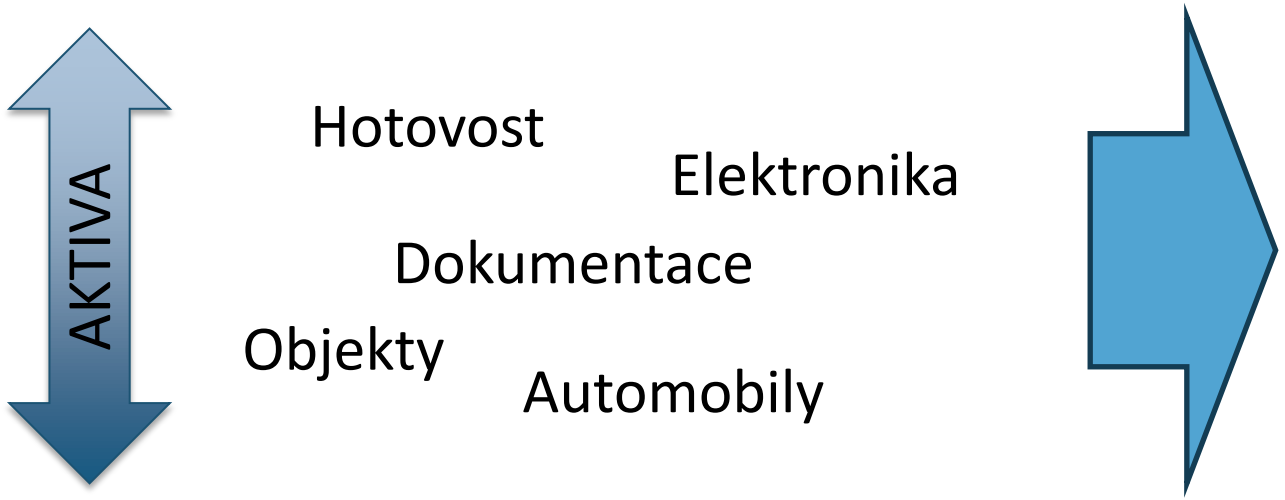
TTC MARCONI

Bezpečnost organizace není pouze kybernetická

Martin Bajer

30.11.2021

Postupná změna aktiv a bezpečnostních hrozeb



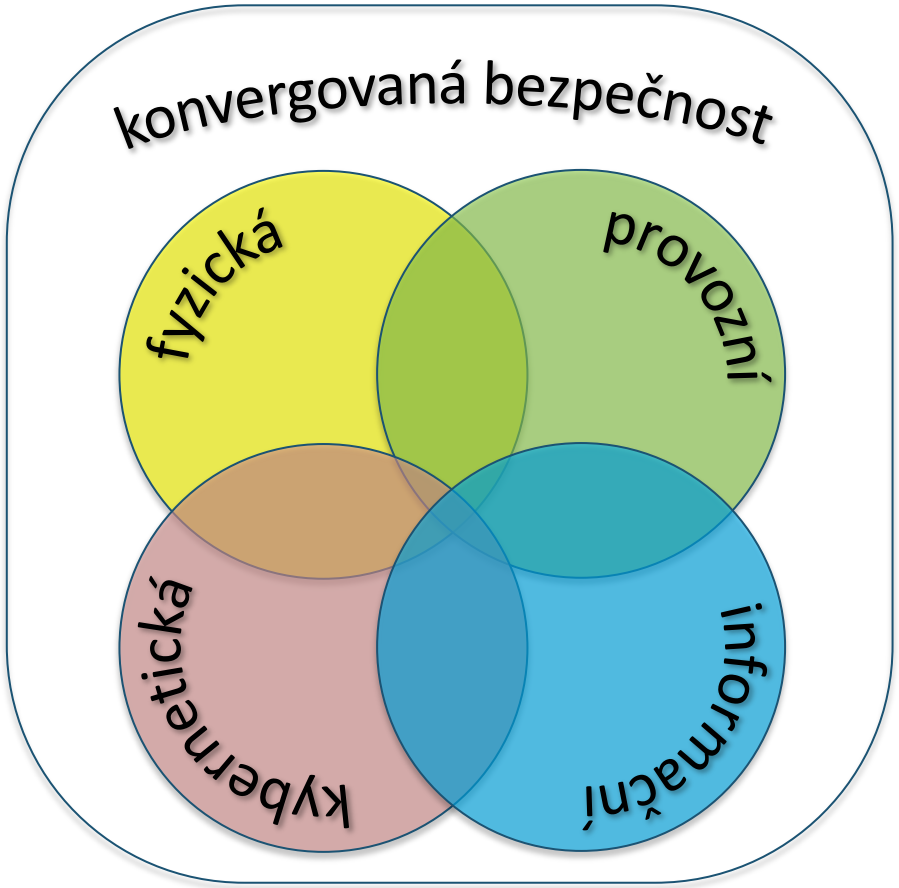
Servery
Infrastruktura
Systémy
Služby
Data
Lidé

hrozby fyzické	hrozby provozní	hrozby kybernetické	hrozby informační
vandalizmus	námraza	DDoS útok	zneužití dat
krádež	sucho	phishing	dezinformace
vydírání	porucha	zneužití identity	ztráta dat
měkké cíle	epidemie	hackeři	průmyslová špionáž
požár	havárie	viry	krádež osobních údajů
terorizmus	povodeň	malware	
fyzické napadení	výpadek elektřiny	ransomware	

Konvergovaná bezpečnost

- Fyzická bezpečnost
- Provozní bezpečnost
- Kybernetická bezpečnost
- Informační bezpečnost

Konvergovaná bezpečnost



Hybridní hrozby

- Hybridní hrozby jsou fenoménem vyplývajícím z **konvergence** a propojení různých prvků, které společně tvoří komplexnější a vícerozměrnější hrozbu.

- Úkolem hybridní kampaně je využít slabin protivníka; **znemožnit jasnou interpretaci událostí** a odhalení jejich **vzájemné souvislosti**; komplikovat či přímo znemožnit identifikaci původce a zastřít jeho úmysly; komplikovat, destabilizovat či přímo paralyzovat rozhodovací proces, a tím **znemožnit včasnou a účinnou reakci** ze strany napadeného.

- Jednotlivé prvky hybridní kampaně nemusí být nutně nezákonné či představovat hrozbu samy o sobě; **nebezpečí spočívá právě v jejich sofistikované kombinaci**, která současně usiluje o zastření pravého účelu jejích jednotlivých komponentů.

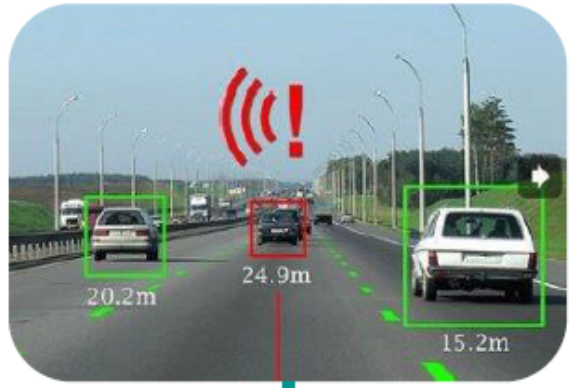
Změna pohledu na bezpečnost

ZPĚTNÉ VYHODNOCENÍ

2000

REÁLNÝ ČAS

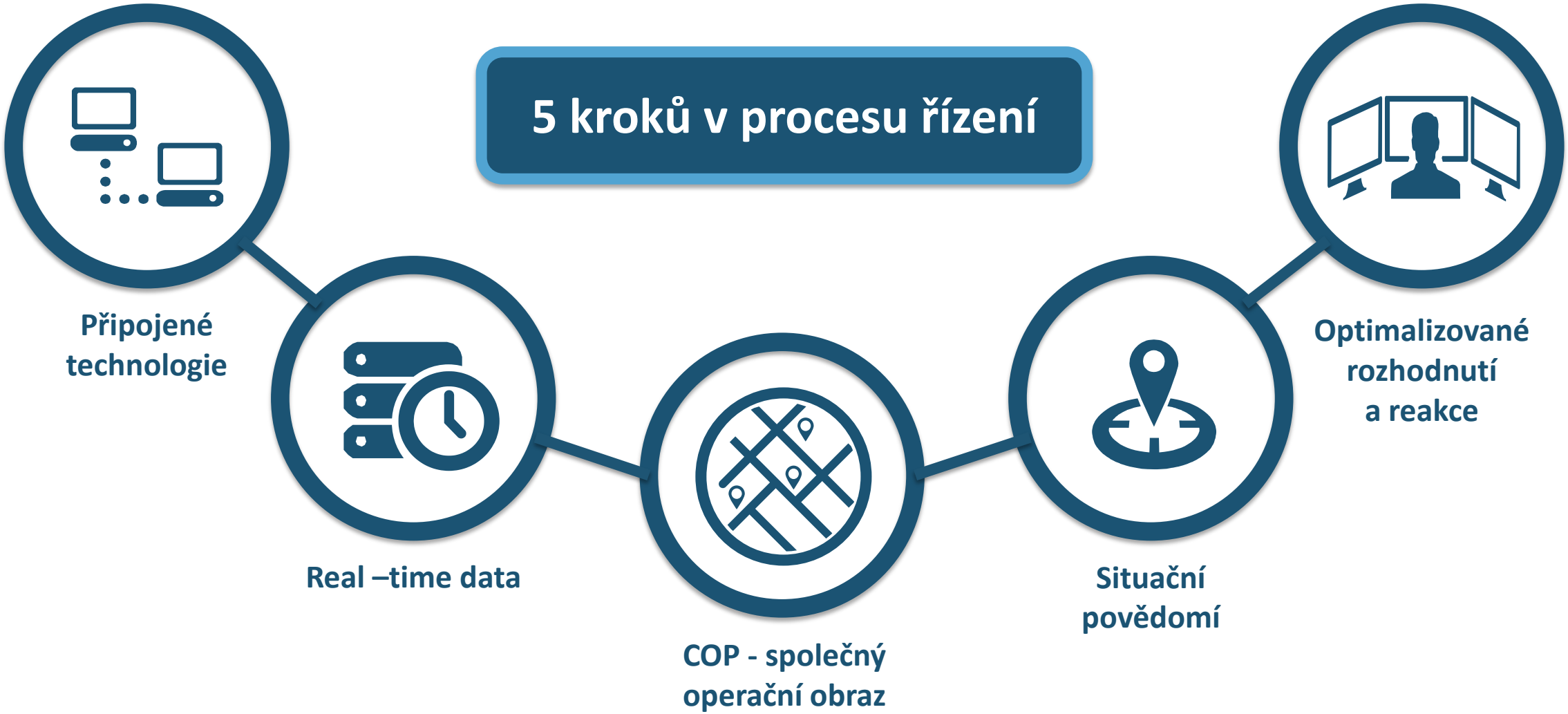
2011



PREDIKCE

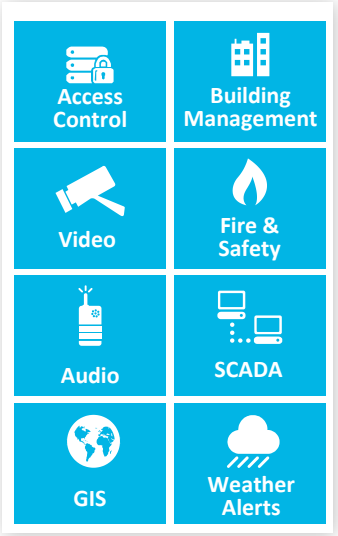
2020

Řízení situace v reálném čase



Zdroje dat pro oblast bezpečnosti

- Klasické systémy a čidla (PZTS, EPS, EKV…)
- Kamery, termokamery
- Biometrické systémy
- Systémy v budovách (výtahy, klimatizace…)
- IT systémy (SIEM, logování, behaviorální analýza…)
- Provozní systémy (SCADA, MaR, čidla, poloha…)
- Dopravní informace, počasí…
- Mapové podklady
- Databázové systémy (Telefonní seznam, jízdní řád, ERP, registr vozidel…)
- Sociální sítě (Facebook, Twitter…)
- Média (Televize, rozhlas, internet…)



Tok dat při mimořádných situacích

ZÍSKÁVÁNÍ DAT

- **Čidla a detektory**
- **Kamery**
  - vyšší rozlišení, inteligence v kameře
- **Logy, chování sítě**
- **Další data**
  - využívání dat, které nejsou primárně určené pro oblast bezpečnosti
- **Člověk**

PŘENOS DAT

- **Zabezpečení**
- **Speciální kabeláž, metalické kabely**
- **Optické kabely**
- **Ethernetová síť**
- **Bezdrátová síť**
  - MRS, TRS
  - GSM-R
  - FRMCS
  - Mobilní sítě

VYHODNOCENÍ

- **Datová analytika**
- **Video**
  - videoanalýza, detekce obličejů, postavy, chůze
- **Operační střediska**
  - sofistikované systémy
- **Korelace dat**
- **Predikce**
- **Inteligence**

SDÍLENÍ DAT

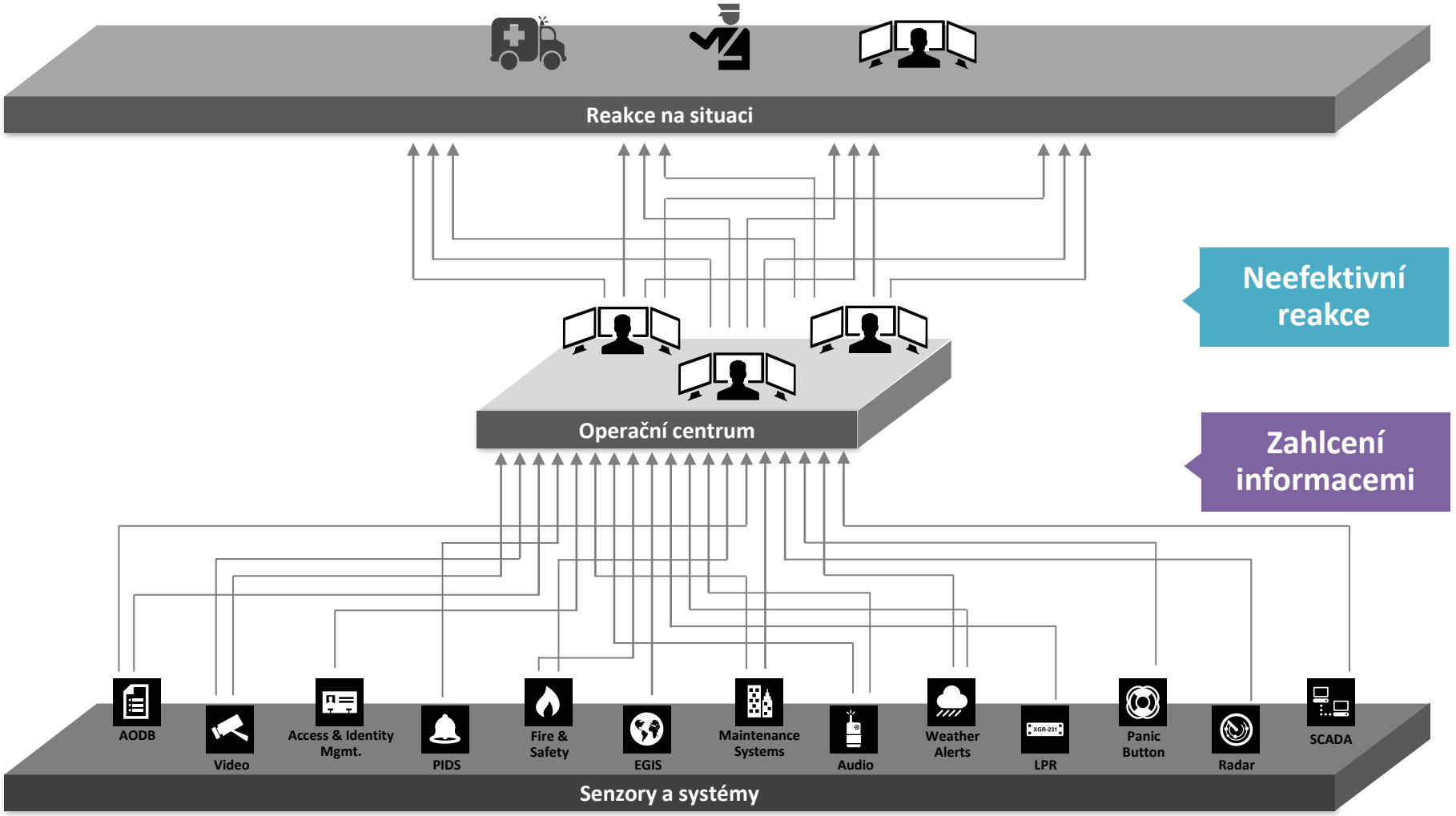
- **Operační střediska**
  - sofistikované systémy
- **Inteligence**
  - scénáře, postupy, automatické reakce
- **Sdílení relevantních dat**
- **Přehledy, reporty, analýzy**

Vyhodnocování a sdílení dat

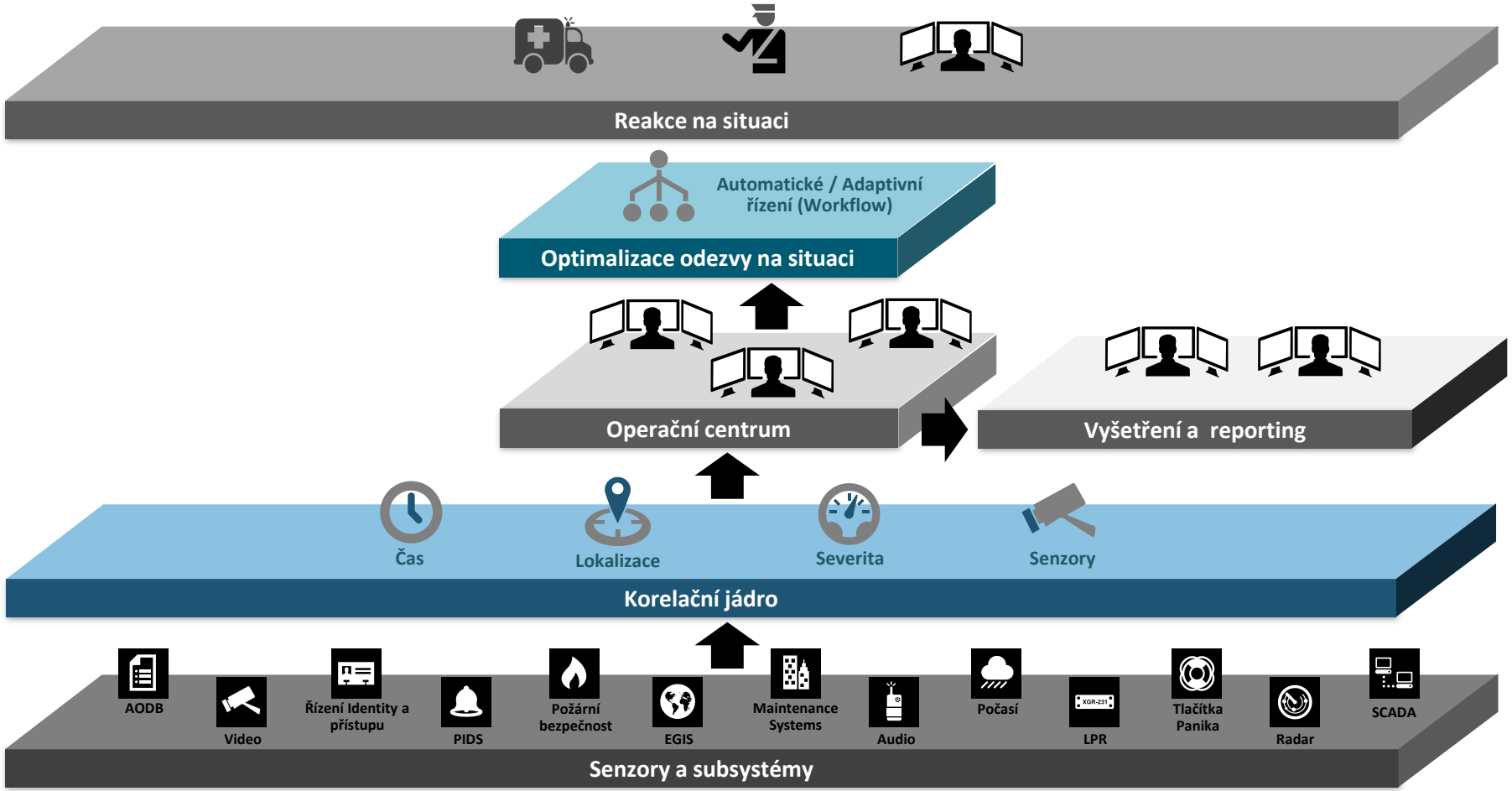
Situační incident management systém

- Dokonalý přehled o situaci
- Správa incidentů
- Pracovní postupy
- Automatické reakce
- Predikce událostí
- Redukce planých poplachů
- Podrobný reporting
- Sledování důležitých ukazatelů organizace

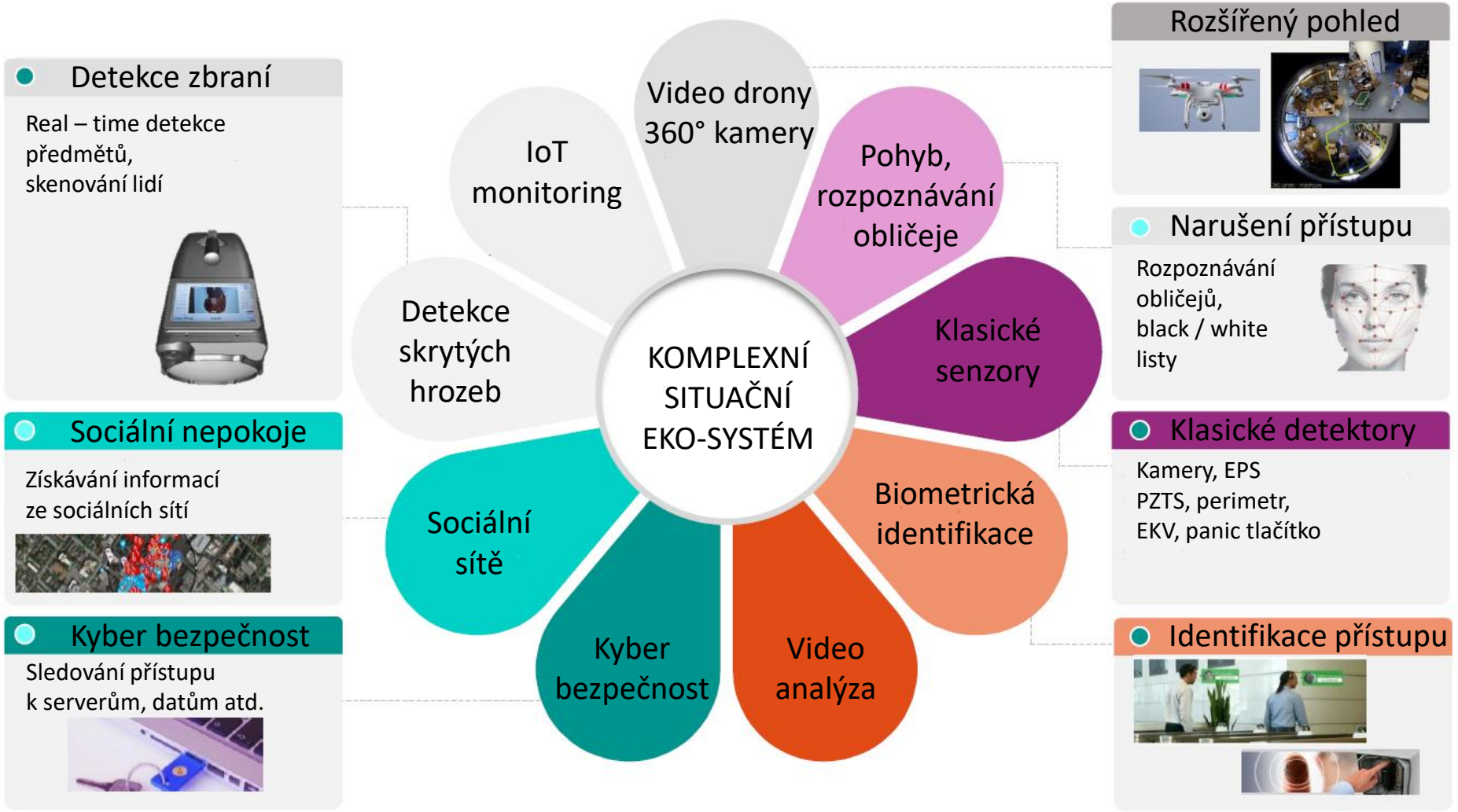
Princip činnosti informačního managementu



Princip činnosti informačního managementu



Komplexní situační ekosystém



Security 3.0

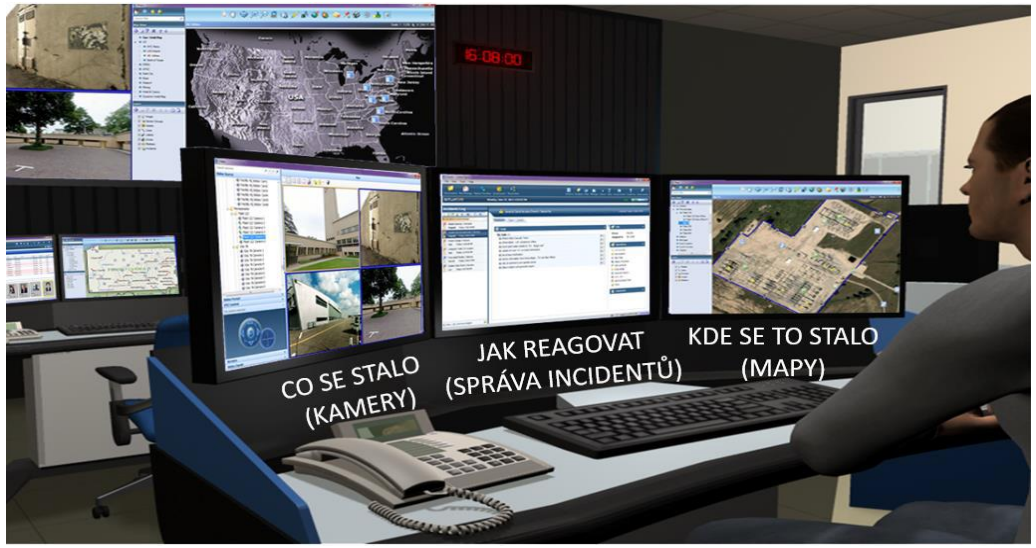
Umožňuje pochopit a využít velké množství různorodých dat

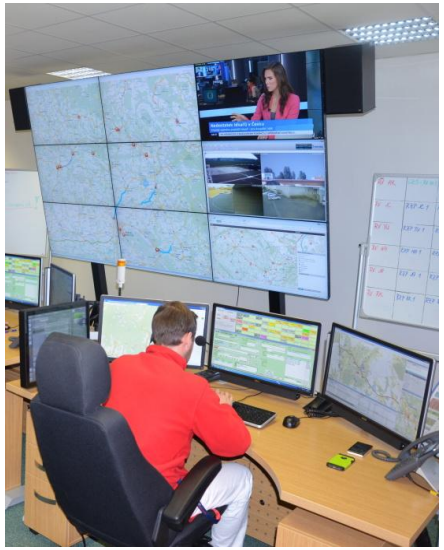
Nabízí potřebné informace těm správným lidem ve správný čas

Optimalizuje správu bezpečnosti, minimalizuje risk

Security 3.0

Produkty x řešení





Qognify splunk> GREYCORTEX allot See. Control. Secure. Nagios®

CISCO FORTINET Check Point SOFTWARE TECHNOLOGIES LTD. paloalto NETWORKS ZABBIX

radware Flowmon Networks anyVISION. TopoNet LYNX®

Cíle řešení

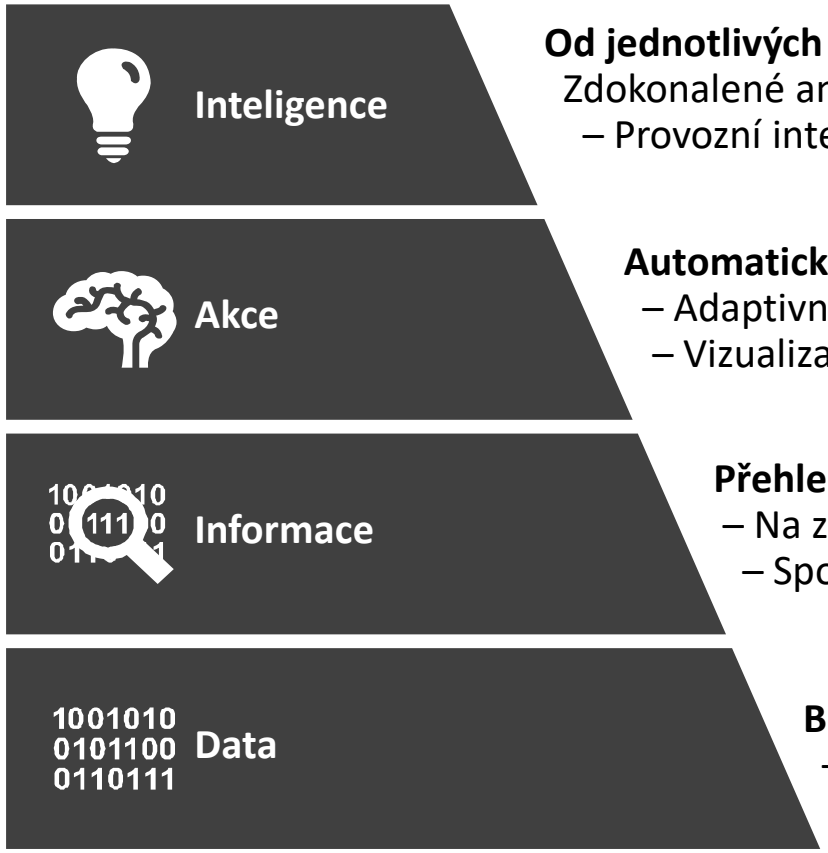
Zajištění kontinuity činnosti organizace

Připravenost na mimořádné události a krizové situace

Ochrana kritické infrastruktury

Cesta od dat po provozní inteligenci

Transformace dat do provozní inteligence



Od jednotlivých incidentů k vícenásobným & celkový pohled
Zdokonalené analytické a reportovací nástroje
– Provozní inteligence

Automatické a definované scénáře
– Adaptivní wokflow transformují osvědčené postupy do operačních scénářů
– Vizualizace užitečných dat

Přehled o situaci
– Na základě korelací a analýzy
– Společný obraz situace (Common operating pictures)

Black Box
– Integruje a sbírá strukturované a nestrukturované zdroje dat

Děkuji Vám za pozornost

Martin Bajer

TTC MARCONI

bajer@ttc.cz

www.ttc-marconi.com