Authorized Training Center

CLICO

SentinelOne

INCIDENT RESPONSE

SENTINELONE
NETWORKS SECURITY

CÍL ŠKOLENÍ :

Pro efektivní řízení kybernetické bezpečnosti v organizacích potřebují profesionálové důkladné porozumění fungování kybernetických kriminalistů a schopnost využívat dostupné nástroje a bezpečnostní řešení k analýze incidentů a přesné reakci. Toto školení je navrženo tak, aby IT pracovníkům a operátorům SOC poskytlo praktické zkušenosti, které jim umožní analyzovat skutečné kybernetické útoky, hodnotit situace a efektivně reagovat na incidenty.

PRAKTICKÁ CVIČENÍ:

Školení zahrnuje praktická cvičení prováděná v dedikovaném školicím prostředí vybaveném bezpečnostními řešeními SentinelOne (EDR SentinelOne) a na jednotlivých pracovních stanicích účastníků běžících na Kali Linux s aplikací Cyber Soldier Project. Prostředí také zahrnuje různé webové/SMB servery a Active Directory pro simulaci reálných kybernetických útoků. Účastníci budou aplikovat techniky běžně používané při skutečných kybernetických útocích, podle rámce MITRE ATT&CK. Tyto techniky zahrnují, ale nejsou omezeny na: vypisování přihlašovacích údajů operačního systému: správce paměťových / bezpečnostních účtů LSASS, webový shell, využití pro eskalaci oprávnění, laterální přenos nástrojů, předávání hashe a zneužívání vzdálených služeb.

JEDINEČNÉ VÝHODY PRO ÚČASTNÍKY ŠKOLENÍ:

Účastníci se zapojí do reálných –
- Techniky útoků Encounte-Red v reálných kybernetických kriminálních aktivitách. Získají také přístup ke specializovaným kybernetickým bezpečnostním systémům, včetně detekce a reakce na koncové body (EDR) s možnostmi živé forenzní analýzy. Tyto nástroje umožní účastníkům sledovat, jak efektivně lze konkrétní techniky kybernetických útoků detekovat pomocí pokročilých bezpečnostních nástrojů. Dovednosti získané během tohoto školení výrazně zvýší schopnost účastníků detekovat a reagovat na skutečné-
-Světové kybernetické útoky v rané fázi.

DEN 1 ÚVOD DO EMULACE RED TEAMU A ADVERSARY

- Jak vlastně funguje skutečný kybernetický útok?
- MITRE ATT&CK v reálných scénářích kybernetických útoků
- Úvod do Cyber Range Lab a Cyber Soldier Offensive Tools

PRAKTICKÁ CVIČENÍ

Objevování systémů, průzkum a sběr citlivých dat

- Základní cvičení útočných dovedností v kybernetickém dosahu – část 1
- Scénář – Active Directory Reconnaissance
- Scénář - Síťový průzkum
- Scénář – nasazení webového shellu na editovatelnou SMB share na webovém serveru, provádění příkazů na systému Windows
- Analýza stop kybernetických útoků pomocí živých forenzních nástrojů v detekci a reakci na koncové zařízení (EDR)

DEN 2 PRAKTICKÉ CVIČENÍ

Útoky na hesla, shromažďování přihlašovacích údajů a boční pohyb

- Základní cvičení útočných dovedností na kybernetickém dosahu – část 2
- Analýza stop kybernetických útoků pomocí živých forenzních nástrojů dostupných v Endpoint Detection and Response (EDR)
- Scénář - Lámání hesel k servisním účtům ve Windows doméně (kerberoasting)
- Scénář – Útok na aplikaci hesel na účty místních administrátorů
- Scénář - Windows Credential Dump pomocí Service Account a Webshellu
- Analýza stop kybernetických útoků pomocí živých forenzních nástrojů v detekci a reakci na koncové zařízení (EDR)

DEN 3 PRAKTICKÉ CVIČENÍ

Zneužití a krádež přihlašovacích údajů, eskalace privilegií

- Zneužívání zranitelností SMB na starších Windows serverech – MS17-010 Eternal
- Analýza stop kybernetických útoků pomocí živých forenzních nástrojů dostupných v Endpoint Detection and Response (EDR)
- Scénář – Vypisování přihlašovacích údajů ze SAM pomocí administrátorského hesla nebo NTLM hashe
- Scénář - Dump přihlašovacích údajů z LSASS pomocí administrátorského hesla nebo NTLM hashe
- Scénář – Laterální přesun do Windows systému jako správce
- Analýza stop kybernetických útoků pomocí živých forenzních nástrojů v detekci a reakci na koncové zařízení (EDR)

Cena školení: €799 na osobu

(termíny školení jsou stanoveny individuálně pro skupiny minimálně 4 osob)

Authorized Training Center CLICO

Více informací:

sales@clico.cz, sales@clico.sk

https://clico.cz/trainings »