



IDŐTARTAM
1 nap

APT

Technical Operations

AZ APT VESZÉLYEK MEGÉRTÉSE

Ez a kurzus arra fókuszál, hogy az APT-k miben térnek el a hagyományos fenyegetésektől. Célja láttatni, hogy a hagyományos fenyegetésekről alkotott fogalmaink sokszor nem érvényesek az APT-kre és megmutatja, hogy ezeket a veszélyeket hogyan lehet a technikai oldalról feltárni.

A kurzus elsősorban a tradicionális IT biztonsági szakértőknek szól.

Az esemény végére a hallgatóság jobban megérti, hogyan is működnek az APT-k, a mögöttük rejlő érdekeket, illetve azt, hogy melyek a megfelelő válaszüzenetek annak érdekében, hogy minimalizálják a szervezetükre leselkedő hosszú távú veszélyeket.



IDŐTARTAM
1 nap

APT

Human Operations

AZ APT VESZÉLYEK MEGÉRTÉSE

Ez a kurzus az APT fenyegetésekkel foglalkozik,

Különösen azzal, hogy miben különböznek a hagyományos fenyegetésektől. A fő téma a távoli fenyegetések és a számítógépek távoli feltörése, illetve a legtöbb esetben a mögöttük rejtőzködő emberek.

Célunk az, hogy a hallgatókat megtanítsuk a különböző fenyegetési szintek és a potenciális támadások első jeleinek felismerésére, valamint arra, hogy a legjobb módon reagáljanak ezekre.

A célhallgatóság jelen esetben a biztonsággal foglalkozó szakemberek és döntéshozók, akik célpontjai lehetnek ilyen támadásoknak otthon és úton is.



ARC4DIA

Információ:
Digital Forensics Kft.
Szabó Attila
+36 20 4330611
szabo@digitalforensics.hu
www.digitalforensics.hu



IDŐTARTAM
2 nap

APT

Simulated Engagement

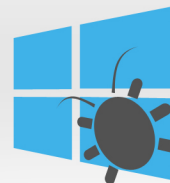
AZ APT VESZÉLYEK MEGÉRTÉSE

Ez a kurzus realiztikusan és a kezdetektől a befejezésig utánozza hogy mi történik, ha az ember harcba száll egy APT-vel.

Először egy valós forensic vizsgálat keretében anomáliákat keresünk a hálózaton, majd visszafejtjük a támadó anyagot. Eltervezzük a hatások csökkentését és az ellen-hírszerzést.

A résztvevők a folyamatot az egyik kutató-szakértőnk vezetése alatt működtetik, a szcenárió pedig a szervezet igényei szerint személyre szabható. Ez egy nagy kihívás, amely igyekszik ellátni a résztvevőket az alapvető eszközökkel arra, hogy szembeszálljanak a leggyakoribb APT-ekkel.

A kurzuson való részvétel megsokszorozza az Ön szervezetének erejét az APT-k elleni harcban.



IDŐTARTAM
2 nap

ADVANCED

Windows Malware
Reverse Engineering

HALADÓ

WINDOWS MALWARE VISSZAFEJTÉS

A kurzus célja, hogy a résztvevőkkel alaposan megértesse a legelőrehatóbb technikákat, amelyeket a fejlett malwarek alkalmaznak.

Megtaníttjuk, hogy ez milyen szerepet játszik a visszafejtésben.

A kurzus elvégzése után a hallgató képes lesz az új malware mintákat olyan módon megközelíteni, hogy a feldolgozási folyamat során teljesen megismerje azok képességeit.

A kurzus a malware visszafejtésére koncentrál, nem az ellene való védekezésre, vagy általános IT gyakorlatokra. Az összes leadott anyag a malwarekről és technikákról az APT modellekre összpontosít.