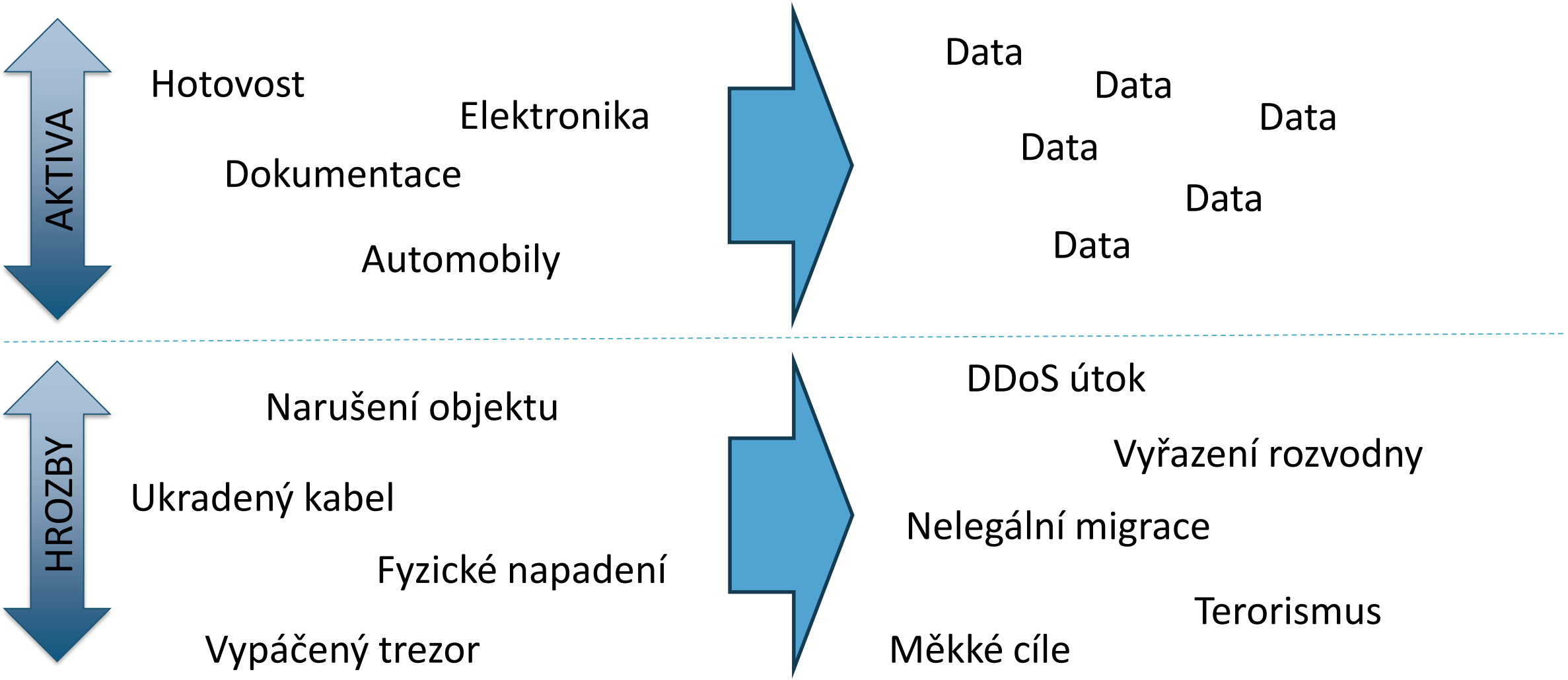
TTC MARCONI

Konvergovaná bezpečnost v infrastrukturních systémech

Martin Bajer

28.11.2018

Postupná změna aktiv a bezpečnostních hrozeb



Konvergovaná bezpečnost

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

- Konvergovaná bezpečnost

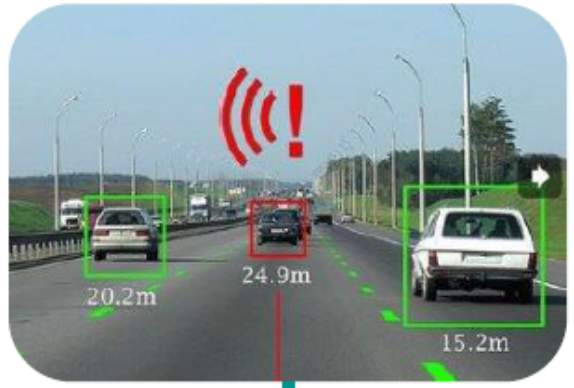
Změna pohledu na bezpečnost

ZPĚTNÉ VYHODNOCENÍ

2000

REÁLNÝ ČAS

2011



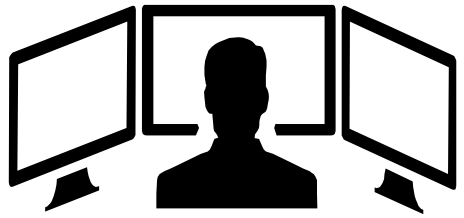
PREDIKCE

2020

Posun od sběru dat k jejich vyhodnocení

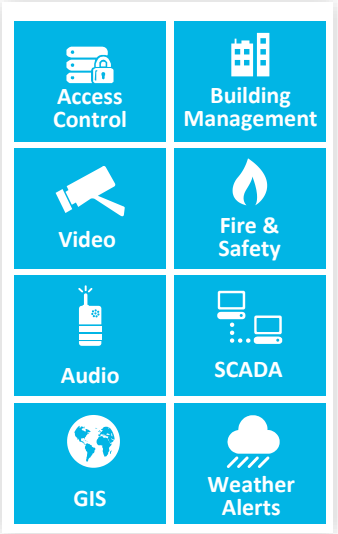
Vyhodnocování dat

- Video – pokročilá videoanalýza, detekce obličejů ,postavy, chůze
- Operační střediska – pulty centrální ochrany jsou nahrazovány sofistikovanými systémy
- Korelace dat
- Inteligence – scénáře, postupy, automatické reakce
- Sdílení relevantních dat
- Přehledy, reporty, analýzy
- Predikce

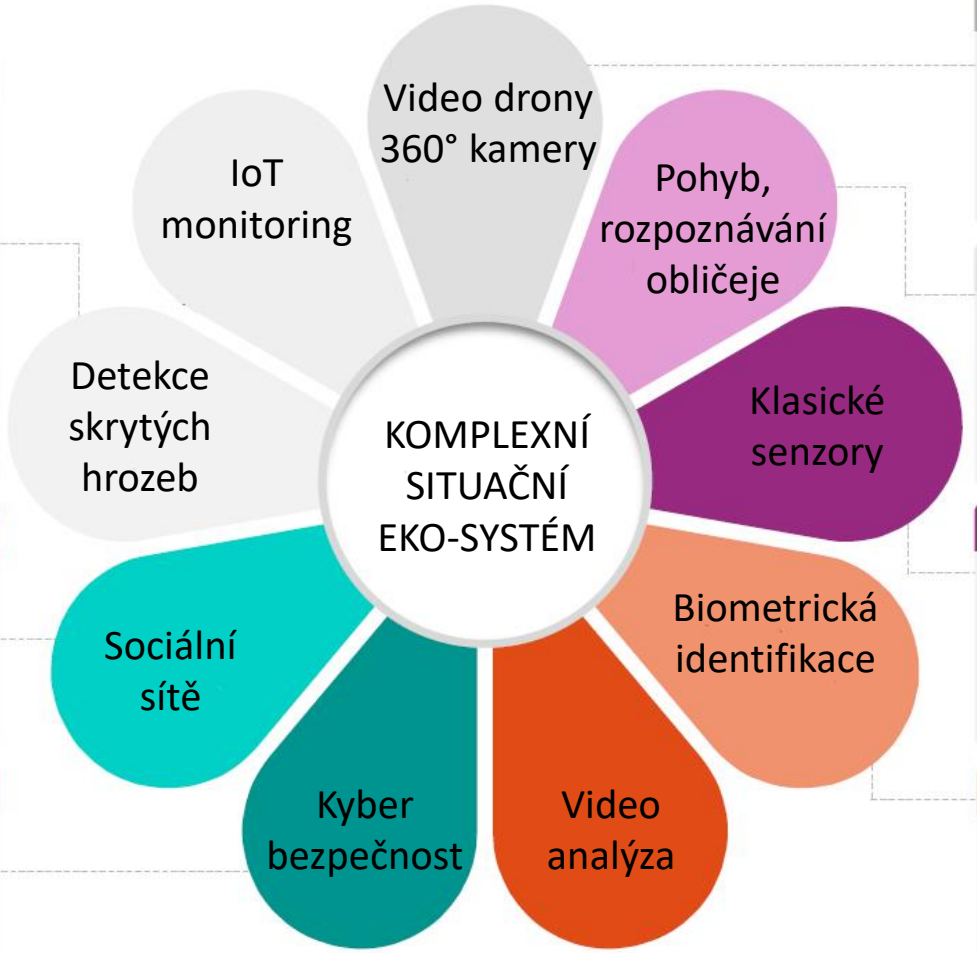


Zdroje dat pro oblast bezpečnosti

- Klasické systémy a čidla (PZTS, EPS, EKV…)
- Kamery
- Biometrické systémy
- Systémy v budovách (výtahy, klimatizace…)
- IT systémy (SIEM, logování…)
- 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…)



Komplexní situační ekosystém



Detekce zbraní

Real – time detekce předmětů, skenování lidí

Sociální nepokoje

Získávání informací ze sociálních sítí

Kyber bezpečnost

Sledování přístupu k serverům, datům atd.

Rozšířený pohled

Narušení přístupu

Rozpoznávání obličejů, black / white listy

Klasické detektory

Kamery, EPS
PZTS, perimetr,
EKV, panic tlačítko

Identifikace přístupu

Security 3.0

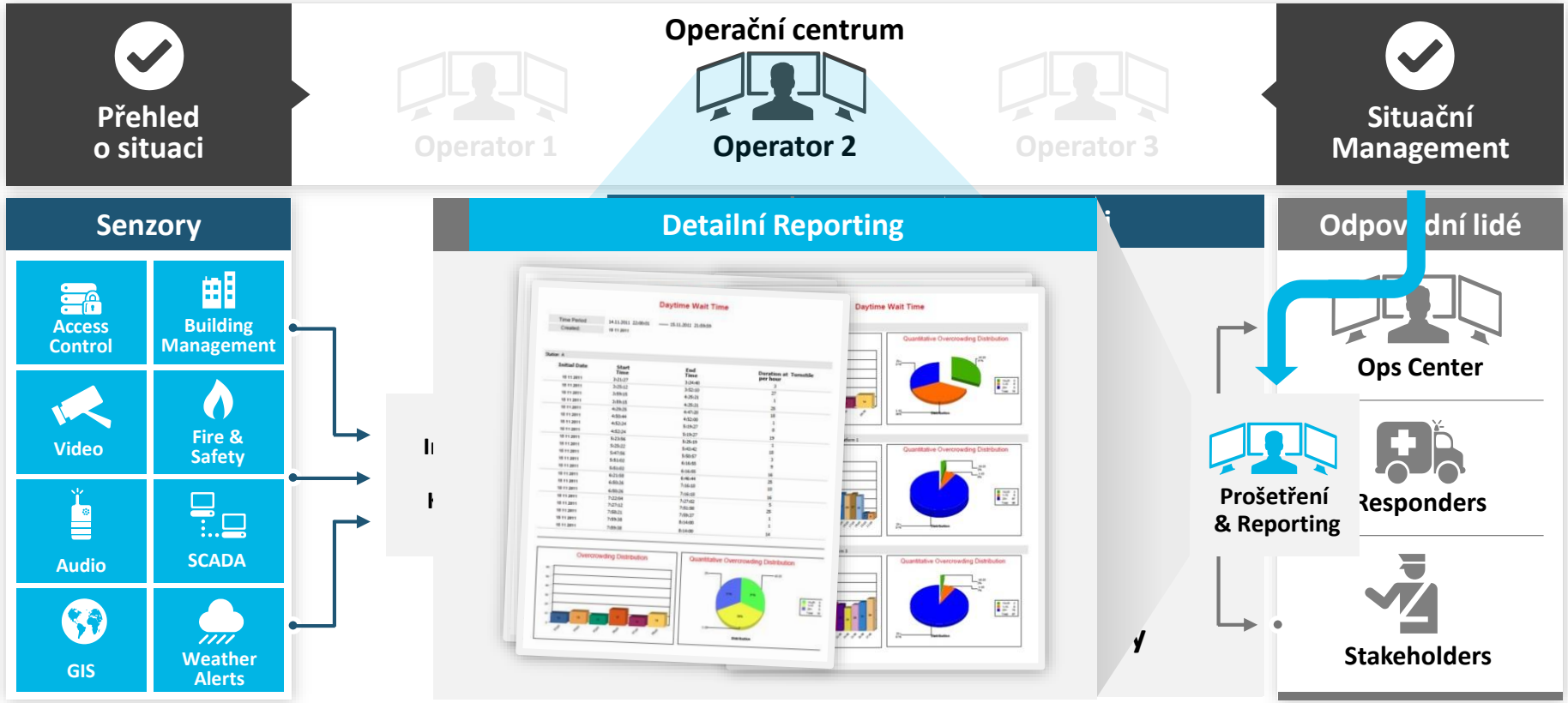
Umožňuje pochopit a využít velké množství různorodých dat

Nabízí potřebné informace těm správným lidem ve správný čas

Optimalizuje správu bezpečnosti, minimalizuje risk

Security 3.0

Informační management konvergované bezpečnosti

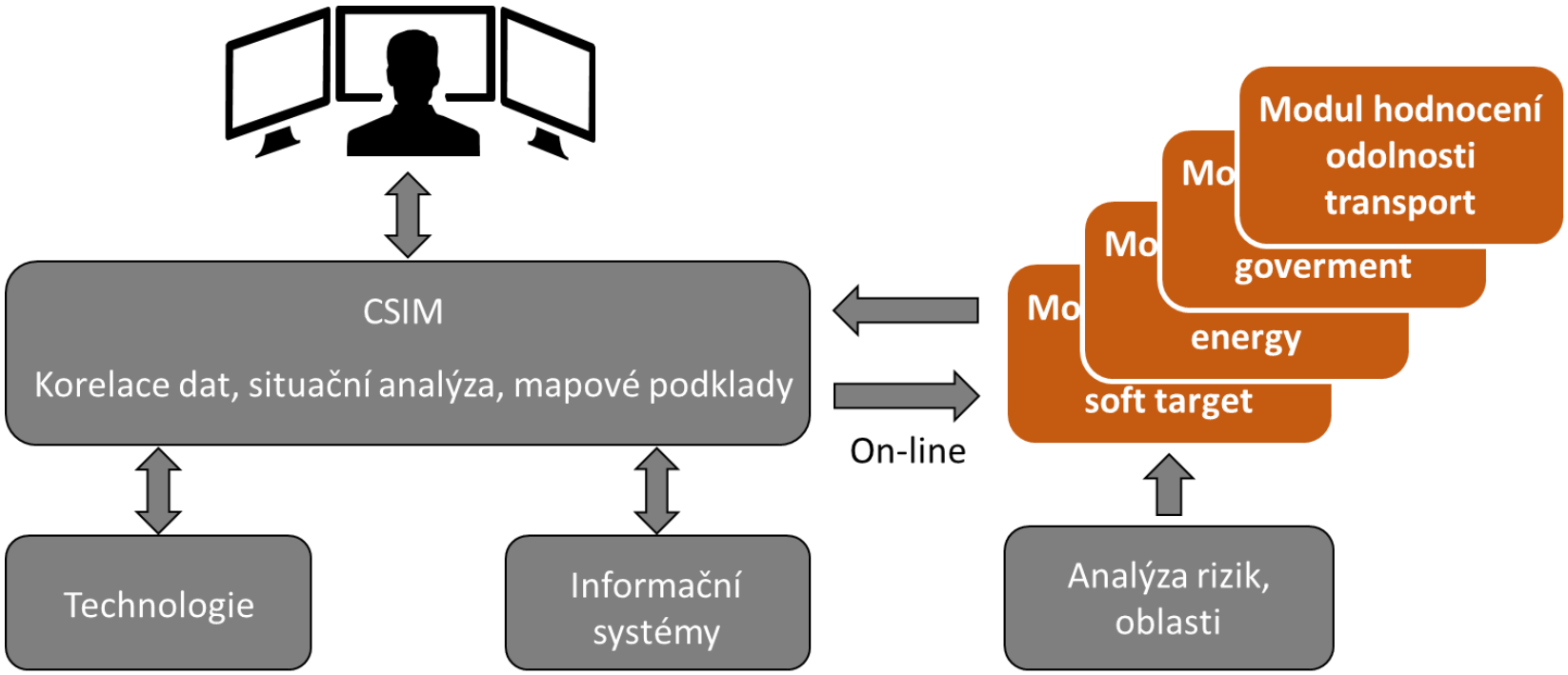


Možnosti rozšíření

Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

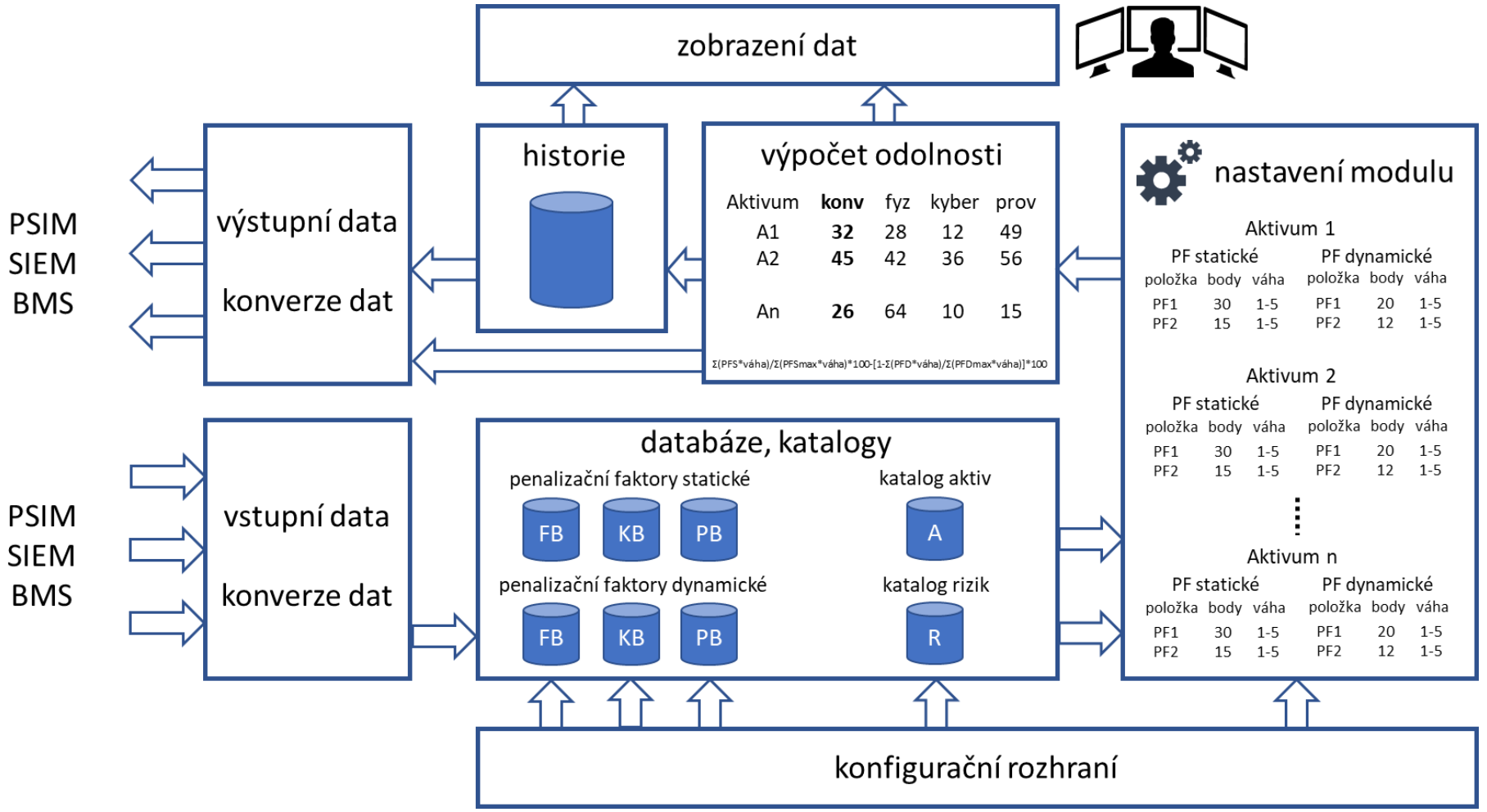
VI20172019054



Modul hodnocení odolnosti

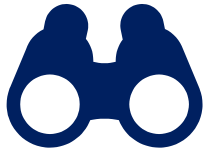
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

VI20172019054



Klíčové body pro úspěšné nasazení CSIM

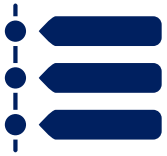
CSIM = Converged Security Information Management



Jasně si předem stanovit, co chci řešit

Investovat pouze do integrací nezbytných pro daný záměr

Mapování klíčových organizačních procesů a uživatelů

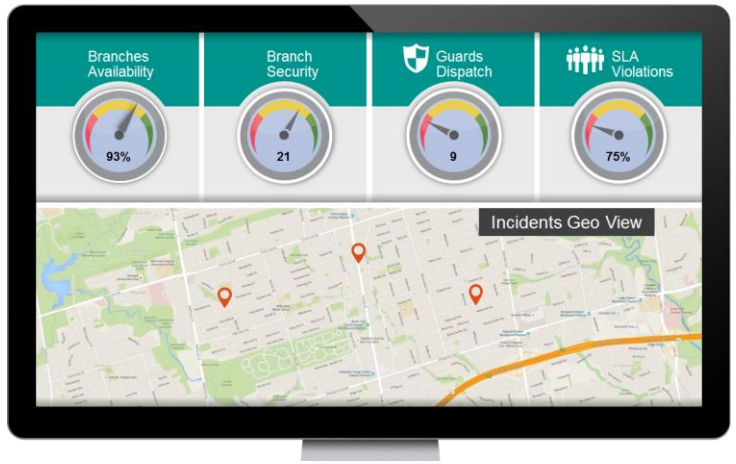


Rozvíjet pouze tak rychle, jak je schopna organizace absorbovat

Školení uživatelů, podpora využívání systému

Průběžné sledování a vylepšování

Big data a provozní inteligence

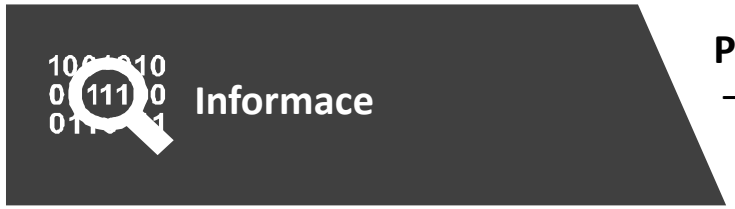


Cesta od dat po provozní inteligenci

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