Cloud Security ,Risk, and Posture Management

Training Methodology

- Digital point is a global classroom. All classes are featured online (No recorded version)
- Students around world can join online live class
- Each live class will be recorded, and students will get access to watch video for practice
- Real-world scenario labs
- Class Notes and Labs for each class

Objectives

The demand for cyber security professionals with expertise in cloud security has evolved with the ever-increasing number of businesses moving to the cloud. Moving away from the historic server or on-premises model and into the cloud model has opened a whole new set of security questions and challenges to overcome.

Cloud Security ,Risk, and Posture Management course ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks.

Course Highlights:

- Cloud Concepts, Architecture and Design
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Cloud Security Operations
- Legal, Risk and Compliance

Phase 1: Foundation Training

Module 1: Overview of enterprise applications and N-Tier Infrastructure
Module 2: Operating System –Windows Server 2012/2016, UNIX
Module 3: Networking, Active Directory and DNS
Module 4: Power Shell Scripting, Batch Scripting
Module 5: Incident, Problem and Change Management process

Phase 2: Security Management

Module 6: Security Fundamentals

- Identifying Security Fundamentals
- Identify Information Security Concepts
- Identify Basic Security Controls
- Identify Basic Authentication and Authorization Concepts
- Identify Basic Cryptography Concepts

Module 7: Cloud Concepts, Architecture and Design

- Cloud computing definitions
- Cloud computing roles and responsibilities (e.g., cloud service customer, cloud service provider, cloud service partner, cloud service broker, regulator)
- Key cloud computing characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)
- Building block technologies (e.g., virtualization, storage, networking, databases, orchestration)
- Cloud computing activities
- Cloud service capabilities (e.g., application capability types, platform capability types, infrastructure capability types)
- Cloud service categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Cloud deployment models (e.g., public, private, hybrid, community, multi-cloud)
- Cloud shared considerations (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and service-level agreements (SLA), auditability, regulatory, outsourcing)
- Impact of related technologies (e.g., data science, machine learning, artificial intelligence (AI), blockchain, Internet of Things (IoT), containers, quantum computing, edge computing, confidential computing, DevSecOps)

Module 8: Security concepts relevant to cloud computing

- Understand design principles of secure cloud computing
- Cloud secure data lifecycle » Cloud-based business continuity (BC) and disaster recovery (DR) plan
- Business impact analysis (BIA) (e.g., cost-benefit analysis, return on investment (ROI))
- Functional security requirements (e.g., portability, interoperability, vendor lock-in)
- Security considerations and responsibilities for different cloud categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Cloud design patterns (e.g., SANS security principles, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture)
- DevOps security
- Verification against criteria (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS))
- System/subsystem product certifications (e.g., Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)
- Cryptography and key management
- Identity and access control (e.g., user access, privilege access, service access)
- Data and media sanitization (e.g., overwriting, cryptographic erase)
- Network security (e.g., network security groups, traffic inspection, geofencing, zero trust network)

Module 9: Cloud Data Security

- Cloud data concepts
- Cloud data life cycle phases
- Design and implement cloud data storage architectures

- Storage types (e.g., long-term, ephemeral, raw storage)
- Threats to storage types
- Design and apply data security technologies and strategies
- Implement data discovery
    - Structured data
    - Unstructured data
    - Semi-structured data
- Plan and implement data classification
- Design and implement Information Rights Management (IRM)
- Encryption and key management
    - Hashing
    - Data obfuscation (e.g., masking, anonymization)
    - Tokenization
    - Data loss prevention (DLP)
    - Keys, secrets, and certificates management
- Data classification policies
    - Data mapping
    - Data labeling
- Plan and implement data retention, deletion and archiving policies
    - Data retention policies
    - Data deletion procedures and mechanisms
    - Data archiving procedures and mechanisms
    - Legal hold

Module 10: Cloud Application Security

- Advocate training and awareness for application security
    - Cloud development basics
    - Common pitfalls
    - Common cloud vulnerabilities (e.g., Open Web Application Security Project (OWASP) Top-10, SANS Top-25)
- Secure Software Development Life Cycle (SDLC) process
    - Business requirements
    - Phases and methodologies (e.g., design, code, test, maintain, waterfall vs. agile)
    - Apply cloud software assurance and validation
    - Functional and non-functional testing
    - Security testing methodologies (e.g., blackbox, whitebox, static, dynamic, Software Composition Analysis (SCA), interactive application security testing (IAST))
    - Quality assurance (QA)
    - Securing application programming interfaces (API)
    - Supply-chain management (e.g., vendor assessment)

- Third-party software management (e.g., licensing)
- Validated open-source software Domain

Module 11: Cloud Security Risks

- Cloud-specific risks
  - Threat modeling (e.g., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE), Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD), Architecture, Threats, Attack Surfaces, and Mitigations (ATASM), Process for Attack Simulation and Threat Analysis (PASTA))
  - Avoid common vulnerabilities during development
  - Secure coding (e.g., Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS), Software Assurance Forum for Excellence in Code (SAFECode))
  - Software configuration management and versioning
- Cloud application architecture
  - Supplemental security components (e.g., web application firewall (WAF), Database Activity Monitoring (DAM), Extensible Markup Language (XML) firewalls, application programming interface (API) gateway)
  - Cryptography
  - Sandboxing
  - Application virtualization and orchestration (e.g., microservices, containers)

Module 12: Identity and Access Management

- Design appropriate identity and access management (IAM) solutions
  - Federated identity
  - Identity providers (IdP)
  - Single sign-on (SSO)
  - Multi-factor authentication (MFA)
  - Cloud access security broker (CASB)
  - Secrets management

Module 13: Manage security operations

- Forensic data collection methodologies
- Evidence management
- Collect, acquire, and preserve digital evidence
- Security operations center (SOC)
- Intelligent monitoring of security controls (e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, network security groups, artificial intelligence (AI))
- Log capture and analysis (e.g., security information and event management (SIEM), log management)

- Incident management
- Vulnerability assessments

Module 14: Cryptography

- **Implementing Cryptography**
    - Identify Advanced Cryptography Concepts
    - Select Cryptographic Algorithms
    - Configure a Public Key Infrastructure
    - Enroll Certificates
    - Back Up and Restore Certificates and Private Keys
    - Revoke Certificates

Module 15: Business Continuity

- **Ensuring Business Continuity**
    - Select Business Continuity and Disaster Recovery Processes
    - Develop a Business Continuity Plan

Module 16: Penetration Test

- **Network Penetration Test**

- Plan for Network Penetration Testing
- Conducting Network Penetration Testing
- Generate report for Network Penetration Testing
- Conduct Application Penetration Testing
- Generate Report for Application Penetration Testing

Module 17: DDoS Protections

- Overview of DDoS
- How to onboard an application under DDoS
- Monitoring Application under DDoS
- Overview of WAF
- How to onboard an application under WAF
- Monitoring Application under WAF
- WAF Blocking mode vs alert mode

Module 18:

- **Policies, Standards, Guideline**
    - Overview of Policies, Standards and Guidelines
    - ISO format
    - Application Security policy, standards
    - Network Security policy, standards

Module 19: Boot Camp

- Boot Camp with real-world project - Each student will be required to complete a real-time project lab that covers the entire course curriculum.

Phase 4: Job Marketing

Module 20: Real-world Job Interview Preparation

- Professional real-world Resume Writing
- Project Analysis
- Interview Preparation
- Mock Interview

Contact Us

Phone: 1-703-652-9640 | 226-972-1877

Web: http://training.digitalpoint.tech **Email:** admin@digitalpoint.tech