SPIKE REPLY – CLOUD SECURITY ASSESSMENT

SECURITY ASSESSMENT METHODOLOGY

Define Context of the Cloud Workload	Identify Applicable Requirements	Assess Security Controls	Idetify Gaps	Propose Suitable Remediations	Monitor Remediations Implementation
Gather context information on workload & assessment needs	Context-dependent security requirements	Automated & manual requirements checks	Prioritized gap analysis & compliance report	Developer focused and actionable remediations	Regular review & advisory on remediations

CONTACT

Spike Reply
www.spike-reply.com
azure.security@reply.de

AZURE SECURITY BEST PRACTICES ASSESSMENT

Technical Analysis	• Expert-lead assessment and architecture security review • Tool-based security checks • Manual review and adjustment on tool-based findings
Interviews & Workshop	• Assess controls not covered in the technical analysis • Discuss findings for relevance and criticality within context
Evaluation & Reporting	• Report security posture and summarize findings & risks • Recommend improvments and activities • Propose a roadmap to implement recommendations
Final Presentation	• Present findings and recommendations to the team • Clarify questions and define next steps

AREAS COVERED BY SECURITY REVIEW

- Network security
- Identity management
- Privileged Access
- Data protection
- Asset management
- DevOps Security
- Logging and threat detection
- Incident response
- Posture and vulnerability management
- Secrets & Key management
- Backup and recovery

AREAS OF COMPETENCE IN CLOUD SECURITY

SECURE CLOUD JOURNEY

- Cloud Security Strategy & Roadmap
- (Multi-) Cloud Reference Architectures
- SASE Architectures
- Data Security

SECURE CLOUD ARCHITECTURE

- Hybrid & Multi-Cloud Infrastructure
- Architecture Security Reviews
- Secure Cloud Native Applications
- Cloud Trust Services
- API Management

CLOUD SECURITY AUTOMATION

- Continuous Risk & Trust Assessment
- Automated Security Posture
- Secure CI/CD Pipelines
- Secure Container Orchestration and Pipelines

SECURE AGILE ORGANIZATION

- Secure Agile Transformation
- DevSecOps Organizational Advisory
- GRC – Agile Alignment

AZURE SECURITY

Assessing security posture of your environments

- Cloud Security Posture Review
- Infrastructure Analysis against Azure Security Best-Practices
- Risk-focused remediation and improvement plans

Architecting secure Azure deployments

- Setup of Azure tenant using Azure best practices such as Microsoft Azure Well-Architected Framework
- Review of Azure native application architecture
- Setup of Azure API Management service
- Adoption of Zero-trust approach to security design

Securing native compute and storage services

- Securing VMs and Blob Storage
- AKS & Serverless applications security
- Securing Azure WebApps, Azure native Databases and other IaaS & PaaS solutions

Designing and implementing sound cloud networking

- Security best practices for Azure Networking & VNETs
- Setup of Azure native security solutions such as Azure Firewall, NSGs, ASGs, ALB, etc.
- Establishing sound network architecture and security (e.g hub-spoke architecture)

Optimally operating and monitoring Azure deployments

- Azure native logging
- Log collection on premise and multi-cloud
- Comprehensive monitoring and alerting using Azure Monitor
- Setup of Azure Sentinel

Achieving Azure security governance

- Role and Administration Concepts
- Security management and compliance via Microsoft Defender
- Continuous Risk & Compliance