Opleiding : Red Team, Blue Team: inzicht in de methoden van je teams

Een duidelijke visie op offensieve (Red Team) en defensieve (Blue Team) methoden

Synthese cursus - 1d - 7u00 - Ref. RTB

Prijs : 540 € V.B.

NEW

Deze eendaagse cursus geeft IT-managers en directeuren een duidelijk beeld van offensieve (Red Team) en defensieve (Blue Team) methoden. Aan de hand van praktische demonstraties en casestudies ontdekt u hoe uw teams aanvallen identificeren, uitvoeren en tegengaan, zodat u uw cyberbeveiligingsprojecten beter kunt beheren.

Pedagogische doelstellingen

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

- De rol van het Red Team en het Blue Team in cyberbeveiliging begrijpen
- Een overzicht krijgen van de methodologieën en tools die door elk team worden gebruikt
- Leren hoe je effectief met deze teams communiceert en hun prestaties beoordeelt
- Red Team- en Blue Team-praktijken integreren in projectbeheer en IT-risicobeheer

Doelgroep

Managers, IT-managers, projectmanagers, beveiligingsmanagers, besluitvormers die het werk van hun technische teams beter willen begrijpen.

Voorafgaande vereisten

Geen speciale kennis vereist.

Opleidingsprogramma

DEELNEMERS

Managers, IT-managers, projectmanagers, beveiligingsmanagers, besluitvormers die het werk van hun technische teams beter willen begrijpen.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

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 Waarom het Red Team en het Blue Team?

- Beveiligingsprincipes: verdediging in de diepte, cyberrisicomodellering.
- Risico's in verband met inbraak, aanvallen en systeembeveiliging.
- Waarom twee aparte teams? De Rode Teams (aanval) en de Blauwe Teams (verdediging).
- _1_ De rol van het Rode Team: de aanval begrijpen :
- Inleiding tot penetratietesten (pentests).
- Aanvalsfasen: verkenning, exploitatie, post-exploitatie.
- Tools gebruikt door Red Teams (bijv. Kali Linux, Metasploit, nmap).
- Aanvalsscenario's en Red Team-doelstellingen: beoordeling van netwerk- en systeembeveiliging.
- _2_ De rol van het Blauwe Team: de verdediging begrijpen :
- Inleiding tot inbraakdetectie, bewaking en incidentbeheer.
- Fasen van incidentrespons: detectie, analyse, indamming, uitroeiing.
- Tools gebruikt door Blue Teams (SIEM, firewalls, IDS/IPS-systemen).
- De sleutelrol van Blue Teams in crisispreventie en -beheersing.

2 Samenwerking tussen Rode Team en Blauwe Team: Simulatie en confrontatie

- Hoe de feedback van het Rode Team helpt om de verdediging van het Blauwe Team te verbeteren en vice versa.
- De rol van het management in het managen van deze interacties.

Demonstratie

Voorbeelden van oefeningen in "Rode Team vs Blauwe Team" (Purple Teaming).

3 Inzicht in methodologieën en rapporten

- Wat zoeken de Red Teams in hun rapporten (zwakke punten, uitgebuite kwetsbaarheden, testresultaten)?
- Hoe een Blue Team een incident analyseert en een crisismanagementrapport opstelt.
- Wat moeten managers weten uit technische rapporten om strategische beslissingen te kunnen nemen?

4 Risico's beheren en rode en blauwe teams integreren in IT-projecten

- Het belang van beveiligingstesten in de softwareontwikkelingscyclus (DevSecOps).
- Hoe de resultaten van Red en Blue Teams te integreren in het risicomanagementproces.
- IT-projecten voorbereiden, rekening houdend met penetratietests en proactieve verdediging.

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 : 20 maa., 19 juni, 18 sep., 11 dec.

PARIS LA DÉFENSE
2026 : 13 maa., 12 juni, 11 sep., 4 dec.