Kybernetické hrozby - Threat modeling aneb zaměřte opatření proti skutečným hrozbám

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

Termín
29.5. - 30.5.2024

Online seminář

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

Cena bez DPH
7 990,00 Kč
9 667,90 Kč s DPH

Profil lektora
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.

Znáte skutečně všechny kybernetické hrozby relevantní pro vaši organizaci? Podle slavného výroku D. Rumsfelda, nejhorší jsou „unknown unknowns“, tedy věci, o kterých ani nevíte, že je nevíte. Tím méně se na ně můžete připravit. Threat Modeling je prověřená metoda, kterou „neznámé neznámé“ z rovnice odstraníte – a se zbytkem si již poradíte.

Cíl semináře

Příloha č. 3 k Vyhlášce o kybernetické bezpečnosti obsahuje celkem 17 vybraných referenčních hrozeb – a poznámku, že identifikace konkrétních zranitelností a hrozeb je odpovědností povinné osoby. Seminář o Threat Modelingu má za cíl zaplnit tuto mezeru a naučit účastníky, jak konkrétní hrozby organizaci identifikovat. Předvede metodu STRIDE, díky níž se vcítíte do pozice potenciálních útočníků a hrozby svým aktivům budete nalézat podle typů dopadů, jaké by měly. Protože je STRIDE nejlépe aplikované na vývoj software, pro účely organizační bezpečnosti seminář přiblíží i metodu OCTAVE.
Seznam hrozeb, které vzejdou z Threat Modelingu, lze pak použít dále v hodnocení rizik a získat tak komplexní přehled o celé oblasti.

Komu je seminář určen

Analytikům, manažerům, architektům i auditorům kybernetické bezpečnosti ve veřejném i privátním sektoru.

Program

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

- Úvod
  - Definice threat modelingu, jeho účel a rozsah
  - Terminologie, typy hrozeb
- STRIDE
  - Popis metody krok za krokem
  - Aplikace na reálný scénář a identifikace modelových hrozeb
- OCTAVE
  - Popis metody krok za krokem
  - Aplikace na reálný scénář a identifikace modelových hrozeb
- Co s nalezenými hrozbami?
- Jak threat modeling začlenit do běžného business procesu
- Závěr

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 nebo Safari) z pohodlí Vašeho domova či kanceláře. Během semináře lze pokládat dotazy lektorovi prostřednictvím mikrofonu či chatu.

Seminář pro Vás nahráváme, záznam ze semináře obdržíte následující pracovní den.

eduzone®

Objednávka: Kybernetické hrozby - Threat modeling aneb zaměřte opatření proti skutečným hrozbám

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**