



## Multidisciplinární bezpečnost

Kybernetická bezpečnost IV, Policejní akademie Praha

Adrian Demeter, Deloitte, 14.09.2016





# Government's cyber challenge

Protecting sensitive data for the public good

**Deloitte**  
University Press

<http://dupress.com/articles/protecting-sensitive-data-government-cybersecurity/>



# Mluví se už o tématu ve světě?

**Google Search Results for 'Multidisciplinary Security':**

- CIA Security Professional Jobs, Degrees and Training Requirements**  
[www.ciaagentedu.org/security-professional/](https://www.ciaagentedu.org/security-professional/)  
How to Become a Security Professional with the Central Intelligence Agency ... The CIA's Multidisciplinary Security Officer occupation is quite extensive, ...
- Security Professional — Central Intelligence Agency**  
<https://www.cia.gov/careers/opportunities/.../security-professional.html>  
Mar 10, 2009 - The mission of the Central Intelligence Agency (CIA) is to provide national security intelligence to the President of the United States and senior ...  
Salary: \$49,509 – \$100,736\* Location: Washington, DC metropolitan ...  
Work Schedule: Full Time

**NIST Poster: A Multidisciplinary Approach to Building Trustworthy Secure Systems**  
*Protecting the Nation's Critical Assets in the 21st Century*  
Dr. Ron Ross  
Computer Security Division  
Information Technology Laboratory  
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

**Trinity Technology Group Website:**

**Multidisciplinary Security**  
Trinity provides security services to the Federal Bureau of Investigations (FBI), US Army Corps of Engineers (USACE), U.S. Navy, Defense Advanced Research Projects Agency (DARPA), Defense Information Systems Agency (DISA), U.S. Air Force, the Joint Strike Fighter Program Office, National Institute of Health (NIH) and the Transportation Security Administration (TSA). Areas of our multidisciplinary security include:

- Antiterrorism and Force Protection (AT/FP)
- Law Enforcement Support
- Personnel Security
- Planning and Policy Development

**CIA Security Professional Job Description**  
Security professionals within the CIA are exposed to a wide variety of security disciplines, including:

- Personnel security
- Physical security
- Technical security
- Cyber security
- Program security
- Acquisitions security

The CIA's Multidisciplinary Security Officer occupation is quite extensive, encompassing work that involves:

- The collection, analysis and reporting of security or counterintelligence information
- Resource and program management
- Policy
- Liaison with other members of the Intelligence

**CIA Careers List:**

- Analytic Methodologist
- Cartographers and Geographers
- CIA Special Agent
- Core Collector
- Counterintelligence Threat Analyst
- Counterterrorism Analyst
- Economic Analyst

2016

# Mluví se o tématu u nás?

Hledat

Multidisciplinární bezpečnost ... Strategie kybernetické bezpečnosti

www.ictsecurity.cz/security-bezpenost/multidisciplinarni-bezpecnost-v-cloudu.html

CALENDÁŘ AKCÍ

ZÁŘÍ

|    |    |    |    |    |
|----|----|----|----|----|
| PO | ÚT | ST | ČT | PÁ |
|    |    |    | 1  | 2  |
| 5  | 6  | 7  | 8  | 9  |
| 12 | 13 | 14 | 15 | 16 |
| 19 | 20 | 21 | 22 | 23 |
| 26 | 27 | 28 | 29 | 30 |

JOBS IN ICT

MEMOS Software NET  
programátor - MEMOS  
Software s.r.o.

memos

IT Project Manager - Senior -  
redtoo s.r.o.

redtoo

JAVA PROGRAMÁTOR -  
redtoo s.r.o.

redtoo

Java programátor - ICZ a.s.

ICZ

**Multidisciplinární bezpečnost v cloudu. Kde čekat úskalí**  
Pátek, 25 Březen 2016 17:46

**Deloitte** S rozvojem cloudových služeb se stává otázka bezpečnosti infrastruktury stále diskutovanějším tématem.  
*Není divu, jakkoli jde stále o IT architekturu a platí zde základní bezpečnostní pravidla, přece jen má cloud svá specifika. plánování bezpečnostní strategie brát zřetel.*

V případě, že společnost připravuje bezpečnostní strategii pro vnitřní IT infrastrukturu, bývá situace obvykle poměrně jednoduchá. Většinu klíčových síťových prvků má pod kontrolou sama společnost. V případě cloudových služeb je situace složitější. V tomto případě je třeba zvážit bezpečnostní aspekty poskytovatele služeb, který může být v zahraničí a mít jiné právní předpisy.

**Deloitte** „Použití prediktivní a behaviorální analytiky bude nezbytné pro všechny organizace, které čelí významným rizikům kybernetického útoku,“  
**říká Adrian Demeter, Senior Manager společnosti Deloitte**



Obrana proti kybernetickým útokům přestává být úkolem IT oddělení, ale stává se součástí obchodních strategií společností. Firmy si uvědomují, že jsou na informačních technologiích stále závislejší. O tom, jak se mění svět kybernetické bezpečnosti a jaké jsou v této oblasti hlavní trendy si ICT Network News povídal se Senior Manažerem společnosti Deloitte Adrianem Demeterem.

**Deloitte**

Integrovaná multidisciplinární bezpečnost

ISSS 2016

Ing. Adrian Demeter  
05.04.2016



**Strategie kybernetické bezpečnosti je třeba propojit s právem, financemi i dalšími oblastmi**  
Neděle, 17 Leden 2016 00:00

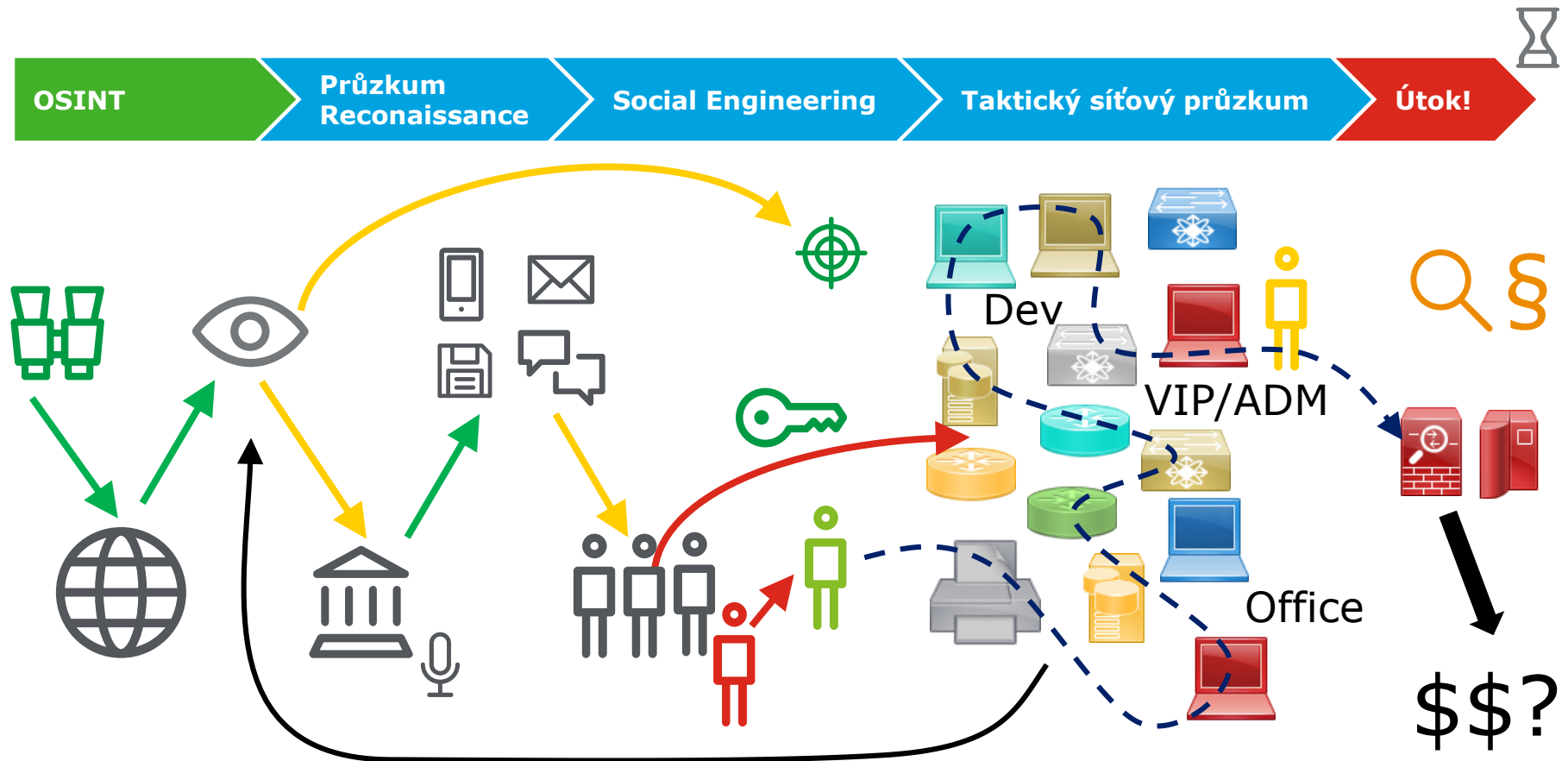


© 2016 Deloitte Česká republika

Multidisciplinární bezpečnost

4

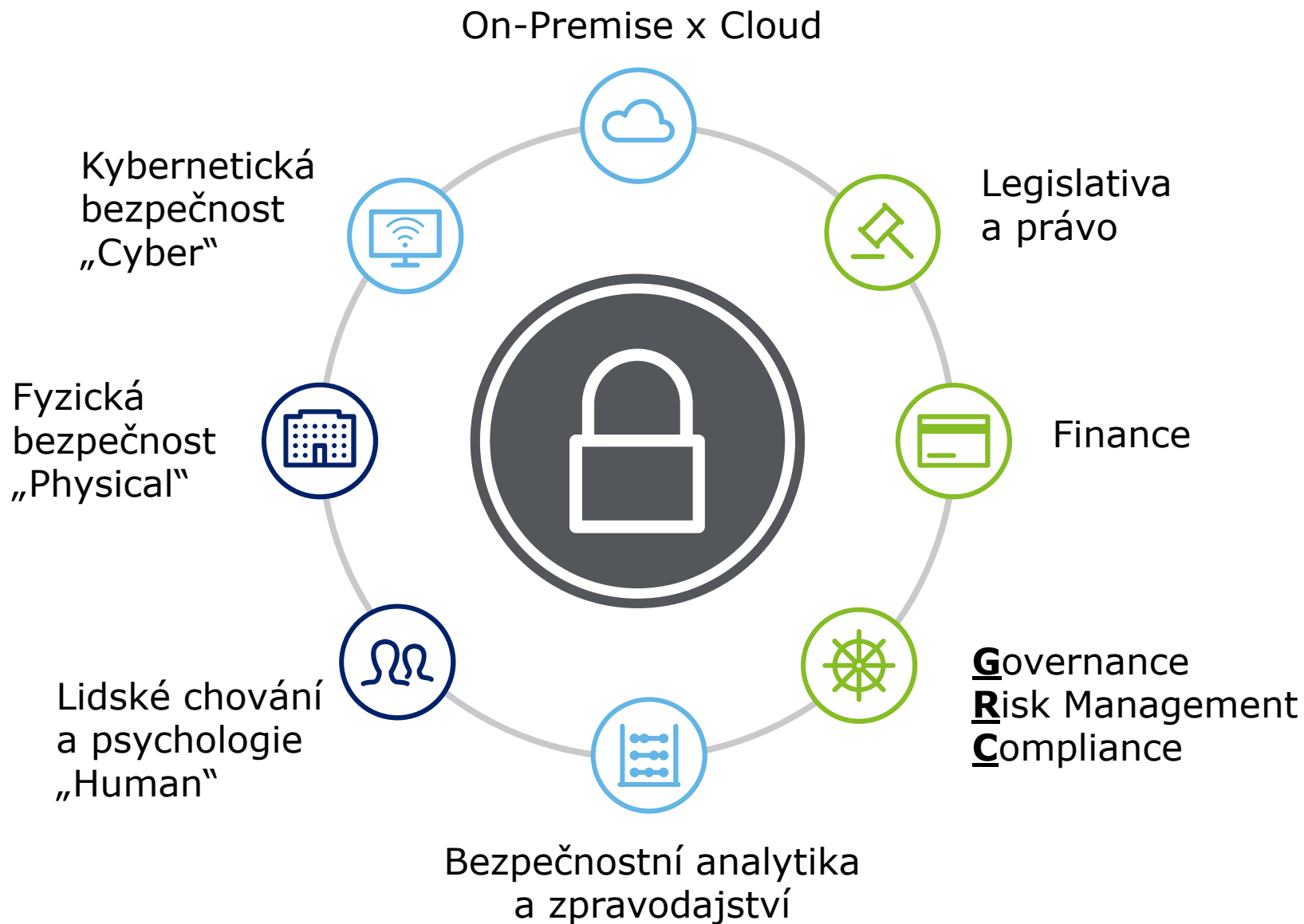
# Proč vlastně potřebujeme multidisciplinární řešení bezpečnosti?



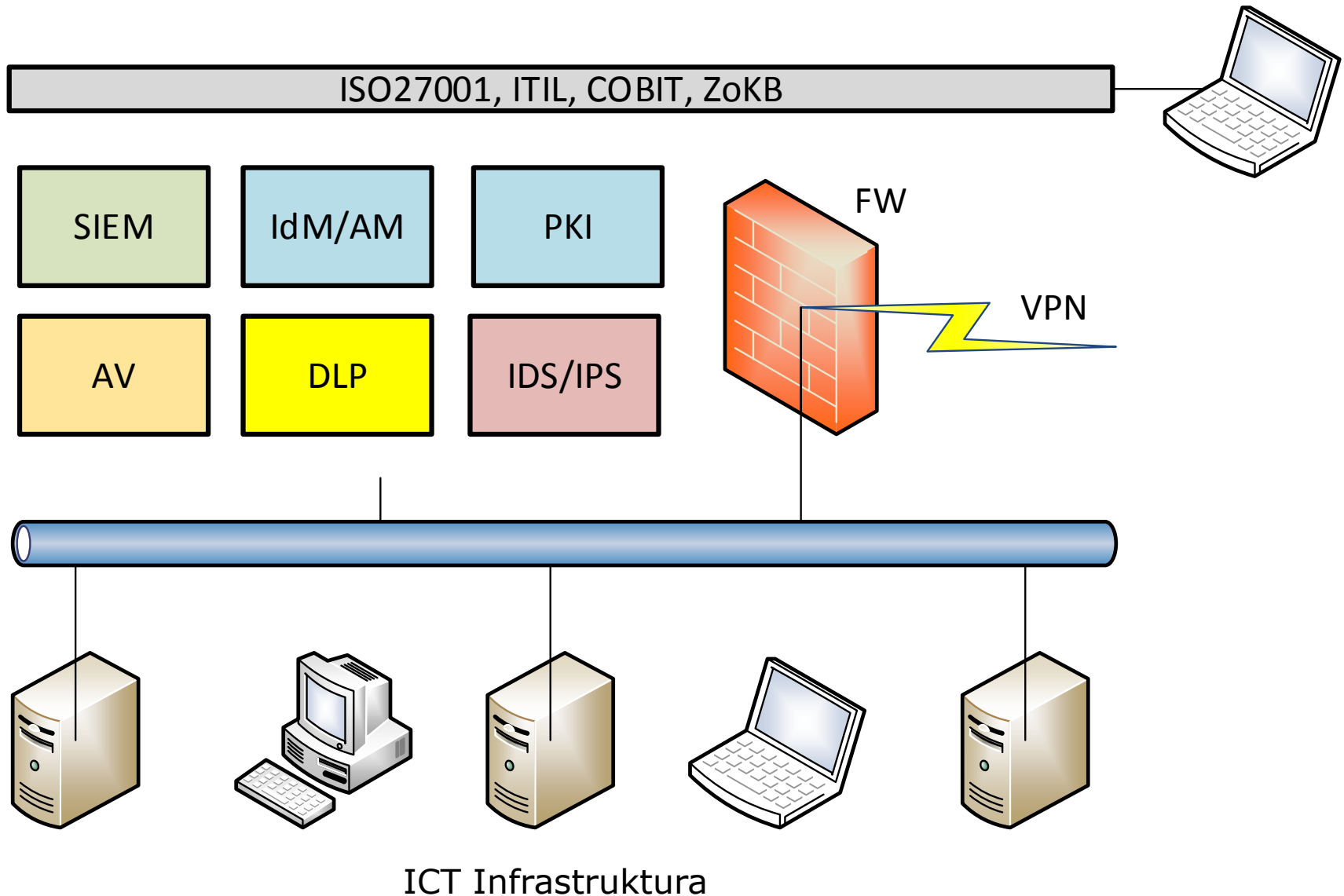
**Útočník se nebude omezovat jenom na slabiny počítačové/síťové infrastruktury, ale zkombinuje všechny možnosti aby identifikoval a využil cestu s nejmenším odporem pro průnik do organizace!!!**

**A co je cílem útoku a má cíl ICT povahu? Jsou to peníze? Informace? Poškození jména?**

# Multidisciplinární bezpečnost



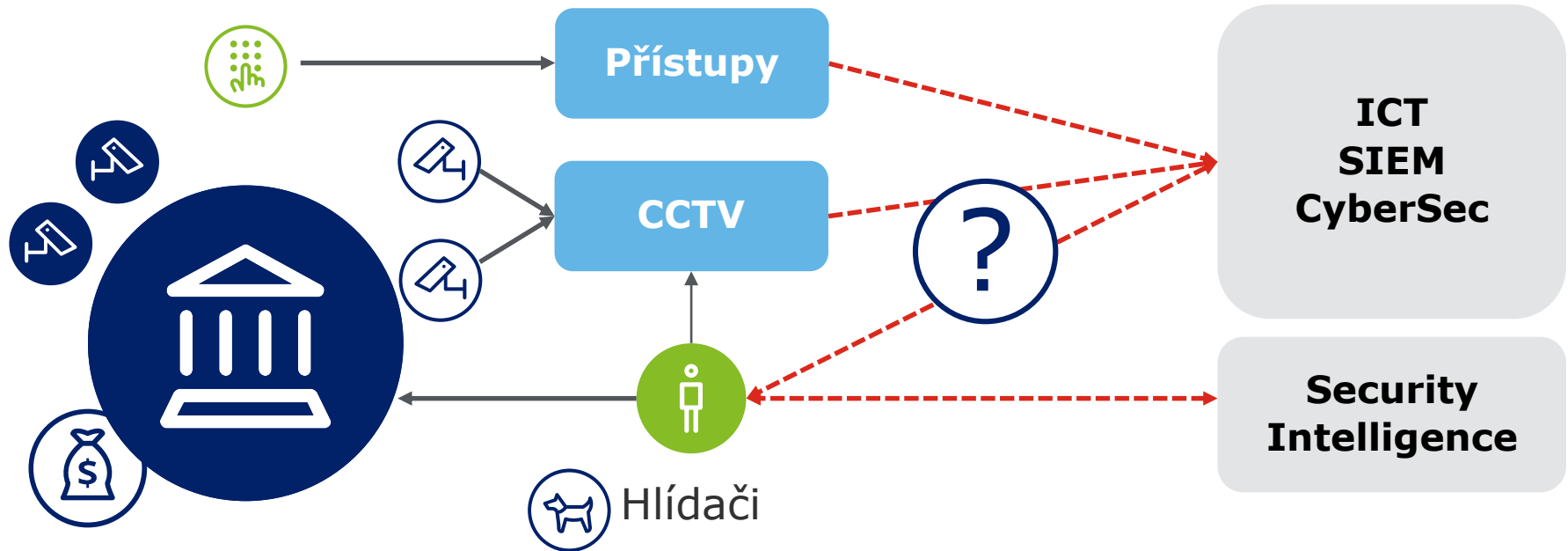
# Kybernetická bezpečnost (Cyber)



# Fyzická bezpečnost (Physical)

## Fyzická bezpečnost

## Kybernetická bezpečnost



- ✓ Propojení informací z přístupů do SIEM
- ✓ Rozpoznání osob a korelace s identitami
- ✓ Propojení ochrany objektu do kybernetické bezpečnosti





# Lidské chování a psychologie (Human)



# Legislativa a právo (Legal)

- Smluvní vztahy subjektů (SLA, licenční, dodavatelsko-odběratelské, ...)
- Mezinárodní právo a jeho aplikace (smlouvy, cloud, ...)
- Aplikace zákonů (ZoKB 181/2014 Sb., ZoOUI 412/2005 Sb., ...)
- Ochrana osobních údajů (ZoOOU 101/200 Sb., směrnice EU)
- Ochrana dat EU (GDPR – General Data Protection Regulation 2016/679)
- Ochrana dat jiných zemí (Rusko, Čína, ...)
- Veřejné zakázky (ZoVZ 137/2006 Sb.)



# Finance (Economic)

- Realistické ohodnocení aktiv a hrozeb (Analýza rizík)
- Předvídatelnost cash-flow a solventnosti
- Vývoj životní úrovně, zaměstnanosti a sociálního zázemí
- Prevence proti „fraud“-ům a praní špinavých peněz (AML)



# GRC – Governance, Risk Management, Compliance

**ISO27001**

**PCI DSS**

**ITIL**

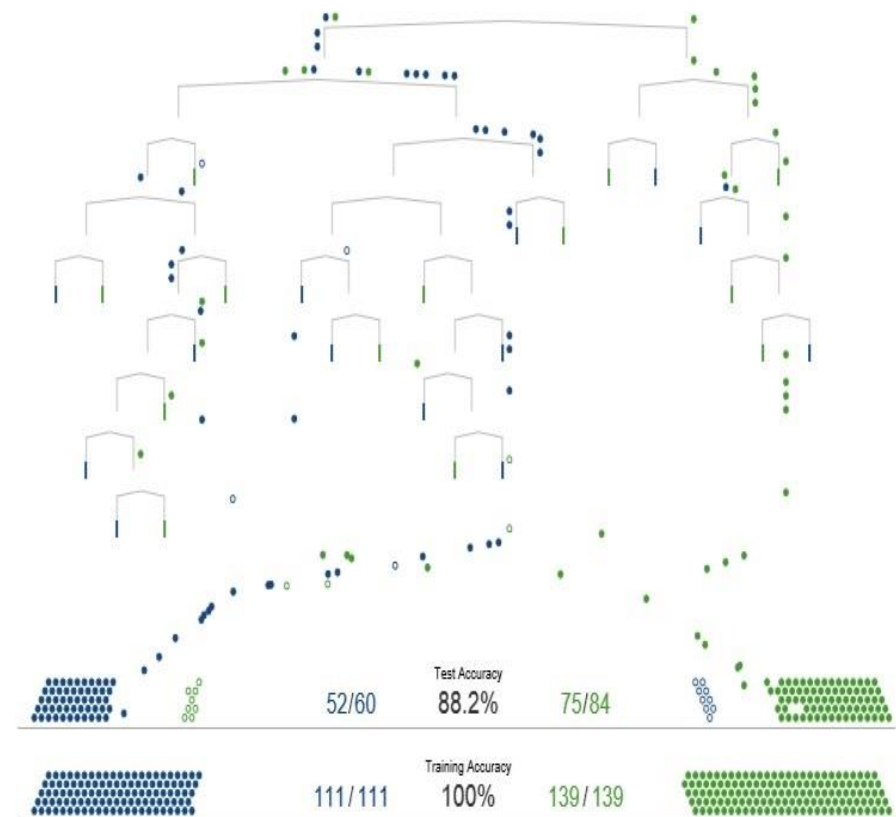
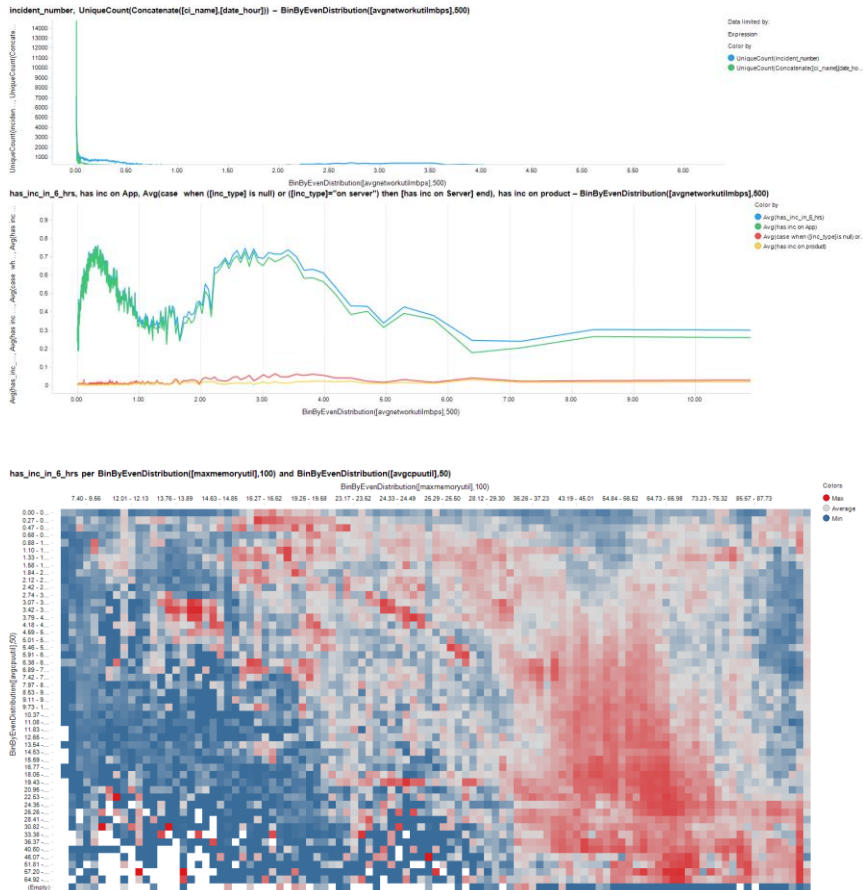
**ZoKB**

**COBIT**

**412/2005 Sb.**



# Bezpečnostní analytika a zpravodajství



Clustering

**Predict:** Classification  
Regression

**ML:**

Naive Bayes      Neural Networks  
K-nearest neighbour (KNN)  
Support Vector Machines (SVN)

# On-premise x Cloud

On-premise



Cloud

Physical

Legal

Cyber

Financial

Intelligence

GRC

Human



V praxi ...

Dnes izolované síly => Potřeba propojit  
Integrovaná multidisciplinární bezpečnost

**Prověření bezpečnosti:**



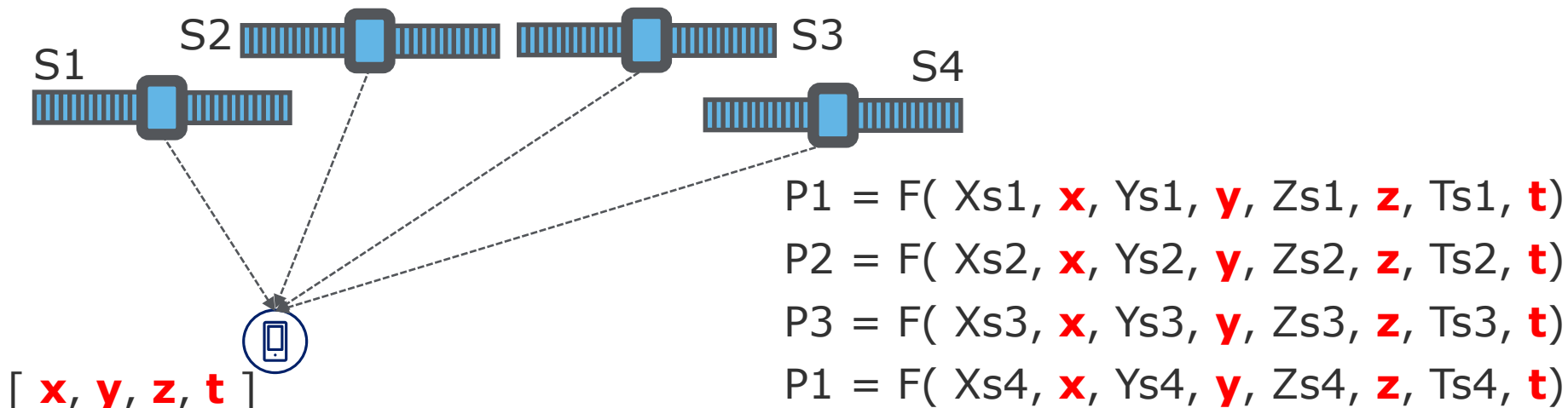
**Státní správa a velké organizace:**

= nejčastěji vlastní implementace

**Střední a malé společnosti:**

= bezpečnost jako služba

# Satelitní bezpečnost – nové téma pro bezpečnost



## Open Service (OS)

Jamming - Spoofing - Meaconing

+ šifrování

+ klíče

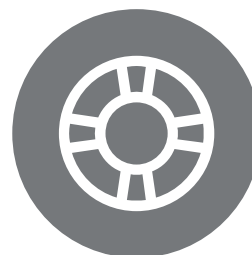
+ monitoring

+ procesy

+ ...



## Commercial Service (CS) - Public Regulated Service (PRS)





Děkuji za pozornost

**Adrian Demeter**  
addemeter@deloittece.com

---

<http://www.deloitte.com/cz/security/>

[CECZSecurity@deloitte.com](mailto:CECZSecurity@deloitte.com)

## Mobilní aplikace Deloitte CZ



[Zpravodaje](#) | [Studie](#) | [Semináře](#) | [Novinky](#) | [Videa](#)

# Deloitte.

Deloitte označuje jednu či více společností Deloitte Touche Tohmatsu Limited, britské privátní společnosti s ručením omezeným zárukou („DTTL“), jejích členských firem a jejich spřízněných subjektů. Společnost DTTL a každá z jejích členských firem představuje samostatný a nezávislý právní subjekt. Společnost DTTL (rovněž označovaná jako „Deloitte Global“) služby klientům neposkytuje. Podrobný popis právní struktury společnosti Deloitte Touche Tohmatsu Limited a jejích členských firem je uveden na adrese [www.deloitte.com/cz/onas](http://www.deloitte.com/cz/onas).

Společnost Deloitte poskytuje služby v oblasti auditu, daní, poradenství a finančního a právního poradenství klientům v celé řadě odvětví veřejného a soukromého sektoru. Díky globálně propojené síti členských firem ve více než 150 zemích a teritoriích má společnost Deloitte světové možnosti a poskytuje svým klientům vysoce kvalitní služby v oblastech, ve kterých klienti řeší své nejkomplexnější podnikatelské výzvy. Přibližně 225 000 odborníků usiluje o to, aby se společnost Deloitte stala standardem nejvyšší kvality.

Společnost Deloitte ve střední Evropě je regionální organizací subjektů sdružených ve společnosti Deloitte Central Europe Holdings Limited, která je členskou firmou sdružení Deloitte Touche Tohmatsu Limited ve střední Evropě. Odborné služby poskytují dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited, které jsou samostatnými a nezávislými právními subjekty. Dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited patří ve středoevropském regionu k předním firmám poskytujícím služby prostřednictvím více než 5 000 zaměstnanců ze 41 pracovišť v 17 zemích.

© 2016 Deloitte Česká republika