Advanced Cloud Security and Zero Trust Architecture Training Course



19 - 23 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB5024_88249

Course Introduction / Overview:

The paradigm of cybersecurity is undergoing a fundamental transformation, moving away from the traditional castle-and-moat security model towards a more dynamic and robust framework. This shift is driven by the widespread adoption of cloud computing and the increasing sophistication of cyber threats. The Advanced Cloud Security and Zero Trust Architecture Training Course is meticulously designed to address this evolution. It provides a comprehensive exploration of designing, implementing, and managing secure cloud environments based on the Zero Trust principle of "never trust, always verify.". As detailed by authors like Jason Garbis in his influential book "Zero Trust Security: An Enterprise Guide," this model mandates that no user or device is trusted by default, regardless of its location. This course, offered by BIG BEN Training Center, delves deep into the practical application of these concepts, equipping participants with the skills to build resilient, identity-centric security architectures. We will navigate through complex topics such as micro-segmentation, identity and access management, cloud native security, and automated compliance, ensuring a holistic understanding from foundational principles to advanced operational strategies. This program is essential for professionals aiming to lead their organizations in building next-generation, breach-resistant cloud infrastructures.

Target Audience / This training course is suitable for:

- Cloud Security Architects.
- Cybersecurity Engineers and Analysts.
- IT Security Managers and Directors.
- Solutions Architects and Cloud Engineers.
- DevOps and DevSecOps Professionals.
- Network Security Engineers.
- Compliance and Risk Management Officers.
- IT professionals seeking to specialize in cloud security.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Life Sciences.
- Technology and Software Development.
- Telecommunications.
- E-commerce and Retail.
- Government and Public Sector Agencies.
- Energy and Utilities.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT) and Infrastructure.
- Cybersecurity and Information Security.
- Cloud Center of Excellence (CCoE).
- DevOps and Application Development.
- Enterprise Architecture.
- Internal Audit and Compliance.
- Risk Management.
- Network Operations.

Course Offerings:

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

- Develop a comprehensive Zero Trust strategy for cloud environments.
- Design and implement robust cloud security architectures.
- Master identity and access management (IAM) principles in a multi-cloud context.
- Apply micro-segmentation to limit lateral movement of threats.
- Secure cloud workloads, containers, and serverless applications.
- Integrate security into the CI/CD pipeline for DevSecOps.
- Automate security controls and compliance monitoring in the cloud.
- Conduct threat modeling for cloud-native applications.
- Develop an effective cloud incident response plan based on Zero Trust principles.
- Evaluate and select appropriate cloud security tools and technologies.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn the theory but can also apply it effectively. This course moves beyond traditional lectures by incorporating a blend of expert-led instruction, real-world case study analysis, and collaborative group workshops. Participants will engage in architectural design sessions where they will tackle complex security challenges and propose Zero Trust solutions for various cloud scenarios. The curriculum includes hands-on lab simulations that provide a safe environment to configure security controls, implement identity policies, and practice micro-segmentation. Team-based projects will encourage peer-to-peer learning and problem-solving, mirroring the collaborative nature of modern cybersecurity teams. Throughout the course, there will be continuous opportunities for Q&A and direct feedback from our experienced instructors. This multi-faceted approach ensures a deep and lasting understanding of cloud security and Zero Trust principles, empowering participants to implement these advanced strategies confidently within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Cloud Security and Zero Trust

- Introduction to Cloud Computing Models (IaaS, PaaS, SaaS).
- The Shared Responsibility Model in Cloud Security.
- Evolution from Perimeter Security to Zero Trust.
- Core Principles of the Zero Trust Model.
- Understanding the Zero Trust Maturity Model.
- Key Pillars of a Zero Trust Architecture.
- Common Cloud Security Threats and Vulnerabilities.

Unit Two: Identity and Access Management (IAM) as the Core

- The Role of Identity as the New Security Perimeter.
- Designing a Robust Cloud IAM Strategy.
- Implementing Multi-Factor Authentication (MFA) and Adaptive Authentication.
- Principles of Least Privilege Access in the Cloud.
- Managing Privileged Access Management (PAM) for Cloud Infrastructure.
- Federated Identity and Single Sign-On (SSO) Solutions.
- Auditing and Monitoring IAM Policies and Roles.

Unit Three: Securing Cloud Networks and Workloads

- Designing Secure Virtual Private Clouds (VPCs) and Virtual Networks.
- Implementing Network Micro-segmentation and Nano-segmentation.
- Introduction to Zero Trust Network Access (ZTNA).
- Securing Cloud Workloads (Virtual Machines, Containers, Serverless).
- Cloud Workload Protection Platforms (CWPP) Explained.
- Data Encryption Strategies for Data-at-Rest and Data-in-Transit.
- API Security Best Practices in a Cloud Environment.

Unit Four: DevSecOps and Security Automation

- Integrating Security into the CI/CD Pipeline (DevSecOps).
- Implementing Security as Code (SaC) Principles.
- Automating Security Scans for Infrastructure, Code, and Containers.
- Cloud Security Posture Management (CSPM) for Continuous Compliance.
- Automated Incident Response and Orchestration (SOAR) in the Cloud.
- Threat Modeling for Cloud-Native Applications.
- Managing Secrets in a DevOps Environment.

Unit Five: Governance, Risk, Compliance, and Operations

- Developing a Cloud Security Governance Framework.
- Mapping Zero Trust Controls to Compliance Standards (NIST, ISO, GDPR).
- Continuous Monitoring and Threat Detection in the Cloud.
- Strategies for Cloud Logging and SIEM Integration.
- Building a Cloud Incident Response Plan.
- Managing Security in Multi-Cloud and Hybrid Environments.
- The Future of Cloud Security and Emerging Trends.

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:

Considering the 'assume breach' principle, how does the implementation of a Zero Trust architecture fundamentally alter an organization's incident response strategy compared to a traditional perimeter-based approach?

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

This course distinguishes itself by moving beyond theoretical discussions to focus on the pragmatic and strategic implementation of a Zero Trust architecture within complex cloud environments. Unlike programs that concentrate on a single cloud provider or specific vendor tools, our curriculum is built on vendor-agnostic principles, providing a versatile skill set applicable across AWS, Azure, GCP, and hybrid models. We place a strong emphasis on the integration of security with modern development practices, offering deep insights into DevSecOps and Security as Code that are critical for today's agile organizations. The course content is uniquely structured to bridge the gap between high-level architectural design and granular-level implementation, covering everything from identity management to workload protection and automated compliance. Furthermore, the learning experience is enriched with architectural workshops and case studies based on real-world security incidents, forcing participants to think critically and develop robust, resilient solutions. This holistic approach ensures that graduates are not just knowledgeable about Zero Trust concepts but are fully equipped to lead, design, and execute a successful Zero Trust transformation.