Integrovaný DDI/NAC a vizualizace komunikace IT aktiv, jako základ rychlé reakce SOC

AddNet

BVS

Vítězslav Šavel

20.09.2018

Kybernetická bezpečnost – současný stav

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

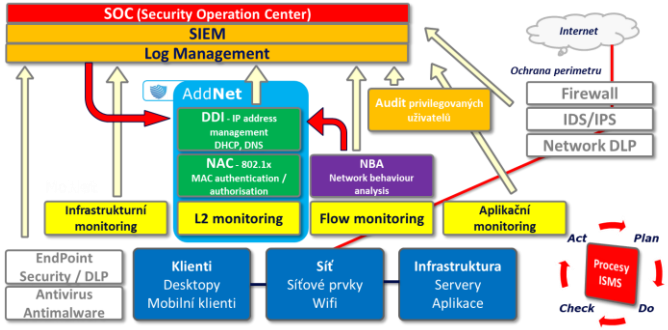
Kybernetická bezpečnost – jaký je optimální model?

- **Pokročilý model bezpečnosti**
- **Zajištění provozních potřeb sítě**
  - Inhouse (alernativně outsourcing)
  - Potřeba provozu typicky 8-17
- **Zajištění bezpečnostních potřeb sítě**
  - Poskytovatel služeb
  - Potřeba provozu 24x7x365

Méně než 5% zákazníků je schopno zajistit vybudování a provoz vlastního bezpečnostního analytického týmu

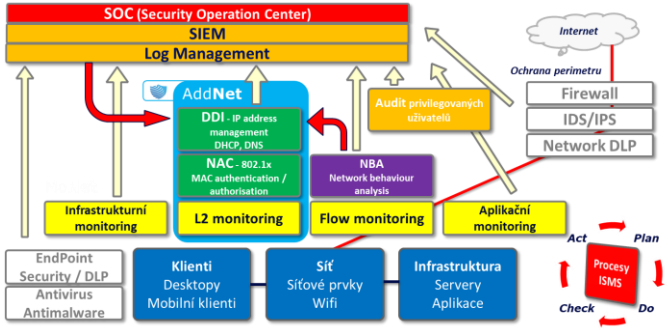
Zajištění provozních potřeb sítě

- **Konvenčně zvládnuto**
  - základní správa sítě a stanic
  - ochrana perimetru (firewall)
  - ochrana klientů (antivirus, antimalware)
  - infrastrukturní monitoring
- **Nezvládnuté nebo podceňované**
  - ***Síťová visibilita a správa IT assetů***
  - ***Komplexní správa IP prostoru***
    - Dílčí řešení: Open source nástroje X Microsoft
    - DDI (DHCP, DNS, IPAM)
  - ***Řízení přístupu do sítě (NAC)***
    - Autentizace, Autorizace (přiřazení zařízení do VLAN)



Zajištění bezpečnostních potřeb sítě

- **Pokročilá detekce**
  - vyhodnocení provozu
    - flow monitoring, syslog,…
    - klienti
- **Bezpečnostní dohled**
  - služba SOC (Security Operating Center)
    - využití nástrojů Logmanagment/SIEM
- **Zajištění incident response**



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

- **Potřeba znalosti chráněného perimetru**
  - **Sběr informací o provozu** zařízení v síti pro jejich vyhodnocení v SOCu (**L2 monitoring, netflow, syslog**)
  - **Visibilita IT aktiv a jejich komunikace**
  - Znalost **souvislostí mezi IT prostředky a business službami** organizace
- **Potřeba zajištění okamžité reakce - schopnost ovládání sítě**
  - **Řízení základních IP síťových služeb** (**DDI** - IPAM/DHCP/DNS)
  - **Řízení přístupu do sítě** a pokročilých síťových politik (**NAC** a izolace zařízení)

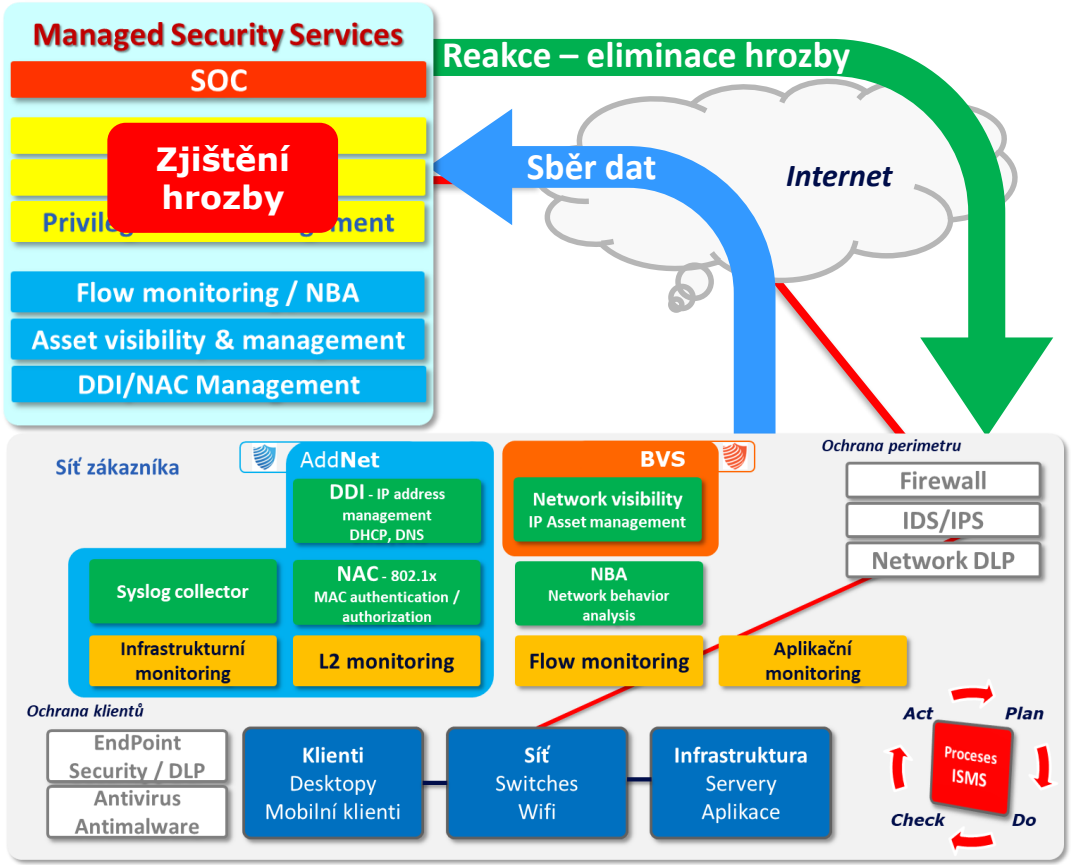
A jak můžou pomoci řešení Novicomu?

- **Potřeba znalosti chráněného perimetru**
  - AddNet: **Sběr informací o provozu** zařízení v síti pro jejich vyhodnocení v SOCu (**L2 monitoring, netflow, syslog**)
  - BVS: **Visibilita IT aktiv a jejich komunikace**
  - BVS: Znalost **souvislostí mezi IT prostředky a business službami** organizace
- **Potřeba zajištění okamžité reakce - schopnost ovládání sítě**
  - AddNet: **Řízení základních IP síťových služeb** (**DDI** - IPAM/DHCP/DNS)
  - AddNet: **Řízení přístupu do sítě** a pokročilých síťových politik (**NAC** a izolace zařízení)

Spolupráce Novicomu s provozovateli SOCu

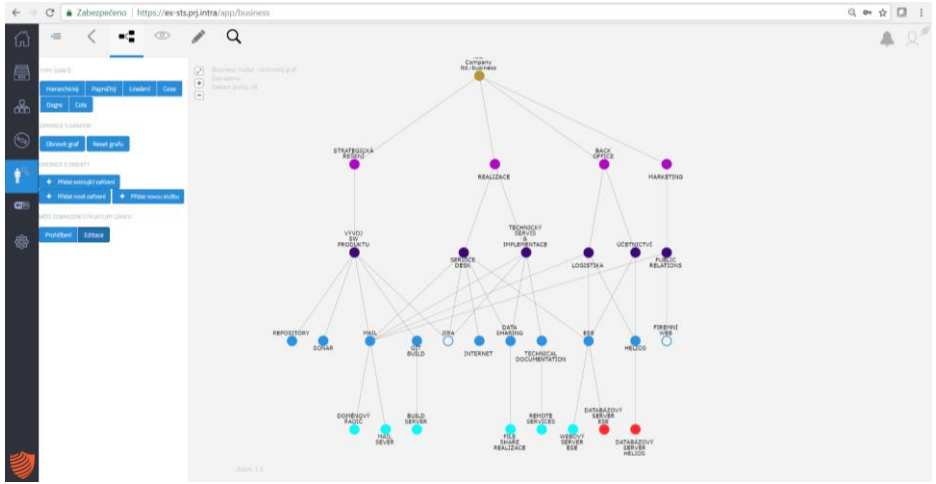
- **Společně se dosahuje výrazně vyšší užitná hodnota služby SOCu**
  - **Správa a visibilita IT assetů**, vč. návaznosti dopadů na business
  - **Zavedení pořádku v síti**
    - DDI/NAC
    - Pokročilé síťové politiky
  - **Standardizovaný sběr informací**
    - L2, Netflow, Syslog
  - **Schopnost okamžité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

Proč ne?



Co je BVS?

- Nástroj pro přehlednou vizualizaci síťových komunikací a modelování souvislostí business služeb s IT infrastrukturou



Jaké problémy řeší?

- Chybějící přehled o aktuálním stavu, rizicích a zdraví IT infrastruktury a jejím dopadu na provoz klíčových služeb.

Co BVS není:

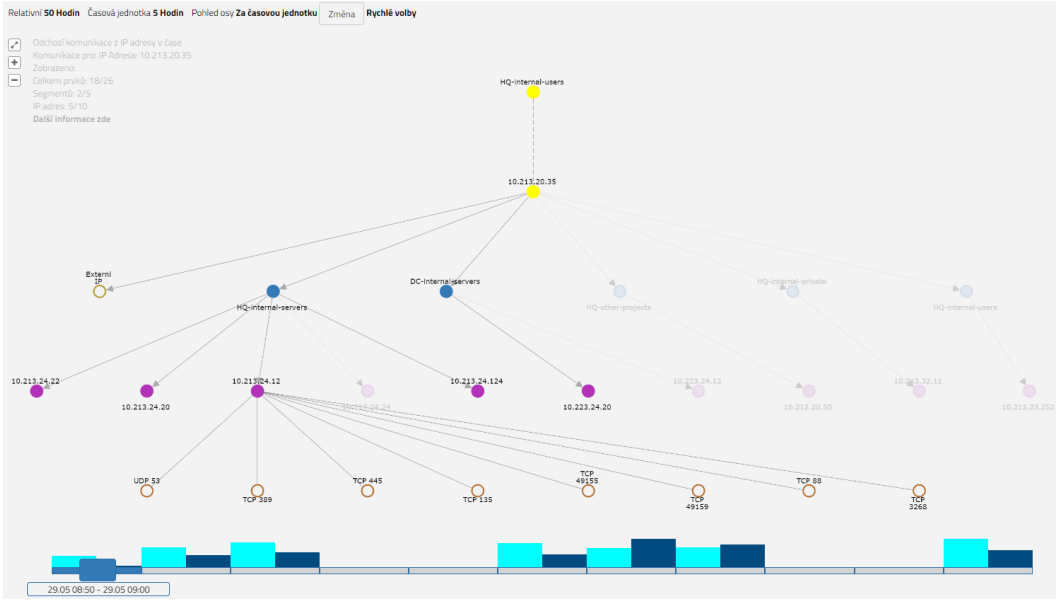
- Analyzátor datových toků, SIEM, AM, performance a application monitoring, velké CMDB

BVS

BVS – Network edition

- **Detekce reálného stavu a komunikací** IT infrastruktury
- **Přehledná vizualizace** s rychlou orientací ve vlastním IT prostředí
- **Získání kontextu bezpečnosti nad IT aktivy** (risk indikátory, zranitelnosti)
- **Pohled na chování infrastruktury v čase**

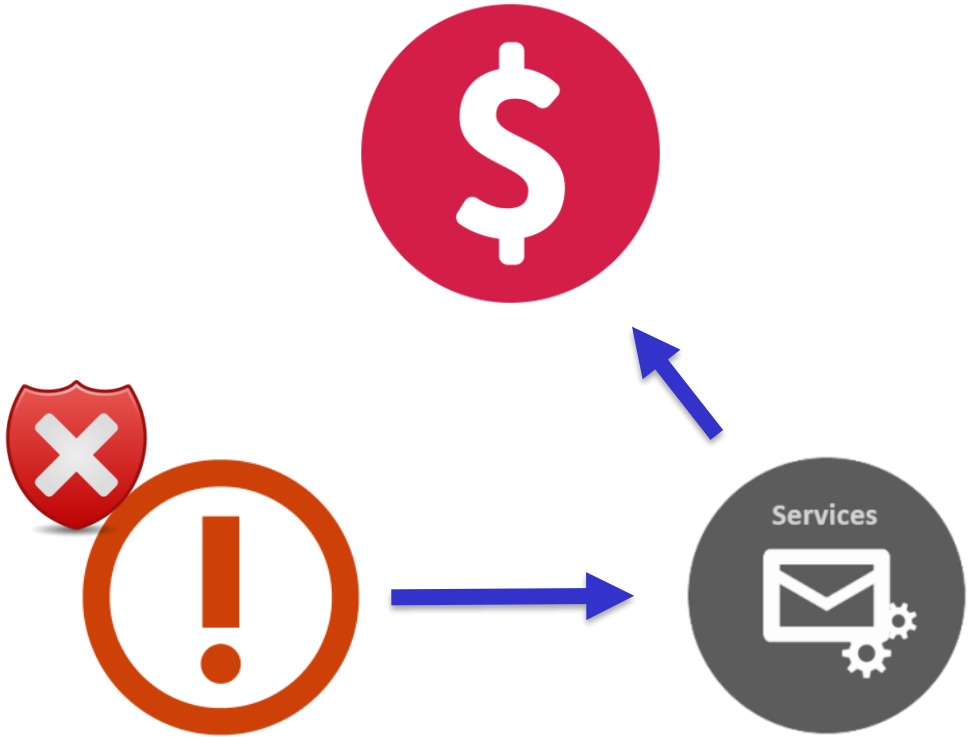
Hlavní výhodou obránců proti kybernetickému útočníkovi je dokonalá znalost vlastní IT infrastruktury



BVS – Business edition

Využití BVS

- Přináší **okamžitý přehled o zdraví a reálném stavu** poskytovaných business služeb
- Vytváří **evidenci klíčových procesů** organizace a jejich kritičnost
- **Mapuje vazby procesů / služeb** na technická aktiva
- **Řídí efektivně vlastní IT a business architekturu s ohledem na IT rizika**
- Spoléhá se vždy na **aktuální data o aktivech a souvislostech**



Hlavní obchodní scénáře

Hlavní případy užití BVS v následujících oblastech

1. Migrace systémů z datových center do prostředí cloudu
2. Onboarding dohledových služeb a podpora Security Operations center (poznání zákazníka)
3. Týmy IT/Security pro šetření dopadů incidentů a eliminace shadow IT
4. Vizibilita business procesů/služeb a vizualizace vztahů s IT provozem
5. Usnadnění iniciálních kroků při implementaci NAC řešení

Business Visibility Suite

- **Nástroj pro přehlednou vizualizaci síťových komunikací a modelování souvislostí business služeb s IT infrastrukturou**
- **Řeší chybějící přehled o aktuálním stavu, rizicích a zdraví IT infrastruktury a jejím dopadu na provoz klíčových služeb**

BVS Network Edition

- vizualizace aktuálního stavu IT infrastruktury
- zachycení komunikací mezi IT zařízeními s uložením historie komunikací
- poskytuje představu o chování sítě – jaký typ provozu se v dané lokalitě vyskytuje

BVS Business Edition

- nadstavba nad síťovým modulem
- umožňuje modelování business služeb a jejich závislostí na IT infrastruktuře
- dává aktuální pohled na význam a kritičnost IT zařízení při provozování klíčových služeb

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

Network

Visibility

•

Control

•

Security

AddNet – provozně bezpečnostní nástroj

- už dnes připravený pro potřeby pokročilého modelu bezpečnosti

- **kompletně zjednodušuje potřeby síťové IP správy a potřeb zabezpečení přístupu do sítě – zavádí pořádek v síti – DDI/NAC**
- **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**
- **zajištění okamžité reakce na zjištěné hrozby – incident response**

Původní Novicom technologie

- **Novicom SGP (Secure Grid Platform)**
  - technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2monitoring a základní síťové služby DHCP/ DNS/ NAC)
  - **vícenásobná redundance typu Active-Active**, **podpora hierarchického a distribuovaného** modelu v prostředí rozsáhlých sítí

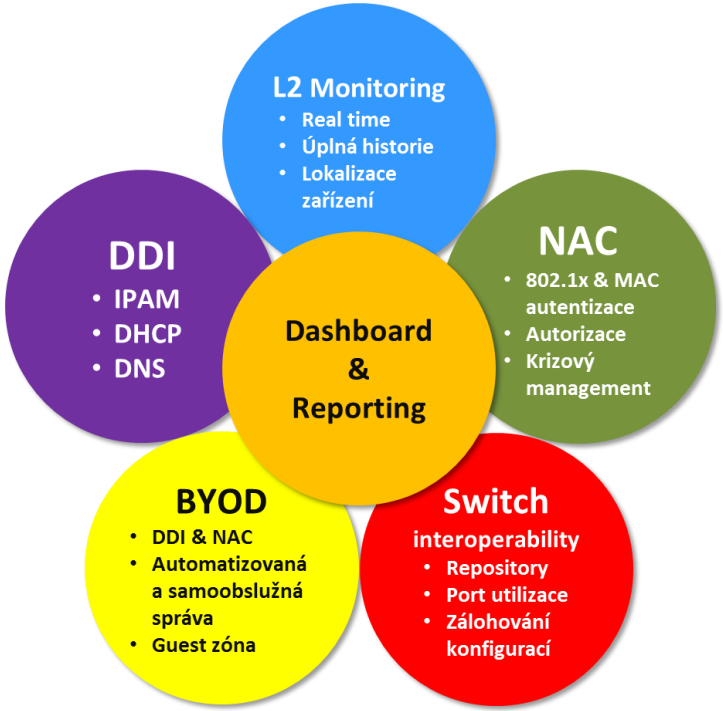
SGP
Secure Grid Platform

- **Novicom SDP (Secure Delivery Protocol)**
  - vlastní komunikační protokol navržený pro zajištění spolehlivé komunikace v prostředí potenciálně nekvalitní sítě
  - **pracuje na linkách s chybovostí až 95%**
  - garance maximálního zabezpečení přenášených dat (military grade security)

SDP
Secure Delivery Protocol

- **Platforma Novicom Appliance**
  - systém HW a virtuálních appliancí, zvyšující bezpečnost, spolehlivost a servisní flexibilitu pro klíčové komunikační a bezpečnostní funkce
  - je založené na OS Linux s bezpečnostními úpravami, s nezávislými prvky centrální správy a zálohování/obnovy
  - Flexibilní správa s Grid Managerem

Novicom appliance



Network Visibility & Security

- Advanced Network Monitoring
- Distributed IP Network Management & Network Access Control
- Integrated Incident Response

novicom

AddNet

DDI/NAC

- ✓**L2 monitoring**
- ✓**Network visibility**
- ✓**DDI** – IPAM, DHCP, DNS
- ✓**NAC** – 802.1x/MAC Autentication /Autorization

Flowmon

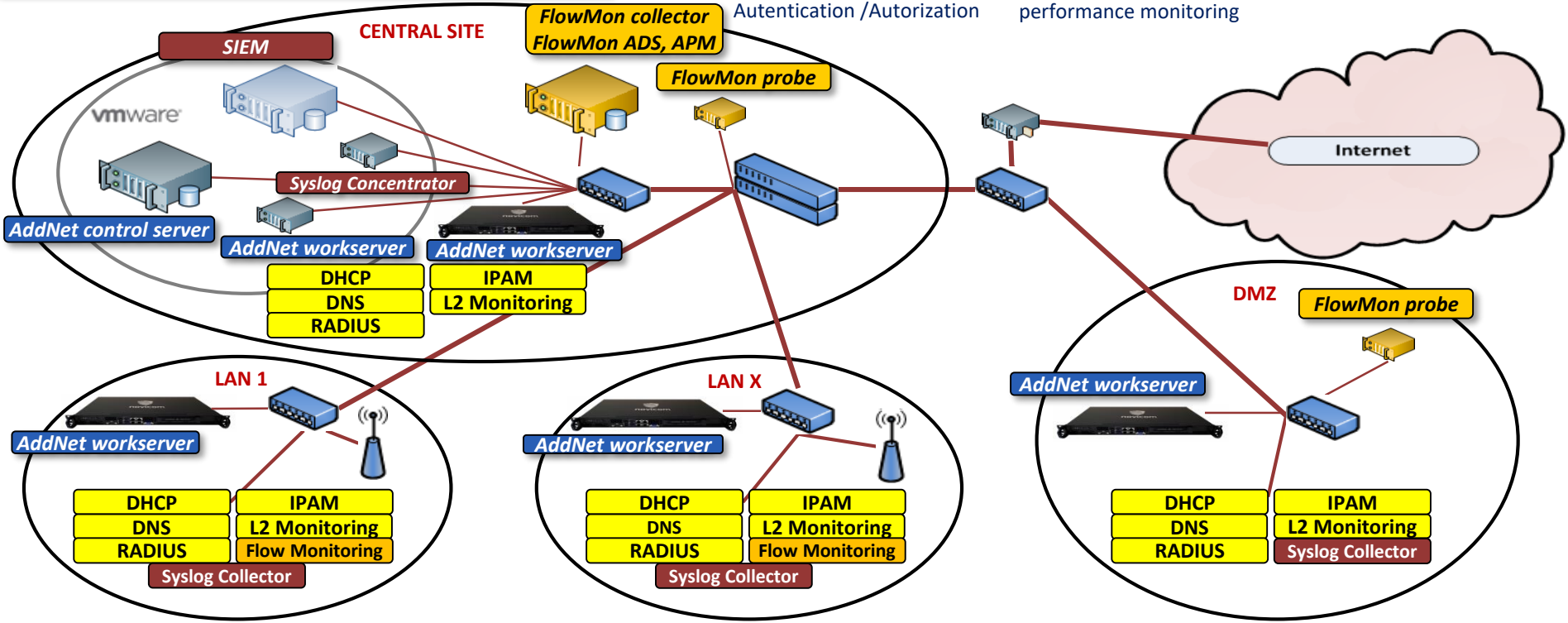
Flowmon (ADS)

Flow monitoring

- ✓**IP-flows monitoring**
- ✓**FlowMon ADS** – Anomaly detection system (NBA)
- ✓**FlowMon APM** – Application performance monitoring

Aktivní SOC

- ✓**Complete data collection**
- ✓**Accurate evaluation and decision making**
- ✓**Immediate incident response**



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
- √ **Plná heterogennost** - bezproblémová spolupráce běžnými síťovými technologiemi
- √ **Schopnost okamžité reakce** na kybernetické bezpečnostní incidenty
- √ **Podpora konceptu Aktivního SOC**
- √ **Snadná implementace** a ověřené projektové postupy – NIM metodika

Další informace

- **Novicom, s.r.o.**
  - Třebohostická 14
  - 100 00 Praha 10
  - www.novicom.cz
  - sales@novicom.cz
- **Vítězslav Šavel**
  - Channel development
  - vitezslav.savel@novicom.cz
  - +420 271 777 231
  - +420 606 551 412