Akademie kybernetické bezpečnosti

Sleva 10% při objednání 2 a více účastníků (sleva bude odečtena ze zobrazené ceny)

Termín
30.5. - 7.6.2024

Online seminář

Živé vysílání sledujete online z domova či kanceláře. S lektorem komunikujete formou chatu nebo pomocí mikrofonu.

Cena bez DPH

13 770,00 Kč

16 661,70 Kč s DPH

Profily lektorů

Dan Kresa

Vystudoval Bezpečnostní a strategická studia na Masarykově univerzitě. Šest let působil na platformě KYBEZ, která se věnuje vzdělávání a spolupráci firem a akademického sektoru v kybernetické bezpečnosti. Pracoval rovněž ve společnosti, která se zabývá kybernetickou bezpečností, jako vedoucí oddělení vzdělávání, kde se věnoval tvorbě a řízení interních kurzů v oblasti kybernetické bezpečnosti a také různým projektům se středními a vysokými školami.

Jakub Skalický

Vystudoval matematické metody informační bezpečnosti na MFF UK. Během své praxe prošel několika českými i zahraničními společnostmi, poslední roky působí jako Principal Security Architect. Kromě teoretického kryptografického základu a softwarové bezpečnosti ho kybernetická bezpečnost zajímá i z celkového pohledu – je certifikovaný CISSP.

Zajímá vás kybernetická bezpečnost? Chcete zjistit, co vězí za všemi podivnými slovy, kterými se zprávy o útocích kyberzločinců jen hemží? Toužíte poznat, jak se útokům co nejlépe bránit, anebo zažít vzrušení z nalezení skutečné zranitelnosti ve webové aplikaci? Počet kybernetických útoků a mimořádných událostí neustále roste. Každý člověk se za svůj život setká s kybernetickým útokem či pokusem o něj. Díky našemu semináři dostanete rozsáhlý přehled kybernetické bezpečnosti – od základních pojmů přes standardizované procesy až k technické části. V ní si vyzkoušíte práci etického hackera, ukážeme si nástroje a metody, jimiž se organizace brání útočníkům a rozebereme několik známých útoků.

Cíl semináře

Na tomto 4denním on-line semináři vám poskytneme komplexní přehled o kybernetické bezpečnosti, jak po procesní, tak i technické stránce. Cílem je ukázat možné směry v oblasti kybernetické bezpečnosti tak, aby jste se mohli dále zaměřit na konkrétní oblast kybernetické bezpečnosti, která vás nejvíce zaujala.

Komu je seminář určen

Seminář je určen především osobám majícím zájem o vstup do oblasti kybernetické bezpečnosti.

Program

Čtyřdenní živé vysílání (9:00 - 13:00 hod.)

DEN 1. (30.5.2024, Mgr. Dan Kresa)

- Co je to kybernetická bezpečnost? (vysvětlení pojmu)
- Krátce z dějin oboru

- Legislativa
- Bezpečnostní role
- Co je internet? (Běžný web, deep web, dark net)
- Kyberkriminalita a typy útočníků (hackeři, bývalí zaměstnanci a další)
- Druhy útoků (jak vypadají, příklady, jak je rozpoznat, jak se jim bránit)
    - Phishing
    - Podvržené emaily
    - Vishing
    - Ransomware
    - Malware (Spyware)
    - MIMT
    - Spam
    - Sociální inženýrství
- Ochrana a obrana před útoky
    - Heslo (životní cyklus, síla hesla, password manager)
    - Softwarová ochrana (antivirus, firewall, aktualizace, webové stránky)
    - Hardwarová ochrana (přenosné nosiče, údržba a správa zařízení)
    - Bezpečnostní povědomí (procesy, směrnice, vzdělávání)
- Co dělat, když…? (hlášení problémů, reakce na útok, jeho řešení)
- Diskuze

DEN 2. (31.5.2024, Mgr. Dan Kresa)

- Co je to analýza rizik? Proč a jak ji zpracovávat?
- Legislativní rámec (Vyhláška o kybernetické bezpečnosti, ISO 27 000, Směrnice NIS 2)
- Zmapování organizace
- Přehled a hodnocení aktiv
- Evidence hrozeb a zranitelností
- Hodnocení rizik
- Návrh opatření
- Plán zvládání rizik
- Plán kontinuity
- Bezpečnostní strategie organizace
- Diskuze

DEN 3. (6.6.2024, Mgr. Jakub Skalický)

- Úvod do kryptologie
    - Symetrické šifry
    - Asymetrické šifry
    - Elektronický podpis
    - Hashovací funkce a ukládání hesel
- Základní architektonická pravidla IT security
    - CIA triad
    - Least-privilege, fail securely, separation of duties a další
- Síťová bezpečnost
    - Základní pravidla síťové bezpečnosti
    - Příklady útoků
- Seznámení s Dark Net a anonymitou na internetu
    - Co je Tor a proč neposkytuje úplnou anonymitu?
    - Známé a zcela legitimní weby na darknetu

DEN 4. (7.6.2024, Mgr. Jakub Skalický)

- Úvod do bezpečnosti OS
    - Hardening – co to je a proč se dělá
    - Útoky, kterým hardening brání
    - Příklady z reálného světa
- Úvod do webové bezpečnosti
    - Typy útoků na webové aplikace
    - Jak se bránit webovým útokům
    - Co může udělat provozovatel webu navíc oproti vývojářům?
    - Supply chain security
    - Známé útoky na webové aplikace
- Lab: zranitelná webová aplikace
    - Hledání chyb ve webové aplikaci
    - Bug bounty programy
    - Penetrační tester/etický hacker
- Kariérní možnosti v IT security
    - EU Cybersecurity Skills Framework – jak vidí cybersec role EU
    - Reálné zkušenosti z několika korporací a co se dá vše dělat

Další informace

Každý účastník kurzu obdrží CERTIFIKÁT o jeho absolvování, který může využít ve svém CV v části o doplňkovém odborném vzdělávání.
Forma semináře - živé vysílání (online seminář). Není potřeba nic instalovat ani stahovat - živé vysílání sledujete pouze po jednom kliku na odkaz, který obdržíte emailem.
Živé vysílání sledujete přímo na PC, notebooku nebo tabletu ve svém prohlížeči (Google Chrome, Mozilla Firefox, Microsoft Edge nebo Safari) z pohodlí Vašeho domova či kanceláře.

Během semináře lze pokládat prostřednictvím chatu dotazy lektorovi. Seminář pro Vás nahráváme, záznam ze semináře obdržíte následující pracovní den.

eduzone®

Objednávka: Akademie kybernetické bezpečnosti

Sleva 10% při objednání 2 a více účastníků (sleva bude odečtena ze zobrazené ceny)

Fakturační údaje objednatele:

IČO:

DIČ:

Firma:

Jméno a přijmení:

Telefon:

Email:

Ulice:

Město:

PSČ:

Vaše č.obj.:
(bude uvedeno na faktuře)

Poznámka:

Účastníci:

Jméno vč. titulů

Telefon:

Email:

Jméno vč. titulů

Telefon:

Email:

Jméno vč. titulů

Telefon:

Email:

Formulář vytiskněte, vyplňte, naskenujte a zašlete nám jej na email: **info@eduzone.cz**
nebo účast objednejte v našem e-shopu **www.eduzone.cz**