DATA SYS

Systém řízení bezpečnosti informací v praxi

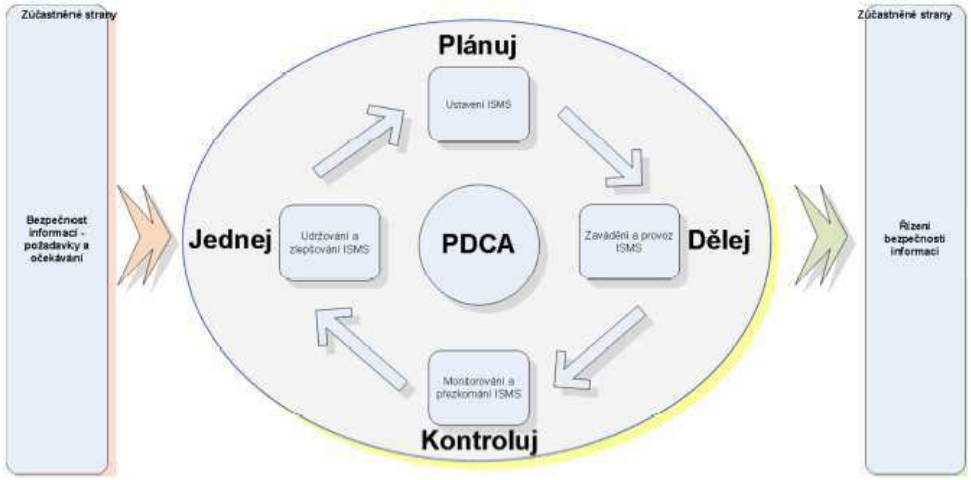
Mgr. Pavel Štros, Ph.D.

Practice Leader pro Bezpečnost&Monitoring

stros@datasys.cz

Systém řízení bezpečnosti informací (ISMS)

- Kybernetická bezpečnost je rozsáhlá disciplína
  - Vyžaduje řízení, systematický přístup
- Norma ČSN **ISO/IEC 27001**
  - Dlouhodobě nejuznávanější mezinárodní norma
  - Definuje doporučené postupy pro ISMS
  - I ZoKB vychází z této normy
    - Certifikací dle ISO/IEC 27001 lze doložit splnění požadavků dle ZoKB



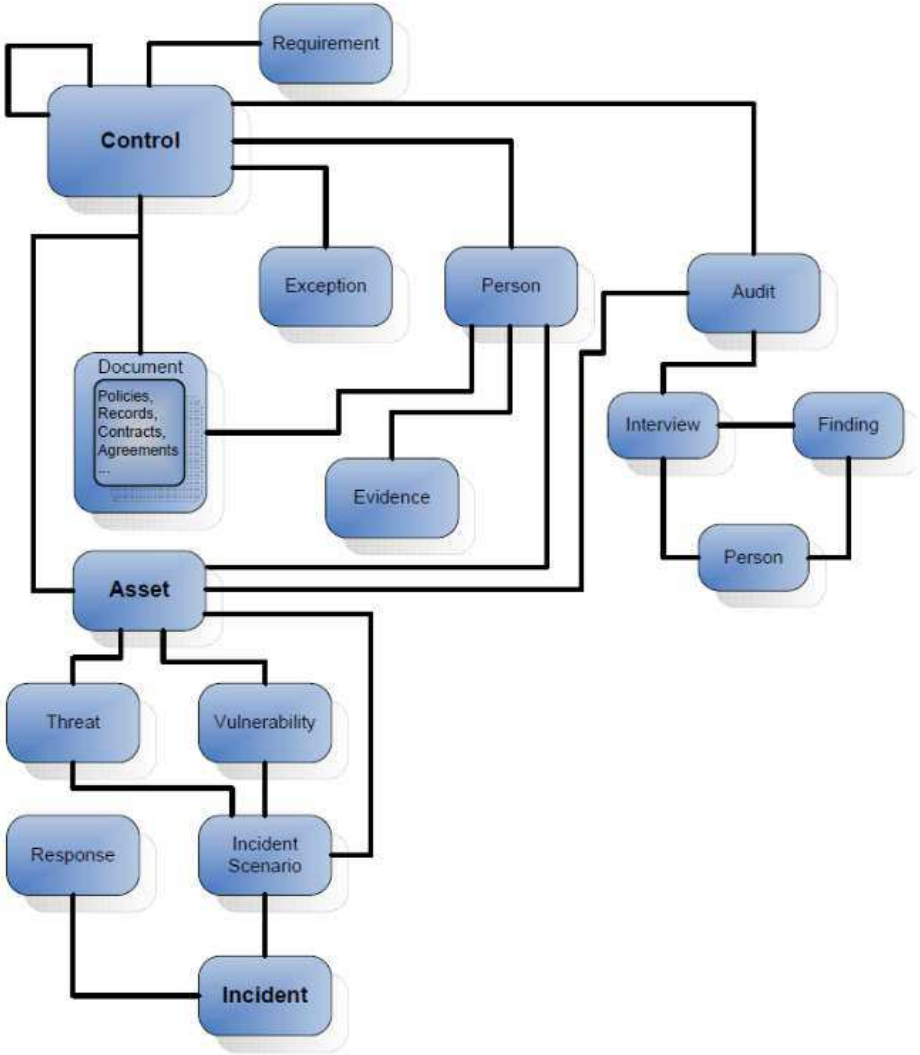
DATA SYS

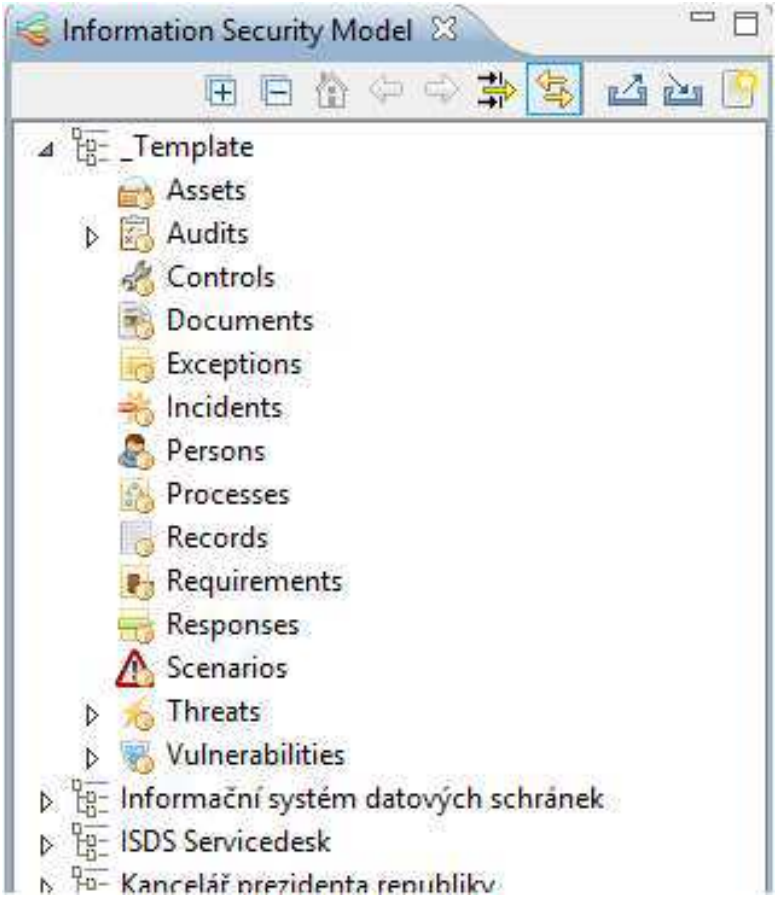
Princip PDCA

- Plánuj (ustavení ISMS)
  - Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a s cíli organizace.
- Dělej (zavádění a provozování ISMS)
  - Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
- Kontroluj (monitorování a přezkoumání ISMS)
  - Posouzení a měření výkonu procesu vůči politice a cílům ISMS.
- Jednej (udržování a zlepšování ISMS)
  - Přijetí preventivních opatření a opatření k nápravě, založených na výsledcích interního nebo externího auditu ISMS tak, aby bylo dosaženo neustálého zlepšování ISMS.

DATA SYS

Verinice – podpůrný nástroj pro řízení ISMS

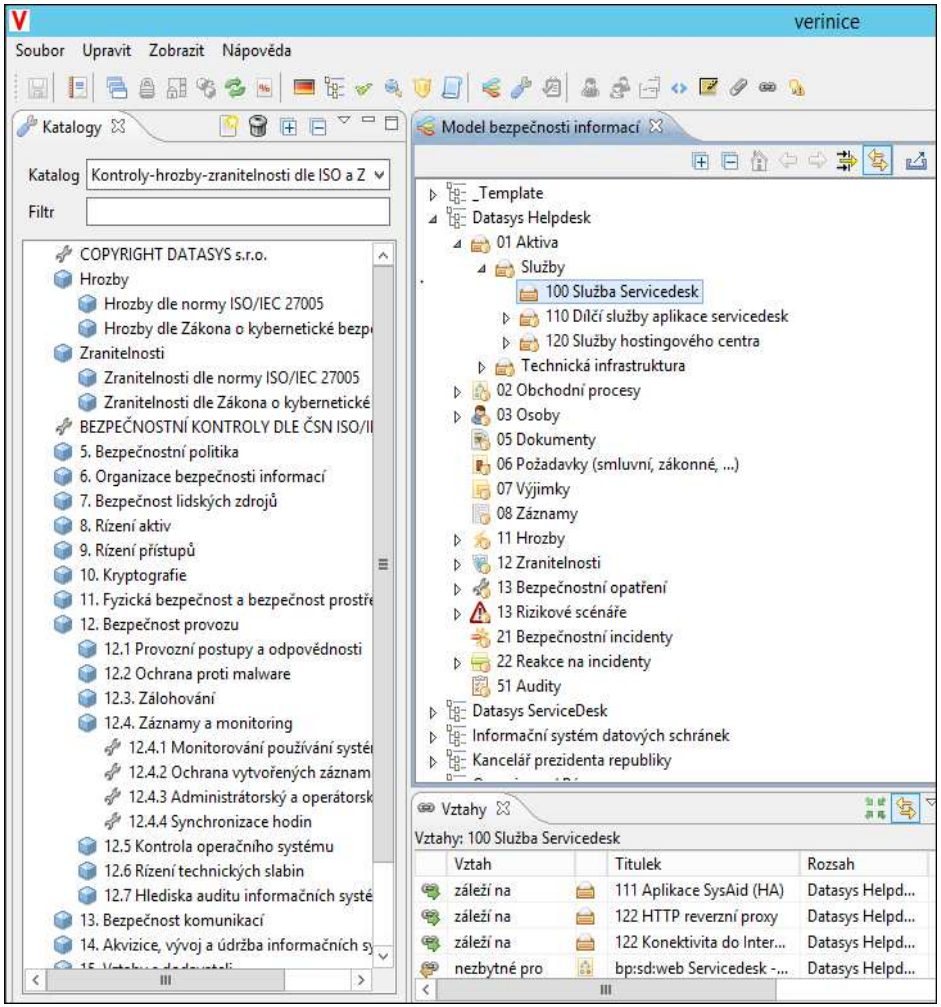




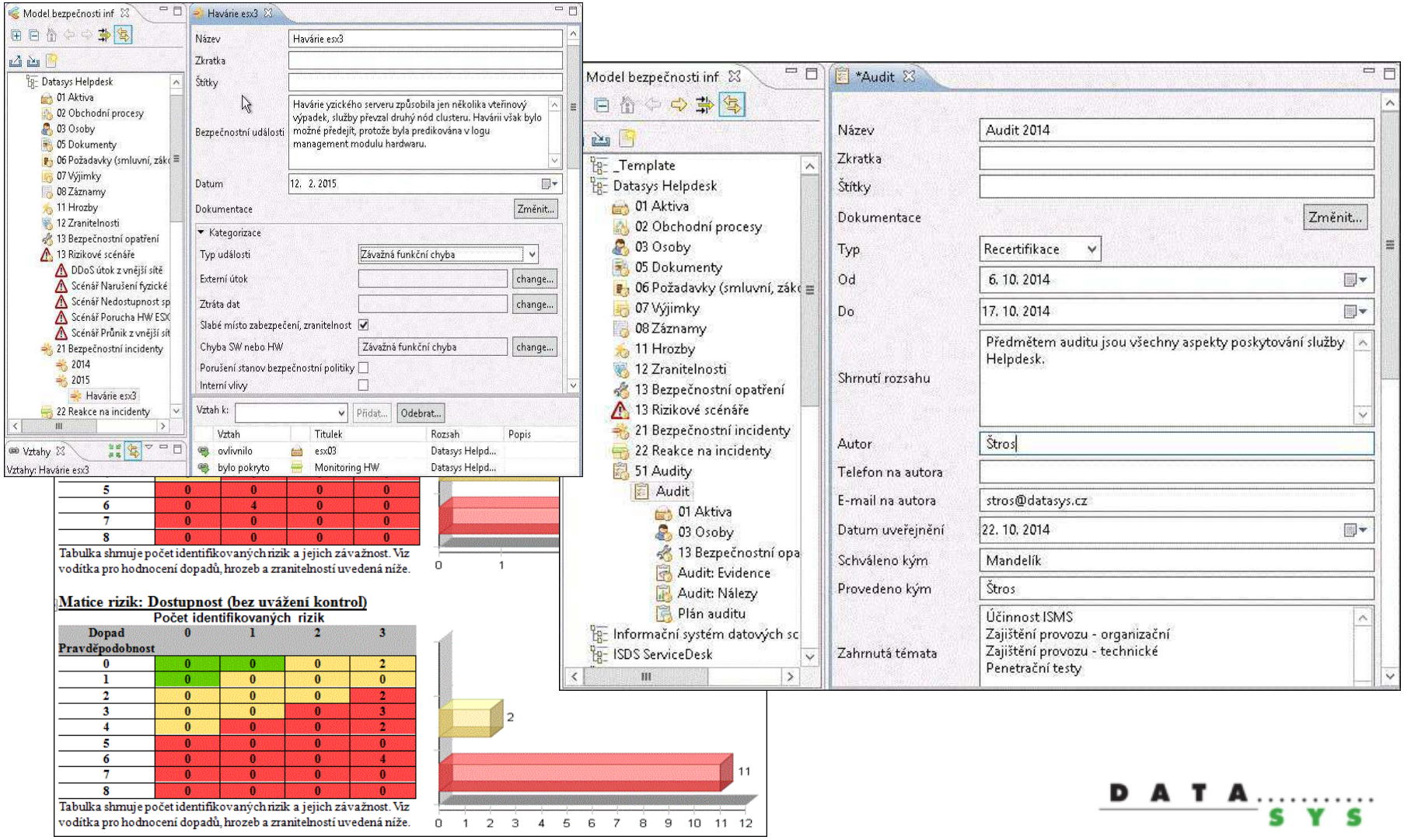
DATA SYS

Verinice a Datasys

- Verinice je svobodný software
- Datasys poskytuje
  - Lokalizované katalogy
    - Hrozeb
    - Zranitelností
    - Bezpečnostních kontrol
  - Lokalizaci softwaru
  - Školení personálu
    - Principy ISMS (jednodenní)
    - Užívání Verinice (jednodenní)
  - Konzultační a analytické práce



Verinice – ISMS velmi pěkně a hezky česky



Hlavní požadavky ZoKB - organizační

- Hlavní požadavky ZoKB
  - Organizační opatření
    - Stanovuje minimální požadavky na pracovní role pro řízení bezpečnosti
      - Pro KII požaduje kompletní ISMS
    - Provedení analýzy rizik
      - V přílohách vyhlášky taxativně určuje kritéria pro hodnocení aktiv, hrozeb a zranitelností
      - Pro KII požadována analýza i pro podpůrná aktiva
  - Bezpečnostní dokumentace
    - Stanovuje minimální požadovanou strukturu bezpečnostní dokumentace
      - Pro KII je sada požadované dokumentace širší (ISMS)

DATA SYS

Hlavní požadavky ZoKB - technické

- Technická opatření
  - Sběr kybernetických bezpečnostních událostí (bezp. relevantních logů)
    - Taxativně určuje, jaké kategorie událostí sbírat
    - Požadavek na **centrální log management**
  - Automatizované vyhodnocování kybernetických bezpečnostních událostí
    - Pro VIS dle požadavků analýzy rizik
    - Pro KII povinně
      - Požadavek na **SIEM**
  - Detekce škodlivých programových kódů
    - Antiviry+
    - Jsme připraveni nabídnout kvalitu (Symantec, McAfee)
      - Pokročilá heuristika (dynamická a statická analýza v sandboxu)
      - Globální hodnocení reputace souborů

DATA SYS

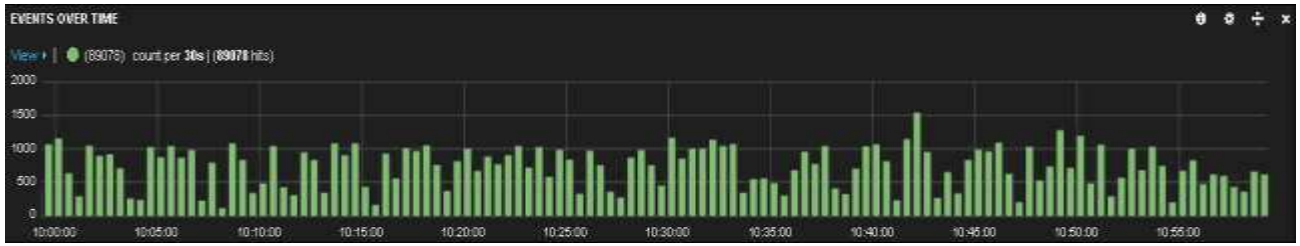
DATASYS - služby poskytované zákazníkům

- Organizační opatření
  - Analýza požadavků na **dosažení souladu se ZoKB**
  - Prosazení požadavků na dosažení souladu se ZoKB, zejména
    - **Provedení analýzy rizik** (umíme to udělat levně)
      - metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik
      - zpráva o hodnocení rizik
      - prohlášení o aplikovatelnosti
      - plán zvládání rizik
    - Sestavení požadované **bezpečnostní dokumentace**
      - bezpečnostní politika
      - plán rozvoje bezpečnostního povědomí
      - zvládání kybernetických bezpečnostních incidentů
      - strategii řízení kontinuity činností
      - přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

DATA SYS

DATASYS - služby poskytované zákazníkům

- Technická opatření
  - Implementace LM/SIEM systému
    - Služby (pre-sales)
      - **Praktické srovnání mnoha LM/SIEM systémů** běžně dostupných na českém trhu
        - Námi provedená komparativní studie (srovnávací tabulka)
        - Praktické předvedení v našem LABu
    - Produkty
      - Máme **vlastní levné řešení ELISA** (GPL) + **OSSIM**
      - **McAfee SIEM** – špička, pro náročné zákazníky
      - **IBM QRadar** – kvalitní, výhodnější v některých prostředích



DATASYS

Na vědomost se dává …

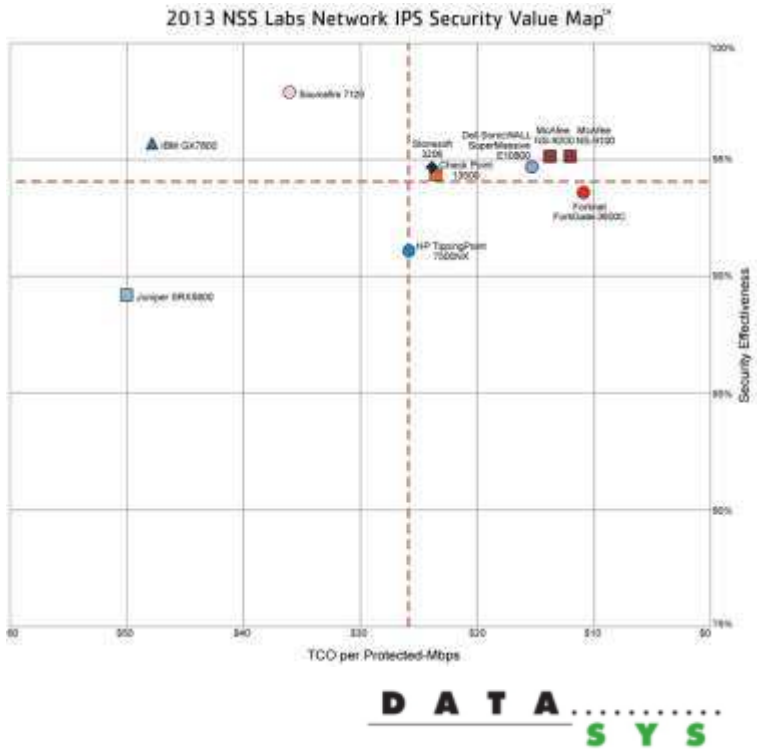
- Nástroje nejsou samospasitelné (žádné překvapení :-)
  - klíčové jsou postupy jejich nasazení a užívání,
    - pak mají významný přínos nejen pro bezpečnost, ale i pro provoz.

- Naše zkušenost:
  - nástroje pro zaznamenávání činnosti uživatelů a administrátorů
    - obvykle vystačíte s běžnými funkcionalitami existujících komponent technické infrastruktury IS, stačí je (řízeně) aktivovat
      - audit na úrovni OS, databází a aplikací, které to podporují,
    - někdy je lepší monitorovat z vnějšku,
      - zejména auditování v DB dokáže pěkně srazit výkon.

DATA SYS

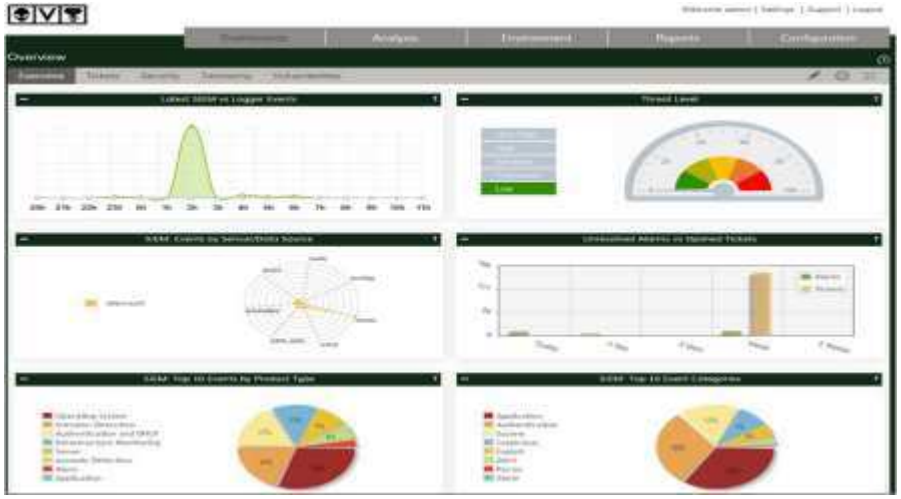
… detekci nelze kvalitně řešit „levně“ …

- Naše zkušenost:
  - vybírejte špičkové **nástroje pro detekci** , které se hodí do vašeho prostředí
    - je tedy nutné investovat i do procedury jejich výběru,
    - antiviry (next gen), IDS/IPS systémy,
    - UTM firewally, detektory DDoS, apod.



… sběr a vyhodnocování lze řešit „levně“ …

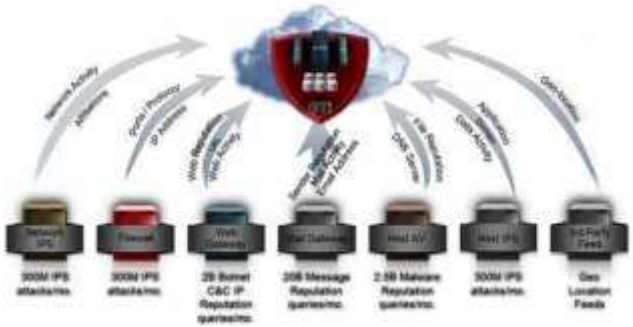
- Naše zkušenost:
  - dnes existují velmi kvalitní „svobodné“ **nástroje pro sběr a vyhodnocení** kybernetických bezp. událostí,
    - stačí vědět, jak je používat,
      - (my jsme do toho investovali),
    - pořizovací náklady jsou nízké,
    - náklady na implementaci a provoz jsou plně srovnatelné s komerčními produkty.



DATA SYS

… nebo i špičkovým integrovaným řešením …

- Naše zkušenost:
  - špičkové **nástroje pro sběr a vyhodnocení** kybernetických bezpečnostních událostí přímo integrují špičkové nástroje pro detekci.



intel Security

DATA SYS

Shrnutí DATASYS nabídky – doporučujeme

Typ nástroje	VIS	KII
Nástroj pro řízení ISMS	Verinice * • Desktopová verze • Dostačuje pro práci s primárními aktivy	Verinice.PRO + Greenbone GSM • Síťová instalace s více uživateli • Rozkrývání podpůrných aktiv • Skenování zranitelností
Log management/SIEM	Datasys ELISA + OSSIM*	McAfee SIEM
Silná autentizace uživatelů	RCDevs OpenOTP *	RCDevs OpenOTP*
Řízení privileg. přístupu	RDP/SSH brána (audit) * • Záznam relací	Agent (audit, analýza, restrikce) • Záznam relací (ObserveIT) • Řízení přístupu ke sdíleným účtům (Dell, IBM)

* nízkonákladová řešení

DATA SYS

Děkuji
za pozornost

Mgr. Pavel Štros, Ph.D.

Practice Leader pro Monitoring&Bezpečnost

stros@datasys.cz