REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Defend – Exercise - Attack

Nataša Klenovšek Arh

Kibernetski center, Ministrstvo za obrambo

NT KONF
NT KONFERENCA

Portorož, 26. 9. 2023

tasha@mo:~/NTK/defend_exercise_attack$

BREZ STOPNJE TAJNOSTI

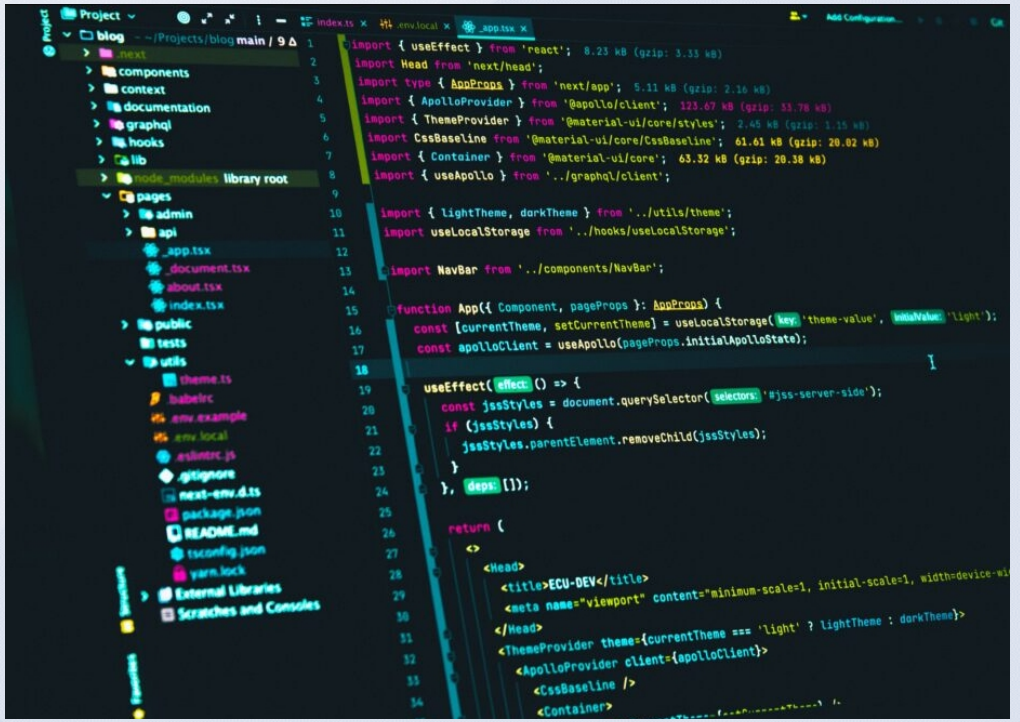
tasha@mo:~/NTK/challenge$

REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/me$

- Programiranje, digitalna forenzika, analiza zlonamerne kode, varnostni pregledi, sistemska administracija...
- SI-CERT (IH)
- Banka Slovenije
- MORS (KC MO)
- CCNA, SANS GREM, CEH Master

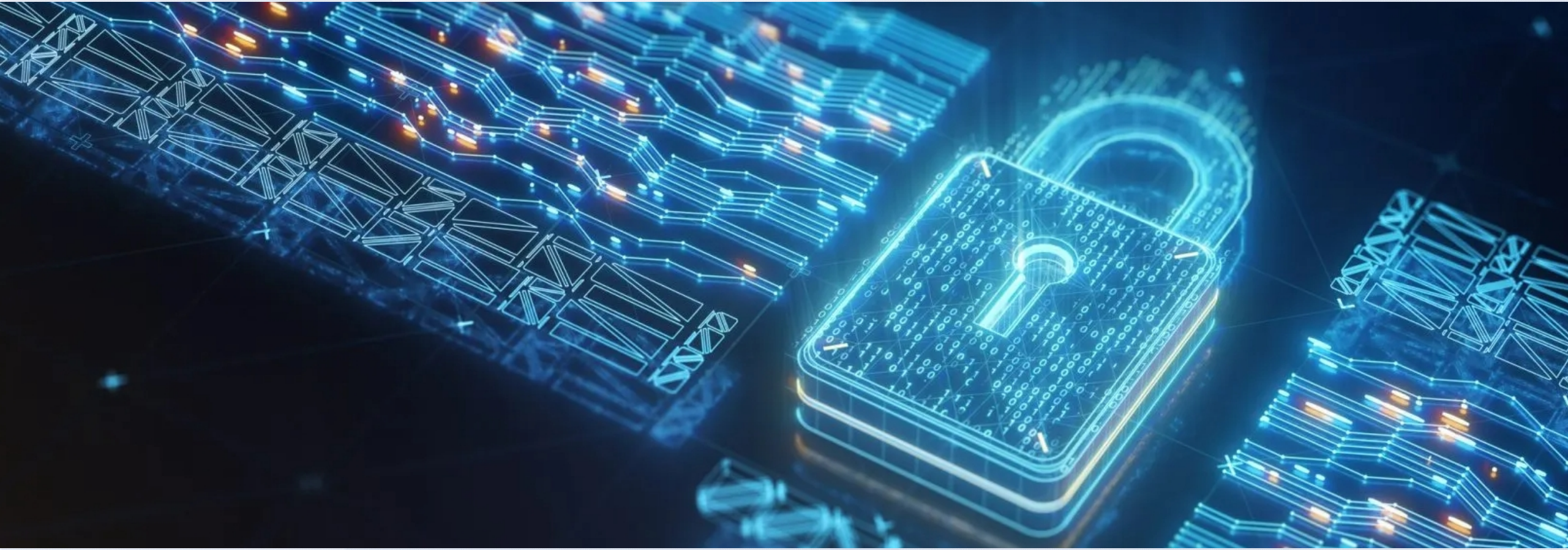


REŠI IZZIV!

TLP:GREEN

BREZ STOPNJE TAJNOSTI

tasha@mo:~/NTK/1_DEFEND$



TLP:GREEN

tasha@mo:~/NTK/1_DEFEND$

Blue Team

- Kaj branimo?
- Kako branimo?
- S čim branimo?
- Zakaj branimo?

REŠI IZZIV!

tasha@mo:~/NTK/1_DEFEND$

Blue Team

- VOC
  - SIEM
  - Orodja za odzivanje in obravnavo incidentov
  - Digitalna forenzika
  - Analize zlonamerne kode (ročno, avtomatizirano)
  - Analize in ocenjevanje kibernetskih groženj
  - Varnostni pregledi
  - Penetracijski testi
  - Usposabljanje

REŠI IZZIV!

tasha@mo:~/NTK/1_DEFEND$

Blue Team

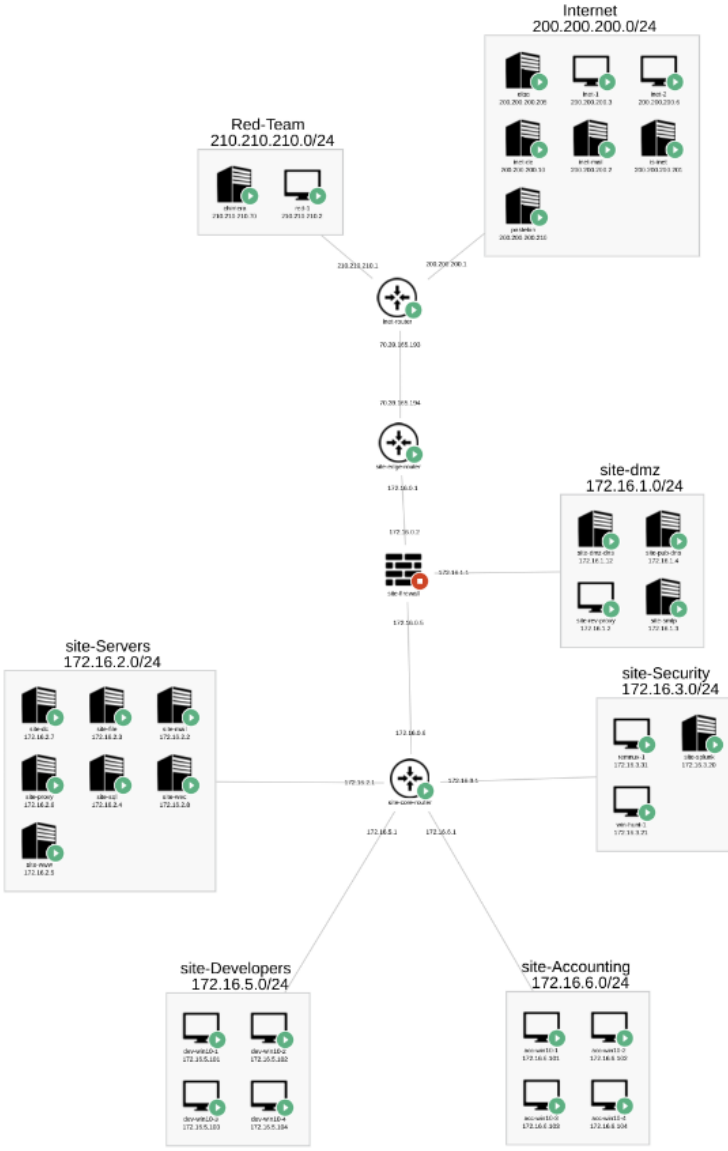
- Kaj pa »izven« VOC?
  - Politike
  - Utrjevanje sistemov
  - Ocena tveganja
  - Omrežne naprave
  - Svetovanja in pomoč pri pripravi različnih rešitev
  - EDR/XDR
  - Uporabniki
  - ...

REŠI IZZIV!

tasha@mo:~/NTK/2_EXERCISE$

tasha@mo:~/NTK/2_EXERCISE$

- Kaj je kibernetsko vadbišče?
  - Virtualno okolje, kjer je možno čim bolj realistično simulirati kibernetske napade.
  - Identična kopija KIS organizacije ali prilagojeno okolje.



REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/2_EXERCISE$

- Namen?
  - Usposabljanje kadra na področju IT
    - Modra ekipa – obramba
    - Rdeča ekipa – napad
    - Rumena ekipa – poročanje
    - Bela ekipa – spremlja potek vaje
    - Zelena ekipa – poskrbi za infrastrukturo
  - Testiranje programske ter strojne opreme.

REŠI IZZIV!

tasha@mo:~/NTK/2_EXERCISE/demo$

REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/3_ATTACK$

tasha@mo:~/NTK/3_ATTACK$

Red Team

- Zakaj?
- Kaj?
- Kako?
- Je sploh potrebno?

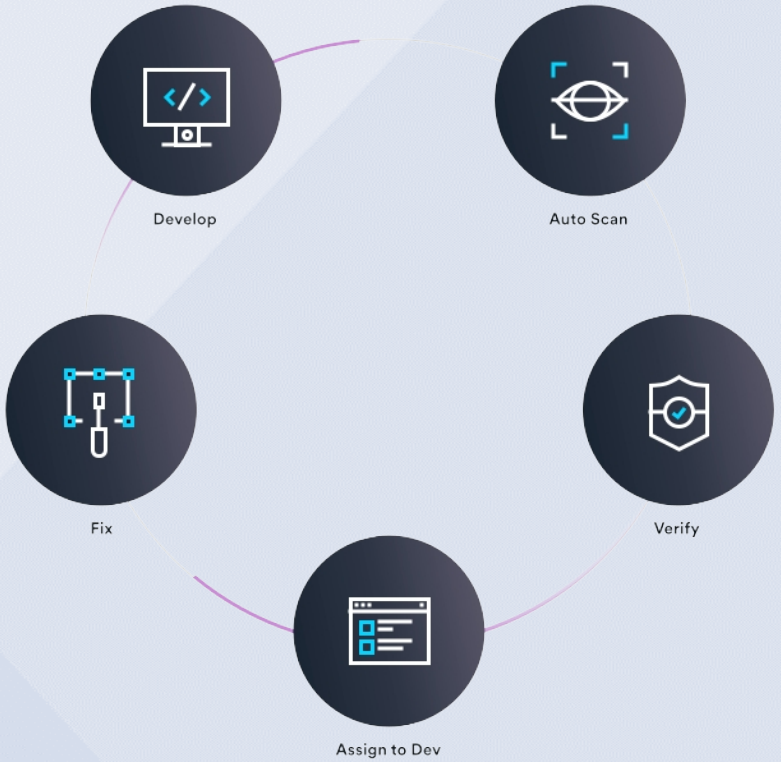
REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/3_ATTACK$

Red Team

- Poznavanje tehnik in taktik napadalcev
- Preverjanje zmogljivosti obrambe sistema
- Iskanje ranljivosti
- Usposabljanje



REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/3_ATTACK/demo$

Red Team

REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/defend_exercise_attack$

- **Cilj je zagotavljati strokovno in kvalitetno usposabljanje, ter nova znanja z namenom izboljšati kibernetsko varnost v RS.**

- Dejstva:
  - Edino kibernetsko vadbišče v RS.
  - V RS je potrebno dvigniti raven kibernetske varnosti v javnem in privatnem sektorju.
  - KIS organizacij so izpostavljeni vedno bolj sofisticiranim kibernetskim napadom, ki imajo v veliko primerih ogromne finančne posledice.
  - Strokovni kader na področju kibernetske varnosti se mora konstantno izobraževati in usposabljati, da lahko uspešno brani KIS organizacije pred novimi kibernetskimi grožnjami.
  - Za več informacij o možnosti uporabe kibernetskega vadbišča nas kontaktirajte na: kibernetski.center@mors.si

REŠI IZZIV!

tasha@mo:~/NTK/defend_exercise_attack$

- Defend vs. Attack

REŠI IZZIV!

TLP:GREEN

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Locked Shields 2024

kibernetski.center@mors.si

LOCKED SHIELDS

tasha@mo:~/NTK/defend_exercise_attack$

KIBERNETSKI CENTER MO

kibernetski.center@mors.si

#JoinOurTeam

REŠI IZZIV!

TLP:GREEN

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Hvala za pozornost!

Natasa K. Arh

kibernetski.center@mors.si

> Sporočilo dneva: Kibernetske vaje so priložnost za utrjevanje!