Publicatiedatum : 16/01/2024

Opleiding : Cursus SOC (Security Operations Center) Analist

Praktijkcursus - 8d - 56u00 - Ref. ASR
Prijs : 4570 € V.B.

BEST

Na afronding van de cursus is de cursist in staat om de taken van een Security Operations Centre (SOC) analist uit te voeren, voornamelijk het detecteren en analyseren van inbraken, hierop te anticiperen en de benodigde bescherming in te stellen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- De organisatie van een SOC begrijpen
- De functie van SOC-analist begrijpen
- Inzicht in de tools die SOC-analisten gebruiken
- De belangrijkste problemen identificeren aan de hand van use cases
- Leren om inbraken te detecteren
- Incidenten beheren
- De beveiliging van een informatiesysteem optimaliseren

Doelgroep

Systeem- en netwerktechnici en -beheerders, IT-managers, beveiligingsconsultants, ingenieurs, technische managers, netwerkarchitecten, projectmanagers, enz.

Voorafgaande vereisten

Bekendheid met de ANSSI-beveiligingsgids, kennis van netwerken, afronding van de inleidende cursus cyberbeveiliging of gelijkwaardige kennis.

DEELNEMERS

Systeem- en netwerktechnici en -beheerders, IT-managers, beveiligingsconsultants, ingenieurs, technische managers, netwerkarchitecten, projectmanagers, enz.

VOORAFGAANDE VEREISTEN

Bekendheid met de ANSSI-beveiligingsgids, kennis van netwerken, afronding van de inleidende cursus cyberbeveiliging of gelijkwaardige kennis.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

Praktische modaliteiten

Praktisch werk

Veel praktisch werk over het opzetten en gebruiken van SOC-analysetools, inbraakdetectie, de meest voorkomende problemen en analyse na een incident.

Composition de la formation

SOC-analist, de baan

Ref. ASH - 2 dagen ★ 4 / 5

Logboeken verzamelen en analyseren, een SIEM om de beveiliging van uw informatiesysteem te optimaliseren

Ref. LCA - 3 dagen ★ 4 / 5

Forensische analyse

Ref. AFB - 3 dagen ★ 4 / 5

Opleidingsprogramma

1 Het SOC (Beveiligingscentrum)

- Wat is een SOC?
- Waar wordt het voor gebruikt? Waarom gebruiken steeds meer bedrijven het?
- SOC-functies: logging, monitoring, audit en beveiligingsrapportage, analyse na een incident.
- De voordelen van een SOC.
- Oplossingen voor een SOC.
- SIM (Security Information Management).
- SIEM (Security Information and Event Management).
- SEM (Security Event Management).
- Voorbeeld van een monitoringstrategie.

2 De taak van de SOC-analist

- Wat doet een SOC-analist?
- Welke vaardigheden heeft het?
- Waarschuwingen en gebeurtenissen bewaken en sorteren.
- Prioriteit geven aan waarschuwingen.

3 Informatie verzamelen

- De heterogeniteit van bronnen. Wat is een veiligheidsgebeurtenis?
- Informatiebeheer beveiligingsgebeurtenissen (SIEM). Gebeurtenissen verzameld uit de IS.
- Systeemlogs van apparatuur (firewalls, routers, servers, databases, etc.).
- Passief verzamelen in luistermodus en actief verzamelen.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

4 IS-beveiliging optimaliseren: tools, best practices, te vermijden valkuilen

- Overzicht van oplossingen en producten.
- Syslog.
- De SEC.
- Splunk-software.
- Franse wetgeving.

5 Inbraakdetectie, de belangrijkste problemen

- Een goed begrip van netwerkprotocollen (TCP, UDP, ARP, ICMP, routers, firewalls, proxies, etc.).
- Aanvallen op TCP/IP (spoofing, denial of service, session theft, SNMP aanvallen, etc.).
- Inlichtingen verzamelen, sporen zoeken, netwerkscans.
- Trojaanse paarden, backdoors, browser bugs, "geheime kanalen", gedistribueerde denial of service agents...
- Aanvallen en uitbuiten van kwetsbaarheden (overname, DDoS, buffer overflow, RootKits, enz.).

6 Hoe ga je om met een incident?

- De tekenen van een succesvolle IS-inbraak.
- Wat hebben de hackers bereikt? Hoe ver zijn ze gekomen?
- Hoe reageer je op een succesvolle inbraak?
- Welke servers worden beïnvloed?
- Zoek het ingangspunt en vul het.
- De Unix/Windows gereedschapskist voor het vinden van bewijs.
- Opschonen en terugbrengen naar productie van gecompromitteerde servers.

7 Incidenten analyseren voor betere bescherming: forensische analyse

- Forensisch computeronderzoek: soorten computercriminaliteit, rol van de computeronderzoeker.
- Moderne cybercriminaliteit.
- Digitaal bewijs.

8 Forensische analyse van een Windows-besturingssysteem

- Verwerving, analyse en reactie.
- Inzicht in opstartprocessen.
- Vluchtige en niet-vluchtige gegevens verzamelen.
- Hoe het wachtwoordsysteem en het Windows-register werken.
- Analyse van gegevens in RAM- en Windows-bestanden.
- Analyse van cache-, cookie- en browsegeschiedenis, gebeurtenisgeschiedenis.

Data en plaats

KLAS OP AFSTAND
2026 : 21 mei, 25 juni, 1 okt., 5 nov.

PARIS LA DÉFENSE
2026 : 5 maa., 21 mei, 25 juni, 1 okt., 5 nov.