Není SOC jako SOC aneb naše cesta i k vaší bezpečnosti

Dalibor Lukeš
Ředitel pro ICT produkty a služby
Vodafone Business

vodafone business

Co to vlastně je SOC a kde je jeho místo v bezpečnostní architektuře

Proč existuje více typů SOCů a jak poznat „správný“ pro vaši organizaci

Jak vybírat platformu a provozní model

vodafone business

SOC – Jedna zkratka, různé významy

SOC – Security Operations Center
Centrum kybernetické bezpečnosti pro monitoring, detekci a reakci na incidenty v režimu 24/7

SOCaaS – SOC as a Service
SOC poskytovaný jako služba – bez nutnosti budovat vlastní tým a infrastrukturu.

SOC – Service Operations Center
Provozní dohled nad IT a síťovými službami (dostupnost, výkon, provoz).

SOC (SOC 1 / SOC 2 / SOC 3)
Auditní reporty hodnotící bezpečnost, procesy a compliance poskytovatele.

vodafone business

Proč potřebujete SOC

Strategická ochrana vaší organizace v současné éře rostoucích kybernetických hrozeb

91K

91 000 kyberútoků v ČR

Počet útoků na klienty českých bank v roce 2025. Česko patří mezi nejvíce napadané státy v EU.

2.1

2,13 mld. CZK ukradeno v ČR

Škody od kybernetických podvodů v ČR vzrostly o 53 % meziročně. Průměrná škoda na incident +47 %.

3 %

3 % firem v EU splňuje kyber-readiness

Pouze 3 % organizací v EU dosáhla úrovně kybernetické připravenosti „Mature" dle Cisco 2025. V EU chybí 200 000 specialistů.

NIS2

ZoKB & NIS2 PLATNÝ ZÁKON

Nový ZoKB platí od 1. 11. 2025. Pokuty až 250 mil. CZK nebo 2 % obratu. Povinný monitoring a hlášení incidentů.

Zdroje: NÚKIB 2026, ČBA 2025, Cisco 2025

vodafone business

Místo pro SOC v bezpečnostní architektuře

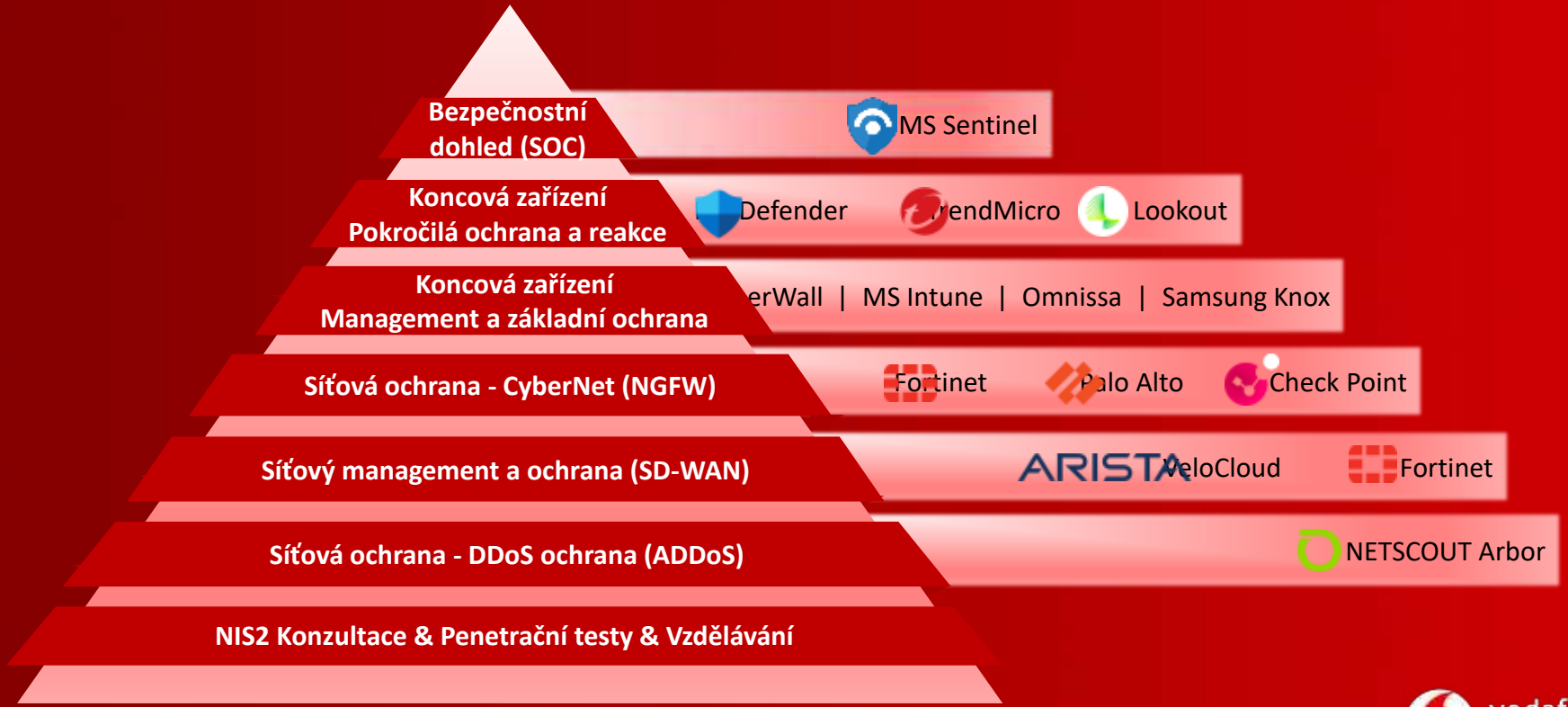
Ochrana zařízení

Celková kyberimunita

Zabezpečení sítě

vodafone business

Příklad – Vodafone koncept kybernetické bezpečnosti



vodafone business

Z čeho se skládá SOC?

vodafone business

Není jen jeden SOC

Interní SOC

- Vlastní tým, nástroje a procesy
- Plná kontrola nad daty, bezpečností a prioritami
- Vysoké náklady (lidé, 24/7, technologie)
- Vhodné pro: velké organizace, kritická infrastruktura

MDR / XDR-driven SOC

- Zaměřeno na Detekci a reakci nad zařízeními
- Silná automatizace, menší důraz na SIEM/komplexní governance
- Rychlá hodnota, ale omezenější rozsah
- Vhodné pro: menší organizace, rychlé „security uplift“

Hybridní / Co-managed SOC

- Sdílený model: zákazník + poskytovatel
- Interní tým + externí detekce / monitoring / tooling
- Flexibilita a postupný rozvoj schopností
- Vhodné pro: organizace s částečnou interní kapacitou

SOC jako služba (SOCaaS)

- SOC provozovaný externím poskytovatelem
- Rychlé nasazení, nižší nároky na interní kapacity
- Jasně definovaný rozsah a SLA (co je / není pokryto)
- Vhodné pro: veřejná správa, mid-market, organizace bez 24/7 týmu

Interní vs. zákaznické služby

vodafone business

3x Vodafone SOC

Interní SOC

Zaměření:
- Ochrana interní infrastruktury Vodafone (IT + network)

Charakteristika:
- Dohled nad celým prostředím a poskytovanými službami
- Přímá vazba na NOC a provoz
- Vysoká integrace do interních procesů

VBSOC

Zaměření:
- Detekce a reakce (MDR)
- Primárně pro menší organizace

Charakteristika:
- Rychlé nasazení
- Vysoká automatizace
- Omezenější rozsah (primárně koncová zařízení)

Vodafone SOC

Zaměření:
- Plnohodnotný SOC jako služba
- Veřejná správa + střední a větší organizace

Charakteristika:
- SIEM + SOAR + governance
- Možnost řešení na míru pro interní SOC klienta
- Jasný rozsah, SLA, reporting

3 modely podle potřeby: interní provoz | rychlá ochrana | enterprise SOC

vodafone business

Jak jsme vybírali platformu pro Vodafone SOC

Očekávání

- End-to-end SOC schopnost(detekce→ investigace → reakce → report)
- Pokrytí: identity | endpoint | network | cloud
- 24/7 provoz + škálovatelnost (multi-tenant)
- Podpora SOC jako služby (SOCaaS)
- Compliance: NIS2 / ZoKB / auditovatelnost

Hodnocení

Technologie

- Integrace dat (IT, cloud, identity)
- Korelace & detekce (rules + anomaly)
- Threat Intelligence enrichment

Provoz

- Automatizace (SOAR, playbooky)
- Multi-tenant & role model
- Reporting & governance

Výsledek – Microsoft Sentinel

- Cloud-native SIEM + SOAR
- Silná integrace: M365, Defender, Entra ID
- Podpora:
    - SOCaaS
    - Custom SOC pro klienty
- Automatizace + škálování

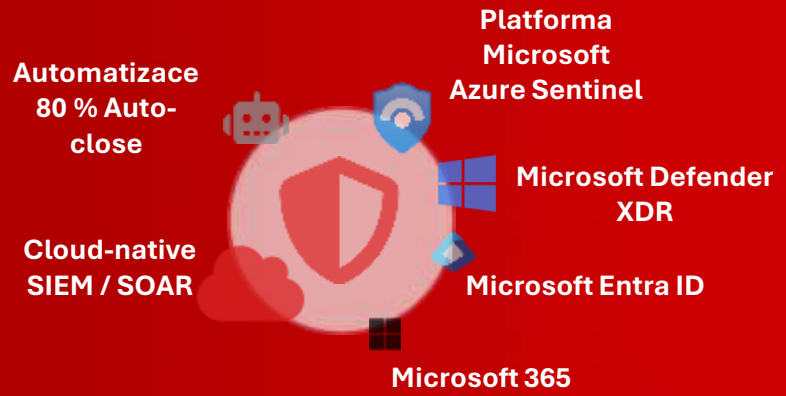
„Nevybírali jsme SIEM nástroj, ale platformu pro dlouhodobý provoz SOC jako služby.“

vodafone business

Vodafone SOC – platforma

Microsoft Sentinel

- Cloud-native škálovatelné a nákladově efektivní SIEM / SOAR řešení
- Kombinuje umělou inteligenci, automatizaci a threat intelligence
- Cíleně podporuje detekci hrozeb, jejich vyšetřování, reakci na incidenty a proaktivní vyhledávání hrozeb



vodafone business

Vodafone SOC – Bezpečnostní dohledové centrum

24/7 Monitoring & Dohled

- Dohled nad infrastrukturou 24x7
- Triáž a klasifikace incidentů
- Reakce v režimu 8×5 / 10×5

Technologická platforma

- B2B propojení tenantů. SIEM / SOAR jádro postavené na MS Azure
- Automatizace bezpečnostních procesů
- Ověřená detekční pravidla

Zaměřeno na identitu

- Active Directory (Entra ID on-prem) jako hlavní zdroj signálů
- Detekce kompromitovaných účtů a neautorizovaných přístupů

Lokální tým v ČR

- SOC centrum v Praze
- Kompletní podpora v CZ, SK a EN
- Osobní konzultace a pravidelný reporting

Onboarding

Napojení systémů, konfigurace pravidel, komunikační matice
Délka: 2 – 4 týdny

Fine-tuning

Ladění korelačních pravidel na míru vašemu prostředí. Zapojení EDR
Délka: 2 – 4 týdny

Ostrý provoz

Automatická detekce, triage zkušeným analytikem, notifikace s doporučením v režimu 24/7

vodafone business

Proč Vodafone Business i pro váš SOC?

Zkušenosti nadnárodní společnosti

Opíráme se o mnohaleté zkušenosti z mezinárodního prostředí.
Díky tomu vytvoříme tu nejvhodnější kombinaci.

Nejvyšší standardy zabezpečení

Jsme součástí kritické infrastruktury státu. Provozujeme vlastní SOC i NOC.
Proto mají naše sítě a datová centra nejvyšší nároky na bezpečnost.

Komplexní zabezpečení firemní sítě

Poskytujeme kompletní služby od spojení a síťového připojení, až po nejkvalitnější zabezpečení dat a ICT služby.

vodafone business

Zajímá Vás víc?

Navštivte nás na našem stánku

vodafone business

vodafone
business

Together we can