



SANS SEC504: Hacker Tools, Techniques, and Incident Handling

Descrición

SEC504 axúdalle a desenvolver as habilidades necesarias para levar a cabo investigacións de resposta a incidentes. Aprenderá a aplicar un proceso dinámico de resposta a incidentes ás ciberamenazas en evolución e a desenvolver intelixencia sobre ameazas para montar estratexias de defensa eficaces para plataformas na nube e locais. Examinará as ameazas máis recentes para as organizacións, desde os ataques de "watering hole" ata o compromiso do correo electrónico empresarial, introducíndolle na mentalidade das/os atacantes e anticipándose aos seus movementos. SEC504 proporciónalle as habilidades que necesita para comprender como as/os atacantes exploran, explotan, pivotan e establecen persistencia en sistemas na nube e convencionais. Para reforzar estas habilidades e axudarlle a reter o material do curso, o 50% do tempo de clase dedícase a exercicios prácticos, utilizando ferramentas de asociación visual para desagregar temas complexos. Este curso, prepáralle para levar a cabo ciber investigacións e impulsará a súa

carreira axudándolle a desenvolver estas habilidades tan demandadas. 33 laboratorios completos, 18 lightning labs e un evento inmersivo de captura a bandeira.

Aprenderá:

- Como aplicar un enfoque dinámico a resposta a incidentes
- Como identificar ameazas mediante o análise rede e análise de rexistros
- As mellores prácticas para unha resposta a incidentes na nube
- Procesos de investigación cibernética, análise en vivo, coñecemento da rede forense
- Estratexias de defensa para protexer activos críticos
- Técnicas dos atacantes para eludir endpoint
- Como aproveitan os atacantes as vulnerabilidades da nube
- Pasos do atacante para o descubrimento interno e o movemento lateral despois dun inicial
- Os ataques máis eficaces para eludir os

controles de acceso ao sistema

- As técnicas astutas que utilizan os atacantes e como detelos

A certificación GIAC Incident Handler (GCIH):

- valida la capacidad de una/un profesional para detectar, responder y resolver incidentes de seguridad informática utilizando una amplia gama de habilidades esenciales de seguridad. Las/os titulares de la certificación GCIH tienen los conocimientos necesarios para gestionar incidentes de seguridad mediante la comprensión de las técnicas de ataque comunes, vectores y herramientas, así como defenderse y responder a tales ataques cuando se producen

- prepara para la gestión de incidentes e investigación de delitos informáticos
- enseña exploits de hackers informáticos y de redes

- enseña herramientas de hacker (Nmap, Metasploit y Netcat)

Exame de certificación:

- 1 proctored exam

- 106 preguntas
- 4 horas
- Calificación mínima de aprobado 69%

A docencia do curso, o material asociado e maila certificación se desenvolverán en inglés.

Obxectivos

O obxectivo dos sistemas modernos na nube e nas instalacións é evitar o perigo, pero a realidade é que a detección e a resposta son fundamentais. Manter á súa organización fóra dos titulares de infraccións depende do ben que se xestionen os incidentes para minimizar as perdas para a empresa.

En SEC504, aprenderá a aplicar un enfoque dinámico á resposta ante os incidentes. Utilizando indicadores de compromiso, practicará os pasos para responder eficazmente as brechas que afectan a Windows, Linux e plataformas na nube. Poderá levar á oficina as habilidades e a experiencia práctica adquiridas no curso e aplicalas inmediatamente.

O curso céntrase na aplicación do aprendido mediante exercicios prácticos: o 50% do curso é práctico; nel atacará, defenderá e avaliará os danos causados polos causantes das ameazas. Traballará con contornas de rede complexas, plataformas e aplicacións host do mundo real e conxuntos de datos complexos que reflicten o tipo de traballo que se lle pode pedir que realice. Nunca perderá o acceso aos exercicios de laboratorio e poderá repetilos tantas veces como desexe. Todos os exercicios de laboratorio veñen acompañados de vídeos detallados que lle axudarán a reforzar os conceptos aprendidos no curso.

Comprender os pasos para levar a cabo eficazmente a resposta a incidentes é só unha parte da ecuación. Para comprender plenamente as accións que as/os atacantes levan a cabo contra unha organización, tamén é necesario entender as súas ferramentas e técnicas. Na contorna práctica proporcionada por SEC504, utilizará as mesmas ferramentas que os atacantes para comprender como se aplican e os artefactos que deixan tras de si. Ao entrar na mentalidade dos atacantes, aprenderá como aplican as súas tácticas, técnicas e procedementos contra a súa organización; e poderá utilizar esa información para anticiparse aos seus movementos e construír mellores defensas.

Dirixido a

- Xestoras/es de incidentes
- Personais responsables de equipos de xestión de incidentes
- Administradoras/es de sistemas en primeira liña defendendo os seus sistemas e responden os ataques
- Outro persoal de seguridade que son os primeiros en responder cando son atacados
- Profesionais da seguridade en xeral e arquitectos de seguridade que desexen deseñar, construír e operar os seus sistemas para previr, detectar e responder os ataques

BENEFICIOS

Diploma de asistencia

Opción gratuita dun exame de certificación oficial

Perfil do docente

Chris Dale, comezou a súa carreira en 2009 traballando para un importante provedor de servizos da internet noruegués, onde se encargaba do desenvolvemento e as operacións de TI. Desde entón, traballou para varias empresas en postos importantes, e o seu último posto foi como xefe de ciberseguridade nunha consultora de ciberseguridade de 60 persoas. Alí, dirixiu varios equipos, incluíndo probas de penetración e resposta a incidentes. En 2020, Chris fundou a súa propia empresa, River Security, especializada en servizos ofensivos, xestión da superficie de ataque e ciberconsultoría.

Instrutor certificado de SANS e analista de SANS, Chris imparte as materias SEC504: Ferramentas, técnicas e xestión de incidentes de hackers e SEC599: Derrotar a adversarios avanzados: tácticas de equipo púrpura e defensas de cadea de ataque.

PROGRAMA

Programación 2026/27

TIPO

CURSO

MATRÍCULA

Gratuíta

PERIODO INSCRICIÓN

01/12/2026 - 15/12/2026

PROBA DE SELECCIÓN

16/12/2026 (00:00)

CRITERIOS DE SELECCIÓN

Proba técnica presencial no CNTG en Santiago de Compostela

Nº PRAZAS

10 (Mínimo 10)

METODOLOXÍA

Virtual

TIPO DE EDICIÓN

Edición única tarde (desempregados/as e ocupados/as)

DURACIÓN

50 horas

SANS SEC504: Hacker Tools, Techniques, and Incident Handling

DATA INICIO	18/01/2027
DATA FIN	23/01/2027
HORARIO	De luns a sábado de 10:00 a 18:00 horas. Luns de 9:30 a 20:
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	GIAC Certified Incident Handler (GCIH)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	SANS
	GIAC
	Ciberseguridade/Ciberseguridad
PERIODO DOCENCIA	18/01/2027 - 23/01/2027

Temario

- SECCIÓN 1. Resposta a incidentes e investigacións cibernética
- SECCIÓN 2. Ataques de recoñecemento, exploración e enumeración
- SECCIÓN 3. Ataques por contrasinal e acceso
- SECCIÓN 4. Ataques de fronte ao público e Drive-By
- SECCIÓN 5. Evasión e Ataques post-explotación
- SECCIÓN 6. Evento captura a bandeira