No spēles līdz drošībai: Jauni risinājumi kiberdrošības apmācībām

Dana Ludviga, Daina Ozoliņa

27.03.2025.

CERT.LV
Kiberincidentu novēršanas institūcija

Spēļošana *(Gamification)*

Spēļošanas apmācību ieguvumi:

- **Lielāka iesaiste** - spēles elementi nodrošina tūlītēju atgriezenisko saiti un atlīdzību, veicinot motivāciju
- **Apgūto zināšanu iegaumēšana** - izmantotie elementi uzlabo atmiņu un izpratni, jo padara mācīšanos aizraujošu un efektīvu
- **Patstāvīga mācīšanās** - Asociatīvā domāšana un pēcspēles mehānismi uztur interesi
- **Drošības kultūras veidošana** - Pozitīva pieeja rada proaktīvu attieksmi pret kiberdrošību, savukārt spēles piemēri, kas pietuvinātu reālās dzīves scenārijiem, veicina drošus kiberdrošības paradumus
- **Sadarbības un komandas salidēšana** - Interaktīvas aktivitātes stiprina un veicina komandas garu
- **Darbinieku apmierinātība -** darbinieku aptauja norāda, ka viņi aktīvāk iesaistās kiberdrošībā, jo apmācību process ir interesants un dinamisks

Talent LMS (https://www.talentlms.com/blog/gamification-statistics/); https://www.sans.org/; Traning Industry, Inc; https://www.nist.gov/cyberframework; https://owasp.org/

Izglītojošas spēles

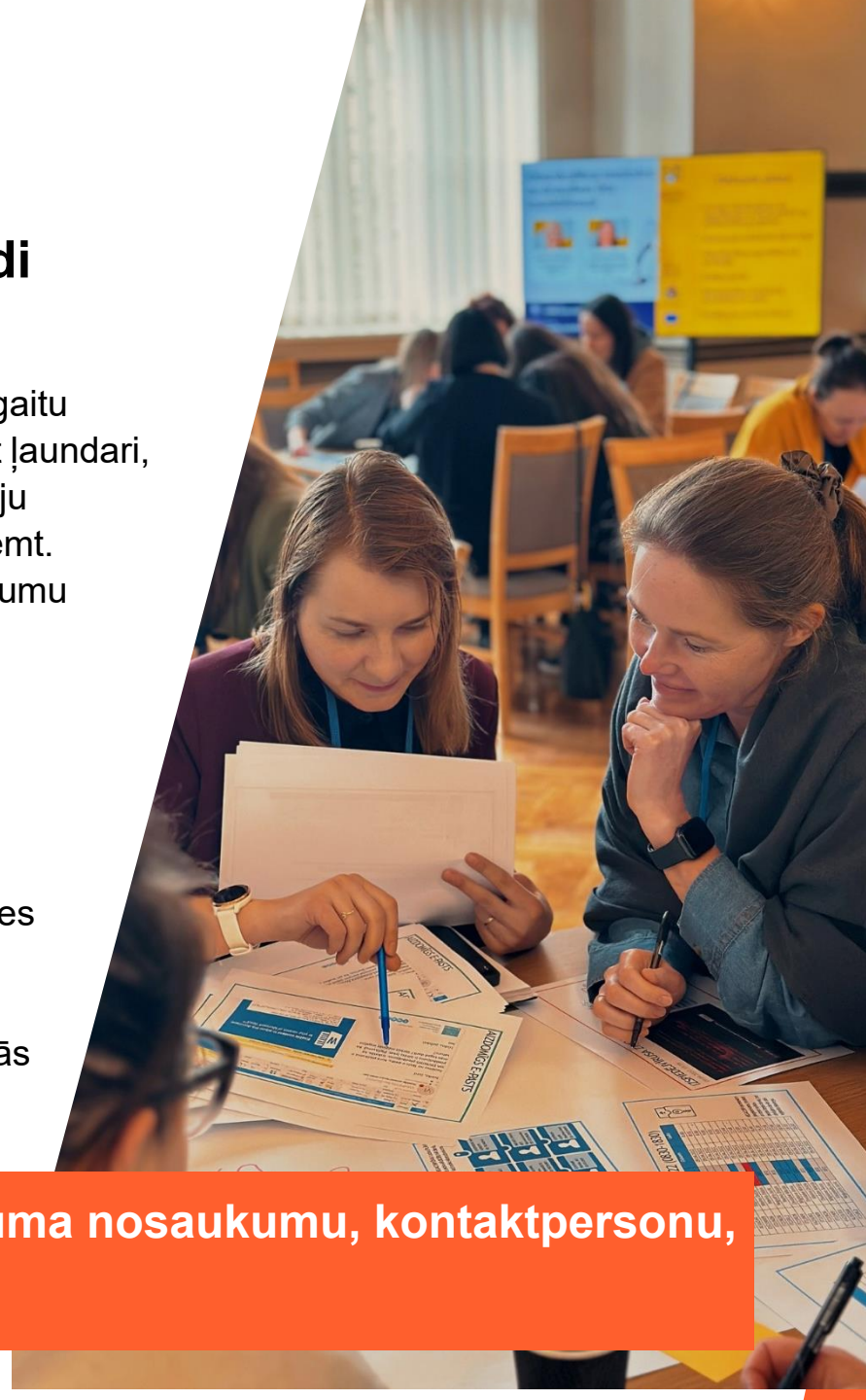
1. Praktiska kiberdrošības incidenta izmeklēšanas spēle "Atrodi hakeri" (~80min)

Dalībnieki iejutīsies kiber-detektīvu lomā un interaktīvā veidā pētīs un analizēs kiberuzbrukuma gaitu kādam starptautiskam uzņēmumam. Viens no izspēles centrālajiem uzdevumiem būs noskaidrot ļaundari, kas atbildīgs par uzbrukumu un tā sekām, analizējot gan aizdomīgus e-pastus, gan sociālo mediju ierakstus. Lai piedalītos izspēlē, nav nepieciešamas tehniskās zināšanas, datorus var līdzi neņemt. Izspēle ir noderīga gan darbiniekiem, gan vadītājiem, lai gūtu labāku priekšstatu par kiberuzbrukumu gaitu un potenciālajiem scenārijiem.

COMING SOON:

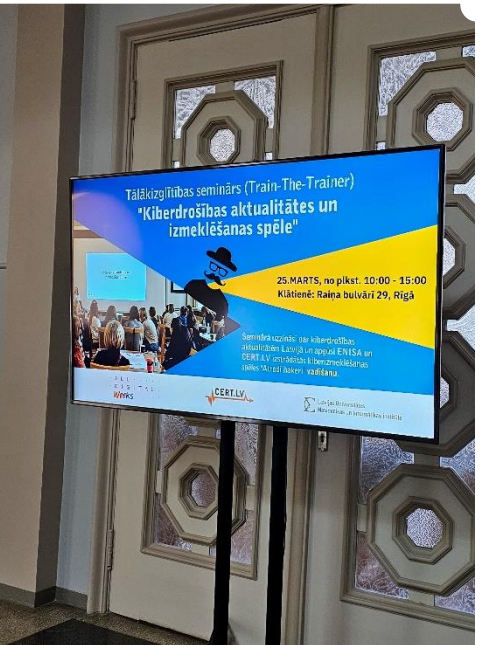
2. Darbības nepārtrauktības stiprināšanas spēle (~120min)

Šis kiberdrošības vingrinājums ir izstrādāts Nacionālā kiberdrošības likuma subjektiem un valsts iestādēm, kurām nepieciešams pārbaudīt un pilnveidot darbības nepārtrauktības plānu kiberkrīzes situācijā. Spēles laikā speciālisti no dažādām jomām praktiski izvērtēs savas zināšanas un gatavību reaģēt uz dažādiem incidentiem – sākot no neliela mēroga kiberincidentiem līdz kompleksiem un plašiem kiberuzbrukumiem. Vingrinājums palīdzēs identificēt nepilnības esošajās procedūrās un veicinās sadarbību krīzes situācijās.



Pieteikšanās: rakstot uz events@cert.lv, norādot iestādes/uzņēmuma nosaukumu, kontaktpersonu, aptuveno dalībnieku skaitu un vēlamo laiku!


Tālākizglītības seminārs (Train-The-Trainer)
"Kiberdrošības aktualitātes un izmeklēšanas spēle"
25.MARTS, no plkst. 10:00 - 15:00
Klātienē: Raiņa bulvārī 29, Rīgā
Semināra uzzināsi par kiberdrošības aktualitātēm Latvijā un apgūsi ENISA un CERT.LV izstrādātās kiberizmeklēšanas spēles 'Atrodi hakeri' vadīšanu.
CERT.LV


Tālākizglītības seminārs (Train-The-Trainer)
"Kiberdrošības aktualitātes un izmeklēšanas spēle"
25.MARTS, no plkst. 10:00 - 15:00
Klātienē: Raiņa bulvārī 29, Rīgā
CERT.LV


11:20 - 12:00 Diskusija: jaunākie kiberdrošības izaicinājumi un vajadzības
12:00 - 12:40 Kafijas pauze un neformālas sarunas
12:40 - 13:00 Kiberizmeklēšanas spēles izvelde un pielāgo
13:00 - 14:00 Praktiskā daļa: Kiberizmeklēšanas spēles "
14:00 - 14:40 Analīze un atziņas: spēles rezultātu pārrunā biežākās kļūdas
14:40 - 15:00 Noslēgums un atgriezeniskā saite

Lekcijas

]{iberdrošības aktualitātes Latvijā: draudi & risinājumi (60 – 80min)

Dalībnieki uzzinās, kādi ir izplatītākie kiberuzbrukuma veidi šobrīd, kādus trikus izmanto uzbrucēji un kā sevi pasargāt, tai skaitā ar bezmaksas praktiskiem rīkiem. Lekcijā uzzinātais, praktiskie piemēri un ieteikumi noderēs gan darba un ikdienas dzīvē, gan praktiskajā izspēlē.

Virtuālā vide - 2025. Apdraudējumu evolūcija (60 - 90min)

Dalībnieki tiks iepazīstināti ar pamata riskiem un apdraudējumiem interneta vidē, kā arī veiks diskusiju ar auditoriju par drošāku interneta lietošanu

Kiberdrošības pamati: Kiberhigiēna, drošība un aktuālie draudi (60–90 min)

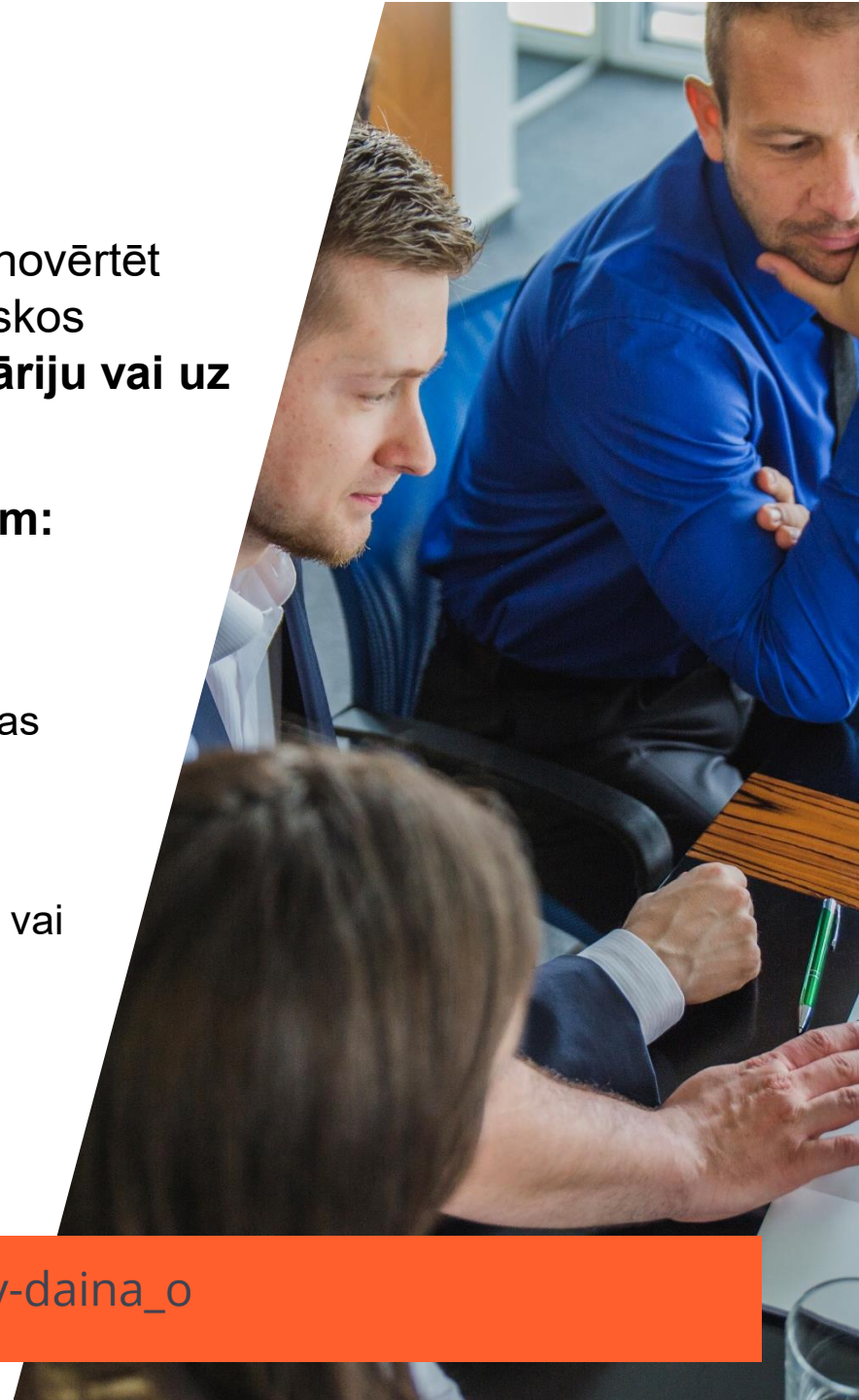
Dalībnieki apgūs vienkāršus un efektīvus veidus, kā pasargāt sevi no kiberuzbrukumiem, pilnveidot savu drošību un stiprināt aizsardzību kibertelpā. Analizēsim reālus piemērus un apgūsim mūsdienīgus risinājumus.

Galda mācības

CERT.LV izstrādā un novada **individuālas galda mācības**, lai palīdzētu novērtēt kiberdrošības procedūras, reaģēšanu uz incidentiem, komunikāciju, tehniskos risinājumus vai citas aktuālas tēmas. **Mācības var tikt balstītas uz scenāriju vai uz konkrēta gadījuma izpēti.**

Mācību laikā varam meklēt atbildes, piemēram, uz šādiem jautājumiem:

- Kādi ir galvenie kiberdrošības riski jūsu organizācijā? Kā tos novērst?
- Kādi kiberincidenti rada vislielākās grūtības?
- Kādas ir komunikācijas procedūras kiberuzbrukumu vai krīzes gadījumā?
- Kāda ir jūsu kiberdrošības stratēģija, vai tā ir līdzsvarā ar valsts stratēģiju, Latvijas un ES normatīvajiem aktiem?
- Kādā gatavības pakāpē ir jūsu kiberincidentu reaģēšanas, krīzes gatavības, darbības nepārtrauktības plāni?
- Kāda ir jūsu sadarbība ar trešajām pusēm/ piegādātājiem, kā tā ir dokumentēta, vai jūs pārzināt viņu kiberdrošības stratēģijas, plānus?



Pieteikšanās: rakstot uz events@cert.lv vai mattermost @lv-cert.lv-daina_o

Mācības

«Medus Pods» - ikgadējās nacionālās kiberdrošības mācības (draudu emulācija)

Organizē CERT.LV, Nacionālie bruņotie spēki un Aizsardzības ministrija. Mācību mērķis ir pārbaudīt noturību pret kiberuzbrukumiem un veicināt ikdienas sadarbību starp militārajiem un civilajiem partneriem, un to pārstāvēto uzņēmumu un organizāciju ekspertiem. Šogad galvenā mērķauditorija šogad bija mediji un telekomunikāciju operatori.

«Cyber Europe» - lielākās kibedrošības mācības Eiropas Savienībā (procedūras, *forensic*)

Organizē ENISA, iesaistās lielākā daļa ES dalībvalstu. Mācību mērķis ir pārbaudīt un uzlabot kiberdrošības, darbības nepārtrauktības un krīzes menedžmenta prasmes dalībvalstīs, kā arī standarta darbības procedūras. Šogad izspēlēsim nacionālā mērogā ar veselības sektoru.

«Locked Shields» - starptautiskas aktīvās kiberaizsardzības mācības

Organizē NATO apvienotais Kiberaizsardzības izcilības centrs (NATO CCDCOE). CERT.LV iesaistās gan BlueTeam, gan organizatoru pusē kopā ar CCD COE, kā arī atbalsta Zemessardzes KbrEK BN mācību organizēšanā Latvijā.

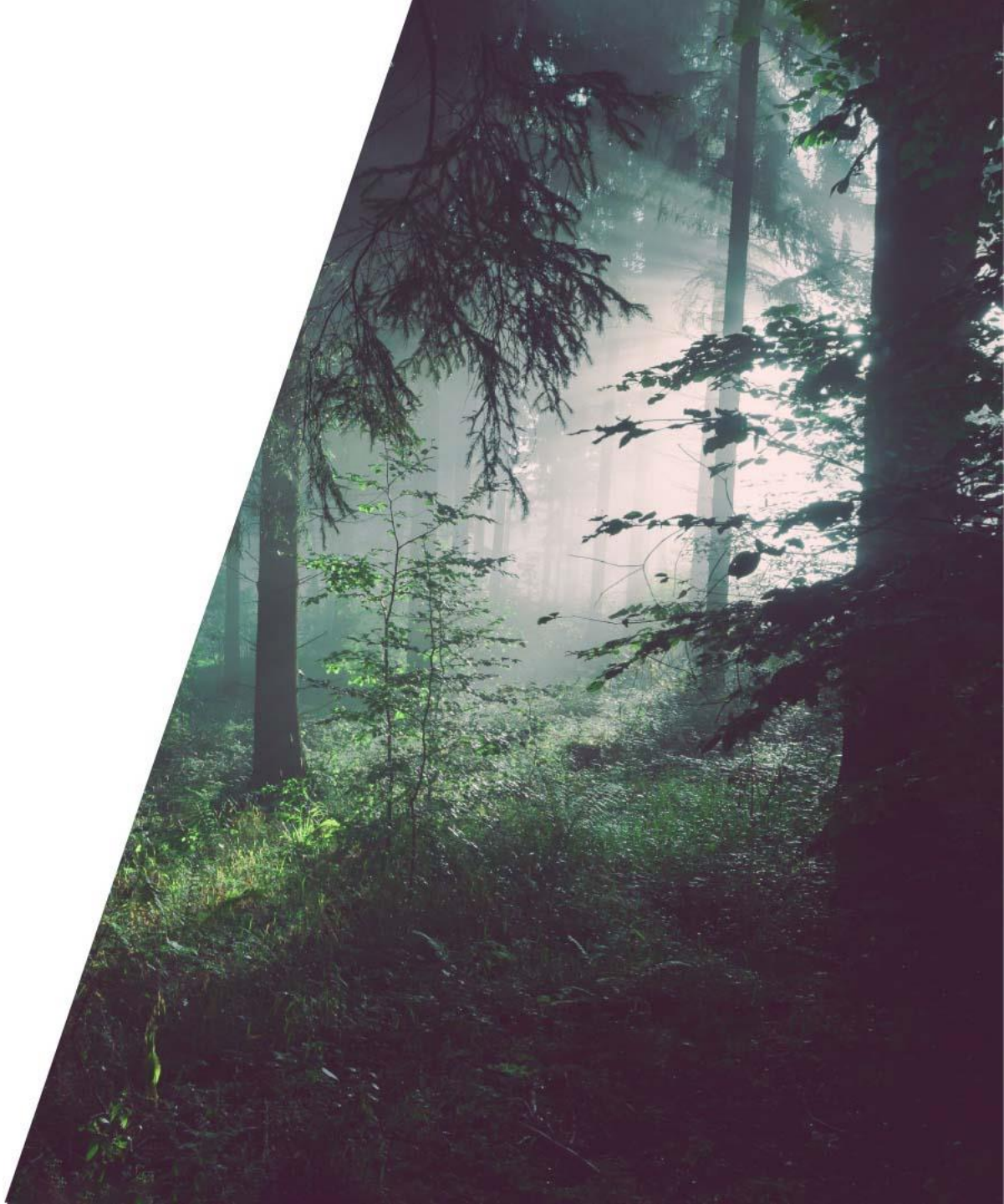
Pieteikšanās: mēs jūs uzaicināsim

CERT.LV

Kādas ir jūsu kiberdrošības izglītības vajadzības?

MENTI.COM

3770 7532



CERT.LV

No spēles līdz drošībai

@cert.lv