Opleiding : Cyberbeveiliging, Emulatie van tegenstanders

emuleer je tegenstander om geavanceerde aanvallen te simuleren

Praktijkcursus - 2d - 14u00 - Ref. RTA

Prijs : 1390 € V.B.

NEW

Adversarial Emulation is een beoordelingsmethode voor cyberbeveiliging waarbij de tactieken, technieken en procedures (TTP's) van echte bedreigingsactoren worden nagebootst om de beveiliging van een organisatie te beoordelen en te verbeteren. Deze training stelt u in staat echte aanvallen te simuleren, technieken van tegenstanders te begrijpen en uw detectie- en reactievermogen te testen in een gecontroleerde omgeving.

Pedagogische doelstellingen

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

- Inzicht in de strategische waarde van nabootsing door tegenstanders
- Atomic Red Team gebruiken als onderdeel van een MITRE ATT&CK-aanpak
- Een realistisch scenario implementeren met Caldera en/of Atomic Red Team
- Resultaten interpreteren, defensieve houding opsporen en versterken

Doelgroep

SOC-analisten, blue teamers, pentesters, red teamers, beveiligingsmanagers, beveiligingsbeheerders.

Voorafgaande vereisten

Goede kennis van IS-beveiliging, netwerken en systemen.

Opleidingsprogramma

1 Emulatie van tegenstanders 101

- Definities en kernbegrippen.
- Emulatie, simulatie en pentesting: vergelijking en waarom emuleren?
- Proactieve defensieve houding, afgestemd op de echte bedreigingen.

DEELNEMERS

SOC-analisten, blue teamers, pentesters, red teamers, beveiligingsmanagers, beveiligingsbeheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van IS-beveiliging, 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 Ontdek MITRE ATT&CK

- Presentatie van de MITRE ATT&CK en D3FEND matrices.
- Hulpmiddelen voor het nabootsen van tactieken, technieken en procedures (TTP).

Praktisch werk
De TTP's van een APT-groep identificeren.

3 Atomisch rood team

- Presentatie van Atomic Red Team, Atomic CLI, Invoke-Atomic.
- Hoe je een test gebruikt, aanpast en maakt.

Praktisch werk
Eenvoudige TTP-tests (bijv. exfiltratie, persistentie, herkenning).

4 Creatie van een nagebootste mini-aanvalcampagne met Atomic Red Team

- Bouw een mini-aanvalcampagne.
- Voer de tests uit met Atomic CLI of Invoke-Atomic.
- Observatie van logs en impact op de doelmachine.

Praktisch werk
Een aanvalscampagne bouwen en de sporen en gevolgen op de doelmachine observeren.

5 Detectie en correlatie van TTP's van Atomic Red Team

- Welke logs, welke Sigma, YARA of EDR detectieregels?
- Implementatie van tools voor verzameling, correlatie en onderzoek om schadelijke activiteiten op te sporen.

Praktisch werk
Detectie van TTP's gegenereerd door Atomic RedTeam.

6 Caldera

- Emulatieplatform van de tegenstander: Caldera.
- Presentatie en verschil met ART: agenten, automatische sequenties.
- Demonstratie en implementatie van een geautomatiseerd scenario.

Praktisch werk
Agenten instellen en een Caldera-scenario uitvoeren.

7 AI en cybercriminelen

- Gebruik van AI door aanvallers (polymorfe scripts, GPT in de aanval).
- Opkomende bedreigingen (LLM-poisoning, AI jailbreak, social engineering 2.0).
- De emulatie van tegenstanders aanpassen aan toegenomen bedreigingen.

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.

8 Paarse Team Uitdaging

- Hoe Atomic Red Team te integreren in een beveiligingspijplijn.
- Best practices voor het verbeteren van SOC-gebruiksgevallen.
- Bronnen, gemeenschapsprojecten, kant-en-klare scenario's.

Praktisch werk
Offensieve/defensieve simulatie: het ene team valt aan, het andere detecteert, beoordeling van resultaten, scoren op basis van MITRE.

Data en plaats

KLAS OP AFSTAND
2026 : 9 juni, 24 sep., 17 dec.

PARIS LA DÉFENSE
2026 : 9 juni, 24 sep., 17 dec.