CYBER SECURITY ACADEMY

KIBERNETINIO SAUGUMO PAGRINDAI

KIBERNETINIO SAUGUMO PAGRINDAI

Kibernetinio saugumo pagrindų mokymai apima teorines paskaitas ir praktinius užsiėmimus.

Kursų esmė – pažinti esamą kibernetinio saugumo problematiką ir pasirengti praktiškai atremti kibernetines atakas.

Pirmosios dienos mokymų turinys universalus, jis skirtas bendram kibernetinio saugumo suvokimui, grėsmių ir priežasčių išsiaiškinimui. Dalyvauti geriausiai tinka įmonių vadovams, IT padalinių vadovams bei informacinių sistemų administratoriams. Teorinės žinios praktiškai taikomos laboratorinių darbų metu ir analizuojant demonstracijas.

Antrosios dienos mokymų metu kibernetinio saugumo teorija kombinuojama su praktine demonstracija ir individualių užduočių atlikimu laboratorijoje. Numatytos užduotys nesudėtingos, specialus pasirengimas nėra būtinas. Dalyvauti geriausiai tinka IT padalinių vadovams ar informacinių sistemų administratoriams.

Po mokymų visiems dalyviams išduodami dalyvavimą patvirtinantys pažymėjimai.

TRUKMĖ: 2 dienos

DĖSTYMO KALBA: lietuvių

KAINA: 750 EUR

NUOLAIDOS:

Išankstinės registracijos nuolaida – 15 %

3 ir daugiau žmonių iš vienos įmonės – 20 %

(nuolaidos nesumuojamos)

Kavos pertraukėlės ir pietūs įskaičiuoti.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

KIBERNETINIO SAUGUMO PAGRINDAI

1-osios dienos paskaitų darbotvarkė:

1. **Internetas ir kibernetinio saugumo perspektyva**
   - Internetas kaip kritinė infrastruktūra
   - Prielaidos kibernetinėms grėsmėms
   - LT interneto tarptautinis junglumas
   - Incidentų mastas Lietuvoje (CERT-LT, LITNET)

2. **"Pasižymėję" ir nauji kibernetiniai incidentai ir jų metodai**
   - Lietuvos kibernetinių grėsmių žemėlapis
   - "WannaCry" Lietuvoje
   - 1.35 Tbps DDOS ataka prieš Github
   - Valstybinių įstaigų puslapiai kripto valiutoms kasti
   - Stuxnet virusas ir jo atmainos
   - Spamhaus DDOS metodai

3. **Interneto protokolų saugumo spragos**
   - Tinkamas IP adresų dalinimas – užkirstas kelias atakoms
   - Apsauga nuo TCP atakų
   - DNS įrašų keitimas

4. **Kibernetinių atakų tipai. Botnet rinka**
   - Brute force, SQL injection
   - Cross Site Scripting
   - Man-in-the-midle
   - Botnet tinklo kūrimas, rinka, kainos, panaudojimas atakoms

5. **Saugumo priemonių taikymas**
   - Simetrinis, Asimetrinis šifravimas ir algoritmų spartos
   - Sertifikatas, PKI, elektroninis parašas
   - Autentifikacija, Challenge-response, sesijos raktas
   - Certificate Signing Request generavimas
   - Viešo ir privataus rakto generavimas
   - Raktų poros panaudojimas SFTP, SSH

6. **Kibernetinių incidentų valdymo reglamentavimas Lietuvoje, incidentų registravimas**
   - Kibernetinio saugumo būklės gerinimas
   - Pasaulinis CERT modelis
   - Grėsmių nacionaliniam saugumui vertinimas

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

KIBERNETINIO SAUGUMO PAGRINDAI

2-iosios dienos paskaitų darbotvarkė:

1. IT saugumo pagrindai organizacijoje
   - Perimetro apsauga
   - Ugniasienės kontrolinis sąrašas
   - Darbo vietų saugumas
   - Sistemų spragų “užtaisymas”
   - Anomalijų tikrinimas
   - Slaptažodžių politika
   - Mobiliojo telefono / planšetės apsaugos pagrindai
   - El. pašto apsaugos pagrindai
   - Vidinės ir išorinės saugumo rizikos

2. Mažų ir vidutinio dydžio organizacijų IT infrastruktūros saugumo didinimas
   - Realaus organizacijos IT tinklo analizė
   - IT tinklo modernizavimas, stebėjimas
   - Saugumo zonos
   - Tinklo segmentavimas (VLAN)
   - saugus DHCP, DNS, DNSsec konfigūravimas
   - VPN rūšys (OpenVPN konfigūravimas)
   - EMAIL pasirašymas kliento pusėje
   - EMAIL pasirašymas serverio pusėje (TLS, DKIM), DMARC
   - Apache vs NGINX vs Internet information services (IIS)
   - HSTS naudojimas

3. Ugniasienės ir atakų prevencijos sistemos
   - OSI 3 lygio ugniasienė
   - Proxy ugniasienė
   - Unified threat management ugniasienė
   - Firewall vs IDS vs IPS

4. Informacinių technologijų saugos atitikties vertinimas
   - Įsilaužimų scenarijai
   - Ethical hacking žingsniai

5. Programinės įrangos saugumas
   - Pažeidžiamumai soft’e
   - Pažeidžiamumai hard’e
   - Programavimo principai, kuriuos taikant didinamas bendras sistemos saugumas
   - Gerosios web deployment praktikos

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

KIBERNETINIO SAUGUMO PAGRINDAI

CYBER SECURITY ACADEMY

Kelių dienų CSA kibernetinio saugumo mokymų programų rezultatas - IT specialistas, gebantis spręsti sudėtingas kibernetinio saugumo problemas tinkamai, greitai ir našiai bei turintis reikiamas IT saugumo žinias įvertinti IT saugumo lygį savo organizacijoje.

Kaip? CSA kibernetinio saugumo mokymų programų turinys pagrįstas realių saugumo problemų simuliacijomis ir geriausiomis sprendimų praktikomis. Tai reiškia, kad per trumpą laiką CSA dėstytojai - geriausi užsienio ir Lietuvos IT saugumo praktikai ir "etiškieji hakeriai" (ang. *ethical hacker*) - padės įgauti daug realios patirties ir išvystyti įgūdžius, reikalingus kibernetiniam saugumui užtikrinti.

Mūsų tikslas - greitai ir kokybiškai parengti kibernetinės erdvės saugumo specialistus, kurie naujus įgūdžius galės iš karto pritaikyti savo organizacijai saugoti.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt