Publicatiedatum : 02/05/2024

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

Praktijkcursus - 2d - 14u00 - Ref. LOG
Prijs : 1480 € V.B.

Deze training geeft je een overzicht van toezichtkwesties, de wettelijke verplichtingen die komen kijken bij het bewaren van gegevens en de vaardigheden die je nodig hebt om snel 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

Praktisch werk

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 Inleiding

- Beveiliging van informatiesystemen.
- Toezicht en registratie.
- Standaardisatieopties.
- Wat zijn de voordelen van gecentraliseerd toezicht?
- Marktoplossingen.

2 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.

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

3 Syslog

- Het Syslog-protocol.
- Het clientgedeelte en het servergedeelte.
- Gebeurtenislogs centraliseren met Syslog.
- Is Syslog voldoende? Voor- en nadelen.

Praktisch werk
Syslog installeren en configureren. Voorbeeld van gegevensanalyse en correlatie.

4 Het SEC-programma

- Presentatie van SEC (Simple Event Correlator).
- Het configuratiebestand en de regels.
- Hoe zie je interessante patronen?
- Correlatie en analyse met SEC.

Praktisch werk
Installatie en configuratie van SEC. Voorbeeld van gegevensanalyse en correlatie.

5 Splunk-software

- MapReduce architectuur en framework. Hoe verzamel en indexeer je gegevens?
- Machinegegevens exploiteren. Verificatie van transacties.
- Integratie met LDAP-directory's en Active Directory-servers.
- Andere software op de markt: Syslog, SEC (Simple Event Correlator), ELK (Elastic suite), Graylog, OSSIM, enz.

Praktisch werk
Software installeren en configureren (Splunk, ELK of andere). Voorbeeld van gegevensanalyse en correlatie.

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.

6 Franse wetgeving

- Hoe lang logboeken worden bewaard. Kader voor gebruik en wetgeving. De CNIL. Arbeidsrecht.
- Het IT-charter, de inhoud ervan en het validatieproces.
- Hoe stel je een IT-charter op?
- De bijdrage aan de veiligheidsketen.

Praktisch werk
Voorbeeld van een IT-charter.

7 Conclusie

- Goede praktijken. Te vermijden valkuilen. De juiste hulpmiddelen kiezen. De toekomst van deze toepassingen.

Data en plaats

KLAS OP AFSTAND
2026 : 22 juni, 5 okt., 16 nov.

PARIS LA DÉFENSE
2026 : 22 juni, 5 okt., 16 nov.