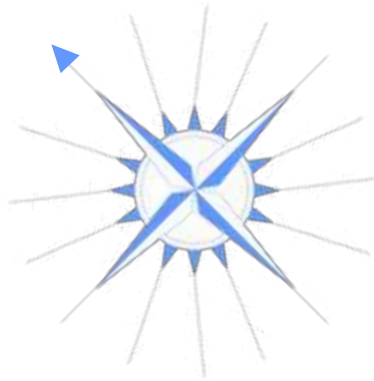


ASSICO

CENTRAL EUROPE



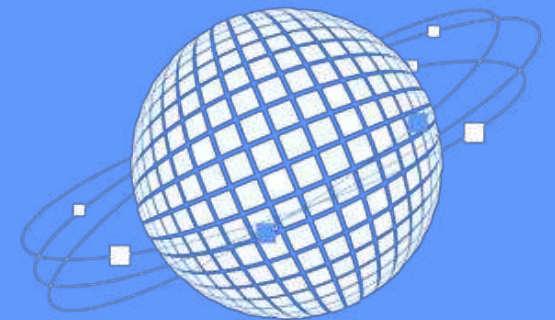
solutions for demanding business

Vyhrajte souboj s kyber útoky „Kdo zvítězí?“

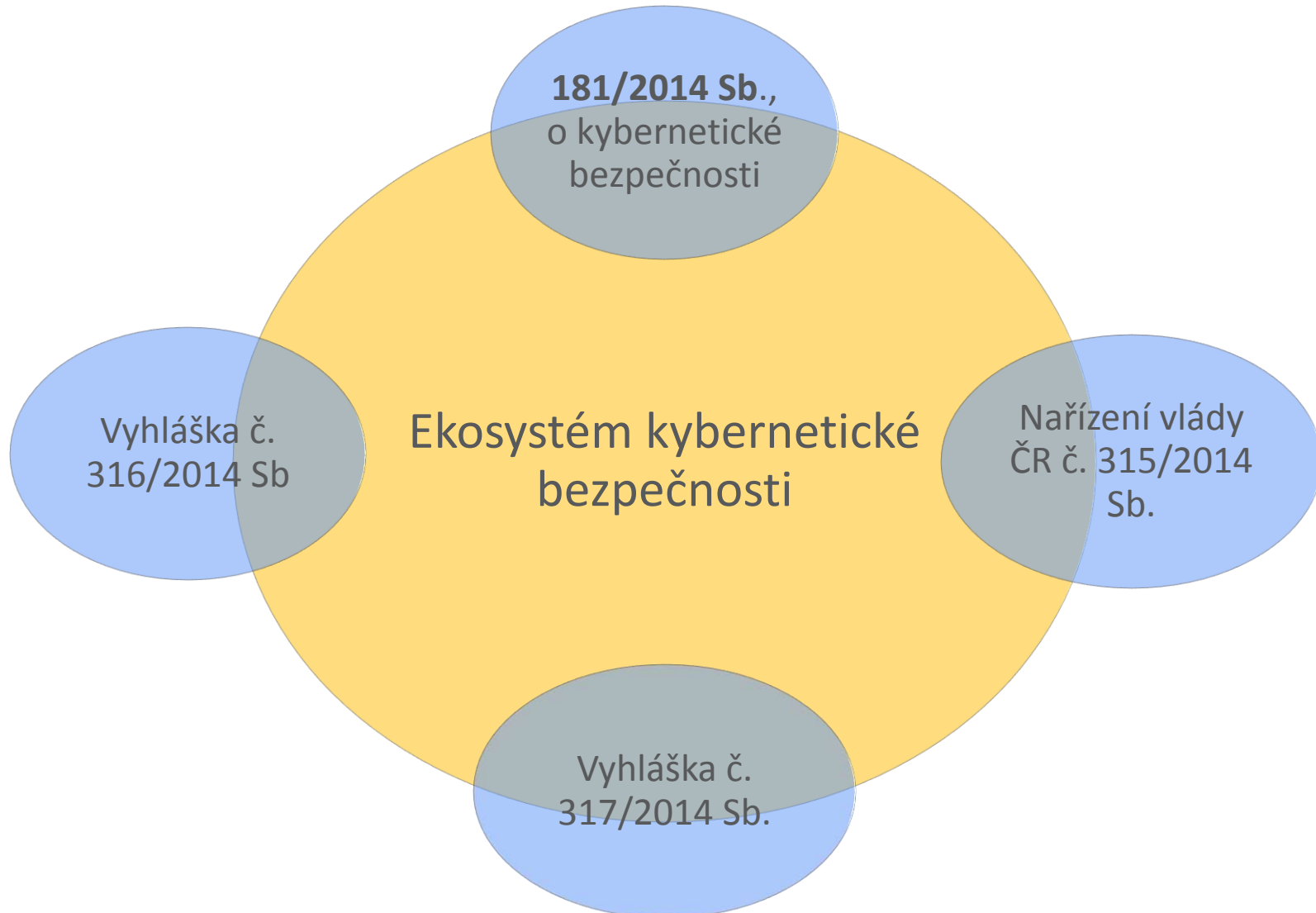
Martin Lukáš, Asseco Central Europe

Agenda

- 1) Vymezení ekosystému kybernetické bezpečnosti
- 2) Kdo jsme my
- 3) Kdo jsou ti na druhé straně
- 4) Pokročilé útoky
- 5) Ochranný štít Verint – Threat Protection System
- 6) Výhody TPS ochranného štítu
- 7) Závěr



Vymezení ekosystému kybernetické bezpečnosti



Kdo jsme my

- Dodavatelé IS
 - Provozovatelé IS
 - Správci IS kritické infrastruktury
 - Správce významného IS
 - Poskytovatelé služeb e-komunikace
 - Administrujeme databáze, data, informace a znalosti
 - Jsme ohroženi individuálními i organizovanými útoky
-
- Kdo na nás útočí ?



Kdo jsou ti na druhé straně

- Společnosti s cílem získat naše aktiva (data, informace, znalosti)
- Entuziasti s cílem si dokázat, že jsou jedineční
- Společnosti najímající kybernetické entuziasty
- Studenti s potřebou seberealizace

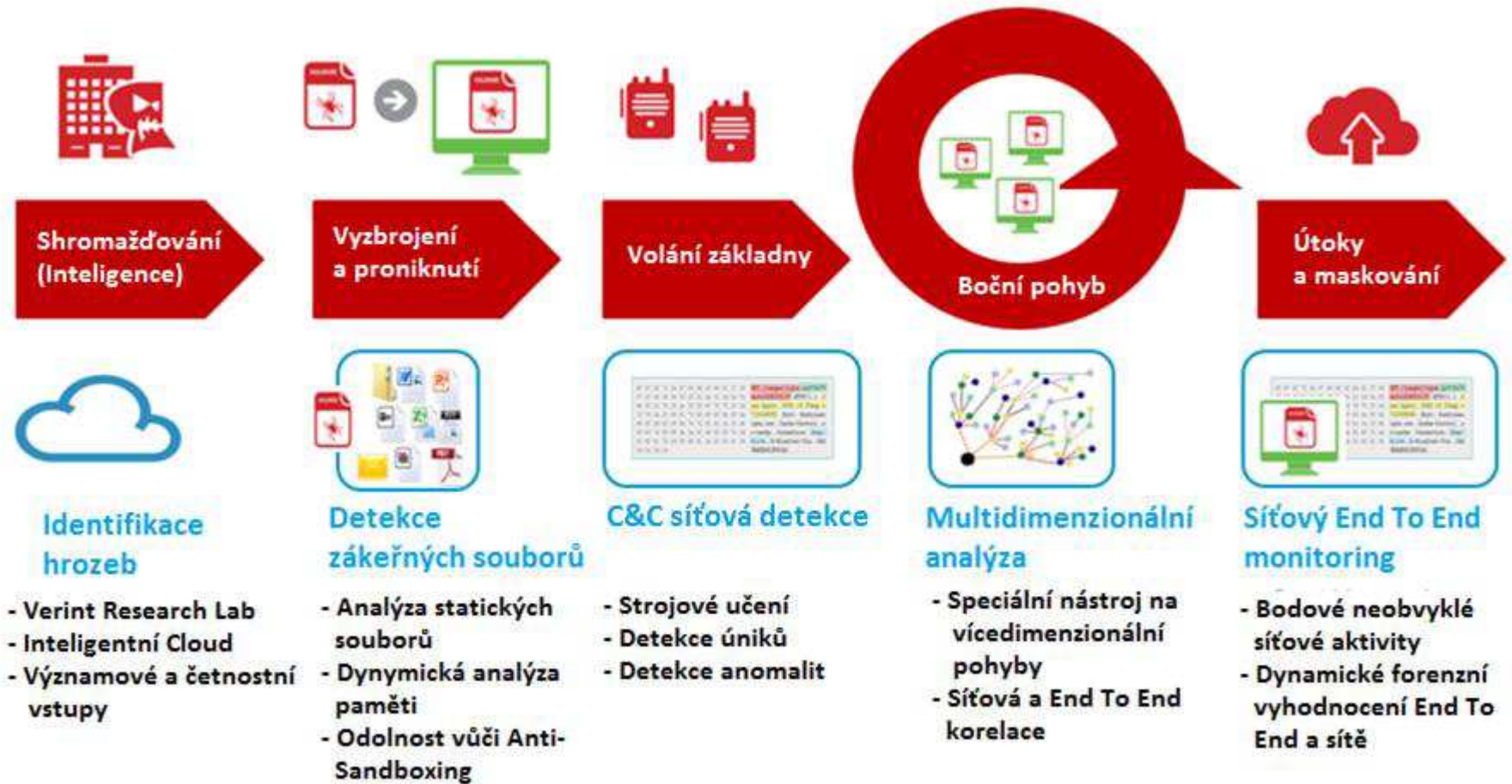
- **Kybernetický prostor**

- umožňuje vznik nových technologicky orientovaných skupin
- je tichým a pro běžného občana těžko rozpoznatelným „bitevním polem“
- umožňuje vymýšlet pokročilé útočné nástroje a strategie útoků

- **Kyberteroristé, kyberšpióni, informační kriminalita**



Fáze pokročilých kybernetických útoků



Nástroje pro detekci a reakci na dílčí fáze kybernetického útoku

Ochranný štít Verint – Threat Protection System

- **Verint** - dlouhodobý dodavatel s 20 letou tradicí se zkušenostmi v oblasti Security and Intelligence a Cyber Protection v segmentech Národní ochrany/obrany, eGovernment, Telekomunikace, Kritická infrastruktura, ochrana před kybernetickými útoky



Výhody TPS ochranného štítu



- Přesná a včasná detekce

Využití vestavěných sad specializovaných detekčních komponent zmírňující celou smyčku cyber útoku



- Rychlá a efektivní analýza a odezva

Upozornění na kybernetické útoky, automatizaci analýzy útoku, možnost aplikace opatření během několika minut



- Zdokonalení provozní efektivity SOC

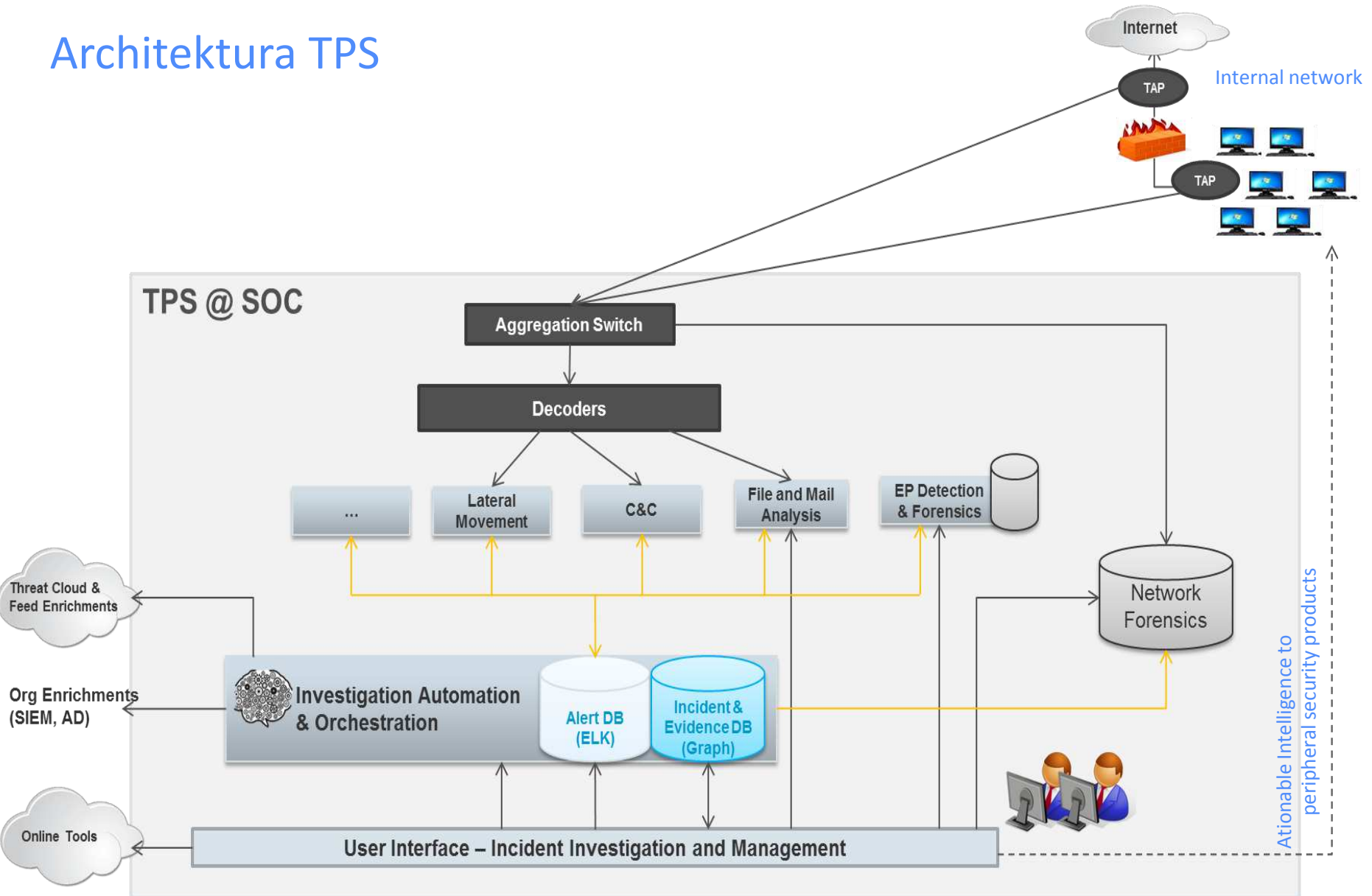
Podpora týmu SOC unifikovanou cyber inteligencí, dohledáváním a potřebnými forenzními systémy



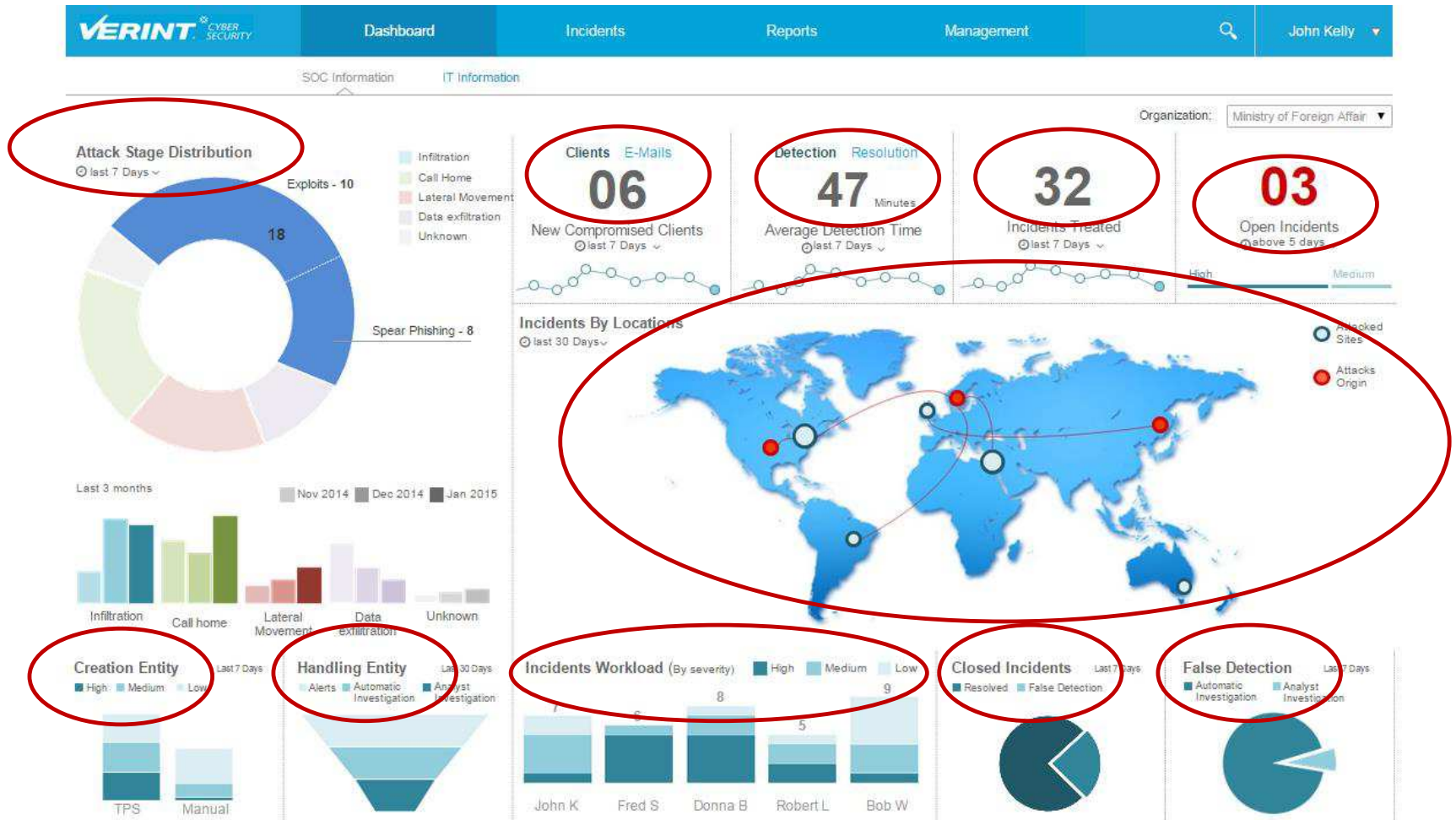
- Zvýšení odolnosti organizace / centrálních IS

Využití adaptivní platformy, rozšiřitelné architektury, a behaviorální analýzy

Architektura TPS



Navržen pro Security Operation Centre (1)



Vizuální sledování hrozeb, dopadů a KPIs pomocí Dashboard (Role Based Dashboard)

Navržen pro Security Operation Centre (2)

VERINT CYBER SECURITY

Dashboard Incidents Reports Management

John Kelly

Manage INC. #88764 INC. #11726

Organization: Ministry of Foreign Affairs

All Incidents | **Your Incidents**

Assigned: Not started (3), In progress (5), On hold (10) → Total 18

Unassigned: 6 New, 0 Re-Opened, 2 Pending Analyst

By Owner: JohnK, FredS, DonnaB, RobertL, MarryC, BobW, UNASSIGNED

Incidents Treated (Last 30 days): severity 1-10

Showing: All Open Incidents | Going back: One month | New Incident

Bulk actions: -select- | Show TPS pending investigations (8) | Find incident...

Showing 10 incidents

ID	Severity	Type	Steps/Evid.	Stage	Originator	Summary	Create@	Modified / Closed	Owner	Status	Open
11726	9	APT	6/1	Data exfiltration	[TPS]		Feb 1 2015, 06:18	Feb 1 2015, 06:18	JohnK	In progress	
88764	6	APT	4/2	Spear phishing	[TPS]		Dec 6, 2014 15:39	Dec 6, 2014 15:41	JohnK	In progress	
88715	7	APT	5/1	Call home	[TPS]		Dec 3, 2014 19:18	Dec 3, 2014 19:18	-- --	New	
88730	5	APT	6/2	Data exfiltration	DonnaB		Dec 3, 2014 15:39	Dec 3, 2014 16:39	RobertL	In Progress	
87122	3	APT	1/1	Unknown	BillR		Dec 2, 2014 00:12	Dec 2, 2014 00:13	-- --	New	
77182	6	APT	7/2	Unknown	JohnK		Dec 1 2014 02:27	Dec 1 2014 02:29	-- --	On Hold	
67726	4	APT	5/3	Data exfiltration	[TPS]		Dec 1 2014 02:27	Dec 1 2014 02:29	DonnaB	In Progress	
12433	7	APT	4/1	Spear phishing	[TPS]		Dec 1 2014 02:27	Dec 1 2014 02:29	BobW	In Progress	
22345	9	APT	9/1	Lateral movement	[TPS]		Dec 1 2014 02:27	Dec 1 2014 02:29	FredS	Not Started	
99484	5	APT	6/3	Call home	[TPS]		Dec 1 2014 02:27	Dec 1 2014 02:29	BobW	In Progress	

Správa, přidělování a sledování stavu incidentů


Verint reference v Evropské Unii

■ Estonia Information System Authority (RIA)

- Dodávka CYBERVISION pro monitorování provozu státních portálů a poštovních serverů na kritické infrastruktuře
- Detekování malware útoků

www.ria.ee/contact/





Estonian Information System's Authority

LETTER OF RECOMMENDATION

October, 2013

To whom it may concern:

Successful Deployment of Verint CYBERVISION ADS Malware Detection Solution

Estonian Information Systems Authority (RIA) – Government ISP

1. Our organization runs a critical government network with tens of thousands of endpoints and a range of standard security tools such as anti-virus, firewall, IDS.

2. Verint CYBERVISION ADS (ADS) solution, as a complementary solution for Internet gateway and generates alerts about malware as well as unknown malware attacks.

3. The solution's behavioral detection of Command and Control channels unique and promising.

5. We highly recommend evaluating Verint CYBERVISION ADS as a complementary solution to standard security tools for detecting advanced and unknown malware in sensitive networks.

„Jsme velmi překvapeni schopnostmi komponenty TPS detekující neznámé malware... „

„Technologie je unikátní a nemá obdoby ...“

„Vysoce doporučujeme pro její další rozvoj a využití v eGovernment...“

nr 70006317

Závěr - vybrané reference v oblasti informační bezpečnosti



- Ministerstvo vnitra ČR
 - Registr práv a povinností

- Česká správa sociálního zabezpečení
 - Informační a komunikační rozhraní ČSSZ

- Český statistický úřad
 - Redesign statistického informačního systému
 - Registr osob

- Ministerstvo financí ČR
 - Administrativní registr ekonomických subjektů (ARES)

Děkuji za pozornost

Martin Lukáš

Asseco Central Europe, a.s. | martin.lukas@asseco-ce.com | www.asseco.com/ce

Budějovická 778/3a, 140 00 Praha 4, Czech Republic
Tel.: +420 234 292 500, Fax: +420 234 292 505

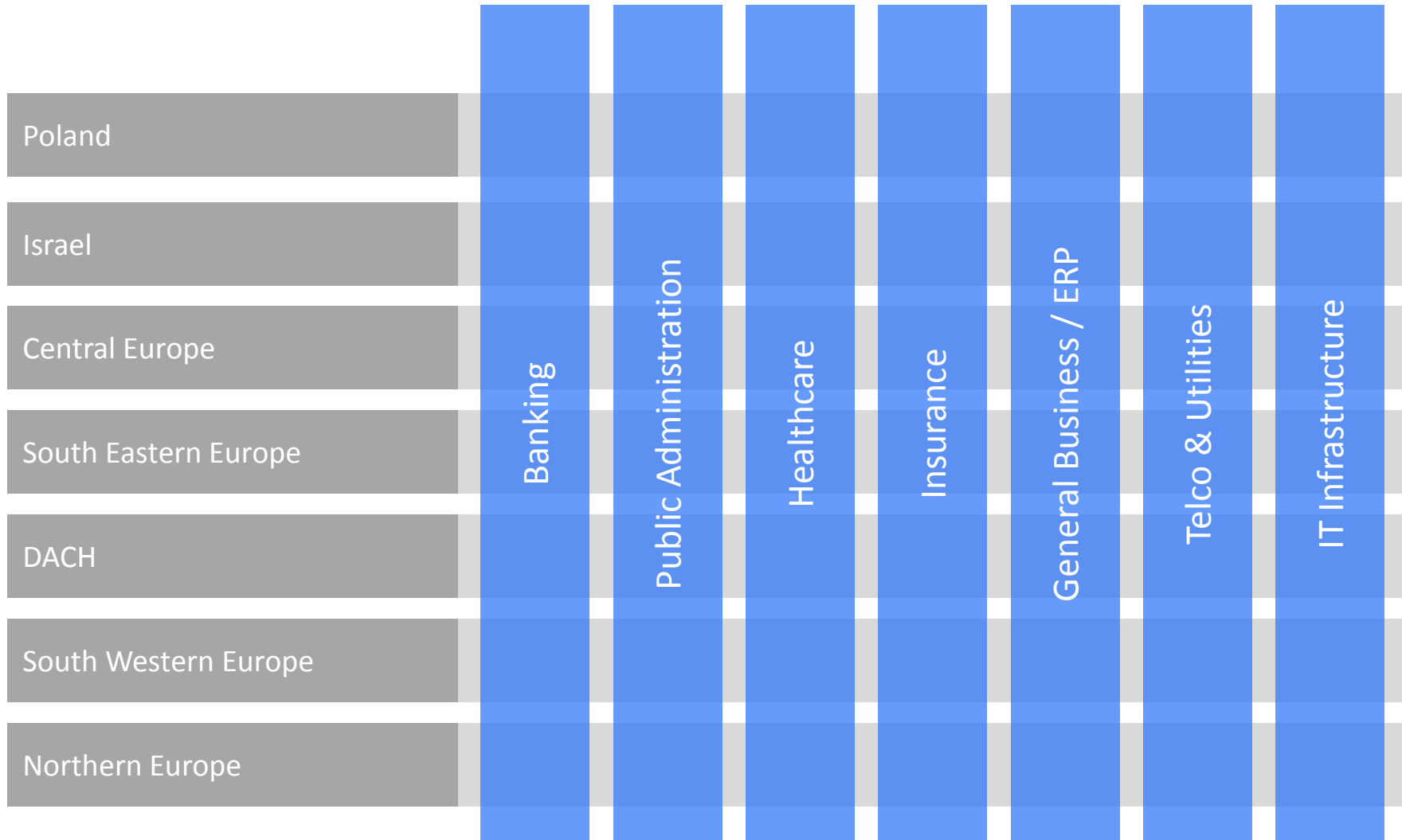
Sender and/or Asseco Central Europe have no intention based on this message to accomplish any legal engagement or to make a written or other contract, to accept or promise any commitment, only if it is directly and concretely written in the message; also is not responsible if recipient earned an incorrect impression. To conclude a valid and effective treaty, there must be a written documentary form signed by statutory bodies, by empowered person, or by confidential clerk of Asseco Central Europe

This presentation is the property of Asseco Central Europe (Asseco CE) business group. Information presented serves for marketing purposes only and constitutes neither an offer to sell nor a solicitation to buy. Asseco CE accepts no liability whatsoever for any loss arising directly or indirectly from the use of, reliance of any information contained in this presentation or for any omission of the information. The processing, copying, recording on information carriers, as well as making this presentation or any part thereof available in any way to third parties requires the prior consent of Asseco CE member.

Asseco Group at a glance



Asseco Group Business Units



Asseco Central Europe at a glance

Founded in

1990

IT Services Provider

no.1

in **Slovakia**

One of the Strongest
Software Houses

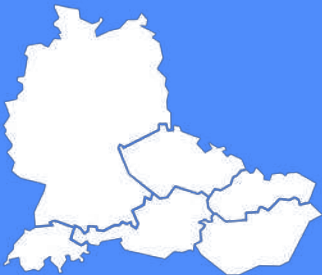


in **CEE** Region

Listed on

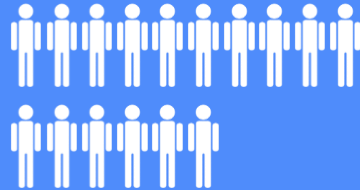
**Warsaw
Stock
Exchange**

Present



in **6** Countries

Headcount



1,600 People

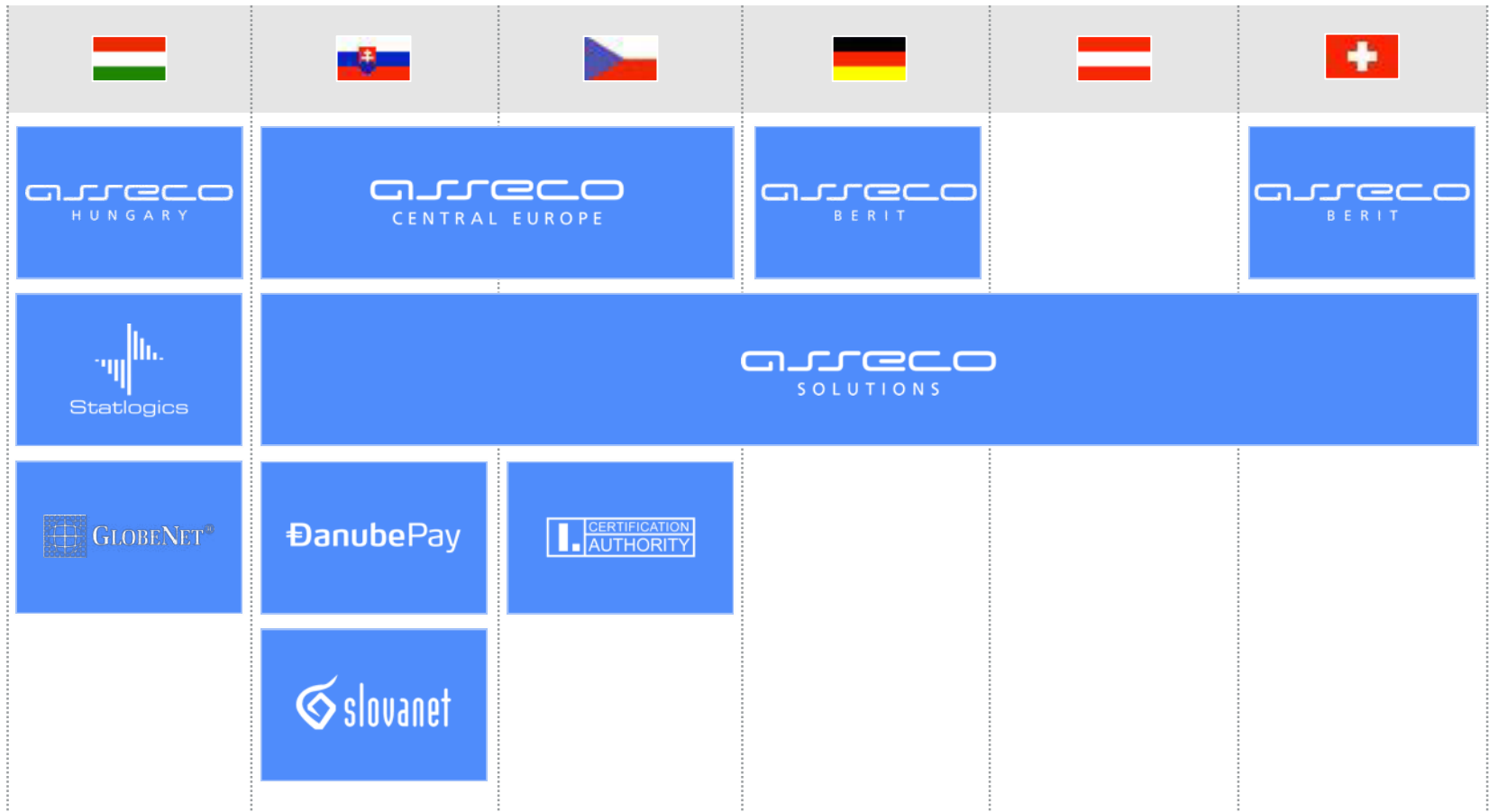
Revenue (2012)

134.44

EUR mil

MEMBER OF
ASSECO
GROUP

Asseco Central Europe Group present in European countries



Portfolio of solutions and services

	Banking	Insurance	Healthcare	Building Savings	Utilities	Public	Telco
SERVICES	Software development						
	System Integration						
	Infrastructure & Security						
	Outsourcing						
SOLUTIONS	StarBANK	StarINS	Mediform	StarBUILD	AMES	EDT	By means of daughter company Slovanet
	eStarBANK	SofiSTAR	MedWorks		TOMS	LIDS	
	StarTREASURY		ZPIS				
	StarCARD®						
	Credilogic						
			StarBI	StarSTAT	AQS	Business Intelligence	
				AGportal	Application Integration & Portals		
				HELIOS	ERP		