PARCOURS COMPÉTENCES+

SOC-ANALIST (SECURITY OPERATIONS CENTER)

Cours pratique de 10 jours

NEW

Prix : 5100 € V.B.

DESCRIPTION

Deze gecertificeerde opleiding heeft tot doel de deelnemers op te leiden voor de belangrijkste taken van een SOC-analist, van het begrijpen van de uitdagingen op het gebied van cyberbeveiliging tot het opsporen, analyseren en beheren van beveiligingsincidenten. Het is gebaseerd op een gestructureerd leertraject, meeslepende workshops en actieve tussensessies ter voorbereiding op de eindcertificering.

DOELGROEP

SOC-analisten, beveiligingsingenieurs, CERT/CSIRT-teams en adjunct-CISO's, evenals beveiligingsverantwoordelijken die hun operationele werkwijzen willen versterken.

PEDAGOGISCHE DOELSTELLINGEN

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

- Inzicht krijgen in de uitdagingen op het gebied van cyberbeveiliging en de strategische rol van een SOC
- Beveiligingsincidenten opsporen, analyseren en classificeren
- Een passende reactie op incidenten implementeren
- De werking van een SOC voortdurend verbeteren
- Anticiperen op bedreigingen dankzij Threat Intelligence
- Een praktijkvoorbeeld in een SOC-context presenteren en onderbouwen

VOORAFGAANDE VEREISTEN

Beschikken over basiskennis op het gebied van systemen, netwerken en cyberbeveiliging, en vertrouwd zijn met IT-tools en het lezen van logbestanden.

FINANCIERINGSOPLOSSINGEN

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.

Découvrez-les sur notre page :
Comment financer sa formation ou contactez votre conseiller formation

TIJDROOSTERS

DE OPLEIDINGEN VINDEN PLAATS VAN 9.00 TOT 17.30 UUR, MET EEN LUNCHPAUZE VAN 1 TOT 1,5 UUR.

Voor praktische stages van 4 of 5 dagen, ongeacht de modaliteit, worden de sessies de laatste dag om 16.00 uur afgesloten..

DEELNEMERS

SOC-analisten, beveiligingsingenieurs, CERT/CSIRT-teams en adjunct-CISO's, evenals beveiligingsverantwoordelijken die hun operationele werkwijzen willen versterken.

VOORAFGAANDE VEREISTEN

Beschikken over basiskennis op het gebied van systemen, netwerken en cyberbeveiliging, en vertrouwd zijn met IT-tools en het lezen van logbestanden.

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.

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.

POURQUOI CHOISIR LE PARCOURS
SOC-analist (Security Operations Center)

Stap over van reactieve monitoring naar proactieve detectie van bedreigingen

- Beveiligingsincidenten sneller opsporen en analyseren
- De reactietijden verkorten en de betrouwbaarheid van de diagnoses vergroten
- Zijn activiteiten doeltreffend afstemmen met de beveiligings- en IT-teams
- De operationele tools en processen van een SOC onder de knie krijgen

Een concreet stappenplan om uw operationele effectiviteit tegen bedreigingen te versterken

VOTRE CERTIFICATION

Certificering Compétences+

01

CERTIFICERINGSVOORWAARDEN

De Compétences+-certificering voor SOC-analisten vindt uitsluitend plaats aan het einde van de opleiding, tijdens de eendaagse certificerin opdrachten die tijdens de tussentijdse sessies worden uitgevoerd, stellen de kandidaat in staat om zich geleidelijk voor te bereiden op zijn eindpresen Deze opdrachten worden niet beoordeeld met een cijfer.terugkarrenbuitenlijnt terugkarrenbuitenlijn

02

VERLOOP VAN DE BEOORDELINGTERUGKARRENBUITENLIJNDE BEOORDELING IS GEBASE DE MONDELINGE PRESENTATIE VAN EEN RODE DRAAD VORMENDE PRAKTIJKCASE, OPGEBOUWD UIT DE SITUATIES EN OPDRACHTEN DIE TIJDENS DE OPLEIDING ZIJN UITGEVOERD.TERUGWAGENTJESOVERSLAANDE KANDIDAAT PRESENTEERT MET NAME: I CONTEXT EN DE VEILIGHEIDSUITDAGINGEN, DE WAARGENOMEN ELEMENTEN EN DE GEÏDENTIFICEERDE WAARSCHUWINGEN, DE ANALYSE EN KWALIFICATIE VAN HET INCID VOORGESTELDE REACTIEMAATREGELEN, DE CORRIGERENDE MAATREGELEN EN DE VERBETERINGSMOGELIJKHEDEN, DE LESSEN DIE UIT DE CASESTUDIE ZIJN GETROKKEN.TERUGKARRENLIJNOVERSCHRIJDINGTERUGKARRENLIJNOVERSCHRIJDING GESPREKKEN MET DE JURYTERUGKARRENLIJNOVERSCHRIJDINGNA AFLOOP VAN DE PRESENTATIE GAAT DE KANDIDAAT IN GESPREK MET DE JURY.TERUGWAGENTJESLIJNOVERSLAANDEZE GESPREKKEN BIEDEN DE MOGELIJKHEID ANALYSE TE VERDIEPEN, NA TE GAAN OF DE KANDIDAAT ZIJN KEUZES GOED KAN ONDERBOUWEN EN TE BEOORDELEN IN HOEVERRE HIJ DE VAARDIGHEDEN BEHEERST D EEN OPERATIONELE SOC-CONTEXT WORDEN INGEZET.TERUGCARETSPRINGREGTERUGCARETSPRINGREG VOORBEREIDENDE WERKZAAMHEDENTERUGCARETSPRINGREGDE TIJDENS DE TUSSENT SESSIES VERVAARDIGDE DOCUMENTEN VORMEN EEN WERKBASIS VOOR DE EINDPRESEI MET NAME: INCIDENTRAPPORTEN, ALARMANALYSES, ONDERZOEKSLOGBOEKEN, RAPPC NA EEN INCIDENT, ERVARINGEN DIE ZIJN TERUGGEKOPPELD, EN MONITORINGWERKZAAMHEDEN MET BETREKKING TOT OPKOMENDE BEDREIGINGEN.TI NAAR BOVEN

03

04

MON PARCOURS

DISPOSITIF PÉDAGOGIQUE HYBRIDE :

5 modules, 4 inter-sessions répartis sur 4 à 5 mois

- **Module** : Sessions en présentiel et distanciel
- **Inter-session** : Travaux en autonomie + accompagnement + plateforme dédiée
- Un formateur référent + un ingénieur pédagogique ORSYS dédié à toute la coordination
- Un suivi individualisé, du démarrage au passage de la certification

MODULE 01
Cyberbeveiliging en de rol van het SOC

2 JOURS
- Meeslepende workshop: “De dag waarop alles op zijn kop kwam”.
- Overzicht van cyberbeveiliging.
- Samenwerkingsworkshop: “Wie ben ik?”.
- Rol en taken van het SOC.
- SOC-tools en -technologieën.
- Organisatie en operationele werking.
- Diagnostische workshop: “Zijn we er klaar voor?”.

INTER-SESSION

- Een echte of gesimuleerde beveiligingswaarschuwing of -gebeurtenis observeren en de belangrijkste aanwijzingen voor detectie identificeren.
- Een beknopt incidentrapport opstellen (symptomen, ernst, eerste maatregelen).
- De analyses van de deelnemers met elkaar vergelijken om goede praktijken en veelvoorkomende fouten in kaart te brengen.
- Een beknopt overzicht van de trainer ontvangen over de nauwkeurigheid van de diagnose en de relevantie van de detectie.

MODULE 02
Monitoring, detectie en analyse van incidenten

3 JOURS
- Meeslepende workshop: “De spookwaarschuwing”.
- Realtime monitoring en detectie.
- Samenwerkingsworkshop: “Op zoek naar het vals-positieve resultaat”.
- Analyse en beoordeling van waarschuwingen.
- Incidentbeheer en -communicatie.
- Praktische workshop: cyberbeveiliging in realtime in beeld brengen.

INTER-SESSION

- Een alarm opnieuw doornemen en de stappen voor de kwalificatie vastleggen (context, ernst, escalatie).
- Een onderbouwd oordeel vellen: „echte dreiging", „vals-positief" of „onvolledig incident".
- De genomen beslissingen vergelijken om de verschillen in interpretatie te begrijpen.
- De toelatingscriteria gezamenlijk aanpassen en de nauwkeurigheid van de analyse verbeteren.

MODULE 03
Incidentafhandeling en onderzoek

2 JOURS
- Interactieve workshop: "Cybercrisis live".
- Procedure voor het afhandelen van incidenten.
- Onderzoeksmiddelen en -technieken.
- Praktische workshop: "In de voetsporen van de piraat".
- Melding bij een incident.
- Samenwerkingsworkshop: "Communiceren onder druk".

INTER-SESSION

- Schrijf een onderzoeksverslag op basis van een echt of gesimuleerd incident.
- Een uittreksel van het rapport na het incident opstellen (samenvatting + belangrijkste lessen).
- De verschillen in onderzoeksmethoden tussen de deelnemers bespreken.
- Gepersonaliseerde feedback ontvangen over de duidelijkheid van het rapport en de relevantie van de conclusies.

MODULE 04
Voortdurende verbetering en Threat Intelligence

2 JOURS
- Meeslepende workshop: "De terugblik op de chaos".
- Voortdurende verbetering van het SOC.
- Threat Intelligence en het anticiperen op bedreigingen.
- Samenwerkingsworkshop: "Het oog van de inlichtingendienst".
- Simulatie van aanvallen en proactieve detectie.
- Praktische workshop: "Red Team vs Blue Team Challenge".

INTER-SESSION

- Een verslag opstellen over de opgedane ervaringen (fouten, corrigerende maatregelen, indicatoren).
- Een monitoringmelding publiceren over een opkomende dreiging (ransomware, kwetsbaarheid, nieuwe techniek).
- Reageer op de bijdragen van andere deelnemers om de gemeenschappelijke kennisbasis te verrijken.
- Deelnemen aan een gezamenlijke evaluatie van de doeltreffendheid van corrigerende maatregelen en gezamenlijke monitoring.

MODULE 05
Competence_Plus-certificering SOC-analist

1 JOUR
- Mondelinge presentatie van de praktijkcase die als rode draad dient.
- Gesprekken met de jury.

Praktisch werk :
De tijdens de tussentijdse bijeenkomsten gerealiseerde producties vormen een uitgangspunt voor de eindpresentatie.

CALENDRIER PROMO 2026

Dit programma is een origineel concept, ontwikkeld door de pedagogische teams van ORSYS Formation. Elke reproductie, weergave, aanpassing of exploitatie, geheel of gedeeltelijk, zonder voorafgaande schriftelijke toestemming van ORSYS, is ten strengste verboden. ORSYS behoudt zich het recht voor om alle nodige maatregelen te nemen ter bescherming van haar intellectuele-eigendomsrechten.