Red Teaming

Nasimulujeme sofistikovaný útok na vašu spoločnosť a poskytneme vám informácie o pripravenosti vašej organizácie na odhalenie, elimináciu a realizáciu nápravných opatrení proti budúcim útokom.

Definícia rolí

RED TEAM
Naši špecialisti, ktorí simulujú taktiku, techniky a postupy útočníkov.

WHITE TEAM
Vybraný tím z vedenia spoločnosti, ktorý bude dohliadať na prebiehajúce cvičenie.

BLUE TEAM
Tím interných bezpečnostných špecialistov spoločnosti zistí útok a prijme potrebné protiopatrenia.

Ako funguje Red Teaming?

Red Team je náš tím etických hackerov, ktorí vykoná **simulovaný útok na vašu organizáciu** s cieľom preskúmať jej bezpečnosť a komunikáciu. Cvičenie pred zamestnancami utajíme a informácie o ňom poskytneme len vyššiemu vedeniu vašej spoločnosti. Použijeme sofistikované moderné nástroje, vyhodnotíme účinnosť ochrany a poskytneme vašim zamestnancom školenie v bezpečnom prostredí. Cieľom praktického testu je vždy **odhaliť rizikové miesta** a pripraviť vás na budúce kybernetické hrozby.

Potrebujem Red Teaming pri penetračných testoch?

Penetračné testovanie a vulnerability scanning sú neoddeliteľnou súčasťou bezpečnosti a tieto činnosti sa musia udržiavať, dodržiavať a rozvíjať. Takýto metodický prístup však nedokáže otestovať skutočnú pripravenosť, a tým ani čeliť kybernetickým hrozbám. Red Teaming ako simulácia skutočného útoku skutočne otestuje pripravenosť, schopnosť reakcie a následnej obnovy.

Penetračné testy

- Krátke trvanie (1-3 týždne)
- Správcovia a vlastníci aplikácie sú si vedomí prebiehajúceho testovania
- Cieľom je nájsť zraniteľnosti v danej aplikácii alebo infraštruktúre
- Prísne vymedzený obmedzený rozsah pôsobnosti
- Ďalšie vrstvy ochrany (WAF, IPS atď.) je možné deaktivovať na účely testovania
- Často sa implementujú v neprodukčnom prostredí

Red Teaming

- Dlhšie trvanie (v priemere 1-3 mesiace)
- Utajovaný priebeh, o činnosti vedia len členovia White Teamu.
- Neobmedzené testovanie všetkých vrstiev ochrany ako celku (technológie, ľudia, procesy, fyzická bezpečnosť)
- Zasahuje v produkčnom prostredí

Testovanie delíme do štyroch skupín:

Technológia
Interná infraštruktúra, cloud, aplikácie (webové, mobilné), servery, koncové zariadenia atď.

Ľudia
Interný a externý personál (zamestnanci, dodávatelia, dodávatelia, obchodní partneri atď.).

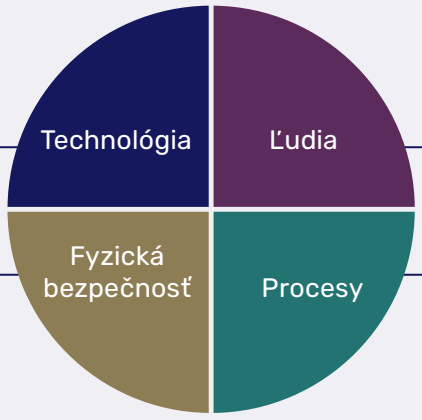
Procesy
Interné procesy (existencia, formálnosť, konzistentnosť a dodržiavanie), komunikácia medzi členmi obranného tímu.

Fyzická bezpečnosť
Testovanie fyzickej bezpečnosti budov, skladov, dátových centier, výrobných závodov atď.

Red Teaming

Red Team preskúma technológiu nielen z hľadiska potenciálnych zraniteľností, ale aj z hľadiska účinnosti nasadených obranných nástrojov.

Preverí sa schopnosť ľudí reagovať v prípade skutočného útoku na rozhodnutia manažmentu prijaté v krízovej situácii.



Testy fyzickej bezpečnosti vašej organizácie. .

Overuje nastavenie procesov vo vašej spoločnosti.