Publicatiedatum : 05/02/2024

Opleiding : IBM QRadar SIEM, de basis

Praktijkcursus - 3d - 21u - Ref. IBF
Prijs : 2100 € V.B.

QRadar is een event correlatie tool voor het verzamelen en sorteren van relevante informatie gegenereerd door verschillende beveiligingsapparaten. In deze cursus kun je de toepassing configureren, de gegevensstroom analyseren en rapporten genereren op basis van vooraf geconfigureerde waarschuwingen.

Pedagogische doelstellingen

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

- Gegevens verzamelen, analyseren en rapporteren met QRadar
- Verrijk operationele gegevens met zoekopdrachten en feeds
- Real-time waarschuwingen aanmaken
- Rapporten genereren

Doelgroep

Systeem- en netwerkbeheerders.

Voorafgaande vereisten

Basiskennis van netwerken en systemen.

Opleidingsprogramma

1 De SIEM

- Wat is een SIEM (Security Information Event Management)?
- Waarom moeten gebeurtenissen worden gecorreleerd?
- SIEM-tools op de markt.

DEELNEMERS

Systeem- en netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Basiskennis van netwerken en systemen.

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.

2 QRadar architectuur en interface

- Presentatie en positionering van de QRadar-tool.
- Hoe QRadar SIEM configureren om gegevens te verzamelen.
- Leer hoe je verdachte activiteiten kunt detecteren.
- De architectuur en componenten van QRadar SIEM en de gegevensstroom.
- De QRadar gebruikersinterface.

Praktisch werk
De QRadar interface onder de knie krijgen.

3 Analyse en zoeken naar verdachte acties

- Onderzoek verdachte aanvallen.
- Zoeken naar inbreuken op het beveiligingsbeleid.
- Veiligheidsgegevens zoeken, filteren, groeperen en analyseren.
- Gebeurtenissen en stromen analyseren.
- Onderzoek activaprofielen.

Praktisch werk
Zoek naar aanvallen of overtredingen van het beveiligingsbeleid. Maak realtime waarschuwingen.

4 Regels en indexbeheer

- Waarom de netwerkhiërarchie.
- Bepaal hoe de regels binnenkomende gegevens onderzoeken en overtredingen creëren.
- Hoe indexen en geaggregeerd gegevensbeheer te gebruiken.

Praktisch werk
Inkomende gegevens onderzoeken en overtredingen maken. Regels en indexen gebruiken.

5 Dashboards

- Dashboardbeheer.
- De verschillende elementen van een dashboard.
- Hoe beweeg ik tussen dashboards?
- Dashboards en hun elementen aanpassen.

Praktisch werk
Aanpasbare dashboards.

6 Rapporten

- Presentatie van verslagen.
- Algemene parameters.
- De verschillende objecten in een rapport en hun parameters.
- Rapporten op maat maken.

Praktisch werk
Rapporten maken en gebruiken.

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.

7 Filters en geavanceerd zoeken

- Filters zijn beschikbaar en kunnen snel worden gebruikt.
- Gebruik filters om te zoeken.
- Gebruik van AQL (Ariel Query Language) voor geavanceerde zoekopdrachten.

Praktisch werk
Filters instellen en geavanceerde zoekopdrachten gebruiken.

Data en plaats

KLAS OP AFSTAND
2026 : 22 juni, 7 okt., 16 nov.

PARIS LA DÉFENSE
2026 : 22 juni, 7 okt., 16 nov.