

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

Praktijkcursus - 3d - 21u00 - Ref. LCA

Prijs : 2100 € V.B.



4,3 / 5

In deze cursus krijg je een overzicht van toezichtkwesties, de wettelijke verplichtingen die komen kijken bij het bewaren van gegevens en kun je snel de vaardigheden onder de knie krijgen die nodig zijn om een softwareoplossing te implementeren die is afgestemd op jouw behoeften.



Pedagogische doelstellingen

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

- ✓ De wettelijke verplichtingen met betrekking tot gegevensbewaring kennen
- ✓ Weten hoe je een logboekanalyse uitvoert
- ✓ Syslog installeren en configureren
- ✓ Inzicht in correlatie en analyse met SEC

Doelgroep

Systeem- en netwerkbeheerders.

Voorafgaande vereisten

Goede kennis van netwerken, systemen en IS-beveiliging.

Praktische modaliteiten

Gedurende de hele cursus worden talloze oefeningen en casestudy's aangeboden.

Opleidingsprogramma

DEELNEMERS

Systeem- en netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van netwerken, systemen en IS-beveiliging.

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.

1 Informatie verzamelen

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

Praktisch werk

Loganalyseprocedure. Een adres geolokaliseren. Logs van verschillende bronnen correleren, bekijken, sorteren en zoeken naar regels.

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

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

Praktisch werk

Installatie en configuratie van Syslog, SEC, Splunk, ELK en andere. Voorbeeld van gegevensanalyse en -correlatie.

3 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 bug exploits, geheime kanalen, distributed denial of service agents, enz. detecteren.
- Aanvallen en uitbuiten van kwetsbaarheden (overname, DDoS, buffer overflow, rootkits, enz.).

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.

Data en plaats

KLAS OP AFSTAND

2026 : 1 juni, 9 sep., 5 okt., 16 nov.

PARIS LA DÉFENSE

2026 : 1 juni, 9 sep., 5 okt., 16 nov.