



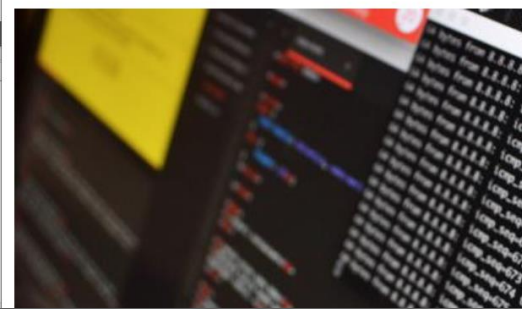
## Budování nákladově efektivní kybernetické ochrany

Jindřich Šavel

CEO

7. 10. 2021

**CYBER SECURITY & NETWORK MANAGEMENT  
HAS NEVER BEEN EASIER**



## HOSPODÁŘSKÉ NOVINY

# Na ochranu před kyberútoky nemáme peníze a stát nepomáhá, tvrdí rok šéfové nemocnic. Aktuálně hackeri útočili v Praze



Fakultní nemocnici Brno vznikla při březnovém kybernetickém útoku škoda v desítkách milionů korun. Nemocnice přišla o některá administrativní a ekonomická data nebo o objednávkový systém u dárců krve.

autor: HN – Tomáš Škoda

Markéta Řeháková, redaktorka

16. 3. 2021 / 19:00 / 9 minut čtení

Další útok hackerů. Napadli systémy Správy železnic, provoz vlaků ale neohrozili

DNES 12:42

ČTK

Kybernetičtí útočníci v minulých dnech napadli počítačové systémy Správy železnic. Podle státní organizace však nijak provoz ani bezpečnost na tratích neohrozili. Případem se nyní zabývá Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Upozornil na to dnes Deník N. Hackeri útočili na síť státních organizací i v minulých týdnech.



li počítačové at citlivé z. I když adá stín ás i firma



# Pohled Novicomu na oblast kybernetické bezpečnosti

## Závažný globální problém

- **Nárůst počtu i závažnosti kybernetických incidentů**
- **Znamé útoky v ČR**
  - Nemocnice Benešov, FN Ostrava, FN Brno, OKD, ...
  - *Škody jsou ve výši stovek miliónů Kč*

## Proč se to děje?

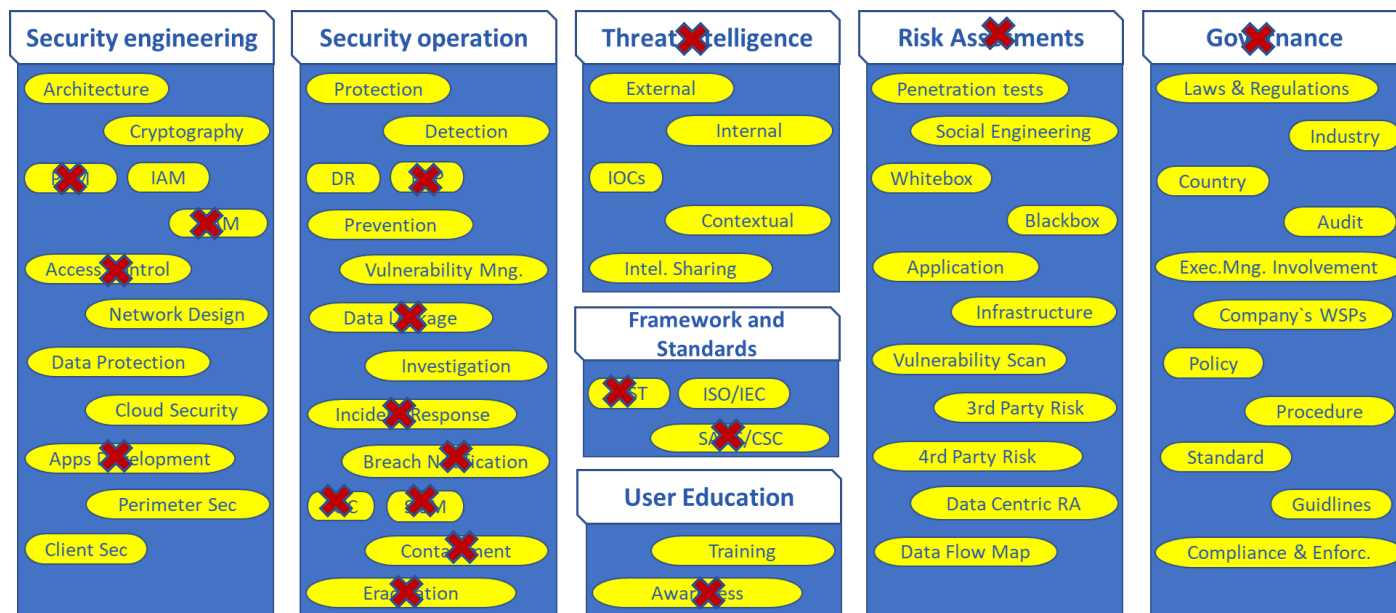
- **Podcenění managementem organizací**
  - není chápána závažnost problematiky
  - není ochota věnovat tomu adekvátní zdroje (finanční a lidské)
- **Kybernetická bezpečnost je svěřována přímo do IT oddělení**
  - IT je zaměřeno na zajištění provozu a za to je i hodnoceno
  - kybernetická bezpečnost odčerpává IT lidské zdroje a finance pro zajištění jejich primárního cíle

# Kyberbezpečnost – příliš komplexní disciplína

Zajištění inhouse security v organizacích

po-pá 8-16

24x7



**Vybudování týmu se znalostmi, které umožní postavit se v reálném čase hackerům, je pro více než 90% organizací ekonomicky nereálné!**

# Řešení problému

- Řešením je sdílení specializovaných zdrojů kybernetické ochrany se specialisty:
  - **SOC – Security Operation Center** – služba vrcholového bezpečnostního dohledu
- Bezpečnostní monitoring nabízí kde kdo. Jaký je ten správný?
  - Pouze SOC, který je **přípravený plně převzít zodpovědnost za boj s hackery a být schopen provádět obranné reakce kdykoliv**, bez součinnosti s administrátory zákazníka
- **Vize aktivního SOCu**
  - Aktivní SOC může nabídnout bezpečnost 24x7 a proaktivní incident response pouze v případě, že se zákazníkem sdílí nástroje zajišťující vhléd do sítě a řízení sítě
- **Vizí Novicomu je poskytovat sofistikované technologie a know-how, které zákazníkům usnadní jejich připojení k aktivnímu SOCu**

# Optimalizace rozdělení oblastí bezpečnosti mezi in-house a sdílené zajištění

Oblast bezpečnosti	Inhouse bezpečnost	Sdílená bezpečnost
Kvalifikovaný personál 24x7		
Ochrana perimetru		
Ochrana klientů		
Řízení sítě a síťových služeb		
Správa a vizualizace asetů		
Síťový a infrastrukturní monitoring		
Základní detekce		
Pokročilá detekce		
Reakce		
Strategie řízení bezpečnosti		
Bezpečnostní standardy a procesy		
Povědomí a vzdělávání		
Správa rizik		
Governance		

## Vhodné rozdělení bezpečnosti mezi inhouse a sdílený mód dokáže

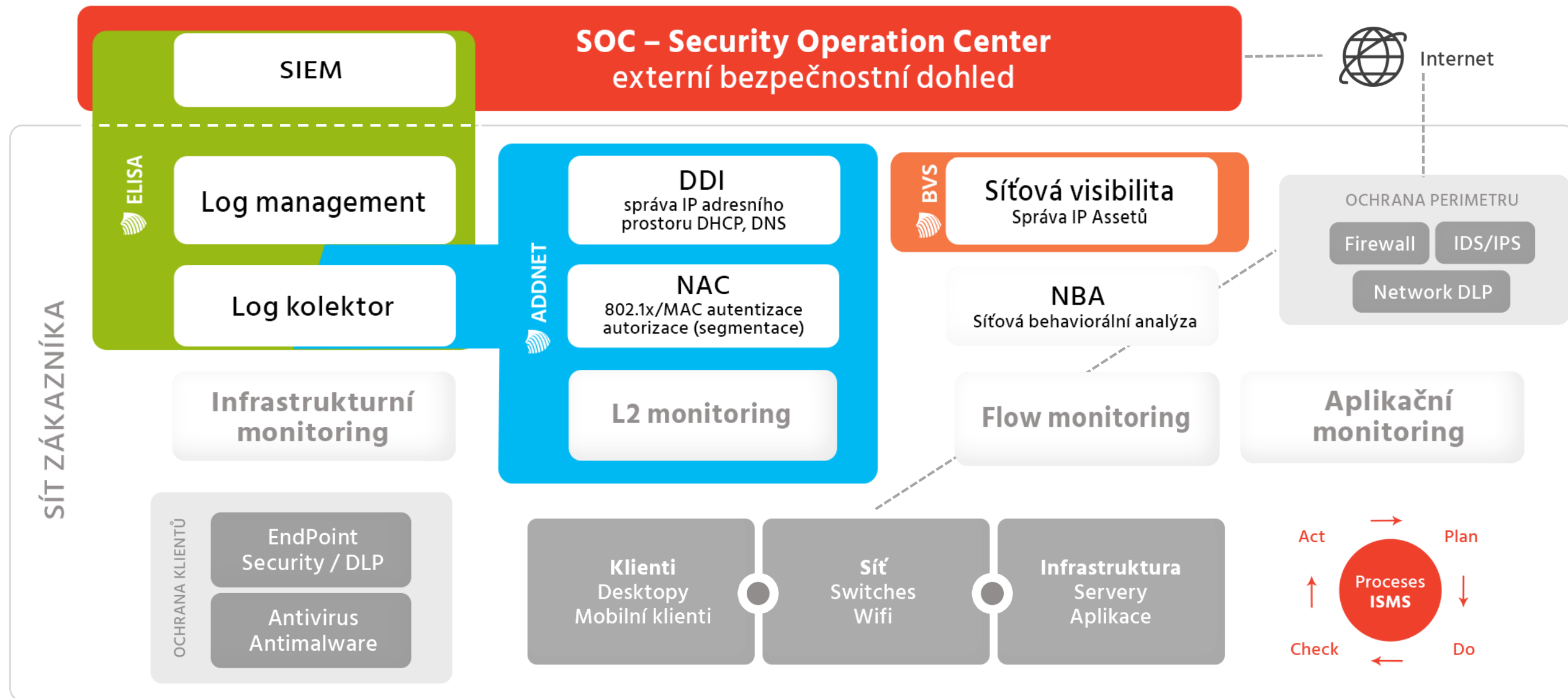
- Garantovat funkční model bezpečnosti
- Zrychlit zavedení funkčního modelu
  - do 6 měsíců
- Přinést zásadní úspory ve výši 50-70%
  - Investice do technologií
  - Podpora technologií
  - Kvalifikovaný personál pro 24x7

**Studie podinvestovanosti kybernetické ochrany**

# Studie podinvestovanosti kybernetické ochrany

- Velmi vhodné pro skupiny organizací
- **Cílem studie je**
  - Změřit stav podinvestovanosti kybernetické ochrany
    - Porovnání stávajícího stavu kyberbezpečnosti organizace s cílovým stavem (benchmarking)
  - Poskytnout managementu představu o potřebách investičních a provozních prostředků
    - Spočítání TCO na 5 let pro chybějící/nedostatečné části kyberbezpečnosti
  - Dát podklady pro rozhodnutí o dalším směřování strategie budování kyberbezpečnosti
    - Porovnání zajištění **IN-HOUSE bezpečnosti** s variantou **SDÍLENÉ bezpečnosti**
    - Porovnání budování SDÍLENÉ bezpečnosti **v rámci skupiny** vs. s využitím **zkušeného poskytovatele SOCu**
  - Navrhnout roadmapu pro naplnění vybrané strategie
- **Cílem studie není**
  - provádět detailní zkoumání a návrhy pro jednotlivé organizace, ale přinést podklady pro rychlé a efektivní strategické rozhodnutí – **cenově dostupná studie s délkou v jednotkách týdnů**

# Naplnění bezpečnostní vize Novicomu





# Novicom řešení pro vizi aktivního SOCu

- **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, včetně segmentace a mikrosegmentace

- **Podpora správy a monitoringu v rozsáhlých sítích**

- Distribuovaný model řízení sítě DDI/NAC a monitoring vzdálených lokalit
  - L2, netflow/IPfix, syslog

- **Sběr a vyhodnocování systémových logů**

- Log management funkcionalita
- SIEM funkcionalita

- **Úplná viditelnost aktiv a jejich komunikace**

- Vizualizace a klasifikace IT aktiv a jejich komunikace

- **Podpora rozhodování při řešení incidentů**

- Vyšetřování komunikace aktiv a znalost důsledků nedostupnosti aktiv na provozované business služby (aplikace)







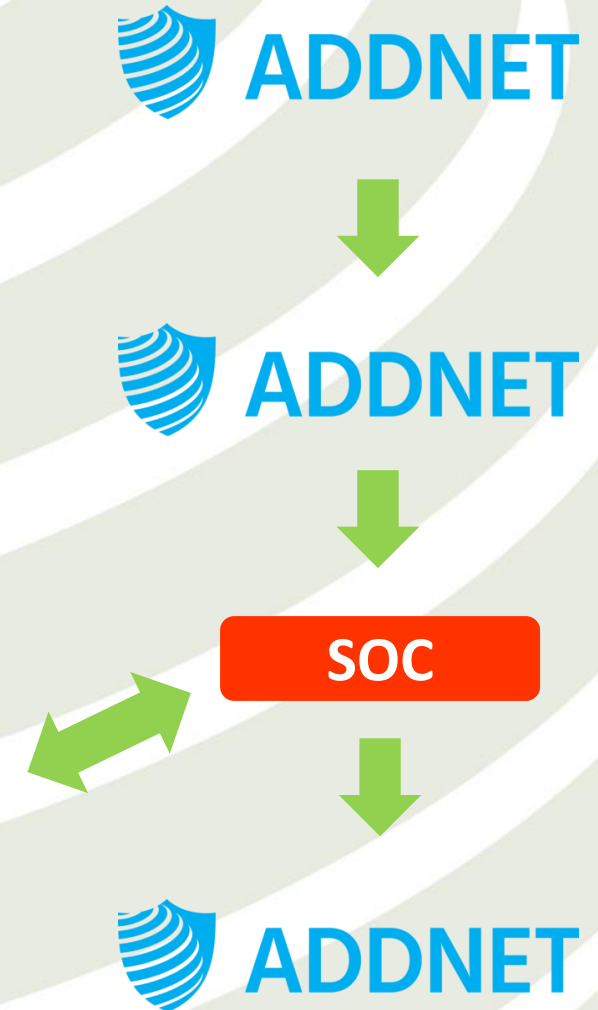
## Novicom ADDNET

Unikátní DDI/NAC nástroj přinášející zásadní zjednodušení a zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích.

# **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**  **ELISA**
  - zjištění dopadů zařízení na business služby  **BVS**
- **zajištění okamžité reakce na zjištěné hrozby – incident response**





# Unikátní rozsah funkcionalit



**NAC**

**L2**  
monitoring

**Switch**  
Interoperability

**DDI**

**Dashboard  
& reporting**

**Aktivní  
SOC**

**Sítová  
viditelnost**

**BYOD**

**Pokročilé  
síťové  
politiky**

**DACL**

**Alert  
Centrum**

**Integrace**





# ELISA

## **Novicom ELISA** Security Manager

Nástroj pro sběr a vyhodnocení  
Kybernetických bezpečnostních událostí

# KLÍČOVÉ VLASTNOSTI

## OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

- Automatizované vyhodnocování
- Korelace – nalézání vzájemných vztahů
- Zabudovaný „Change Auditor“
- Propracovanější alarmy a notifikace
- Centrální správa agentů
- Distribuovaný sběr logů
- Výpočet míry rizika
- Zjišťování zranitelností
- Normalizace logů a systematizace dat
- Agregace logů



# CO ZJISTÍTE?

**Z JAKÝCH MÍST  
LIDÉ PŘÍSTUPUJÍ  
NA FIREMNÍ WEB?**



**KDO PROVEDL  
ZMĚNU  
V DATABÁZI?**



**KTEŘÍ UŽIVATELE  
STAHUJÍ NEJVÍCE  
DAT Z INTERNETU?**



**KDO SMAZAL  
SOUBORY  
NA SDÍLENÉM DISKU?**



**K JAKÝM CHYBÁM  
DOCHÁZÍ  
V PODNIKOVÉM IS?**



**KDO SE SNAŽÍ  
UHÁDNOUT  
PŘÍSTUPOVÉ HESLO?**





# Novicom BVS

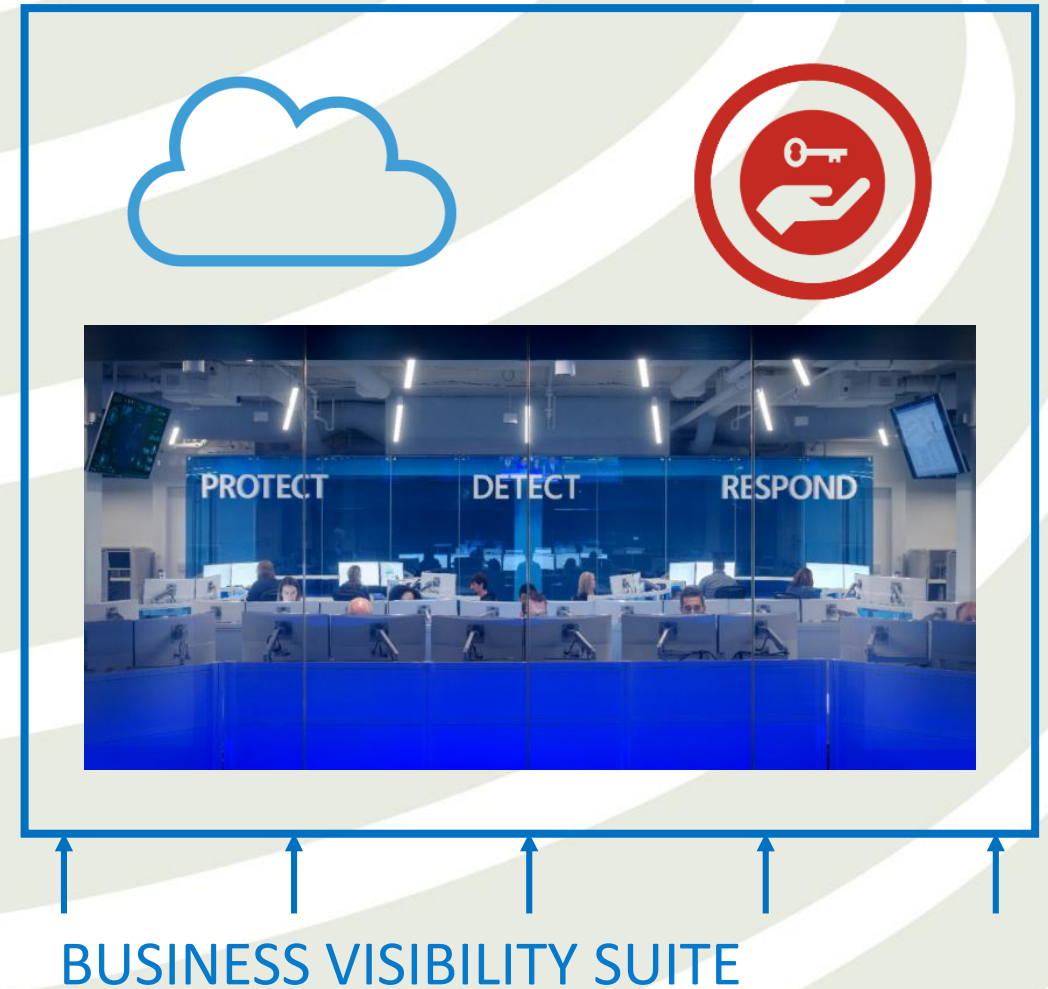
## Business Visibility Suite

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



# Základní využitelnost BVS

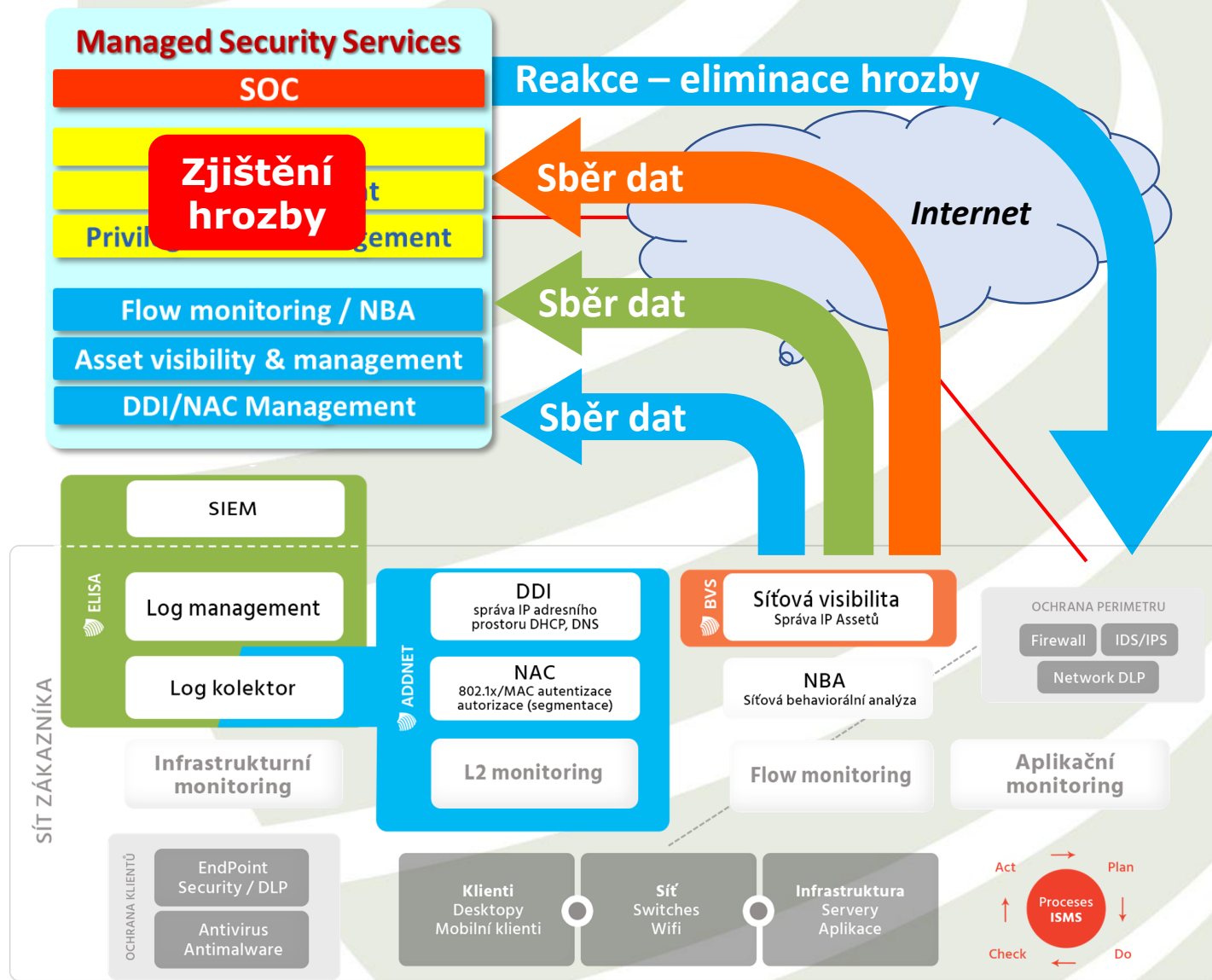
- Onboarding dohledových služeb a podpora Security Operations center (poznání zákazníka)
- Visibilita business služeb a vizualizace vztahů s IT provozem
- Týmy IT/Security pro šetření dopadů incidentů a eliminace shadow IT
- Usnadnění iniciálních kroků při implementaci NAC řešení
- Migrace systémů z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



# Spolupráce Novicomu se SOC provozovateli

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

**Proč ne?**



- Jednotlivé **organizace a společnosti nemají dostatek zdrojů** na zajištění kybernetické ochrany na úrovni schopné odolat útokům hackerů
- Zásadním problémem je **nedosažitelnost kvalifikovaných odborníků** v počtu umožňujícím zajistit **kybernetickou ochranu 24x7**
- Nutností bude **sdílení kybernetické ochrany mezi více organizací**
  - Komerční SOC vs. Státní SOC vs. Krajský SOC
- **Spočítejte si to a správně se rozhodněte**
  - Studie podinvestovanosti kybernetické ochrany
- **Využijte získané zkušenosti**
  - Jsme připraveni sdílet získané zkušenosti s jednotlivými organizacemi i skupinami organizací

# Další informace?

## Sledujte nás na:

- [www.novicom.cz](http://www.novicom.cz)
- [LinkedIn](#)
- [Facebook](#)

## Kontaktujte nás na:

- E-mail: [sales@novicom.cz](mailto:sales@novicom.cz)
- Tel.: +420 271 777 231

## Adresa:

- Třebohostická 14
- 100 00 Praha 10