Cybersecurity Specialization: Architecture and Policy Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Acquire the skills to design secure architectures in adherence with industry standards, best practices, and policies.

Organizations require people with the skills to make decisions to secure information systems based on best practices, standards, and industry recommendations. Security architects fill this need. These skilled cybersecurity professionals design and implement secure architectures and translate business processes and risk into policy and implementation rules.

Cybersecurity Specialization: Architecture and Policy provides an overview for designing and deploying a security architecture. In this course, you will integrate security policies across network, application, information, and access control architectures as well as cloud and hybrid cloud models. You will review and implement industry standard best practices and policies (NIST, etc.), along with standard architecture framework models.

The course uses a challenge-based design that focuses on what a learner should be able to do at the end of the course and back on the job. The practice opportunities and challenge activities resemble—as much as possible—tasks the learner would be asked to perform in a real-life situation.

Who Should Attend?

Any mid-career or intermediate level person with an interest in security architecture and who has been in a cybersecurity role or organization for at least 2 years.

While security architect is typically a senior role in many organizations,*Cybersecurity Specialization: Architecture and Policy* is a mid-level course focused on building the skills a security architect will use on the job.

As such, the ideal candidate for this course will already have strong technical skills and experience in more than one technical area (for example, network infrastructure configuration, web services, and identity and access management), but may have more limited experience in cybersecurity.

They may have an interest in security architecture but no experience, or they may be performing some architecture tasks already as part of their job.

Cybersecurity Specialization: Architecture and Policy Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Security architect's role in the security lifecycle
- Use recognized frameworks to support controls and reduce risk
- Capture security requirements for network, application, data, and access control architectures
- Design appropriate access controls based on the mission of the organization including role based, task based, or other access controls
- Verify compliance to standards for an architecture
- Update an architecture to mitigate risk in response to a security auditor's list of findings
- Establish security policy creation and management
- Design secure virtualized environments
- Identify components and concerns that might impact a cloud migration
- Examine options for incorporating key management into your architecture
- Document an architecture in an appropriate format representing requirements and domains

Outline

Frameworks and the Lifecycles

- IT lifecycle management
- Frameworks
- Stakeholders
- Security policies

Design a Network Security Architecture

- Network segmentation
- Network components
- Practice: Identify network flows
- Industry best practices
- Roles and responsibilities

Design a Secure Application Architecture

- History of development
- The application architect
- Application architecture goals
- Service-oriented architecture (SOA)
- Modular framework development
- Authentication
- Patching
- Vulnerability testing

Design a Data Security Architecture

- Data architecture
- Classification of data
- Privacy
- Database security
- Encryption
- Big data

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Data architecture analysis
- Data architecture influences

Design an Access Control Security Architecture

- Identity and access management
- Access control policy
- Access control models
- Centralized access control
- Bring your own device
- Access reviews

Update a Security Architecture

- Impact of change
- Life cycle management
- Architecture changes

Document a Security Architecture

- Documentation life cycle
- Input documentation
- Architecture documentation
- Output documentation
- Security requirements traceability matrix (RTM)

Examine Alternative Architectures

- Virtualization
- Cloud security architecture
- Shared responsibility
- Encryption
- Key management for cloud

Course Look Around

- Look back at what you learned
- Look ahead
- Consider additional training