AddNet

Detailní L2 monitoring a spolehlivé základní síťové služby (DDI/NAC) – základ kybernetické bezpečnosti organizace

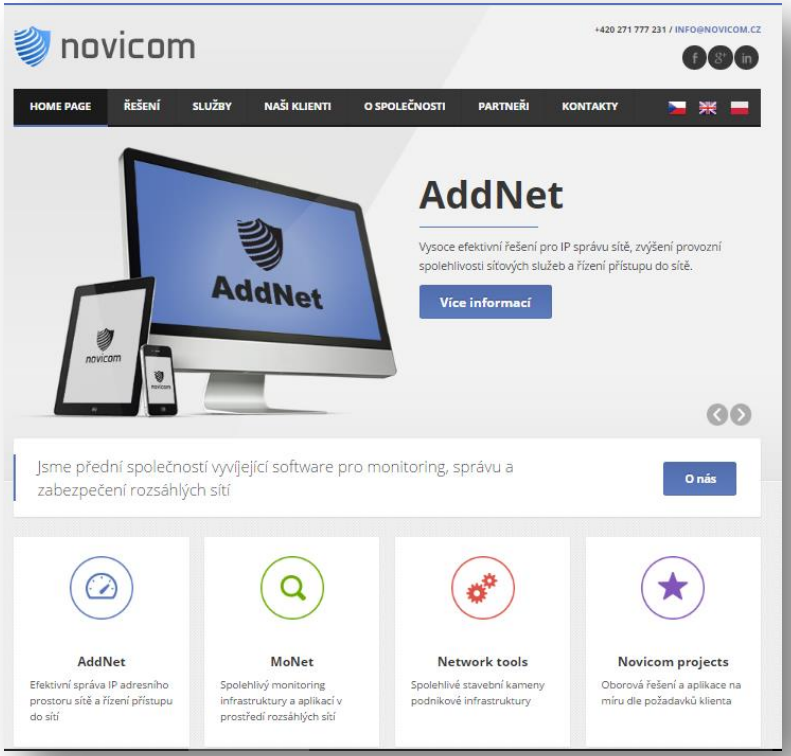
Jindřich Šavel

19.9.2016

Představení společnosti Novicom

- **Česká společnost zabývající se**
  - **vývojem**
  - **dodávkami**
  - **provozem**

  systémů pro síťovou
  - **správu**
  - **monitoring**
  - **bezpečnost**



- **Orientace na střední a velké zákazníky a na zákazníky vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých systémů**
- **Společnost s historií – více než 22 let IT trhu**
- **Společnost s ambicemi – úspěšně se prosazuje v zahraničí**

Významní zákazníci

MINISTERSTVO VNITRA ČR

MINISTERSTVO OBRANY ČR

MINISTERSTVO FINANCÍ ČR

MINISTERSTVO KULTURY

ICOM TRANSPORT A.S.

TOPTRANS EU, A.S.

ČESKÁ POŠTA

OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA

ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD

HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY

THOMAYEROVA NEMOCNICE

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ

ČESKÝ ROZHLAS

KOFOLA ČESKOSLOVENSKO A.S.

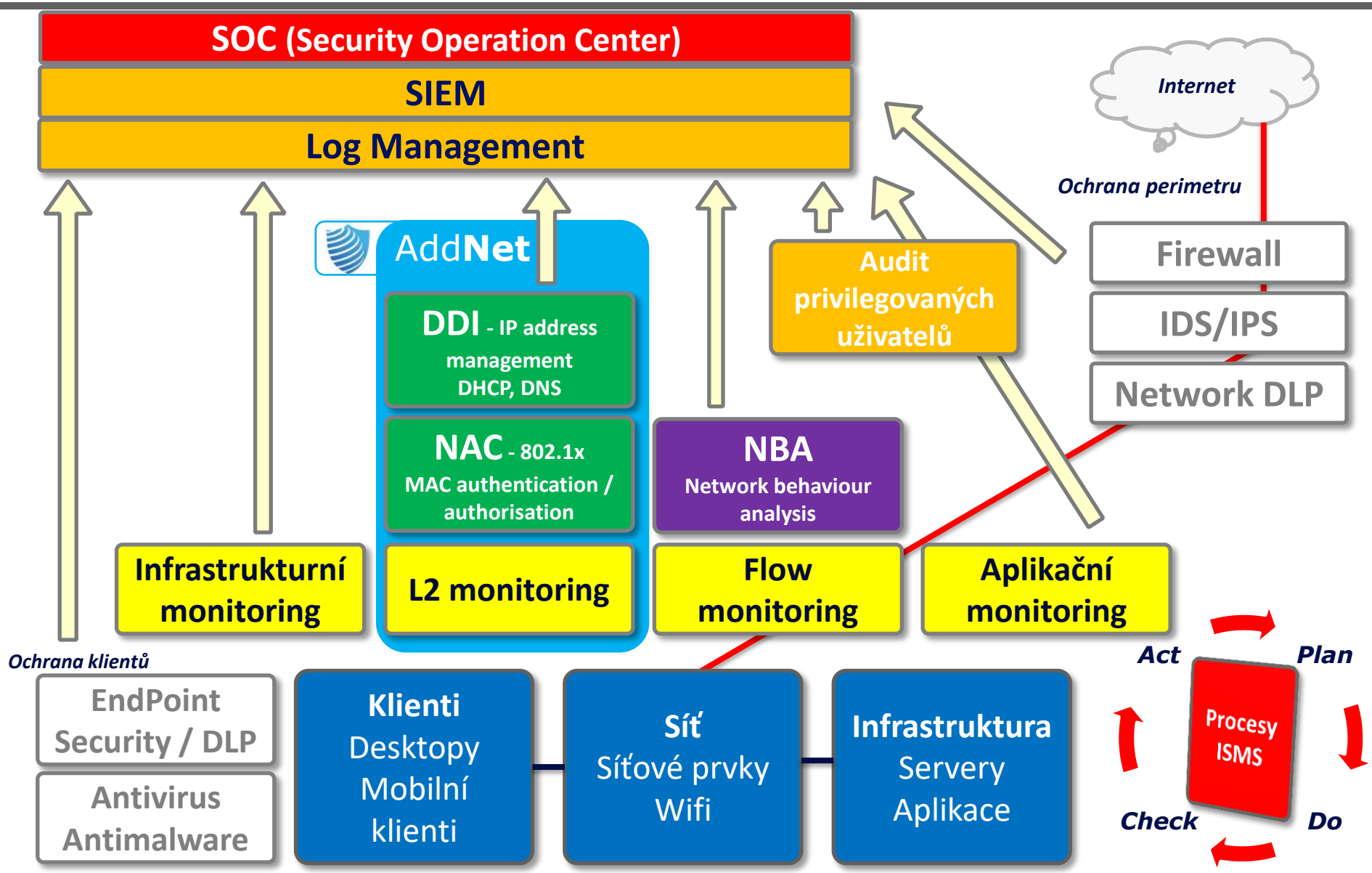
WÜSTENROT - STAVEBNÍ SPOŘITELNA A.S.

OFFICE DEPOT S.R.O.

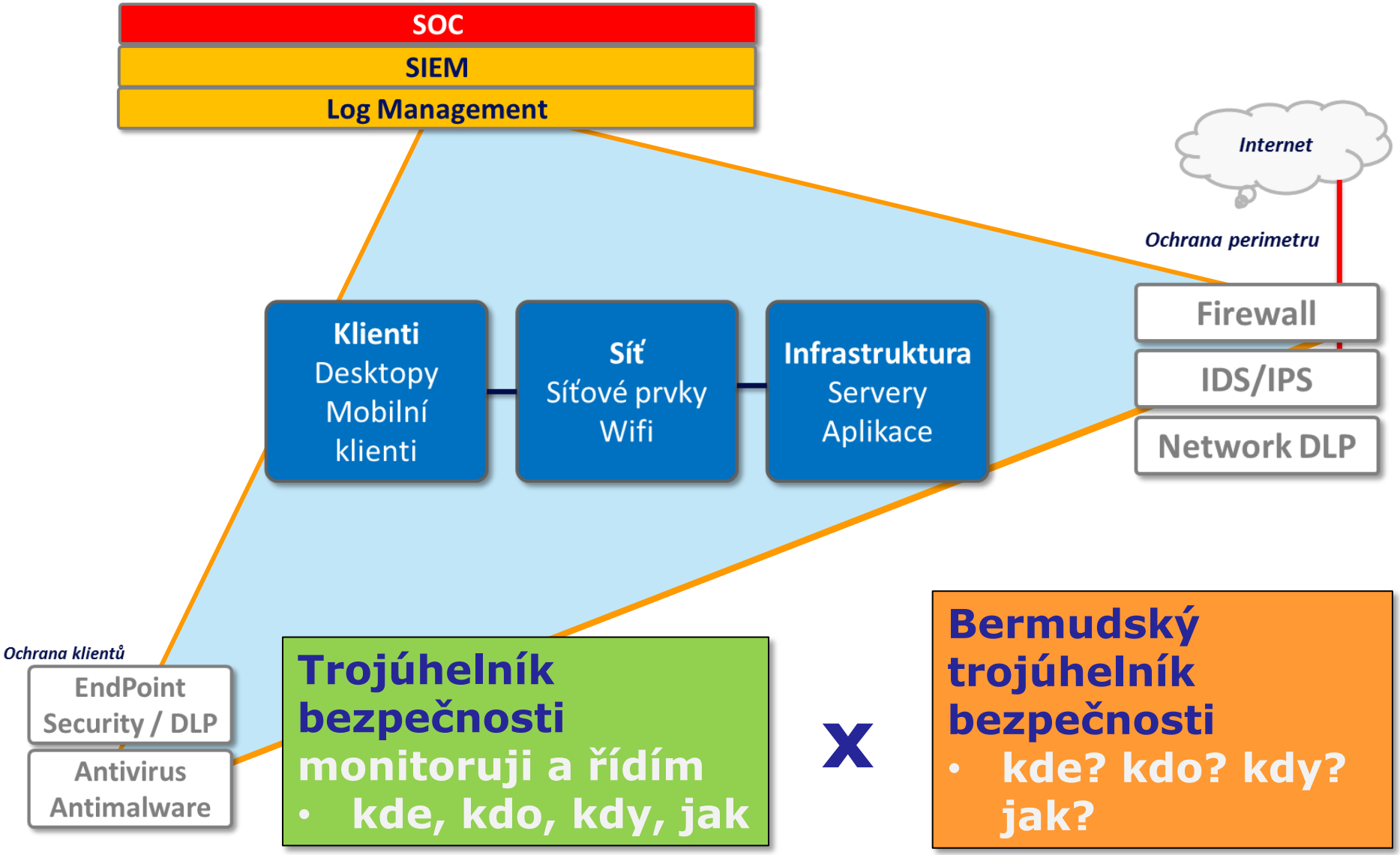
MĚSTSKÁ ČÁST PRAHA 8

MAGISTRÁT MĚSTA OSTRAVY

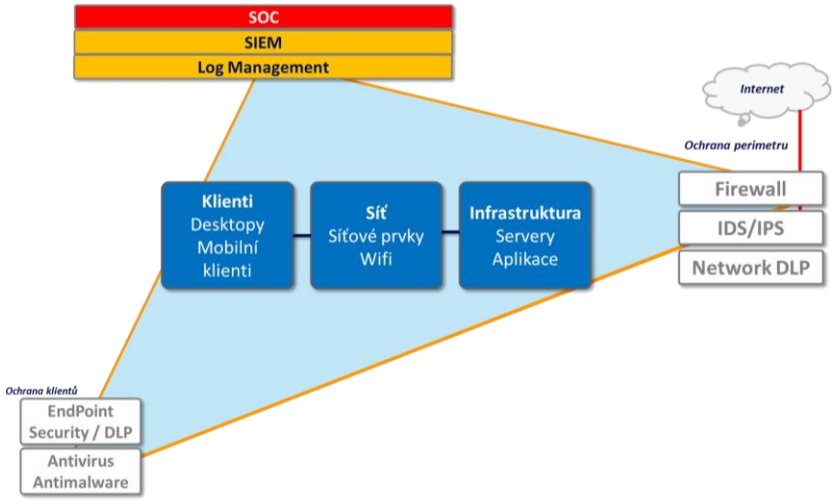
Koncept Aktivní bezpečnosti sítě



Bezpečnost interní sítě



Bermudský trojúhelník bezpečnosti

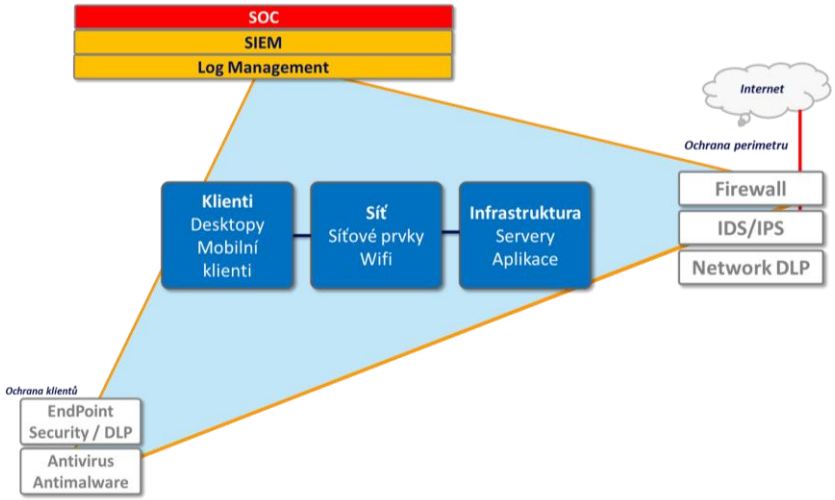


Bermudský trojúhelník bezpečnosti

- kde? kdo? kdy? jak?

- Žádné řízení přístupu do sítě (NAC)
- Evidence IP adres v excelu
- Dynamicky přidělované IP adresy DHCP
- Samostatné DNS
- Pouze základní monitoring
  - Infrastruktura
- Žádný pokročilý monitoring síťového provozu

Trojúhelník bezpečnosti



Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
  - ✓ **IPAM, DHCP a DNS**
- ✓ **Pevné IP přidělované DHCP**
- ✓ **Multispektrální monitoring**
  - ✓ **L2 Monitoring, Flow Monitoring, Infrastruktura, Aplikace**
- ✓ **Pokročilá ochrana vnitřní sítě - NBA**

Konvenční řešení kybernetických incidentů

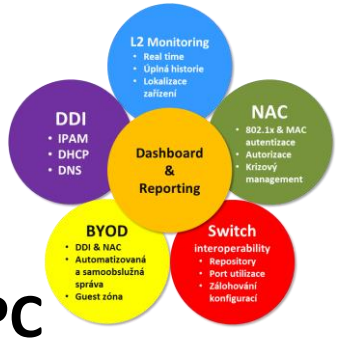
- **Identifikace hrozby – Operátor SOC**
  - **SIEM** vyhodnotí bezpečnostní incident
  - **SOC** operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne **lokalizovat zařízení**
    - dynamická adresa?/ hledání v logách…
  - Přihlásí se na switch a **odpojí port**
  - Informuje admina PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá síťaře o znovuzapojení do sítě

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá správce sítě o znovupřipojení zařízení do sítě

AddNet

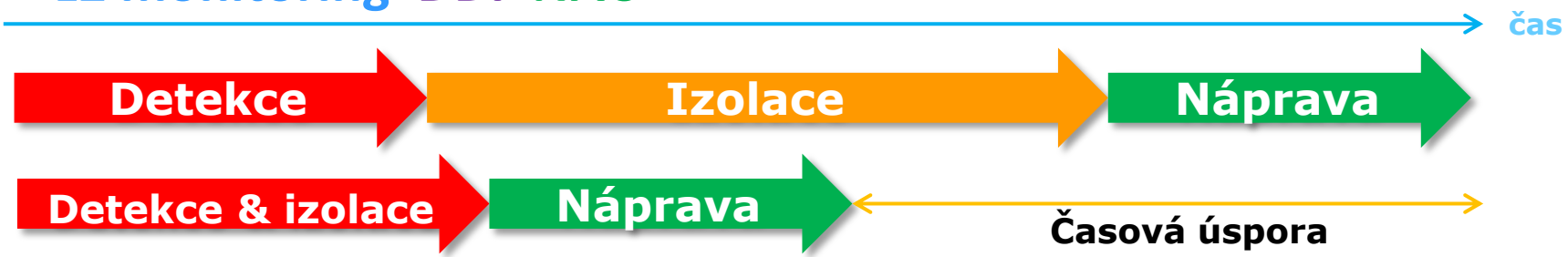
minuty



minuty/ hodiny

Shrnutí

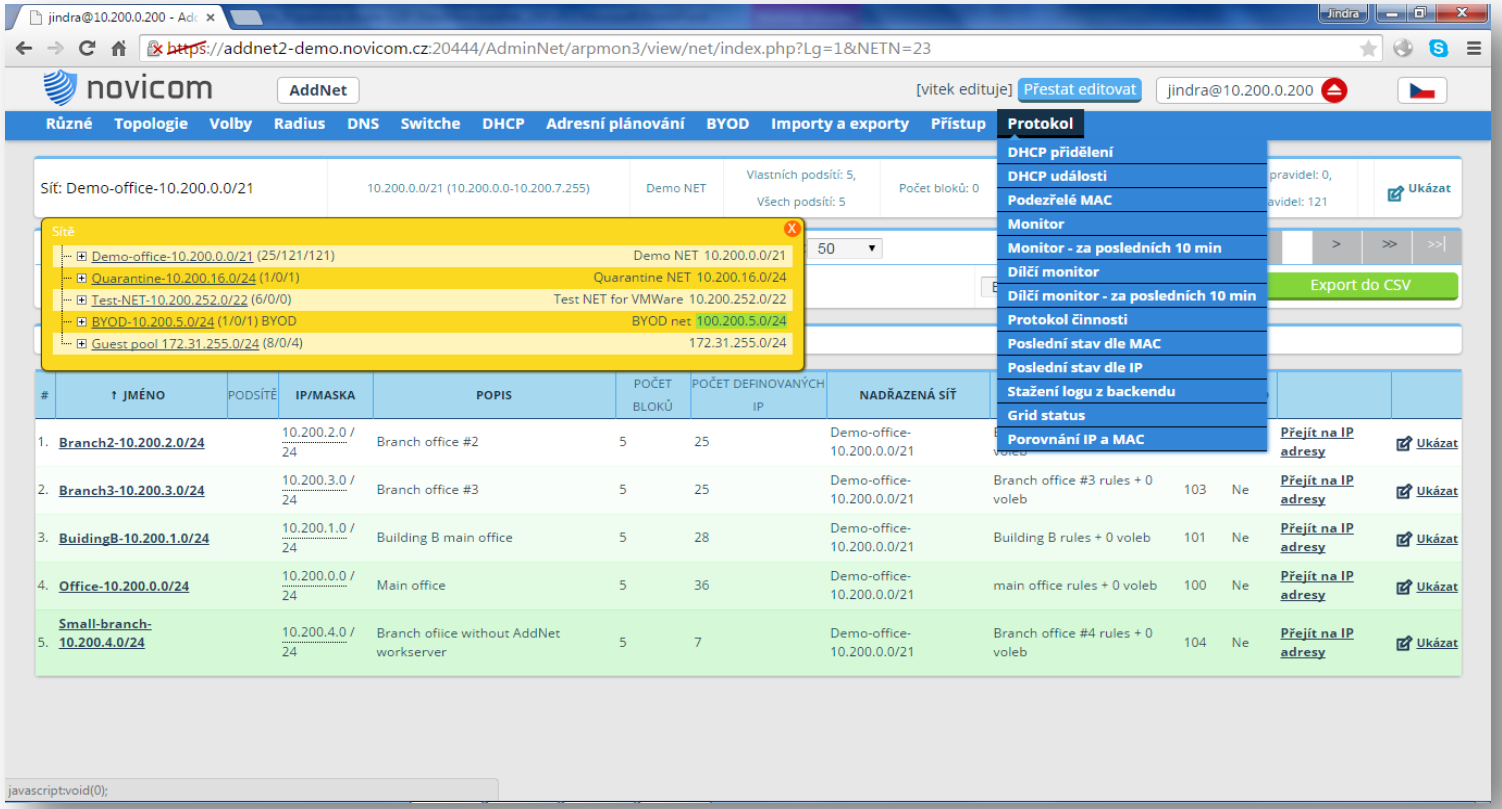
- Je v pořádku, že se věnujete ochraně
  - Perimetru a Klientů
- Počítejte ale s tím, že tato ochrana bude překonána
  - Signature based protection
- Zajistěte si nástroje pokročilé detekce a monitoringu v síti
  - NBA
  - SIEM
- Investujte do integrovaných nástrojů, které vám pomohou výrazně zkrátit reakční dobu při řešení zjištěných bezpečnostních incidentů a navíc řádově usnadní správu sítí
  - L2 monitoring DDI NAC



AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů** L2 monitoringu, správy IP adresního prostoru, základních síťových služeb (DHCP, DNS), řízení přístupu do sítě (NAC) a pokročilé komunikace s aktivními prvky sítě.



Původní Novicom technologie

- **Novicom SGP (Secure Grid Platform)**
  - technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2/infrastrukturní monitoring 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 velice nekvalitní sítě
  - **pracuje na linkách s chybovostí až 95%**
  - garance maximálního zabezpečení přenášených dat (military grade security)

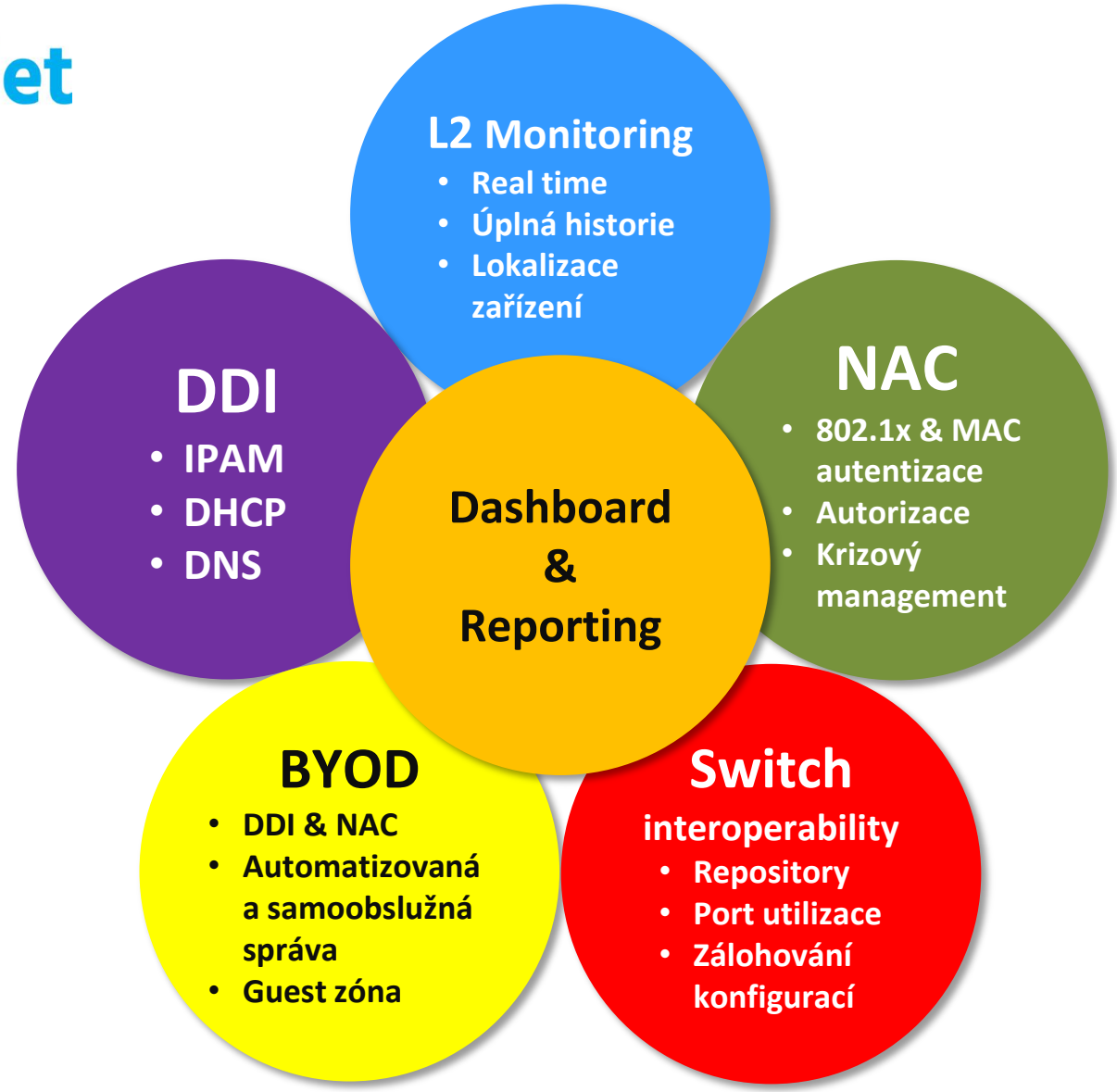
SDP
Secure
Delivery
Protocol

- **Novicom FireBox platforma**
  - systém HW a virtuálních appliancí, zvyšující bezpečnost, spolehlivost a servisní flexibilitu pro klíčové komunikační a bezpečnostní funkce
  - je založené na OS Linux s bezp. úpravami kernelu, s nezávislými prvky centrální správy a zálohování/obnovy

FireBox
appliances

Co je AddNet?

AddNet



Network Visibility & Security

Advanced Network Monitoring
Distributed IP Network Management

novicom

AddNet

DDI/NAC

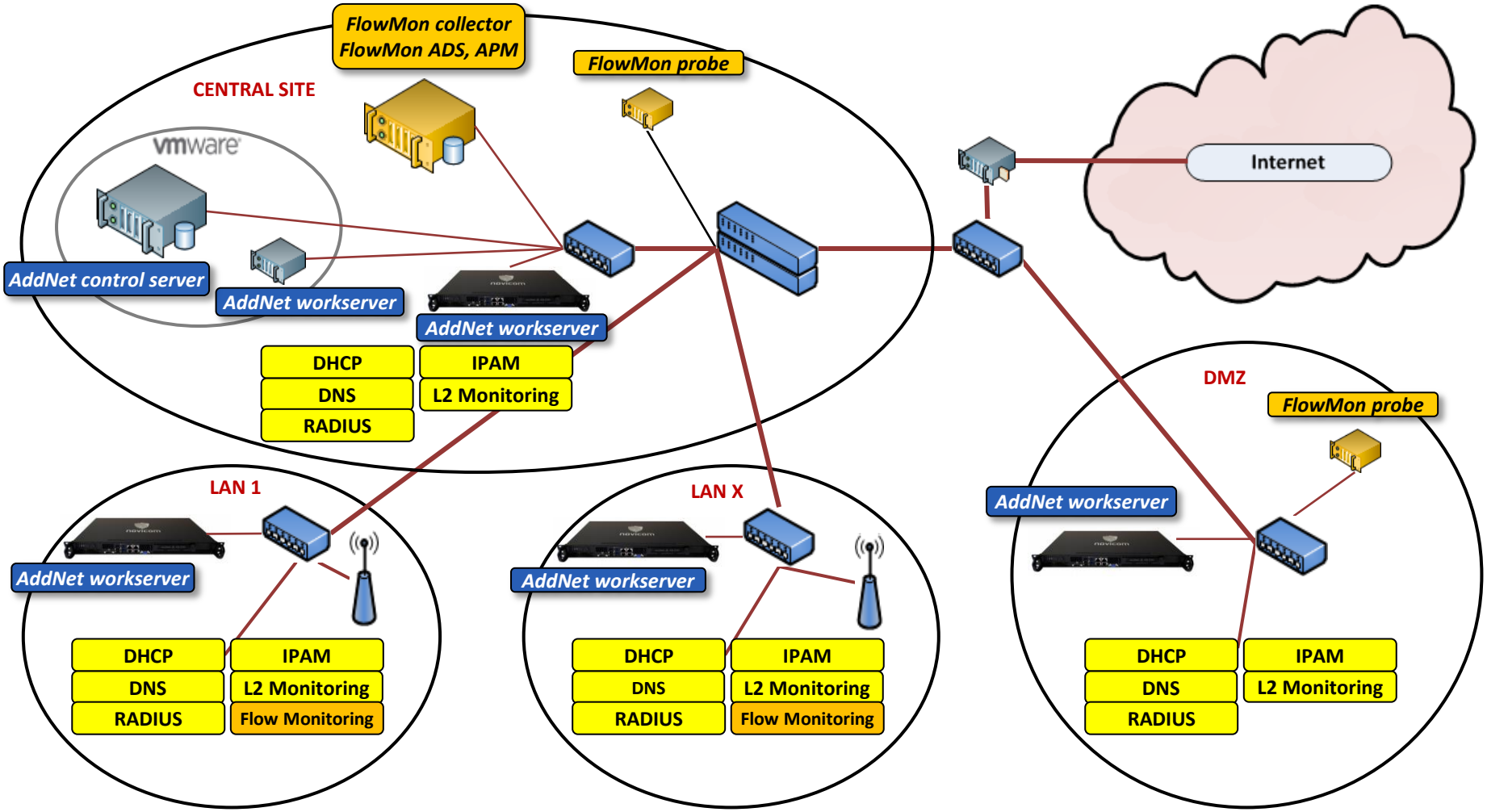
- ✓**L2 monitoring**
- ✓**IPAM** – address space management
- ✓**DDI** - DHCP, DNS
- ✓**NAC** – 802.1x/MAC Autentication /Autorization

Flowmon

Flowmon (ADS)

Flow monitoring

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



Klíčové přínosy AddNetu

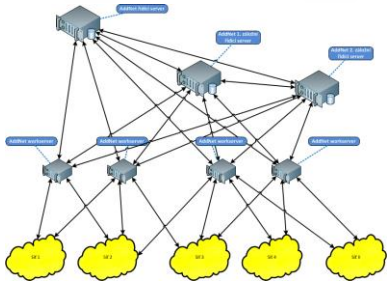
- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa
  - 802.1x / MAC autentizace s ochranou, následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná 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
- **Snadná implementace** a ověřené projektové postupy

NIM
Novicom Implementation Methodology

V čem je AddNet jiný?

- **Využití vlastních technologií**
  - **Novicom SGP** – Secure Grid Platform
  - **Novicom SDP** – Secure Delivery Protocol
  - **Novicom FireBox appliance**

- **Flexibilní podpora topologie nasazení**
  - Centralizované nasazení
  - Plně distribuovaného nasazení
  - Kombinované nasazení



- **Nadstandardní provozní spolehlivost a škálovatelnost**
  - Provoz v distribuovaných lokalitách i při nedostupnosti řídící lokality
  - Podpora aktivního clusteringu na všech úrovních
  - Nadstandardní bezpečnost dat (appliance, komunikace, architektura)
- **Unikátní spojení DDI a NAC**

Přináší flexibilní kontrolu a řízení interní sítě,
což je nezbytné pro budování efektivní kybernetické ochrany

Další informace

- **Novicom s.r.o.**
  - Koněvova 67
  - 130 00 Praha 3
  - www.novicom.cz
  - sales@novicom.cz
- **Jindřich Šavel**
  - obchodní ředitel
  - jindrich.savel@novicom.cz
  - +420 271 777 231
  - +420 777 222 961