Objetivos do Exame de Certificação CompTIA de Analista de Segurança Cibernética (CySA+)

NÚMERO DO EXAME: CS0-003

Sobre o exame

O exame de certificação CompTIA de Analista de Segurança Cibernética (CySA+) certificará se o candidato tem o conhecimento e as habilidades necessárias para:

- Detectar e analisar indicadores de atividades maliciosas
- Compreender os conceitos de Threat Hunting e Threat Intelligence
- Usar ferramentas e métodos apropriados para gerenciar, priorizar e responder a ataques e vulnerabilidades
- Executar processos de resposta a incidentes
- Compreender os conceitos de relatórios e comunicação relacionados ao gerenciamento de vulnerabilidades e atividades de resposta a incidentes

ELABORAÇÃO DO EXAME

Os exames CompTIA são provenientes de seminários especializados e focados no assunto e pesquisas abrangentes em todo o setor quanto às habilidades e conhecimentos exigidos de um profissional de TI avançado.

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 CompTIA. Se um candidato não tiver a 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	CS0-003
Número de questões	No máximo 85
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	165 minutos
Experiência recomendada	4 anos de experiência prática como analista de resposta a incidentes ou analista de centro de operações de segurança (SOC)

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	Operações de segurança	33%
2.0	Gerenciamento de vulnerabilidades	30%
3.0	Gerenciamento e resposta a incidentes	20%
4.0	Relatórios e comunicação	17%
Total		**100%**

1.0 Operações de segurança

1.1 Explique a importância dos conceitos de arquitetura de sistema e rede nas operações de segurança.

- **Ingestão de logs**
  - Sincronização de tempo
  - Níveis de log
- **Conceitos de Sistema operacional (SO)**
  - Registro do Windows
  - Hardening do sistema
  - Estrutura de arquivo
    - Locais dos arquivos de configuração
  - Processos do sistema
  - Arquitetura de hardware
- **Conceitos de infraestrutura**
  - Sem servidor
  - Virtualização
  - Conteinerização
- **Arquitetura de redes**
  - Local (On-premise)
  - Nuvem
  - Híbrida
  - Segmentação de redes
  - Confiança zero (Zero Trust)
  - Borda segura de acesso seguro (SASE)
  - Rede definida por software (SDN)
- **Gerenciamento de identidade e acesso**
  - Autenticação multifator (MFA)
  - Logon único (SSO)
  - Federação
  - Gerenciamento de acesso privilegiado (PAM)
  - Sem senha
  - Agente de segurança de acesso à nuvem (CASB)
- **Criptografia**
  - Infraestrutura de chave pública (PKI)
  - Inspeção de Secure Sockets Layer (SSL Inspection)
- **Proteção de dados sensíveis**
  - Prevenção contra perda de dados (DLP)
  - Informações de identificação pessoal (PII)
  - Dados do titular do cartão (CHD)

1.2 Considerando determinado cenário, analise os indicadores de atividade potencialmente maliciosa.

- **Relacionado à rede**
  - Consumo de largura de banda
  - Beaconing
  - Comunicação ponto a ponto irregular
  - Dispositivos não autorizados na rede
  - Verificações/varreduras
  - Picos de tráfego incomuns
  - Atividade em portas inesperadas
- **Relacionado ao host**
  - Consumo do processador
  - Consumo de memória
  - Consumo de capacidade da unidade
  - Software não autorizado
  - Processos maliciosos
  - Alterações não autorizadas
  - Privilégios não autorizados
  - Exfiltração de dados
  - Comportamento anormal de processo do SO
  - Alterações ou anomalias do sistema de arquivos
  - Alterações ou anomalias do registro
  - Tarefas agendadas não autorizadas
- **Relacionado à aplicação**
  - Atividade anômala
  - Adição de novas contas
  - Saída inesperada
  - Comunicação de saída inesperada
  - Interrupção do serviço
  - Logs de aplicativos
- **Outro**
  - Ataques de engenharia social
  - Links ofuscados

1.3 Considerando determinado cenário, use as ferramentas ou técnicas apropriadas para determinar a atividade maliciosa.

- **Ferramentas**
  - Captura de pacote
    - Wireshark
    - tcpdump
  - Análise/correlação de logs
    - Gerenciamento de eventos e informações de segurança (SIEM)
    - Orquestração, automação e resposta de segurança (SOAR)
  - Segurança do ponto de extremidade
    - Detecção e resposta do ponto de extremidade (EDR)
  - Serviço de nomes de domínio (DNS) e reputação de Protocolo de Internet (IP)
    - WHOIS
    - AbuseIPDB
  - Análise de arquivo
    - Strings
    - VirusTotal
  - Sandboxing
    - Joe Sandbox
    - Cuckoo Sandbox
  - Análise de arquivo
    - Hash
  - Análise de comportamento do usuário
    - Atividade anormal da conta
    - Viagem impossível
- **Técnicas comuns**
  - Reconhecimento de padrões
    - Comando e controle
  - Interpretação de comandos suspeitos
  - Análise de e-mail
    - Cabeçalho
    - Personificação
    - DomainKeys Identified Mail (DKIM)
    - Autenticação de mensagens baseada em domínio, relatórios e conformidade (DMARC)
    - Sender Policy Framework (SPF)
    - Links incorporados
- **Linguagens de programação/scripting**
  - Notação de objetos JavaScript (JSON)
  - Linguagem de marcação extensível (XML)
  - Python
  - PowerShell
  - Shell script
  - Expressões regulares

1.4 Compare e diferencie os conceitos de threat intelligence e threat hunting.

- **Atores de ameaças**
  - Ameaça avançada persistente (APT)
  - Hacktivistas
  - Crime organizado
  - Estado-nação
  - Hacker amador
  - Ameaça interna
    - Intencional
    - Não intencional
  - Cadeia de suprimento
- **Táticas, técnicas e procedimentos (TTP)**
- **Níveis de confiança**
  - Pontualidade
  - Relevância
  - Precisão
- **Métodos de coleta e fontes**
  - Código aberto
    - Redes sociais
    - Blogs/fóruns
    - Boletins do governo
    - Grupo de resposta às emergências de computador (CERT)
    - Grupo de Respostas a Incidentes de Segurança em Computadores (CSIRT)
    - Deep/dark web
  - Fonte fechada
    - Feeds pagos
    - Organizações de compartilhamento de informações
    - Fontes internas
- **Compartilhamento de inteligência de ameaças**
  - Resposta a incidentes
  - Gerenciamento de vulnerabilidades
  - Gerenciamento de riscos
  - Engenharia de segurança
  - Detecção e monitoramento
- **Threat hunting**
  - Indicadores de comprometimento (IoC)
    - Coleta
    - Análise
    - Aplicação
  - Áreas de foco
    - Configurações/configurações incorretas
    - Redes isoladas
    - Ativos e processos críticos para os negócios
  - Defesa ativa
  - Honeypot

1.5 Explique a importância da eficiência e melhoria de processos nas operações de segurança.

- Padronizar processos
  - Identificação de tarefas adequadas para automação
    - Repetível/não requer interação humana
  - Coordenação de equipe para gerenciar e facilitar a automação
- Simplificar as operações
  - Automação e orquestração
    - Orquestração, automação e resposta de segurança (SOAR)
  - Orquestrar dados de threat intelligence
    - Enriquecimento de dados
    - Combinação de feed de ameaças
  - Minimizar o envolvimento humano
- Integração de tecnologia e ferramentas
  - Interface de programação de aplicativos (API)
  - Webhooks
  - Plugins
- Painel de controle centralizado

2.0 Gerenciamento de vulnerabilidades

2.1 Considerando determinado cenário, implemente métodos e conceitos de varredura de vulnerabilidades.

- **Descoberta de ativos**
  - Varreduras e mapeamento
  - Impressão digital do dispositivo
- **Considerações especiais**
  - Agendamento
  - Operações
  - Desempenho
  - Níveis de sensibilidade
  - Segmentação
  - Requisitos regulatórios
- **Varredura interna vs. varredura externa**
- **Com agente vs. sem agente**
- **Com credencial vs. sem credencial**
- **Passivo vs. ativo**
- **Estático vs. dinâmico**
  - Engenharia reversa
  - Fuzzing
- **Infraestrutura crítica**
  - Tecnologia operacional (OT)
  - Sistema de controle industrial (ICS)
  - Controle de supervisão e aquisição de dados (SCADA)
- **Varredura de linha de base de segurança**
- **Estruturas da indústria**
  - Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS)
  - Referências do Center for Internet Security (CIS)
  - Open Worldwide Application Security Project (OWASP)
  - Organização Internacional para Padronização (ISO) série 27000

2.2 Considerando determinado cenário, analise a saída das ferramentas de avaliação de vulnerabilidades.

- **Ferramentas**
  - Varredura e mapeamento de rede
    - Angry IP Scanner
    - Maltego
  - Ferramentas de aplicações web
    - Burp Suite
    - Zed Attack Proxy (ZAP)
    - Arachni
    - Nikto
  - Varreduras de vulnerabilidades
    - Nessus
    - OpenVAS
  - Depuradores
    - Immunity Debugger
    - GNU Debugger (GDB)
  - Multiuso
    - Nmap
    - Metasploit Framework (MSF)
    - Recon-ng
  - Ferramentas de avaliação de infraestrutura em nuvem
    - Scout Suite
    - Prowler
    - Pacu

2.3 Considerando determinado cenário, analise os dados para priorizar as vulnerabilidades.

- Interpretação do Sistema de pontuação de vulnerabilidade comum (CVSS)
  - Vetores de ataque
  - Complexidade do ataque
  - Privilégios necessários
  - Interação com o usuário
  - Escopo
  - Impacto
    - Confidencialidade
    - Integridade
    - Disponibilidade
- Validação
  - Verdadeiros/falsos positivos
  - Verdadeiros/falsos negativos
- Conscientização do contexto
  - Interno
  - Externo
  - Isolado
- Explorabilidade/preparação para ataques
- Valor do ativo
- Dia zero

2.4 Considerando determinado cenário, recomende controles para mitigar ataques e vulnerabilidades de software.

- Cross-Site Scripting (XSS)
  - Refletido
  - Persistente
- Vulnerabilidades de Estouro (overflow)
  - Buffer
  - Integer
  - Heap
  - Pilha
- Envenenamento de dados
- Quebra de controle de acesso
- Falhas criptográficas
- Falhas de injeção
- Falsificação de solicitação entre sites (CSRF)
- Diretório transversal
- Projeto inseguro
- Configurações de segurança incorretas
- Componentes em fim de vida ou desatualizados
- Falhas de identificação e autenticação
- Falsificação de solicitação do lado do servidor (SSRF)
- Execução de código remoto
- Escalação de privilégio
- Inclusão de arquivo local (LFI)/ inclusão de arquivo remoto (RFI)

2.5 Explique os conceitos relacionados à resposta, tratamento e gerenciamento de vulnerabilidades.

- Controle compensatório
- Tipos de controles
  - Gerencial
  - Operacional
  - Técnico
  - Preventivo
  - Detectivo
  - Responsivo
  - Corretivo
- Gerenciamento de patches e configuração
  - Teste
  - Implementação
  - Reversão
  - Validação
- Janelas de manutenção
- Exceções
- Princípios de gerenciamento de riscos
  - Aceitar
  - Transferir
  - Evitar
  - Mitigar
- Políticas, governança e objetivos de nível de serviço (SLOs)
- Priorização e escalonamento
- Gerenciamento da superfície de ataque
  - Descoberta de borda
  - Descoberta passiva
  - Teste de controles da segurança
  - Teste de invasão e emulação de adversário
  - Bug bounty
  - Redução da superfície de ataque
- Melhores práticas de programação segura
  - Validação de entrada
  - Codificação de saída
  - Gerenciamento de sessão
  - Autenticação
  - Proteção de dados
  - Consultas parametrizadas
- Ciclo de vida de desenvolvimento seguro de software (SDLC)
- Modelagem de ameaças

3.0 Gerenciamento e resposta a incidentes

3.1 Explique os conceitos relacionados a estruturas de metodologia de ataque.

- Cadeias de destruição cibernética (cyber kill chains)
- Modelo Diamond de análise de intrusão
- MITRE ATT&CK
- Manual de metodologia de teste de segurança de código aberto (OSS TMM)
- Guia de teste OWASP

3.2 Considerando determinado cenário, execute as atividades de resposta a incidentes.

- Detecção e análise
  - IoC
  - Aquisições de evidências
    - Cadeia de custódia
    - Validação da integridade dos dados
    - Preservação
    - Retenção legal
  - Análise de dados e logs
- Contenção, erradicação e recuperação
  - Escopo
  - Impacto
  - Isolamento
  - Remediação
  - Restauração da imagem
  - Controles compensatórios

3.3 Explique as fases de preparação e atividade pós-incidente do ciclo de vida do gerenciamento de incidentes.

- Preparação
  - Plano de resposta a incidentes
  - Ferramentas
  - Playbooks
  - Teste de mesa (Tabletop)
  - Treinamento
  - Continuidade de negócios (BC)/ recuperação de desastres (DR)
- Atividade pós-incidente
  - Análise forense
  - Análise de causa raiz
  - Lições aprendidas

4.0 Relatórios e comunicação

4.1 Explique a importância dos relatórios e da comunicação do gerenciamento de vulnerabilidades.

- **Relatórios de gerenciamento de vulnerabilidades**
  - Vulnerabilidades
  - Hosts afetados
  - Pontuação de risco
  - Mitigação
  - Recorrência
  - Priorização
- **Relatórios de conformidade**
- **Planos de ação**
  - Gerenciamento de configurações
  - Patching
  - Controles compensatórios
  - Conscientização, educação e treinamento
  - Mudança de requisitos de negócios
- **Inibidores para remediação**
  - Memorando de intenções (MOU)
  - Contrato de nível de serviço (SLA)
  - Governança organizacional
  - Interrupção do processo de negócios
  - Degradação de Funcionalidade
  - Sistemas legados
  - Sistemas proprietários
- **Métricas e indicadores-chave de desempenho (KPIs)**
  - Tendências
  - TOP 10
  - Vulnerabilidades críticas e de Dia zero
  - SLOs
- **Identificação e comunicação das partes interessadas**

4.2 Explique a importância dos relatórios e da comunicação de resposta a incidentes.

- **Identificação e comunicação das partes interessadas**
- **Declaração e escalonamento de incidentes**
- **Reporte de resposta a incidentes**
  - Resumo executivo
  - Quem, o quê, quando, onde e por quê
  - Recomendações
  - Cronograma
  - Impacto
  - Escopo
  - Evidência
- **Comunicações**
  - Jurídico
  - Relações públicas
    - Comunicação com o cliente
    - Mídia
  - Relatórios regulatórios
  - Autoridade policial
- **Análise de causa raiz**
- **Lições aprendidas**
- **Métricas e KPIs**
  - Tempo médio para detectar
  - Tempo médio para responder
  - Tempo médio para remediar
  - Volume de alertas

Lista de acrônimos do CS0-003 CompTIA CySA+

A seguir é exibida uma lista de acrônimos que aparecem no exame CS0-003 da CompTIA CySA+. 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
ACL	Access Control List
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AV	Antivirus
BC	Business Continuity
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
C2	Command and Control
CA	Certificate Authority
CASB	Cloud Access Security Broker
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CHD	Cardholder Data
CI/CD	Continuous Integration and Continuous Delivery
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technologies
CSIRT	Cybersecurity Incident Response Team
CSRF	Cross-site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name Service
DoS	Denial of Service
DR	Disaster Recovery
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
GDB	GNU Debugger
GPO	Group Policy Objects
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol

ACRÔNIMO	ESCRITO POR EXTENSO
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IoC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LAN	Local Area Network
LDAPS	Lightweight Directory Access Protocol
LFI	Local File Inclusion
LOI	Letter of Intent
MAC	Media Access Control
MFA	Multifactor Authentication
MOU	Memorandum of Understanding
MSF	Metasploit Framework
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair
NAC	Network Access Control
NDA	Non-disclosure Agreement
NGFW	Next-generation Firewall
NIDS	Network-based Intrusion Detection System
NTP	Network Time Protocol
OpenVAS	Open Vulnerability Assessment Scanner
OS	Operating System
OSSTMM	Open Source Security Testing Methodology Manual
OT	Operational Technology
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PHP	Hypertext Preprocessor
PID	Process Identifier
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POC	Proof of Concept
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFI	Remote File Inclusion
RXSS	Reflected Cross-site Scripting
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SASE	Secure Access Secure Edge
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Life Cycle

ACRÔNIMO	ESCRITO POR EXTENSO
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SLO	Service-level Objective
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SPF	Sender Policy Framework
SQL	Structured Query Languge
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSRF	Server-side Request Forgery
STIX	Structured Threat Information Expression
SWG	Secure Web Gateway
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TRACE	Trade Reporting and Compliance Engine
TTP	Tactics, Techniques, and Procedures
UEBA	User and Entity Behavior Analytics
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XDR	Extended Detection Response
XML	Extensible Markup Language
XSS	Cross-site Scripting
XXE	XML External Entity
ZAP	Zed Attack Proxy
ZTNA	Zero Trust Network Access

Lista de hardware e software do CS0-003 CompTIA CySA+

A CompTIA incluiu esta lista de sugestões de hardware e software para ajudar os candidatos a se prepararem para o exame de certificação CS0-003 de CySA+. 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

- Estações de trabalho (ou notebook) com capacidade de executar VM
- Firewall
- IDS/IPS
- Servidores

SOFTWARE

- Sistemas operacionais Windows
  - Commando VM
- Sistemas operacionais Linux
  - Kali
- Dispositivo UTM de código aberto
- Metasploitable
- SIEM
  - Greylog
  - ELK
  - Splunk
- TCPDump
- Wireshark
- Varredura de vulnerabilidades (ex. OpenVAS)
- Nessus
- Acesso a instâncias de nuvem
  - Azure
  - AWS
  - GCP