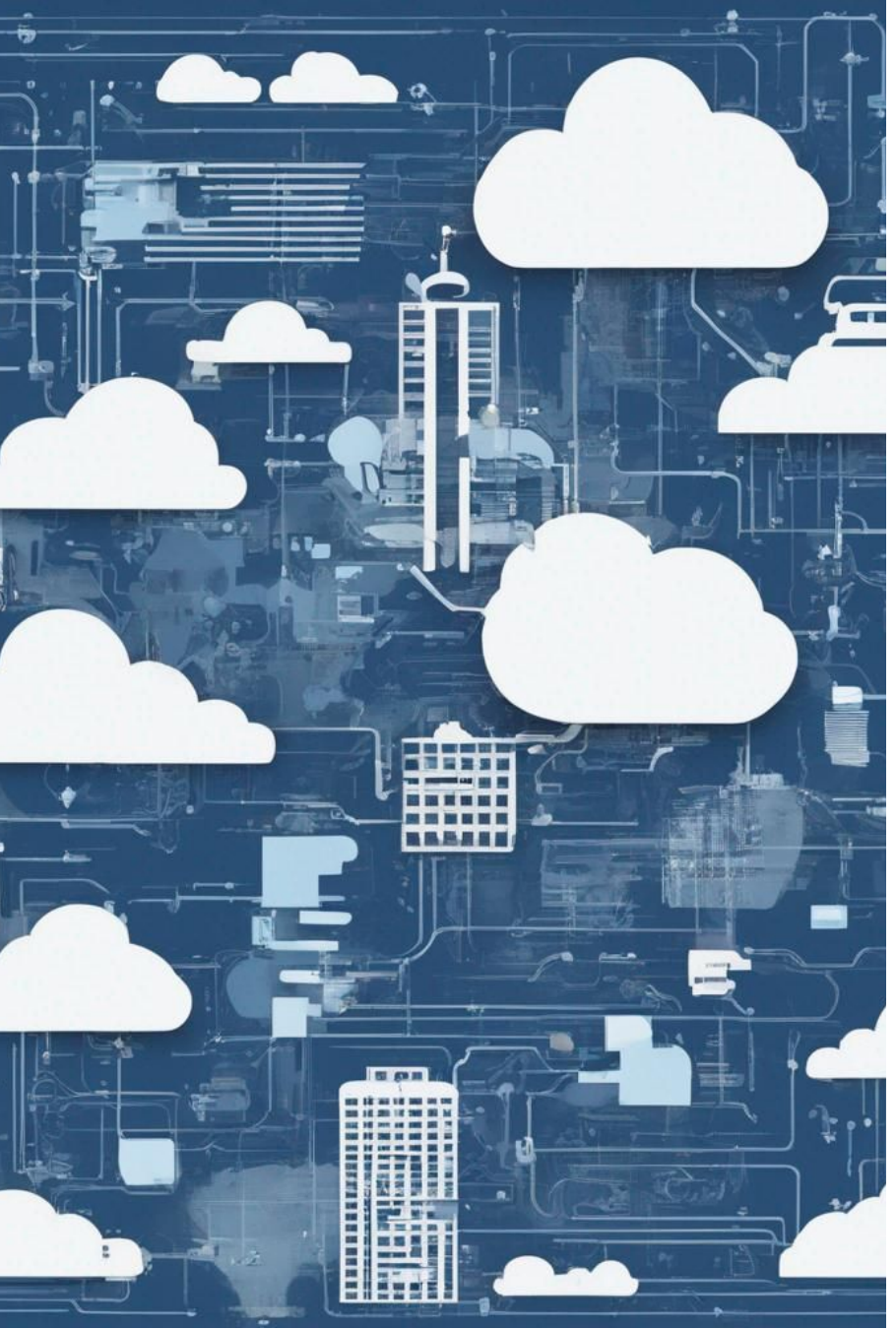
Cloud Application Security

CCSP Series - Chapter # 4



Introduction to Cloud Application Security

- Organizations migrating to the cloud hold a shared responsibility with the cloud provider for security.
- Importance of securing software in identity/access management, networking, and infrastructure.
- Focusing on the Software Development Life Cycle (SDLC) for application security.

Secure Culture and SSDLC

1. Security culture development through executive support, program design, implementation, and sustainment.

2. SSDLC mandates security integration from inception, ongoing training, and awareness.

Cloud Development Fundamentals

Security by design: Integrating security in every development step.

Shared responsibility model: Joint security efforts between cloud provider and consumer.

Viewing security as a business objective to manage risks and foster customer trust.

Common Pitfalls in Cloud Security

- Misconception on cloud provider responsible for all aspects of IT security.
- Importance of leadership support and adequate resources for security initiatives.
- The need for understanding and adapting to organizational culture for a successful security program.

Frameworks for Secure Software Development

1. **NIST Secure Software Development Framework:** Inclusive of organization preparation, protecting software, producing secured software, and responding to vulnerabilities.

2. **OWASP Software Assurance Maturity Model (SAMM):** Evaluates software security maturity and develops plans for SSDLC improvement.

Business Requirements for SSDLC

Cost-effectiveness of integrating security early in SDLC vs. post-development mitigation.

Ensuring a mature SSDLC is a mandated requirement for consistent secure software development.

Phases and Methodologies in SDLC

- **Enumerating SDLC stages:** requirements, design, development, testing, deployment, and O&M.
- Security-focused practices embedded within SDLC stages to create an SSDLC.

SDLC Methodologies - Waterfall to DevOps

1. **Waterfall:** Rigorous, sequential approach with inherent security benefits and inflexibility.

2. **Agile and DevOps:** Flexible and fast-paced methodologies favor security adjustments and prioritize automation and testing.

Applying the Secure Software Development Life Cycle

Integrating security practices throughout the SDLC phases.

The role of SSDLC in risk mitigation, cost reduction, and compliance with data security standards.

Common Cloud Vulnerabilities and CSA Top Threats

- Addressing data breaches, misconfiguration, and inadequate change control amongst cloud vulnerabilities.
- **CSA Top Threats to Cloud Computing:** Delivering insights into prioritizing cloud application security risks.

Threat Modeling in Software Development

1. Utilizing frameworks like STRIDE and DREAD for identifying and classifying potential threats.

2. The relevance of threat modeling in prioritizing secure development activities.

Avoiding Common Vulnerabilities and Secure Coding

Training and awareness as key to avoiding common vulnerabilities.

Incorporating documented processes, test-driven development, and OWASP's secure coding practices.

Software Configuration Management and Versioning

- Managing software assets for integrity and proper deployment.
- Implementing formal SCM tools/processes to avoid misreleases and compliance issues.

Cloud Software Assurance and Validation

1. Essential testing types for assuring software security like SAST, DAST, and IAST.

2. Manual testing augmenting automated testing for comprehensive risk assessment.

Multifactor Authentication for Enhanced Security

MFA/2FA as an essential IAM solution for cloud environments.

Benefits and considerations in utilizing MFA within organizational security practices.

Concluding Cloud Application Security

- Summary of implementing SSDLC for application security in the cloud.
- Incorporating necessary tools following organization-specific security architecture for optimal protection and monitoring.

Information Security Buzz

Discover more at our InfoSec Knowledge Hub