Digital Identity & Access Management Advanced Systems Training Course

Ref: #CYB2226

Course Introduction / Overview:

This comprehensive training course is designed to provide IT and cybersecurity professionals with advanced knowledge and practical skills in Digital Identity and Access Management (IAM). In today's interconnected world, managing who has access to what data is not just a security measure, it is a core business function. This program delves into the complexities of modern authentication systems, from multi-factor authentication (MFA) to single sign-on (SSO) and explores the strategic importance of a robust IAM framework. Participants will learn how to design, implement, and maintain secure and scalable identity solutions that protect an organization's most valuable assets. We will also cover the legal and regulatory aspects of identity management, drawing from the academic work of prominent authors like Annie I. Anton and her research on privacy policies and requirements engineering. Her work highlights the critical link between user trust and effective privacy management. This course at BIG BEN Training Center will equip you with the expertise to lead your organization's digital identity strategy.

Target Audience / This training course is suitable for:

- Cybersecurity analysts.
- Identity and Access Management (IAM) specialists.
- System administrators.
- IT auditors.
- Compliance officers.
- Security architects.
- Risk managers.

Target Sectors and Industries:

- Financial services.
- Technology and software.
- Healthcare.
- Telecommunications.
- E-commerce.
- Government agencies and equivalents.
- Managed security service providers.

Target Organizations Departments:

- Information Security.
- Information Technology (IT).
- Compliance and Audit.
- Risk Management.
- Human Resources.
- Systems Administration.
- Legal.

Course Offerings:

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

- Design and implement a comprehensive IAM strategy.
- Configure and manage advanced authentication systems.
- Integrate single sign-on (SSO) and federated identity.
- Assess and mitigate identity-related security risks.
- Ensure compliance with major data privacy regulations.
- Develop policies for privileged access management (PAM).
- Utilize modern identity management tools and platforms.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, scenario-based methodology that focuses on practical applications. The program includes extensive lab exercises where participants will configure and troubleshoot real-world identity management systems. You will work on case studies that involve designing an IAM framework for a multi-national corporation, a healthcare provider, and an e-commerce platform, exposing you to the unique challenges of different sectors. The course will also cover the strategic side of IAM. You will learn how to communicate the business value of identity management to stakeholders. The instructor provides personalized feedback and leads interactive discussions, ensuring a deep understanding of the concepts. This approach ensures you will leave with the skills to confidently tackle complex IAM projects.

Course Agenda (Course Units):

Unit One: Fundamentals of Identity and Access Management

- Introduction to IAM concepts.
- Core components of an IAM framework.
- The difference between authentication and authorization.
- IAM in a modern enterprise.
- Key benefits of a robust IAM system.
- The identity lifecycle.
- Case study: a corporate identity audit.

Unit Two: Advanced Authentication Systems

- Multi-factor authentication (MFA) and its types.
- Biometric and passwordless authentication.
- Single sign-on (SSO) and its implementation.
- Federated identity and its protocols (SAML, OAuth 2.0).
- Adaptive authentication and risk-based access.
- Managing authentication for privileged accounts.
- Practical lab: configuring SSO.

Unit Three: Privileged Access and Governance

- What is privileged access management (PAM)?.
- Securing administrative and service accounts.
- Implementing PAM tools and policies.
- Role-based access control (RBAC).
- Access reviews and recertification.
- Governance and compliance in IAM.
- Case study: a PAM implementation scenario.

Unit Four: IAM Implementation and Integration

- The IAM project lifecycle.
- Integrating IAM with various applications and systems.
- Connecting IAM to HR systems.
- API security and managing access for machines.
- IAM for cloud environments.
- On-premises vs. cloud-based IAM solutions.
- Practical lab: cloud IAM integration.

Unit Five: Identity in the Age of Zero-Trust

- Introduction to the zero-trust security model.
- The role of IAM in zero-trust architecture.
- Continuous authentication and authorization.
- Micro-segmentation.
- The future of digital identity.
- Emerging threats to identity systems.
- Final project: a zero-trust IAM plan.
- 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:

With the increasing reliance on biometrics and other personal data for authentication, how can organizations balance the need for enhanced security with a user's right to privacy?

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

This course provides a uniquely advanced and holistic perspective on Identity and Access Management. Unlike many introductory programs that focus on basic concepts, this curriculum dives deep into the strategic, technical, and regulatory complexities of modern IAM systems. It moves beyond simple tools. It teaches you how to design and manage a comprehensive identity framework that supports business goals while mitigating risk. The hands-on labs and real-world case studies ensure that you not only understand the theory but can also apply it to solve practical problems. This course is for security professionals who need to go beyond the basics. It gives them the expertise to lead their organization's identity strategy and protect against today's most sophisticated cyber threats.