ReadyBell
Software Services Pvt. Ltd.

Course Name	AWS CERTIFIED SECURITY – SPECIALITY (SCS-C02)
About the Course	This course ensures your expertise in creating and implementing security solutions in the AWS Cloud. This certification also validates your understanding of specialized data classifications and AWS data protection mechanisms; data-encryption methods and AWS mechanisms to implement them; and secure internet protocols and AWS mechanisms to implement them.
Key Skills You Will Learn	AWS shared security responsibility model, Advanced encryption methods, Automated security checks, Secure authentication, Securing network communications within Amazon VPC, Automating security responses, Managing sensitive data
Course Pre-Requisite	Basic understanding of the AWS Cloud Practitioner essentials or equivalent experience, Foundational knowledge of AWS Security Fundamentals, Working knowledge of IT security practices and infrastructure concepts, Familiarity with cloud computing concepts
Target Audience	IT professionals focusing on cloud security and seeking advanced skills in AWS security operations, Security Engineers, Security Architects, Information Security Professionals, Cloud Security Specialists, IT Security Analysts, Cloud Architects, Cloud Engineers with a focus on security, Systems Administrators with responsibilities in security, Network Security Professionals
Job prospects with this role	Cloud Security Engineer, Cloud Network Engineer, Cloud Consultant, Security Engineer, IT Architect, Information Security Analyst, IT Security Specialist, Network Engineer, Cloud Engineer
Course Duration	~ 30 Hrs
Course Customisation	Not applicable
Certification	READYBELL AWS Security - Speciality Certificate
Mode of Training	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner
Course Fees	Please contact us
Refund Policy	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don't give refunds
Job Assistance	Will assist candidate in securing a suitable job
Contact	**READYBELL SOFTWARE SERVICES PVT. LIMITED** **AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091** **E-MAIL: contact@readybellsoftware.com** **PH: +91 - 9147708045/9674552097, +91 - 33-79642872**

ReadyBell
Software Services Pvt. Ltd.

CURRICULUM		
Topic	**Sub-Topic**	**Duration (Hrs)**
AWS CERTIFIED SECURITY – SPECIALITY (SCS-C02)	**Domain 1: Threat Detection and Incident Response**	30 Hrs
	Design and implement an incident response plan	
	Incident Response Strategy	
	Roles and responsibilities in IR plan specific to cloud incidents.	
	Use case 1: Credentials compromise.	
	Use case 2: Compromised EC2 Instances	
	Playbooks and Runbooks for IR	
	AWS Specific services helpful in Incident Response	
	Third-party integration concepts	
	Centralize security finding with security hub	
	Detect security threats and anomalies by using AWS services	
	Threat detection services specific to AWS	
	Visualizing and Detecting anomalies and correlation techniques	
	Evaluate finding from security services	
	Performing queries for validating security events	
	Create metrics filters and dashboards to detect Anomalous activity	
	Respond to compromised resources and workloads	
	AWS Security IR Guide	
	Automating remediation by using AWS services	
	Compromised resource management.	
	Investigating and analyzing to conduct Root cause and log analysis.	
	Capturing relevant forensics data from a compromised resource	
	Protecting and preserving forensic artifacts	
	Post-incident recovery	
	Domain 2: Security Logging and Monitoring	
	Design and Implement monitoring and alerting to address security events	
	Key AWS services for monitoring and alerting	
	Monitoring metrics and baselines	
	Analyzing environments and workloads to determine monitoring requirements according to	
	business and security requirements	
	Setting up tools and scripts to perform regular audits	
	Troubleshoot security monitoring and alerting	
	Configuring of monitoring services and collecting event data	
	Application monitoring, alerting, and visibility challenges	

	Design and implement a logging solution	
	Key logging services and attributes	
	Log destinations, Ingestion points and lifecycle management	
	Logging specific to services and applications	
	Troubleshoot logging solutions	
	AWS services that provide data sources and logging capabilities	
	Access permissions that are necessary for logging	
	Identifying misconfigurations and remediations specific to logging	
	Reasons for missing logs and performing remediation steps	
	Design a log analysis solution	
	Services and tools to analyze captured logs	
	Identifying patterns in logs to indicate anomalies and known threats	
	Log analysis features for AWS services	
	Log format and components	
	Normalizing, parsing, and correlating logs	
	Domain 3: Infrastructure Security	
	Design and implement security controls for edge services	
	Define edge security strategies and security features	
	Select proper edge services based on anticipated threats and attacks and define proper	
	protection mechanisms based on that	
	Define layered Defense (Defense in Depth) mechanisms	
	Applying restrictions based on different criteria	
	Enable logging and monitoring across edge services to indicate attacks	
	Design and implement network security controls	
	VPC security mechanisms including Security Groups, NACLs, and Network firewall	
	Traffic Mirroring and VPC Flow Logs	
	VPC Security mechanisms and implement network segmentation based on security requirements	
	Network traffic management and segmentation	
	Inter-VPC connectivity, Traffic isolation, and VPN concepts and deployment	
	Peering and Transit Gateway	
	AWS Point to Site and Site to Site VPN, Direct Connect	
	Continuous optimization by identifying and removing unnecessary network access	
	Design and implement security controls for compute workloads	
	Provisioning and maintenance of EC2 instances	
	Create hardened images and backups	
	Applying instance and service roles for defining permissions	

	Host-based security mechanisms	
	Vulnerability assessment using AWS Inspector	
	Passing secrets and credentials security to computing workloads	
	Troubleshoot network security	
	Identifying, interpreting, and prioritizing network connectivity and analyzing reachability	
	Analyse log sources to identify problems	
	Network traffic sampling using traffic mirroring	
	Domain 4: Identity and Access Management	
	Design, implement and troubleshoot authentication for AWS resources	
	Identity and Access Management	
	Establish identity through an authentication system based on requirements.	
	Managed Identities, Identity federation	
	AWS Identity center, IAM and Cognito	
	MFA, Conditional access, STS	
	Troubleshoot authentication issues	
	Design, implement and troubleshoot authorization for AWS resources	
	IAM policies and types	
	Policy structure and troubleshooting	
	Troubleshoot authorization issues	
	ABAC and RBAC strategies	
	Principle of least privilege and Separation of duties	
	Investigate unintended permissions, authorization, or privileges	
	Domain 5: Data Protection	
	Design and implement controls that provide confidentiality and integrity for data in transit	
	Design secure connectivity between AWS and on-premises networks	
	Design mechanisms to require encryption when connecting to resources.	
	Requiring DIT encryption for AWS API calls.	
	Design mechanisms to forward traffic over secure connections.	
	Designing cross-region networking	
	Design and implement controls that provide confidentiality and integrity for data at rest	
	Encryption and integrity concepts	
	Resource policies	
	Configure services to activate encryption for data at rest and to protect data integrity by preventing	
	modifications.	
	Cloud HSM and KMS	

	Design and implement controls to manage the data lifecycle at rest	
	Lifecycle policies and configurations	
	Automated life cycle management	
	Establishing schedules and retention for AWS backup across AWS services.	
	Design and implement controls to protect credentials, secrets, and cryptographic key materials	
	Designing management and rotation of secrets for workloads using a secret manager	
	Designing KMS key policies to limit key usage to authorized users.	
	Establishing mechanisms to import and remove customer-provider key material.	
	Domain 6: Management and Security Governance	
	Design and strategy to centrally deploy and manage AWS accounts	
	Multi account strategies using AWS organization and Control tower	
	SCPs and Policy multi-account policy enforcement	
	Centralized management of security services and aggregation of findings	
	Securing root account access	
	Implement a secure and consistent deployment strategy for cloud resources	
	Deployment best practices with Infrastructure as a code	
	Tagging and metadata	
	Configure and deploy portfolios of approved AWS services.	
	Securely sharing resources across AWS accounts	
	Visibility and control over AWS infrastructure	
	Evaluate compliance of AWS resources	
	Data classification by using AWS services	
	Define config rules for detection of non-compliant AWS resources.	
	Collecting and organizing evidence by using Security Hub and AWS audit manager	
	Identify security gaps through architectural reviews and cost analysis	
	AWS cost and usage anomaly identification	
	Strategies to reduce attack surfaces	
	AWS well-architected framework to identify security gaps	

To register for this course please e-mail/call us