

Přínosy integrace nástrojů detekce a reakce pro budování kybernetické bezpečnosti



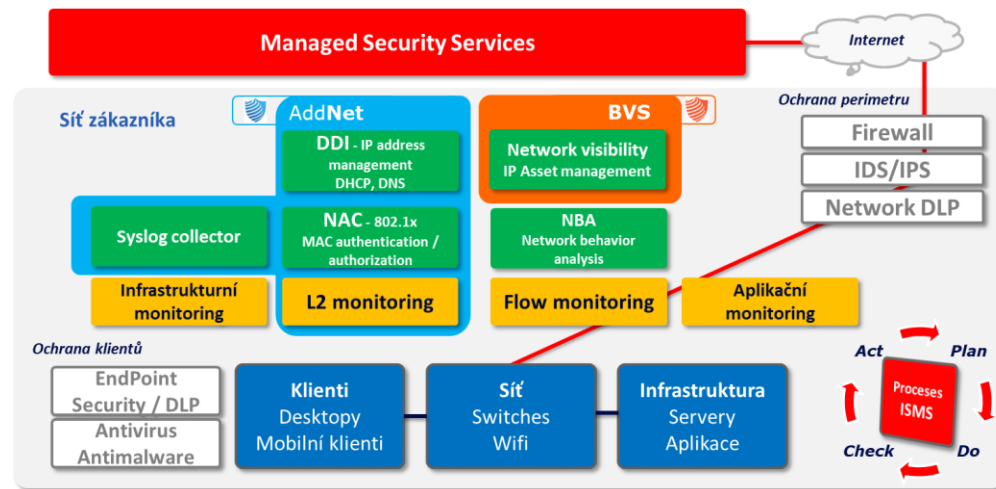
Jindřich Šavel

26.09.2019

Kam kráčí kybernetická bezpečnost?

■ Komplexnost

- Správa rizik a řízení systému bezpečnosti
- Ochrana perimetru
- Ochrana klientů
- Ochrana vnitřní sítě
- Nástroje pokročilé detekce
- Log management
- Nástroje řízení bezpečnostních incidentů
- ...



Kam kráčí kybernetická bezpečnost?

■ **Nedostatek lidí a jejich nedostatečná připravenost**

- **Školy neprodukují bezpečnostní specialisty** v dostatečné kvalitě a množství
- **IT specialisti nejsou trénováni** na řešení bezpečnostních incidentů
- **Bezpečnostní specialisté nejsou trénováni na spolupráci** při řešení bezpečnostních incidentů
- **Management organizací není trénován** a připraven na postupy při řešení bezpečnostních incidentů

Technologie

velký výběr:
- komerční řešení
- opensource nástroje



Lidské zdroje

- **nedostatek sil na pracovním trhu**
- **nepřipravenost pro 24x7x365**



Znalosti

- **nedostatečné detekční znalosti**
- **neschopnost reagovat na incidenty**



■ Automatizace

- **Využívání umělé inteligence** pro zrychlení řešení incidentů
 - detekce, reakce
 - jejich kombinace
- **Nová generace nástrojů**
 - nahrazují pracné vyhodnocování bezpečnostních incidentů v neustále se rozšiřujícím proudu informací
 - ADR, UEBA apod.
 - dramaticky zjednodušují operace síťové správy
 - DDI/NAC

■ Outsourcing

- **Využití externího SOC (Security Operating Centre)**
 - Zajištění provozu 24x7
 - Řešení problému nedostatku kvalifikovaných odborníků
 - Operátoři helpdesku
 - Bezpečnostní analytici



■ Pasivní SOC

- První generace bezpečnostních služeb se zaměřuje na vyhodnocování provozu organizací a vyhledávání bezpečnostních incidentů
 - Bezpečnostní hotline a metodické doporučení ke zjištěným hrozbám
- Zjištěné bezpečnostní incidenty jsou předávány organizaci k dořešení
 - Nutná součinnost s interními zdroji organizace
- Problematická akceschopnost v mimopracovní dobu

■ Aktivní SOC

- Dokáže zajistit plnohodnotný incident response bez nutné součinnosti s interními zdroji organizace

Služba SOC bez integrovaných nástrojů řízení sítě zákazníka nedokáže aktivně a samostatně řešit incident response

Nástroje pokročilé detekce

- **Klienti**
 - sledování chování uživatelů
- **Sít'**
 - sledování síťových anomálií
- **Kombinované pokročilé nástroje**
 - využívající
 - více zdrojů dat,
 - metody strojového učení
 - Nabízející obsluhu návrh vhodného řešení



Jsem schopen vždy reagovat?

- Co potřebuji pro reakci?

- **Vidět a mít detailní povědomí o chráněném prostoru**

- Úplnou visibility aktiv a jejich komunikace
- Znalost důsledků nedostupnosti aktiv na provozované business služby (aplikace)



- **Být schopen reagovat – tj. sdílet nástroje s provozovatelem SOC**

- Integrovaná správa sítě
 - základní síťové služby – DDI/NAC
- Podpora správy a monitoringu v rozsáhlých sítích



- už dnes připravený pro potřeby pokročilého modelu bezpečnosti

- kompletně zjednodušuje potřeby síťové IP správy a potřeb zabezpečení přístupu do sítě – **zavádí pořádek v síti**
- flexibilní podpora distribuovaného modelu sítě umožňuje zajistit kompletní **sběr informací**
 - z provozu **DDI/NAC**
 - z **L2 monitoringu** o výskytu zařízení v síti
 - o datových tocích v rámci vzdálených lokalit (**Netflow/IPFIX**)
 - o logách díky možnosti sběru **syslogů** ve vzdálených lokalitách
- **vyhodnocení bezpečnostních incidentů v rámci SOC**
 - zjištění dopadů zařízení na buss. služby
- **zajištění okamžité reakce na zjištěné hrozby – incident response**



Integrovaný **DDI/NAC nástroj** pro síťovou viditelnost, pokročilou správu IP adresního prostoru a řízení bezpečnosti přístupů v síti

**Network
Visibility**
•
Control
•
Security



NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER

Klíčové přínosy AddNetu

- ✓ **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- ✓ **Řádové snížení pracnosti síťové správy**
- ✓ **Standardizace činností a centralizace správy** v rozsáhlých sítích
- ✓ **DDI** – zavedení integrovaných základních síťových služeb (IPAM/DHCP/DNS)
- ✓ **NAC – snadné zavedení a správa**
 - Autentizace - full 802.1x a/nebo MAC
 - Autorizace - řízení VLAN
- ✓ **Pokročilé síťové politiky**
 - Prevence nákaz typu **ransomware**
 - Automatizovaná správa důvěryhodných zařízení – **trusted pools**
- ✓ **BYOD** – automatizovaná správa a identifikace BYOD a mobilních zařízení
- ✓ **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- ✓ **Úspora nákladů** díky sledování utilizace aktivních prvků, zvýšené produktivitě apod.
- ✓ **Plná heterogenost** - bezproblémová spolupráce běžnými síťovými technologiemi
- ✓ **Schopnost okamžité reakce** na kybernetické bezpečnostní incidenty
- ✓ **Podpora konceptu Aktivního SOC**
- ✓ **Snadná implementace** a ověřené projektové postupy – NIM metodika

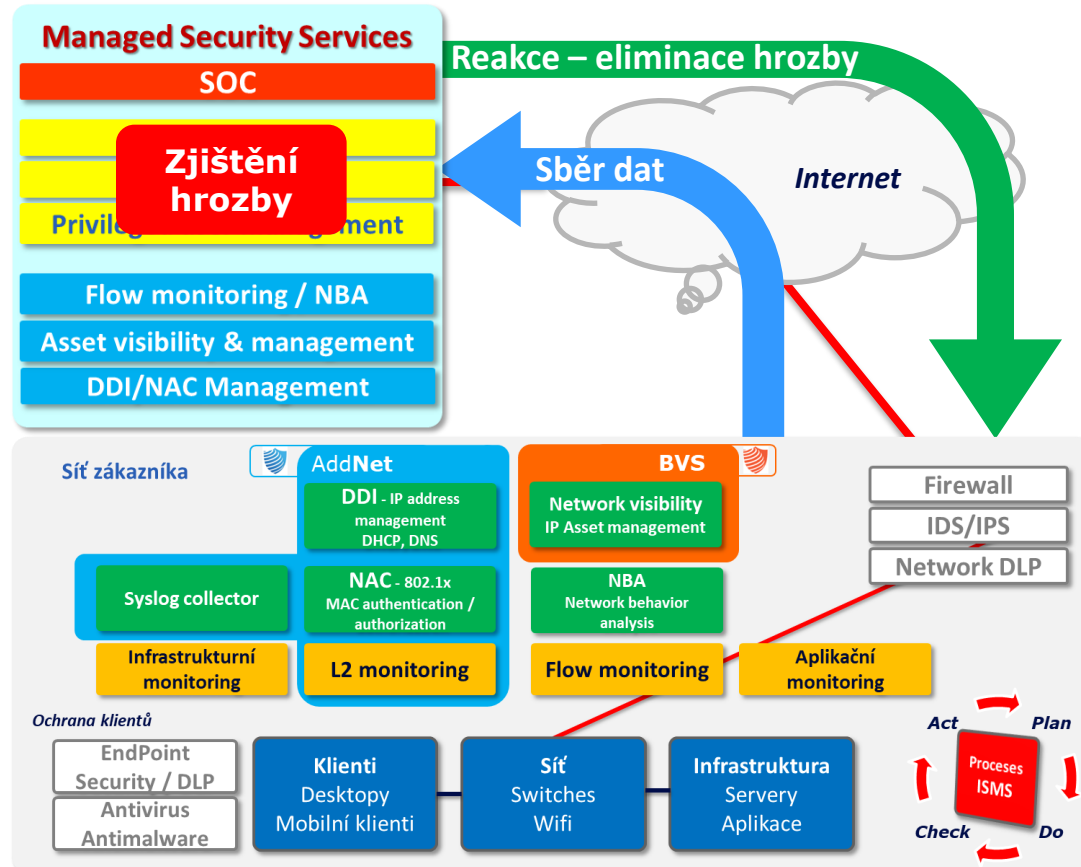
- navržený pro potřeby pokročilého modelu bezpečnosti

- pomáhá zmapovat stav provozovaných IT aktiv, držet jejich reálný přehled a vizualizovat jejich komunikaci – **zavádí přehled a pořádek v síti**
- umožňuje bezpečnostním operátorům stanovit dopady útoků na provozované business služby
 - přináší možnost provést kvalifikované rozhodnutí pro realizaci **incident response**
- umožňuje provádět zpětné vyšetření bezpečnostních incidentů a jejich šíření v organizaci



Spolupráce Novicomu s provozovateli služby SOC

- Společně se dosahuje výrazně vyšší užitná hodnota služby SOCu
 - **Správa a viditelnost IT assetů**, vč. návaznosti dopadů na business
 - **Zavedení pořádku v síti**
 - DDI/NAC
 - Pokročilé síťové politiky
 - **Standardizovaný sběr informací**
 - L2, Flow, Syslog
 - **Schopnost okamžité reakce 24x7** bez nutné součinnosti zákazníka
- **SOC za 2 dny?** **Proč ne?**



- **Plně podporuje nastupující trend SOC jako služby**
- **Zajištění okamžité reakce**
 - a jasné definice odpovědnosti mezi interní bezpečnost/IT a poskytovatelem služby bezpečnostního dohledu
 - **Pasivní SOC x Aktivní SOC**
- **Vyzkoušené spolupracující nástroje**
 - zvyšující celkovou efektivitu a rychlost reakce
 - **Detekce**
 - Flowmon ADS
 - SIEMy,...
 - **Reakce**
 - Novicom AddNet
 - Novicom BVS



- **Novicom, s.r.o.**
 - **Třebohostická 14**
 - **100 00 Praha 10**
 - **www.novicom.cz**
 - **sales@novicom.cz**

- **Jindřich Šavel**
 - **Sales Director**
 - **jindrich.savel@novicom.cz**
 - **[+420 271 777 231](tel:+420271777231)**
 - **[+420 777 222 961](tel:+420777222961)**