

Ofenzivna sigurnost

Planiranje kibernetičkih operacija

Bruna Matić, 22.12.2025.

Pregled predavanja

- Kontekst i osnove
- Okruženje za planiranje i obuku
- Akteri i organizacija
- Operativno planiranje
- Ključni elementi planiranja
- Agilni pristup i podrška
- Zaključak

Motivacija

- Kibernetički prostor izravno utječe na vojne i sigurnosne sposobnosti
- Loše planirane kibernetičke operacije nose visok operativni i politički rizik
- Sustavno planiranje omogućuje predvidljivost, kontrolu i učinkovitost
- Stečeno znanje primjenjivo je u stvarnim operacijama i obuci

Pitanja za ispite

1. Što su kibernetičke operacije?
2. Koja je uloga kibernetičkih poligona?
3. Koja je uloga bijelog tima?
4. Koje su razine planiranja kibernetičkih operacija?
5. Koja je karakteristika ljubičastog tima?

Što su kibernetičke operacije?

- Ofenzivne, defenzivne i potporne aktivnosti u kibernetičkom prostoru
- Cilj: utjecaj na informacijske sustave, mreže i podatke protivnika
- Provode se paralelno s konvencionalnim vojnim operacijama

Kibernetički prostor kao operativna domena

- NATO prepoznaje kibernetički prostor kao domenu ratovanja
- Usporediv s kopnom, morem i zrakom
- Ključan za zapovijedanje, komunikacije i obavještajne sustave

Zašto je planiranje kibernetičkih operacija drugačije

- Kibernetičke operacije nisu ograničene geografijom
- Okruženje je dinamično i tehnički složeno
- Planiranje mora uključivati tehničke i operativne elemente



Uloga kibernetičkih poligona (Cyber Range)

- Sigurno i zakonito simulacijsko okruženje
- Uvježbavanje stvarnih scenarija bez operativnog rizika
- Razvoj i testiranje taktika, tehnika i procedura (TTP)



Iskustveno učenje i ratne igre

- Simulacija stvarnih kibernetičkih sukoba
- Gamifikacija povećava angažman i realizam
- Priprema za stvarne operacije bez stvarnih posljedica



Timovi u kibernetičkim operacijama

- **Crveni tim** – ofenzivni napadi i eksploatacija ranjivosti
- **Plavi tim** – obrana, detekcija i sanacija
- **Bijeli tim** – planiranje scenarija, nadzor i održavanje sustava



Organizacija i ljudi

- Jasno definirane uloge u cyber HQ-u
- Ujednačena razina znanja i iskustva
- Kontinuirana obuka i vježbe

Operativno planiranje (Cyber OPLAN)

- Kibernetički OPLAN-i sadrži
 1. Cyber ISR – prikupljanje obavještajnih podataka
 2. OOB (Order of Battle) – identifikacija protivničkih sustava i sposobnosti
 3. BDA (Battle Damage Assessment) – procjena učinka kibernetičkog napada

Razine planiranja kibernetičkih operacija

1. **Strateška razina** - ciljevi, mandat, pravila uporabe
2. **Operativna razina** - koordinacija, ciljanje, učinci
3. **Taktička razina** - alati, tehnike i tehnička provedba

Strateški preduvjeti za planiranje

- Jasna pravila uporabe (ROE)
- Mandat za djelovanje u protivničkom prostoru
- Zapovjednikova namjera i ciljevi operacije
- Početni prijedlozi ciljeva

Uloga obavještajnih podataka (Cyber ISR)

- NATO nema vlastitu kibernetičku obavještajnu strukturu
- Oslanja se na dijeljenje među saveznicima
- Potrebni podaci o mrežama, sustavima i akterima

Operativno planiranje i situacijska svijest

- Stalna slika vlastitih i protivničkih sposobnosti
- Prioritizacija ciljeva (energija, logistika, vojska, financije)
- Upravljanje očekivanjima zapovjednika

Učinci kibernetičkih operacija (Cyber Effects)

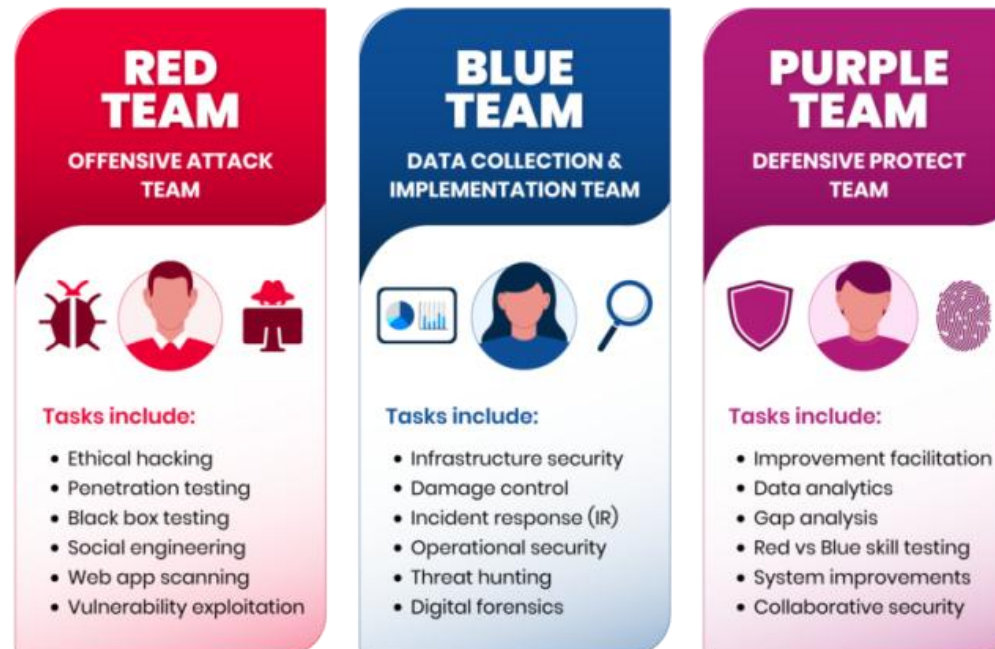
- Degradirati, poremetiti, uskratiti, uništiti
- Izravni i neizravni učinci
- Učinci se definiraju mjerljivo (npr. 50 % dostupnosti)

Taktička razina: tehnička priprema

- Pripremljeno i prikriveno ICT okruženje
- Distribuirana infrastruktura za smanjenje atribucije
- Alati i računi spremni prije operacije

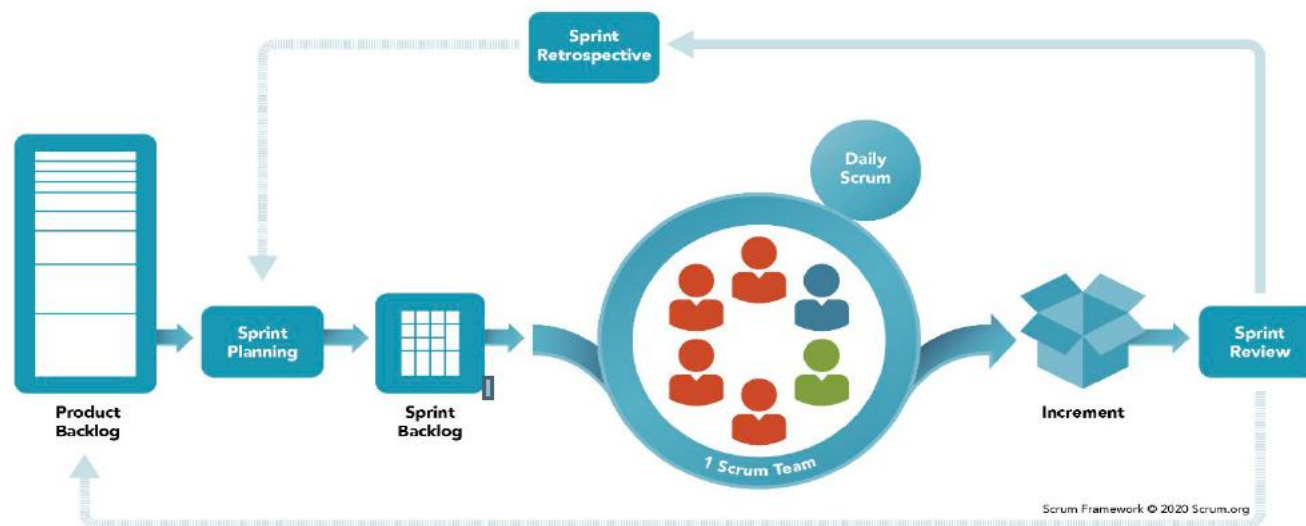
Wargaming i Purple Teaming

- Testiranje planova prije stvarne operacije
- Kombinacija ofenzivnih i obrambenih timova
- Sigurno okruženje za eksperimentiranje i učenje



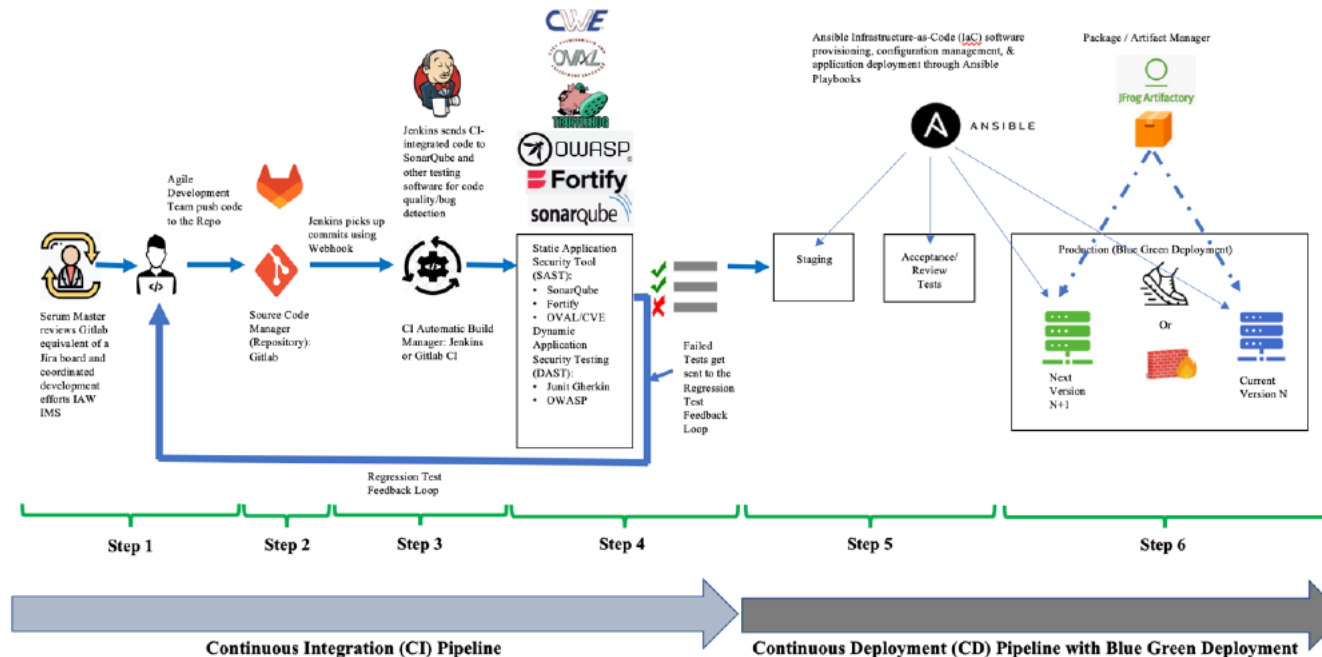
Uloga agilnih metoda (Scrum)

- Kratki ciklusi planiranja (sprintovi)
- Brza prilagodba promjenama i prijetnjama
- Kontinučno poboljšanje sposobnosti i scenarija



DevSecOps u planiranju

- Automatizacija razvoja, sigurnosti i operacija
- Brzo uvođenje novih ranjivosti i obrambenih mjera
- Visoka dostupnost i brza obnova sustava



Ključne prednosti ovakvog pristupa

- Brže planiranje i izvođenje operacija
- Bolja koordinacija timova
- Veća spremnost za stvarne prijetnje
- Skalabilnost i ponovljivost obuke

Zaključak

- Kibernetičke operacije su punopravna operativna domena
- Uspjeh ovisi o ljudima, procesima i tehnologiji
- Planiranje mora biti kontinuirano, agilno i utemeljeno na obavještajnim podacima
- Kibernetički poligoni, Scrum i DevSecOps povećavaju spremnost i otpornost

Literatura

- Arik, M.A. Venables, and R. Ottis. "Planning Cyberspace Operations." Journal of Information Warfare 21.4 (2022)
- Carroll, Jami M. "Agile Methods For Improved Cyber Operations Planning." ECCWS 2023 22nd European Conference on Cyber Warfare and Security. No. 1. Academic Conferences and publishing limited, 2023.

Dodatna literatura

- Barber, B., Bobo, M., & Sturm, J. "Cyber Operations Planning: Considerations for Military Planners." U.S. Army Cyber Institute, 2015.

Hvala!