SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Descrición

As tácticas e procedementos de caza de ameazas e resposta a incidentes evolucionaron rapidamente nos últimos anos. O seu equipo xa non pode permitirse utilizar técnicas anticuadas de resposta a incidentes e caza de ameazas que non identifican correctamente os sistemas comprometidos. A clave está en buscar constantemente ataques que burlen os sistemas de seguridade e en atrapar as intrusións en curso, en lugar de facelo despois de que as/os atacantes completen os seus obxectivos e causen danos peores á organización. Para o persoal de resposta a incidentes, este proceso coñécese como "caza de ameazas". FOR508 ensina habilidades avanzadas para cazar, identificar, contrarrestar e recuperarse dunha ampla gama de ameazas dentro das redes empresariais, incluíndo adversarios APT nación-estado, sindicatos do crime organizado e operadores de ransomeware.

O curso axudaralle a:

- Comprender as técnicas dos atacantes para realizar avaliacións de compromiso
- Detectar como e cando se produciu unha brecha
- Identificar rapidamente os sistemas comprometidos e infectados
- Realizar avaliacións de danos e determinar que se leu, roubado ou modificado
- Conter e remediar incidentes de todo tipo
- Rastrexar aos adversarios e desenvolver intelixencia sobre ameazas para delimitar unha rede
- Cazar novas brechas utilizando o coñecemento das técnicas dos adversarios
- Desenvolver habilidades forenses avanzadas para contrarrestar as técnicas antiforense e a ocultación de datos dos suxeitos técnicos

Os exercicios do curso e os desafíos finais ilustran rastros reais de atacantes atopados a través de artefactos de punto final, rexistros de eventos, memoria do sistema, etc.:

- Fase 1: compromiso cero do paciente e instalación de balizas C2 de malware
- Fase 2: elevación de privilexios, movemento lateral a outros sistemas, descarga de utilidades de malware, instalación de balizas adicionais e obtención de credenciais de administrador de dominio
- Fase 3: procura de propiedade intelectual, creación de perfís de rede, compromiso do correo electrónico empresarial, envorcado de hashes empresariais
- Fase 4: atopar o punto de exfiltración, recompilar e preparar os datos para o roubo
- Fase 5: exfiltración de arquivos do servidor de montaxe, limpeza e establecemento de mecanismos de persistencia a longo prazo (alternativamente, esta fase utilizaríase para despregar ransomware)

A certificación GIAC Certified Forensic Analyst (GCFA) centrase en:

- As competencias básicas necesarias para recompilar e analizar datos de sistemas informáticos.

As/os candidatas/os teñen os coñecementos, as habilidades e a capacidade para levar a cabo investigacións formais de incidentes e manexar escenarios avanzados de xestión de incidentes, incluídas intrusións internas e externas de violación de datos, ameazas persistentes avanzadas, técnicas antiforense utilizadas polos atacantes e casos forenses dixitais complexos

- Dar resposta avanzada a incidentes e análises forense dixital
- Análise forense de memoria, análise de liñas de tempo e detección antiforense
- Caza de ameazas e resposta a incidentes de intrusión APT

Examen: existen dúas opcións de avaliación: avaliación remota a través de ProctorU e avaliación in situ a través de PearsonVUE

- 1 proctored exam
- 82 preguntas
- 3 horas
- Calificación mínima de aprobado 71%

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

Obxectivos

- Aprender e dominar as ferramentas, técnicas e procedementos necesarios para detectar e conter unha variedade de adversarias/os e solucionar incidentes
- Detectar e cazar malware descoñecido vivo, latente e personalizado en memoria en varios sistemas Widows nun contorna empresa
- Buscar e responder a incidentes en centos de sistemas simultaneamente con F-Response Enterprise e a estación de traballo SIFT
- Identificar e rastrexar o malware cara á súa canle de mando e control (C2) mediante análises forenses e residuos de conexión de rede
- Determinar como se produciu a brecha identificando a cabeza de praia e os phishing - Identifique as técnicas de "vivir da terra" incluíndo o uso malicioso de PowerShell e WMI
- Apuntar a técnicas antiforense avanzadas da/o adversario como o malware oculto xunto coas técnicas utilizadas para moverse na rede e manter a presenza dun atacante
- Utilizar análise de memoria, resposta a incidentes e ferramentas de caza de ameazas en SIFT Workstation para detectar procesos ocultos, malware, liñas de comandos de atacantes, rootkits, conexións de rede etc.
- Rastrexar a actividade de usuarias/os e atacantes segundo a segundo no sistema que está a analizar mediante a análise en profundidade da liña de tempo e a superlínea de tempo
- Recuperar datos borrados mediante técnicas antiforense Volume Shadow Copy/ Análises de puntos de restauración
- Identificar o movemento lateral e os pivotes dentro da súa empresa a través das súas endpoints, mostrando como os atacantes se trasladan dun sistema a outro sen detección
- Comprender como a/o atacante pode adquirir credenciais lexítimas, incluídos os de dominio, mesmo nunha contorna bloqueada
- Rastrexar o movemento de datos a medida que as/os atacantes recompilan datos críticos e trasládanos a puntos de exfiltración
- Recuperar os datos borrados mediante técnicas antiforenses mediante a análise de Volume Shadow Copy e análise de puntos de restauración e esculpido de artefactos
- Utilizar os datos recompilados de forma efectiva en toda a empresa

Dirixido a

- Xestoras/es de incidentes
- Personas 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

Jess Garcia é o fundador e director técnico de One eSecurity, unha empresa global de seguridade da información especializada en resposta a incidentes e análise forense dixital. Jess é hoxe un experto en análise forense dixital e ciberseguridade recoñecido internacionalmente, liderando a resposta e a investigación forense dalgúns dos incidentes máis graves do mundo nos últimos tempos.

Jess, instrutor sénior de SANS con case 15 anos de experiencia, é tamén relator convidado habitual en conferencias de seguridade e DFIR en todo o mundo. É membro do profesorado do Instituto de Tecnoloxía SANS, un Centro de Excelencia Académica en Ciberdefensa da NSA e gañador en múltiples ocasións da liga Nacional de Ciberseguridade.

PROGRAMA Programación 2026/27

TIPO CURSO

MATRÍCULA Gratuíta

PERIODO INSCRICIÓN 01/02/2027 - 15/02/2027

PROBA DE SELECCIÓN 16/02/2027 (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	48 horas
DATA INICIO	15/03/2027
DATA FIN	20/03/2027
HORARIO	De luns a sábado de 09:00 a 17:00 horas. O luns comeza ás 8:
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	GIAC Certified Forensic Analyst (GCFA)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	GIAC Ciberseguridade/Ciberseguridad SANS
PERIODO DOCENCIA	15/03/2027 - 20/03/2027

Temario

- SECCIÓN 1: Resposta avanzada a incidentes e caza de ameazas
- SECCIÓN 2: Análise de intrusións

- SECCIÓN 3: Análise forense da memoria na resposta a incidentes e a caza de ameazas
- SECCIÓN 4: Análise da liña de tempo
- SECCIÓN 5: Resposta a incidentes e caza en toda a empresa | Detección avanzada de adversarios e antiforense
- SECCIÓN 6: O desafío de resposta a incidentes do grupo de ameazas APT