

COMPTIA · PLUS SERIES

VERSIÓN 4

CompTIA Cybersecurity Analyst (CySA+) V4

Examen CS0-004

Detecta, analiza y responde a amenazas: la certificación de referencia para analistas de operaciones de seguridad y gestión de vulnerabilidades.

¿Por qué debería asistir?

CompTIA CySA+ valida que el profesional puede detectar, analizar y responder a amenazas en roles de operaciones de seguridad (SOC) y gestión de vulnerabilidades. La versión 4, lanzada en junio de 2026, pone el foco en la detección y respuesta a incidentes y en el monitoreo continuo en entornos actuales, además de la gestión de vulnerabilidades y la comunicación clara de los riesgos críticos.

Durante el curso, los participantes aprenden a investigar actividad sospechosa en redes, endpoints y entornos en la nube; a monitorear y analizar datos con plataformas SIEM y EDR; a priorizar y mitigar vulnerabilidades con un enfoque basado en riesgo; a responder a incidentes con procesos estructurados y marcos como MITRE ATT&CK, y a comunicar hallazgos a las partes interesadas mediante reportes y dashboards. Esta versión incorpora además el uso de la inteligencia artificial y la automatización en el SOC.

5 días	4	15	Prácticos	Intermedio
DURACIÓN	DOMINIOS OFICIALES	OBJETIVOS	LABORATORIOS	NIVEL



¿Quién debería participar?

Analistas de SOC
Analistas de nivel 1 y 2 que monitorean alertas, investigan eventos y escalan incidentes en un centro de operaciones de seguridad.

Analistas de vulnerabilidades
Profesionales que ejecutan escaneos, interpretan resultados y priorizan la remediación según el riesgo para el negocio.

Equipos de respuesta a incidentes y threat hunting
Integrantes de CSIRT y cazadores de amenazas que necesitan una metodología estructurada de investigación y contención.

Administradores e ingenieros de seguridad
Profesionales con Security+ o experiencia equivalente que desean avanzar hacia roles de análisis y defensa.

Objetivos de aprendizaje

- Identificar e investigar actividad sospechosa en redes, endpoints y entornos en la nube para descubrir amenazas potenciales.
- Monitorear y analizar datos con herramientas estándar de la industria, como plataformas SIEM y EDR.
- Aplicar inteligencia de amenazas y técnicas de threat hunting en la investigación de eventos.
- Identificar, priorizar y mitigar vulnerabilidades con enfoques basados en riesgo.
- Investigar y responder a incidentes de seguridad con procesos estructurados y técnicas del mundo real.
- Comprender el uso de la inteligencia artificial y la automatización en el SOC, con sus riesgos y su gobierno.
- Comunicar con claridad hallazgos y riesgos a las partes interesadas mediante reportes y dashboards.
- Aplicar prácticas de seguridad en entornos en la nube e híbridos con operaciones eficientes y eficaces.

Áreas de habilidad

Operaciones de seguridad (SOC) | SIEM y EDR | Análisis de paquetes | Inteligencia de amenazas | Threat hunting | IA en el SOC | Automatización | Escaneo de vulnerabilidades | Gestión de riesgos | MITRE ATT&CK | Respuesta a incidentes | Reportes y métricas

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 **Objetivos 1.1–1.3** **Día 1**	**1.1 Conceptos de arquitectura de sistemas y redes en operaciones de seguridad** Componentes de arquitectura de seguridad, gestión de identidades y prácticas de registro (logging). **1.2 Indicadores de actividad potencialmente maliciosa** Comportamientos sospechosos en redes, endpoints, nube y sistemas de identidad. **1.3 Herramientas para determinar actividad maliciosa** SIEM, EDR, análisis de paquetes y plataformas de inteligencia de amenazas.
Dominio 1 **Objetivos 1.4–1.6** **Día 2**	**1.4 Inteligencia de amenazas y threat hunting** Marcos de referencia, fuentes de datos y métodos de investigación. **1.5 Eficiencia y mejora de procesos en operaciones de seguridad** Automatización, orquestación, flujos de trabajo y procesos operativos. **1.6 Uso de la IA en operaciones de seguridad** Casos de uso de la inteligencia artificial en el SOC, sus riesgos y su gobierno.
Dominio 2 **Objetivos 2.1–2.3** **Día 3**	**2.1 Métodos de escaneo de vulnerabilidades** Herramientas y técnicas de escaneo de sistemas, redes y aplicaciones. **2.2 Análisis de resultados de herramientas de evaluación** Interpretación de hallazgos y brechas de seguridad identificadas. **2.3 Priorización y mitigación de vulnerabilidades** Enfoque basado en riesgo con puntuaciones, inteligencia de amenazas y contexto del negocio.
Dominios 2 · 3 **Objetivos 2.4 3.1–3.2** **Día 4**	**2.4 Tipos de controles, riesgos y gestión de vulnerabilidades** Controles, políticas y prácticas de cumplimiento. **3.1 Marcos de metodologías de ataque** MITRE ATT&CK, Cyber Kill Chain y otros modelos. **3.2 Proceso de respuesta a incidentes** Preparación, detección, análisis, contención, erradicación y recuperación.
Dominios 3 · 4 **Objetivos 3.3 4.1–4.2** **Día 5**	**3.3 Técnicas de respuesta a incidentes** Triaje, manejo de evidencias, escalamiento, remediación y análisis de causa raíz. **4.1 Reportes y comunicación de la gestión de vulnerabilidades** Informes, dashboards y escalamiento durante eventos de seguridad. **4.2 Reportes y comunicación de operaciones y respuesta a incidentes** Documentación de incidentes, revisiones posteriores y métricas como tiempo de detección, de respuesta y efectividad de la remediación.

Los objetivos siguen el temario oficial del examen CompTIA CySA+ CS0-004. Peso de cada dominio: 1. Operaciones de seguridad (34 %), 2. Gestión de vulnerabilidades (26 %), 3. Respuesta y gestión de incidentes (24 %), 4. Reportes y comunicación (16 %).

Examen y certificación

Título	CompTIA Cybersecurity Analyst (CySA+) – Versión 4
Código	CS0-004
Preguntas	Máximo 85
Formato	Opción múltiple y preguntas basadas en desempeño
Duración	165 minutos
Aprobación	750 (escala de 100–900)
Idioma	Inglés (español, francés, japonés y portugués, próximamente)
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda unos 4 años de experiencia como analista de SOC o de vulnerabilidades, y conocimientos equivalentes a Network+ y Security+.
- La versión anterior (CS0-003) se retira del examen en inglés el 22 de diciembre de 2026.

Ruta profesional CompTIA

CySA+ es la certificación intermedia de la ruta de ciberseguridad de CompTIA: se apoya en Network+ y Security+, se complementa con PenTest+ en el lado ofensivo y prepara el camino hacia SecurityX, el nivel experto.



Información general

- Material oficial de CompTIA, con laboratorios prácticos y preguntas de práctica.
- Instructor certificado y Savant Consultores como CompTIA Authorized Partner.
- Certificación acreditada por ANAB bajo la norma ISO/IEC 17024.
- Vigencia de 3 años, renovable mediante el programa de Educación Continua (CE) de CompTIA.

CompTIA Authorized Partner | ACADEMIC PARTNER

CompTIA CySA+ CERTIFICATION Plus Series