CompTIA Cybersecurity Analyst (CySA+) Examen de Certificación Objetivos

NÚMERO DE EXAMEN: CS0-003

Acerca del examen

El examen de certificación CompTIA Cybersecurity Analyst (CySA+) certificará que el candidato aprobado tenga los conocimientos y las habilidades requeridas para lo siguiente:

- Detectar y analizar indicadores de actividad maliciosa
- Entender los conceptos de caza de amenazas e inteligencia de amenazas
- Usar herramientas y métodos adecuados para administrar, priorizar y responder a ataques y vulnerabilidades
- Realizar procesos de respuesta ante incidentes
- Entender los conceptos de informes y comunicación relacionados con administración de vulnerabilidades y actividades de respuesta a incidentes

DESARROLLO DEL EXAMEN

Los exámenes de CompTIA son resultado de talleres de expertos del área temática y resultados de encuestas de toda la industria con respecto a las habilidades y conocimientos necesarios para un profesional de TI avanzado.

POLÍTICA DE USO DE MATERIALES AUTORIZADOS CompTIA

CompTIA Certifications, LLC no está afiliado y no autoriza, aprueba o tolera la utilización de cualquier contenido proporcionado por otros sitios de capacitación no autorizados (conocidos como “brain dumps”). A las personas que utilicen este tipo de materiales en la preparación de cualquier examen CompTIA se les anularán los certificados y será suspendida la realización de futuras pruebas en concordancia con el Acuerdo para Candidatos de CompTIA. En un esfuerzo por comunicar más claramente las políticas de exámenes de CompTIA en relación con el uso de materiales de estudio autorizados, CompTIA dirige a todos los candidatos de certificación a las Políticas de Examen de Certificación CompTIA. Revise todas las políticas CompTIA antes de comenzar el proceso de estudio para cualquier examen CompTIA. Se requerirá que los candidatos acaten el Acuerdo de Candidato CompTIA. Si un candidato tiene una pregunta acerca de qué materiales de estudio se consideran no autorizados (conocidos como “brain dumps”), él/ella debe comunicarse con CompTIA en examsecurity@comptia.org para confirmar.

RECUERDE

Las listas de ejemplos proporcionadas en formato con viñetas no son listas completas. Otros ejemplos de tecnologías, procesos o tareas relativas a cada objetivo también pueden ser incluidos en el examen, aunque no estén enumerados o cubiertos en este documento de objetivos. CompTIA revisa constantemente el contenido de nuestros exámenes y actualiza las preguntas de las pruebas para asegurar que nuestros exámenes sean actuales y la seguridad de las preguntas esté protegida. Cuando sea necesario, publicaremos exámenes actualizados, basados en objetivos de examen existentes. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

DETALLES DE LA PRUEBA

Examen requerido	CS0-003
Número de preguntas	85 como máximo
Tipos de preguntas	Selección múltiple y basadas en la ejecución
Longitud de la prueba	165 minutos
Experiencia recomendada	4 años de experiencia práctica como analista de respuesta a incidentes o analista en centro de operaciones de seguridad (SOC)

OBJETIVOS DEL EXAMEN (DOMINIOS)

La siguiente tabla enumera los dominios medidos en este examen y el grado en el que están representados.

DOMINIO		PORCENTAJE DEL EXAMEN
1.0	Operaciones de Seguridad	33%
2.0	Administración de Vulnerabilidades	30%
3.0	Respuesta y administración de incidentes	20%
4.0	Informes y comunicación	17%
Total		**100%**

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

1.0 Operaciones de Seguridad

1.1 Explicar la importancia de los conceptos de arquitectura de redes y sistemas en las operaciones de seguridad.

- **Manejo de registros**
  - Sincronización del tiempo
  - Niveles de registro
- **Conceptos de sistemas operativos (OS)**
  - Registro de Windows
  - Fortalecimiento de sistema
  - Estructura de archivos
    - Ubicaciones de archivos de configuración
  - Procesos del sistema
  - Arquitectura de hardware
- **Conceptos de infraestructura**
  - Sin servidor
  - Virtualización
  - Contenedorización
- **Arquitectura de redes**
  - En sitio
  - Nube
  - Híbrido
  - Segmentación de red
  - Confianza cero
  - Sector de servicio de acceso seguro (SASE)
  - Redes definidas por software (SDN)
- **Administración de identidad y acceso**
  - Autenticación de Multifactores (MFA)
  - Inicio de sesión único (SSO)
  - Federación
  - Administración de acceso privilegiado (PAM)
  - Sin contraseña
  - Agente de Seguridad de Acceso a la Nube (CASB)
- **Cifrado**
  - Infraestructura de Clave Pública (PKI)
  - Inspección de Secure sockets layer (SSL)
- **Protección de datos sensibles**
  - Prevención de pérdida de datos (DLP)
  - Información de Identificación Personal (PII)
  - Datos del titular de la tarjeta (CHD)

1.2 A partir de un escenario, analizar indicadores de actividad potencialmente maliciosa.

- **Relacionado con la red**
  - Consumo de ancho de banda
  - Envío de señales
  - Comunicación irregular interpares
  - Dispositivos mal intencionados en la red
  - Escaneos/sweeps
  - Aumentos inusuales de tráfico
  - Actividad anómala en puertos inesperados
- **Relacionado al host**
  - Consumo de procesador
  - Consumo de memoria
  - Consumo de capacidad de unidad
  - Software no autorizado
  - Procesos maliciosos
  - Cambios no autorizados
  - Privilegios no autorizados
  - Exfiltración de datos
  - Conducta de proceso anormal de OS
  - Cambios o anomalías en sistema de archivos
  - Cambios o anomalías en registro
  - Tareas programadas no autorizadas
- **Relacionadas con la aplicación**
  - Actividad anómala
  - Introducción a nuevas cuentas
  - Salida no esperada
  - Comunicación de salida no esperada
  - Interrupción de servicio
  - Registros de aplicación
- **Otro**
  - Ataques de ingeniería social
  - Enlaces ofuscados

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

1.3 A partir de un escenario, usar herramientas o técnicas apropiadas para determinar actividad maliciosa.

- **Herramientas**
  - Captura de paquetes
    - Wireshark
    - tcpdump
  - Análisis/correlación de registro
    - Gestión de información y eventos de seguridad (SIEM)
    - Orquestación, automatización y respuesta de seguridad (SOAR)
  - Seguridad de endpoint
    - Detección y respuesta de endpoint (EDR)
  - Reputación de Servicio de Nombre de Dominio (DNS) y Protocolo de Internet (IP)
    - WHOIS
    - AbuseIPDB
  - Análisis de archivo
    - Cadenas
    - VirusTotal
  - Sandboxing (caja de arena / área de pruebas)
    - Joe Sandbox
    - Cuckoo Sandbox
- **Técnicas comunes**
  - Reconocimiento de patrones
    - Comando y control
  - Interpretación de comandos sospechosos
  - Análisis de correos electrónicos
    - Encabezado
    - Suplantación
    - DomainKeys Identified Mail (DKIM)
    - Autenticación de mensajes, informes y conformidad basada en dominios (DMARC)
    - Marco de políticas de remitente (SPF)
    - Enlaces insertados / integrados
  - Análisis de archivo
    - Hashing
  - Análisis del comportamiento del usuario
    - Actividad anormal de la cuenta
    - Viaje imposible
- **Lenguajes/scripting de programación**
  - Notación de objetos JavaScript (JSON)
  - Lenguaje Extensible de Marcas (XML)
  - Python
  - PowerShell
  - Shell script
  - Expresiones regulares

1.4 Comparar y contrastar los conceptos de inteligencia de amenazas y caza de amenazas.

- **Actores de amenazas**
  - Amenaza avanzada persistente (APT)
  - Hacktivistas
  - Crimen organizado
  - Nation-state
  - Script kiddie
  - Amenazas internas
    - Intencional
    - No intencional
  - Cadena de suministro
- **Tácticas, técnicas y procedimientos (TTP)**
- **Niveles de confianza**
  - Puntualidad
  - Relevancia
  - Precisión
- **Métodos y fuentes de recolección**
  - Código abierto
    - Redes sociales
    - Blogs/foros
    - Boletines gubernamentales
    - Computer emergency response team (CERT)
    - Equipo de respuesta a incidentes de ciberseguridad (CSIRT)
    - Dark web/web profunda
  - Código cerrado
    - Informes pagados
    - Organizaciones que comparten información
    - Fuentes internas
- **Intercambio de inteligencia de amenazas**
  - Respuesta a incidentes
  - Administración de vulnerabilidades
  - Administración de riesgos
  - Ingeniería de seguridad
  - Detección y monitoreo
- **Caza de amenazas**
  - Indicadores de compromiso (IoC)
    - Recolección
    - Análisis
    - Aplicación
  - Áreas de atención
    - Configuraciones/malas configuraciones
    - Redes aisladas
    - Activos y procesos esenciales para negocios
  - Defensa activa
  - Honeypot

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

1.5 Explicar la importancia de la eficiencia y la mejora de procesos en las operaciones de seguridad.

- **Estandarizar procesos**
  - Identificación de tareas apropiadas para automatización
    - Repetible/no requiere interacción humana
  - Coordinación del equipo para administrar y facilitar la automatización
- **Simplificar operaciones**
  - Automatización y orquestación
    - Orquestación, automatización y respuesta de seguridad (SOAR)
  - Orquestación de datos de inteligencia de amenazas
    - Enriquecimiento de datos
    - Combinación de informes sobre amenazas
  - Minimizar participación humana
- **Integración de tecnología y herramientas**
  - Interfaz de programación de aplicación (API)
  - Webhooks
  - Complementos
- **Panel único de vidrio**

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

2.0 Administración de Vulnerabilidades

2.1 A partir de un escenario, implementar métodos y conceptos de escaneo de vulnerabilidad.

- **Descubrimiento de activos**
  - Escaneo de mapas
  - Huella digital de dispositivo
- **Consideraciones especiales**
  - Programación
  - Operaciones
  - Desempeño
  - Niveles de sensibilidad
  - Segmentación
  - Requisitos regulatorios
- **Escaneo externo vs. interno**
- **Con agente vs. sin agente**
- **Con credenciales vs. sin credenciales**
- **Pasivo vs. activo**
- **Estático vs. dinámico**
  - Ingeniería inversa
  - Fuzzing
- **Infraestructura crítica**
  - Tecnología operativa (OT)
  - Sistemas de control industrial (ICS)
  - Control de supervisión y adquisición de datos (SCADA)
- **Escaneo de puntos de partida de seguridad**
- **Marcos industriales**
  - Estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS)
  - Referencias del Centro para Seguridad de Internet (CIS)
  - Proyecto de seguridad de aplicaciones web abiertas (OWASP)
  - Serie 27000 de la Organización Internacional de Normalización (ISO)

2.2 A partir de un escenario, analizar el resultado de las herramientas de evaluación de vulnerabilidad.

- **Herramientas**
  - Escaneo y mapeo de red
    - Angry IP Scanner
    - Maltego
  - Escáneres de aplicaciones web
    - Burp Suite
    - Zed Attack Proxy (ZAP)
    - Arachni
    - Nikto
  - Escáneres de vulnerabilidad
    - Nessus
    - OpenVAS
  - Depuradores
    - Immunity debugger
    - GNU debugger (GDB)
  - Multipropósitos
    - Nmap
    - Metasploit framework (MSF)
    - Recon-ng
  - Herramientas de evaluación de infraestructura en la nube
    - Scout Suite
    - Prowler
    - Pacu

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

2.3 A partir de un escenario, analizar datos para priorizar las vulnerabilidades.

- **Interpretación del Sistema de puntuación de vulnerabilidades comunes (CVSS)**
  - Vectores de ataque
  - Complejidad del ataque
  - Privilegios requeridos
  - Interacción del usuario
  - Alcance
  - Impacto
    - Confidencialidad
    - Integridad
    - Disponibilidad
- **Validación**
  - Verdaderos/falsos positivos
  - Verdaderos/falsos negativos
- **Conocimiento del contexto**
  - Interno
  - Externo
  - Aislado
- **Explotabilidad/militarización**
- **Valor del activo**
- **Día cero**

2.4 A partir de un escenario, recomendar controles para mitigar los ataques y vulnerabilidades.

- **Cross-site scripting**
  - Reflejado
  - Persistente
- **Vulnerabilidades de desbordamiento**
  - Búfer
  - Enteros
  - Heap
  - Stack
- **Envenenamiento de datos**
- **Control de acceso roto**
- **Fallas criptográficas**
- **Errores de inyección**
- **Falsificación de solicitudes entre sitios**
- **Directory traversal**
- **Diseño inseguro**
- **Mala configuración de seguridad**
- **Componentes obsoletos o en el final de la vida**
- **Fallas de identificación y autenticación**
- **Falsificación de solicitudes de servidores**
- **Ejecución de código remoto**
- **Escalamiento de privilegios**
- **Inclusión de archivo local (LFI)/ inclusión de archivo remoto (RFI)**

2.5 Explicar conceptos relacionados con la respuesta, el manejo y la administración de vulnerabilidades.

- **Control de compensación**
- **Tipos de control**
  - Gerencial
  - Operacional
  - Técnico
  - Preventivo
  - Detectivo
  - Reactivo
  - Correctivo
- **Administración de parches y configuración**
  - Pruebas
  - Implementación
  - Rollback
  - Validación
- **Ventanas de mantenimiento**
- **Excepciones**
- **Principios de administración de riesgos**
  - Aceptar
  - Transferir
  - Evitar
  - Mitigar
- **Políticas, gobernanza y objetivos de nivel de servicio (SLO)**
- **Priorización y escalamiento**
- **Administración de superficie de ataque**
  - Descubrimiento de borde
  - Descubrimiento pasivo
  - Pruebas de control de seguridad
  - Pruebas de penetración y emulación de adversarios
  - Recompensa por errores
  - Reducción de superficie de ataque
- **Mejores prácticas de codificación segura**
  - Validación de entrada
  - Codificación de salida
  - Administración de sesión
  - Autenticación
  - Protección de datos
  - Consultas parametrizadas
- **Ciclo de vida del desarrollo de software (SDLC) seguro**
- **Modelamiento de amenazas**

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

3.0 Respuesta y administración de incidentes

3.1 Explicar conceptos relacionadas con marcos de metodologías de ataque.

- **Cyber kill chains**
- **Modelo diamante de análisis de intrusión**
- **MITRE ATT&CK**
- **Manual de Metodología de Pruebas de Seguridad en Código abierto (OSS TMM)**
- **Guía de pruebas OWASP**

3.2 A partir de un escenario, realizar las actividades de respuesta a incidentes.

- **Detección y análisis**
  - IoC
  - Adquisición de evidencia
    - Cadena de custodia
    - Validación de integridad de datos
    - Preservación
    - Retención legal
  - Análisis de datos y registros
- **Contención, erradicación y recuperación**
  - Alcance
  - Impacto
  - Aislamiento
  - Remediación
  - Recreación de imagen
  - Controles de compensación

3.3 Explicar las fases de preparación y actividad posterior a incidentes del ciclo de vida de la administración de incidentes.

- **Preparación**
  - Plan de respuesta ante incidentes
  - Herramientas
  - Playbooks
  - Tabletop
  - Capacitación
  - Continuidad de negocios (BC)/ recuperación de desastres (DR)
- **Actividad post-incidentes**
  - Análisis forense
  - Análisis de causa principal
  - Lecciones aprendidas

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

4.0 Informes y comunicación

4.1 Explicar la importancia de los informes y comunicación en la administración de vulnerabilidades.

- **Informes de administración de vulnerabilidades**
  - Vulnerabilidades
  - Estaciones afectadas
  - Calificación de riesgo
  - Mitigación
  - Recurrencia
  - Priorización
- **Informe de cumplimiento**
- **Planes de acción**
  - Administración de la configuración
  - Parches
  - Controles de compensación
  - Conocimiento, educación y capacitación
  - Cambio de requisitos de negocios
- **Inhibidores para la remediación**
  - Memorándum de entendimiento (MOU)
  - Acuerdo de Nivel de Servicio (SLA)
  - Gobernanza organizacional
  - Interrupción de procesos de negocios
  - Degradación de funcionalidad
  - Sistemas heredados
  - Sistemas propios
- **Métricas e indicadores claves de desempeño (KPI)**
  - Tendencias
  - Las 10 principales
  - Vulnerabilidades críticas y de día cero
  - SLO
- **Identificación y comunicación de partes involucradas**

4.2 Explicar la importancia de los informes y comunicación en la respuesta a incidentes.

- **Identificación y comunicación de partes involucradas**
- **Declaración y escalamiento de incidentes**
- **Informes de respuesta ante incidentes**
  - Resumen ejecutivo
  - Quién, qué, cuándo, dónde y por qué
  - Recomendaciones
  - Cronología
  - Impacto
  - Alcance
  - Evidencia
- **Comunicaciones**
  - Legal
  - Relaciones públicas
    - Comunicación con clientes
    - Medios
  - Informes regulatorios
  - Cumplimiento de la ley
- **Análisis de causa principal**
- **Lecciones aprendidas**
- **Métricas y KPI**
  - Tiempo medio para detectar
  - Tiempo medio para responder
  - Tiempo medio para remediar
  - Volumen de alerta

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

Lista de siglas de CompTIA CySA+ CS0-003

A continuación hay una lista de siglas que aparecen el examen de CompTIA CySA+ CS0-003. Se insta a los candidatos a revisar la lista completa y alcanzar un conocimiento práctico de todas las siglas listadas, como parte de un programa completo de preparación para el examen.

Siglas	Frase completa
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

Siglas	Frase completa
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
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

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

Siglas	Frase completa
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
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

Derechos de autor © 2022 CompTIA, Inc. Todos los derechos reservados.

Lista de hardware y software para CompTIA CySA+ CS0-003

CompTIA ha incluido esta lista de muestra de hardware y software para asistir a los candidatos mientras se preparan para el examen de certificación CySA+ CS0-003. Esta lista también puede ser útil para las empresas de capacitación que desean crear un componente de laboratorio en su capacitación ofertada. Las listas con viñetas debajo de cada tema son listas de muestra y no están completas.

Equipos

- Estaciones de trabajo (o computadoras portátiles) con capacidad de ejecutar VM
- Firewall
- IDS/IPS
- Servidores

Software

- Sistemas operativos Windows
  - Comando VM
- Sistemas operativos Linux
  - Kali
- Dispositivo UTM de código abierto
- Metasploitable
- SIEM
  - Greylog
  - ELK
  - Splunk
- TCPDump
- Wireshark
- Escáner de vulnerabilidad (por ejemplo, OpenVAS)
- Nessus
- Acceso a instancias en la nube
  - Azure
  - AWS
  - GCP

© 2022 CompTIA, Inc., usado con licencia de CompTIA, Inc. Todos los derechos reservados. Todos los programas de certificación y la educación relacionada con tales programas son operados exclusivamente por CompTIA, Inc. CompTIA es una marca registrada de CompTIA, Inc. en Estados Unidos e internacionalmente. Otras marcas y nombres de compañías mencionados en este documento pueden ser marcas comerciales o marcas de servicios de CompTIA, Inc. o de sus propietarios respectivos. Está prohibida la reproducción o difusión sin el consentimiento escrito de CompTIA, Inc. Impreso en Estados Unidos 09804-Julio 2022