

Ofenzivna sigurnost

Purple teaming

Petra Buršić, 15.12.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Penetracijsko testiranje
- Crveni i plavi tim
- Purple teaming
- Iterativni ciklus (PEIR)
- TIBER-EU okvir
- Zaključak

Motivacija

- Klasični sigurnosni testovi ne daju odgovor na pitanje koliko je sustav stvarno otporan
- Organizacije ne znaju mogu li napad otkriti i zaustaviti na vrijeme
- Napadi su složeni, dugotrajni i uključuju više tehnika istovremeno
- Potrebna je metoda koja povezuje napad i obranu u stvarnim uvjetima

Pitanja za ispite

- Objasnite što je *Purple Teaming*.
- Koja je razlika između *Purple Teaminga* i penetracijskog testiranja?
- Objasnite uloge i ciljeve crvenog tima (eng. *Red Team*) i plavog tima (eng. *Blue Team*).
- Objasni kako se koristi *Purple Teaming* u okviru TIBER-EU koji je razvila *ECB* (Europska središnja banka).
- Navedite barem dva izazova ili ograničenja provedbe *Purple Teaminga* u praksi.

Penetracijsko testiranje

- Jednokratna procjena ranjivosti sustava
- Cilj je pronaći tehničke ranjivosti, a ne testirati otpornost
- Ograničeno opsegom i trajanjem
- Izvještaj s pronađenim ranjivostima
- Penetracijsko testiranje ≠ testiranje otpornosti

Tradicionalni sigurnosni model

- Crveni tim (*Red team*) – napadači
 - Simulira stvarne napadače
 - Koristi napredne TTP-ove (taktike, tehnike i procedure)
 - Cilj: probiti sigurnosne mehanizme
- Plavi tim (*Blue team*) – obrana
 - Nadzor, detekcija i odgovor na napade
 - Analiza logova i poboljšanje sigurnosnih kontrola
 - Cilj: obrana i očuvanje dostupnosti sustava
- Testiranje otpornosti kroz simulaciju napada

Problemi tradicionalnog pristupa [\[1\]](#)[\[4\]](#)[\[6\]](#)

- Odvojeno djelovanje timova
- Slab prijenos znanja između timova
- Kašnjenje u dijeljenju informacija
- Obrana ne uči tijekom napada
- Fragmentirana percepcija stvarnih rizika

Purple teaming (PT)

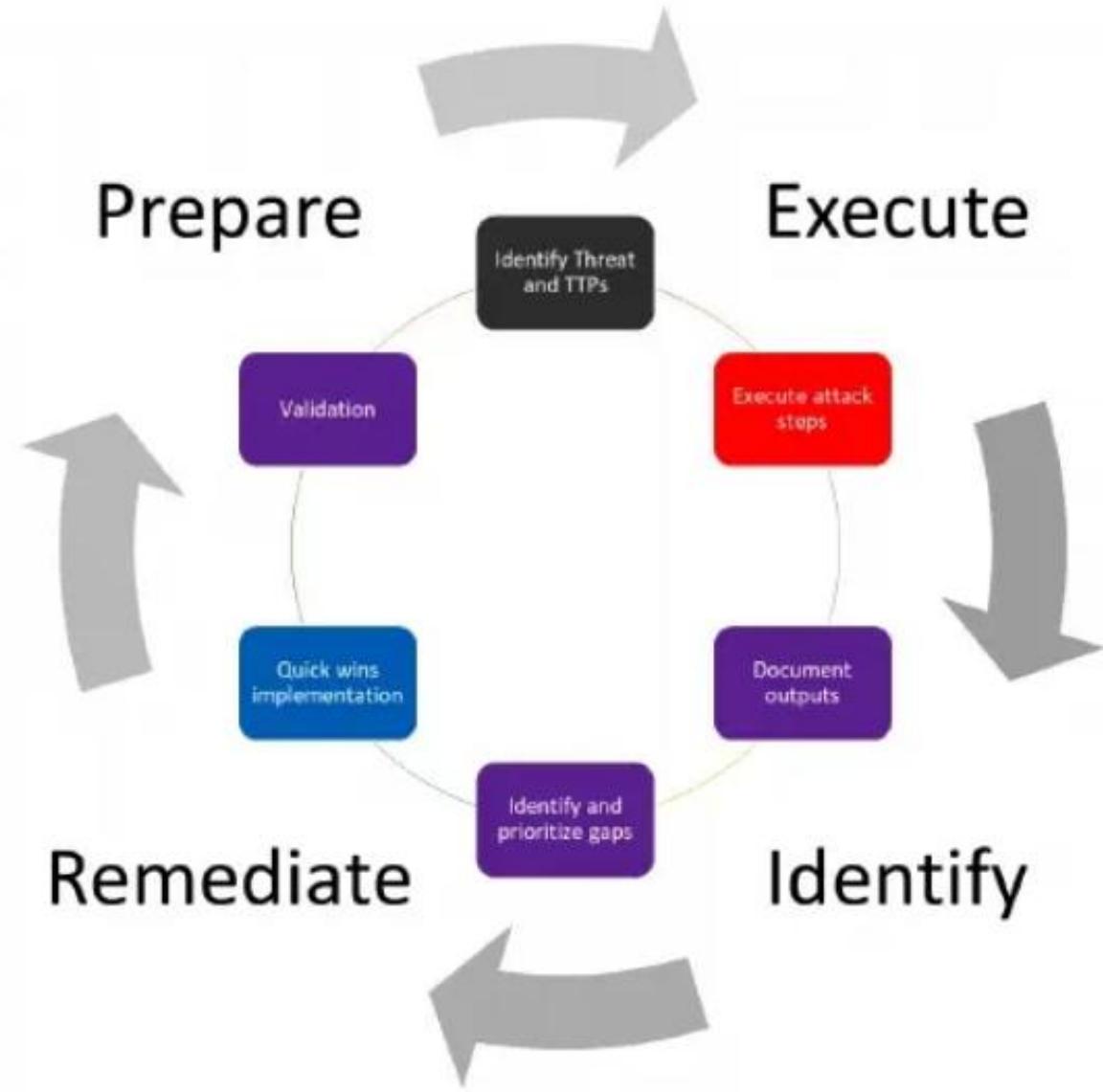
- Suradnički sigurnosni pristup koji se temelji na suradnji crvenog i plavog tima
- U praksi postoje dva osnovna modela [1]
 - Model 1: crveni i plavi tim ostaju odvojeni, ali surađuju tijekom napada
 - Model 2: formira se jedinstveni tim sastavljen od članova oba tima

Ključne karakteristike PT-a [3]

- Suradnički (eng. *Collaborative*)
- Višedisciplinaran (eng. *Multi-disciplinary*)
 - SOC analitičari
 - analitički developeri
 - oponašatelji napadača
 - mrežni i sistemske administratori
- Provodi se kao kontinuirani i **iterativni** proces
 - Svaki ciklus dovodi do poboljšanja obrane
- Fokusiran na jačanje obrane u odnosu na realne prijetnje

Iterativni ciklus PT-a

- Faze ciklusa [4]
 - Priprema - definiranje prijetnji i TTP-ova
 - **Izvođenje napada**
 - Detekcija i analiza
 - Otklanjanje ranjivosti
 - Provjera učinkovitosti
- Ciklus se neprekidno ponavlja
- Obrana postaje otpornija



Slika 1: PEIR iterativni ciklus djelovanja [4]

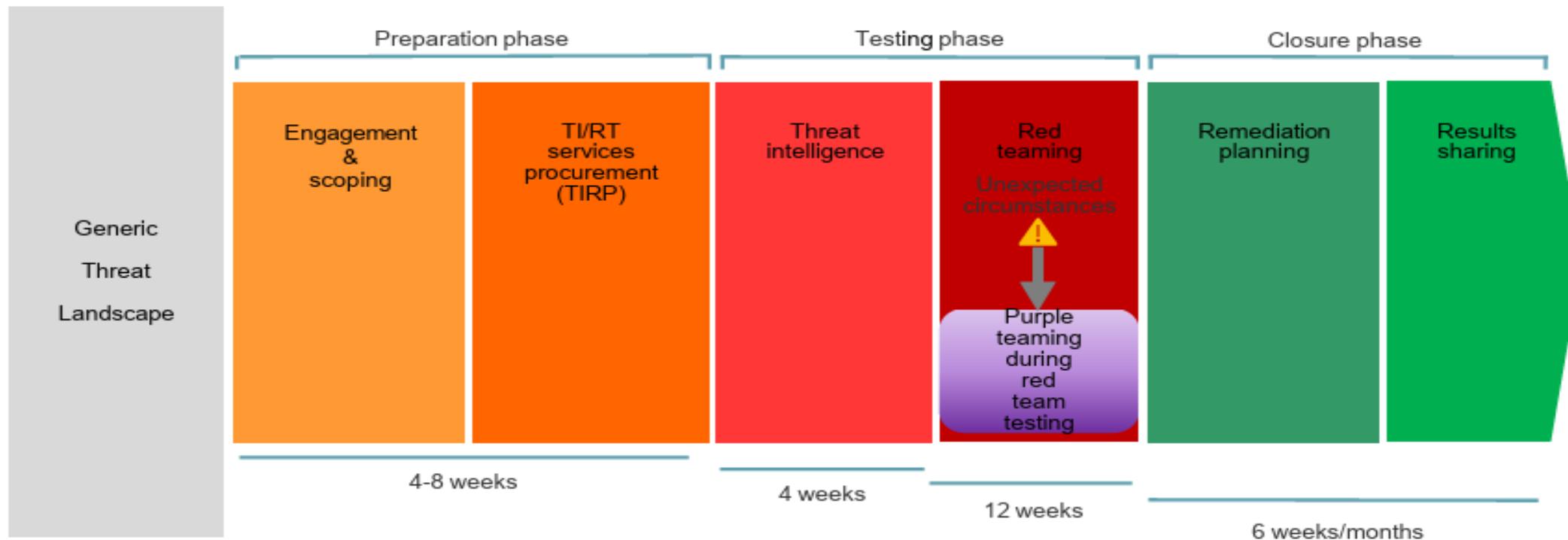
TIBER-EU okvir (1/3) [2]

- *Threat Intelligence-based Ethical Red Teaming – European framework*
- Europski okvir za testiranje kibernetičke otpornosti
 - Razvila Europska središnja banka (ECB)
 - Namijenjen financijskim institucijama
- Izvodi se u 3 faze
 - Pripremna faza (eng. *Preparation phase*)
 - **Faza testiranja** (eng. *Testing phase*)
 - primarno red teaming testiranje nad proizvodnim sustavima
 - **PT se uvodi u posebnim, nepredviđenim okolnostima**
 - Završna faza (eng. *Closure phase*)

TIBER-EU okvir (2/3) [2]

Indicative PT timeline in the testing phase

Process: circumstances leading to purple teaming during testing phase



Slika 2: Faze TIBER-EU okvira [2]

TIBER-EU okvir (3/3) [2]

- Različiti oblici suradnje tijekom faze testiranja

1. Catch-and-release

- Koristi se kada BT prerano otkrije RT
- Napad se nastavlja u kontroliranim uvjetima uz suradnju RT–BT

2. Collaborative Proof-of-Concept (PoC)

- Koristi se kada je puni napad preopasan za produkciju
- RT i BT zajednički izvode sigurnu PoC verziju napada

3. War Game

- Oba tima znaju ciljeve i otvoreno sudjeluju u vježbi
- Fokus na taktiku, reakciju i timsku koordinaciju

Ključni pokazatelji uspješnosti (KPI) [7]

- Vrijeme otkrivanja napada (eng. *Mean Time To Detect - MTTD*)
- Vrijeme odgovora (eng. *Mean Time To Respond - MTTR*)
- Slijepe točke u detekciji (eng. *Blind Spots*)
- Pokrivenost MITRE ATT&CK tehnika (eng. *ATT&CK Coverage*)
- Poboljšanje kroz iteracije (eng. *Iteration-to-Iteration Improvement*)

Prednosti i izazovi PT-a

- **Prednosti**
 - Poboljšava detekciju i odgovor *tijekom napada*
 - Brži prijenos znanja između timova
 - Iterativno jača obranu
 - Testiranje stvarnih TTP-ova
- **Izazovi**
 - Visoka potreba za stručnim timovima
 - Organizacijski i logistički zahtjevno za koordinirati
 - Oslanja se na kvalitetan obavještajni rad
 - Resursno i vremenski intenzivno

Zaključak

- PT daje stvarni uvid u otpornost obrane
- Najkorisniji je organizacijama s već uspostavljenom sigurnosnom funkcijom
- Zahtjeva visoku razinu stručnosti i organizacijskih resursa
- Postaje sve važniji zbog naprednih prijetnji i okvira poput TIBER-EU
- Očekuje se rast primjene PT kao nadogradnje *Red teamingu*

Literatura

- [1] Karhunen, E., „*Purple Teaming in System Hacking*”, 2025.,
<https://www.utupub.fi/handle/10024/180054>
- [2] European Central Bank (ECB), „*TIBER-EU Framework – Purple Teaming Best Practices*”, 2022.,
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_purple_best_practices.20220809~0b677a75c7.en.pdf
- [3] MITRE ATT&CK, „*Purple Teaming Fundamentals*”, <https://attack.mitre.org/resources/learn-more-about-attack/training/purple-teaming-fundamentals>
- [4] Routin, D.; Thoores, S.; Rossier, S., „*Purple Team Strategies – Enhancing Global Security Posture Through Uniting Red and Blue Teams With Adversary Emulation*. Packt Publishing”, 2022.
- [6] Picus Security, „*How to Leverage the MITRE ATT&CK Framework for Purple Teaming*”, 2023.
<https://www.picussecurity.com/how-to-leverage-the-mitre-attack-framework-for-purple-teaming>
- [7] Gaifulina, A. (2025). *The Concept of Red Team and Blue Team Synergy as a Factor in Enhancing an Organization's Resilience to Cyberattacks. Emerging Frontiers Library for The American Journal of Applied Sciences*, 7(11), 55–60., <https://emergingsociety.org/index.php/efltajas/article/view/445>

Dodatna literatura

- Ding, Y. et al. (2024). '*Purple-teaming LLMs with Adversarial Defender Training*',
<https://arxiv.org/abs/2407.01850>

Hvala!