Objetivos do Exame de Certificação CompTIA Security+

NÚMERO DO EXAME: SY0-701

Sobre o exame

O exame de certificação CompTIA Security+ certificará se o candidato tem o conhecimento e as habilidades necessárias para:

- Avaliar o perfil de segurança de um ambiente empresarial e recomendar e implementar soluções de segurança adequadas.
- Monitorar e proteger ambientes híbridos, incluindo nuvens, dispositivos móveis e IoT.
- Trabalhar com conhecimento dos regulamentos e políticas aplicáveis, incluindo princípios de governança, risco e conformidade.
- Identificar, analisar e responder a eventos e incidentes de segurança.

ELABORAÇÃO DO EXAME

O resultado dos exames CompTIA é proveniente de workshops especializados e focados no assunto e pesquisas abrangentes em toda a indústria quanto às habilidades e conhecimentos exigidos de um profissional de TI.

POLÍTICA DE USO AUTORIZADO DE MATERIAIS DA CompTIA

A CompTIA Certifications, LLC não está afiliada a, nem autoriza, endossa ou admite o uso de qualquer conteúdo fornecido por sites de treinamento externos não autorizados (também conhecidos como "brain dumps"). Os candidatos que usarem esses materiais como preparação para qualquer exame da CompTIA terão suas certificações anuladas e serão suspensos de futuros testes de acordo com o contrato do candidato CompTIA. Com o intuito de comunicar com maior clareza as políticas dos exames CompTIA referentes ao uso de materiais de estudo não autorizados, a CompTIA encaminha todos os candidatos à certificação para as Políticas do Exame de Certificação da CompTIA. Leia todas as políticas da CompTIA antes de iniciar o processo de estudo para qualquer exame CompTIA. Os candidatos serão obrigados a respeitar o Contrato do Candidato da CompTIA. Se um candidato não tiver certeza se determinado material de estudo é considerado não autorizado (conhecido como "brain dump"), deverá entrar em contato com a CompTIA pelo e-mail examsecurity@comptia.org para confirmação.

OBSERVAÇÃO

As listas de exemplos fornecidas em formato de marcadores não são listas abrangentes. Outros exemplos de tecnologias, processos ou tarefas pertinentes a cada objetivo podem ser incluídos no exame, embora não estejam listados ou cobertos neste documento de objetivos. A CompTIA revisa constantemente o conteúdo de seus exames e atualiza as questões para assegurar que sejam atuais e que a segurança de suas perguntas estejam protegidas. Quando necessário, publicaremos exames atualizados baseados nos objetivos existentes. Lembre-se que todos os materiais de preparação dos exames ainda serão válidos.

DETALHES DO TESTE

Exame exigido	SY0-701
Número de questões	No máximo 90
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	90 minutos
Experiência recomendada	Um mínimo de 2 anos de experiência em administração de TI com foco em segurança, experiência prática com segurança técnica da informação e amplo conhecimento de conceitos de segurança

OBJETIVOS DO EXAME (DOMÍNIOS)

A tabela abaixo lista os domínios medidos por este exame e o peso que cada um representa.

DOMÍNIO		PORCENTAGEM DO EXAME
1.0	Conceitos gerais de segurança	12%
2.0	Ameaças, vulnerabilidades e mitigações	22%
3.0	Arquitetura de segurança	18%
4.0	Operações de segurança	28%
5.0	Gerenciamento e supervisão do programa de segurança	20%
Total		**100%**

1.0 Conceitos gerais de segurança

1.1 Comparar e diferenciar vários tipos de controles de segurança.

- **Categorias**
  - Técnico
  - Gerencial
  - Operacional
  - Físico
- **Tipos de controles**
  - Preventivo
  - Dissuador
  - Detectivo
  - Corretivo
  - Compensatório
  - Diretivo

1.2 Resumir os conceitos fundamentais de segurança.

- **Confidencialidade, integridade, e disponibilidade (CIA)**
- **Não repúdio**
- **Autenticação, Autorização e Auditoria (AAA)**
  - Autenticação de pessoas
  - Autenticação de sistemas
  - Modelos de autorização
- **Análise de lacunas**
- **Confiança zero**
  - Plano de controle
    - Identidade adaptativa
    - Redução do escopo da ameaça
    - Controle de acesso orientado por políticas
    - Administrador de políticas
    - Mecanismo de política
  - Plano de dados
    - Zonas de confiança implícitas
    - Assunto/Sistema
    - Ponto de aplicação de políticas
- **Segurança física**
  - Barreiras
  - Entrada de controle de acesso
  - Cercas
  - Vigilância de vídeo
  - Proteções de segurança
  - Crachá de acesso
  - Iluminação
  - Sensores
    - Infravermelho
    - Pressão
    - Microondas
    - Ultrassônico
- **Tecnologia de engano e interrupção**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

1.3 Explicar a importância dos processos de gestão de mudanças e o impacto na segurança.

- **Processos de negócios que impactam a operação de segurança**
  - Processo de aprovação
  - Propriedade
  - Partes interessadas
  - Análise de impacto
  - Resultado dos testes
  - Plano de remediação
  - Janelas de manutenção
  - Procedimentos operacionais padrão
- **Implicações técnicas**
  - Listas de permissão/listas de negação
  - Atividades restritas
  - Tempo de inatividade
  - Reinicialização do serviço
  - Reinicialização do aplicativo
  - Aplicativos legados
  - Dependências
- **Documentação**
  - Atualização de diagramas
  - Atualização de políticas/procedimentos
- **Controle de versões**

1.4 Explicar a importância de usar soluções criptográficas apropriadas.

- **Infraestrutura de chave pública (PKI)**
  - Chave pública
  - Chave privada
  - Key escrow
- **Criptografia**
  - Nível
    - Disco completo
    - Partição
    - Arquivo
    - Volume
    - Banco de dados
    - Registro
  - Transporte/comunicação
  - Assimétrico
  - Simétrico
  - Troca de chave
  - Algoritmos
  - Tamanho de chave
- **Ferramentas**
  - Módulo de plataforma confiável (TPM)
  - Módulo de segurança de hardware (HSM)
  - Sistema de gerenciamento de chaves
  - Enclave seguro
- **Ofuscação**
  - Esteganografia
  - Tokenização
  - Mascaramento de dados
- **Hashing**
- **Salting**
- **Assinaturas digitais**
- **Key stretching**
- **Blockchain**
- **Livro razão público**
- **Certificados**
  - Autoridades certificadoras
  - Lista de revogação de certificados (CRLs)
  - Online Certificate Status Protocol (OCSP)
  - Autoassinado
  - Terceiros
  - Raiz de confiança
  - Geração de Solicitação de assinatura de certificado (CSR)
  - Wildcard

2.0 Ameaças, vulnerabilidades e mitigações

2.1 Comparar e contrastar motivações e agentes de ameaças comuns.

- **Atores de ameaças**
  - Estado-nação
  - Invasor não qualificado
  - Hacktivista
  - Ameaça interna
  - Crime organizado
  - Shadow IT
- **Atributos dos agentes**
  - Interno/externo
  - Recursos/financiamento
  - Nível de sofisticação/capacidade
- **Motivações**
  - Exfiltração de dados
  - Espionagem
  - Interrupção do serviço
  - Chantagem
  - Ganhos financeiros
  - Crenças filosóficas/políticas
  - Ética
  - Vingança
  - Perturbação/caos
  - Guerra

2.2 Explicar vetores de ameaças comuns e superfícies de ataque.

- **Baseado em mensagens**
  - E-mail
  - Serviço de mensagens curtas (SMS)
  - Mensagens instantâneas (IM)
- **Baseado em imagem**
- **Baseado em arquivo**
- **Chamada de voz**
- **Dispositivo removível**
- **Software vulnerável**
  - Baseado no cliente vs. sem agente
- **Sistemas e aplicativos não suportados**
- **Redes inseguras**
  - Sem fio
  - Com fio
  - Bluetooth
- **Portas de serviço abertas**
- **Credenciais padrão**
- **Cadeia de suprimento**
  - Provedores de serviços gerenciados (MSPs)
  - Vendedores
  - Fornecedores
- **Vetores humanos/ engenharia social**
  - Phishing
  - Vishing
  - Smishing
  - Informação errada/ desinformação
  - Personificação
  - Comprometimento de e-mail comercial
  - Pretexting
  - Watering hole
  - Personificação da marca
  - Typosquatting

CompTIA

2.3 Explicar vários tipos de vulnerabilidades.

- **Aplicação**
  - Injeção de memória
  - Buffer overflow
  - Condições de corrida
    - Tempo de verificação (TOC)
    - Tempo de uso (TOU)
  - Atualização maliciosa
- **Baseado no Sistema operacional (SO)**
- **Baseado na web**
  - Injeção de linguagem de consulta estruturada (SQLi)
  - Cross-site scripting (XSS)
- **Hardware**
  - Firmware
  - Fim da vida útil
  - Legado
- **Virtualização**
  - Escape de máquina virtual (VM)
  - Reutilização de recursos
- **Específico para nuvem**
- **Cadeia de suprimento**
  - Provedor de serviços
  - Fornecedor de hardware
  - Fornecedor de software
- **Criptográfico**
- **Configuração incorreta**
- **Dispositivo móvel**
  - Sideloading
  - Jailbreaking
- **Dia zero**

2.4 Considerando determinado cenário, analisar os indicadores de atividade maliciosa.

- **Ataques de malware**
  - Ransomware
  - Trojan
  - Worm
  - Spyware
  - Bloatware
  - Vírus
  - Keylogger
  - Bomba lógica
  - Rootkit
- **Ataques físicos**
  - Força bruta
  - Clonagem de identificação por radiofrequência (RFID)
  - Ambiental
- **Ataques de rede**
  - Negação de serviço distribuído (DDoS)
    - Amplificado
    - Refletido
  - Ataques ao Sistema de nomes de domínio (DNS)
  - Sem fio
  - On-path
  - Repetição de credenciais
  - Código malicioso
- **Ataques de aplicativos**
  - Injeção
  - Buffer overflow
  - Reprodução
  - Escalação de privilégio
  - Falsificação
  - Travessia de diretórios
- **Ataques criptográficos**
  - Downgrade
  - Colisão
  - Aniversário
- **Ataques a senhas**
  - Spraying
  - Força bruta
- **Indicadores**
  - Bloqueio de conta
  - Uso de sessão simultânea
  - Conteúdo bloqueado
  - Viagem impossível
  - Consumo de recursos
  - Inacessibilidade de recursos
  - Registro fora do ciclo
  - Publicado/documentado
  - Logs ausentes

2.5 Explicar o propósito das técnicas de mitigação para proteger a empresa.

- **Segmentação**
- **Controle de acesso**
  - Lista de controle de acesso (ACL)
  - Permissões
- **Lista de aplicações permitidas**
- **Isolamento**
- **Patching**
- **Criptografia**
- **Monitoramento**
- **Privilégio mínimo**
- **Aplicação de configuração**
- **Descomissionamento**
- **Técnicas de hardening**
  - Criptografia
  - Instalação de proteção de endpoint
  - Firewall baseado em host
  - Sistema de prevenção de intrusões baseado em host (HIPS)
  - Desativação de portas/ protocolos
  - Alterações de senha padrão
  - Remoção de software desnecessário

3.0 Arquitetura de segurança

3.1 Comparar e contrastar as implicações de segurança de diferentes modelos de arquitetura.

- **Conceitos de arquitetura e infraestrutura**
  - Nuvem
    - Matriz de responsabilidade
    - Considerações híbridas
    - Fornecedores terceirizados
  - Infraestrutura como código (IaC)
  - Sem servidor
  - Microsserviços
  - Infraestrutura de rede
    - Isolamento físico
      - Air-gapped
    - Segmentação lógica
    - Rede definida por software (SDN)
  - Local
  - Centralizado vs. descentralizado
  - Conteinerização
  - Virtualização
  - IoT
  - Sistemas de controle industrial (ICS)/controle de supervisão e aquisição de dados (SCADA)
  - Sistema operacional de tempo real (RTOS)
  - Sistemas embarcados
  - Alta disponibilidade
- **Considerações**
  - Disponibilidade
  - Resiliência
  - Custo
  - Responsivo
  - Escalabilidade
  - Facilidade de implantação
  - Transferência de risco
  - Facilidade de recuperação
  - Disponibilidade de patches
  - Impossibilidade de fazer patch
  - Alimentação
  - Computação

3.2 Considerando determinado cenário, aplicar princípios de segurança para proteger a infraestrutura empresarial.

- **Considerações sobre infraestrutura**
  - Posicionamento do dispositivo
  - Zonas de segurança
  - Superfície de ataque
  - Conectividade
  - Modos de falha
    - Abertura com falha
    - Fechado com falha
  - Atributo do dispositivo
    - Ativo vs. passivo
    - Em linha vs. tap/monitor
  - Dispositivos de rede
    - Jump servers
    - Servidor proxy
    - Sistema de prevenção de intrusão (IPS)/sistema de detecção de intrusão (IDS)
    - Balanceador de carga
    - Sensores
  - Segurança de porta
    - 802.1X
    - Protocolo de autenticação extensível (EAP)
  - Tipos de firewall
    - Firewall de aplicação Web (WAF)
    - Gerenciamento unificado de ameaças (UTM)
    - Firewall de próxima geração (NGFW)
    - Camada 4/Camada 7
- **Comunicação/acesso seguro**
  - Rede privada virtual (VPN)
  - Acesso remoto
  - Túnel
    - Segurança da camada de transporte (TLS)
    - Internet Protocol security (IPsec)
  - Rede de longa distância definida por software (SD- WAN)
  - Serviço de acesso seguro de borda (SASE)
- **Seleção de controles eficazes**

CompTIA

3.3 Comparar e contrastar conceitos e estratégias para proteger dados.

- **Tipos de dados**
  - Regulados
  - Segredo comercial
  - Propriedade intelectual
  - Informações legais
  - Informações financeiras
  - Legível/Ilegível por humanos
- **Classificação de dados**
  - Sensível
  - Confidencial
  - Público
  - Restrito
  - Privado
  - Crítico
- **Considerações gerais sobre dados**
  - Estados de dados
    - Dados em repouso
    - Dados em trânsito
    - Dados em uso
  - Soberania dos dados
  - Geolocalização
- **Métodos para proteção de dados**
  - Restrições geográficas
  - Criptografia
  - Hashing
  - Mascaramento
  - Tokenização
  - Ofuscação
  - Segmentação
  - Restrições de permissão

3.4 Explicar a importância da resiliência e recuperação na arquitetura de segurança.

- **Alta disponibilidade**
  - Balanceamento de carga vs. clusterização
- **Considerações sobre o local**
  - Hot
  - Cold
  - Warm
  - Dispersão geográfica
- **Diversidade de plataformas**
- **Sistemas multinuvem**
- **Continuidade de operações**
- **Planejamento de capacidade**
  - Pessoal
  - Tecnologia
  - Infraestrutura
- **Testes**
  - Teste de mesa
  - Failover
  - Simulação
  - Processamento paralelo
- **Backups**
  - No local/externo
  - Frequência
  - Criptografia
  - Snapshots
  - Recuperação
  - Replicação
  - Registro no diário
- **Alimentação**
  - Geradores
  - Fonte de energia ininterrupta (UPS)

4.0 Operações de segurança

4.1 Considerando determinado cenário, aplicar técnicas de segurança comuns aos recursos de computação.

- **Linhas de base seguras**
  - Estabelecimento
  - Implantação
  - Manutenção
- **Alvos de hardening**
  - Dispositivos móveis
  - Estações de trabalho
  - Switches
  - Roteadores
  - Infraestrutura em nuvem
  - Servidores
  - ICS/SCADA
  - Sistemas embarcados
  - RTOS
  - Dispositivos IoT
- **Dispositivos sem fio**
  - Considerações sobre a instalação
    - Pesquisas de site
    - Mapas de calor
- **Soluções móveis**
  - Gerenciamento de dispositivos móveis (MDM)
  - Modelos de implantação
    - Traga seu próprio aparelho (BYOD)
    - Pertencente à empresa, ativado para uso pessoal (COPE)
    - Escolha seu próprio aparelho (CYOD)
  - Métodos de conexão
    - Celular
    - Wi-Fi
    - Bluetooth
- **Configurações de segurança sem fio**
  - Acesso protegido Wi-Fi 3 (WPA3)
  - Serviço de usuário discado de autenticação AAA/ remota (RADIUS)
  - Protocolos criptográficos
  - Protocolos de autenticação
- **Segurança dos aplicativos**
  - Validação de entrada
  - Cookies seguros
  - Análise de código estático
  - Assinatura de código
- **Sandboxing**
- **Monitoramento**

4.2 Explicar as implicações de segurança do gerenciamento adequado de hardware, software e ativos de dados.

- **Processo de aquisição/compra**
- **Atribuição/contabilidade**
  - Propriedade
  - Classificação
- **Monitoramento/rastreamento de ativos**
  - Inventário
  - Enumeração
- **Descarte/descomissionamento**
  - Sanitização
  - Destruição
  - Certificação
  - Retenção de dados

4.3 Explicar várias atividades associadas ao gerenciamento de vulnerabilidades.

- **Métodos de identificação**
  - Verificação de vulnerabilidades
  - Segurança dos aplicativos
    - Análise estática
    - Análise dinâmica
    - Monitoramento de pacotes
  - Feed de ameaças
    - Inteligência de código aberto (OSINT)
    - Proprietário/terceiro
    - Organização de compartilhamento de informações
    - Dark Web
  - Teste de intrusão
  - Programa de divulgação responsável
    - Programa de bug bounty
  - Auditoria de sistema/processo
- **Análise**
  - Confirmação
    - Falso positivo
    - Falso negativo
  - Priorização
  - Sistema de pontuação de vulnerabilidade comum (CVSS)
  - Enumeração de vulnerabilidade comum (CVE)
  - Classificação de vulnerabilidade
  - Fator de exposição
  - Variáveis ambientais
  - Impacto na indústria/organização
  - Tolerância de risco
- **Resposta e correção de vulnerabilidades**
  - Patching
  - Seguro (apólice)
  - Segmentação
  - Controles compensatórios
  - Exceções e isenções
- **Validação de remediação**
  - Nova verificação
  - Auditoria
  - Verificação
- **Geração de relatórios**

4.4 Explicar conceitos e ferramentas de alertas e monitoramento de segurança.

- **Monitoramento de recursos computacionais**
  - Sistemas
  - Aplicativos
  - Infraestrutura
- **Atividades**
  - Agregação de log
  - Alertas
  - Digitalização
  - Geração de relatórios
  - Arquivamento
  - Resposta de alerta e remediação/validação
    - Quarentena
    - Ajuste de alerta
- **Ferramentas**
  - Security Content Automation Protocol (SCAP)
  - Regional benchmarks
  - Agentes/sem agente
  - Gerenciamento de eventos e informações de segurança (SIEM)
  - Antivírus
  - Prevenção contra perda de dados (DLP)
  - Traps de Simple Network Management Protocol (SNMP)
  - NetFlow
  - Scanners de vulnerabilidades

4.5 Considerando determinado cenário, modificar os recursos empresariais para aumentar a segurança.

- **Firewall**
  - Regras
  - Listas de acesso
  - Portas/protocolos
  - Sub-rede filtrada
- **IDS/IPS**
  - Tendências
  - Assinatura
- **Filtro web**
  - Baseado em agente
  - Proxy centralizado
  - Verificação do Localizador universal de recursos (URL)
  - Categorização de conteúdo
  - Regras de bloqueio
  - Reputação
- **Segurança do sistema operacional**
  - Política de grupo
  - SELinux
- **Implementação de protocolos seguros**
  - Seleção de protocolo
  - Seleção de porta
  - Método de transporte
- **Filtro de DNS**
- **Segurança de e-mail**
  - Autenticação de mensagens baseada em domínio, relatórios e conformidade (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Gateway
- **Monitoramento de integridade de arquivo**
- **DLP**
- **Controle de acesso de rede (NAC)**
- **Detecção e resposta de endpoint (EDR)/detecção e resposta estendida (XDR)**
- **Análise do comportamento do usuário**

4.6 Considerando determinado cenário, implementar e manter o gerenciamento de identidade e acesso.

- **Provisionamento/ desprovisionamento de contas de usuário**
- **Atribuições e implicações de permissão**
- **Prova de identidade**
- **Federação**
- **Logon único (SSO)**
  - Lightweight Directory Access Protocol (LDAP)
  - Autorização aberta (OAuth)
  - Linguagem de marcação de asserção de segurança (SAML)
- **Interoperabilidade**
- **Atestado**
- **Controles de acesso**
  - Obrigatório
  - Discricionário
  - Baseado em função
  - Baseado em regra
  - Baseado em atributos
  - Restrições de horas do dia
  - Privilégio mínimo
- **Autenticação multifator**
  - Implementações
    - Biometria
    - Tokens de autenticação hard/soft
    - Chaves de segurança
  - Fatores
    - Algo que você sabe
    - Algo que você tem
    - Algo que você é
    - Algum local em que você está
- **Conceitos de senha**
  - Melhores práticas em relação a senhas
    - Comprimento
    - Complexidade
    - Reutilização
    - Expiração
    - Idade
  - Gerenciadores de senhas
  - Sem senha
- **Ferramentas de gerenciamento de acesso privilegiado**
  - Permissões just-in-time
  - Cofre de senha
  - Credenciais efêmeras

4.7 Explicar a importância da automação e orquestração relacionadas a operações seguras.

- **Casos de uso de automação e scripts**
  - Provisionamento de usuários
  - Provisionamento de recursos
  - Limitações de ações
  - Grupos de segurança
  - Criação de tíquetes
  - Escalação
  - Habilitação/desabilitação de serviços e acesso
  - Integração e testes contínuos
  - Integrações e Interfaces de programação de aplicativos (APIs)
- **Benefícios**
  - Eficiência/economia de tempo
  - Aplicação de linhas de base
  - Configurações de infraestrutura padrão
  - Dimensionamento de maneira segura
  - Retenção de funcionários
  - Tempo de reação
  - Multiplicador de força de trabalho
- **Outras considerações**
  - Complexidade
  - Custo
  - Ponto único de falha
  - Débito técnico
  - Suporte contínuo

4.8 Explicar as atividades apropriadas de resposta a incidentes.

- **Processo**
  - Preparação
  - Detecção
  - Análise
  - Contenção
  - Erradicação
  - Recuperação
  - Lições aprendidas
- **Treinamento**
- **Testes**
  - Teste de mesa
  - Simulação
- **Análise de causa raiz**
- **Caça a ameaças**
- **Forense digital**
  - Retenção legal
  - Cadeia de custódia
  - Aquisição
  - Geração de relatórios
  - Preservação
  - Descoberta eletrônica

4.9 Considerando determinado cenário, usar fontes de dados para apoiar uma investigação.

- **Dados de log**
  - Logs de firewall
  - Logs de aplicativos
  - Logs de endpoint
  - Logs de segurança específicos do sistema operacional
  - Logs do IPS/ IDS
  - Logs de rede
  - Metadados
- **Fontes de dados**
  - Verificações de vulnerabilidade
  - Relatórios automatizados
  - Painéis
  - Capturas de pacote

5.0 Gerenciamento e supervisão do programa de segurança

5.1 Resumir os elementos de uma governança de segurança eficaz.

- **Diretrizes**
- **Políticas**
  - Política de uso aceitável (AUP)
  - Políticas de Segurança da informação
  - Continuidade de negócios
  - Recuperação de desastre
  - Resposta a incidentes
  - Ciclo de vida de desenvolvimento de software (SDLC)
  - Gestão de mudanças
- **Padrões**
  - Senha
  - Controle de acesso
  - Segurança física
  - Criptografia
- **Procedimentos**
  - Gestão de mudanças
  - Integração/desligamento
  - Playbooks
- **Considerações externas**
  - Regulatório
  - Jurídico
  - Indústria
  - Local/regional
  - Nacional
  - Global
- **Monitoramento e revisão**
- **Tipos de estruturas de governança**
  - Conselhos
  - Comitês
  - Entidades governamentais
  - Centralizado/descentralizado
- **Funções e responsabilidades para sistemas e dados**
  - Proprietários
  - Controladores
  - Processadores
  - Custodiantes/administradores

5.2 Explicar os elementos do processo de gerenciamento de riscos.

- **Identificação de riscos**
- **Avaliação de riscos**
  - Ad hoc
  - Recorrente
  - Uso único
  - Contínuo
- **Análises de risco**
  - Qualitativo
  - Quantitativo
  - Expectativa de perda única (SLE)
  - Expectativa de perda anualizada (ALE)
  - Taxa de ocorrência anualizada (ARO)
  - Probabilidade
  - Possibilidade
  - Fator de exposição
  - Impacto
- **Registro de risco**
  - Indicadores-chave de risco
  - Proprietários de risco
  - Limiar de risco
- **Tolerância de risco**
- **Apetite ao risco**
  - Expansionista
  - Conservador
  - Neutro
- **Estratégias de gerenciamento de riscos**
  - Transferir
  - Aceitar
    - Isenção
    - Exceção
  - Evitar
  - Mitigar
- **Relatório de riscos**
- **Análise do impacto nos negócios**
  - Objetivo de tempo de recuperação (RTO)
  - Objetivo de ponto de recuperação (RPO)
  - Tempo médio de reparo (MTTR)
  - Tempo médio entre falhas (MTBF)

5.3 Explicar os processos associados à avaliação e gestão de riscos de terceiros.

- **Avaliação do fornecedor**
  - Teste de intrusão
  - Cláusulas de direito de auditoria
  - Evidência de auditoria interna
  - Avaliações independentes
  - Análise na cadeia de suprimentos
- **Seleção de fornecedores**
  - Devida diligência
  - Conflito de interesses
- **Tipos de acordo**
  - Contrato de nível de serviço (SLA)
  - Memorando de acordo (MOA)
  - Memorando de entendimento (MOU)
  - Contrato de serviço mestre (MSA)
  - Ordem de serviço (WO)/ declaração de trabalho (SOW)
  - Acordo de confidencialidade (NDA)
  - Acordo de parceiros de negócios (BPA)
- **Monitoramento de fornecedores**
- **Questionários**
- **Regras de engajamento**

5.4 Resumir os elementos de uma conformidade de segurança eficaz.

- **Relatório de conformidade**
  - Interno
  - Externo
- **Consequências de não conformidade**
  - Multas
  - Sanções
  - Danos à reputação
  - Perda de licença
  - Impactos contratuais
- **Monitoramento de conformidade**
  - Devida diligência/cuidado
  - Atestado e reconhecimento
  - Interno e externo
  - Automação
- **Privacidade**
  - Implicações legais
    - Local/regional
    - Nacional
    - Global
  - Titular dos dados
  - Controlador vs. processador
  - Propriedade
  - Inventário e retenção de dados
  - Direito ao esquecimento

5.5 Explicar os tipos e finalidades das auditorias e avaliações.

- **Atestado**
- **Interno**
  - Conformidade
  - Comitê de auditoria
  - Autoavaliações
- **Externo**
  - Regulatório
  - Exames
  - Avaliação
  - Auditoria independente de terceiros
- **Teste de intrusão**
  - Físico
  - Ofensivo
  - Defensivo
  - Integrado
  - Ambiente conhecido
  - Ambiente parcialmente conhecido
  - Ambiente desconhecido
  - Reconhecimento
    - Passivo
    - Ativo

5.6 Considerando determinado cenário, implementar práticas de conscientização de segurança.

- **Phishing**
  - Campanhas
  - Reconhecimento de tentativa de phishing
  - Resposta a mensagens suspeitas relatadas
- **Reconhecimento de comportamento anômalo**
  - Arriscado
  - Inesperado
  - Não intencional
- **Orientação e treinamento do usuário**
  - Política/manuais
  - Percepção situacional
  - Ameaça interna
  - Gerenciamento de senha
  - Mídia e cabos removíveis
  - Engenharia social
  - Segurança operacional
  - Ambientes de trabalho híbridos/remotos
- **Relatórios e monitoramento**
  - Inicial
  - Recorrente
- **Desenvolvimento**
- **Execução**

Lista de acrônimos do CompTIA Security+ SY0-701

A seguir é exibida uma lista de acrônimos que aparecem no exame CompTIA Security+ SY0-701. Os candidatos são incentivados a rever a lista completa e a obter conhecimentos de todos os acrônimos listados como parte de um programa de preparação abrangente para o exame.

Acrônimo	Escrito por extenso
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AES-256	Advanced Encryption Standards 256-bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
AV	Antivirus
BASH	Bourne Again Shell
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partners Agreement
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter Mode/CBC-MAC Protocol

Acrônimo	Escrito por extenso
CCTV	Closed-circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operation Planning
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-site Request Forgery
CSU	Channel Service Unit
CTM	Counter Mode
CTO	Chief Technology Officer
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention

Acrônimo	Escrito por extenso
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Translation
DNS	Domain Name System
DoS	Denial of Service
DPO	Data Privacy Officer
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EFS	Encrypted File System
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Management
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois Counter Mode
GDPR	General Data Protection Regulation
GPG	Gnu Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-time Password
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation Air Conditioning
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol

Acrônimo	Escrito por extenso
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISO	International Standards Organization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol Label Switching
MSA	Master Service Agreement

Acrônimo	Escrito por extenso
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Recover
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGFW	Next-generation Firewall
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over the Air
OVAL	Open Vulnerability Assessment Language
P12	PKCS #12
P2P	Peer to Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Privileged Access Management
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy

Acrônimo	Escrito por extenso
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PTZ	Pan-tilt-zoom
PUP	Potentially Unwanted Program
RA	Recovery Agent
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAN	Subject Alternative Name
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SD-WAN	Software-defined Wide Area Network

Acrônimo	Escrito por extenso
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDLM	Software Development Lifecycle Methodology
SDN	Software-defined Networking
SE Linux	Security-enhanced Linux
SED	Self-encrypting Drives
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip
SOC	Security Operations Center
SOW	Statement of Work
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXchange
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Indicator Information
TCP/IP	Transmission Control Protocol/ Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC	Time-of-check
TOTP	Time-based One-time Password
TOU	Time-of-use
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On the Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VBA	Visual Basic
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WO	Work Order
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
XDR	Extended Detection and Response
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

Lista de hardware e software do CompTIA Security+ SY0-701

A CompTIA incluiu esta lista de exemplos de hardware e software para ajudar os candidatos a se prepararem para o exame de certificação Security+ SY0-701. Esta lista também pode ser útil para as empresas de treinamento que desejam criar um ambiente de laboratório como componente para sua oferta de treinamento. As listas abaixo de cada tópico são exemplos e não exaustivos.

Equipamento

- Tablet
- Notebook
- Servidor Web
- Firewall
- Roteador
- Switch
- IDS
- IPS
- Ponto de acesso sem fio
- Máquinas virtuais
- Sistema de e-mail
- Acesso à Internet
- Servidor DNS
- Dispositivos IoT
- Tokens de hardware
- Smartphones

Hardware sobressalente

- NICs
- Fontes de energia
- GBICs
- SFPs
- Switch gerenciado
- Ponto de acesso sem fio
- UPS

Ferramentas

- Analisador de Wi-Fi
- Mapeador de rede
- NetFlow Analyzer

Software

- SO Windows
- SO Linux
- Kali Linux
- Software de captura de pacotes
- Software de teste de intrusão
- Ferramentas de análise estática e dinâmica
- Varredura de vulnerabilidade
- Emuladores de rede
- Código de amostra
- Editor de código
- SIEM
- Keyloggers
- Software MDM
- VPN
- Serviço DHCP
- Serviço de DNS

Outro

- Acesso a ambientes em nuvem
- Exemplo de documentação/diagramas de rede
- Logs de amostra

CompTIA