

Incident Response



SOC a CSIRT aaS

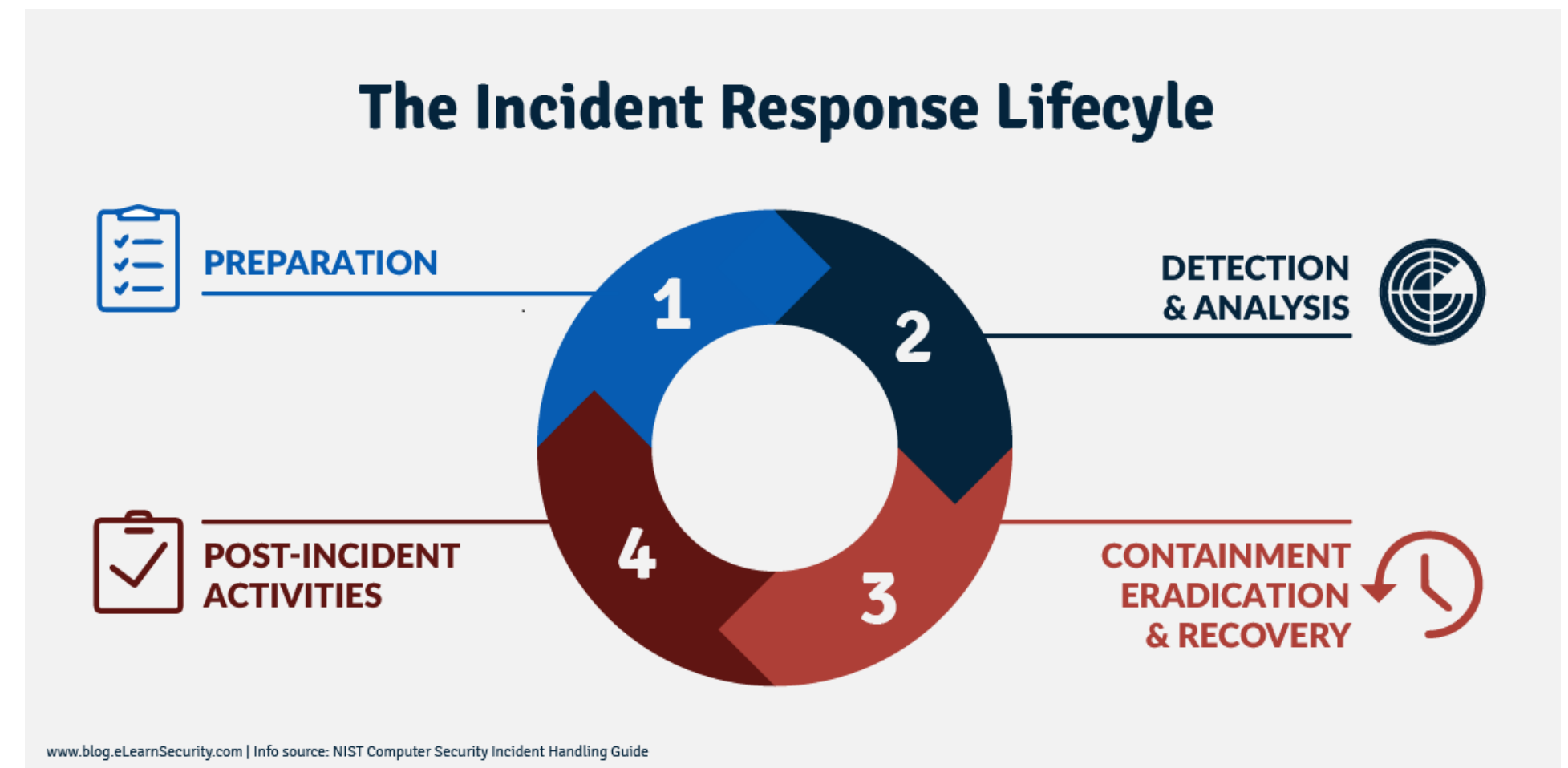
- Od roku 2014 prevádzkovateľ prvého SOCaaS na Slovensku
- Vznikol zo SOC tímu pre ochranu infraštruktúry EK
- Prvý slovenský komerčný člen medzinárodnej organizácie CSIRT tímov - TF-CSIRT
- 6 rokov organizátor slovenskej súťaže CSIRT tímov Guardians.sk
- Pravidelne sa umiestnuje na popredných miestach prestýžnych súťaží obranných tímov, ako napríklad openSOC pri DEF CON - 6 z 80 teamov vo finále 2021 a 2 v roku 2022



Čo je incident response?

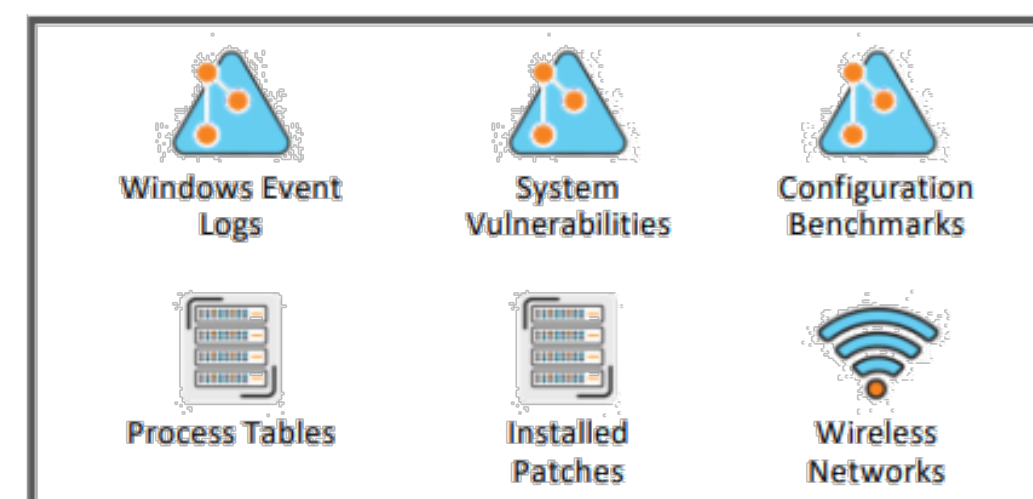
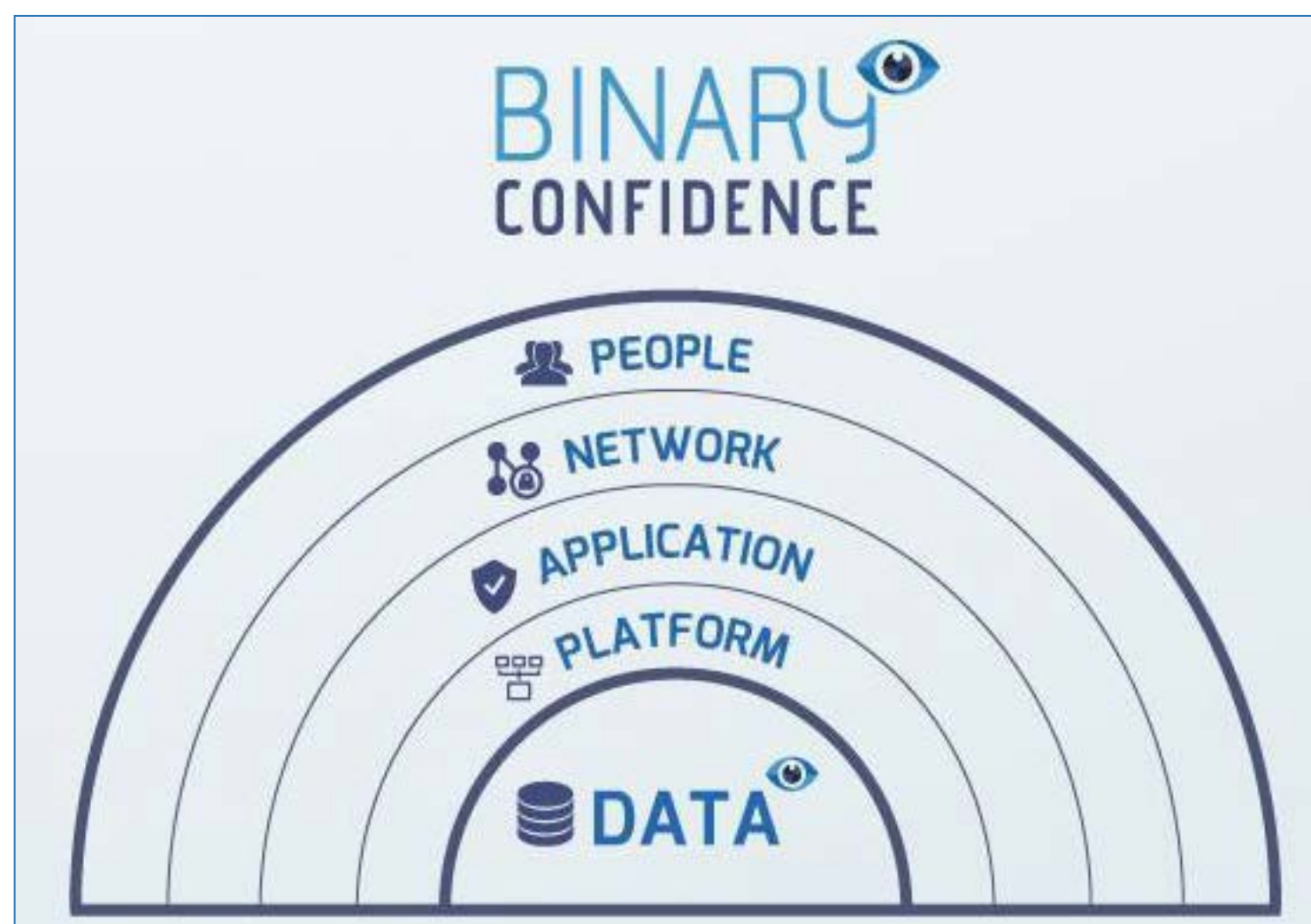
Reakcia na incident

1. Príprava
(nástroje, procedúry a tréning)
2. Detekcia a analýza
3. Izolácia a ochrana
Odstránenie hrozby
Obnovenie činnosti
4. Report a mitigation activities



Nástroje

Kontrola na čo najviac úrovniach
Logy logy logy
Zálohy



IR tím

Nie je dobré spoliehať sa na preposielača upozornení zo SIEMu

Dobrý ochranca musí vedieť útočiť

Dobrý ochranca musí mať skúsenosti, vedomosti a zručnosti

Part 1 - System administration

Part 2 - Network

Part 3 - Basic programming and scripting

Part 4 - Cryptography

Part 5 - Vulnerabilities search and penetration testing

Part 6 - Intrusions

Part 7 - Hardening and patching

Part 8 - Monitoring

Part 9 - Security standards and policies

Part 10 - tools and procedures

Incident podľa kritickosti

Operačný incident s nižším rizikom

Včasné varovanie napríklad z monitoringu

Pokus o aktívny prienik

Aktíva sú reálne ohrozené

Došlo k vážnemu porušeniu bezpečnostných politík

Rieši bežný IR/SOC analytik

Kritický incident

Došlo k vážnemu prieniku

Integrita, dostupnosť, alebo dôvernosť
bola stratená

Došlo k závažným škodám

Skladá sa ad hoc SIRT

CSIRTaaS

Počas, alebo po kritickom incidente

Zväčša externý klient bez monitoringu a SOCu

Približne 7-10 krát do roka

Motivácia: Obnoviť službu, zastaviť útok, zistiť čo sa stalo a nastaviť prevenciu, odhaliť útočníka.

Priebeh CSIRTaaS

1. Prvotný zber informácií a vyhodnotenie (do 2h)
2. Zloženie CSIRT tímu podľa potrieb z bodu 1 (bezpečnostné technológie, komunikácia, právnik, obnova systémov atd...)
3. Občas hĺbková analýza uskutočniteľnosti (1-2 dni)
4. Ochrana prostredia, odstránenie hrozby a obnova služieb
5. Report a návrh ďalších a preventívnych opatrení

Kritické incidenty

1. 67% Ransomware
2. 16 % Podhodené faktúry (5000EURO - 40 000EURO)
3. 1 prípad APT (strata 250 000EURO)
4. 12 % Pomsta bývaleho zamestnanca
5. 1 prípad priemyselná špionáž
6. 2 prípady vyhrážania a vydierania korporácie

Postrehy

1. Prevencia, monitoring a SOC prudko znižuje riziko kritického incidentu
2. Nie každý si to môže dovoliť a nie každému sedí business case
3. Keď už si to niekto môže dovoliť, mal by vedieť rozoznať kvalitu. Niekedy sú SOC vyhodené peniaze.
4. CTF a rôzne súťaže zlepšujú pripravenosť riešiť incident
5. Vzdialené riešenie aj kritických incidentov (pre nás od 2019)
6. Riešenie incidentov v cloud technológiách sa stáva štandardom od 2020.



Ďakujem za pozornosť

www.binconf.com