SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Firewall, IDS a jak dále? Flow monitoring a NBA, případové studie

Jiří Tobola

INVEA-TECH

INVEA-TECH

- Český výrobce řešení FlowMon pro monitorování a bezpečnost síťového provozu
- Desítky referencí na českém trhu
  - akademická sféra – univerzity, knihovny, AV
  - státní sféra – magistráty, kraje, nemocnice
  - soukromá sféra – od malých až po největší společnosti
  - poskytovatelé internetu
- Mnoho referencí i ze zahraničí, např. Korea Telecom, monitoring páteřních evropských sítí

Doporučení Gartner

Recommendation

After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

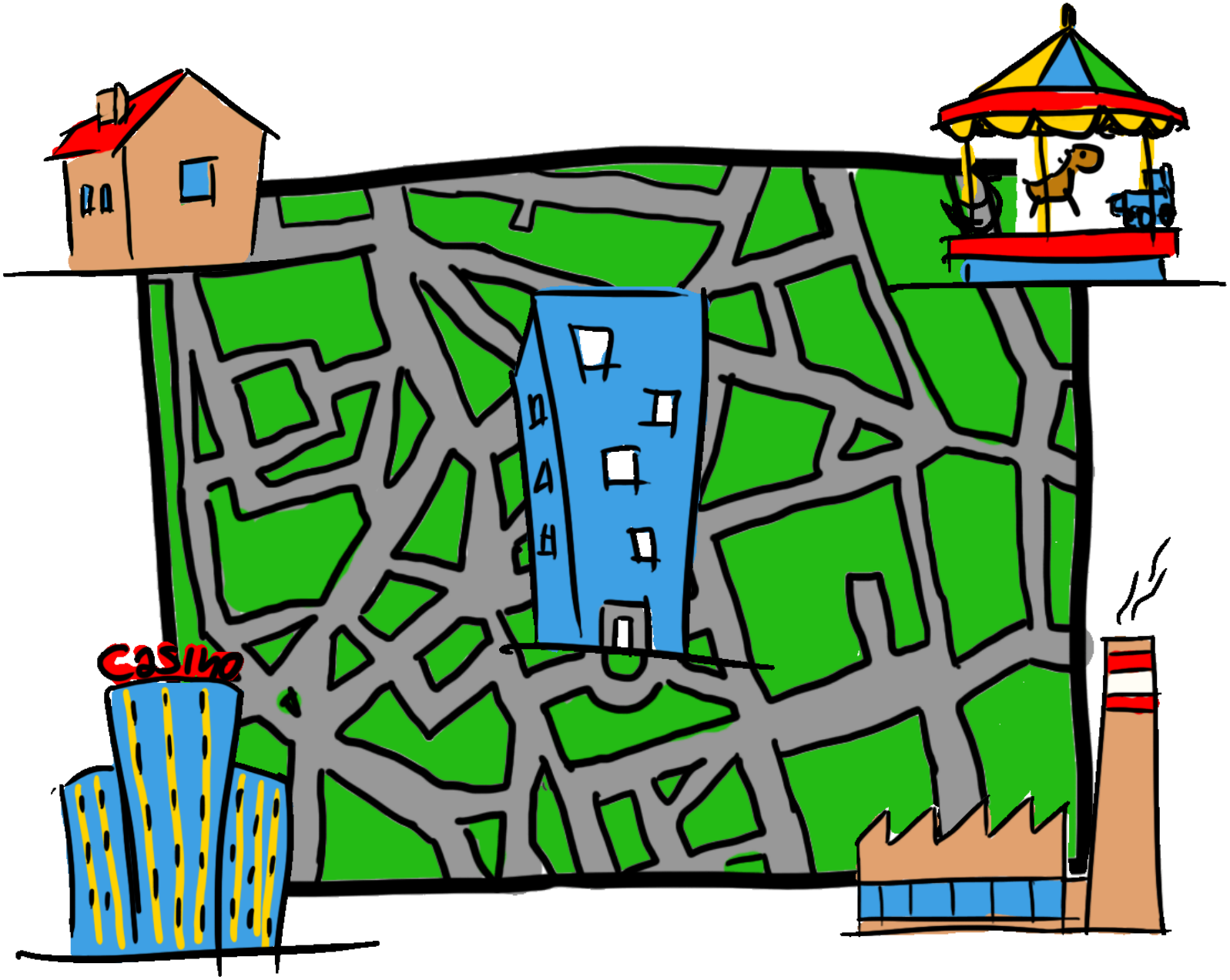
Paul Proctor

Lawrence Orans

Gartner

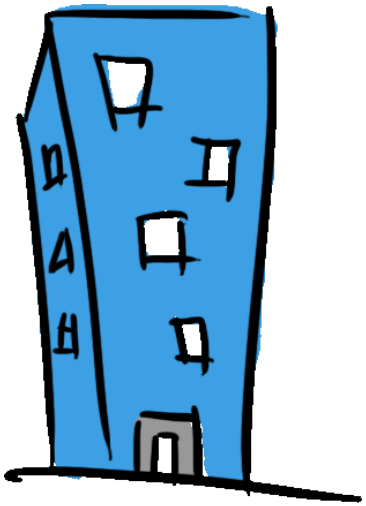
Přehled technologií

- Monitoring
  - SNMP
- Bezpečnost
  - Firewall
  - IDS/IPS
  - Antivir
  - Antimalware
  - Identity Management
  - SIEM
- Network Security Monitoring
  - NetFlow
  - NBA/ADS

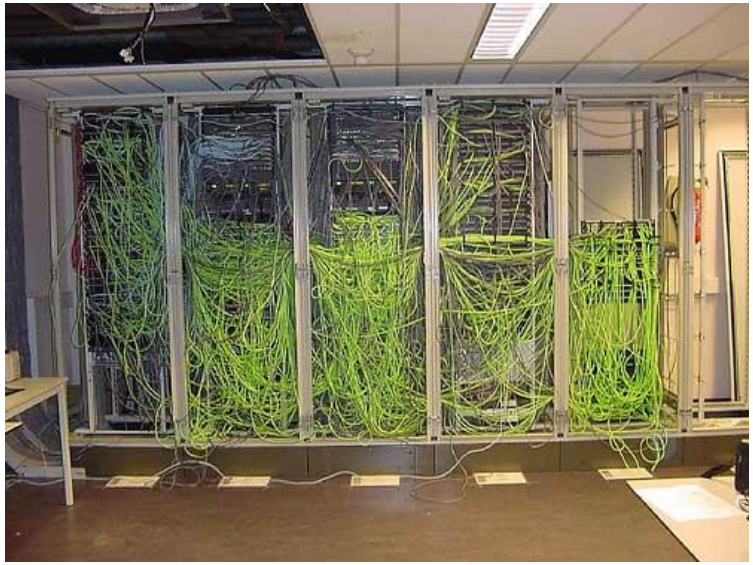

CASINO

Počítače

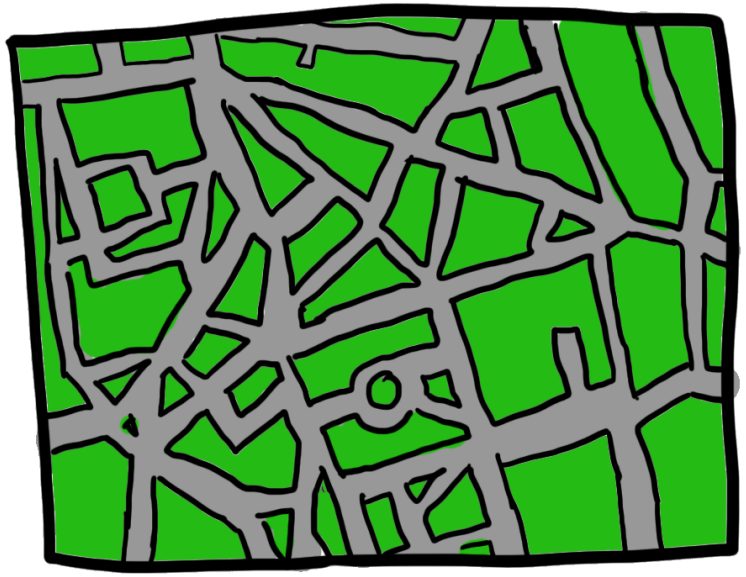
Domy



Kabely



Cesty

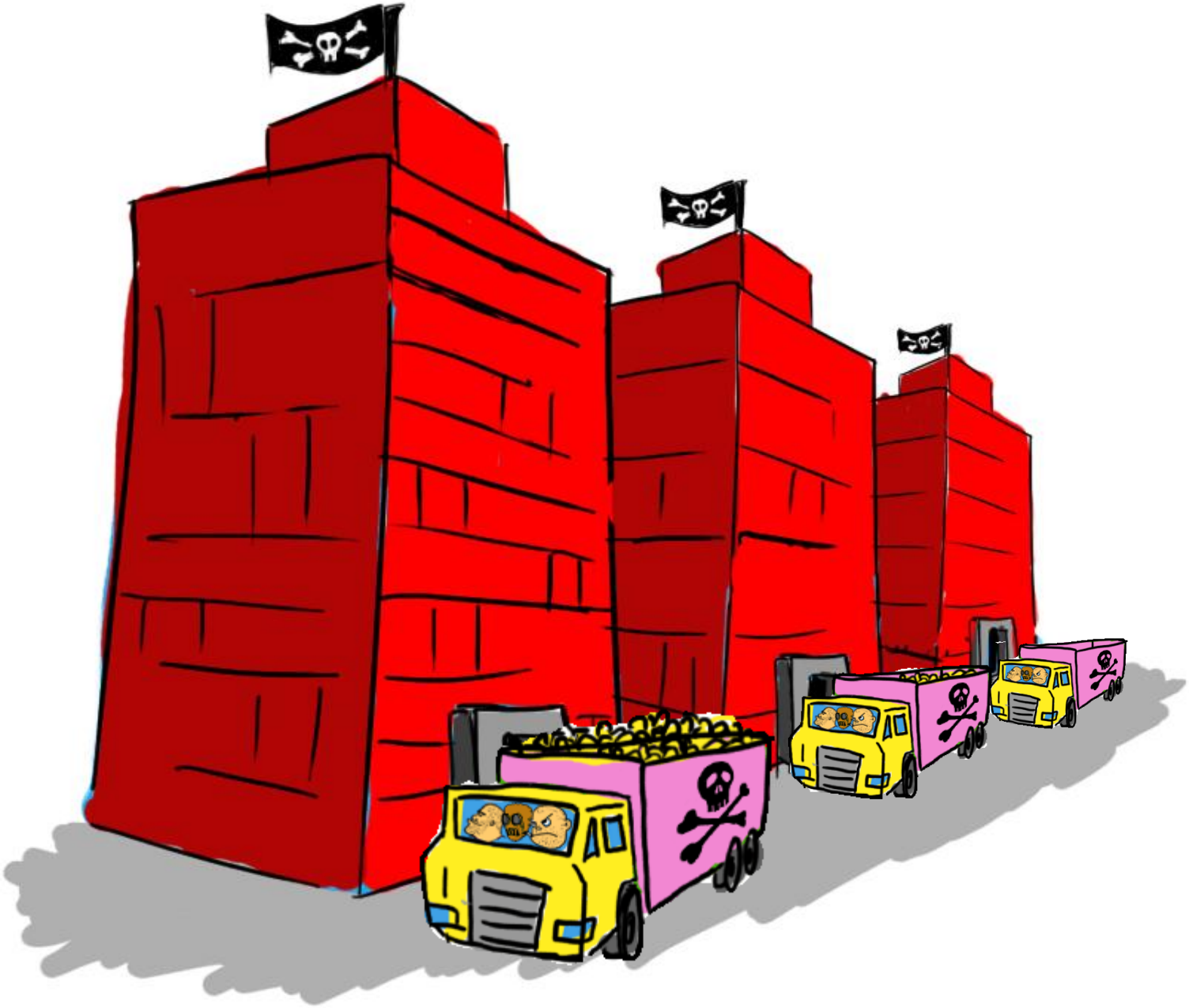


Uživatelé

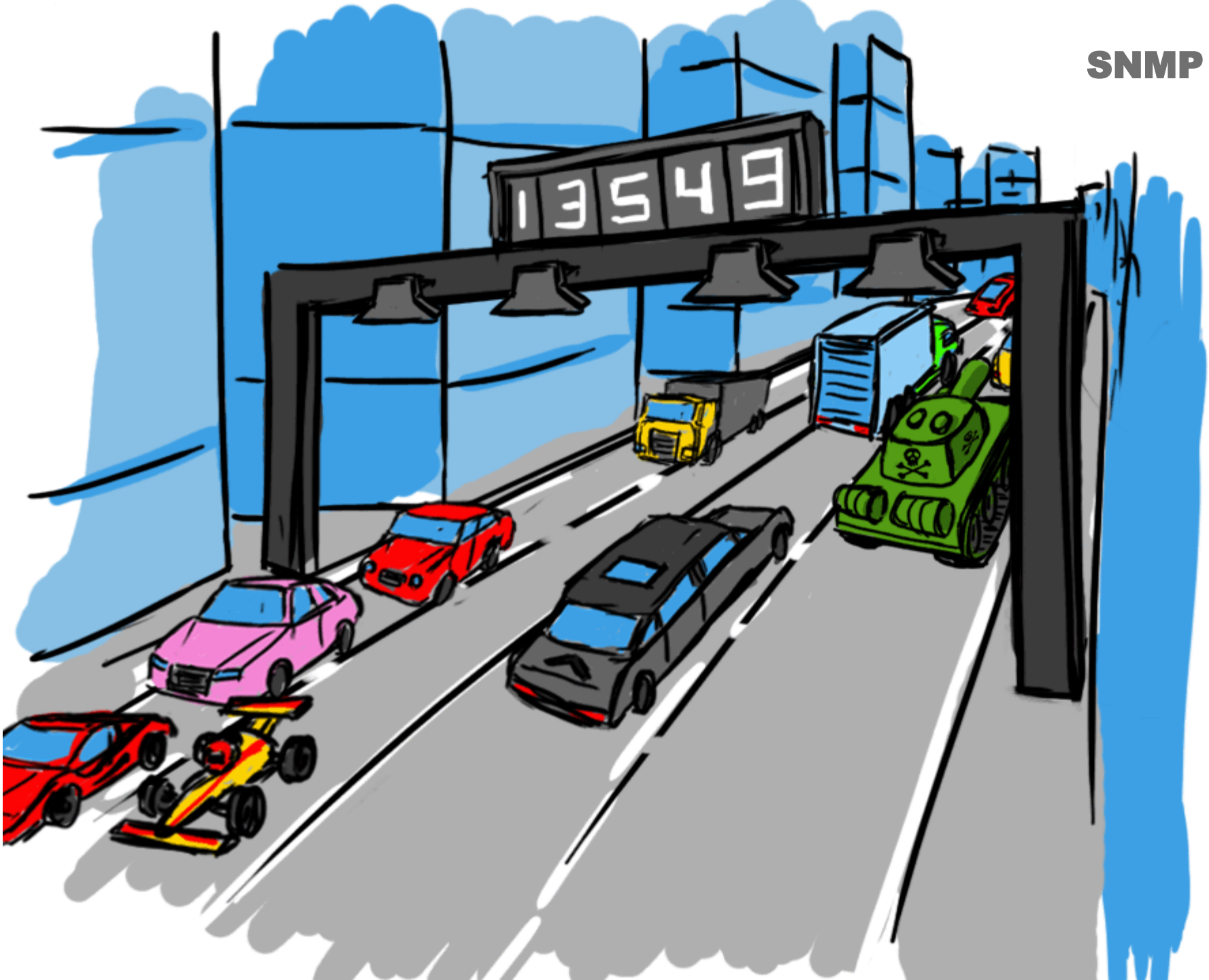
Obyvatelé

Co je cílem


FASTER
BETTER
EASIER

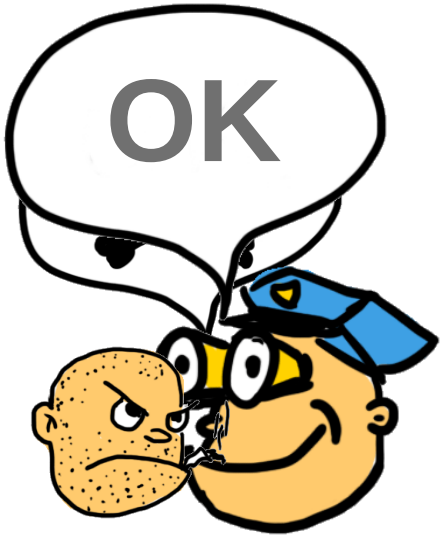


SNMP Monitoring


SNMP
13549

Firewall

FIREWALL



Intrusion Detection System
Intrusion Prevention System

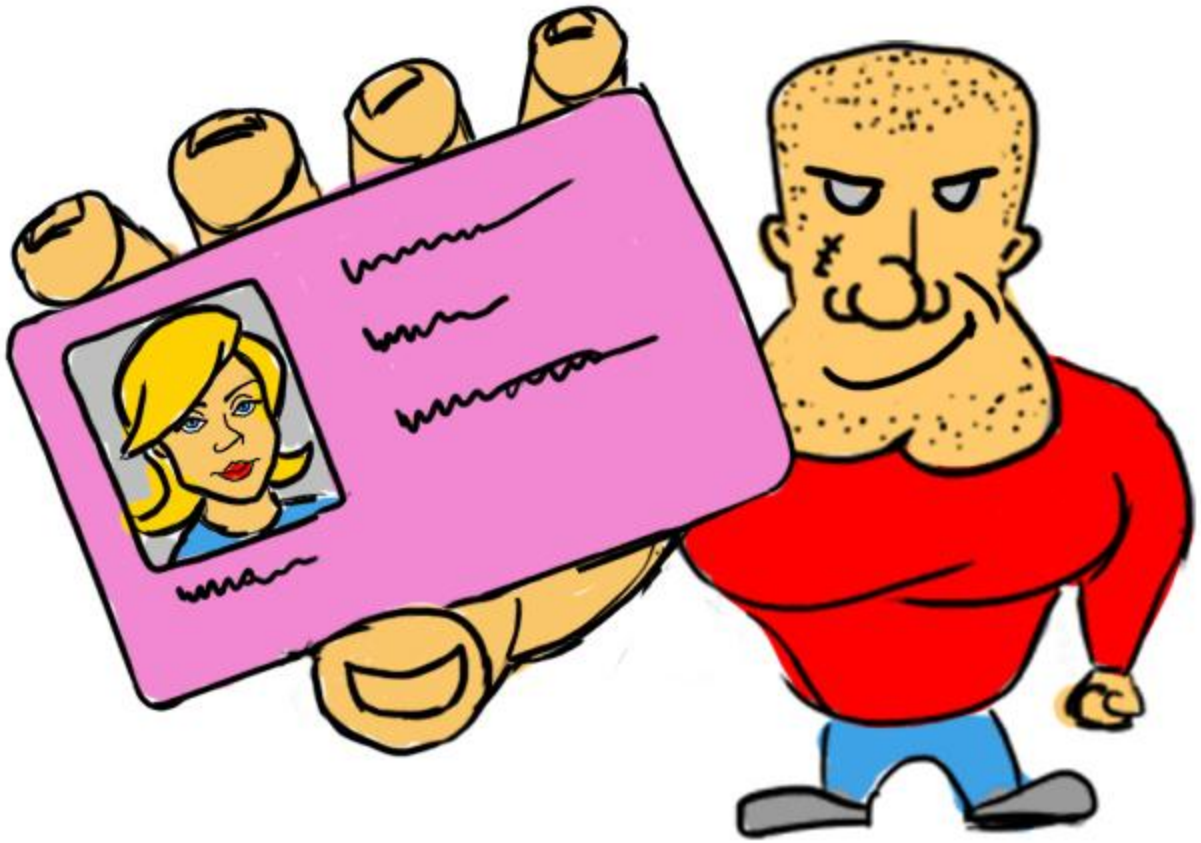
IDS/IPS

Anti Virus, Anti Spyware, …

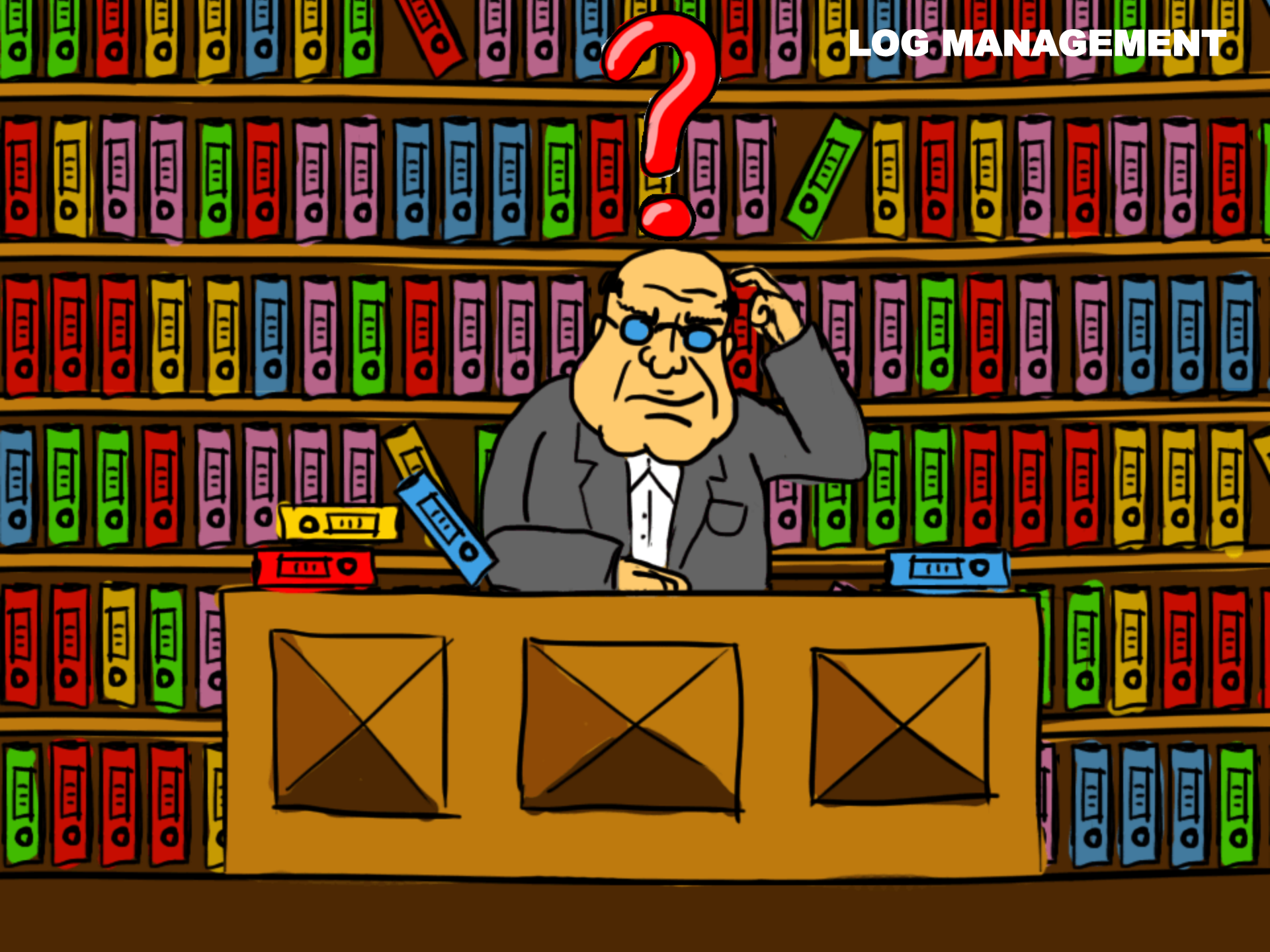
ANTI-X

Identity Management

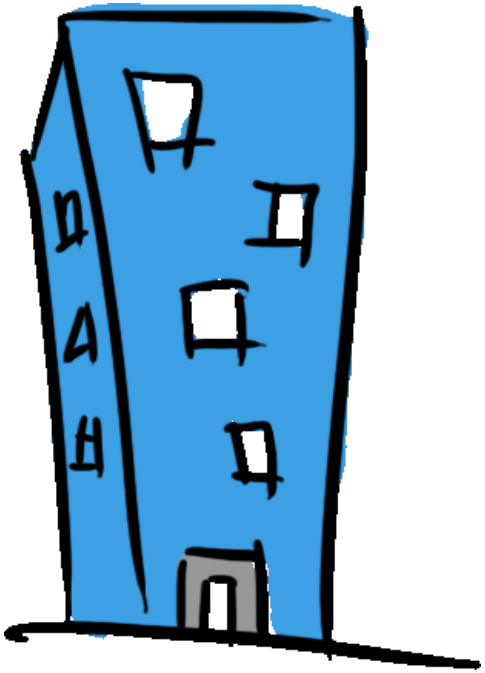
IDENTITY MANAGEMENT

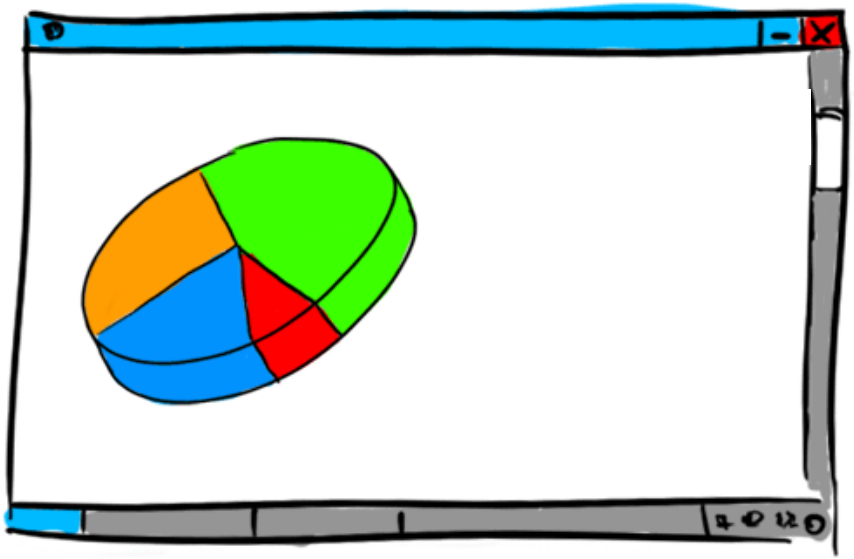


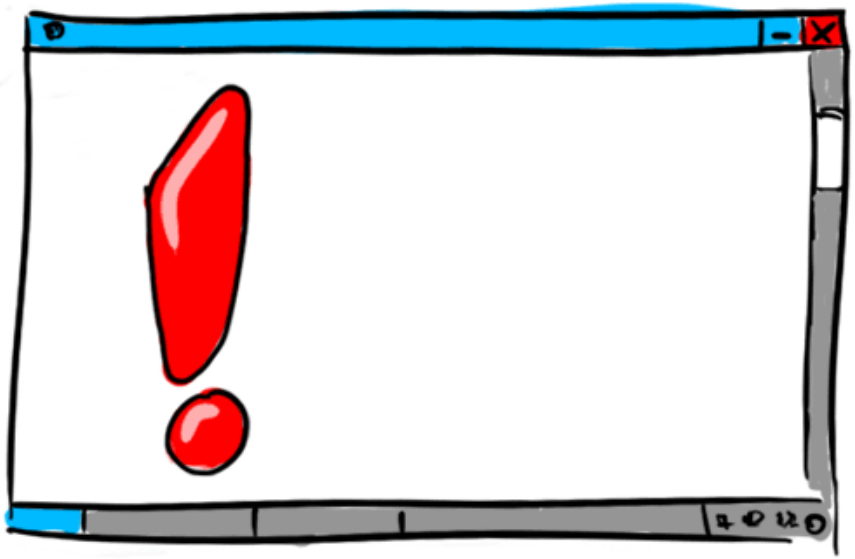
Log Management


LOG MANAGEMENT

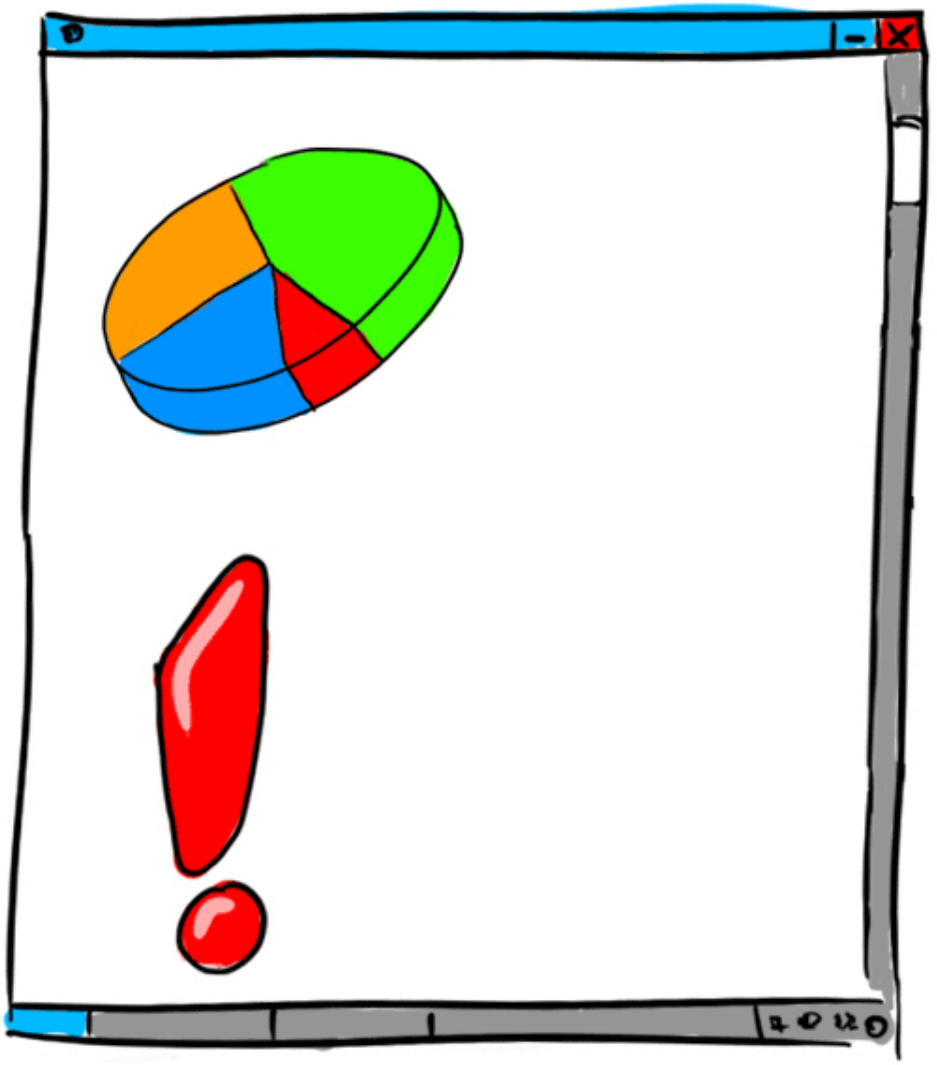
Network Security Monitoring (Bezpečnostní monitoring sítí)





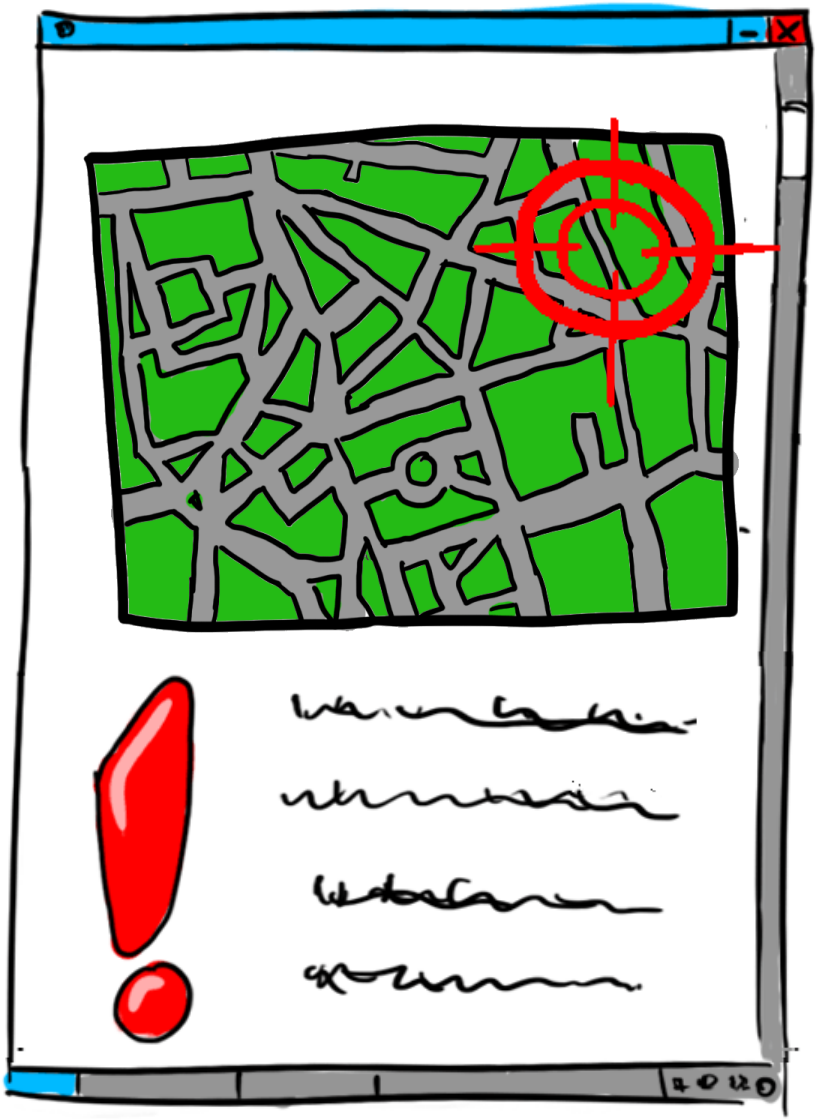


Detekce známých vzorů nežádoucího chování



Detekce anomálií


Moulin Rouge

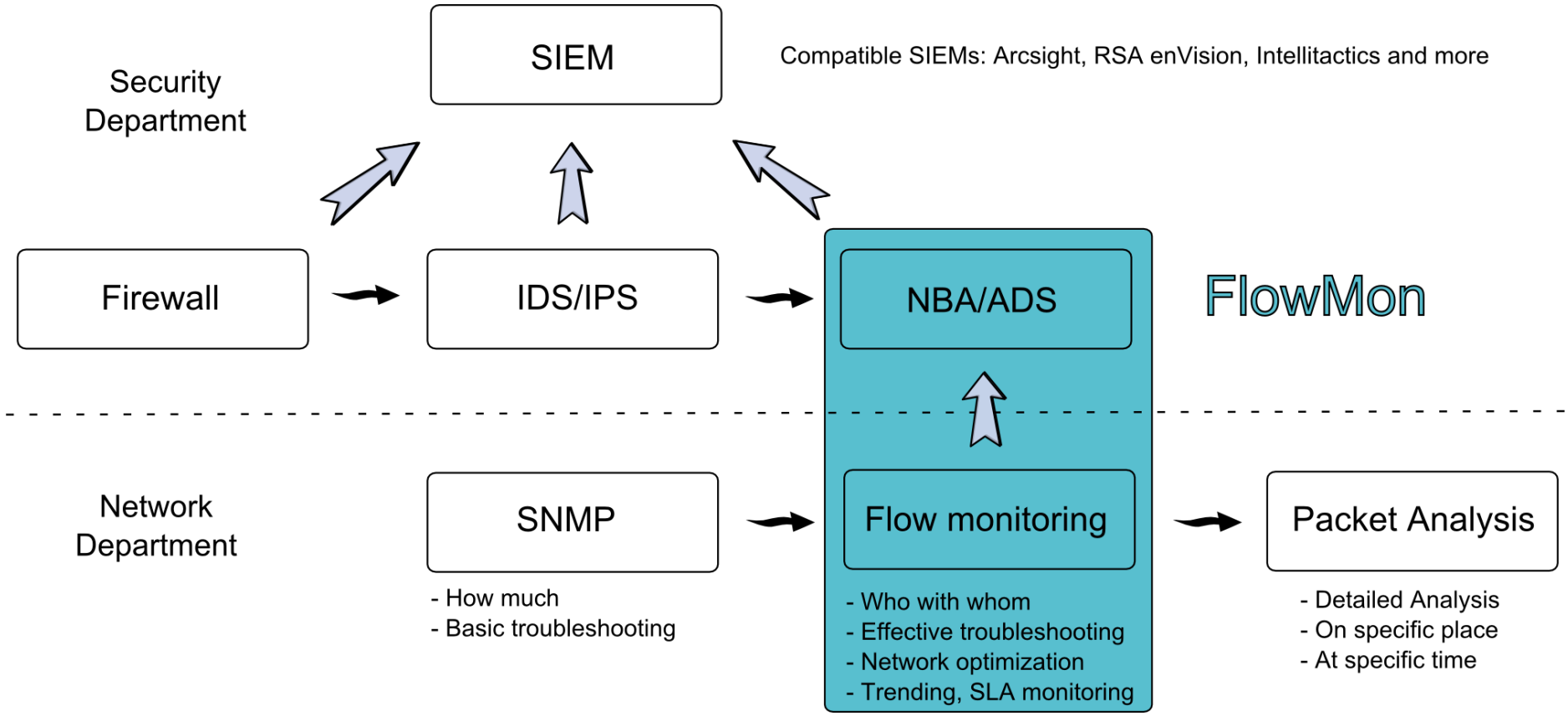


Přehled technologií

- Monitoring
  - SNMP – informace kolik paketů a dat, základní troubleshooting
- Bezpečnost
  - Firewall – perimetr, pravidla
  - IDS/IPS – perimetr, vzory v paketech, ochrana proti známým hrozbám
  - Antivir – koncové stanice, vzory známých virů
  - Antimalware – koncové stanice, vzory známého malware
  - Identity Management – ověřování uživatelů
- Network Security Monitoring – doplnění technologií výše
  - NetFlow – co se děje v síti (kdo, s kým, co, jak...)
  - NBA/ADS – odhalení i dosud neznámých hrozeb a nestandardního chování stanic

Přehled technologií

- Doporučená architektura síťové bezpečnosti

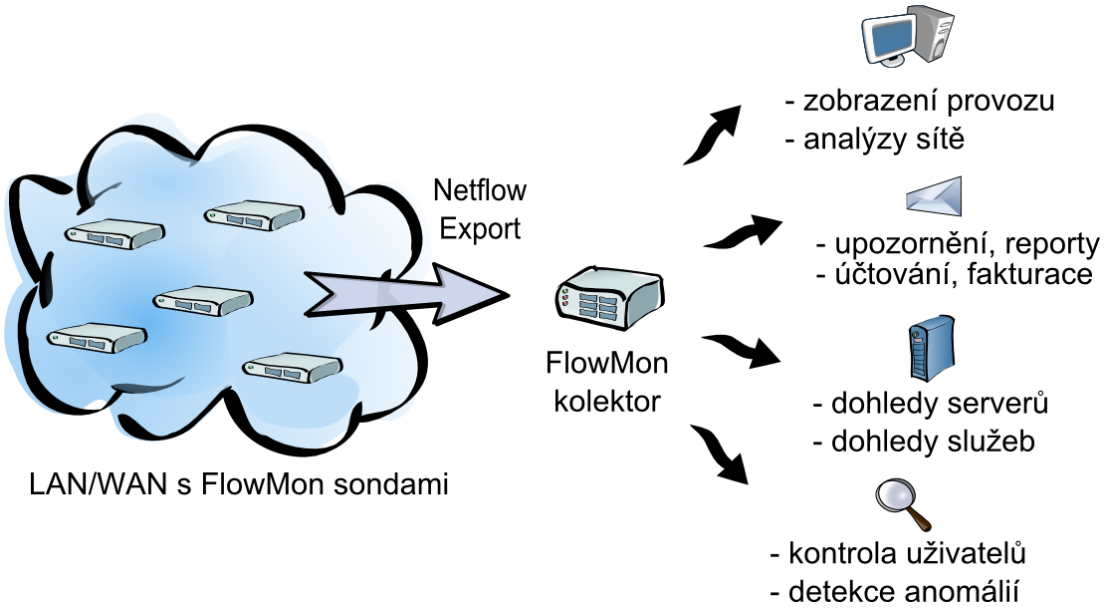


Gartner & Praxe

- Gartner
  - „Neexistuje bezpečnost bez monitoringu. Mnoho lidí bylo dlouho přesvědčeno že bezpečnost stačí budovat na perimetru a monitoring je zbytečná práce navíc. Opak je pravdou.“
  - bezpečná organizace = firewall + IPS + NBA/NBAD/ADS
  - monitoring síťových komunikací a nework behavior analysis zařazen do TOP10 nejdůležitějších technologií roku
- Praxe
  - 90% organizací nemá implementován systém monitorování datových toků / síťových komunikací
  - vzrůstající požadavky na monitoring a bezpečnost, audity finančních institucí, budování CSIRT týmů na mnoha úrovních
  - chybějící nástroje pro podporu implementace a kontroly ISO 27000, ISMS

FlowMon – síť pod kontrolou!

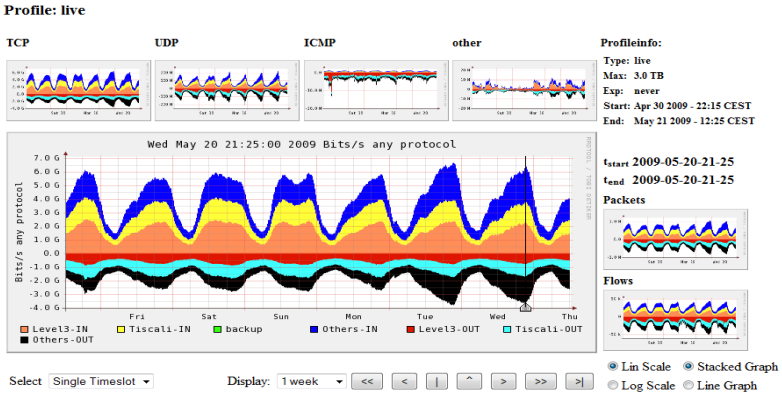
- Kompletní řešení pro monitorování sítí na základě IP toků
- Poskytuje informace kdo, s kým, jak dlouho, jakým protokolem komunikoval a kolik přenesl dat
- Zaměření na poměr cena/výkon a přínos pro uživatele
- Řešení pro sítě všech velikostí, technologie vytvořená v ČR

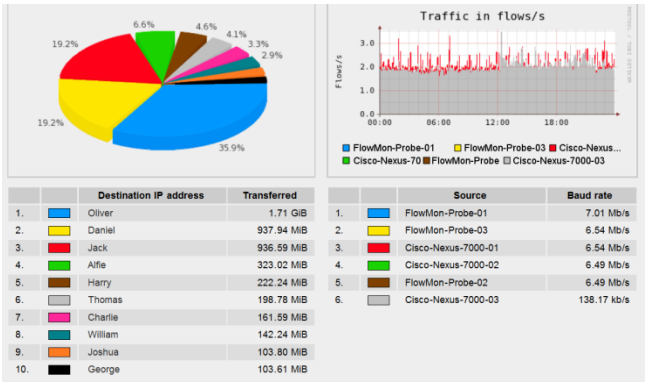


FlowMon Analýza & Reporting

- Grafy, tabulky, TOP N statistiky, formuláře
- Dynamické alerty
- Uživatelské pohledy

- Online&offline statistiky
- HTML, PDF, CSV export
- Administrátorské i manažerské reporty

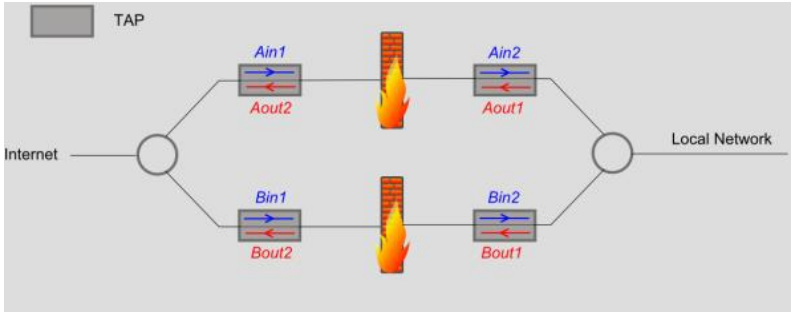


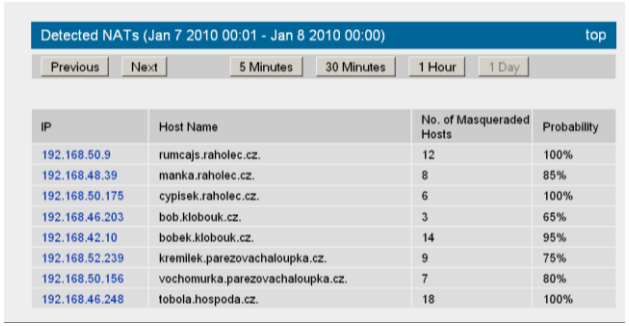


FlowMon FW auditor & NAT Detectiv

- Analýza a konfigurace firewallů
- Auditování

- Detekce NATů
- Odhalení nežádoucích wifi hotspotů





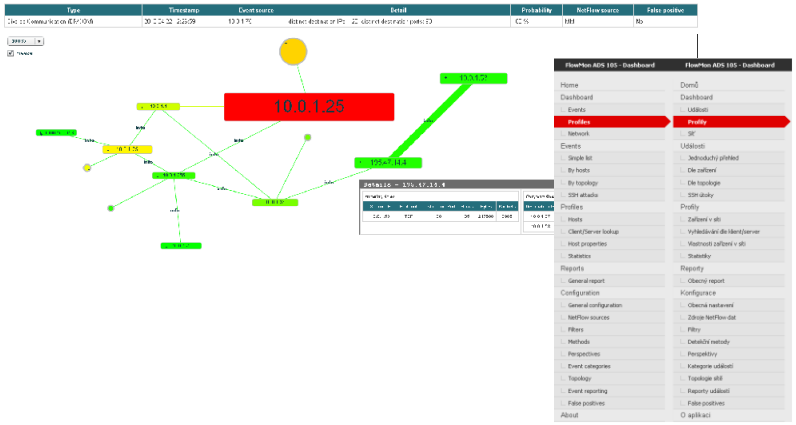
Detected NATs (Jan 7 2010 00:01 - Jan 8 2010 00:00) top

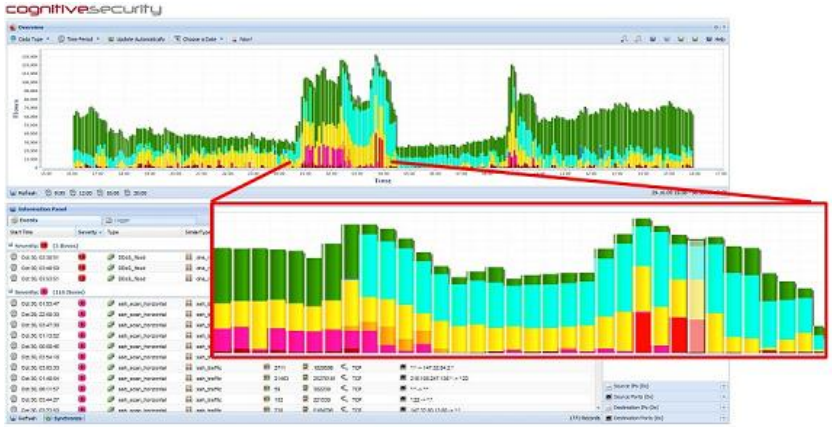
Previous | Next | 5 Minutes | 30 Minutes | 1 Hour | 1 Day

IP	Host Name	No. of Masqueraded Hosts	Probability
192.168.50.9	rumcajs.raholec.cz.	12	100%
192.168.48.39	manka.raholec.cz.	8	85%
192.168.50.175	cypisek.raholec.cz.	6	100%
192.168.46.203	bob.klobouk.cz.	3	65%
192.168.42.10	bobek.klobouk.cz.	14	95%
192.168.52.239	kremilek.parezovachaloupka.cz.	9	75%
192.168.50.156	vochomurka.parezovachaloupka.cz.	7	80%
192.168.46.248	tobola.hospoda.cz.	18	100%

FlowMon NBA

- Detekce anomálií a behaviorální analýza
- Upozornění na změny chování stanic a zařízení
- Detekce červů, virů, botnetů, skenů
- Odhalení slovníkových útoků a útoků na služby



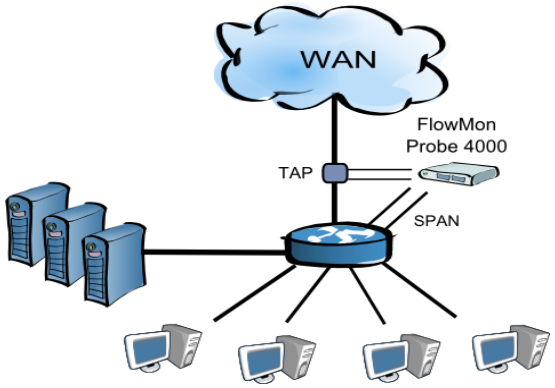


Případová studie – Aegon, SK

- O společnosti AEGON
  - jedna z největších světových společností v oblasti životního a penzijního pojištění, jejíž kořeny sahají do roku 1759
  - více než 40 milionů klientů na celém světě
  - svěřeno více než 368 miliard euro
- Požadavky IT oddělení
  - kompletní monitorování ředitelství SK (síť se stovkami PC), WAN linek na místní pobočky a zahraniční konektivity do centrály
  - splnění legislativních norem a požadavku externího auditora na monitoring datových komunikací
  - zvýšení bezpečnosti počítačové sítě
  - kontrola přístupu k datovým zdrojům
  - efektivnější správa sítě a zjišťování chybných konfigurací
  - dohledový systém pro správu síťových zařízení

Případová studie – Aegon, SK

- Řešení
  - nasazena 4-portová sonda FlowMon
  - monitorována LAN, DMZ, připojení do Internetu a připojení místních poboček
  - plugin Zabbix pro dohled serverů a služeb
  - plugin FlowMon Reporter pro automatickou tvorbu reportů



- Vyjádření ředitele IT pana Štěrbáka

„Projekt nasazení řešení FlowMon se podařil realizovat ve velmi krátké době a díky němu nyní nejenom splňujeme bezpečnostní legislativní požadavky na monitoring sítě, ale také jsme výrazně zrychlili a zefektivnili správu naší sítě. V každém okamžiku víme, co se v naší síti děje a můžeme na danou situaci ihned reagovat.“

Případová studie – Masarykova Un.

- Masarykova univerzita
  - druhá největší univerzita v České republice
  - 9 fakult s více než 200 katedrami, ústavy a klinikami
  - 44370 studentů v řádném studiu

- Požadavky bezpečnostního oddělení
  - Nástroj pro efektivní práci CSIRT-MU týmu
  - Sledování dodržování bezpečnostních politik
  - Dohledávání bezpečnostních incidentů
  - Detekce virů a červů v síti MU
  - Monitorování a detekce slovníkových útoků na SSH
  - Monitorování e-mailového provozu (SPAM)
  - Monitorování provozu přicházejícího na honeypoty
- Další využití na MU
  - monitorování přístupů k elektronickým zdrojům
  - podpora pro výzkum a vývoj v oblasti počítačových sítí

Případová studie – Masarykova Un.

- Příklady využití
  - Každý stroj v síti MU musí mít reverzní DNS záznam
  - Mail ze sítě MU lze odeslat jen přes vybrané SMTP servery
  - Automatické hledání zavirovaných počítačů a report jeho majiteli, pokud není problém vyřešen, je počítač odpojen od sítě

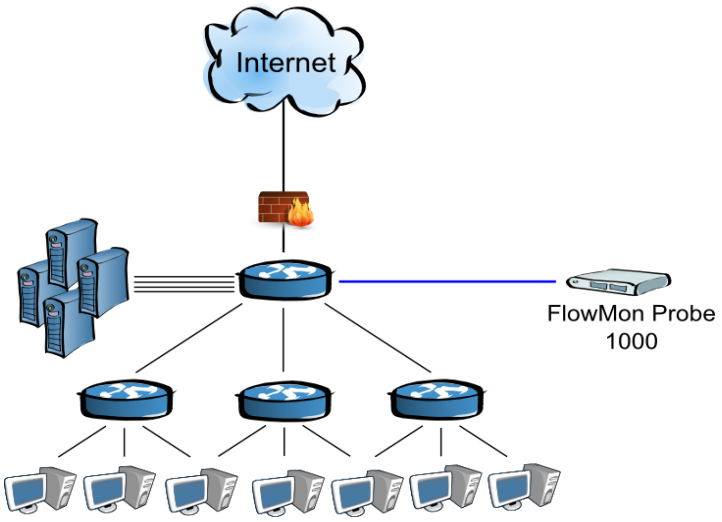
- Zkušenosti se systémem, vedoucí CSIRT-MU, RNDr. Jan Vykopal
  - NetFlow data získaná FlowMon sondami a jejich následné zpracování se staly základním kamenem síťové bezpečnosti na MU
  - Objeven nový botnet, nalezeny nové, dosud neznámé formy virů
  - automatizované upozorňování šetří čas bezpečnostním analytikům
  - Nad technologií NetFlow je realizován další výzkum
  - Kladná odezva správců
  - Chladnější odezva studentů, ale čistší síť
  - Výrazné zvýšení bezpečnosti sítě

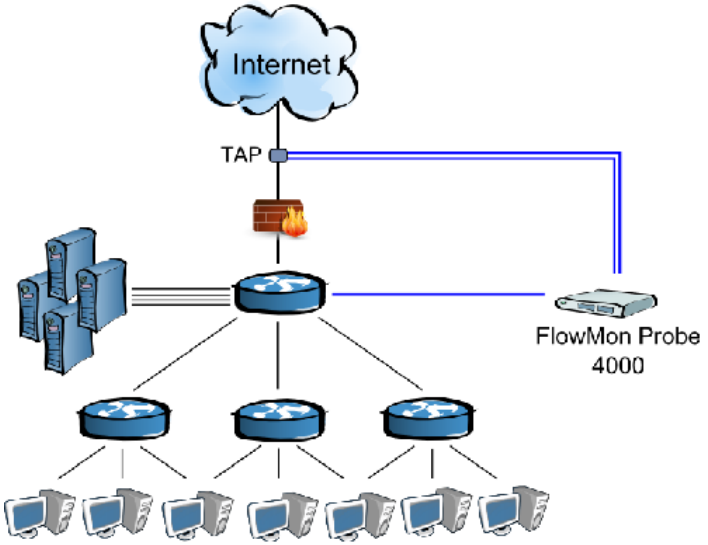
Případová studie – Masarykova Un.

- Botnet Chuck Norris
  - Napadá ADSL modemy, WIFI routery, satelitní přijímače (linux)
  - Napadená zařízení šíří nákazu - skenování portů (telnet), slovníkové útoky – jen 15 hesel a připojují se k centrálnímu serveru, jenž jim udílí příkazy (IRC)
  - Uživatel neví, že se podílí na nelegální činnosti
  - Nelze detekovat standardními ANTI řešeními
  - Možnost manipulace s veškerým provozem do/z napadené sítě
- Odhalení botnetu
  - Pomocí řešení FlowMon odhaleny opakované pokusy o komunikace na telnetu
  - Zpětné trasování, analýza činnosti, připojení na řídící server
  - Ohlášení botnetu CSIRTem MU
  - Dočasné odpojení botnetu, nyní botnet opět aktivní
  - => Je potřeba se účinně bránit (bezpečnostní zásady, hesla, NBA)

Typické projekty

- Flow monitoring a NBA nejsou drahé technologie a jsou dostupné pro většinu organizací
- Příklady nasazení:
  - FlowMon sonda pro monitoring vnitřní sítě: 100tis Kč
  - FlowMon sonda pro monitoring LAN, WAN, Internet: 200tis Kč
  - Rozšiřující modul NBA pro detekci anomálií: 200tis Kč
  - Rozšiřující modul pro pokročilý reporting: 50tis Kč





Klíčové přínosy

- Monitoring datových toků v sítí
  - Přehled o síťových komunikacích: Internet, WAN a LAN
  - Audity a prokazování bezpečnostních incidentů
  - Optimalizace infrastruktury (náklady na konektivitu, „pomalá síť“)
  - Efektivita zaměstnanců (správců, uživatelů)
- Bezpečnost
  - Detekce anomálií a nežádoucích vzorů chování v síti
  - Zvýšení nejen vnější ale zejména vnitřní bezpečnosti sítě
  - Odhalení specifických hrozeb pro které neexistují signatury
  - Detekce skenování, slovníkových útoků, útoků typu DoS, útoků na aplikační protokoly, P2P aktivit, spamů, virů nebo botnet sítí
  - Budování profilů chování jednotlivých počítačů a detekce změn komunikačních partnerů, objemů provozu či struktury provozu
  - Obrana proti sociálnímu inženýrství a před úniky informací
  - Účinné i pro šifrovaný provoz
  - Network-based řešení – automaticky monitorována každá stanice

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Jiří Tobola
INVEA-TECH
tobola@invea.cz