

Curso CompTIA CySA+

Plan de Estudio



COMUNICACIÓN
INTEGRAL
Haciendo futuro con ideas.



Descripción

Este curso de **CompTIA CySA+** está diseñado para formar analistas de ciberseguridad altamente competentes capaces de identificar, analizar y mitigar amenazas de seguridad en entornos empresariales. Se centra en el desarrollo de habilidades prácticas para la detección y respuesta a incidentes, así como en la gestión de vulnerabilidades. Los estudiantes adquirirán las competencias necesarias para prepararse para la certificación **CompTIA CySA+** y desempeñarse exitosamente como analistas de seguridad cibernética.

CompTIA CySA+ es una certificación para profesionales de la ciberseguridad que se encargan de la detección, prevención y respuesta a incidentes a través del monitoreo continuo de la seguridad. Esta certificación cubre temas como las operaciones de seguridad, la gestión de vulnerabilidades, la respuesta y gestión de incidentes, los informes y la comunicación, y los marcos de metodología de ataque.

El curso está estructurado en 5 unidades, donde encontrarás contenidos teóricos puntuales, junto a prácticas y ejercicios auto gestionables basados en la metodología de aprendizaje en línea o e-learning.



Dirigido a:

A profesionales de TI que buscan obtener habilidades como capturar, monitorear y responder proactivamente a los hallazgos del tráfico de la red. Enfatiza la seguridad del software y las aplicaciones, la automatización, la búsqueda de amenazas y el cumplimiento normativo de TI.



¿Qué aprenderás?

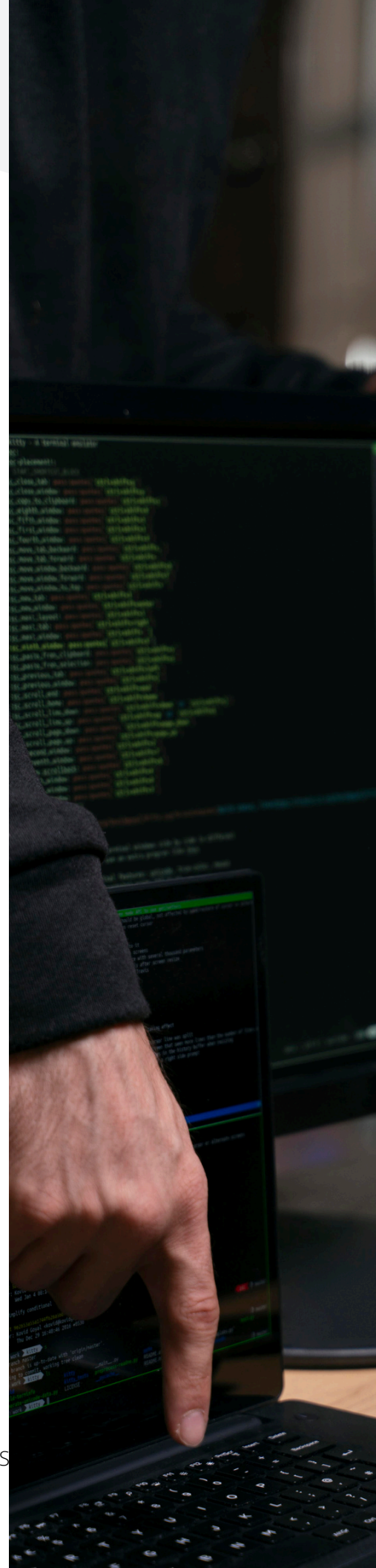
- Comprenderá y aplicará técnicas avanzadas de análisis de seguridad.
- Identificará y evaluará amenazas y vulnerabilidades en sistemas y redes.
- Implementará prácticas de seguridad efectivas para proteger la integridad de los datos.
- Detectará y responder a incidentes de seguridad en tiempo real.
- Participará en actividades de cumplimiento y seguridad empresarial.
- Desarrollará planes y políticas de seguridad específicas para organizaciones.

Incluye

- Clases en vivo.
- Videos tutoriales.
- Recursos descargables.
- Acceso en diferentes dispositivos.
- Actividades para desarrollar habilidades.
- Autoevaluación de habilidades.
- Tutores online para resolver tus dudas.
- Asesoría en el plan de tu desarrollo personal y profesional
- Certificado de participación.

¿Qué necesitas?

- Computador o tablet.
- Acceso a internet.



Unidad I: Fundamentos de Ciberseguridad Avanzada

- **Conceptos avanzados de seguridad cibernética**
 - Amenazas y tendencias actuales.
 - Principios de seguridad avanzados.
 - Introducción a la seguridad en la nube.
- **Análisis avanzado de amenazas**
 - Análisis de malware y técnicas de evasión.
 - Análisis de tráfico de red.
 - Identificación de indicadores de compromiso (IoC).
- **Herramientas avanzadas de seguridad**
 - Uso de SIEM (Gestión de Eventos e Información de Seguridad).
 - Herramientas de detección y respuesta avanzada.
 - Automatización de tareas de seguridad.
- **Políticas y normativas de seguridad avanzadas**
 - Cumplimiento normativo avanzado.
 - Creación de políticas de seguridad personalizadas.
 - Seguridad en entornos virtuales y en la nube.

Unidad II: Análisis de Vulnerabilidades y Amenazas

- **Identificación de amenazas y vulnerabilidades**
 - Evaluación de riesgos y amenazas.
 - Metodologías de pruebas de vulnerabilidad.
 - Análisis de sistemas y redes.
- **Evaluación de sistemas y aplicaciones**
 - Pruebas de penetración avanzadas.
 - Identificación de vulnerabilidades de seguridad.
 - Herramientas y técnicas de evaluación de aplicaciones.
- **Gestión de vulnerabilidades**
 - Priorización y gestión de vulnerabilidades.
 - Informe y seguimiento de vulnerabilidades.
 - Automatización de escaneos de seguridad.
- **Políticas y procedimientos de seguridad**
 - Políticas de seguridad de aplicaciones.
 - Pruebas de seguridad y revisión de código.
 - Auditorías de seguridad avanzadas.



Unidad III: Detección y Respuesta a Incidentes

- **Detección de amenazas en tiempo real**
 - Detección de intrusos y sistemas de prevención de intrusiones (IPS).
 - Análisis de registros y eventos de seguridad.
 - Creación de reglas de detección.
- **Respuesta a incidentes**
 - Planificación de respuesta a incidentes.
 - Escalación y contención de incidentes.
 - Recuperación de sistemas y datos.
- **Investigación de incidentes**
 - Análisis forense de sistemas y redes.
 - Recopilación de evidencia y cadena de custodia.
 - Presentación de informes de incidentes.
- **Simulacros de incidentes**
 - Escenarios de simulación de incidentes reales.
 - Evaluación y mejora de la respuesta a incidentes.
 - Comunicación y coordinación de equipos.

Unidad IV: Operaciones de Seguridad

- **Configuración y gestión de seguridad**
 - Configuración de sistemas y dispositivos seguros.
 - Control de acceso y autenticación avanzada.
 - Monitoreo de seguridad y alertas.
- **Administración de amenazas y eventos**
 - Análisis y evaluación de eventos de seguridad.
 - Gestión de registros y registros de seguridad.
 - Políticas y procedimientos de seguridad.
- **Seguridad en la nube y virtualización**
 - Consideraciones de seguridad en la nube.
 - Virtualización segura.
 - Cumplimiento en entornos virtuales.
- **Protección de la red**
 - Protección avanzada contra amenazas en la red.
 - Firewall avanzado y técnicas de filtrado.
 - Segmentación de red y políticas de seguridad.



Unidad V: Cumplimiento y Seguridad Empresarial

- **Cumplimiento y regulaciones**
 - Normativas de seguridad cibernética.
 - Evaluación de cumplimiento y auditoría.
 - Gestión de riesgos y cumplimiento.
- **Políticas y procedimientos empresariales**
 - Desarrollo y revisión de políticas de seguridad.
 - Planificación y gestión de políticas de seguridad.
 - Educación y concienciación de seguridad.
- **Estrategias de seguridad empresarial**
 - Continuidad del negocio y recuperación de desastres.
 - Implementación de medidas de seguridad avanzadas.
 - Seguridad en la cadena de suministro.
- **Simulacro de auditoría y cumplimiento**
 - Simulacro de auditoría de seguridad.
 - Pruebas de cumplimiento y revisión.
 - Preparación para exámenes de certificación.

Soluciones empresariales

- Presencial o virtual
- Grupos online 6+ participantes
- InHouse desde 10 participantes
- Contenidos personalizados
- Plataforma interactiva moderna

Modalidad

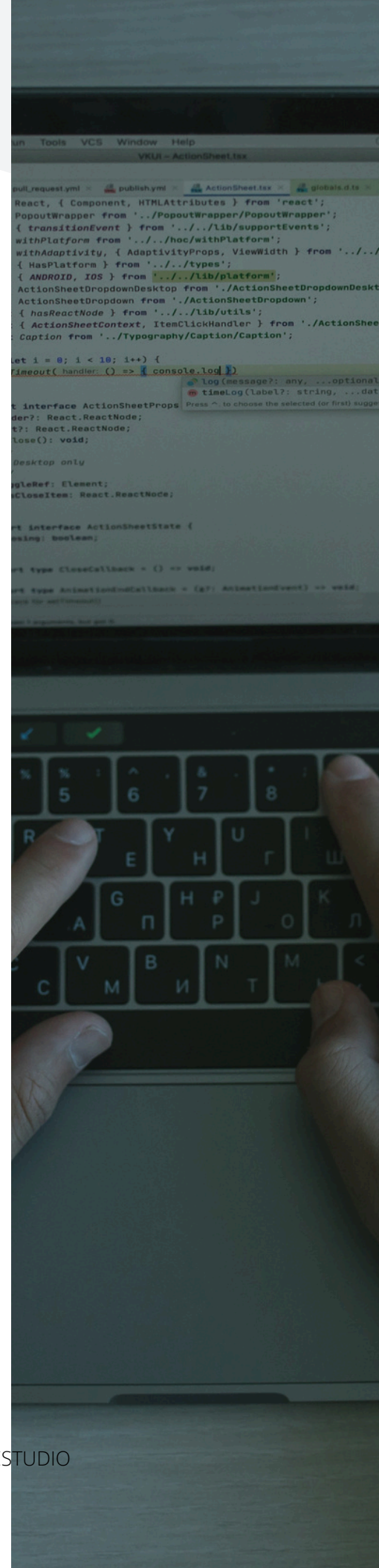
100% Virtual

Duración

6 semanas

Inversión

RD\$27,500.00



Transacciones bancarias

Banreservas: Cuenta corriente: 9601879916 a nombre de CI Comunicación Integral, SRL.

RNC: 131805851.

Correo electrónico: ci.comunicacionintegral@gmail.com

**Para completar el proceso de inscripción debes enviar el comprobante de la transacción vía correo electrónico, indicando tu nombre, datos del curso pagado.*

Contacto

Oficina: 809-476-9975

WhatsApp: 829-773-9975

Calle Ana Teresa Paradas No. 10, Mirador Sur, Santo Domingo, República Dominicana.

Certificado

En el **Curso de CompTIA CySA+** te puede certificar cuando completes los reportes de actividades y estudios de casos, desarrollo de proyecto que evidencian los conocimientos adquiridos.

