

UTAH TREINAMENTOS

SY0-801 (V8) – Fundamentos de Cibersegurança. Hands On.

COMPTIA SECURITY+

SOBRE O CURSO:

Não existe empresa sem dados, e não existe dado sem risco. Ataques de ransomware, engenharia social, vazamentos e agora ameaças potencializadas por Inteligência Artificial fazem parte do dia a dia das organizações. Quem entende de segurança deixa de ser apenas um técnico e passa a ser um protetor do negócio.

A CompTIA Security+ é a certificação de cibersegurança de nível inicial mais reconhecida do mundo, acreditada pela ISO 17024 e adotada como referência por governos e grandes corporações. Ela comprova as competências práticas necessárias para avaliar a postura de segurança de uma empresa, proteger ambientes híbridos e em nuvem, monitorar, responder a incidentes e atuar com governança, risco e conformidade.

O treinamento foi desenvolvido com base nos objetivos oficiais do exame SY0-801 (Security+ V8), lançado em 17 de novembro de 2026, cobrindo seus cinco domínios: Conceitos Gerais de Segurança; Ameaças, Vulnerabilidades e Ataques; Arquitetura de Segurança; Operações de Segurança; e Gestão e Supervisão do Programa de Segurança. A versão anterior (SY0-701) permanece disponível em inglês até 11 de junho de 2027.

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:** CompTIA Security+ V8 (SY0-801)
- ✓ **Formato:** Até 90 questões de múltipla escolha e baseadas em desempenho (performance-based)
- ✓ **Duração:** 90 minutos
- ✓ **Aprovação:** 750 em uma escala de 100 a 900
- ✓ **Experiência recomendada:** Administrador de segurança com 2 anos de experiência prática
- ✓ **Domínios:** Conceitos Gerais (16%), Ameaças, Vulnerabilidades e Ataques (24%), Arquitetura de Segurança (19%), Operações de Segurança (27%), Gestão e Supervisão do Programa de Segurança (14%)

CARGA HORÁRIA:

- ✓ **40 Horas**

APÓS ESTE CURSO VOCÊ ESTARÁ APTO A:

- ✓ Comparar tipos de controles de segurança e aplicar os conceitos da tríade CIA, AAA e Zero Trust.
- ✓ Utilizar soluções criptográficas adequadas (PKI, certificados, hashing, assinatura digital).
- ✓ Identificar agentes de ameaças, vetores de ataque e indicadores de atividade maliciosa.
- ✓ Avaliar riscos de segurança relacionados à Inteligência Artificial.
- ✓ Aplicar princípios de segurança em arquiteturas on-premises, em nuvem, híbridas e com contêineres.
- ✓ Proteger dados e projetar ambientes resilientes, com backup e recuperação.

- ✓ Aplicar hardening em recursos computacionais e gerenciar ativos e vulnerabilidades.
- ✓ Monitorar, gerar alertas e utilizar automação e orquestração em operações de segurança.
- ✓ Gerenciar identidades e acessos (MFA, SSO, federação, PAM).
- ✓ Conduzir atividades de resposta a incidentes e investigações.
- ✓ Atuar em governança, gestão de riscos, riscos de terceiros, conformidade e privacidade.
- ✓ Prestar o exame de certificação CompTIA Security+ (SY0-801).

PRÉ-REQUISITOS:

- ✓ Conhecimento em Redes de Computadores (recomendado CompTIA Network+ ou equivalente).
- ✓ Conhecimento básico em administração de sistemas Linux e Windows.

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 CompTIA Security+.
- ✓ 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 – CONCEITOS GERAIS DE SEGURANÇA (16%)

- **1.1 – Comparar e contrastar os tipos de controles de segurança.**
  - Categorias de controles: técnicos, gerenciais, operacionais e físicos.
  - Tipos de controles: preventivo, dissuasivo, detectivo, corretivo, compensatório e diretivo.
  - Conceitos fundamentais: confidencialidade, integridade e disponibilidade (CIA), não repúdio e AAA.
  - Análise de lacunas (gap analysis) e modelo Zero Trust (plano de controle e plano de dados).
  - Segurança física: barreiras, vigilância, controle de acesso e sensores.
  - Tecnologias de engano e disrupção: honeypots, honeynets, honeyfiles e honeytokens.

- **1.2 – Avaliar como a gestão de mudanças afeta a segurança.**
  - Processos de negócio: aprovação, responsáveis, partes interessadas, análise de impacto, plano de rollback e janelas de manutenção.
  - Implicações técnicas: listas de permissão e bloqueio, reinicializações, dependências e aplicações legadas.
  - Documentação e controle de versões.
- **1.3 – Utilizar soluções criptográficas apropriadas.**
  - Infraestrutura de chaves públicas (PKI), chaves públicas e privadas e custódia de chaves (key escrow).
  - Criptografia de disco, partição, arquivo, volume, banco de dados, registro, transporte e criptografia simétrica x assimétrica.
  - Ferramentas: TPM, HSM, KMS e secure enclave.
  - Ofuscação: esteganografia, tokenização e mascaramento de dados.
  - Hashing, salting, assinaturas digitais, alongamento de chaves e blockchain.
  - Certificados digitais: autoridades certificadoras, CRL, OCSP, certificados autoassinados, curinga (wildcard) e CSR.
  - Criptografia pós-quântica.

DOMÍNIO 2 – AMEAÇAS, VULNERABILIDADES E ATAQUES (24%)

- **2.1 – Identificar os agentes de ameaças e suas motivações.**
  - Agentes: estados-nação, atacantes não qualificados, hacktivistas, ameaças internas, crime organizado e shadow IT.
  - Atributos: interno x externo, recursos e financiamento, nível de sofisticação.
  - Motivações: exfiltração de dados, espionagem, interrupção de serviços, chantagem, ganho financeiro, crenças filosóficas e políticas e guerra cibernética.
- **2.2 – Explicar vetores de ameaças e superfícies de ataque.**
  - Vetores baseados em mensagens, imagens, arquivos, voz, mídias removíveis e softwares vulneráveis.
  - Redes sem fio, cabeadas e Bluetooth; portas abertas e credenciais padrão.
  - Cadeia de suprimentos: provedores de serviços gerenciados, fornecedores e terceiros.
  - Engenharia social: phishing, vishing, smishing, desinformação, pretexting, comprometimento de e-mail corporativo (BEC), watering hole e typosquatting.
- **2.3 – Analisar indicadores de atividade maliciosa.**
  - Ataques de malware: ransomware, trojan, worm, spyware, rootkit, keylogger, bloatware, vírus e logic bomb.
  - Ataques físicos: força bruta, clonagem de RFID e ataques ambientais.
  - Ataques de rede: DDoS (amplificação e reflexão), ataques a DNS, ataques a redes sem fio, on-path, replay de credenciais e malware code.
  - Ataques a aplicações: injeção, estouro de buffer, replay, escalonamento de privilégios, falsificação de requisições e directory traversal.
  - Ataques criptográficos: downgrade, colisão e birthday.

- Ataques a senhas: spraying e força bruta.
- Indicadores: bloqueio de contas, viagens impossíveis, consumo de recursos, logs ausentes e atividades fora do horário.

- **2.4 – Examinar vulnerabilidades comuns e seus riscos.**
  - Vulnerabilidades de aplicações: vazamento de memória, estouro de buffer, race conditions (TOC/TOU) e atualizações maliciosas.
  - Vulnerabilidades de sistemas operacionais, web (SQLi e XSS), hardware (firmware, fim de vida, legado) e virtualização (VM escape).
  - Vulnerabilidades específicas de nuvem, da cadeia de suprimentos e criptográficas.
  - Configurações incorretas, dispositivos móveis (sideloading e jailbreaking) e ataques de dia zero.

- **2.5 – Explicar os riscos de segurança relacionados à Inteligência Artificial.**
  - Uso de IA por atacantes: phishing automatizado, deepfakes e geração de malware.
  - Ataques contra sistemas de IA: prompt injection, envenenamento de dados de treinamento e extração de modelos.
  - Vazamento de dados sensíveis em ferramentas de IA e shadow AI.
  - Controles e políticas de uso seguro de IA nas organizações.

DOMÍNIO 3 – ARQUITETURA DE SEGURANÇA (19%)

- **3.1 – Comparar as implicações de segurança dos modelos de arquitetura.**
  - Nuvem: modelo de responsabilidade compartilhada, nuvem híbrida e terceiros.
  - Infraestrutura como Código, serverless, microsserviços e contêineres.
  - Infraestrutura de rede: isolamento físico (air-gapped), segmentação lógica e SDN.
  - On-premises, centralizado x descentralizado, virtualização, IoT, ICS/SCADA, RTOS e sistemas embarcados.
  - Considerações: disponibilidade, resiliência, custo, capacidade de resposta, escalabilidade e facilidade de recuperação.

- **3.2 – Aplicar princípios de segurança à infraestrutura corporativa.**
  - Considerações de infraestrutura: posicionamento de dispositivos, zonas de segurança, superfície de ataque e conectividade.
  - Modos de falha (fail-open e fail-closed), dispositivos ativos x passivos, inline x tap/monitor.
  - Dispositivos: jump server, proxy, IPS/IDS, balanceador de carga, sensores, firewalls (WAF, UTM, NGFW, camada 4/7).
  - Acesso seguro: VPN, acesso remoto, túneis (TLS e IPSec), SD-WAN e SASE.
  - Seleção de controles efetivos.

- **3.3 – Compreender os conceitos de proteção de dados.**
  - Tipos de dados: regulados, segredos comerciais, propriedade intelectual, dados legais e financeiros.
  - Classificação de dados: sensível, confidencial, público, restrito, privado e crítico.
  - Estados dos dados: em repouso, em trânsito e em uso; soberania de dados e geolocalização.

- Métodos de proteção: restrições geográficas, criptografia, hashing, mascaramento, tokenização, ofuscação, segmentação e restrições de permissão.

- **3.4 – Explicar resiliência e recuperação em arquiteturas de segurança.**
  - Alta disponibilidade: balanceamento de carga x clustering.
  - Considerações de site: hot, cold e warm sites; dispersão geográfica.
  - Diversidade de plataformas, cenários multicloud e continuidade de operações.
  - Planejamento de capacidade: pessoas, tecnologia e infraestrutura.
  - Testes: exercícios de mesa (tabletop), failover, simulações e testes paralelos.
  - Backups: onsite/offsite, frequência, criptografia, snapshots, replicação e journaling.
  - Energia: geradores e UPS.

DOMÍNIO 4 – OPERAÇÕES DE SEGURANÇA (27%)

- **4.1 – Aplicar técnicas de segurança comuns a recursos computacionais.**
  - Baselines seguras: estabelecer, implantar e manter.
  - Hardening de dispositivos móveis, estações, switches, roteadores, nuvem, servidores, ICS/SCADA, sistemas embarcados e IoT.
  - Instalação e segurança de redes sem fio: site survey, WPA3, AAA/RADIUS e protocolos de autenticação.
  - Soluções móveis: MDM, BYOD, COPE e CYOD.
  - Segurança de aplicações: validação de entradas, cookies seguros, análise estática e assinatura de código.
  - Sandboxing e monitoramento.

- **4.2 – Explicar os conceitos de gestão de ativos.**
  - Aquisição e compras, atribuição e responsabilidade (ownership) e classificação.
  - Monitoramento e rastreamento de ativos: inventário e enumeração.
  - Descarte e desativação: sanitização, destruição, certificação e retenção de dados.

- **4.3 – Analisar indicadores de vulnerabilidade e estratégias de mitigação.**
  - Métodos de identificação: varredura de vulnerabilidades, análise de aplicações, threat feeds (OSINT), testes de penetração e programas de bug bounty.
  - Análise: confirmação (falsos positivos e falsos negativos), priorização, CVSS, CVE, classificação, exposição e tolerância a riscos.
  - Remediação: patching, seguro, segmentação, controles compensatórios e exceções.
  - Validação da remediação: nova varredura, auditoria e verificação; relatórios.

- **4.4 – Descrever monitoramento e alertas de segurança.**
  - Recursos monitorados: sistemas, aplicações e infraestrutura.
  - Atividades: agregação de logs, alertas, varredura, relatórios, arquivamento e resposta a alertas.
  - Ferramentas: SCAP, benchmarks, agentes, SIEM, antivírus, DLP, SNMP traps, NetFlow e scanners de vulnerabilidades.

- **4.5 – Gerenciar controles de identidade e acesso.**
  - Provisionamento e desprovisionamento de contas, prova de identidade e federação.
  - Single sign-on (SSO): LDAP, OAuth e SAML; interoperabilidade e atestação.
  - Modelos de controle de acesso: obrigatório (MAC), discricionário (DAC), baseado em funções (RBAC), em regras, em atributos (ABAC) e por tempo.
  - Autenticação multifator: biometria, tokens de hardware e software, chaves de segurança e passkeys.
  - Senhas: boas práticas, gerenciadores de senhas e autenticação sem senha (passwordless).
  - Gerenciamento de acesso privilegiado (PAM): permissões just-in-time, cofres de senha e credenciais efêmeras.

- **4.6 – Explicar automação e orquestração em operações de segurança.**
  - Casos de uso: provisionamento de usuários e recursos, guardrails, grupos de segurança, criação de tickets, escalonamento e integrações via API.
  - Benefícios: eficiência, aplicação de baselines, reação rápida e alívio da carga das equipes.
  - Considerações: complexidade, custo, ponto único de falha, dívida técnica e suporte contínuo.
  - Uso de IA e SOAR na automação de segurança.

- **4.7 – Implementar atividades de resposta a incidentes.**
  - Processo: preparação, detecção, análise, contenção, erradicação, recuperação e lições aprendidas.
  - Treinamento e testes: exercícios de mesa e simulações.
  - Análise de causa raiz e threat hunting.
  - Forense digital: retenção legal (legal hold), cadeia de custódia, aquisição, relatórios, preservação e e-discovery.

- **4.8 – Utilizar fontes de dados para apoiar investigações.**
  - Dados de logs: firewall, aplicação, endpoint, sistema operacional, IPS/IDS, rede e metadados.
  - Fontes de dados: resultados de varreduras de vulnerabilidade, dashboards e capturas de pacotes.

DOMÍNIO 5 – GESTÃO E SUPERVISÃO DO PROGRAMA DE SEGURANÇA (14%)

- **5.1 – Definir os elementos de um programa de governança de segurança.**
  - Diretrizes, políticas (AUP, segurança da informação, continuidade de negócio, recuperação de desastres, resposta a incidentes, SDLC), padrões e procedimentos.
  - Considerações externas: regulatórias, legais, setoriais, locais, nacionais e globais.
  - Monitoramento e revisão; estruturas de governança (conselhos, comitês, entidades governamentais).
  - Papéis e responsabilidades: proprietários, controladores, operadores, custodiantes e responsáveis por dados.

- **5.2 – Gerenciar os processos de gestão de riscos de segurança.**
  - Identificação e avaliação de riscos: ad hoc, recorrente, pontual e contínua.

- Análise de riscos qualitativa e quantitativa: SLE, ALE, ARO, probabilidade, impacto e fator de exposição.
- Registro de riscos, indicadores-chave de risco, apetite e tolerância a riscos.
- Estratégias: transferir, aceitar (isenção e exceção), evitar e mitigar.
- Análise de impacto nos negócios (BIA): RTO, RPO, MTTR e MTBF.

- **5.3 – Explicar a gestão de riscos de terceiros.**
  - Avaliação e seleção de fornecedores: testes de penetração, direito de auditoria, evidências internas e due diligence.
  - Acordos: SLA, MOA, MOU, MSA, WO/SOW, NDA e BPA.
  - Monitoramento de fornecedores, questionários e regras de engajamento.

- **5.4 – Apoiar considerações de conformidade e privacidade.**
  - Relatórios de conformidade internos e externos.
  - Consequências do não cumprimento: multas, sanções, danos à reputação e perda de licença.
  - Monitoramento da conformidade: due diligence, atestação, automação.
  - Privacidade: implicações legais (LGPD, GDPR), titular, controlador x operador, inventário e retenção de dados e direito ao esquecimento.

- **5.5 – Comparar auditorias e avaliações.**
  - Atestação e auditorias internas (conformidade, comitê de auditoria, autoavaliações).
  - Auditorias externas: regulatórias, exames, avaliações e auditorias independentes.
  - Testes de penetração: físico, ofensivo, defensivo, integrado, ambiente conhecido, parcialmente conhecido e desconhecido.
  - Reconhecimento passivo e ativo.

- **5.6 – Promover práticas de conscientização em segurança.**
  - Campanhas de phishing: reconhecimento de tentativas, resposta e comunicação de incidentes.
  - Comportamentos anômalos: arriscados, inesperados e não intencionais.
  - Treinamento de usuários: manuais de políticas, situational awareness, ameaças internas, gestão de senhas, mídias removíveis, engenharia social, segurança operacional e trabalho remoto/híbrido.
  - Relatórios e monitoramento do programa de conscientização; desenvolvimento e execução.

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