Guida all'esame AWS Certified Security - Specialty (SCS-C02)

Introduzione

L'esame AWS Certified Security - Specialty (SCS-C02) è rivolto a persone che svolgono un ruolo nell'ambito della sicurezza. In questo esame vengono valutate le capacità di un candidato di dimostrare efficacemente le proprie conoscenze in merito ai prodotti e ai servizi AWS.

Viene inoltre verificato che il candidato abbia:

- Conoscenze sulle categorie di dati speciali e sui meccanismi di protezione dei dati AWS
- Conoscenze sui metodi di crittografia dei dati e sui meccanismi AWS per implementarli
- Conoscenze sui protocolli di sicurezza Internet e sui meccanismi AWS per implementarli
- Conoscenze pratiche riguardo ai servizi di AWS Security e alle loro funzionalità per fornire un ambiente di produzione sicuro
- Due o più anni di esperienza nella distribuzione in ambienti di produzione utilizzando servizi e caratteristiche di AWS Security
- Capacità di prendere decisioni di compromesso in termini di costi, sicurezza e complessità di implementazione per soddisfare una serie di requisiti specifici di un'applicazione
- Conoscenze sulle operazioni e sui rischi legati alla sicurezza

Descrizione del candidato target

Il candidato target ha l'equivalente di 3-5 anni di esperienza nella progettazione e nell'implementazione di soluzioni di sicurezza. Ha inoltre almeno 2 anni di esperienza pratica nella protezione dei carichi di lavoro AWS.

Conoscenze AWS consigliate

Il candidato target dovrebbe possedere conoscenze su:

- Modello di responsabilità condivisa di AWS e sua applicazione
- Conoscenza generale dei servizi AWS e dell'implementazione di soluzioni cloud
- Controlli di sicurezza per ambienti e carichi di lavoro AWS
- Strategie di registrazione di log e monitoraggio
- Gestione delle vulnerabilità e automazione della sicurezza
- Metodi per integrare i servizi di sicurezza AWS con strumenti di terze parti
- Controlli per il ripristino d'emergenza, comprese le strategie di backup
- Crittografia e gestione delle chiavi
- Identity and Access Management
- Conservazione dei dati e gestione del ciclo di vita
- Modalità di risoluzione dei problemi relativi alla sicurezza
- Governance multi-account e conformità dell'organizzazione
- Strategie di rilevamento delle minacce e risposta agli incidenti

Attività lavorative che non rientrano nelle competenze del candidato target

Il seguente elenco illustra le attività lavorative che non rientrano nelle competenze previste per il candidato target. L'elenco non è esaustivo. Le seguenti attività non rientrano nell'ambito dell'esame:

- Sviluppo di software in un linguaggio specifico (ad esempio Python e Java).
- Rispetto della conformità alle normative.
- Gestione dei cicli di vita dello sviluppo software.
- Progettazione di topologie di rete.
- Creazione dell'architettura di implementazioni cloud globali.
- Configurazione dei servizi di archiviazione in base ai requisiti di residenza dei dati, ad esempio il Regolamento generale sulla protezione dei dati (GDPR).

Consulta l'Appendice per un elenco di tecnologie e concetti che potrebbero essere inclusi nell'esame, nonché per un elenco di servizi e funzionalità AWS trattati in sede d'esame e un elenco di quelli esclusi.

Contenuto dell'esame

Tipi di risposta

L'esame prevede due tipi di domande:

- **Scelta multipla:** una risposta corretta e tre risposte errate (distrattori)
- **Risposta multipla:** due o più risposte corrette su cinque o più opzioni di risposta

Selezionare una o più risposte che meglio completano l'affermazione o rispondono alla domanda. I distrattori, o risposte errate, sono opzioni di risposta che possono essere scelte da candidati con conoscenze o competenze insufficienti. Solitamente, i distrattori sono risposte plausibili che rientrano nell'ambito dei contenuti trattati.

Le domande senza risposta sono valutate come errate; non è applicata alcuna penalità se il candidato tenta una risposta. L'esame prevede 50 domande che influiscono sul punteggio finale.

Contenuto senza punteggio

L'esame include 15 domande alle quali non viene assegnato un punteggio e che non influiscono sul risultato finale. AWS raccoglie informazioni sulle prestazioni relativamente a queste domande, al fine di valutare la possibilità di convertirle in futuro in domande a punteggio. In sede di esame, le domande che non influiscono sul punteggio non verranno distinte dalle altre.

Risultati dell'esame

L'esame AWS Certified Security - Specialty (SCS-C02) prevede un esito netto, superamento o mancato superamento. La valutazione avviene in base a uno standard minimo stabilito da professionisti AWS che seguono le best practice e le linee guida del settore delle certificazioni.

I risultati dell'esame sono espressi da un punteggio compreso tra 100 e 1.000. Il punteggio minimo richiesto per il superamento della prova è 750. Il punteggio riflette le prestazioni complessive del candidato all'esame e indica se quest'ultimo è stato superato o meno. I modelli di punteggio scalare aiutano a equiparare i punteggi tra moduli dell'esame che potrebbero presentare livelli di difficoltà leggermente diversi.

Il report relativo al punteggio può contenere una tabella di classificazione del rendimento in ogni sezione. Per l'esame viene impiegato un modello di punteggio compensativo; ciò significa che non è necessario ottenere un punteggio sufficiente in ogni sezione. L'esame viene superato se il punteggio complessivo ottenuto corrisponde almeno al minimo richiesto.

Ogni sezione ha un proprio peso specifico, quindi alcune di esse presentano più domande di altre. La seguente tabella delle classificazioni include informazioni generali che evidenziano i punti forti e deboli del candidato. Interpreta con la massima attenzione il feedback relativo a ogni sezione.

Descrizione del contenuto

Questa guida all'esame include informazioni sui pesi, sui domini dei contenuti e sugli obiettivi dell'esame. Non fornisce un elenco esaustivo dei contenuti dell'esame. Tuttavia, per ogni obiettivo è disponibile maggiore contesto come aiuto durante la preparazione all'esame.

Di seguito sono elencati i domini dei contenuti e i pesi dell'esame:

- Dominio 1. Rilevamento delle minacce e risposta agli incidenti (14% dei contenuti a punteggio)
- Dominio 2. Monitoraggio della sicurezza e registrazione di log (18% dei contenuti a punteggio)
- Dominio 3. Sicurezza dell'infrastruttura (20% dei contenuti a punteggio)
- Dominio 4. Identity and Access Management (16% dei contenuti a punteggio)
- Dominio 5. Protezione dei dati (18% dei contenuti a punteggio)
- Dominio 6. Gestione e governance della sicurezza (14% dei contenuti a punteggio)

Dominio 1. Rilevamento delle minacce e risposta agli incidenti

Obiettivo 1.1: progettazione e implementazione di un piano di risposta agli incidenti.

Conoscenza di:

- Best practice AWS per la risposta agli incidenti
- Incidenti relativi al cloud
- Ruoli e responsabilità nel piano di risposta agli incidenti

- AWS Security Finding Format (ASFF)

Competenze in:

- Implementazione di strategie di invalidazione e rotazione delle credenziali in risposta a compromissioni (ad esempio tramite AWS Identity and Access Management [IAM] e AWS Secrets Manager)
- Isolamento delle risorse AWS
- Progettazione e implementazione di playbook e runbook per le risposte agli incidenti di sicurezza
- Implementazione di servizi di sicurezza (ad esempio AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- Configurazione delle integrazioni con servizi AWS nativi e servizi di terze parti (ad esempio tramite Amazon EventBridge e il formato ASFF)

Obiettivo 1.2: rilevamento di anomalie e minacce alla sicurezza tramite i servizi AWS.

Conoscenza di:

- Servizi di sicurezza gestiti da AWS in grado di rilevare le minacce
- Anomalie e tecniche di correlazione per unire i dati tra i servizi
- Visualizzazioni per identificare le anomalie
- Strategie per centralizzare i risultati di sicurezza

Competenze in:

- Valutazione dei risultati dei servizi di sicurezza (ad esempio GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)
- Ricerca e correlazione delle minacce alla sicurezza tra i servizi AWS (ad esempio tramite Detective)
- Esecuzione di query per convalidare gli eventi di sicurezza (ad esempio tramite Amazon Athena)
- Creazione di dashboard e filtri di metriche per rilevare attività anomale (ad esempio tramite Amazon CloudWatch)

Obiettivo 1.3: risposta alla compromissione di risorse e carichi di lavoro.

Conoscenza di:

- Guida alle risposte agli incidenti di sicurezza di AWS
- Meccanismi di isolamento delle risorse
- Tecniche per l'analisi della causa principale
- Meccanismi di acquisizione dei dati
- Analisi dei log per la convalida degli eventi

Competenze in:

- Automazione delle correzioni tramite i servizi AWS (ad esempio AWS Lambda, AWS Step Functions, EventBridge, runbook di AWS Systems Manager, Security Hub, AWS Config)
- Risposta alla compromissione delle risorse (ad esempio isolando le istanze Amazon EC2)
- Studio e ricerca per condurre l'analisi della causa principale (ad esempio tramite Detective)
- Acquisizione di dati forensi pertinenti da una risorsa compromessa (ad esempio snapshot di volumi Amazon Elastic Block Store [Amazon EBS], dump della memoria)
- Esecuzione di query sui log in Amazon S3 per informazioni contestuali relative agli eventi di sicurezza (ad esempio tramite Athena)
- Protezione e conservazione degli artefatti forensi (ad esempio tramite blocco oggetti S3, account forensi isolati, ciclo di vita di S3 e replica S3)
- Preparazione dei servizi per gli incidenti e ripristino dopo gli incidenti

Dominio 2. Monitoraggio della sicurezza e registrazione di log

Obiettivo 2.1: progettazione e implementazione del monitoraggio e degli avvisi per affrontare gli eventi di sicurezza.

Conoscenza di:

- Servizi AWS che monitorano gli eventi e forniscono allarmi (ad esempio CloudWatch, EventBridge)
- Servizi AWS che automatizzano gli avvisi (ad esempio Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub)
- Strumenti che monitorano metriche e basi di riferimento (ad esempio GuardDuty, Systems Manager)

Competenze in:

- Analisi delle architetture per identificare i requisiti di monitoraggio e le origini di dati per il monitoraggio della sicurezza
- Analisi degli ambienti e dei carichi di lavoro per stabilire i requisiti di monitoraggio
- Progettazione del monitoraggio dell'ambiente e del carico di lavoro in base ai requisiti aziendali e di sicurezza
- Configurazione di strumenti e script automatizzati per eseguire verifiche regolari (ad esempio creando informazioni personalizzate in Security Hub)
- Definizione delle metriche e delle soglie che generano gli avvisi

Obiettivo 2.2: risoluzione dei problemi di monitoraggio e avvisi di sicurezza.

Conoscenza di:

- Configurazione dei servizi di monitoraggio (ad esempio Security Hub)
- Dati pertinenti indicativi di eventi di sicurezza

Competenze in:

- Analisi della funzionalità del servizio, delle autorizzazioni e della configurazione delle risorse dopo un evento che non ha fornito visibilità o avvisi
- Analisi e correzione della configurazione di un'applicazione personalizzata che non esegue il report delle proprie statistiche
- Valutazione dei servizi di registrazione di log e monitoraggio per l'allineamento ai requisiti di sicurezza

Obiettivo 2.3: progettazione e implementazione di una soluzione di registrazione di log.

Conoscenza di:

- Servizi e funzionalità AWS che forniscono funzionalità di registrazione di log (ad esempio log di flusso VPC, log DNS, AWS CloudTrail, Amazon CloudWatch Logs)
- Attributi delle funzionalità di registrazione di log (ad esempio livelli di log, tipo, dettaglio)
- Registrazione delle destinazioni e gestione del ciclo di vita (ad esempio periodo di conservazione)

Competenze in:

- Configurazione della registrazione di log per servizi e applicazioni
- Identificazione dei requisiti di registrazione e delle origini per l'acquisizione dati dei log
- Implementazione dell'archiviazione dei log e della gestione del ciclo di vita in base alle best practice di AWS e ai requisiti dell'organizzazione

Obiettivo 2.4: risoluzione dei problemi relativi alle soluzioni di registrazione di log.

Conoscenza di:

- Funzionalità e casi d'uso dei servizi AWS che forniscono origini dei dati (ad esempio livello di log, tipo, dettaglio, cadenza, tempestività, immutabilità)
- Servizi e funzionalità AWS che forniscono funzionalità di registrazione di log (ad esempio log di flusso VPC, registri DNS, CloudTrail, CloudWatch Logs)
- Autorizzazioni di accesso necessarie per la registrazione di log

Competenze in:

- Identificazione degli errori di configurazione e definizione delle misure correttive per le autorizzazioni di accesso assenti, ma necessarie per la registrazione di log (ad esempio gestendo le autorizzazioni di lettura/scrittura, le autorizzazioni del bucket S3, l'accesso pubblico e l'integrità)
- Definizione della causa dei log mancanti ed esecuzione delle operazioni di correzione

Obiettivo 2.5: progettazione di una soluzione di analisi dei log.

Conoscenza di:

- Servizi e strumenti per analizzare i log acquisiti (ad esempio filtro Athena, CloudWatch Logs)
- Funzionalità di analisi dei log dei servizi AWS (ad esempio CloudWatch Logs Insights, CloudTrail Insights, informazioni di Security Hub)
- Formato e componenti dei log (ad esempio i log di CloudTrail)

Competenze in:

- Identificazione dei modelli nei log per indicare anomalie e minacce note
- Normalizzazione, analisi e correlazione dei log

Dominio 3. Sicurezza dell'infrastruttura

Obiettivo 3.1: progettazione e implementazione dei controlli di sicurezza per i servizi edge.

Conoscenza di:

- Funzionalità di sicurezza sui servizi edge (ad esempio AWS WAF, bilanciatori del carico, Amazon Route 53, Amazon CloudFront, AWS Shield)
- Attacchi, minacce ed exploit comuni (ad esempio Open Web Application Security Project [OWASP] Top 10, DDoS)
- Architettura delle applicazioni web a più livelli

Competenze in:

- Definizione di strategie di sicurezza edge per i casi d'uso più comuni (ad esempio sito web pubblico, app serverless, back-end per applicazioni per dispositivi mobili)
- Selezione dei servizi edge appropriati in base alle minacce e agli attacchi previsti (ad esempio OWASP Top 10, DDoS)
- Selezione delle misure di protezione appropriate in base alle vulnerabilità e ai rischi previsti (ad esempio software, applicazioni, librerie vulnerabili)
- Definizione dei livelli di difesa coniugando servizi di sicurezza edge all'avanguardia (ad esempio CloudFront con AWS WAF e bilanciatori del carico)
- Applicazione di restrizioni a livello edge in base a vari criteri (ad esempio geografia, geolocalizzazione, limite di velocità)
- Attivazione di log, metriche e monitoraggio dei servizi edge per indicare gli attacchi

Obiettivo 3.2: progettazione e implementazione dei controlli di sicurezza della rete.

Conoscenza di:

- Meccanismi di sicurezza VPC (ad esempio gruppi di sicurezza, liste di controllo degli accessi di rete, AWS Network Firewall)
- Connettività tra VPC (ad esempio AWS Transit Gateway, endpoint VPC)
- Origini di telemetria di sicurezza (ad esempio funzione Mirroring del traffico, log di flusso VPC)
- Tecnologia, terminologia e utilizzo di VPN

- Opzioni di connettività on-premises (ad esempio AWS VPN, AWS Direct Connect)

Competenze in:

- Implementazione della segmentazione di rete in base ai requisiti di sicurezza (ad esempio sottoreti pubbliche e private, VPC sensibili, connettività on-premises)
- Progettazione di controlli di rete per consentire o impedire il traffico di rete secondo necessità (ad esempio tramite gruppi di sicurezza, liste di controllo degli accessi di rete e Network Firewall)
- Progettazione di flussi di rete per tenere i dati lontani dalla rete Internet pubblica (ad esempio tramite Transit Gateway, endpoint VPC e Lambda nei VPC)
- Definizione delle origini di telemetria da monitorare in base alla progettazione della rete, alle minacce e agli attacchi (ad esempio log di bilanciatori del carico, log di flusso VPC, funzione Mirroring del traffico)
- Definizione dei requisiti di ridondanza e sicurezza del carico di lavoro per la comunicazione tra ambienti on-premises e il Cloud AWS (ad esempio tramite AWS VPN, AWS VPN su Direct Connect e MACsec)
- Identificazione e rimozione degli accessi di rete non necessari
- Gestione delle configurazioni di rete al variare dei requisiti (ad esempio tramite AWS Firewall Manager)

Obiettivo 3.3: progettazione e implementazione dei controlli di sicurezza dei carichi di lavoro di calcolo.

Conoscenza di:

- Provisioning e manutenzione delle istanze EC2 (ad esempio applicazione di patch, ispezione, creazione di snapshot e AMI, utilizzo di EC2 Image Builder)
- Ruoli di istanza IAM e ruoli di servizio IAM
- Servizi che analizzano le vulnerabilità nei carichi di lavoro di elaborazione (ad esempio Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR])
- Sicurezza basata su host (ad esempio firewall, rafforzamento)

Competenze in:

- Creazione di AMI EC2 rafforzate
- Applicazione dei ruoli di istanza e dei ruoli di servizio in modo appropriato per autorizzare i carichi di lavoro di elaborazione
- Scansione delle istanze EC2 e delle immagini dei container per individuare vulnerabilità note
- Applicazione di patch su un parco istanze EC2 o immagini dei container
- Attivazione di meccanismi di sicurezza basati su host (ad esempio firewall basati su host)
- Analisi dei risultati di Amazon Inspector e definizione delle tecniche di mitigazione appropriate
- Trasmissione sicura di segreti e credenziali ai carichi di lavoro di elaborazione

Obiettivo 3.4: risoluzione dei problemi di sicurezza della rete.

Conoscenza di:

- Come analizzare la raggiungibilità (ad esempio tramite VPC Reachability Analyzer e Amazon Inspector)
- Concetti fondamentali di rete TCP/IP (ad esempio UDP rispetto a TCP, porte, modello Open Systems Interconnection [OSI], utilità per il sistema operativo di rete)
- Come leggere le origini dei log pertinenti (ad esempio i log di Route 53, i log di AWS WAF, i log di flusso VPC)

Competenze in:

- Identificazione e interpretazione dei problemi di connettività di rete e relativa assegnazione di priorità (ad esempio tramite Amazon Inspector Network Reachability)
- Definizione di soluzioni per produrre il comportamento di rete desiderato
- Analisi delle origini dei log per identificare i problemi
- Acquisizione di campioni di traffico per l'analisi dei problemi (ad esempio tramite la funzione Mirroring del traffico)

Dominio 4. Identity and Access Management

Obiettivo 4.1: progettazione, implementazione e risoluzione dei problemi di autenticazione delle risorse AWS.

Conoscenza di:

- Metodi e servizi per la creazione e la gestione delle identità, ad esempio federazione, provider di identità, AWS IAM Identity Center (AWS Single Sign-On), Amazon Cognito
- Meccanismi di emissione di credenziali temporanee e a lungo termine
- Come risolvere i problemi di autenticazione (ad esempio tramite CloudTrail, IAM Access Advisor e il simulatore di policy IAM)

Competenze in:

- Definizione dell'identità tramite un sistema di autenticazione, in base ai requisiti
- Configurazione dell'autenticazione a più fattori (MFA)
- Definizione dei casi in cui utilizzare AWS Security Token Service (AWS STS) per emettere credenziali temporanee

Obiettivo 4.2: progettazione, implementazione e risoluzione dei problemi di autorizzazione delle risorse AWS.

Conoscenza di:

- Diverse policy IAM (ad esempio policy gestite, inline, basate sull'identità o sulle risorse, di controllo delle sessioni)
- Componenti di una policy (ad esempio Principale, Azione, Risorsa, Condizione) e impatto
- Come risolvere i problemi di autorizzazione (ad esempio tramite CloudTrail, IAM Access Advisor e il simulatore di policy IAM)

Competenze in:

- Creazione di strategie di controllo degli accessi basato sugli attributi (ABAC) e di controllo degli accessi basato sui ruoli (RBAC)
- Valutazione dei tipi di policy IAM per determinati requisiti e carichi di lavoro
- Interpretazione dell'effetto di una policy IAM su ambienti e carichi di lavoro
- Applicazione del principio del privilegio minimo in un ambiente

- Attuazione di un'adeguata separazione dei doveri
- Analisi degli errori di accesso o di autorizzazione per stabilire la causa o l'effetto
- Indagine sulla concessione non voluta di permessi, autorizzazioni o privilegi a una risorsa, un servizio o un'entità

Dominio 5. Protezione dei dati

Obiettivo 5.1: progettazione e implementazione di controlli che garantiscano riservatezza e integrità per i dati in transito.

Conoscenza di:

- Concetti relativi al protocollo TLS
- Concetti relativi alla VPN (ad esempio IPsec)
- Metodi di accesso remoto sicuri (ad esempio SSH, RDP su Systems Manager Session Manager)
- Concetti relativi a Systems Manager Session Manager
- Come funzionano i certificati TLS con vari servizi e risorse di rete (ad esempio CloudFront, bilanciatori del carico)

Competenze in:

- Progettazione di connettività sicura tra AWS e reti on-premises (ad esempio tramite Direct Connect e gateway VPN)
- Progettazione di meccanismi per richiedere la crittografia durante la connessione alle risorse (ad esempio Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, bilanciatori del carico, Amazon Elastic File System [Amazon EFS], Amazon API Gateway)
- Richiesta di TLS per le chiamate API AWS (ad esempio con Amazon S3)
- Progettazione di meccanismi per inoltrare il traffico su connessioni sicure (ad esempio tramite Systems Manager ed EC2 Instance Connect)
- Progettazione di reti fra regioni con VIF private e VIF pubbliche

Obiettivo 5.2: progettazione e implementazione di controlli che garantiscano riservatezza e integrità per i dati a riposo.

Conoscenza di:

- Selezione della tecnica di crittografia (ad esempio lato client, lato server, simmetrica, asimmetrica)
- Tecniche di controllo dell'integrità (ad esempio algoritmi di hashing, firme digitali)
- Policy relative alle risorse (ad esempio per DynamoDB, Amazon S3 e AWS Key Management Service [AWS KMS])
- Ruoli e policy IAM

Competenze in:

- Progettazione di policy di risorse per limitare l'accesso agli utenti autorizzati (ad esempio policy per bucket S3 o DynamoDB)
- Progettazione di meccanismi per impedire l'accesso pubblico non autorizzato (ad esempio blocco dell'accesso pubblico S3, prevenzione di snapshot pubblici e AMI pubbliche)
- Configurazione dei servizi per attivare la crittografia dei dati a riposo (ad esempio Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS)
- Progettazione di meccanismi per proteggere l'integrità dei dati impedendo le modifiche (ad esempio tramite blocco oggetti S3, policy delle chiavi KMS, vault lock di S3 Glacier e vault lock di AWS Backup)
- Progettazione della crittografia a riposo utilizzando AWS CloudHSM per database relazionali (ad esempio Amazon RDS, RDS Custom, database su istanze EC2)
- Scelta delle tecniche di crittografia in base ai requisiti aziendali

Obiettivo 5.3: progettazione e implementazione di controlli per gestire il ciclo di vita dei dati a riposo.

Conoscenza di:

- Policy del ciclo di vita
- Standard di conservazione dei dati

Competenze in:

- Progettazione di meccanismi del ciclo di vita S3 per la conservazione dei dati per i periodi richiesti (ad esempio blocco oggetti S3, vault lock di S3 Glacier, policy del ciclo di vita S3)
- Progettazione della gestione automatica del ciclo di vita per servizi e risorse AWS (ad esempio Amazon S3, snapshot di volumi EBS, snapshot di volumi RDS, AMI, immagini di container, gruppi di log CloudWatch, Amazon Data Lifecycle Manager)
- Definizione di pianificazioni e conservazione per AWS Backup tra i servizi AWS

Obiettivo 5.4: progettazione e implementazione di controlli per proteggere credenziali, segreti e materiali delle chiavi di crittografia.

Conoscenza di:

- Secrets Manager
- Archivio dei parametri Systems Manager
- Utilizzo e gestione di chiavi simmetriche e asimmetriche (ad esempio AWS KMS)

Competenze in:

- Progettazione della gestione e della rotazione dei segreti per i carichi di lavoro (ad esempio credenziali di accesso al database, chiavi API, chiavi di accesso IAM, chiavi gestite dai clienti AWS KMS)
- Progettazione di policy per le chiavi KMS per limitare l'utilizzo delle chiavi agli utenti autorizzati
- Attuazione di meccanismi per importare e rimuovere il materiale della chiave fornito dal cliente

Dominio 6. Gestione e governance della sicurezza

Obiettivo 6.1: sviluppo di una strategia per distribuire e gestire centralmente gli account AWS.

Conoscenza di:

- Strategie multi-account
- Servizi gestiti che consentono l'amministrazione delegata

- Guardrail definiti da policy
- Best practice per l'account root
- Ruoli IAM multi-account

Competenze in:

- Implementazione e configurazione di AWS Organizations
- Definizione di quando e come distribuire AWS Control Tower (ad esempio quali servizi devono essere disattivati per una distribuzione corretta)
- Implementazione di policy di controllo dei servizi come soluzione tecnica per l'applicazione delle policy (ad esempio limitazioni all'uso di un account root, implementazione di controlli in AWS Control Tower)
- Gestione centralizzata dei servizi di sicurezza e aggregazione dei risultati (ad esempio tramite l'amministrazione delegata e gli aggregatori AWS Config)
- Protezione delle credenziali dell'utente root nell'account AWS

Obiettivo 6.2: implementazione di una strategia di distribuzione sicura e coerente per le risorse cloud.

Conoscenza di:

- Best practice di implementazione con Infrastructure as Code (IaC) (ad esempio rafforzamento dei template di AWS CloudFormation e rilevamento delle deviazioni)
- Best practice per l'assegnazione di tag
- Gestione, distribuzione e controllo delle versioni centralizzati dei servizi AWS
- Visibilità e controllo sull'infrastruttura AWS

Competenze in:

- Utilizzo di CloudFormation per distribuire le risorse cloud in modo coerente e sicuro
- Implementazione e applicazione di strategie multi-account per l'assegnazione di tag
- Configurazione e implementazione di portafogli di servizi AWS approvati (ad esempio tramite AWS Service Catalog)
- Organizzazione delle risorse AWS in diversi gruppi per la gestione
- Implementazione di Firewall Manager per l'applicazione delle policy

- Condivisione sicura delle risorse tra account AWS (ad esempio tramite AWS Resource Access Manager [AWS RAM])

Obiettivo 6.3: valutazione della conformità delle risorse AWS.

Conoscenza di:

- Classificazione dei dati con i servizi AWS
- Metodi per vagliare, verificare e valutare le configurazioni delle risorse AWS (ad esempio tramite AWS Config)

Competenze in:

- Identificazione dei dati sensibili tramite Macie
- Creazione di regole AWS Config per il rilevamento di risorse AWS non conformi
- Raccolta e organizzazione delle prove tramite Security Hub e AWS Audit Manager

Obiettivo 6.4: identificazione delle lacune di sicurezza attraverso valutazioni dell'architettura e analisi dei costi.

Conoscenza di:

- Costi e utilizzo di AWS per l'identificazione delle anomalie
- Strategie per ridurre le superfici di attacco
- Framework AWS Well-Architected

Competenze in:

- Identificazione delle anomalie in base all'utilizzo e alle tendenze delle risorse
- Identificazione delle risorse inutilizzate tramite servizi e strumenti AWS (ad esempio AWS Trusted Advisor, AWS Cost Explorer)
- Utilizzo di AWS Well-Architected Tool per identificare le lacune di sicurezza

Appendice

Tecnologie e concetti che potrebbero essere inclusi nell'esame

Il seguente elenco contiene tecnologie e concetti che potrebbero essere inclusi nell'esame. Si tratta di un elenco non esaustivo e soggetto a modifiche. L'ordine e la posizione delle voci nell'elenco non sono rappresentativi del loro peso o importanza in relazione all'esame:

- AWS CLI
- SDK AWS
- Console di gestione AWS
- Accesso remoto sicuro
- Gestione dei certificati
- Infrastructure as Code (IaC)

Servizi e funzionalità AWS trattati in sede di esame

Nota: la sicurezza influisce su tutti i servizi AWS. Molti servizi non compaiono in questo elenco perché il loro funzionamento generale non rientra tra gli argomenti d'esame, ma solo gli aspetti del servizio relativi alla sicurezza. Ad esempio, questo esame potrebbe includere domande circa la configurazione di una policy relativa ai bucket S3, ma non verrà chiesto al candidato di descrivere i passaggi per impostare la replica di un bucket S3.

Il seguente elenco contiene i servizi e le funzionalità AWS trattati nell'esame. Si tratta di un elenco non esaustivo e soggetto a modifiche. Le offerte AWS sono suddivise in categorie in funzione delle loro funzioni principali:

Gestione e governance su AWS:

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Organizations
- AWS Systems Manager
- AWS Trusted Advisor

Reti e distribuzione di contenuti:

- Amazon VPC
  - Network Access Analyzer
  - Liste di controllo degli accessi di rete
  - Gruppi di sicurezza
  - Endpoint VPC

Sicurezza, identità e conformità:

- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS IAM Identity Center (AWS Single Sign-On)
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- AWS WAF

Servizi e funzionalità AWS non trattati in sede di esame

Il seguente elenco contiene i servizi e le funzionalità AWS non trattati nell'esame. Si tratta di un elenco non esaustivo e soggetto a modifiche. Sono esclusi da questo elenco le offerte AWS del tutto estranee ai ruoli target per l'esame:

Blockchain:

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database (Amazon QLDB)

Applicazioni aziendali:

- Alexa for Business
- Amazon Chime
- SDK di Amazon Chime
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- Catena di approvvigionamento di AWS
- AWS Wickr
- Amazon WorkDocs

Servizi informatici per utenti finali:

- Amazon AppStream 2.0

Servizi multimediali:

- Amazon Elastic Transcoder
- Appliance e software AWS Elemental
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Interactive Video Service (Amazon IVS)
- Amazon Kinesis Video Streams
- Amazon Nimble Studio

Migrazione e trasferimento:

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service (AWS DMS)
- Sistema di valutazione della migrazione
- AWS Migration Hub
- AWS Transfer Family

Tecnologie quantistiche:

- Amazon Braket

Robotica:

- AWS RoboMaker

Comunicazioni satellitari:

- AWS Ground Station

Sondaggio

Quanto è stata utile questa guida all'esame? Per farci sapere cosa ne pensi, partecipa al sondaggio