



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

BREZ STOPNJE TAJNOSTI

Defend – Exercise - Attack

Nataša Klenovšek Arh

Kibernetski center, Ministrstvo za obrambo

Portorož, 26. 9. 2023



TLP:GREEN

tasha@mo:~/NTK/defend_exercise_attack\$



tasha@mo:~/NTK/challenge\$

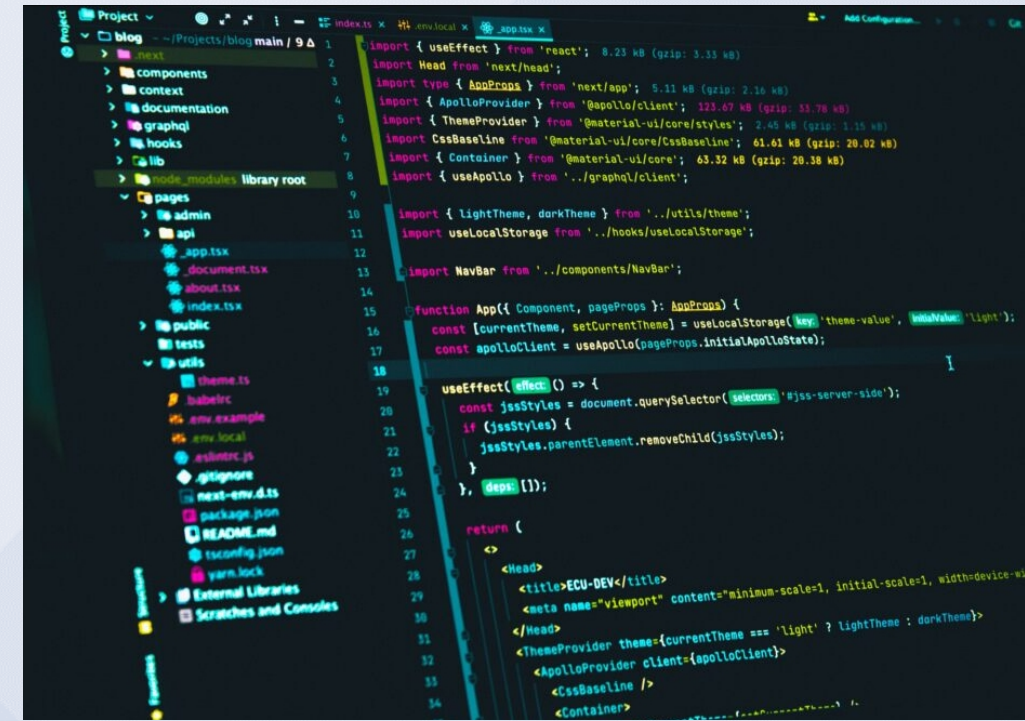


REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/me\$

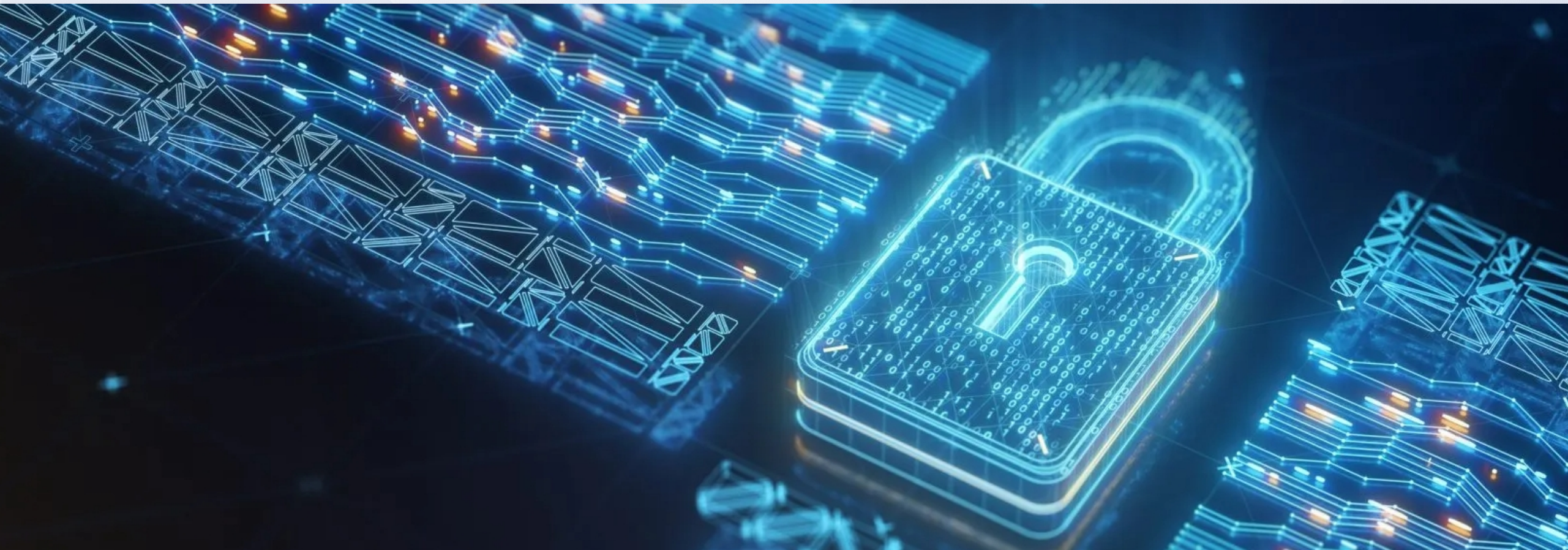
- Programiranje, digitalna forenzika, analiza zlonamerne kode, varnostni pregledi, sistemska administracija...
- SI-CERT (IH)
- Banka Slovenije
- MORS (KC MO)
- CCNA, SANS GREM, CEH Master



The screenshot shows a code editor with a file explorer on the left and code on the right. The file explorer shows a project structure for a Next.js application, including files like `app.tsx`, `document.tsx`, `index.tsx`, `theme.ts`, `babelrc`, `env.example`, `env.local`, `eslint.js`, `gitignore`, `next-env.d.ts`, `package.json`, `README.md`, `tsconfig.json`, `yarn.lock`, `External Libraries`, and `Scratches and Consoles`. The code on the right is a TypeScript file, likely `app.tsx`, showing imports for `useEffect`, `Head`, `AppProps`, `ApolloProvider`, `ThemeProvider`, `CssBaseline`, `Container`, `useApollo`, `LightTheme`, `darkTheme`, `useLocalStorage`, and `NavBar`. It defines a `function App` that takes `Component` and `pageProps` as arguments and returns a JSX element. The code includes a `useEffect` hook that updates the document title and theme based on the page props.



tasha@mo:~/NTK/1_DEFEND\$



tasha@mo:~/NTK/1_DEFEND\$

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



REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/1_DEFEND\$



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



REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/1_DEFEND\$



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



REŠI IZZIV!

TLP:GREEN

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



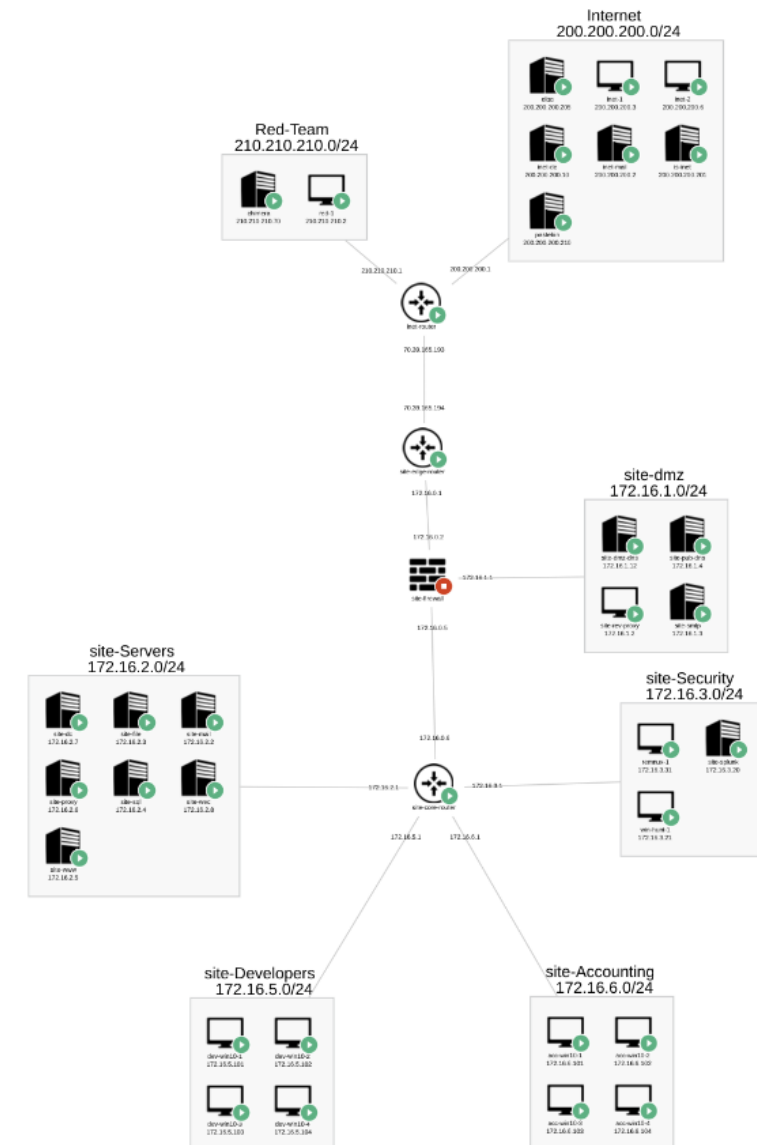
tasha@mo:~/NTK/2_EXERCISE\$

- Kaj je kibernetско vadbišče?
- Virtualno okolje, kjer je možno čim bolj realistično simulirati kibernetске 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.



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



REŠI IZZIV!

TLP:GREEN

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



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

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

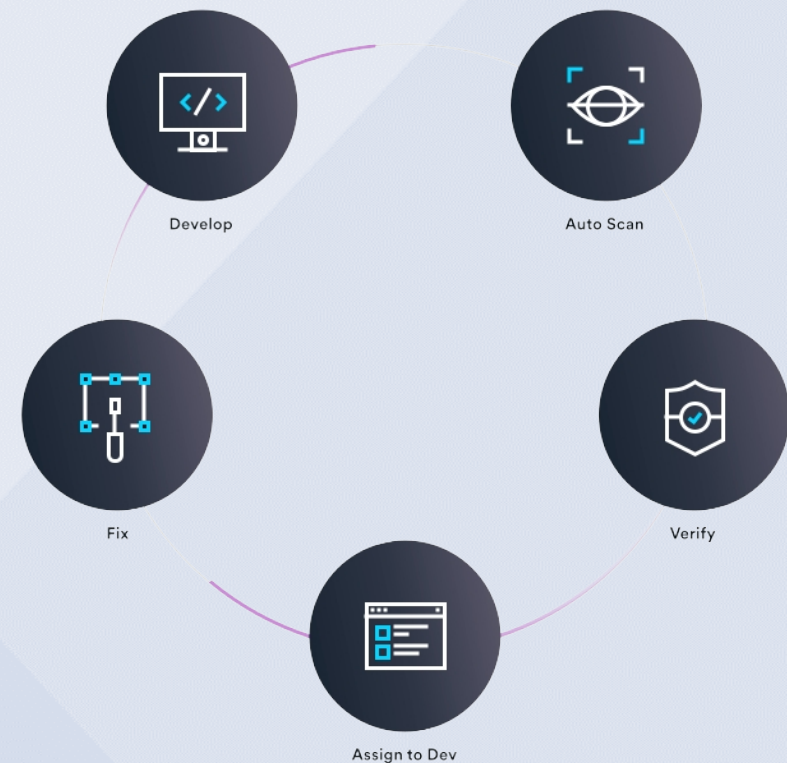


REŠI IZZIV!

TLP:GREEN

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

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



REŠI IZZIV!

TLP:GREEN

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



REŠI IZZIV!

TLP:GREEN

tasha@mo:~/NTK/defend_exercise_attack\$

- **Cilj je zagotavljati strokovno in kvalitetno usposabljanje, ter nova znanja z namenom izboljšati kibernetско varnost v RS.**
- Dejstva:
 - Edino kibernetско vadbišče v RS.
 - V RS je potrebno dvigniti raven kibernetске varnosti v javnem in privatnem sektorju.
 - KIS organizacij so izpostavljeni vedno bolj sofisticiranim kibernetским napadom, ki imajo v veliko primerih ogromne finančne posledice.
 - Strokovni kader na področju kibernetске varnosti se mora konstantno izobraževati in usposablјati, da lahko uspešno brani KIS organizacije pred novimi kibernetскими grožnjami.
- Za več informacij o možnosti uporabe kibernetского vadbišča nas kontaktirajte na: kibernetски.center@mors.si



tasha@mo:~/NTK/defend_exercise_attack\$



• Defend



vs.

Attack



REŠI IZZIV!

TLP:GREEN



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

BREZ STOPNJE TAJNOSTI



Locked Shields 2024

kibernetски.center@mors.si



LOCKED
SHIELDS

TLP:GREEN

tasha@mo:~/NTK/defend_exercise_attack\$

KIBERNETSKI CENTER MO

kibernetски.center@mors.si



#JoinOurTeam



REŠI IZZIV!

TLP:GREEN



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

BREZ STOPNJE TAJNOSTI



Hvala za pozornost!

Natasa K. Arh

kibernetски.center@mors.si

> **Sporočilo dneva:** Kibernetске vaje so priložnost za utrjevanje!

TLP:GREEN