Zetlan Technologies

Certified Cloud Security Professional

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

Cloud Concepts Architecture and Design

1. Understand cloud computing concepts

- Cloud computing definitions
- Cloud computg roles & responsibilities (e.g., cloud service cust)
- cloud service broker, regulator)
- Key cloud computing characteristics (e.g., on-demand self-srvc)
- Buildg block technologies (e.g., virtualization, storage, netwrkg)

2. Describe cloud reference architecture

- Cloud computing activities
- Cloud service capabilities (e.g., app capability types, platform)
- Cloud service categories (e.g., (SaaS), (IaaS), (PaaS))
- Cloud deployment models (e.g., public, private, hybrid, comm)
- Cloud shared considerations (e.g., interoperability, portability)
- Impact of related technologies (data science, machine learning)

3. Understand security concepts relevant to cloud computing

- Cryptography and key management
- Identity and access control (user access, privilege access, service)
- Data and media sanitization (e.g., overwritg, cryptographic erase)
- Network security (e.g., network security groups, traffic inspectn)
- Virtualizatn security (e.g., hypervisor security, container security
- Common threats
- Security hygiene (e.g., patching, baselining)

4. Understand design principles of secure cloud computing

- Cloud secure data lifecycle
- Cloud-based businss continuity (BC) & disaster recovery (DR) plan
- Busins impact analysis (BIA) (e.g., cost-benefit analysis, return)
- Functional security requirements (e.g.portability, interoperability)
- Security consideratns & responsibilities for difft cloud categories
- Cloud design pattns (e.g.SANS security principles, Well-Architectd
- DevOps security

5. Evaluate cloud service providers

- Verification against criteria (e.g., International Organization)
- System/subsystem product certifications (e.g.,(CC), (FIPS) 140-2)

Cloud Data Security

6. Describe cloud data concepts

- Cloud data life cycle phases
- Data dispersion
- Data flows

7. Design and implement cloud data storage architectures

- Storage types (e.g., long-term, ephemeral, raw storage)
- Threats to storage types

8. Design and apply data security technologies and strategies

- Encryption and key management
- Hashing
- Data obfuscation (e.g., masking, anonymization)
- Tokenization
- Data loss prevention (DLP)
- Keys, secrets and certificates management

9. Implement data discovery

- Structured data
- Unstructured data
- Semi-structured data
- Data location

10. Implement data classification

- Data classification policies
- Data mapping
- Data labeling

11. Design and implement Information Rights Management (IRM)

- Objectives (e.g., data rights, provisioning, access models)
- Appropriate tools (e.g., issuing and revocation of certificates)

12. Plan and implement data retention, deletion, & archiving policies

- Data retention policies
- Data deletion procedures and mechanisms
- Data archiving procedures and mechanisms
- Legal hold

13. Design & implement auditability, traceability, and accountability

- Definition of event sources and requirement of event attributes
- Logging, storage and analysis of data events
- Chain of custody and non-repudiation

Cloud Platform and Infrastructure Security

14. Comprehend cloud infrastructure components

- Physical environment
- Network and communications
- Compute
- Virtualization
- Storage
- Management plane

15. Design a secure data center

- Logical design (e.g., tenant partitioning, access control)
- Physical design (e.g., location, buy or build)
- Environmental design (e.g., Heating, Ventilation, & Air Conditiong
- Design resilient

16. Analyze risks associated with cloud infrastructure

- Risk assessment (e.g., identification, analysis)
- Cloud vulnerabilities, threats and attacks
- Risk mitigation strategies

17. Design and plan security controls

- Physical and environmental protection (e.g., on-premises)
- System, storage and communication protection
- Identification, authentication & authorization in cloud envirnmnts
- Audit mechanisms (e.g., log collectn, correlation, packet capture)

18. Plan Disaster Recovery (DR) and Business Continuity (BC)

- Business continuity (BC) / disaster recovery (DR) strategy
- Business requirements (e.g., (RTO), Recovery (RPO)
- Creation, implementation and testing of plan

Cloud Application Security

19. Advocate training and awareness for application security

- Cloud development basics
- Common pitfalls
- Common cloud vulnrabilities (e.g.,Open Web App Securty Projct)

20.The Secure Software Development Life Cycle (SDLC) process

- Business requirements
- Phases and methodologies (e.g., design, code, test, maintain,)

21. Apply the Secure Software Development Life Cycle (SDLC)

- Cloud-specific risks
- Threat modeling (e.g., Spoofing, Tampering, Repudiation, Info)
- Avoid common vulnerabilities during development
- Secure coding (e.g., Open Web App Security Project (OWASP)
- Verificatn Standard (ASVS), Software Assurnce Forum for Excelnt
- Software configuration management and versioning

22. Apply cloud software assurance and validation

- Functional and non-functional testing
- Security testing methodologies (e.g., blackbox, whitebox, static)
- Quality assurance (QA)
- Abuse case testing

23. Use verified secure software

- Securing application programming interfaces (API)
- Supply-chain management (e.g., vendor assessment)
- Third-party software management (e.g., licensing)
- Validated open-source software

24. **Comprehend the specifics of cloud application architecture**
    - Supplemental securty components (e.g., web app firewall (WAF))
    - Cryptography
    - Sandboxing
    - Application virtualization and orchestration (e.g., microservices)

25. **Design appropriate Identity and Access Management (IAM) solns**
    - Federated identity
    - Identity providers (IdP)
    - Single sign-on (SSO)
    - Multi-factor authentication (MFA)
    - Cloud access security broker (CASB)
    - Secrets management

Cloud Security Operations

26. **Build & implemt physical & logicl infrastructure for cloud envirmt**
    - Hardware specific security configuration requirements
    - Installation and configuration of management tools
    - Virtual hardware specific security configuration requirements
    - Installation of guest operating system (OS) virtualization toolsets

27. Operate & maintain physical & logical infrastructure for cloud

- Access controls for local & remote access (e.g., Remote Desktop)
- Secure network config (e.g., (VLAN), (TLS), (DHCP), (DNSSEC)..)
- Network security ctrls (e.g., firewalls, intrusion detection systm)
- Operating system (OS) hardening through the app of baselines
- Patch management
- Infrastructure as Code (IaC) strategy
- Availability of clustered hosts (e.g.,distributed resource schedulg)
- Availability of guest operating system (OS)
- Performance and capacity monitoring (e.g., network, compute)
- Hardware monitoring (e.g., disk, central processing unit (CPU)..)
- Configuration of host and guest (OS) backup & restore functions
- Managemnt plane (e.g., scheduling, orchestration, maintenance)

28. Implement operational controls and standards

- Incident management
- Problem management
- Release management
- Deployment management
- Configuration management
- Service level management
- Availability management
- Capacity management

29.Support digital forensics

- Forensic data collection methodologies
- Evidence management
- Collect, acquire, and preserve digital evidence

30.Manage communication with relevant parties

- Vendors
- Customers
- Partners
- Regulators
- Other stakeholders

31. Manage security operations

- Forensic data collection methodologies
- Evidence management
- Collect, acquire, and preserve digital evidence
- Security operations center (SOC)
- Intelligent monitoring of security ctrls (e.g., firewalls,(IDS), etc.,)
- Log capture and analysis (e.g., security info & event managemnt)
- Incident management
- Vulnerability assessments

Legal, Risk and Compliance

32. Articulate legal requrmts & unique risks within the cloud envrnmt

- Conflicting international legislation
- Evaluation of legal risks specific to cloud computing
- Legal framework and guidelines
- eDiscovery (e.g., International Organization for Standardization
- Forensics requirements

33. Understand privacy issues

- Difference between contractual and regulated private data
- Country-specific legislation related to private data
- Jurisdictional differences in data privacy
- Standard privacy requirements (e.g., International Organization)
- Privacy Impact Assessments (PIA)

34.Understd audit process, methodologies, and required adaptations

- Internal and external audit controls
- Impact of audit requirements
- Identify assurance challenges of virtualization and cloud
- Types of audit reports (e.g., (SSAE), (SOC), (ISAE))
- Restrictions of audit scope statements (e.g.,(SSAE), (ISAE))
- Gap analysis (e.g., control analysis, baselines)
- Audit planning
- Internal information security management system
- Internal information security controls system
- Policies (e.g., organizational, functional, cloud computing)
- Identification and involvement of relevant stakeholders
- Specialized compliance requrmnts for highly-regulated industries
- Impact of distributed information technology (IT) model

35. Understand implications of cloud to enterprise risk management

- Providers risk management programs (e.g., controls, methodolgs)
- Diff between data owner/controller vs. data custodian/processor
- Regulatory transparency requirements
- Risk treatment (i.e., avoid, mitigate, transfer, share, acceptance)
- Different risk frameworks
- Metrics for risk management
- Assessment of risk envrnmnt (e.g., service, vendor, infrastructure)

36. Understand outsourcing and cloud contract design

- Business requirements (e.g., (SLA),(MSA), (SOW))
- Vendor managmnt (e.g., vendor assessmnts, vendor lock-in risks)
- Contract mangmnt (e.g., right to audit, metrics, definitions)
- Supply-chain management (e.g., International Organization)

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474