novicom

Doba kybernetické (ne)bezpečnosti

Case study nemocnice Benešov

Jindřich Šavel
CEO
15. 9. 2020

NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

Kybernetická bezpečnost

Závažný globální problém

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

Proč se to děje?

- **Podcenění managementem firem a 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

Nemocnice Benešov - fakta

Co se stalo

- V noci z 10. na 11. prosince 2019 došlo k masívnímu šíření škodlivého kódu, který provedl zašifrování uživatelských dat
- Útočníky bylo požadováno zaplacení výkupného, na základě kterého by poskytly klíče pro zpětné rozšifrování

Průběh

- Vzhledem k masívnímu šíření po síti a její naprosté kompromitaci, je zpětně velmi obtížné detailně prokázat způsob nákaza sítě
- Předpoklady
  - díky tomu, že síť nemocnice byla tzv. plochá (bez plné segmentace pomocí VLAN), tak bylo možné přímo šířit nákazu mezi zařízeními bez jakéhokoliv omezení
  - hrozba se šířila již za firewallem - nebyla tak zaznamenána neobvyklá činnost až do doby plošného zašifrování zařízení v síti

Důsledky

- Zašifrování počítačů znemožnilo aplikacím a uživatelům přistupovat k uloženým datům
- Většina počítačů, zdravotních zařízení a provozovaných centrálních aplikací se zastavila - to znamenalo praktické zastavení činnosti nemocnice na dobu cca dvou týdnů
- Nemocnice poskytovala pouze základní manuální úkony, zastaven byl i urgentní příjem pacientů
- Přímé finanční ztráty jsou vyčíslené ve výši více než 50 miliónů korun (neprováděné výkony)

Nemocnice Benešov - fakta

Obnova provozu

- Po zjištění závažnosti útoku pracovníky IT byl kontaktován NÚKIB. Pracovníci NÚKIBu ve spolupráci s PČR zajistili auditní stopy nezbytné pro vyšetřování
- Následně bylo rozhodnuto o postupu pro obnovení provozu - bylo rozhodnuto o postupném obnovení všech IT systémů ze záloh
- U všech PC a technických zařízení došlo k obnovení systémového nastavení a následně byly data obnoveny ze záloh
- U několika agend bylo kvůli stáří záloh nutné opětovně pořídit data

Přijatá opatření

- Mezi základní uplatněné opatření, bylo alespoň základní nastavení VLAN (kdy došlo k oddělení skupiny uživatelských počítačů, serverů a zdravotních zařízení)
- Po obnově provozu jsou postupně implementovány další opatření vedoucí k předcházení podobného stavu a schopnosti rychlejší reakce

Nemocnice Benešov – provoz obnoven, a co dál?

- **Obnova provozu**
  - Úspěšně provedena
  - Delší čas byl věnován sbírání auditních stop při vyšetřování
- **Povýšení bezpečnosti**
  - Přijata opatření pro zodolnění a povýšení stávající infrastruktury
    - Zálohování
    - Ochrana klientů a perimetru
    - Nastavení dynamického řízení sítě a monitoringu sítě
  - Nastaveny vrcholové procesy pro krizové řázení
- **Může se to opakovat?**
  - **ANO!**

Více otázek než odpovědí…

Vyřeší to nákup technologií pro kybernetickou ochranu?

Ano, ale…

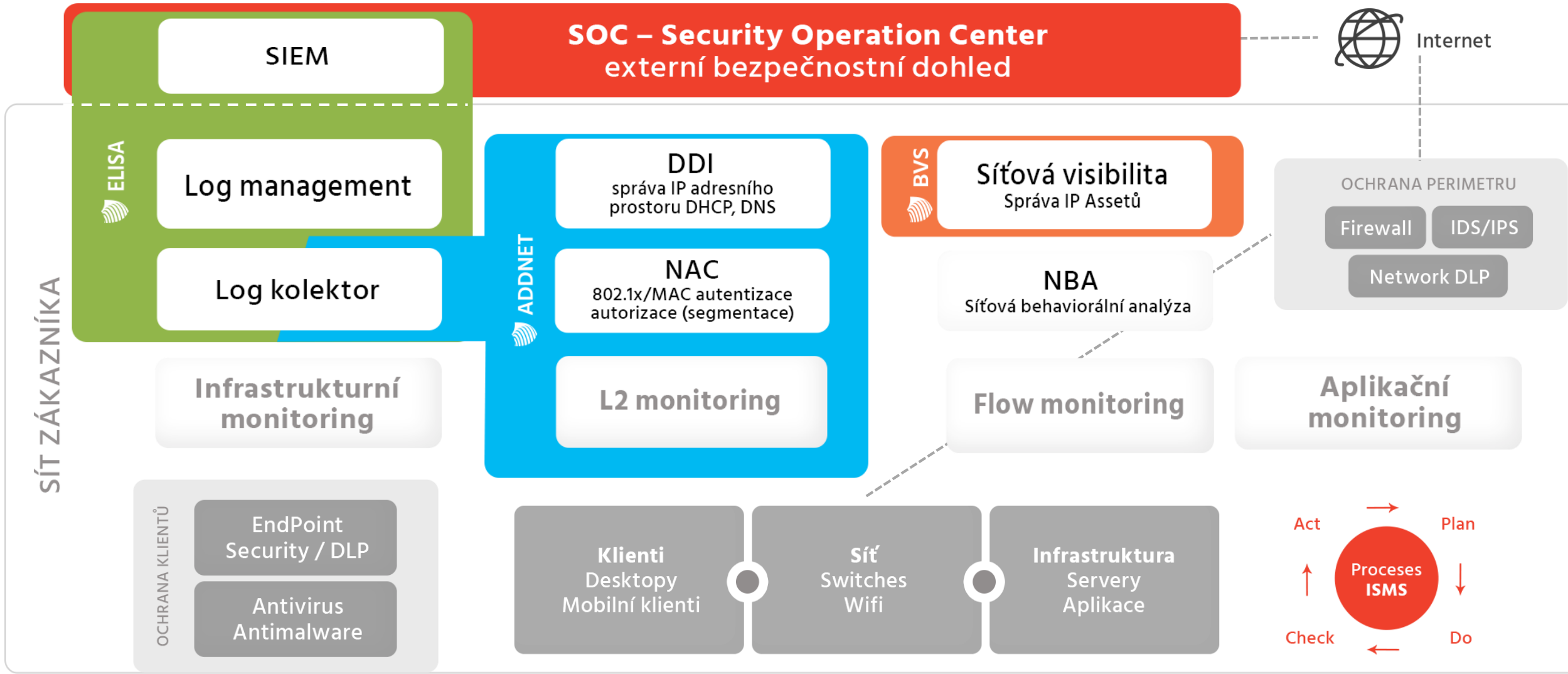
- **Jsou zapotřebí pro desítky oblastí**
  - monitoring, detekce, řízení technologií…
- **Opravdu je k dispozici kvalifikovaná obsluha?**
  - která si je jista, co má dělat v případě útoku?
- **Opravdu je k dispozici tato kvalifikovaná obsluha nepřetržitě?**
  - v režimu 24x7x365?
- **Opravdu se to vyplatí?**

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 připravený 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 vhled do sítě a řízení sítě**
- **Vizí Novicomu je poskytovat sofistikované technologie a know-how, které zákazníkům usnadní jejich připojení k aktivnímu SOCu**

Naplnění bezpečnostní vize Novicomu



Novicom řešení pro vizi aktivního SOCu

- **Úplná visibilita 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)
- **Sběr a vyhodnocování systémových logů**
  - Log managment funkcionalita
  - SIEM funkcionalita
- **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

BVS

ELISA

ADDNET

BVS

Novicom BVS

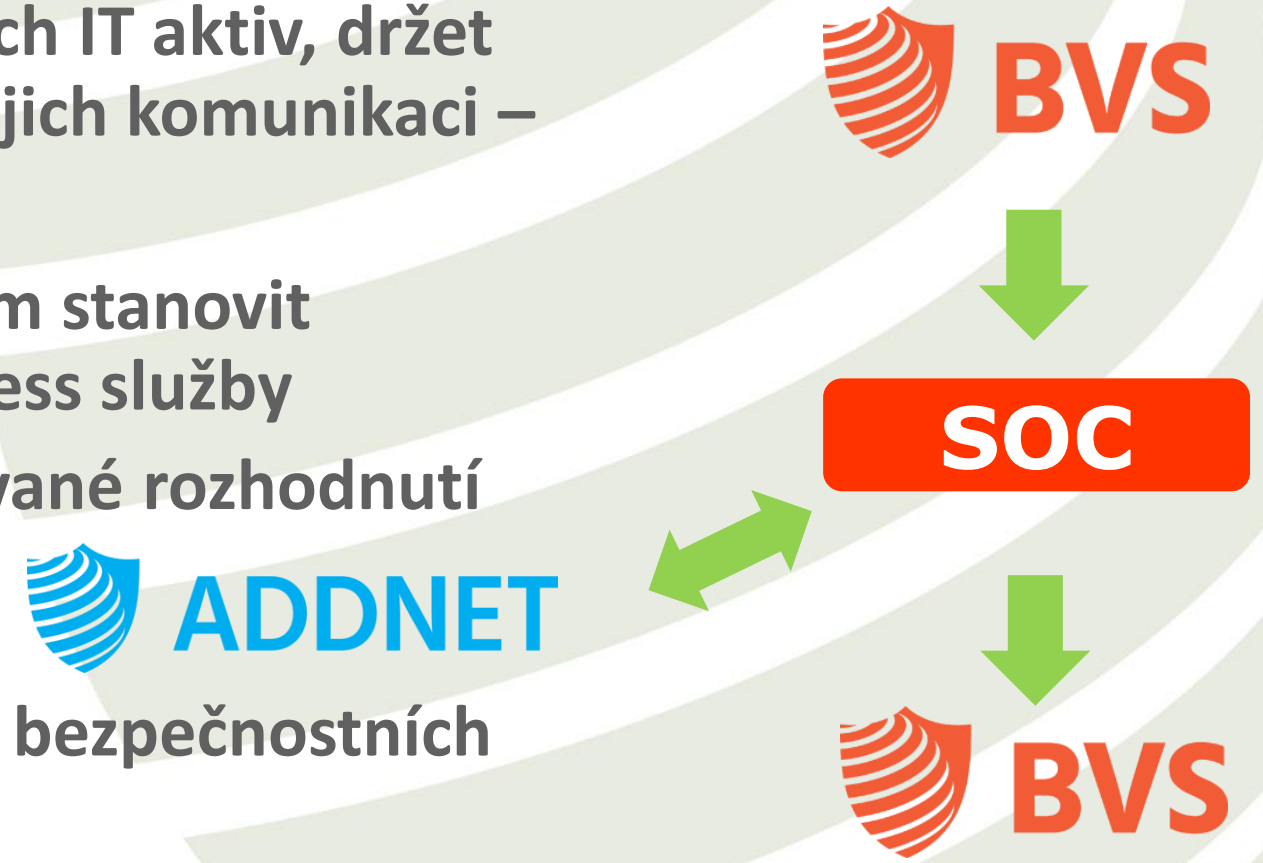
Business Visibility Suite

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

BVS – nástroj pro visibilitu komunikací IT aktiv

- navržený pro potřeby aktivního SOCu

- 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

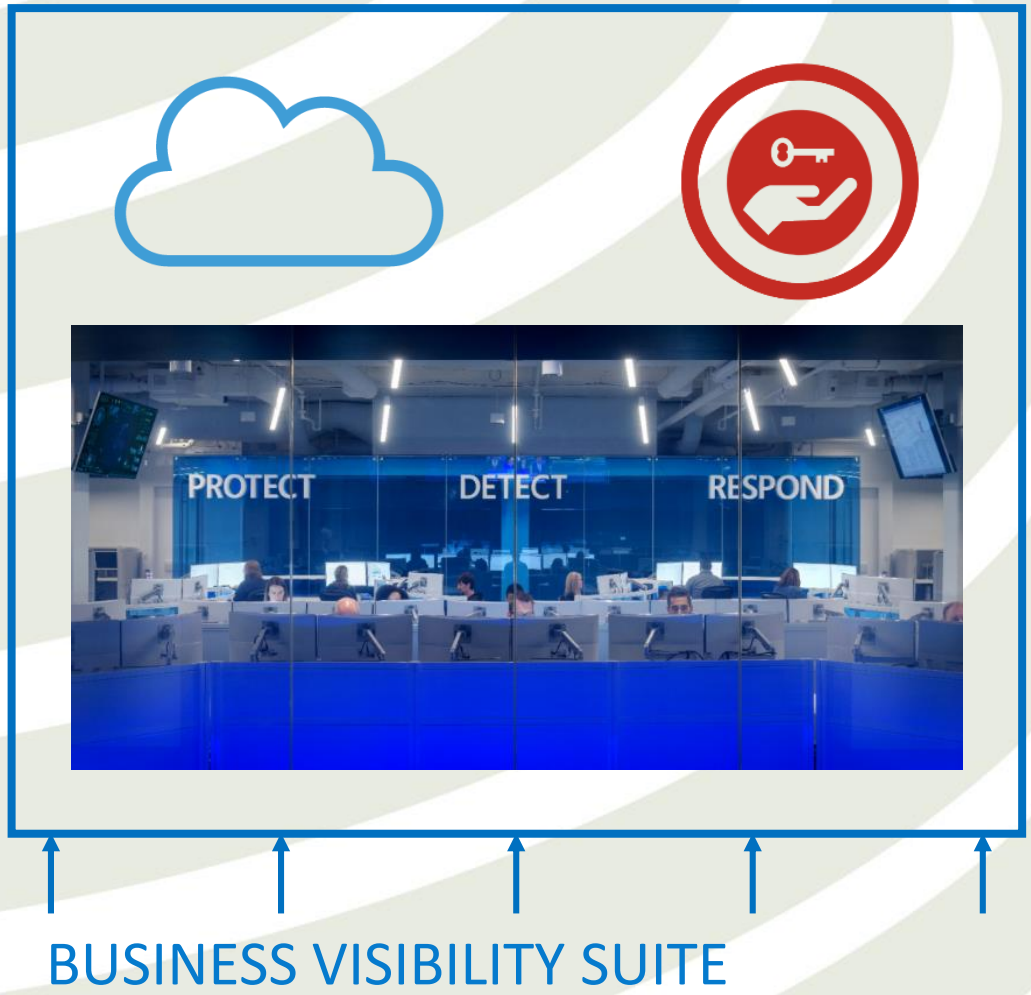


BVS potřebujete, když…

- Chybí nástroj pro správu IT aktiv, nebo není funkční/aktuální
- Nedostatečný přehled nad provozovanou IT infrastrukturou
- Chybí zaručené informace pro podporu integrací a migrací IT systémů (např. do nových segmentů, do DC/CLOUD)
- Identifikace dopadů plánovaných provozních zásahů
- Problém s identifikací rozsahu kybernetického incidentu
- Neschopnost interpretovat technické a bezpečnostní incidenty do jazyka businessu
- Existence šedých zón
- Chybí souvislost mezi aplikacemi a IT aktivy
- Není přehled a report nad aktuálními zranitelnostmi
- Analýza rizik infrastruktury není realizována na úrovni jednotlivých zařízení ve vazbě na dopady na organizaci

Základní využitelnost BVS

- Onboarding dohledových služeb a podpora Security Operations center (poznání zákazníka)
- Vizibilita 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



ELISA

Novicom ELISA

Security Manager

Nástroj pro sběr a vyhodnocení
Kybernetických bezpečnostních událostí

Novicom ELISA Security Manager (ESM)

- Robustní nástroj pro sběr a analýzu bezpečnostních událostí
- Chytřejší konzole bezpečnostního dohledu

KLÍČOVÉ VLASTNOSTI

DETEKCE BEZPEČNOSTNÍCH RIZIK

- Soulad se ZKB, GDPR, ISO, PCI
- Rychlé odezvy
- Snadno nastavitelné filtry
- Horizontální škálovatelnost

NÍZKÉ NÁKLADY

- Integrace s OpenVAS a GSM
- Integrace s Flowmon ADS
- Fyzické i virtuální appliance
- Vysoký výkon (až 10 000 EPS)

PŘEHLEDNÉ UŽIVATELSKÉ PROSTŘEDÍ

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 PŘISTUPUJÍ
NA FIREMNÍ WEB?

KDO PROVEDL ZMĚNU
V DATABÁZI?

KTEŘÍ UŽIVATELÉ STAHUJÍ NEJVÍCE
DAT Z INTERNETU?

KDO SMAZAL SOUBORY
NA SDÍLENÉM DISKU?

K JAKÝM CHYBÁM DOCHÁZÍ
V PODNIKOVÉM IS?

KDO SE SNAŽÍ UHÁDNOUT
PŘÍSTUPOVÉ HESLO?

ADDNET

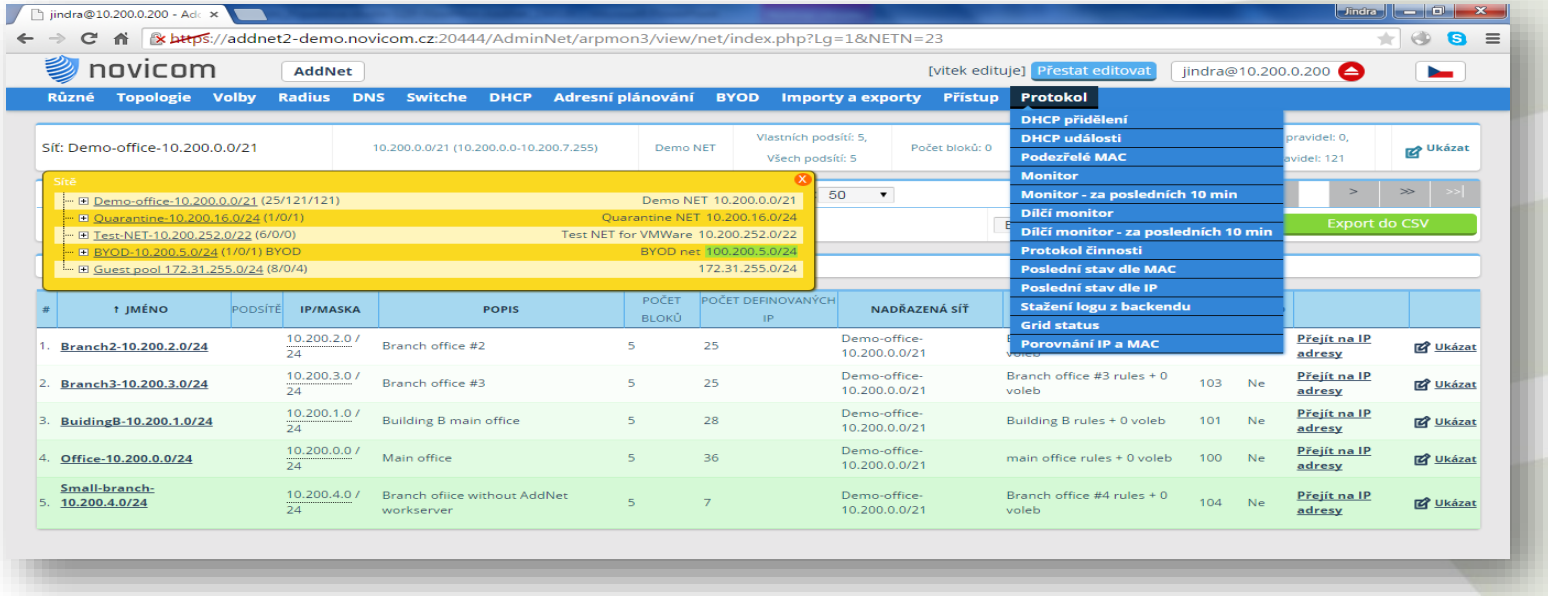
Novicom ADDNET

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

ADDNET

Je unikátní **DDI/NAC nástroj** pro zajištění **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.



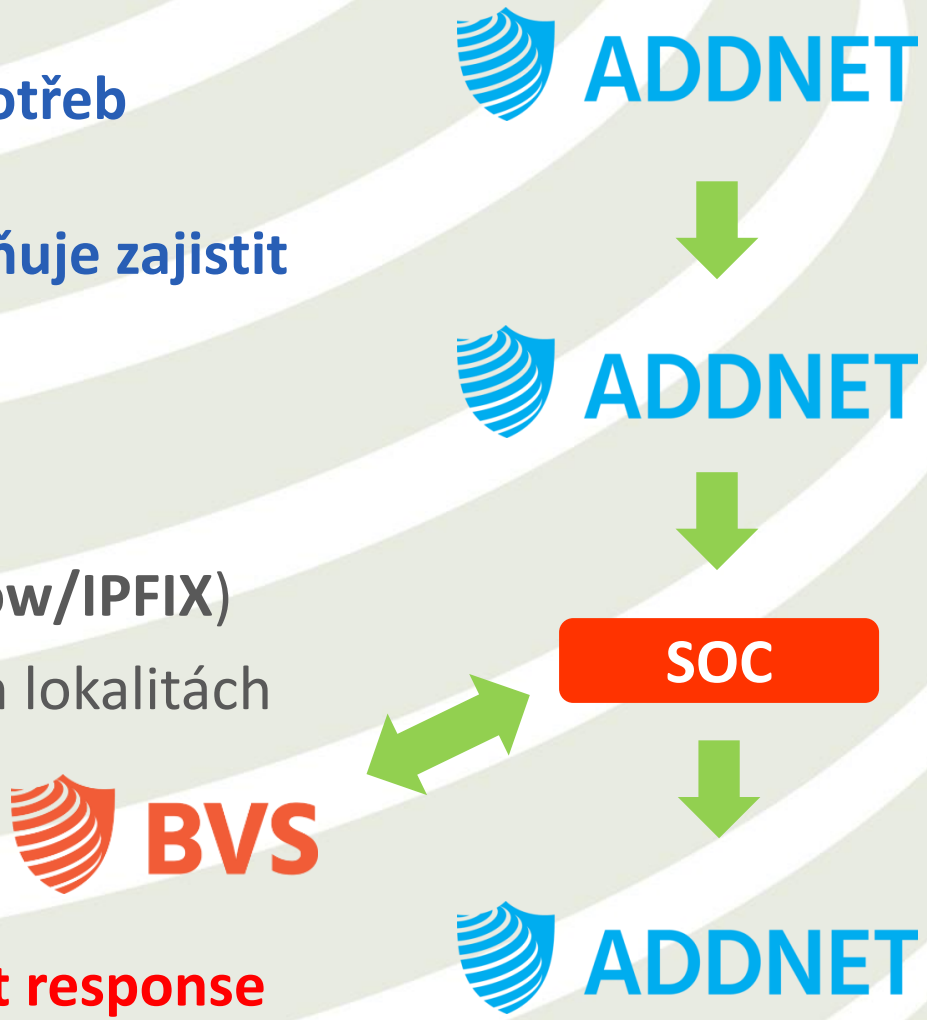
Unikátní rozsah funkcionality

ADDNET

ADDNET provozně bezpečnostní nástroj

už dnes připravený pro potřeby aktivního SOCu

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



Klíčové přínosy AddNetu

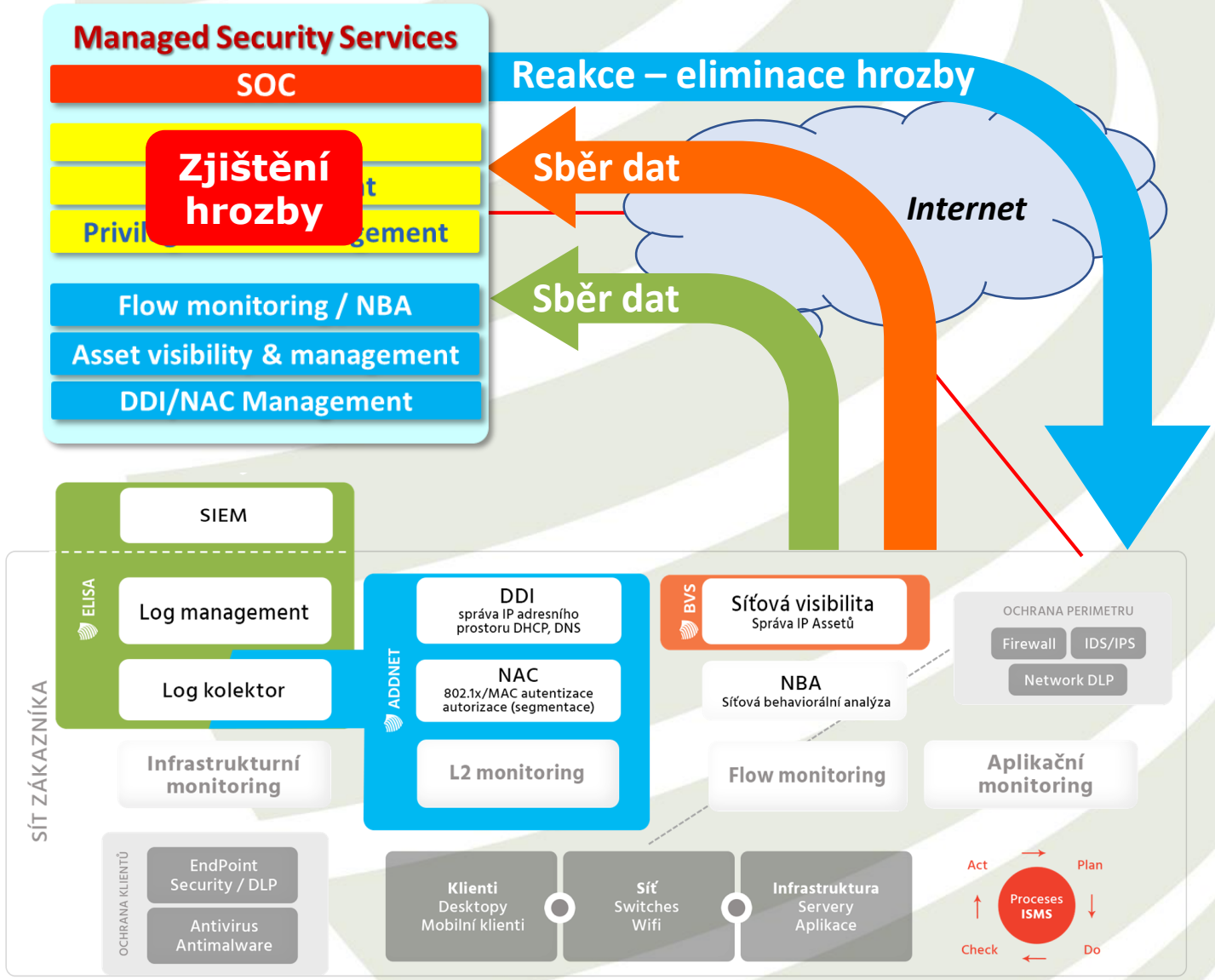
- √ **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- √ **Řádové snížení pracnosti síťové správy**
- √ **Standardizace činností a centralizace správy** v rozsáhlých sítích
- √ **DDI – zavedení integrovaných základních síťových služeb (IPAM/DHCP/DNS)**
- √ **NAC – snadné zavedení a správa**
  - Autentizace - full 802.1x a/nebo MAC
  - Autorizace - řízení VLAN/mikrosegmentace
- √ **Pokročilé síťové politiky**
  - Prevence nákaz typu ransomware
  - Automatizovaná správa důvěryhodných zařízení – trusted pools

- √ **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

Spolupráce Novicomu se SOC provozovateli

- **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, Netflow/ipfix, Syslog
  - **Schopnost okamžité reakce 24x7** bez nutné součinnosti zákazníka
- **SOC za 2 dny?**

Proč ne?



Další informace?

Sledujte nás na

- www.novicom.cz
- LinkedIn
- Facebook

Kontaktujte nás na

- Email: sales@novicom.cz
- Tel. +420 271 777 231

Adresa

- Třebohostická 14
- 100 00 Praha 10