Zero Trust Security: Designing Secure Enterprise Networks Training Course

Ref: #CYB6972

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals with the strategic and practical knowledge required to design and implement a Zero Trust security model. In a world where the traditional network perimeter is disappearing due to remote work and cloud services, the "trust but verify" approach is no longer effective. The Zero Trust model, with its core principle of "never trust, always verify," offers a powerful alternative. This program goes beyond a theoretical overview and focuses on the practical steps needed to transition an organization to Zero Trust architecture. Participants will learn how to implement strong identity and access controls, microsegment networks, and use automation to continuously monitor and secure their environments. We will cover key topics like device trust, least privilege of access, and the challenges of managing a distributed workforce. Drawing from the academic research of renowned authors like John Kindervag, who originally coined the term, this program provides a strategic and practical framework for securing modern enterprise networks. This course at BIG BEN Training Center will empower you to build a resilient and adaptive security program that protects your organization's data regardless of its location.

Target Audience / This training course is suitable for:

- Cybersecurity architects.
- Network security engineers.
- Information security leaders.
- Cloud security professionals.
- IT and security managers.
- IT auditors.
- System administrators.

Target Sectors and Industries:

- Technology and software.
- Financial services.
- Telecommunications.
- Healthcare.
- Manufacturing.
- Government agencies and equivalents.
- Global corporations.

Target Organizations Departments:

- Information Security.
- IT.
- Network Engineering.
- Cloud Operations.
- Risk Management.
- IT Audit.
- Data Management.

Course Offerings:

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

- Design a Zero Trust architecture.
- Implement micro segmentation and network security.
- Establish a strong identity and access management program.
- Develop a continuous monitoring and verification strategy.
- Secure remote and mobile workforces.
- Manage risk in a perimeter-less environment.
- Communicate the value of Zero Trust to stakeholders.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, scenario-based methodology that simulates the challenges of transitioning an enterprise to a Zero Trust model. The program includes a series of workshops where participants will design and present Zero Trust architecture for a fictional company. You will learn to use threat modeling to identify the most critical assets and to develop a phased implementation plan. The course emphasizes a practical, vendor-neutral approach. It teaches participants to prioritize core principles over specific tools. The instructor will provide expert guidance and feedback throughout the exercises, ensuring that you develop the critical thinking and strategic planning skills required for modern security roles. This approach ensures the knowledge and skills gained are directly applicable to building a secure enterprise network.

Course Agenda (Course Units):

Unit One: The Zero Trust Framework

- Introduction to Zero Trust.
- Core principles (never trust, always verify).
- The pillars of a Zero Trust model.
- The limitations of a traditional perimeter.
- Identity as the new perimeter.
- The Zero Trust maturity model.
- Case study: a successful Zero Trust implementation.

Unit Two: Identity and Access Management

- Implementing strong identity controls.
- Multi-factor authentication (MFA).
- Least privilege access.
- Managing privileged accounts.
- Role-based access control (RBAC).
- Just-in-time access.
- Practical lab: a privileged access management scenario.

Unit Three: Micro segmentation and Network Security

- What is micro segmentation?
- Designing a segmented network.
- Securing east-west traffic.
- Using firewalls and security gateways.
- Zero Trust for cloud and hybrid environments.
- Monitoring and logging network traffic.
- Practical lab: a micro segmentation exercise.

Unit Four: Device Trust and Continuous Monitoring

- Assessing device health and compliance.
- Endpoint security solutions.
- The role of security information and event management (SIEM).
- Threat intelligence and automation.
- Continuous monitoring and policy enforcement.
- User behavior analytics.
- Case study: an endpoint security incident.

Unit Five: Implementation and Communication

- Developing a Zero Trust roadmap.
- The business case for Zero Trust.
- Communicating Zero Trust to the organization.
- The role of automation and orchestration.
- Future trends in Zero Trust.
- Final project: a comprehensive Zero Trust plan.
- Continuous verification.
- Frequently Asked Questions:

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:

The Zero Trust model relies on the principle of "never trust, always verify" for all users and devices, both inside and outside the network. However, how can organizations implement this without creating so much friction that it hinders employee productivity and the adoption of new technologies?

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

This course stands out by providing a unique and vital focus on the strategic implementation of the Zero Trust security model. Unlike many technical courses that focus on a single tool, this program teaches you how to design comprehensive, principles-based architecture. The curriculum is built around a practical, vendor-neutral approach. It emphasizes the foundational concepts of Zero Trust, enabling you to apply them regardless of your organization's specific technology stack. The focus on strategic planning and on communicating the value of Zero Trust to leadership distinguishes this course from others. It is for professionals who are ready to move from reacting to threats to proactively build a secure and resilient enterprise for the future.