

DOBRODOŠLI

HARD ROCK SECURITY

Rok energija koja se sreće sa vrhunskom cyber zaštitom!

Demonstracije. Stvarne konverzacije. Jači smo zajedno!

Podignimo šiber na maksimum!

POWERED BY **NET++ TECHNOLOGY**

Net++
TECHNOLOGY

Agenda

9:30 – 10:00

Before the show

Registracija

10:00 – 10:30

Welcome to the Jungle

Sajber bezbednost u novoj eri napada (Vladimir Vučinić, Davor Kodrnja, MBCOM)

10:30 – 11:00

Who are you?

Identitet je novi perimetar (Vladimir Vučinić, Net++ technology)

11:00 – 11:30

Brake On Through

Prisma Access Browser (Srđan Vranić, Co.Next)

Agenda - nastavak

12:00 – 12:30

Come Together

Symantec CBX (Miodrag Milenković, MBCOM)

12:30 – 13:00

Under Pressure

Nemesis BAS (Nikos Leleas, Persistent Security)

13:00 – 13:30

Smells like a Breach?

Od napada do odgovora, Live Demo (Dimitrije Veličanin, Net++ technology)

13:30 – 14:00

We Will Rock You

Q & A, nagradna igra

Nagradna igra

Podelite fotografije sa današnjeg događaja na **LinkedIn-u** i pomenite [**@Net++ technology**](#) ili [**@IT klinika**](#).

Svi koji to urade učestvuju u našoj nagradnoj igri!



O čemu danas pričamo?

01

Identitet

Upravljanje identitetom je postalo ključno u današnjem IT svetu...

02

Prisma Access Browser

Browser pod kontrolom i upravljanjem, siguran, uz sve najnovije tehnologije zaštite...

03

Symantec CBX

PREMIJERA, među prvima u svetu, predstavljamo novo rešenje za srednja preduzeća...

04

Nemesis BAS

BreachGym – kako trenirati incident response timove i kako poboljšati rešenja koja koristite za zaštitu...

05

Live Demo

Nemesis i Symantec CBX u praksi...

SAJBER BEZBEDNOST U NOVOJ ERI NAPADA

POWERED BY **NET++** TECHNOLOGY



Net++
TECHNOLOGY

Sajber bezbednost u novoj eri napada

01 Ubrzanje

AI skraćuje lanac od otkrivanja ranjivosti do eksploatacije sa dana na sate, ponekad na minute. Skoro 40.000 CVE samo u prvoj polovini godine. Automatizovani lanci sa desetinama koraka. AI pokriva sve više faza kill chain-a, bez operatera u petlji. Odbrana gubi u „sledećem patch ciklusu“.

02 Identitet

Ulaz je identitet, ne perimetar. Napadači se sve češće „uloguju“, ne „provaljuju“. Kompromitovani nalog je ispred klasičnog exploit-a. Rastu ne-ljudski identiteti (API ključevi, servisni nalozi, agenti).

03 Phishing, deepfake

AI uklanja greške i pravi poruke koje liče na stvarne. Deepfake prevario ključnog čoveka Banca Intesa grupe, prevara od 36 miliona €. ClickFix-stil naredbi Microsoft je video na više od 1,1 milion uređaja za nekoliko meseci. Tehnička kontrola bez obučenog čoveka više nije dovoljna.

04 Lanac snabdevanja

Napad na softver, MSP, cloud ili dobavljača nudi ulaz. Incident kod jednog dobavljača gasi operacije kod stotina klijenata. Za MSP/MSSP to znači da su i meta i vektor: jedan kompromitovani alat ili nalog otvara portfolio klijenata.

05 Regulativa

DORA i NIS2 nameću upravljanje ranjivostima i otpornošću dobavljačima, nije više „imamo firewall“ dovoljno. Anketa pokazuju da je 60% firmi već imalo ozbiljan incident u prethodnoj godini. Kazna i prekid rada stižu zajedno.

Sajber bezbednost u novoj eri napada

Šta nam je činiti?

-
- 01** Inventar i identitet
 - 02** Skratiti vreme reakcije, praćenje na jednom mestu, izolacija
 - 03** Backup
 - 04** Kontrola dobavljača/lanca snabdevanja
 - 05** Trening ljudi, ne obuka, trening!
 - 06** Regulativa pod kontrolom

HVALA!

HVALA

Rok energija koja se sreće sa vrhunskom cyber zaštitom!

Podignimo šiber na maksimum!

POWERED BY **NET++ TECHNOLOGY**



Net++
TECHNOLOGY