

AWS Certified Security – Specialty

SCS-C03 – Segurança Avançada em Nuvem AWS. Hands On.

AWS CERTIFIED SECURITY - SPECIALTY

SOBRE O CURSO:

Na nuvem, um único bucket exposto ou uma política de acesso permissiva demais pode custar a reputação de uma empresa inteira. Por isso, o profissional que domina segurança em nuvem é hoje um dos mais disputados do mercado de tecnologia.

A certificação AWS Certified Security – Specialty valida a capacidade de proteger produtos e serviços AWS: detecção de ameaças, resposta a incidentes, segurança de infraestrutura, gerenciamento de identidades e acessos, proteção de dados e governança em escala. A versão atual do exame, SCS-C03, está em vigor desde 2 de dezembro de 2025 e incorporou temas como Security Lake, AWS Control Tower, políticas declarativas e proteção de aplicações de IA generativa.

O treinamento foi desenvolvido com base no guia oficial do exame SCS-C03, cobrindo seus seis domínios: Detecção; Resposta a Incidentes; Segurança de Infraestrutura; Gerenciamento de Identidades e Acessos; Proteção de Dados; e Fundamentos de Segurança e Governança.

O Grupo Utah criou este treinamento utilizando uma metodologia onde o aluno não apenas irá adquirir conhecimento técnico, mas também competências comportamentais que irão apoiá-lo em todo o seu processo de desenvolvimento de carreira. A metodologia DILDIP proporciona isso porque é baseada no modelo 70/20/10.

SOBRE A CERTIFICAÇÃO:

- ✓ **Exame:** AWS Certified Security – Specialty (SCS-C03)
- ✓ **Formato:** 65 questões (50 pontuadas e 15 não pontuadas): múltipla escolha, múltipla resposta, ordenação e associação
- ✓ **Duração:** 170 minutos
- ✓ **Aprovação:** Pontuação escalonada de 100 a 1.000, mínimo de 750
- ✓ **Aplicação:** Centro de testes Pearson VUE ou online com supervisão remota
- ✓ **Domínios:** Detecção (16%), Resposta a Incidentes (14%), Segurança de Infraestrutura (18%), Identidades e Acessos (20%), Proteção de Dados (18%), Fundamentos de Segurança e Governança (14%)

CARGA HORÁRIA:

- ✓ **48 Horas**

APÓS ESTE CURSO VOCÊ ESTARÁ APTO A:

- ✓ Projetar soluções de monitoramento, alertas e logs de segurança em contas e organizações AWS.
- ✓ Construir data lakes de segurança com Amazon Security Lake e integrar ferramentas de terceiros.
- ✓ Elaborar, testar e automatizar planos de resposta a incidentes e análise forense.
- ✓ Proteger serviços de borda com AWS WAF, AWS Shield Advanced e Amazon CloudFront.
- ✓ Proteger cargas de trabalho de computação, contêineres, pipelines e aplicações de IA generativa.
- ✓ Projetar controles de segurança de rede, segmentação e conectividade híbrida segura.
- ✓ Implementar estratégias de autenticação e autorização (RBAC e ABAC) com menor privilégio.

@grupoutah 11-9.6939-1515 11-9.6040-1515 utah.com.br

- ✓ Proteger dados em trânsito e em repouso com AWS KMS, AWS CloudHSM e AWS Private CA.
- ✓ Gerenciar segredos, chaves e certificados em uma ou várias Regiões.
- ✓ Governar ambientes com AWS Organizations, AWS Control Tower, SCPs e RCPs.
- ✓ Avaliar a conformidade de recursos e coletar evidências para auditorias.
- ✓ Prestar o exame de certificação AWS Certified Security – Specialty (SCS-C03).

PRÉ-REQUISITOS:

- ✓ Conhecimento em Redes de Computadores, Linux e fundamentos de Segurança da Informação.
- ✓ Recomendado: AWS Certified Solutions Architect – Associate ou AWS Certified SysOps Administrator (CloudOps Engineer) – Associate.
- ✓ Recomendado pela AWS: experiência equivalente de 3 a 5 anos protegendo soluções em nuvem.

POR QUE A UTAH:

- ✓ Aulas gravadas e disponibilizadas para acesso na central do aluno durante 3 meses após o treinamento.
- ✓ Simulados baseados na prova oficial AWS SCS-C03.
- ✓ Descontos e parcelamentos na prova de certificação.
- ✓ Laboratórios práticos (Hands On) em ambiente real, com cenários do dia a dia corporativo.
- ✓ Aqui você terá o desenvolvimento de uma carreira, não apenas um treinamento.
- ✓ Pioneira em Treinamentos Linux / Software Livre no Brasil, com 26 anos de mercado.
- ✓ Material Didático Impresso.
- ✓ Técnicas de Coaching utilizadas para desenvolvimento de comportamentos (metodologia DILDIP, modelo 70/20/10).
- ✓ Grupos exclusivos no WhatsApp / Telegram para tirar dúvidas.
- ✓ Encaminhamento de Profissionais para empresas parceiras.
- ✓ Certificado Utah reconhecido pelo mercado de trabalho.
- ✓ Possibilidade de reposição de aula presencial.
- ✓ E muito mais.

EMENTA:

DOMÍNIO 1 – DETECÇÃO (16%)

- **1.1 – Projetar e implementar soluções de monitoramento e alertas para uma conta ou organização AWS.**
  - Analisar cargas de trabalho para determinar requisitos de monitoramento.
  - Projetar estratégias de monitoramento de cargas de trabalho (health checks de recursos).
  - Agregar eventos de segurança e de monitoramento.
  - Criar métricas, alertas e dashboards para detectar anomalias: Amazon GuardDuty, Amazon Security Lake, AWS Security Hub e Amazon Macie.
  - Automatizar avaliações e investigações periódicas: AWS Config conformance packs, Security Hub e Systems Manager State Manager.

@grupoutah 11-9.6939-1515 11-9.6040-1515 utah.com.br

- **1.2 – Projetar e implementar soluções de logs.**
  - Identificar fontes de ingestão e armazenamento de logs conforme requisitos.
  - Configurar logs de serviços e aplicações: trilha organizacional do AWS CloudTrail, conta dedicada de logs do CloudWatch e agente do CloudWatch Logs.
  - Implementar armazenamento de logs e data lakes (Security Lake) e integrar ferramentas de segurança de terceiros.
  - Analisar logs com CloudWatch Logs Insights, Amazon Athena e achados do Security Hub.
  - Normalizar, interpretar e correlacionar logs com Amazon OpenSearch Service, AWS Lambda e Amazon Managed Grafana.
  - Configurar fontes de logs conforme o desenho de rede e as ameaças: VPC Flow Logs, transit gateway flow logs e logs do Route 53 Resolver.
- **1.3 – Solucionar problemas de monitoramento, logs e alertas de segurança.**
  - Analisar funcionalidade, permissões e configuração de recursos: logs de Lambda, Amazon API Gateway, health checks e Amazon CloudFront.
  - Remediar configurações incorretas: agente do CloudWatch e logs ausentes.

DOMÍNIO 2 – RESPOSTA A INCIDENTES (14%)

- **2.1 – Projetar e testar um plano de resposta a incidentes.**
  - Elaborar planos e runbooks de resposta a incidentes (Systems Manager OpsCenter e notebooks do Amazon SageMaker AI).
  - Preparar serviços para incidentes: provisionamento de acesso, ferramentas de segurança, redução do raio de impacto (blast radius) e proteções do AWS Shield Advanced.
  - Testar e validar a efetividade do plano com AWS Fault Injection Service e AWS Resilience Hub.
  - Remediar incidentes automaticamente com Systems Manager, Automated Forensics Orchestrator for Amazon EC2, AWS Step Functions, Amazon Application Recovery Controller e funções Lambda.
- **2.2 – Responder a eventos de segurança.**
  - Capturar e armazenar logs de sistema e aplicação como artefatos forenses.
  - Pesquisar e correlacionar logs de eventos de segurança entre aplicações e serviços AWS.
  - Validar achados dos serviços de segurança para avaliar escopo e impacto.
  - Conter e erradicar ameaças e recuperar recursos (contenção de rede e restauração de backups).
  - Métodos de análise de causa raiz com Amazon Detective.

DOMÍNIO 3 – SEGURANÇA DE INFRAESTRUTURA (18%)

- **3.1 – Projetar, implementar e solucionar problemas de controles de segurança para serviços de borda.**
  - Definir estratégias de segurança de borda com base em ameaças e ataques previstos.
  - Implementar proteção de borda: cabeçalhos do CloudFront, AWS WAF, políticas do AWS IoT, OWASP Top 10, CORS no Amazon S3 e Shield Advanced.
  - Criar regras por geografia, geolocalização, limitação de taxa (rate limiting) e fingerprinting de clientes.

@grupoutah 11-9.6939-1515 11-9.6040-1515 utah.com.br

- Integrar serviços de borda com terceiros (formato OCSF e regras de WAF de terceiros).

- **3.2 – Projetar, implementar e solucionar problemas de controles de segurança para cargas de computação.**
  - Criar AMIs e imagens de contêiner endurecidas (hardening) com Systems Manager e EC2 Image Builder.
  - Aplicar instance profiles, service roles e execution roles.
  - Varrer vulnerabilidades de imagens de contêiner e funções Lambda com Amazon Inspector; monitorar runtime com GuardDuty.
  - Automatizar a aplicação de patches com Systems Manager Patch Manager e validação contínua.
  - Configurar acesso administrativo seguro com Session Manager e EC2 Instance Connect.
  - Descobrir e remediar vulnerabilidades no pipeline com Amazon Q Developer e Amazon CodeGuru Security.
  - Implementar proteções e guardrails para aplicações de IA generativa (OWASP Top 10 for LLM Applications).

- **3.3 – Projetar e solucionar problemas de controles de segurança de rede.**
  - Permitir ou bloquear tráfego com security groups, ACLs de rede e AWS Network Firewall.
  - Conectividade segura entre redes híbridas e multicloud: Site-to-Site VPN, Direct Connect e MACsec.
  - Requisitos de comunicação entre ambientes híbridos e AWS com AWS Verified Access.
  - Segmentação de rede: proteção de tráfego norte/sul e leste/oeste e sub-redes isoladas.
  - Identificar acessos de rede desnecessários com Network Access Analyzer e achados de alcançabilidade do Amazon Inspector.

DOMÍNIO 4 – GERENCIAMENTO DE IDENTIDADES E ACESSOS (20%)

- **4.1 – Projetar, implementar e solucionar problemas de estratégias de autenticação.**
  - Soluções de identidade para pessoas, aplicações e sistemas: AWS IAM Identity Center, Amazon Cognito, MFA e integração com provedores de identidade (IdP).
  - Emissão de credenciais temporárias com AWS STS e URLs pré-assinadas do Amazon S3.
  - Solução de problemas de autenticação com CloudTrail, Cognito, permission sets do IAM Identity Center e AWS Directory Service.

- **4.2 – Projetar, implementar e solucionar problemas de estratégias de autorização.**
  - Controles de autorização: Amazon Verified Permissions, IAM paths, IAM Roles Anywhere, políticas de recurso entre contas e trust policies.
  - Estratégias ABAC e RBAC baseadas em tags e atributos.
  - Políticas IAM com menor privilégio: permission boundaries e session policies.
  - Análise de falhas de autorização com IAM Policy Simulator e IAM Access Analyzer.
  - Investigar e corrigir permissões não intencionais com IAM Access Analyzer.

@grupoutah 11-9.6939-1515 11-9.6040-1515 utah.com.br

DOMÍNIO 5 – PROTEÇÃO DE DADOS (18%)

- **5.1 – Projetar e implementar controles para dados em trânsito.**
  - Exigir criptografia nas conexões: políticas de segurança do ELB e configurações de TLS.
  - Acesso privado e seguro a recursos: AWS PrivateLink, VPC endpoints, AWS Client VPN e AWS Verified Access.
  - Criptografia em trânsito entre recursos: Amazon EMR, Amazon EKS, SageMaker AI e criptografia Nitro.
- **5.2 – Projetar e implementar controles para dados em repouso.**
  - Escolher o serviço de chaves (AWS KMS ou AWS CloudHSM) e o tipo de criptografia (client-side ou server-side).
  - Proteger a integridade dos dados: S3 Object Lock, S3 Glacier Vault Lock, versionamento, assinatura de código e validação de arquivos.
  - Ciclo de vida e retenção: políticas do S3 Lifecycle, Object Lock, EFS Lifecycle e backups do FSx for Lustre.
  - Replicação e backup seguros: Amazon Data Lifecycle Manager, AWS Backup, proteção contra ransomware e AWS DataSync.
- **5.3 – Proteger dados confidenciais, credenciais, segredos e material criptográfico.**
  - Gerenciamento e rotação de credenciais e segredos com AWS Secrets Manager.
  - Gerenciar e rotacionar material de chave importado; configurar external key stores.
  - Diferenças entre material de chave importado e gerado pela AWS.
  - Mascarar dados sensíveis: políticas de proteção de dados do CloudWatch Logs e do Amazon SNS.
  - Criar e gerenciar chaves e certificados em uma ou várias Regiões: chaves gerenciadas pelo cliente no AWS KMS e AWS Private Certificate Authority.

DOMÍNIO 6 – FUNDAMENTOS DE SEGURANÇA E GOVERNANÇA (14%)

- **6.1 – Desenvolver uma estratégia para implantar e gerenciar contas AWS de forma centralizada.**
  - Implantar e configurar organizações com AWS Organizations.
  - Implementar AWS Control Tower em ambientes novos e existentes, com controles opcionais e personalizados.
  - Políticas organizacionais: SCPs, RCPs, políticas de opt-out de serviços de IA e políticas declarativas.
  - Gerenciar serviços de segurança de forma centralizada (contas de administrador delegado).
  - Gerenciar credenciais do usuário raiz: centralização do acesso root, MFA e procedimentos de break-glass.
- **6.2 – Implementar uma estratégia de implantação segura e consistente.**
  - Infraestrutura como código entre contas: CloudFormation StackSets, ferramentas de IaC de terceiros, CloudFormation Guard e cfn-lint.
  - Uso de tags para organizar recursos (departamento, centro de custo, ambiente).
  - Aplicar políticas a partir de uma fonte central com AWS Firewall Manager.
  - Compartilhar recursos com segurança: AWS Service Catalog e AWS RAM.

@grupoutah 11-9.6939-1515 11-9.6040-1515 utah.com.br

- **6.3 – Avaliar a conformidade dos recursos AWS.**
  - Regras para detectar e remediar recursos não conformes com AWS Config e Security Hub.
  - Coletar evidências de auditoria com AWS Audit Manager e AWS Artifact.
  - Avaliar a arquitetura frente às melhores práticas com a ferramenta AWS Well-Architected.

FORMAS DE PAGAMENTO:

CARTÃO DE CRÉDITO: Em até **12X** sem juros.
BOLETO: Em até **12X** sem juros ou **24X** com juros de **1.8% a.m.**

Atenciosamente,

PALOMA MORAES
Sales Trainning – Grupo Utah
55 11 96931-1515
paloma@utah.com.br
www.utah.com.br