



# System řízení bezpečnosti informací v praxi

Mgr. Pavel Štros, Ph.D.

*Practice Leader pro Bezpečnost&Monitoring*

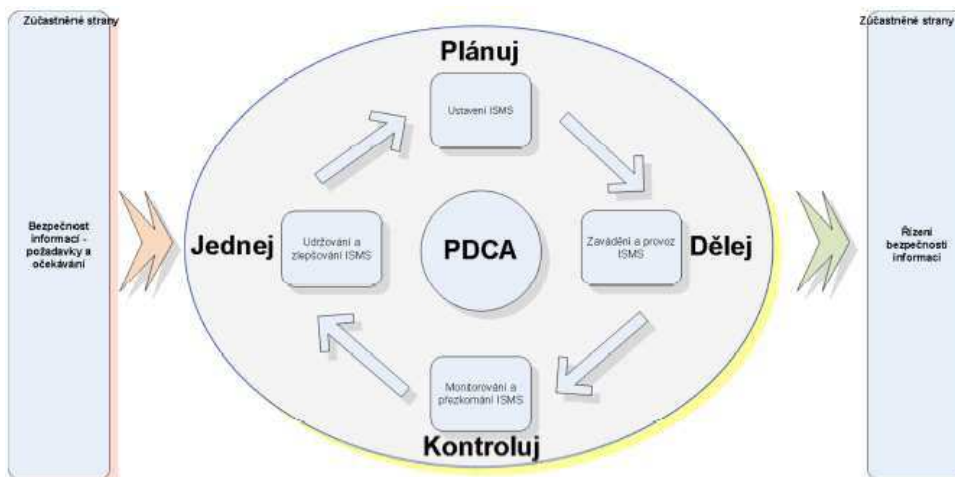
✉ [stros@datasys.cz](mailto:stros@datasys.cz)

DATASYS s.r.o. - všechna práva vyhrazena

Obsah prezentace je chráněn autorským zákonem a jakékoliv jeho šíření, kopírování,  
a to celku i jakékoliv jeho částí, je bez předchozího souhlasu výslovně zakázáno.

# System řízení bezpečnosti informací (ISMS)

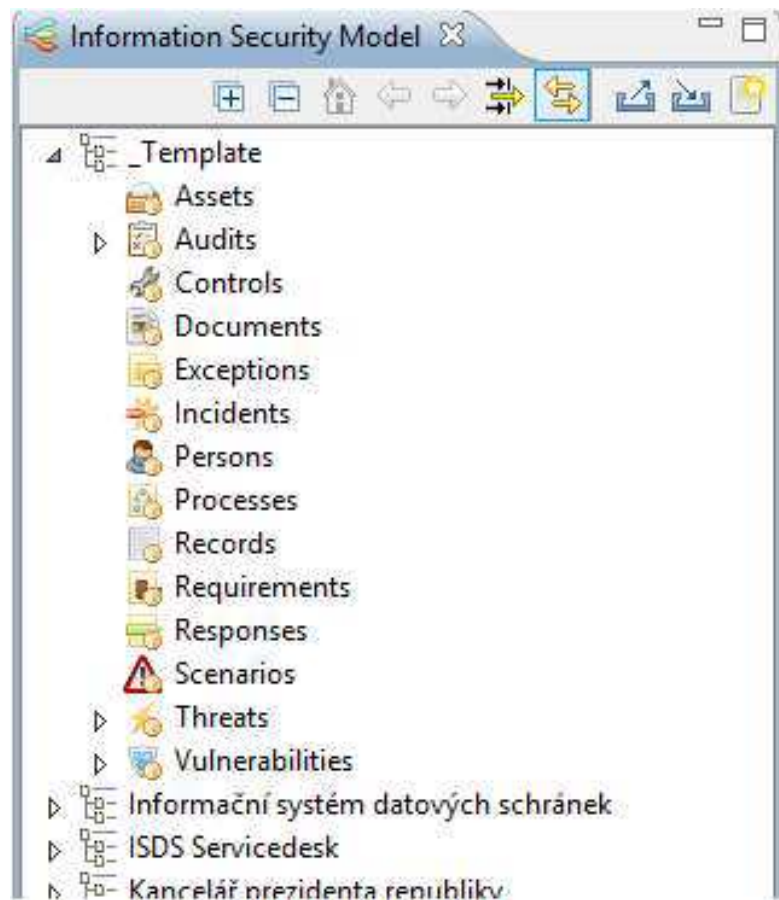
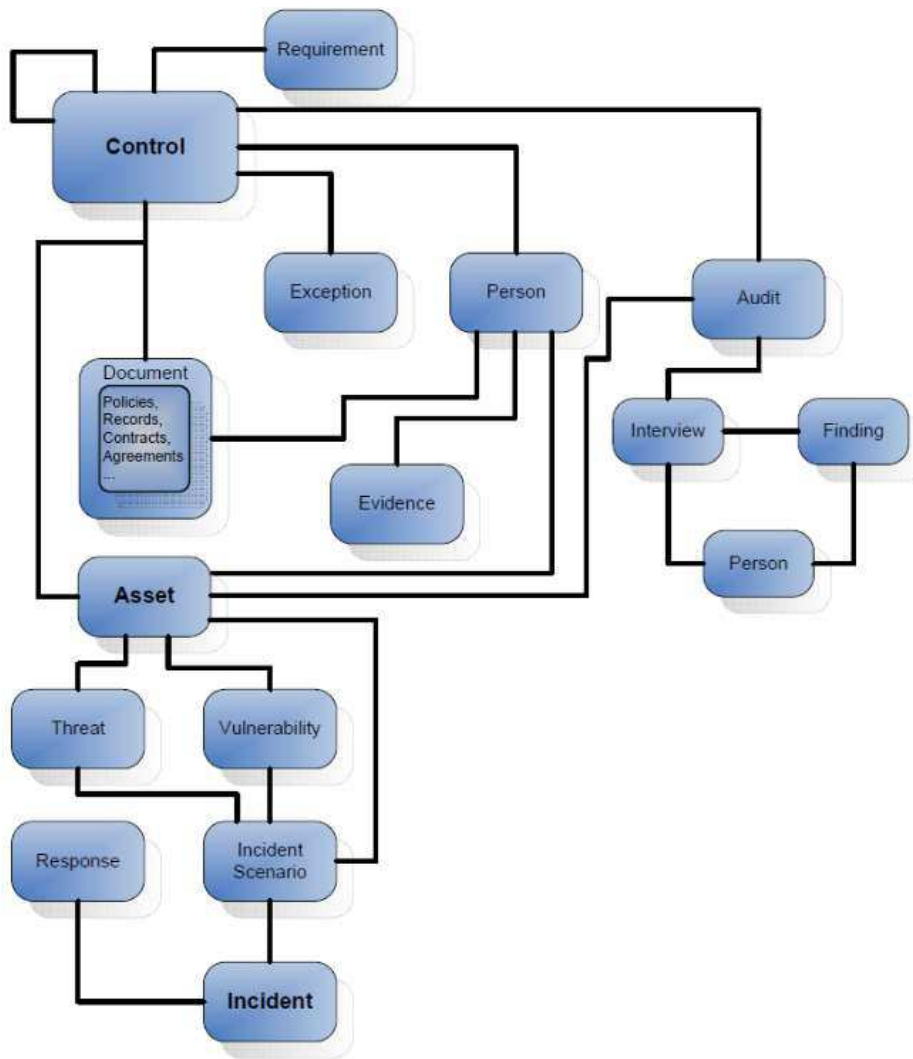
- Kybernetická bezpečnost je rozsáhlá disciplína
  - Vyžaduje řízení, systematický přístup
- Norma ČSN ISO/IEC 27001
  - Dlouhodobě nejuznávanější mezinárodní norma
  - Definiuje doporučené postupy pro ISMS
  - I ZoKB vychází z této normy
    - Certifikací dle ISO/IEC 27001 lze doložit splnění požadavků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



# 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.

# Verinice – podpůrný nástroj pro řízení ISMS



# 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

The screenshot displays the Verinice software interface. The main window is titled 'verinice' and features a menu bar with 'Soubor', 'Upravit', 'Zobrazit', and 'Nápověda'. Below the menu is a toolbar with various icons. The interface is divided into several panes:

- Katalogy:** A pane on the left showing a tree view of catalogs. The selected catalog is 'Kontroly-hrozby-zranitelnosti dle ISO a Z'. The tree structure includes:
  - COPYRIGHT DATASYS s.r.o.
  - Hrozby
    - Hrozby dle normy ISO/IEC 27005
    - Hrozby dle Zákona o kybernetické bezpečnosti
  - Zranitelnosti
    - Zranitelnosti dle normy ISO/IEC 27005
    - Zranitelnosti dle Zákona o kybernetické bezpečnosti
  - BEZPEČNOSTNÍ KONTROLY DLE ČSN ISO/IEC 27005
    - 5. Bezpečnostní politika
    - 6. Organizace bezpečnosti informací
    - 7. Bezpečnost lidských zdrojů
    - 8. Řízení aktiv
    - 9. Řízení přístupů
    - 10. Kryptografie
    - 11. Fyzická bezpečnost a bezpečnost prostředí
    - 12. Bezpečnost provozu
      - 12.1 Provozní postupy a odpovědnosti
      - 12.2 Ochrana proti malware
      - 12.3 Zálohování
      - 12.4 Záznamy a monitoring
        - 12.4.1 Monitorování používání systémů
        - 12.4.2 Ochrana vytvořených záznamů
        - 12.4.3 Administrátorský a operátorský přístup
        - 12.4.4 Synchronizace hodin
      - 12.5 Kontrola operačního systému
      - 12.6 Řízení technických slabín
      - 12.7 Hlediska auditu informačních systémů
    - 13. Bezpečnost komunikací
    - 14. Akvizice, vývoj a údržba informačních systémů
    - 15. Vztahy s datovými partnery

- Model bezpečnosti informací:** A pane on the right showing a tree view of the information security model. The selected node is '100 Služba Servicedesk'. The tree structure includes:
- \_Template
- Datasys Helpdesk
  - 01 Aktiva
    - Služby
      - 110 Dílčí služby aplikace servicedesk
      - 120 Služby hostingového centra
    - Technická infrastruktura
  - 02 Obchodní procesy
  - 03 Osoby
  - 05 Dokumenty
  - 06 Požadavky (smluvní, zákonné, ...)
  - 07 Výjimky
  - 08 Záznamy
  - 11 Hrozby
  - 12 Zranitelnosti
  - 13 Bezpečnostní opatření
  - 13 Rizikové scénáře
  - 21 Bezpečnostní incidenty
  - 22 Reakce na incidenty
  - 51 Audity
- Datasys ServiceDesk
- Informační systém datových schránek
- Kancelář prezidenta republiky
- Vztahy:** A pane at the bottom showing a table of relationships for '100 Služba Servicedesk'. The table has columns for 'Vztah', 'Titulek', and 'Rozsah'.

Vztah	Titulek	Rozsah
záleží na	111 Aplikace SysAid (HA)	Datasys Helpd...
záleží na	122 HTTP reverzní proxy	Datasys Helpd...
záleží na	122 Konektivita do Inter...	Datasys Helpd...
nezbytné pro	bp:sd:web Servicedesk - ...	Datasys Helpd...

# Verinice – ISMS velmi pěkně a hezky česky

Model bezpečnosti inf. > Havárie esx3

Název: Havárie esx3

Zkratka:

Štítky:

Bezpečnostní události: Havárie fyzického serveru způsobila jen několika vteřinový výpadek, služby převzal druhý nód clusteru. Havárii však bylo možné předejít, protože byla predikována v logu management modulu hardware.

Datum: 12. 2. 2015

Dokumentace:

Kategorizace

Typ události:

Externí útok:

Ztráta dat:

Slabé místo zabezpečení, zranitelnost:

Chyba SW nebo HW:

Porušení stanov bezpečnostní politiky:

Interní vlivy:

Vztah k:

Vztah	Titulek	Rozsah	Popis
<input checked="" type="checkbox"/>	ovlivnilo	esx03	Datasy Helpd...
<input checked="" type="checkbox"/>	bylo pokryto	Monitoring HW	Datasy Helpd...

Model bezpečnosti inf. > \*Audit

Název: Audit 2014

Zkratka:

Štítky:

Dokumentace:

Typ:

Od:

Do:

Shmutí rozsahu:

Autor:

Telefon na autora:

E-mail na autora:

Datum uveřejnění:

Schváleno kým:

Provedeno kým:

Zahnutá témata:

Informační systém datových sc  
ISDS ServiceDesk

5	0	0	0	0
6	0	4	0	0
7	0	0	0	0
8	0	0	0	0

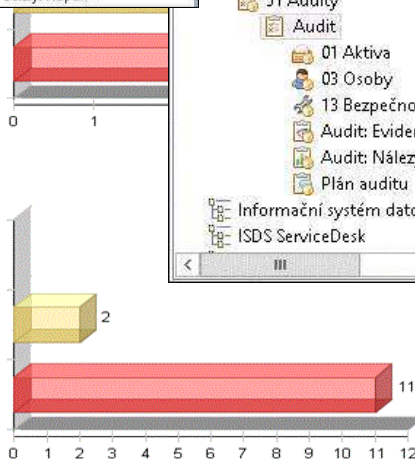
Tabulka shrnuje počet identifikovaných rizik a jejich závažnost. Viz vodítka pro hodnocení dopadů, hrozeb a zranitelnosti uvedená níže.

### Maticе rizik: Dostupnost (bez uvážení kontrol)

Počet identifikovaných rizik

Dopad	0	1	2	3
0	0	0	0	2
1	0	0	0	0
2	0	0	0	2
3	0	0	0	3
4	0	0	0	2
5	0	0	0	0
6	0	0	0	4
7	0	0	0	0
8	0	0	0	0

Tabulka shrnuje počet identifikovaných rizik a jejich závažnost. Viz vodítka pro hodnocení dopadů, hrozeb a zranitelnosti uvedená níže.



# 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)

# 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

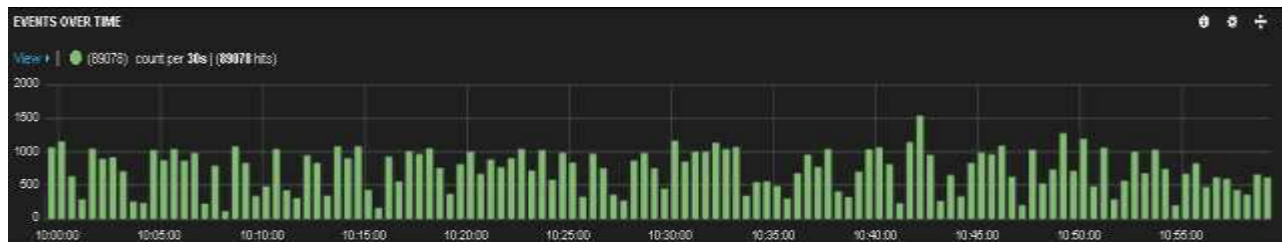


# DATASYS - služby poskytované zákazníkům

- 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 zvládnutí rizik
    - Sestavení požadované **bezpečnostní dokumentace**
      - bezpečnostní politika
      - plán rozvoje bezpečnostního povědomí
      - zvládnutí kybernetických bezpečnostních incidentů
      - strategii řízení kontinuity činností
      - přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

# 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

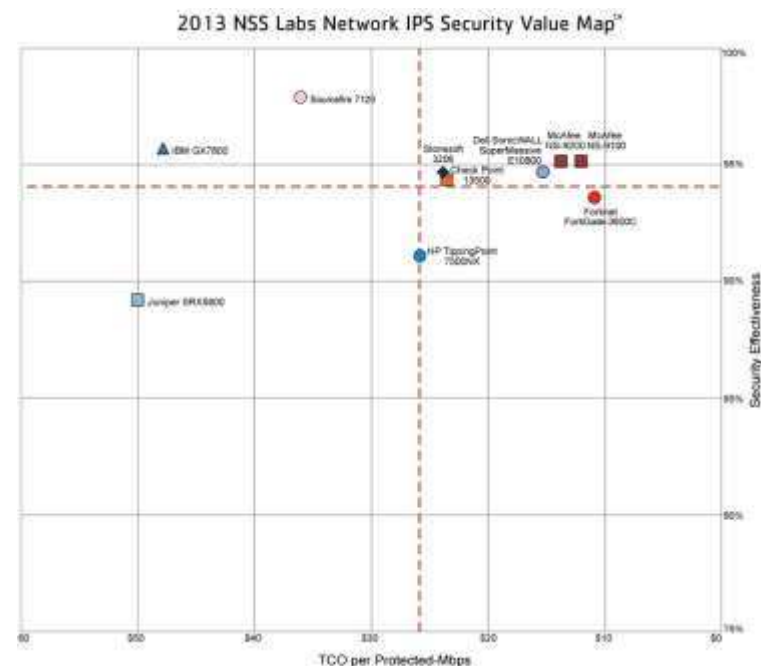


# Na vědomost se dává ...

- 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.

# ... 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.

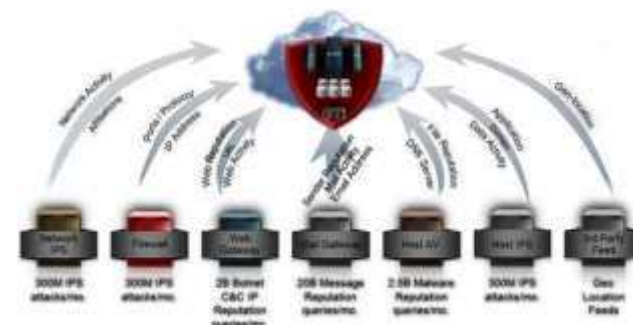


Figure 1. Magic Quadrant for Security Information and Event Management



# ... nebo i špičkovým integrovaným řešením ...

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



# Shrnutí DATASYS nabídky – doporučujeme

Typ nástroje	VIS	KII
Nástroj pro řízení ISMS	<b>Verinice *</b> <ul style="list-style-type: none"><li>• Desktopová verze</li><li>• Dostačuje pro práci s primárními aktivy</li></ul>	Verinice.PRO + Greenbone GSM <ul style="list-style-type: none"><li>• Síťová instalace s více uživateli</li><li>• Rozkrývání podpůrných aktiv</li><li>• Skenování zranitelností</li></ul>
Log management/SIEM	<b>Datasys ELISA + OSSIM*</b>	McAfee SIEM
Silná autentizace uživatelů	<b>RCDevs OpenOTP *</b>	<b>RCDevs OpenOTP*</b>
Řízení privileg. přístupu	<b>RDP/SSH brána (audit) *</b> <ul style="list-style-type: none"><li>• Záznam relací</li></ul>	Agent (audit, analýza, restrikce) <ul style="list-style-type: none"><li>• Záznam relací (ObserveIT)</li><li>• Řízení přístupu ke sdíleným účtům (Dell, IBM)</li></ul>

\* nízkonákladová řešení

Děkuji  
za pozornost

Mgr. Pavel Štros, Ph.D.

*Practice Leader pro Monitoring&Bezpečnost*



stros@datasys.cz

**D A T A** .....  
**S Y S**

DATASYS s.r.o. - všechna práva vyhrazena

Obsah prezentace je chráněn autorským zákonem a jakékoliv jeho šíření, kopírování,  
a to celku i jakékoliv jeho částí, je bez předchozího souhlasu výslovně zakázáno.