Přínos integrovaného řízení a zabezpečení sítě pro rychlé řešení incidentů

AddNet – integrovaný DDI/NAC

Jindřich Šavel

10.04.2018

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?

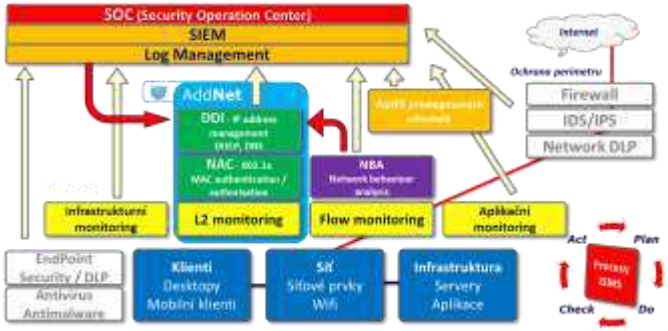
- **Pokročilý model bezpečnosti**

- **Zajištění provozních potřeb sítě**
  - Inhouse (alternativně outsourcing)
  - Potřeba provozu typicky 8-17

- **Zajištění bezpečnostních potřeb sítě**
  - Poskytovatel služeb
  - Potřeba provozu 24x7x365

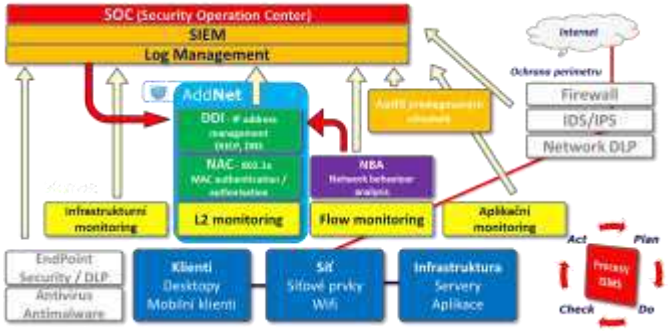
Zajištění provozních potřeb sítě

- **Konvenčně zvládnuto**
  - základní správa sítě a stanic
  - ochrana perimetru (firewall)
  - ochrana klientů (antivirus, antimalware)
  - infrastrukturní monitoring
- **Nezvládnuté nebo podceňované**
  - ***Síťová visibilita***
  - ***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 postavené na
    - Síťovém provozu
      - DHCP/DNS/Radius/Netflow…
    - Klientech a infrastruktuře
      - Syslog …
- **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

Bezpečnost formou služby

Managed Security & Security as a Service

Managed Security Services

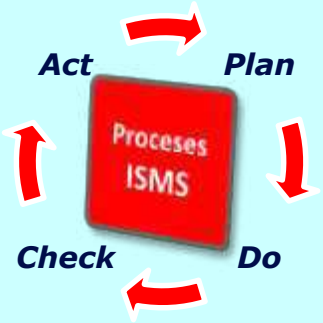
- SOC
- SIEM
- Log Management
- Privileged user management
- Flow monitoring / NBA
- DDoS Protection
- DDI/NAC Management

Cloud Services - Security

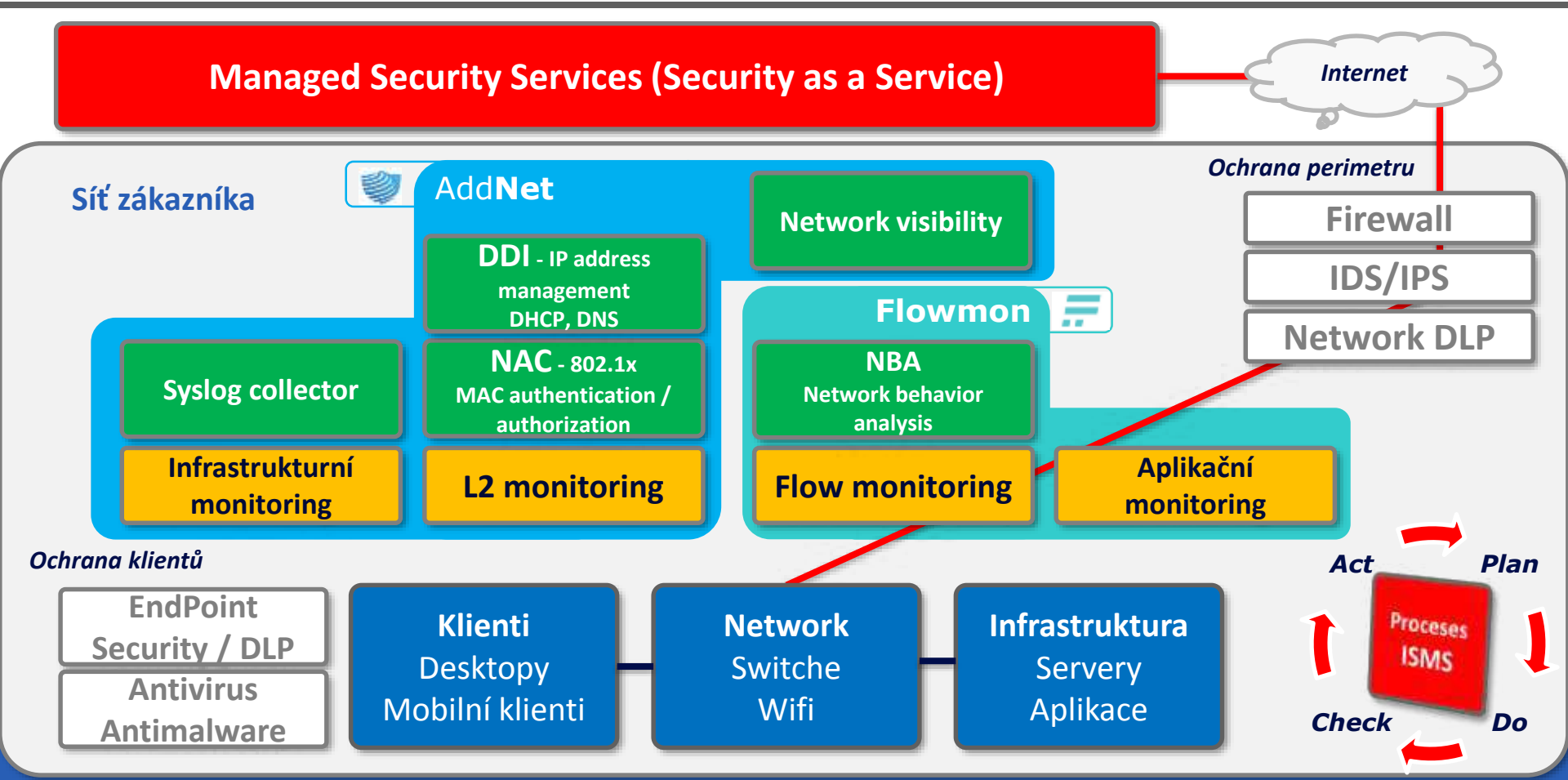
- Applications
- Infrastructure
- Business continuity & DR
- Continuous Monitoring
- Email protection
- Encryption
- DLP Protection
- Intrusion management

Security Expert Services

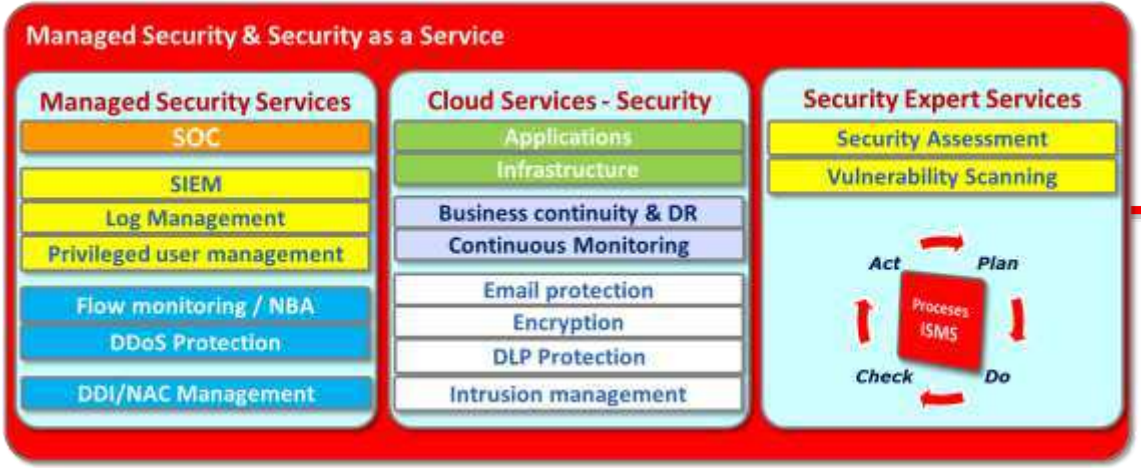
- Security Assessment
- Vulnerability Scanning

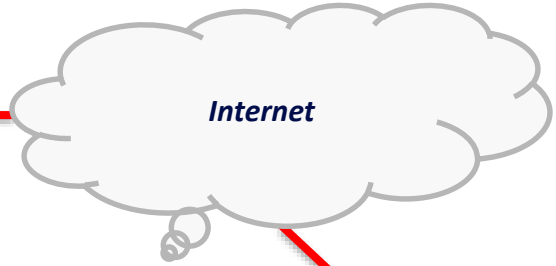


Zabezpečení sítě zákazníků



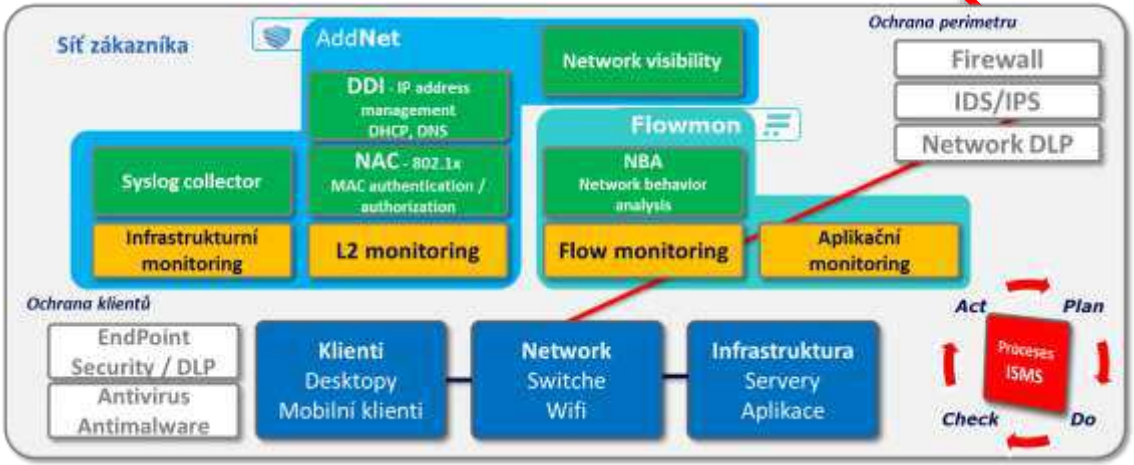
Pokročilý model bezpečnosti





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**
- **zajištění okamžité reakce na zjištěné hrozby – incident response**

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

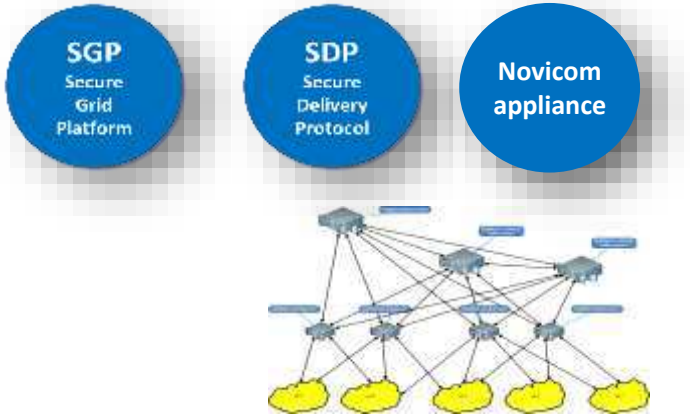
- **Novicom SGP (Secure Grid Platform)**
  - technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2monitoring a základní síťové služby DHCP/ DNS/ NAC)
  - **vícenásobná redundance typu Active-Active**, **podpora hierarchického a distribuovaného**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

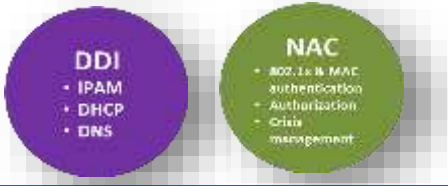
Klíčové přínosy AddNetu

- √ **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- √ **Síťová visibilita** - správa IT aktiv a jejich vztahu na klíčové procesy organizace
- √ **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**
- √ **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

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





Další informace

- **Novicom, s.r.o.**
  - Třebohostická 14
  - 100 00 Praha 10
  - www.novicom.cz
  - sales@novicom.cz
- **Jindřich Šavel**
  - obchodní ředitel
  - jindrich.savel@novicom.cz
  - +420 271 777 231
  - +420 777 222 961