Přínosy integrovaného DDI/NAC nástroje pro zvýšení ochrany sítě a schopnosti reagovat na útoky

AddNet

integrovaný DDI/NAC nástroj

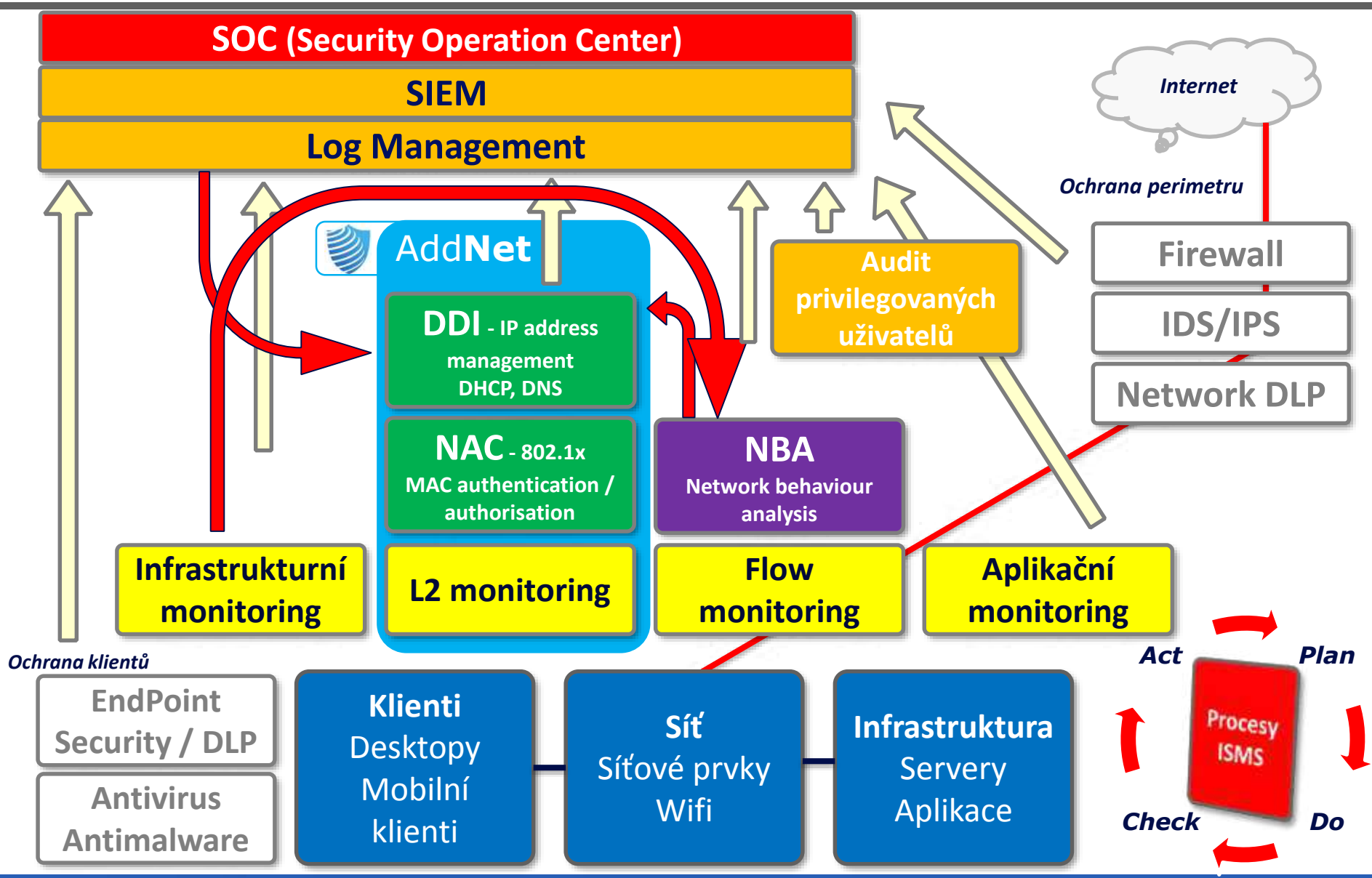
Jindřich Šavel

4.4.2017

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 – více než 22 let IT trhu**
- **Společnost s ambicemi – úspěšně se prosazuje v zahraničí**
  - v roce 2016 aktivní v 8 zemích

Koncept Aktivní bezpečnosti sítě



Legislativa a zabezpečení sítí

- **Stávající legislativa**
  - **Dílčí normy, nejvýznamnější:**
    - ZoKB *(181/2014 Sb.)* + prováděcí vyhlášky *(316 a317/2014 Sb.)* + nařízení vlády *(315/2014 Sb.)*
    - Zákon o ochraně osobních údajů *(101/2000 Sb.)*
    - Občanský zákoník (*Péče řádného hospodáře apod.*)
  - **Dopad pouze na omezenou množinu subjektů**
    - Správcové kritické a významné infrastruktury
    - Pro ostatní subjekty – významný PR aspekt
    - Pouze nevýznamné sankce při neplnění
    - Pozvolná akceptace nutnosti komplexního řešení kybernetické ochrany

Přicházející legislativa

- **Změny vycházející z EU směrnice NIS – úpravy/rozšíření ZoKB**
  - rozšíření dotčených subjektů dle ZoKB
  - ostatní změny jsou minoritní

- **Nová EU nařízení GDPR – *General Data Protection Regulation***
  - významné zpřísnění v oblasti ochrany osobních dat
  - dopad na všechny subjekty – instituce i firmy
  - přináší **zásadní pokuty za porušování nových pravidel**
    - až **20.000.000 Euro** nebo **4% z obratu** a
    - a dále **náhradu škody**
  - zavádí novou nezávislou kontrolní funkci **DPO – Data Protection Officer** (Pověřenec pro ochranu osobních údajů)

Jak se s GDPR vypořádat?

Cesta ke splnění GDPR požadavků

- Srovnávací analýza stavu ochrany OÚ
- Plán implementace
- Analýza rizik zpracování OÚ
- Posouzení vlivu na ochranu OÚ
- Implementace a zdokumentování procesů
- Zahájení technické úpravy IS (+ možné zavedení podpůrných nástrojů)
- Technická úprava IS
- Školení uživatelů
- Testy a přezkoumání systému ochrany

GDPR – akceptování závažnosti

- Platí pro všechny firmy a organizace
- Rozšiřuje definici významu osobních dat
- Zpřísňuje pravidla pro získání platného souhlasu s použitím osobních údajů
- Požaduje jmenování inspektora ochrany údajů (DPO – Data Protection Officer)
- Zavádí povinné PIA – Privacy Impact Assessment
- Zavádí podmínku oznámení úniků dat pro všechny
- Zavádí právo být zapomenut
- Rozšiřuje odpovědnost správce údajů osobních dat
- Vyžaduje ochranu soukromí již v návrhu systému
- Zavádí koncept jednotného přístupu

A jak to souvisí s Novicom a jeho řešeními?

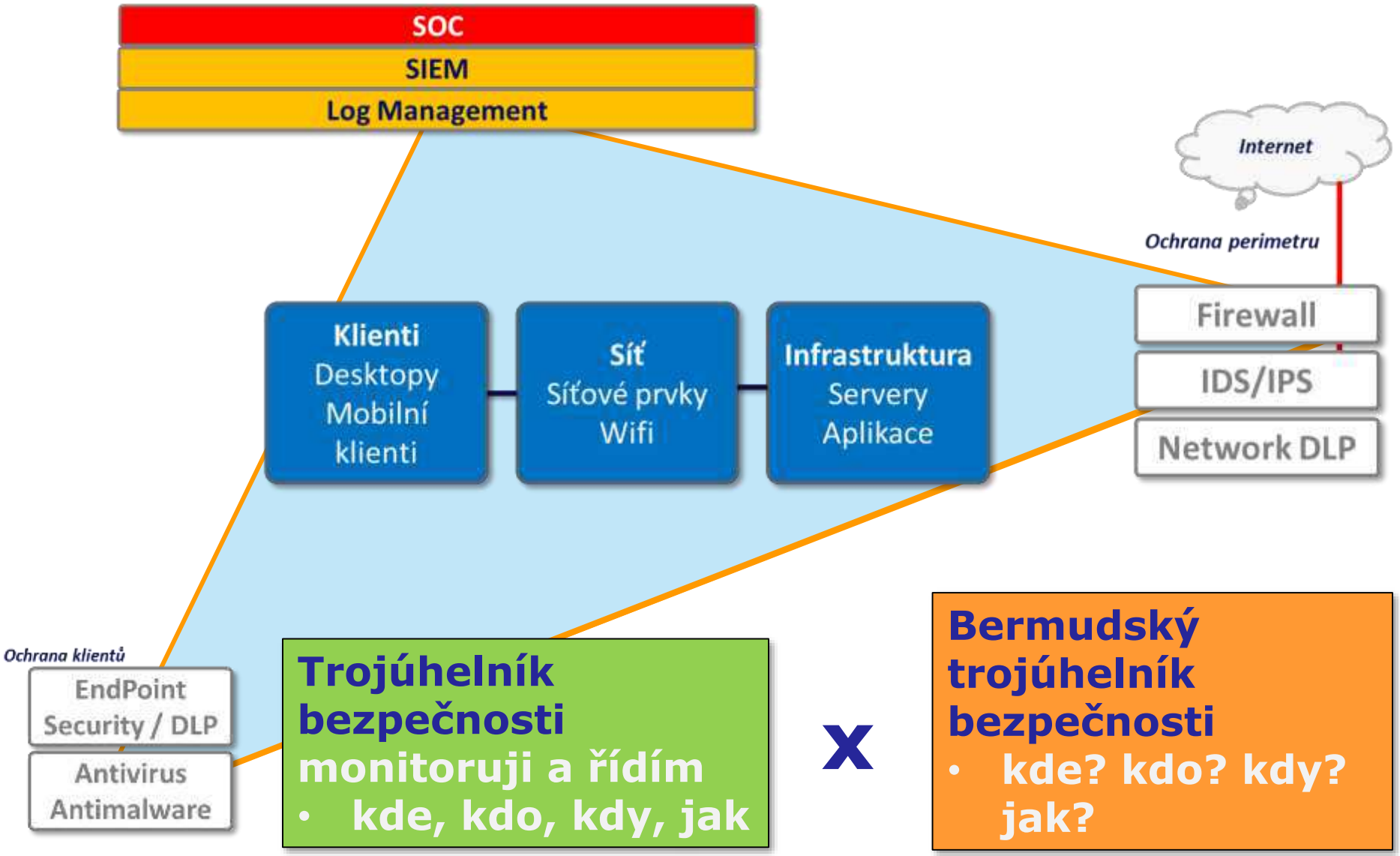
- **GDPR se zaměřuje především na zajištění ochrany osobních údajů**

Bez zajištění bezpečnosti počítačové sítě není možné zajistit ochranu osobních údajů

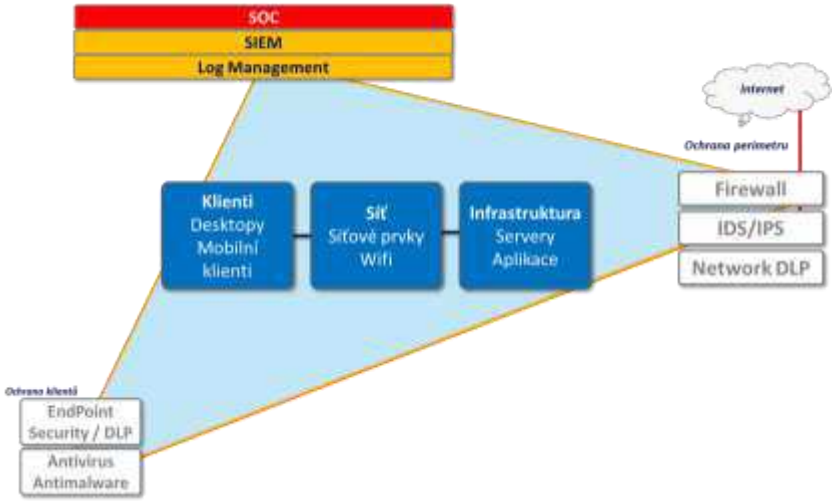
Jak vám Novicom pomůže?

- **Se svými partnery vám pomůže při systematickým zaváděním GDPR**
- **Řešení Novicomu se pak přímo zaměřuje na**
  - zajištění interní sítě proti provozu neoprávněných zařízení v síti
    - L2 monitoring
    - NAC – autentizace a autorizace
  - zvýšení dostupnosti a zajištění bezpečnosti i pro distribuované sítě (DDI/NAC)
  - ve spojení s nástroji pokročilé detekce (NBA, SIEM) - minimalizace doby nezbytné pro eliminaci škodlivých zařízení v síti

Bezpečnost vnitřní sítě



Bermudský trojúhelník bezpečnosti

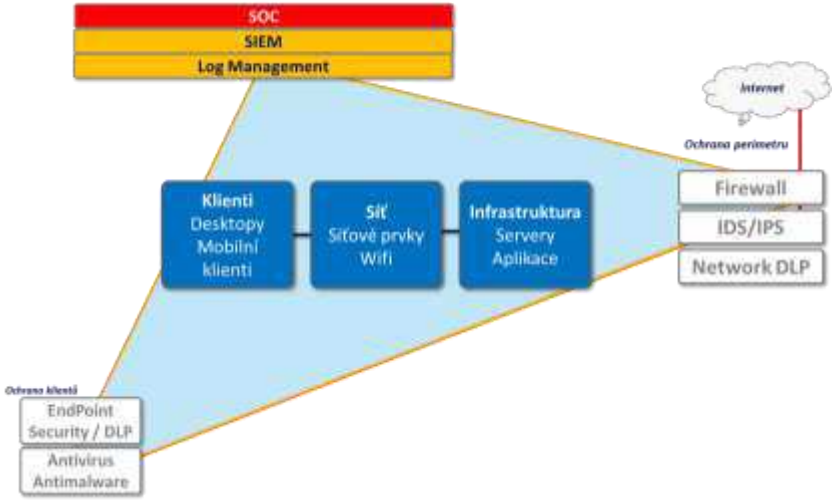


Bermudský trojúhelník bezpečnosti

- 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

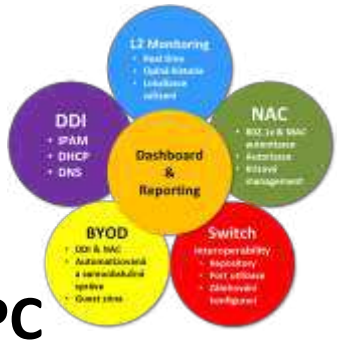
- **Identifikace hrozby – Operátor SOC**
  - **SIEM** vyhodnotí bezpečnostní incident
  - **SOC** operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne **lokalizovat zařízení**
    - 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

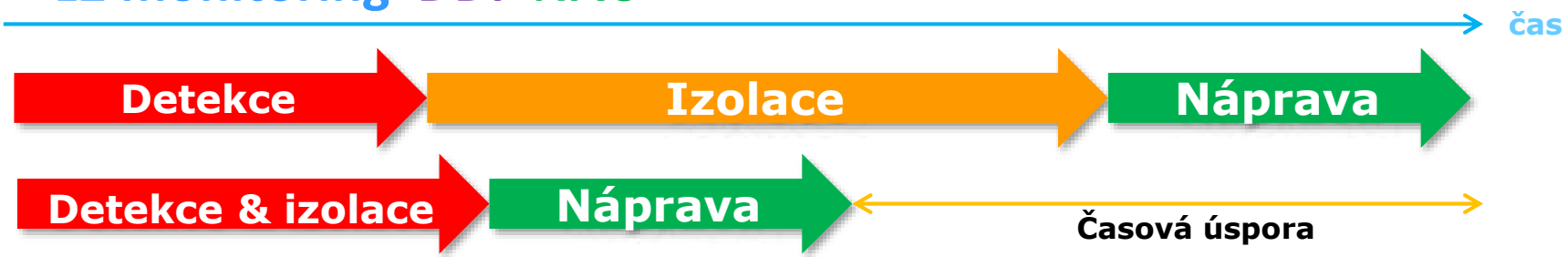
minuty



minuty/ hodiny

Shrnutí

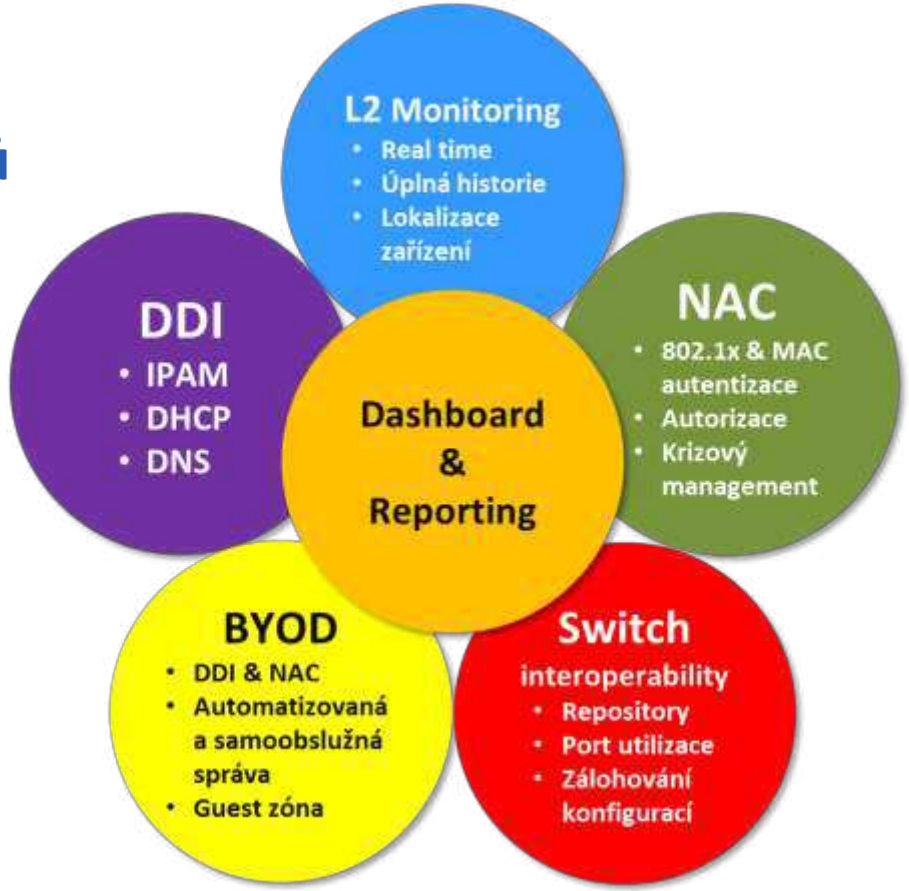
- Je v pořádku, že se věnujete ochraně
  - Perimetru a Klientů
- Počítejte ale s tím, že tato ochrana bude překonána
  - Signature based protection
- Zajistěte si nástroje pokročilé detekce a monitoringu v síti
  - NBA
  - SIEM
- Investujte do integrovaných nástrojů, které vám pomohou výrazně zkrátit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



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)
- pokročilé komunikace s aktivními prvky sítě



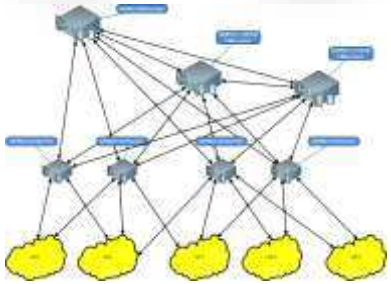
Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace a auditovaní činností operátorů 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

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, datový přenos, architektura)
- **Unikátní spojení DDI a NAC**
  - DDI nástroj je doplněný o NAC
  - Optimalizované pro rozsáhlé distribuované sítě

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