Síťová visibilita a integrovaná správa sítě – nezbytná součást strategie budování kybernetické ochrany

AddNet

Jindřich Šavel

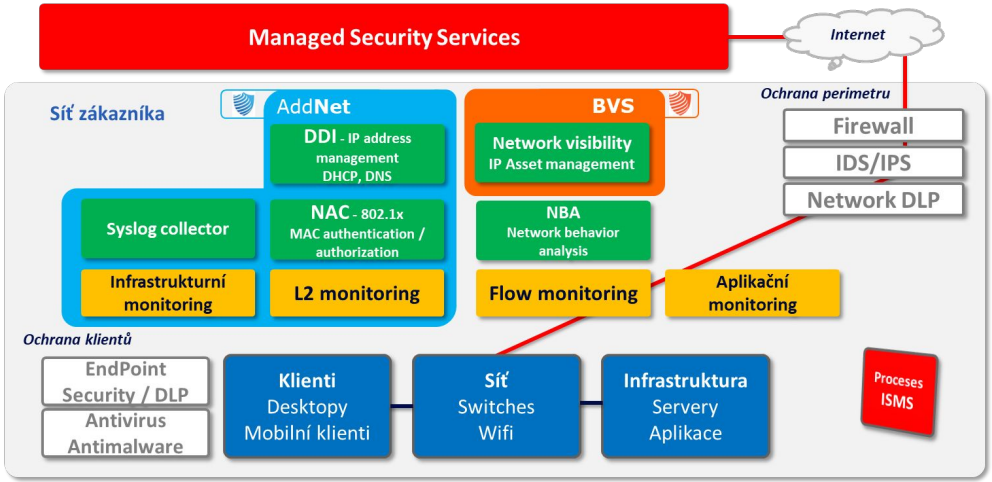
25.04.2019

Představení společnosti Novicom

- **Český výrobce řešení pro síťovou**
  - **Správu, monitoring, bezpečnost**
- **Orientace na**
  - střední a velké zákazníky
  - zákazníky vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých sítí
- **Společnost s historií – 25 let IT trhu**
- **Společnost s ambicemi – úspěšně se prosazuje v zahraničí**
- **Výhradně partnerský prodej**

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 trénování** na řešení bezpečnostních incidentů
  - **Bezpečnostní specialisté nejsou trénovaní na spolupráci** při řešení bezpečnostních incidentů
  - **Management organizací není trénován** a připraven na postupy při řešení bezpečnostních incidentů

Řešení stavu

- **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

Řešení stavu

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

SOC jako služba

- **Pasivní SOC**
  - **První generace bezpečnostních služeb se zaměřuje na vyhodnocování provozu** organizací a vyhledávání bezpečnostních incidentů
    - Bezpečnostní hotline
    - Metodické doporučení ke zjištěným hrozbám
  - **Zjištěné bezpečnostní incidenty jsou předávány organizaci k dořešení**
    - Nutná součinnost s interními zdroji organizace
      - např. Izolace/odpojení zařízení
  - **Problematická akceschopnost v mimopracovní dobu**

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

Nedostatky současné nabídky služeb SOCu

- **Neznalost prostředí**
  - Většinou **pracují pouze se statickým snímkem chráněného prostředí** na základě předaných informací při zavedení služby
  - **Spoléhá se na neaktuální CMDB**
  - **Neznalost informací o změnách v chráněném prostředí**
    - Nové zařízení / infrastruktura
    - Změna / odstranění
      - Infrastruktury
      - Služby
      - Aplikace

Nedostatky současné nabídky služeb SOCu

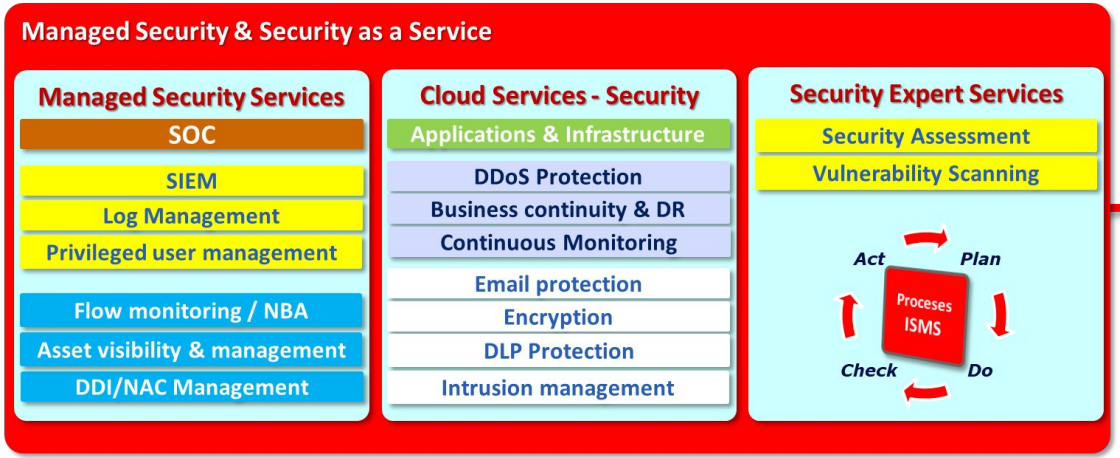
- **Nemožnost aktivního incident response**
  - **Neznalost významu zařízení pro zajištění provozu organizace**
    - Vazba IT assetů na business služby
  - **Nemožnost samostatně provádět zásahy do konfigurace sítě a zařízení**
    - DDI/NAC

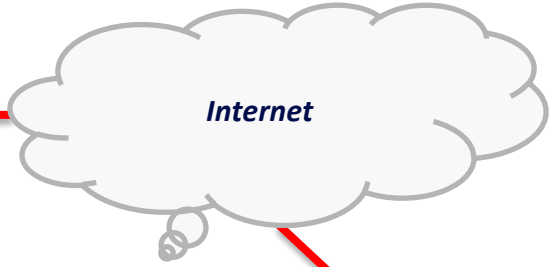
Služba SOC bez integrovaných nástrojů řízení sítě zákazníka nedokáže aktivně a samostatně řešit incident response

Řešení pro prosazení aktivního SOCu

- **Úplná visibilita aktiv a jejich komunikace**
  - Vizualizace a klasifikace IT aktiv
  - Vizualizace komunikací IT aktiv
- **Integrovaná správa sítě**
  - Sdílené využívání integrovaného nástroje pro
    - L2 monitoring – lokalizace zařízení v síti
    - DDI (IPAM/DHCP/DNS) – správu IP adresního prostoru a síťových služeb
    - NAC – řízení přístupu do sítě
- **Podpora správy a monitoringu v rozsáhlých sítích**
  - Distribuovaný model řízení sítě DDI/NAC
  - Monitoring vzdálených lokalit
    - L2, netflow, syslog
- **Podpora rozhodování při řešení incidentů**
  - Vyšetřování komunikace aktiv
  - Znalost důsledků nedostupnosti aktiv na provozované business služby (aplikace)

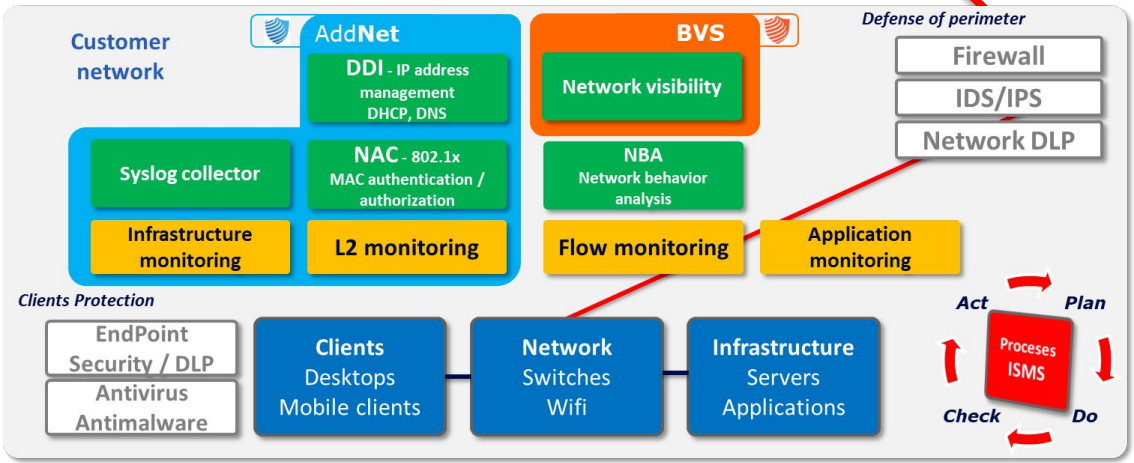
Pokročilý model bezpečnosti





Přínosy modelu pro zákazníky

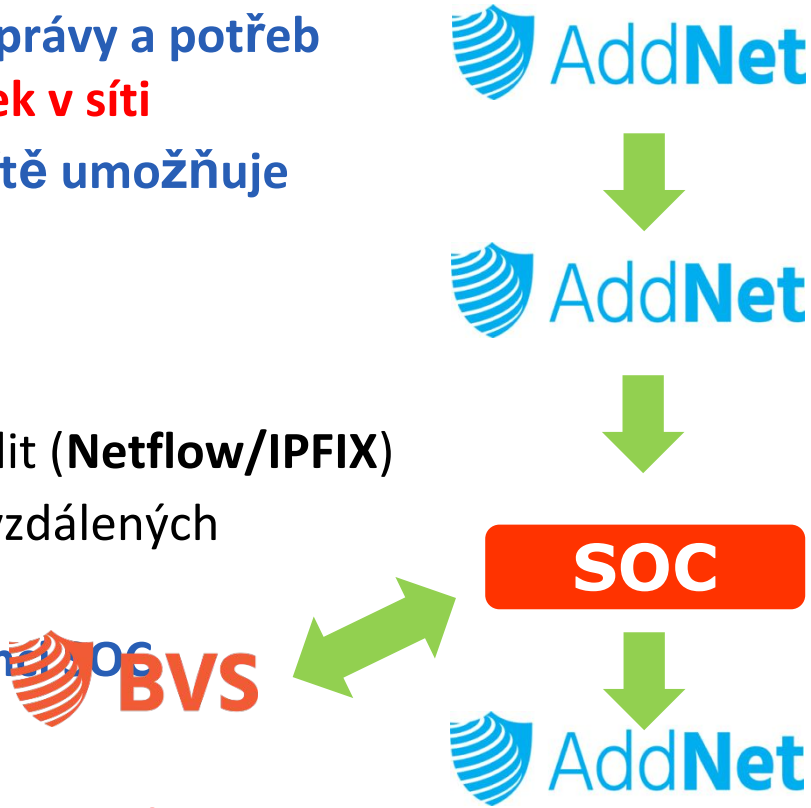
- Využití špičkových znalostí cyber defense
- Provoz 24 x 7 x 365
- Okamžitá reakce na bezpečnostní incidenty
- CAPEX úspory
  - Odpadají investice do nástrojů pokročilé detekce a řízení sítě
- OPEX optimalizace
  - Odpadá nutnost zajistit kvalifikovaný tým pro práci v režimu 24x7



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**
- **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
- **[illegible] incident**



BVS – nástroj pro visibilitu komunikací IT aktiv

- 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

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

Network

Visibility
•
Control
•
Security

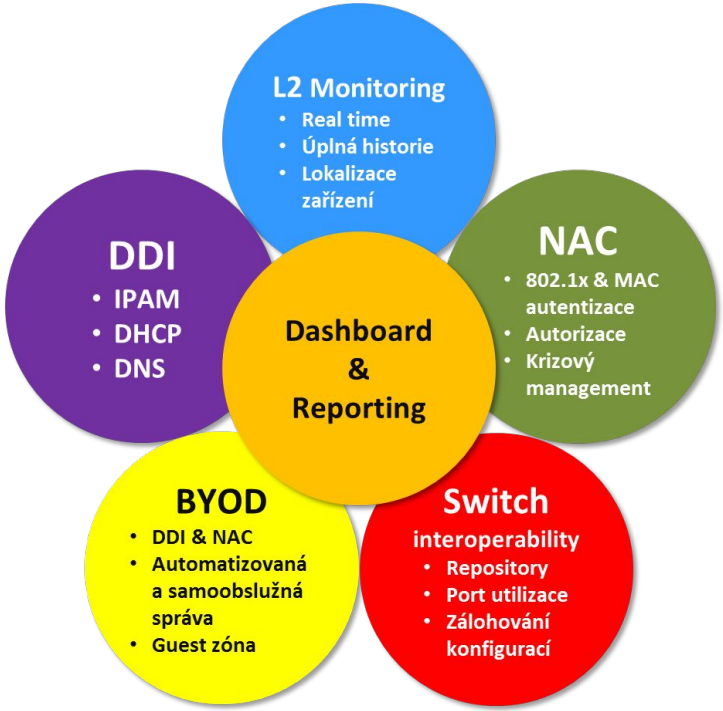
Původní Novicom technologie

- **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
- **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)
- **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

SGP Secure Grid Platform

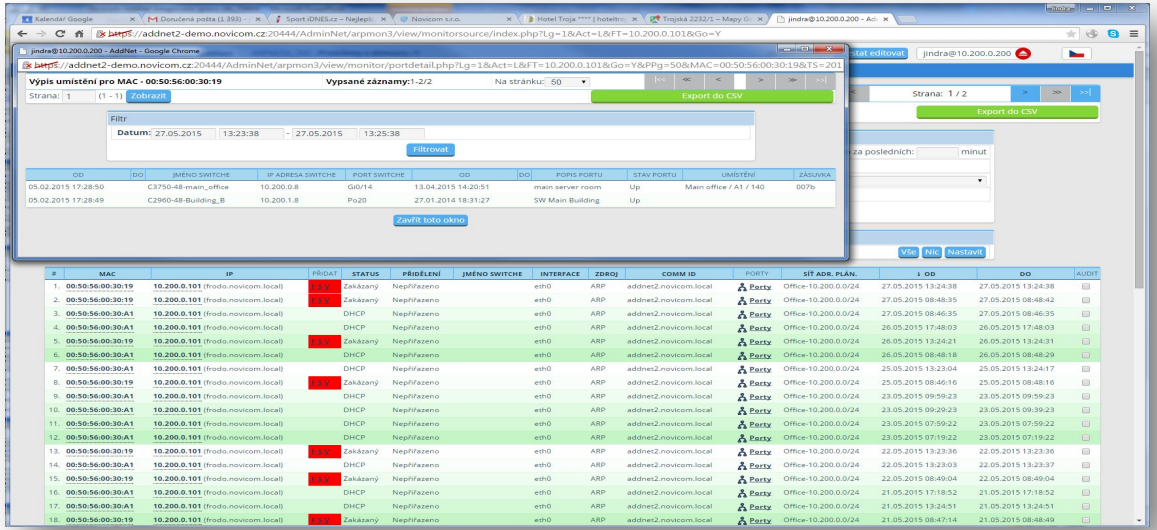
SDP Secure Delivery Protocol

Novicom appliance


L2 Monitoring
• Real time
• Úplná historie
• Lokalizace zařízení
DDI
• IPAM
• DHCP
• DNS
Dashboard & Reporting
NAC
• 802.1x & MAC autentizace
• Autorizace
• Krizový management
BYOD
• DDI & NAC
• Automatizovaná a samoobslužná správa
• Guest zóna
Switch
interoperability
• Repository
• Port utilizace
• Zálohování konfigurací

L2 monitoring

- Základní stavební kámen AddNetu
- Poskytuje informace o výskytu zařízení v síti
  - KTERÁ
    - IP/MAC
  - KDE
    - se nachází v síti
- Real-time monitoring
- Úplná historie výskytu zařízení v síti
- Podpora kabelové knihy
  - Možnost importu



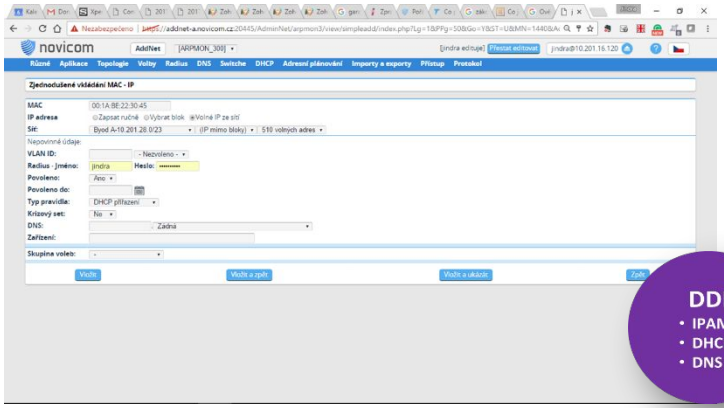
AddNet L2 monitoring je schopný v reálném čase upozornit na rozpor mezi adresním a přístupovým plánem a realitou v síti!

L2 Monitoring
- Real time
- Full history
- Physical locality

IPAM – Repository síťových zařízení

Umožňuje řízení DNS, IP adresních dat a přístupové politiky (pro NAC) na úrovni rozsáhlých organizací s jednotnou správou, monitoringem a auditem.

- **Repository zařízení**
  - Filozofie umožnění komunikace pouze známých (povolených zařízení) v síti
  - Možná správa doplňkových informací
  - Vazba na L2 monitoring
  - Vazba na aktivní prvky
- **IP Adresní plánování**
  - **IPAM** – vytváření a správa IP adresního plánu
  - Správa **DHCP a DNS**
- **Správa NAC**
  - **Autentizace**
    - řízení přístupů zařízení do sítě (802.1x / MAC autentizace)
  - **Autorizace**
    - řízení přiřazování zařízení do VLAN
  - **Podpora krizového řízení**



NAC – Řízení přístupů do sítě

Integrovaná komunikace s aktivními prvky a podpora standardu 802.1x (RADIUS) a jeho subsetů – MAC autentizace a autorizace (dynamické řízení VLAN)

- **Podpora standardního NAC s využitím full 802.1x**
- **Alternativní MAC autentizace s ochranou**
  - odhalování duplicitních a podvržených MAC adres
  - bez nákladů na administraci
- **Vysoce efektivní segmentace sítí**
  - řízení přidělení zařízení do VLAN (globální politiky, VLAN izolace apod.)
- **Výhodná dvoufázová implementace**
  - **Fáze 1.** – součást DDI – **zavedení MAC autentizace s ochranou**
  - **Fáze 2.** – následné zvyšování ochrany formou **postupného zavádění full 802.1x**

Řeší problémy nedokončených NAC implementací s 802.1x

- *omezená podpora suplikantů, nezvládnutá správa výjimek*

NAC
- 802.1x & MAC authentication
- Authorization
- Crisis management

Pokročilý NAC

- **Zavedení izolace zařízení v rámci specifické VLAN**
  - Postavené na dynamickém řízení ACL – ***DACL***
  - Zařízení se „nevidí“ v rámci stejné VLAN
  - AddNet řeší nebezpečí nakažení škodlivým virem (ransomware) preventivně – povýšením bezpečnostních politik sítě
- **Zjednodušení a zpřehlednění bezpečnostních politik**
  - Globální bezpečnostní politiky - odpadá nutnost vytvářet politiky dle lokalit
  - Dynamické řízení ACL na switchích (DACL)
  - ***Trusted pooly***
    - Zavedení důvěryhodných zařízení pro jejich automatizovanou správu ve vzdálených lokalitách
    - Unikátní kombinace DHCP poolů a NAC (autentizace a autorizace)

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 Autentikace /Autorizace

Flowmon

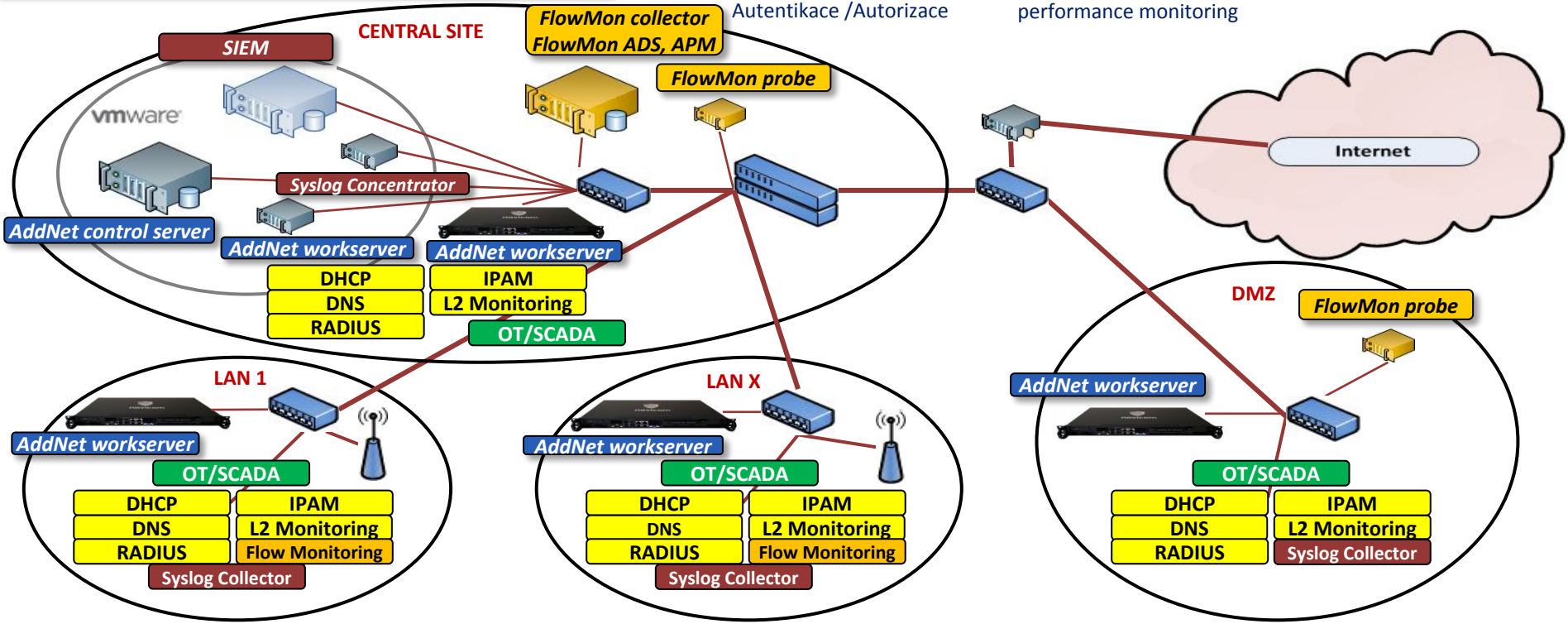
Flowmon (ADS)

Flow monitoring

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

Aktivní SOC

- ✔ **Kompletní sběr provozních dat**
- ✔ **Vyhodnocení a rozhodování**
- ✔ **Okamžitý incident response**

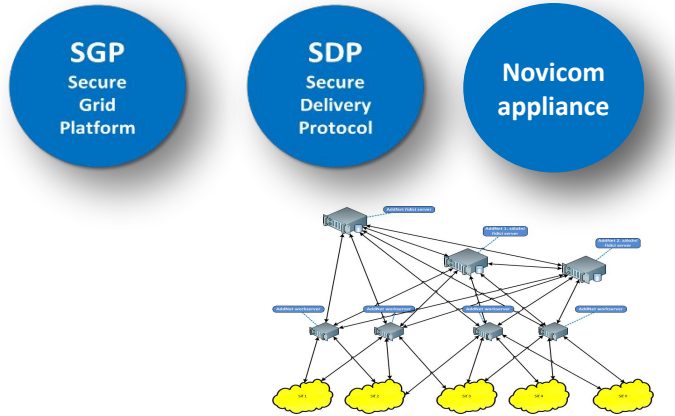


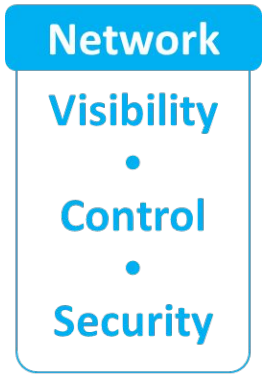
Klíčové přínosy AddNetu

- √ **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
- √ **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 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

V čem je AddNet jiný?

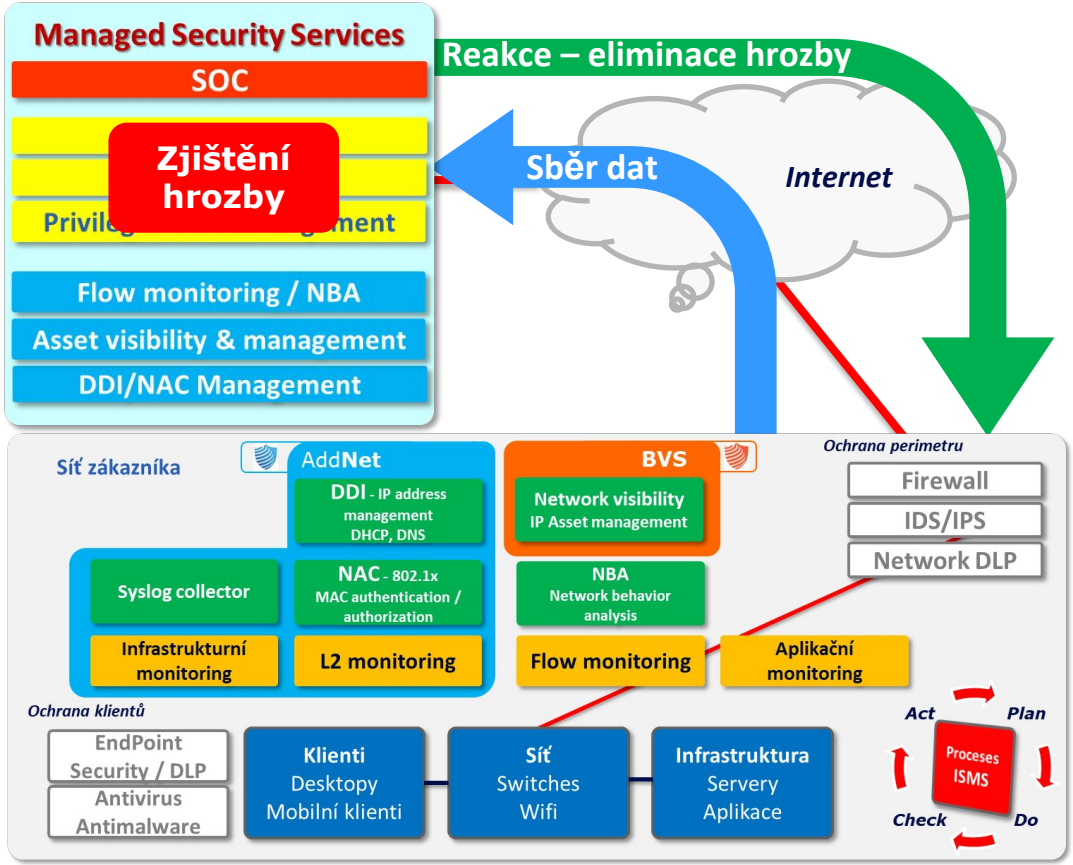
- **Využití vlastních technologií**
  - **Novicom SGP** – Secure Grid Platform
  - **Novicom SDP** – Secure Delivery Protocol
  - **Novicom appliance**
- **Flexibilní podpora topologie nasazení**
  - Centralizované nebo distribuované nasazení
  - Snadná realizace změn
- **Nadstandardní provozní spolehlivost a škálovatelnost**
  - Provoz v distribuovaných lokalitách i při nedostupnosti řídící lokality
- **Nadstandardní bezpečnost**
  - Appliance, datový přenos, architektura
- **Unikátní spojení DDI, NAC a SOC**
  - DDI nástroj je doplněný o NAC
  - Optimalizované pro rozsáhlé distribuované sítě
  - Posouvá SOC do jiné úrovně – Aktivní SOC





Spolupráce Novicomu s provozovateli služby SOC

- **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, Flow, Syslog
  - **Schopnost okamžité reakce 24x7** bez nutné součinnosti zákazníka
- **SOC za 2 dny?** **Proč ne?**



Shrnutí

- **SOC jako služba je budoucnost**
  - Zlomek ceny (odhadováno 20-35% oproti inhouse zajištění)
    - Technologie, lidské zdroje
- **Pojďte se na to připravit už dnes s Novicomem**
  - Vyznejte se ve své síti
  - Zvyšte efektivitu správy sítě
  - Zaveďte pokročilé modely bezpečnosti
  - Připravte se na aktivní incident response díky možnému sdílení pokročilých řešení Novicomu se svým SOC providerem
  - Vyzkoušejte to formou služby s partnery Novicomu

Více informací

- **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
  - +420 777 222 961