Red Teaming

Nasimulujeme sofistikovaný útok na vaši společnost a poskytneme vám informace o připravenosti vaší organizace budoucí útoky detekovat, eliminovat a provádět nápravná opatření.

Definice rolí

RED TEAM
Naši specialisté, kteří simulují taktiku, techniky a postupy útočníků.

WHITE TEAM
Vybraný tým z managementu společnosti, který dohlíží na probíhající cvičení.

BLUE TEAM
Tým interních security specialistů společnosti, který detekuje útok a provádí nutná protiopatření.

Jak Red Teaming funguje?

Red Team je tým našich etických hackerů, který provede **simulovaný útok na vaši organizaci** a prozkoumá její bezpečnost a komunikaci. Cvičení před zaměstnanci utajíme a informace o něm předáme jen vyššímu vedení vaší společnosti. Použijeme sofistikované moderní nástroje, zhodnotíme efektivitu ochrany a poskytneme vašim zaměstnancům trénink v bezpečném prostředí. Cílem praktického testu je vždy **odhalit riziková místa** a připravit vás na budoucí kybernetické hrozby.

Potřebuji Red Teaming při penetračních testech?

Penetrační testování a vulnerability scanning jsou nedílnou součástí bezpečnosti a je nutné tyto aktivity zachovat, dodržovat a rozvíjet. Avšak takový metodický přístup není schopen otestovat reálnou připravenost a tím čelit kybernetickým hrozbám. Red Teaming, jako simulace reálného útoku, skutečně ověří připravenost, schopnost reakce i následného zotavení.

Penetrační testy

- Krátká doba trvání (1-3 týdny)
- Administrátoři a vlastníci aplikace vědí o probíhajícím testování
- Cílí na nalezení zranitelností v dané aplikaci či infrastruktuře
- Striktně definovaný omezený rozsah
- Dodatečné vrstvy ochrany (WAF, IPS, atp) mohou být pro účel testů deaktivovány
- Často realizovány na neprodukčním prostředí

Red Teaming

- Delší doba trvání (průměrně 1-3 měsíce)
- Utajený průběh, pouze členové White Teamu vědí o aktivitě
- Neomezené testování všech vrstev ochrany jako celku (technologie, lidé, procesy, fyzická bezpečnost)
- Zasahuje v produkčním prostředí

Testování dělíme do čtyř skupin:

Technologie
Interní infrastruktura, cloud, aplikace (webové, mobilní), servery, koncová zařízení atd.

Lidé
Interní a externí personál (zaměstnanci, kontraktoři, dodavatelé, obchodní partneři atd.).

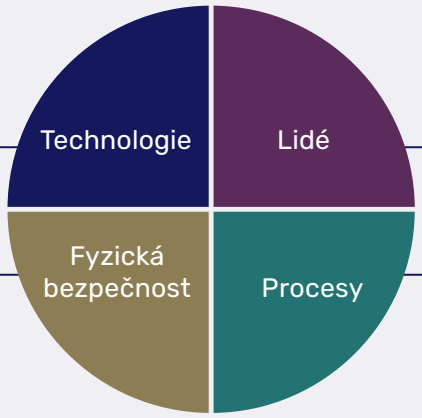
Procesy
Interní procesy (existence, formálnost, ucelenost a dodržování), komunikace mezi členy obranného týmu.

Fyzická bezpečnost
Testování fyzické bezpečnosti budov, skladišť, datacenter, výrobních závodů atd.

Red Teaming

Red Team prověří technologie nejen z pohledu možných zranitelností, ale z pohledu účinnosti nasazených obranných nástrojů.

Prověří schopnost lidí reagovat v případě reálného útoku na učiněné rozhodnutí managementu v krizové situaci.



Otestuje fyzické zabezpečení vaší organizace.

Ověří nastavení procesů uvnitř vaší společnosti.