NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Security Operations Center

Koncepce, provoz, rozvoj

25.4.2019 Praha Petr Slavík

Koncepce SOC

Účel budování SOC

- Monitoring a eskalace
- + incident response
- + poradenská činnost apod.

Režim

- Faktory určující režim – počet lidí a počet hodin zajištění SOC
- X x Y
- X x Y + pohotovost
- 24 x 7
- Fyzické prostory

SLA

NAKIT

Faktory ovlivňující úspěch SOC

Zdroje a podpora managementu

- Chránit a podporovat misi SOC
- Finance

Kultura organizace

- Jeden z klíčových faktorů
- Spolurozhoduje o rychlosti implementace a výsledcích práce

Umístění v rámci organizace

- V rámci IT bezpečnosti (pod CISO)
- Ve struktuře IT
- Mimo IT

Oprávnění/mandát v režimu řešení závažných incidentů

- Primárně pro incident response
- Začlenění do krizového řízení v společnosti

NAKIT

Personální zabezpečení SOC

Rozvoj personálních zdrojů SOCu

- Pyramidová struktura pro standardní provoz (L1/L2/L3) ?
- Identifikace lidského potenciálu a práce s ním
- Najímání zkušených L2/L3 mimo společnost vs. povyšování v rámci týmu

Zapojení HR do osobnostního rozvoje

- „výzvy“ ($) v oblasti specifických technických školení
- Soft skills pro analytiky na vyšších úrovních
- Rotace v rámci funkcí SOC i lokací kde SOC operuje (v případě více regionů)

Komunikace a kooperace mimo SOC

- Zaměření na budování sítě kontaktů mimo SOC – kritické primárně pro incident response
- Budování reputace SOC v rámci (IT) organizace – od generátoru incidentů k „partnerství“
- Spolupráce s NUKIB a CSIRTs (Computer Security Incident Response Team)

NAKIT

Organizace a fungování SOC

Zaměření bezpečnosti nebo jednotky

- Koncentrace na „čistou“ bezpečnost vs. pokrývání části provozních aktivit
- Co různá prostředí DEV/TEST/PROD
- Jak v cloudu, pojmy jako DevSecOps aj.

Funkční bloky jednotky

- Tým operátorů a analytiků pro standardní provoz
- Správa/rozvoj nástrojů
- Threat Intel / externí komunikace
- Incident response tým
- Propojení na ostatní funkce IT bezpečnosti v organizaci (vzdělávací a osvětové programy, architektura, risk assessment, service desk)

NAKIT

Potenciál nástrojů pro SOC

V rámci monitoringu jsou primárně používány

- SIEM systémy
- Nástroje pro řízení bezpečnostních incidentů (v rámci ITSM, či samostatně)
- Specializované prostředky pro vyšetřování (EDR/MDR – antivirus, threat intel, machine learning, sand box)

Maximalizace potenciálu vs. rozšíření počtu nástrojů

- Ladění stávajícího řešení vs. implementace dalšího produktu
- Výzva pro vedení – nutná schopnost „prodat“ technickou analýzu
- Komu patří management FW, IDS, Vulnerability scany apod.?
- Je to skutečně jen o nástrojích ?
- Assume breach, Security by default, Security by design…

NAKIT

Služby SOC DCeGOV

Primární zákazník MV ČR

- SOC pro eGovernment
- Služby pro státní a veřejnou správu
- PREVENCE - DETEKCE – REAKCE (dle pokynů a na základě souhlasu správce-zákazníka)

Možnosti spolupráce

- Vzdělávání, výměna zkušeností
- Komunikace v rámci CSIRT/CERT komunity
- Možnost nabízet služby SOC dalším subjektům?

NAKIT

O jakých datech to je?

Log Management statistika a trendy

Parametr	Měsíc 1	Měsíc 2	Měsíc 3
Uloženo zpráv (GB)	14 293	12 922	11 871
Průměr uložených zpráv (GB/day)	461	417	383
Počet přijatých a uložených zpráv (mil)	28 327	25 879	28 504
Průměrný počet EPS	10 929	10 697	10 997

	Měsíc 1	Měsíc 2	Měsíc 3
SIEM alerty (Triage)	1089	2 085	2 078
Bezpečnostní incident	1	4	1
Bezpečnostní událost	49	28	17
Analytická činnost	42	98	151
Optimalizace a správa bezpečnostních nástrojů	57	68	67

NAKIT

Děkuji

Q&A

Petr Slavík
Vedoucí odboru Informační bezpečnosti a BCM

E: petr.slavik@nakit.cz
M: +420 731 553 223
W: www.nakit.cz

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.