation, tackling challenges related to legacy systems, budget constraints, and stakeholder buy-in. Interactive sessions, facilitated discussions, and expert-led Q&A segments ensure that complex concepts are clarified and understood in the context of participants' own organizational environments. The instructor will provide continuous feedback and guide participants through practical exercises that simulate policy creation, access control configuration, and threat modeling within a Zero Trust framework. This hands-on, problem-solving approach ensures that participants leave not just with knowledge, but with the confidence and skills to lead ZTA initiatives in their own organizations.

Course Agenda (Course Units):

Unit One Foundations of Zero Trust Security

- Introduction to the Zero Trust model.
- The evolution from perimeter security to identity-centric security.
- Debunking common myths and misconceptions about Zero Trust.
- Core principles: never trust, always verify, and least-privilege access.
- Understanding the business case and ROI for Zero Trust.
- Key industry frameworks and standards (NIST SP 800-207).
- The Zero Trust Maturity Model.

Unit Two The Core Pillars of Zero Trust Architecture

- Identity as the new perimeter: users, services, and devices.
- Device visibility, health, and compliance management.
- Network security and micro-segmentation strategies.
- Application workload security and API protection.
- Data-centric security: classification, encryption, and access policies.
- Visibility, analytics, and security automation.
- Integrating the pillars into a cohesive architecture.

Unit Three Designing a Zero Trust Implementation Strategy

- Conducting a Zero Trust readiness assessment.
- Identifying protect surfaces and critical assets.
- Mapping transaction flows and dependencies.
- Developing a phased implementation roadmap.
- Creating a Zero Trust policy engine and rule base.
- Gaining executive and stakeholder buy-in.
- Budgeting and resource planning for a ZTA project.

Unit Four Implementing Zero Trust Technologies and Controls

- Advanced Identity and Access Management (IAM) and Privileged Access Management (PAM).
- Implementing robust Multi-Factor Authentication (MFA) and adaptive authentication.
- Deploying Zero Trust Network Access (ZTNA) solutions.
- Practical micro-segmentation with next-generation firewalls and software-defined networking.
- Endpoint Detection and Response (EDR) in a Zero Trust environment.
- Integrating with SIEM and SOAR for enhanced visibility and response.
- Securing cloud environments (IaaS, PaaS, SaaS) with Zero Trust.

Unit Five Operationalizing and Optimizing Zero Trust

- Continuous monitoring and validation of Zero Trust controls.
- Automating policy enforcement and incident response.
- Managing the user experience and cultural shift.
- Measuring success with key performance indicators (KPIs).
- Integrating Zero Trust with compliance frameworks (GDPR, HIPAA, PCI DSS).
- The role of AI and Machine Learning in enhancing Zero Trust.
- Future trends and the evolution of Zero Trust security.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As automation and AI become more integrated into security operations, how might the principle of 'never trust, always verify' evolve to apply to non-human entities and autonomous systems within a Zero Trust framework?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing intensely on the strategic and operational aspects of implementing a Zero Trust Architecture, rather than merely surveying available technologies. While other programs may concentrate on specific vendor solutions, our curriculum is fundamentally vendor-agnostic, empowering participants with the core principles and design patterns applicable across any technology stack. We emphasize the creation of a bespoke, phased implementation roadmap, recognizing that a successful ZTA is a long-term strategic initiative, not a one-time project. The curriculum moves beyond theoretical discussions to include practical workshops on mapping transaction flows, defining micro-segmentation policies, and building a business case for executive stakeholders. A key differentiator is our focus on the human element, addressing the cultural shift required to move an organization from a mindset of implicit trust to one of explicit verification. Participants will not just learn what Zero Trust is; they will learn how to think like a Zero Trust architect, enabling them to make informed, strategic decisions that align security controls directly with business processes and risk tolerance.