SECURITY DAYS

Od penetračných testov k Red Teamingu

14. apríl 2026 / hotel NH Bratislava Gate One

Cybersecurity Progress. Protected. & SME KONFERENCIE

Pavol Michalec

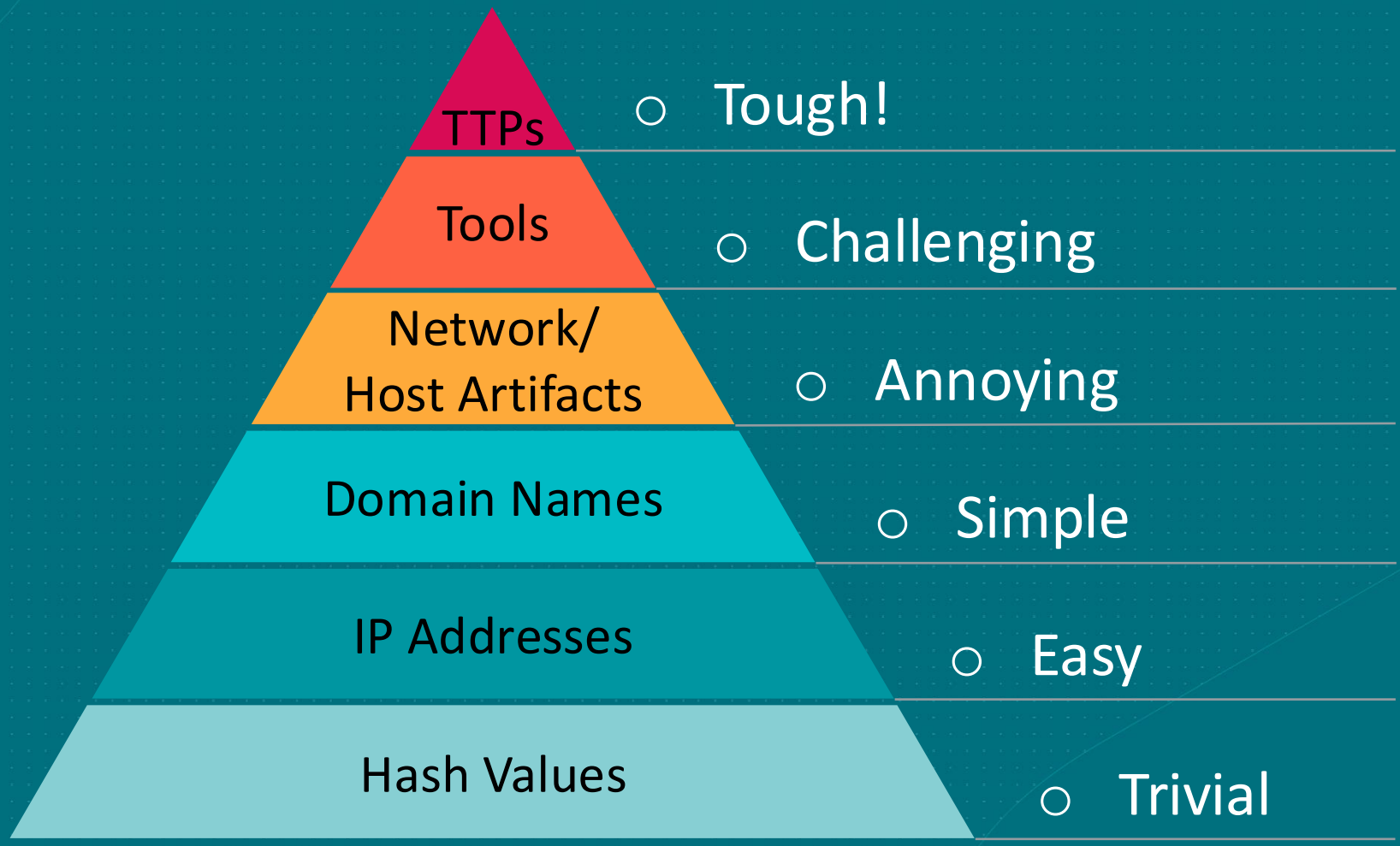
Senior Penetration Tester

pavol.michalec@eset.com

Red Teaming

- Pokročilá forma hodnotenia bezpečnosti
- Simuluje reálne útoky na Vašu organizáciu
- Preveruje celú obrannú schopnosť organizácie
- Využíva rovnaké taktiky, techniky a procedúry (TTPs) ako reálny útočníci

Pyramída bolesti



Penetračný test vs. Red Teaming

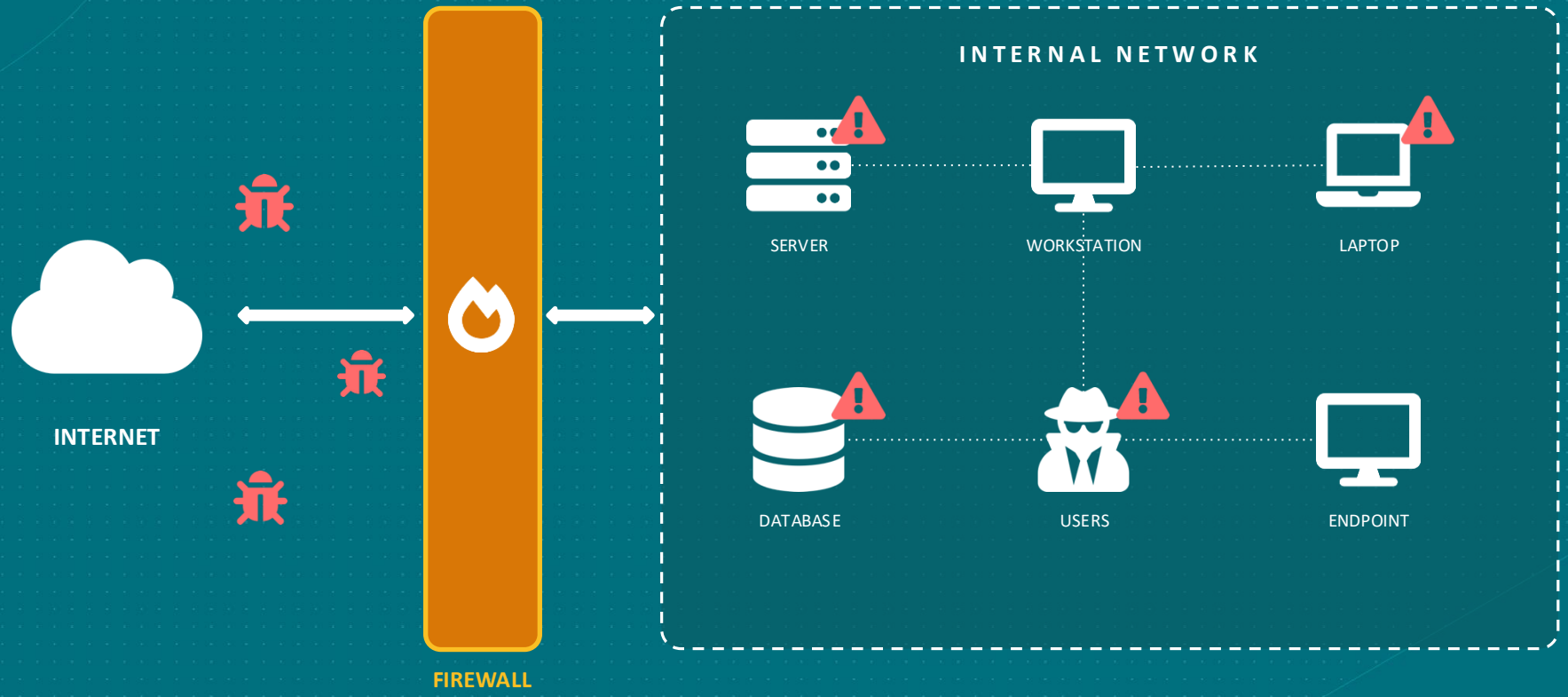
Penetračný test

- Identifikácia technických zraniteľností v definovanom rozsahu
- Zameraný na jednu aplikáciu, časť alebo komponentu
- Obranný tím je upovedomený o teste

Red Teaming

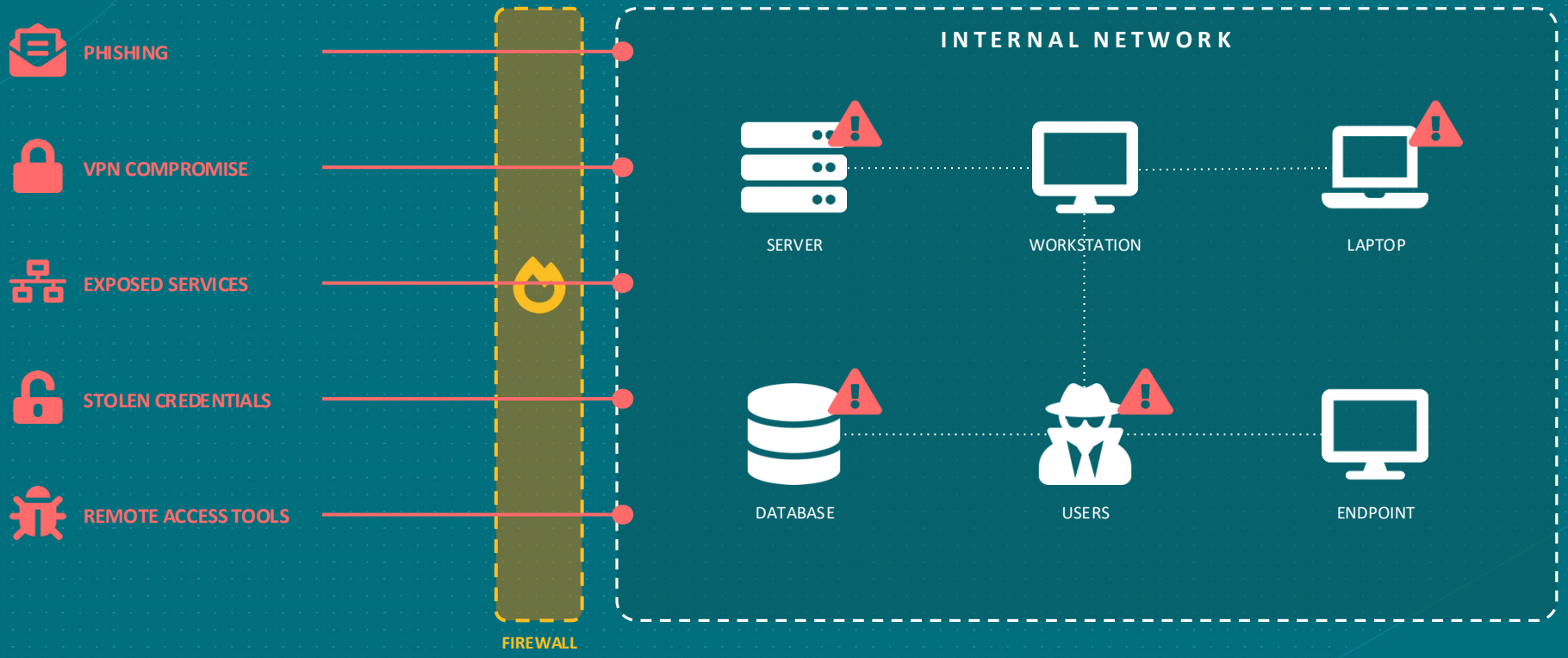
- Simuluje celý útočný reťazec
- Overuje schopnosť obrany detegovať a zastaviť protivníka
- Preveruje celú obrannú schopnosť vrátane technológií, procesov, detekčných mechanizmov a ľudí
- Prebieha bez vedomia obranného tímu

Hĺbková ochrana (Defense in Depth)

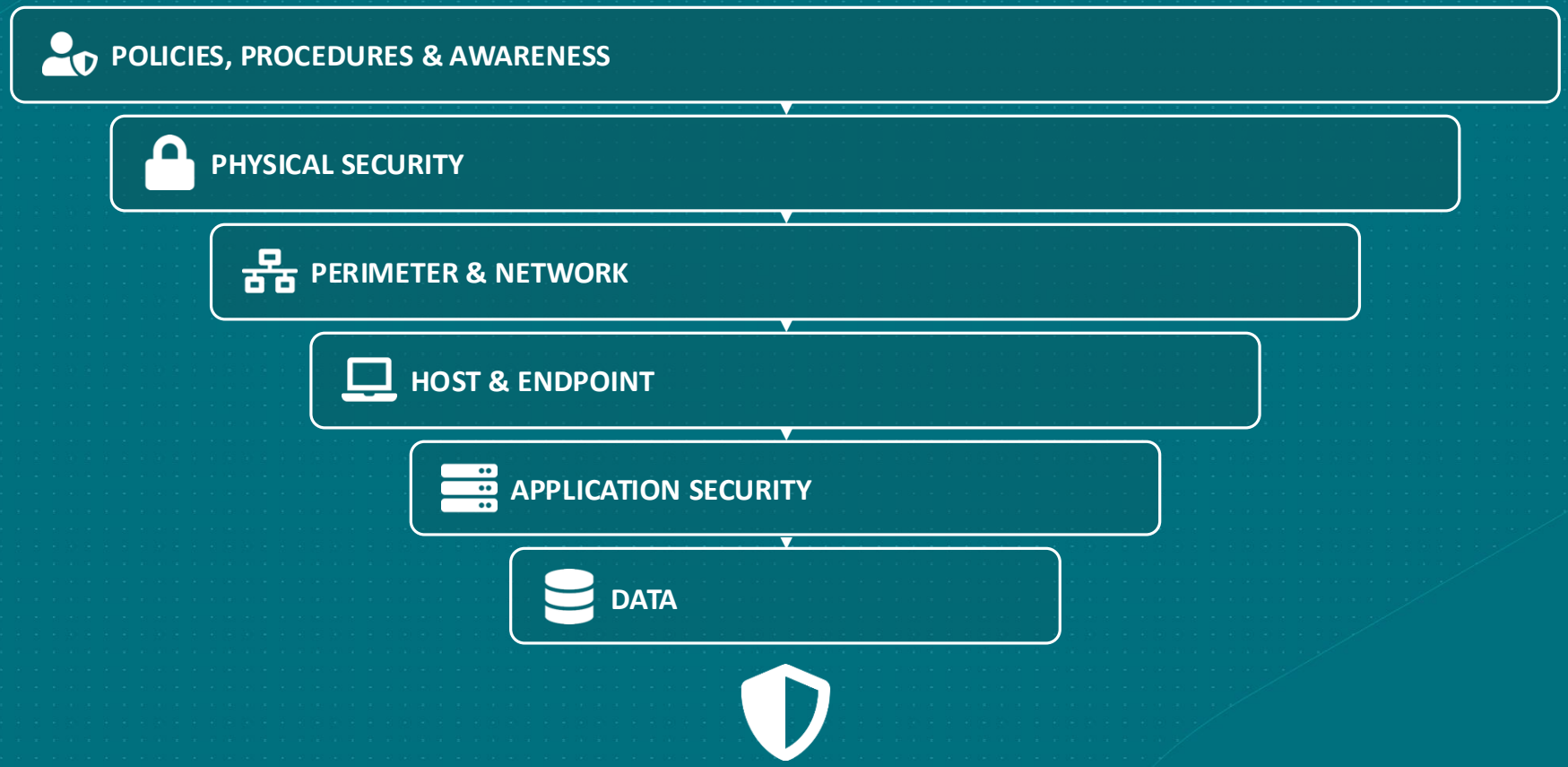


SECURITY DAYS

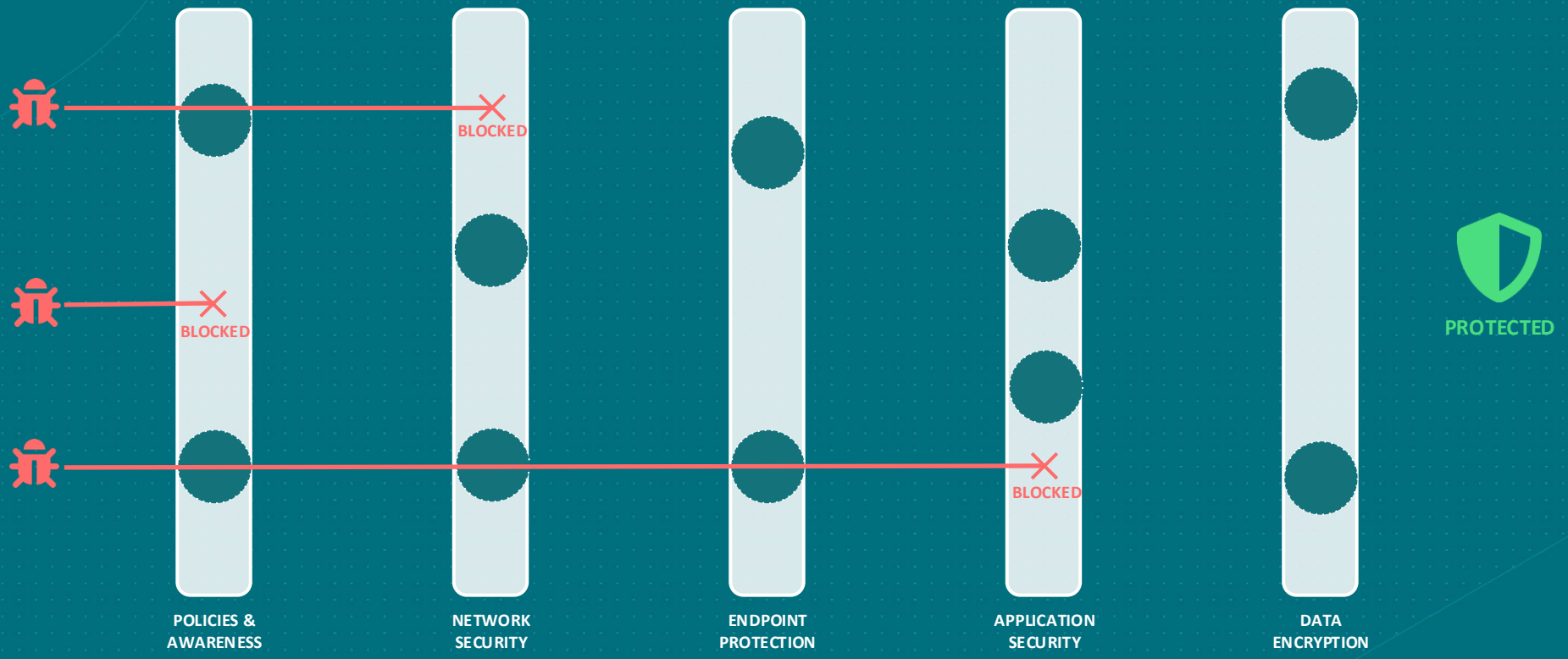
Hĺbková ochrana (Defense in Depth)



Hĺbková ochrana (Defense in Depth)



Hĺbková ochrana (Defense in Depth)



Each layer has weaknesses — but misaligned gaps prevent threats from passing through all layers

Výhody Red Teamingu

- Poskytuje realistický obraz o odolnosti celej organizácie
- Overuje schopnosť bezpečnostného tímu detegovať a reagovať na skutočný útok
- Identifikuje slabé miesta v procesoch, technológiách aj v reakciách ľudí na všetkých vrstvách (Defense in Depth)
- Príprava na sofistikované hrozby
- Simuluje celý útočný reťazec

Red Teaming v praxi

- Značne chránený perimeter siete
- Interná sieť s množstvom zraniteľností
- Nálezy z praxe:
  - Prihlasovacie údaje voľne dostupné na Confluence, Jira, zdieľaných sieťových diskoch,…
  - API kľúče a heslá uložené v zdrojových kódoch
  - Nedostatočne zabezpečená CI/CD pipeline
  - Nedostatočné pravidlá v EDR a slabá integrácia so SIEM
  - Nechránená LAN sieť

Pre koho je Red Teaming určený

- Každá organizácia, ktorá chce realisticky overiť a zlepšiť svoju kybernetickú odolnosť (od startup-ov až po nadnárodné spoločnosti)
- Organizácie disponujúce základnými bezpečnostnými opatreniami – EDR, SIEM, SOC,…
- Firmy pripravujúce sa na regulačné požiadavky DORA/NIS2
- Organizácie v citlivých/kritických sektoroch (financie, energetika, telekomunikácie a pod.)
- Organizácie dotknuté geopolitickou situáciou

Emulácia konkrétnej hrozby

- Scenáre útokov založené na realistických hrozbách vďaka ESET Threat Intelligence
- Možnosť emulovať konkrétnu hrozbu (APT skupinu, eCrime,…) zameriavajúcu sa na Váš sektor
- Threat-led Penetration Testing (TLPT) podľa DORA a TIBER-EU

Purple Teaming

- Štruktúrované kolaboratívne cvičenie
- Aktívna spolupráca Red Teamu a Blue Teamu, obrancovia vedia o teste a aktívne sa zapájajú
- Cieľom spoločne identifikovať a odstrániť medzery v detekcii a reakcii
- Súčasť Red Teamu alebo samostatne (navzájom komplementárne)

Red Teaming od ESETu

- Realistická emulácia útokov založená na dátach z celého sveta
- Tím odborníkov
- Test šitý na mieru Vašej spoločnosti (od najmenších firiem až po najväčšie)
- Možnosť kombinovať s inými našimi službami:
  - Sociálne inžinierstvo
  - Penetračné testy
  - Vzdelávanie pre developerov/používateľov/manažérov/...
  - Audity
  - Testy infraštruktúry

Viac informácii

- Služby ESET Services
  - https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/overview/
- Kontaktný formulár
  - https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/kontakt/
- Ubránili by ste sa reálnemu útoku? Red Team testovanie to preverí
  - https://bezpecnevofirme.eset.com/sk/nezaradene/ubranili-by-ste-sa-realnemu-utoku-red-team-testovanie-to-preveri/

SECURITY DAYS

Ďakujem za pozornosť!

Cybersecurity
Progress. Protected. & SME KONFERENCIE