SOCA
SOC powered by ANECT

ANECT

SOCA & Zákon o kybernetické bezpečnosti

od teorie k praxi

Ivan Svoboda & SOCA

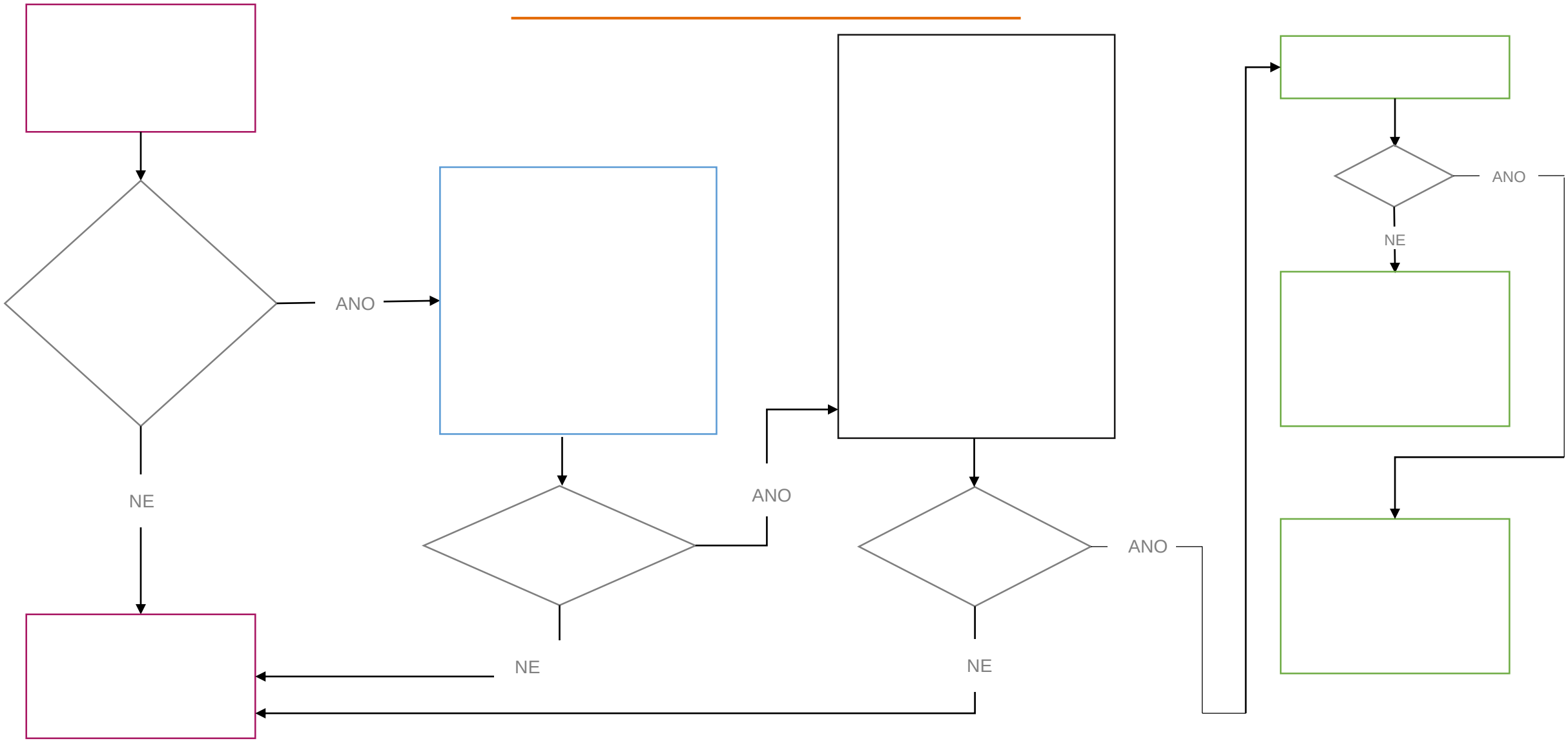
SOCA

SOC powered by ANECT

Týká se vás ZKB?

Nebojte se zeptat

Provedeme vás …



zdroj: nckb

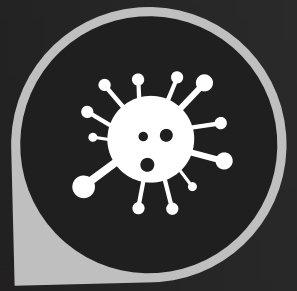
Ne pro zákon, pro bussines

Ochráníte, co vás živí …

… a současně splníte požadavky zákona

Zajímáte ale hackera …

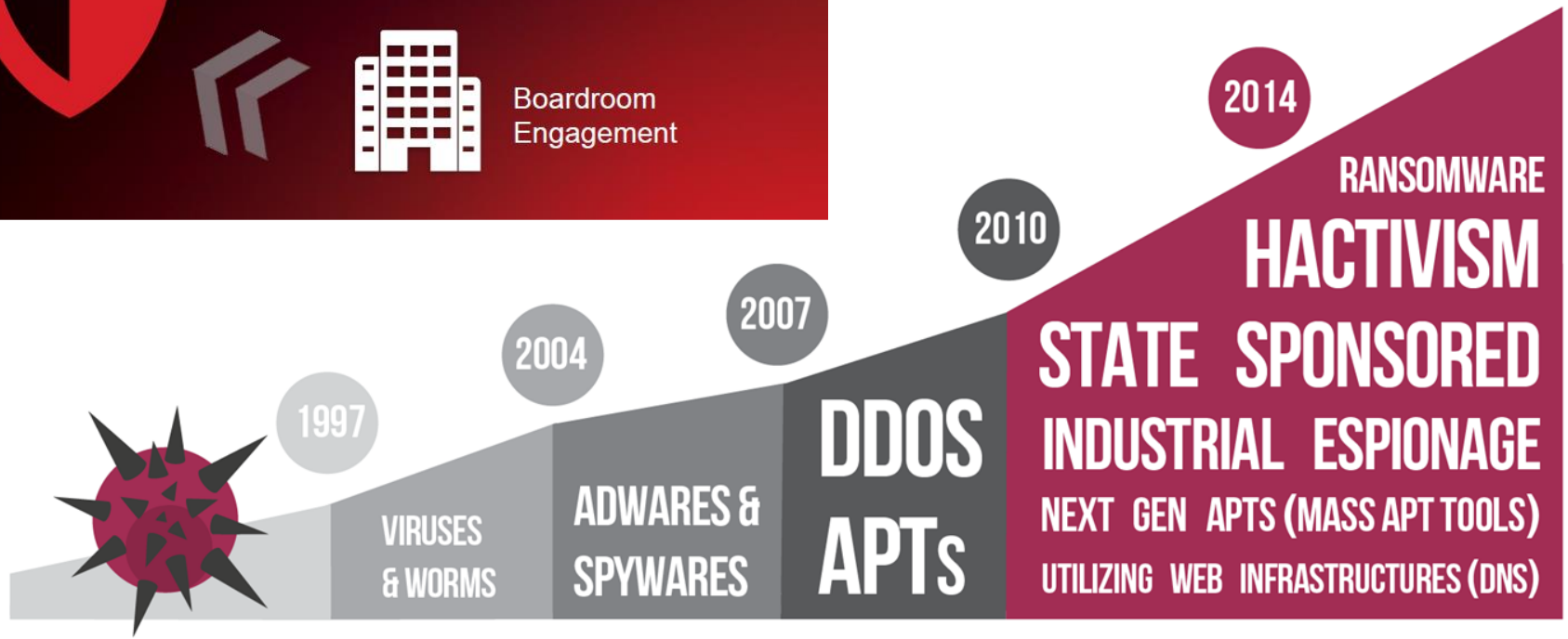
… z druhého konce světa?



Cisco Annual Security Report Summary

Check Point SOFTWARE TECHNOLOGIES LTD.

THREATS



globální reporty můžete mít

české reporty byste měli mít

Hrozby, reporty - ČR

https://www.govcert.cz/cs/informacni-servis/zranitelnosti
https://www.csirt.cz/news/security

globální reporty můžete mít

české reporty byste měli mít

---

vlastní měření musíte mít!

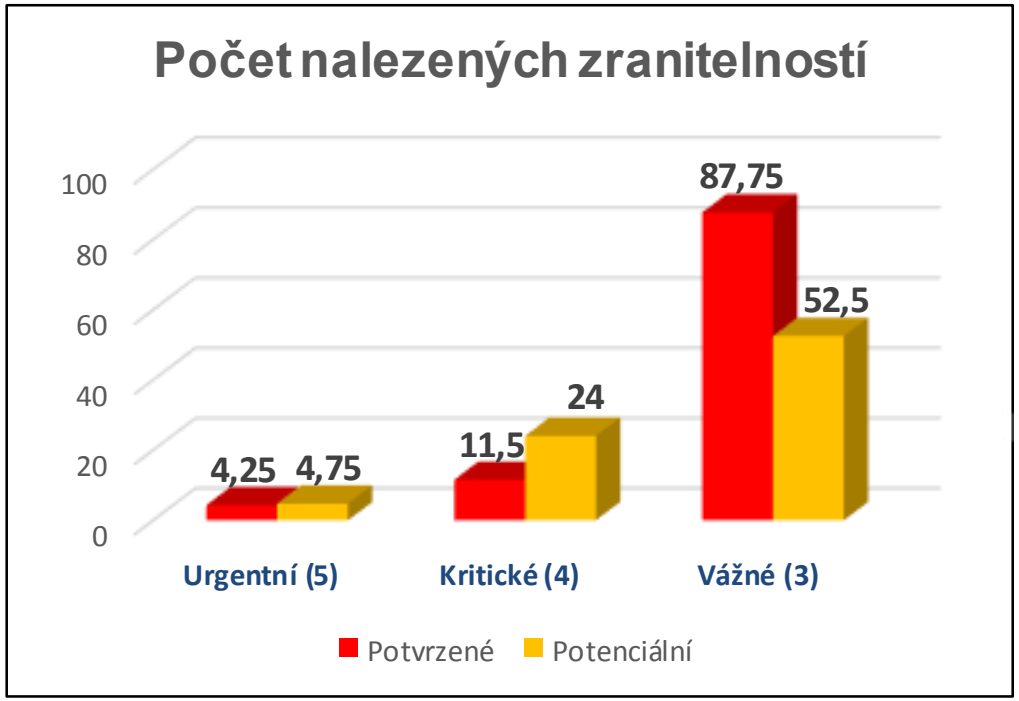
měřte vlastním testováním

SOCA Scan

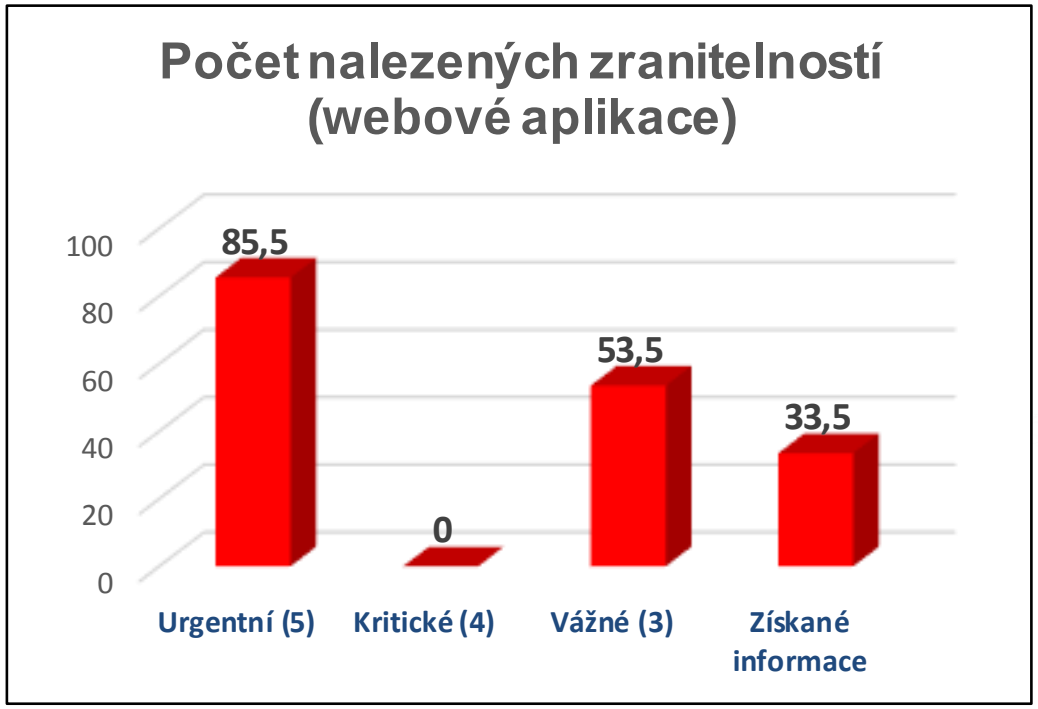

WEB APPLICATION SCAN
ASSET MANAGEMENT (DEVICE INVENTORY)
EXTERNAL VULNERABILITY SCAN
INTERNAL VULNERABILITY SCAN
NETFLOW SCAN
SENSITIVE DATA (DLP SCAN)
PERIMETER SECURITY SCAN

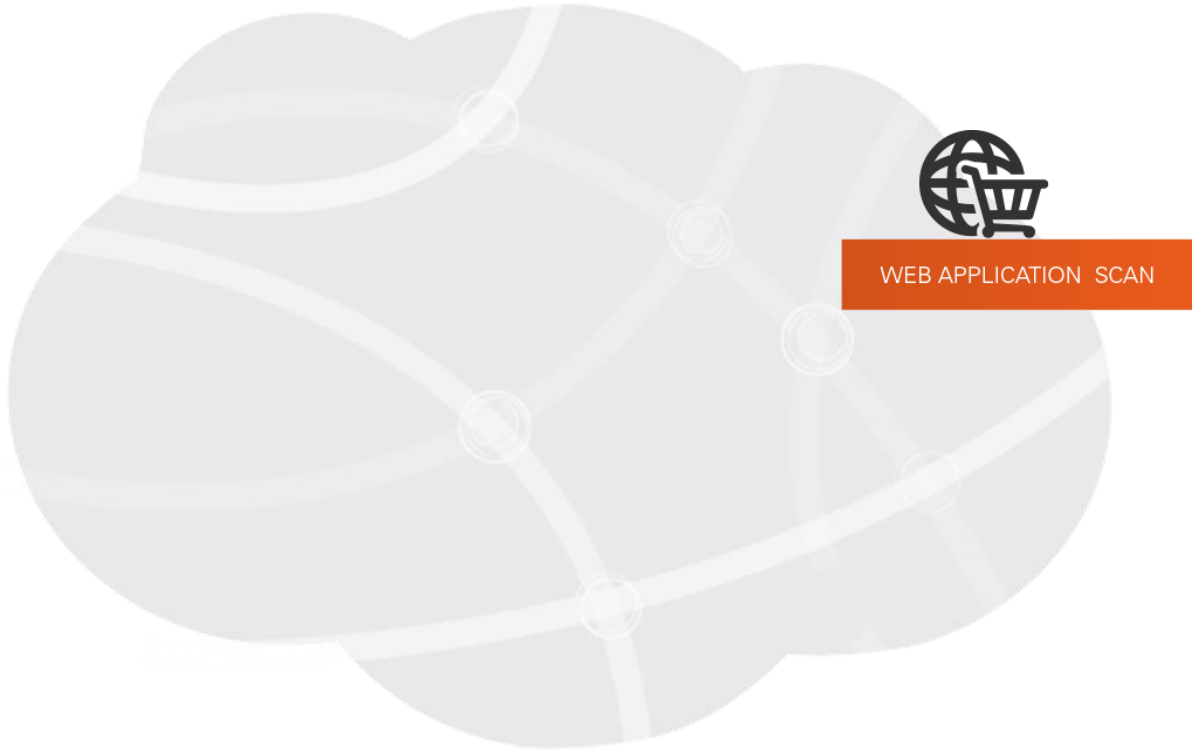
Výsledky testů zranitelnosti

Testy zranitelností: externí & interní

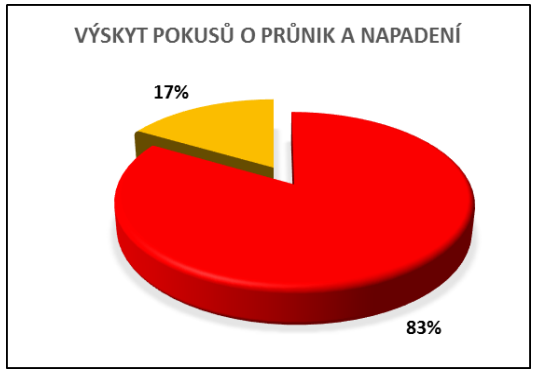


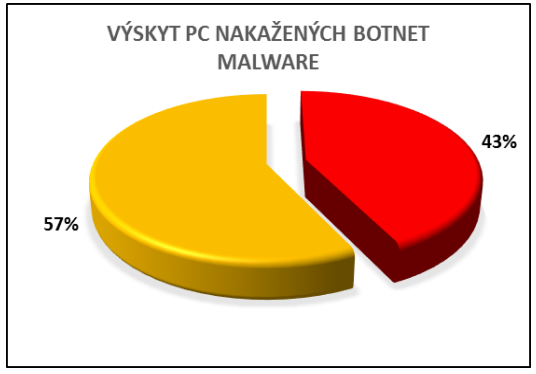
Testy zranitelností webových aplikací





Testy zranitelností: bezpečnost perimetru





otestujte se zdarma

http://www.anect.com/testy-zranitelnosti/

Technologická základna

Bezpečnostní technologie

Security Intelligence, Analytics & GRC

Identity & Access Management

Data Security

Application & Fraud Security

Perimeter / Network Security

Data Center (Server) Security

Endpoint / Device security

High Availability

Physical Security

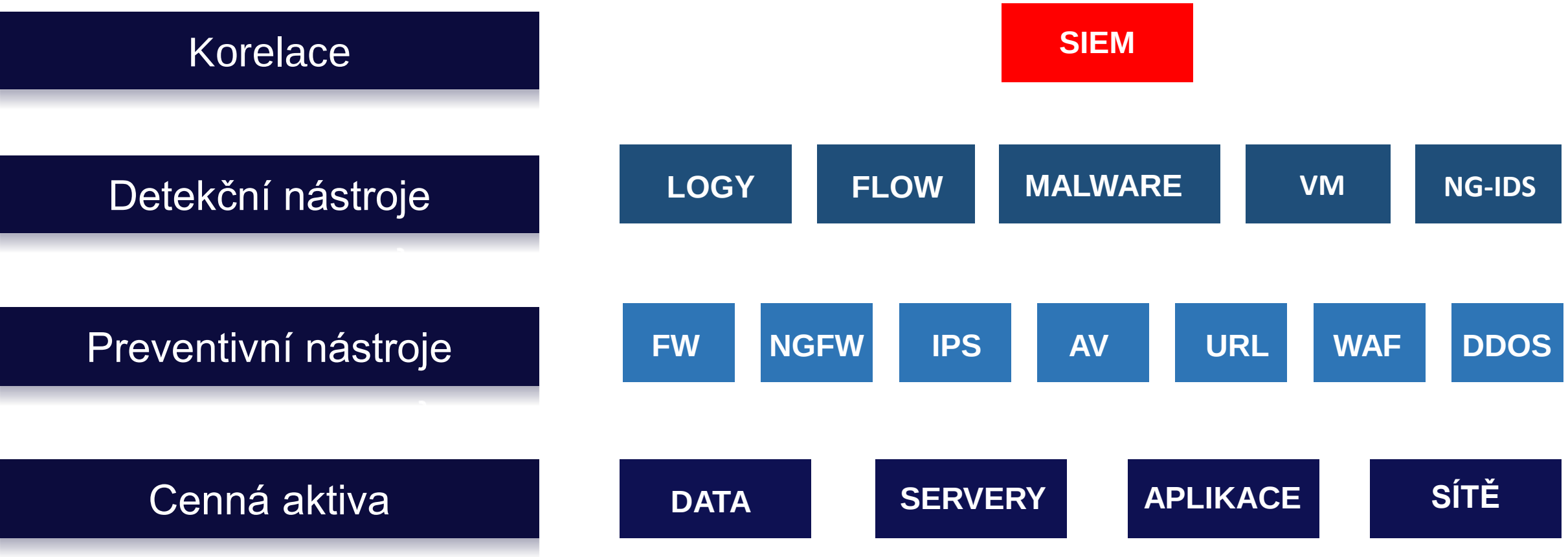
Fáze bezpečnosti

REAKCE — **„mám to pod kontrolou“**

DETEKCE — **„vidím“**

PREVENCE — **„doufám“**

Vaše technologická základna



Vaše technologická základna

Korelace

SIEM IBM

Detekční nástroje

LOGY IBM FLOW inveaTECH MALWARE QUALYS VM NBA CISCO

Preventivní nástroje

FW CISCO NGFW Check Point SOFTWARE TECHNOLOGIES LTD. IPS AV URL WAF f5 DDOS

Cenná aktiva

DATA SERVERY APLIKACE SÍTĚ

ZKB technicko - procesní opatření

ORGANIZAČNÍ OPATŘENÍ

§3 Systém řízení bezpečnosti informací
§4 Řízení rizik
§5 Bezpečnostní politika
§6 Organizační bezpečnost
§7 Stanovení bezpečnostních požadavků pro dodavatele
§8 Řízení aktiv
§9 Bezpečnost lidských zdrojů
§10 Řízení provozu a komunikací
§11 Řízení přístupu a bezpečné chování uživatelů
§12 Akvizice, vývoj a údržba
§13 Zvládání kybernetických bezpečnostních událostí a incidentů
§14 Řízení kontinuity činností
§15 Kontrola a audit kybernetické bezpečnosti

TECHNICKÁ OPATŘENÍ

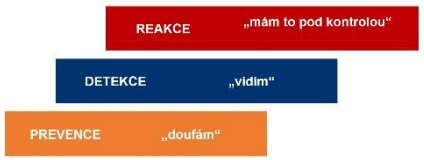
§16 Fyzická bezpečnost
§17 Nástroj pro ochranu integrity komunikačních sítí
§18 Nástroj pro ověřování identity uživatelů
§19 Nástroj pro řízení přístupových oprávnění
§20 Nástroj pro ochranu před škodlivým kódem
§21 Nástroj pro zaznamenávání činností kritické informační ….
§22 Nástroj pro detekci kybernetických bezpečnostních událostí
§23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
§24 Aplikační bezpečnost
§25 Kryptografické prostředky
§26 Nástroj pro zajišťování úrovně dostupnosti
§27 Bezpečnost průmyslových a řídicích systémů

Bezpečnost obecně

PROCESY

TECHNOLOGIE

LIDÉ



SANS TOP 20 Critical Security Controls

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High
13.	Boundary Defense	Moderate
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15.	Controlled Access Based on the Need to Know	Moderate
16.	Account Monitoring and Control	Moderate
17.	Data Loss Prevention	Moderately Low to Moderate
18.	Incident Response Capability	Moderately Low to Moderate
19.	Secure Network Engineering	Low
20.	Penetration Tests and Red Team Exercises	Low

www.sans.org/critical-security-controls

ANECT

NIST CyberSecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Inf. Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

http://www.nist.gov/cyberframework/

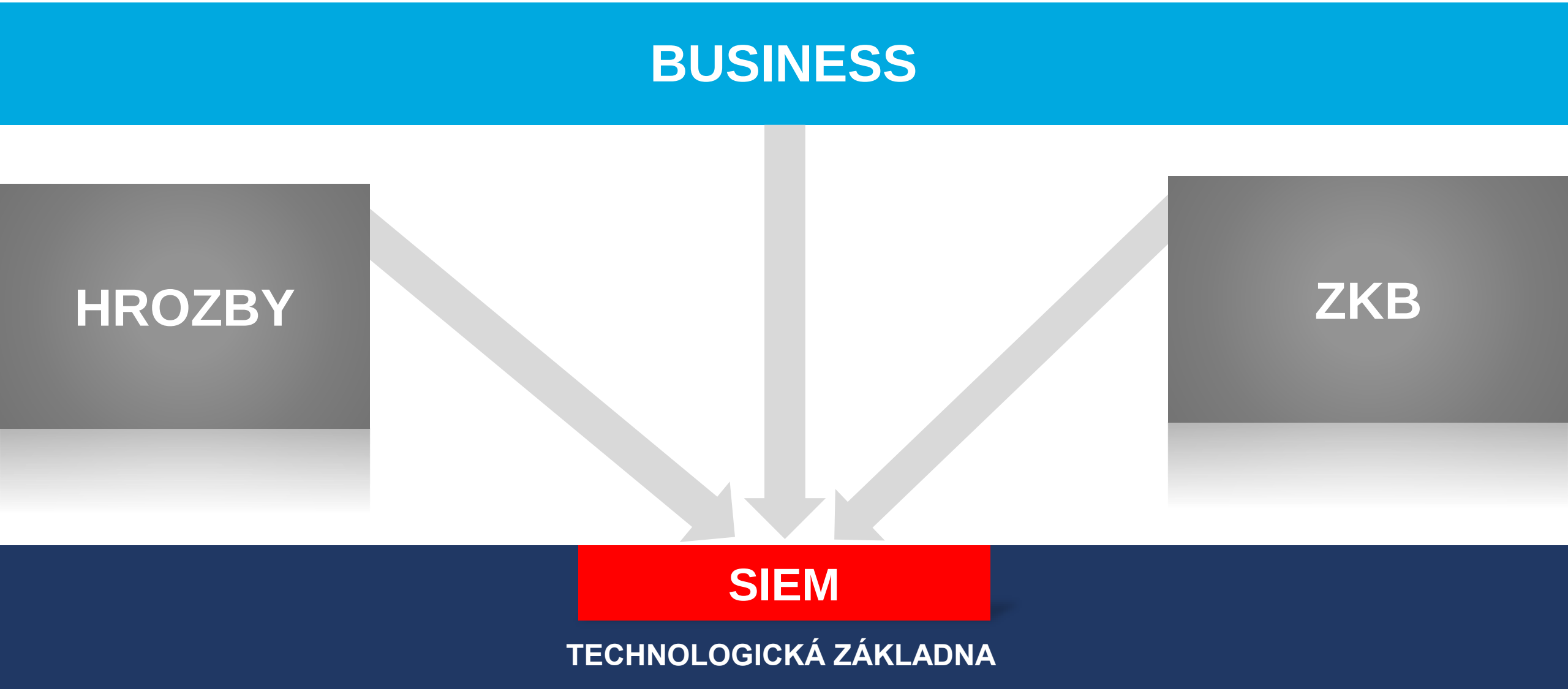
ANECT

Znáte svůj business

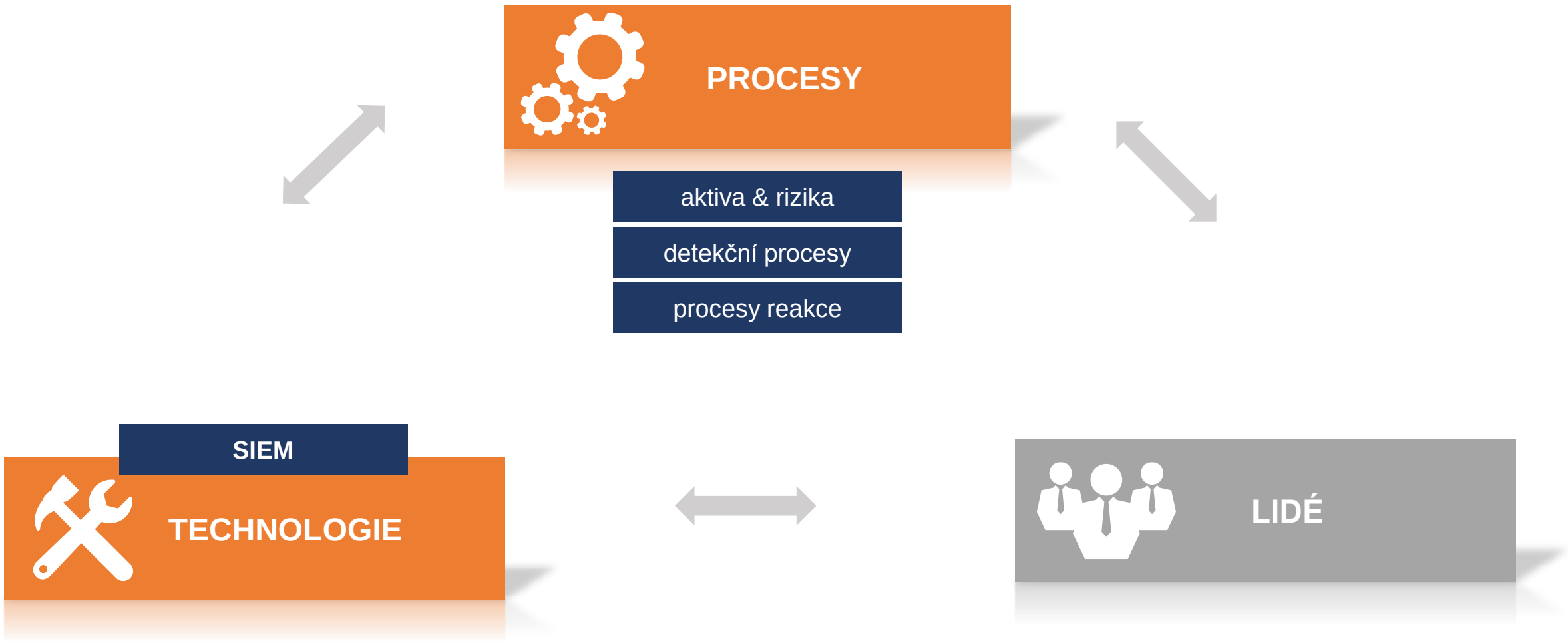
Víte, co vám konkrétně hrozí

Víte, jaké potřebujete technologie

Jak to dát do vzájemné souvislosti?


BUSINESS
HROZBY
ZKB
SIEM
TECHNOLOGICKÁ ZÁKLADNA

Spojení technologií a procesů

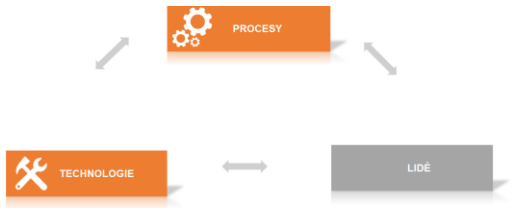


Spojení technologií a procesů

aktiva & rizika

detekční procesy

procesy reakce



Aktiva a rizika

Business -> Aktiva

ZKB –> návod na jejich ohodnocení

Důvěrnost

Dostupnost

Integrita

Aktiva -> Podpůrná aktiva -> Komponenty

Statistiky, skeny, zkušenosti ->Hrozby

ZKB -> návod na analýzu hrozeb

Pravděpodobnost

Zranitelnost

Dopad

ZKB -> návod na vyhodnocení rizika

Hodnota rizika -> Kritičnost události v SIEM

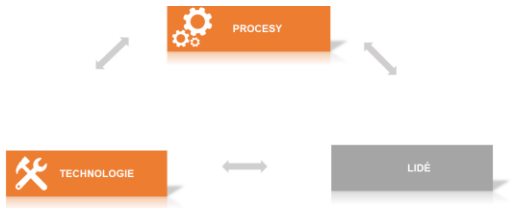
Managed SIEM

Spojení technologií a procesů

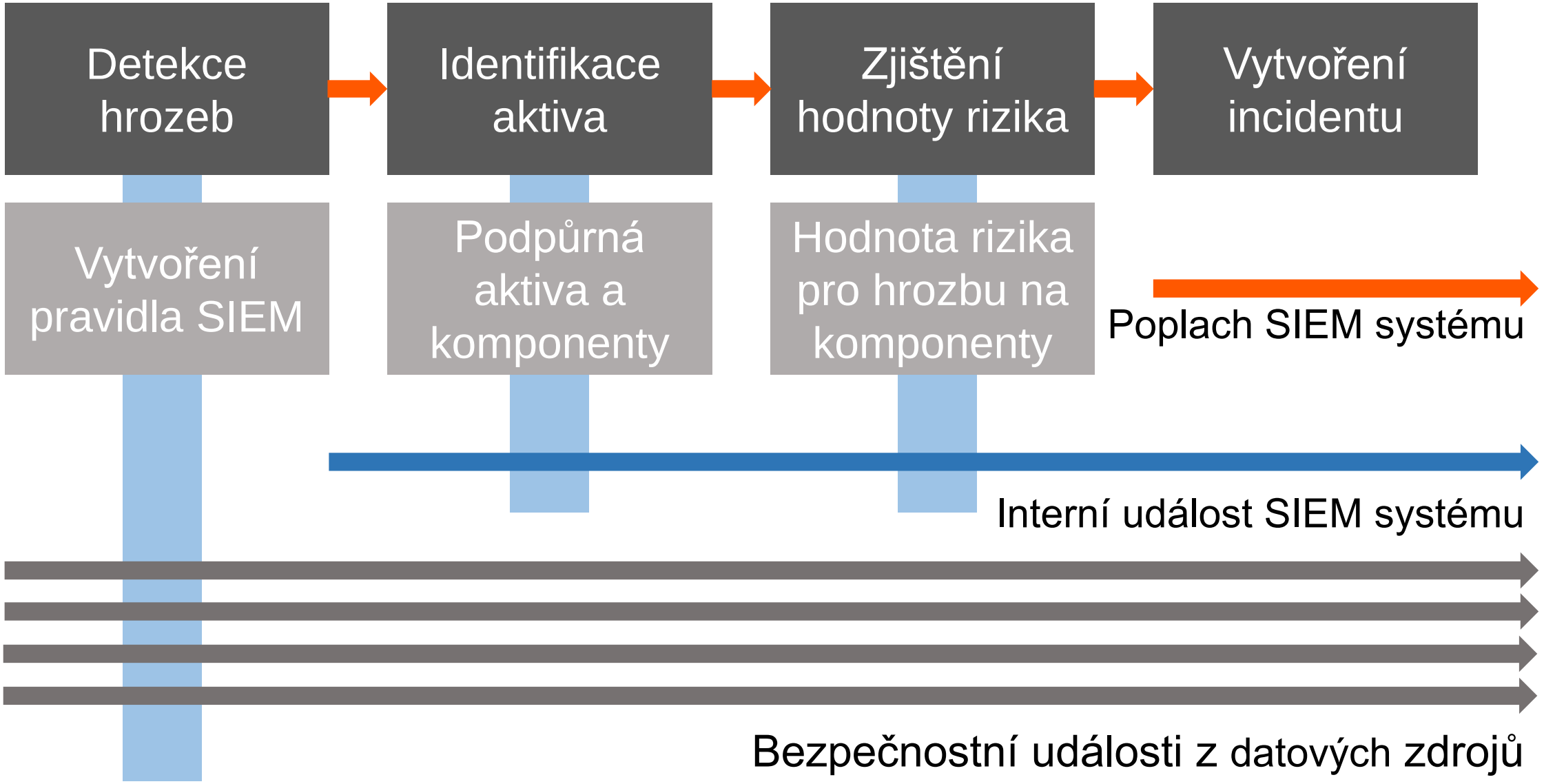
aktiva & rizika

detekční procesy

procesy reakce



Detekční procesy

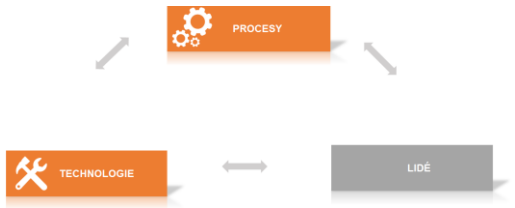


Spojení technologií a procesů

aktiva & rizika

detekční procesy

procesy reakce



Procesy reakce a lidé

Procesní podpora

SOCA používá provozní procesy podle ITIL a Servicedesk

Role

Manažer KB

Architekt KB

Auditor KB

Vlastníci aktiv

Administrátor

Operátor

Analytik

Manažer

Všechny role můžete outsourcovat ! SOCA je připravena …


PROCESY
SOCA
TECHNOLOGIE
LIDÉ

Služby SOCA

premium SOCA

mějte vše pod kontrolou

active SOCA

buďte aktivní

start SOCA

nebojte se začít

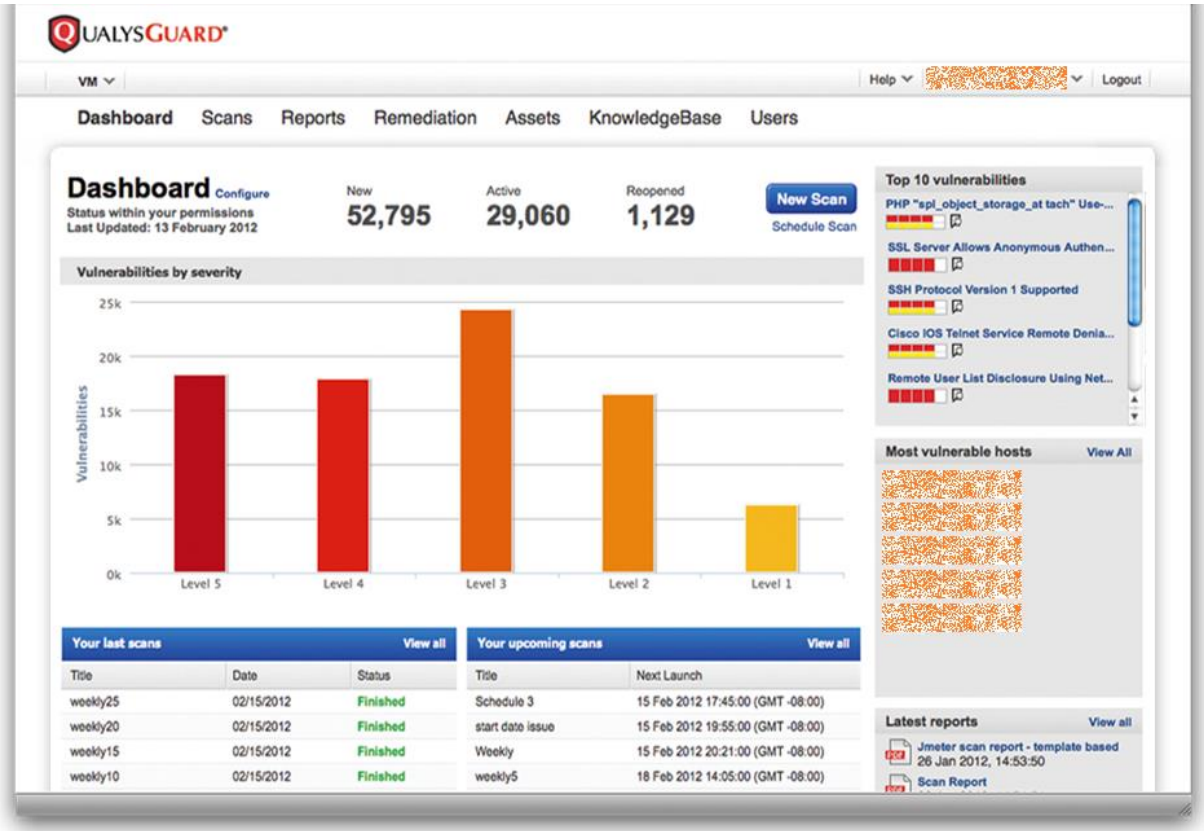
scan SOCA

zjistěte, jak jste na tom

technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace

SOCA v praxi



ACCESS CONTROL & DATA PROTECTION

30,670	High Risk Applications Events
22	Data Loss Events

THREAT PREVENTION

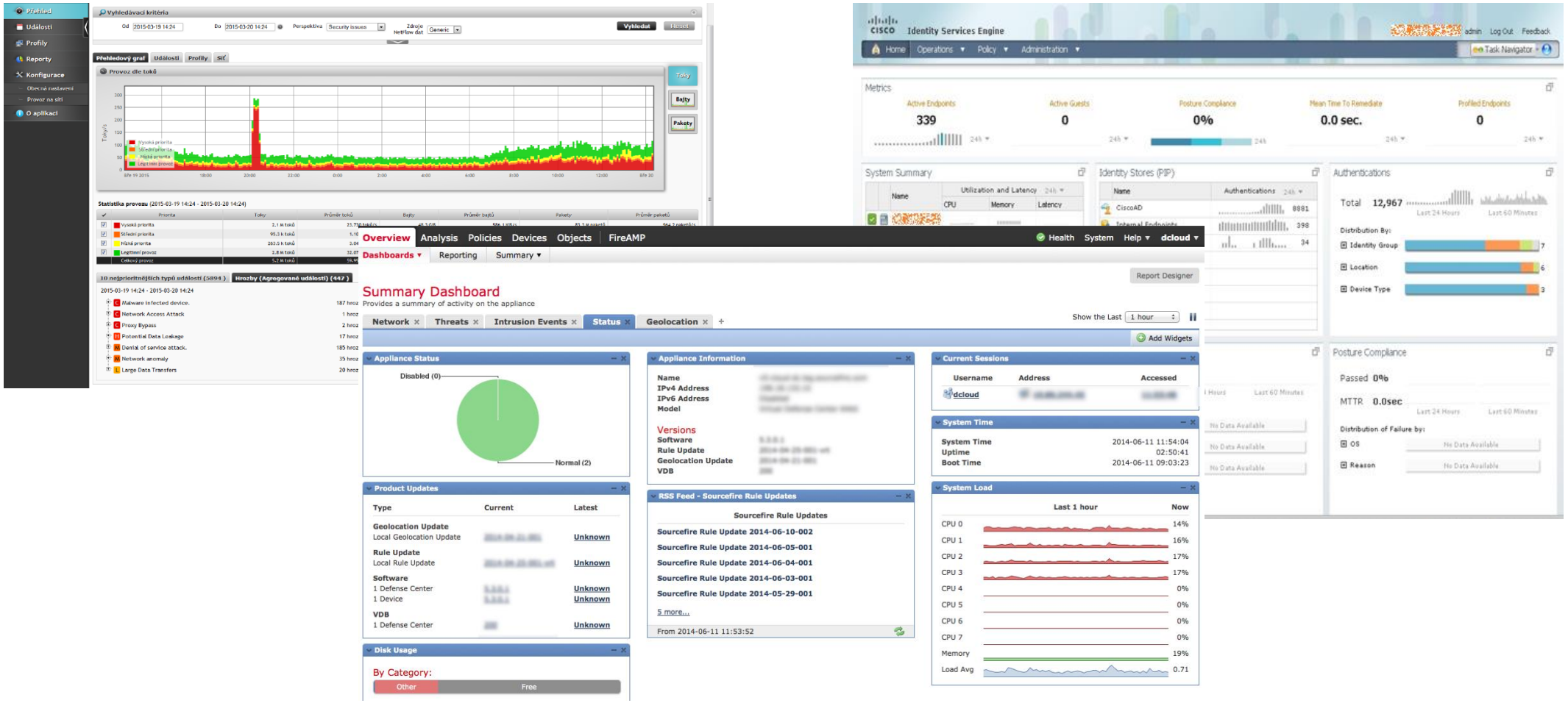
9	Bot Events
5	Viruses Events
16	Zero-day Events
18	Intrusions & Attacks Events

ENDPOINT

893	Endpoints Involved in High Risk Events

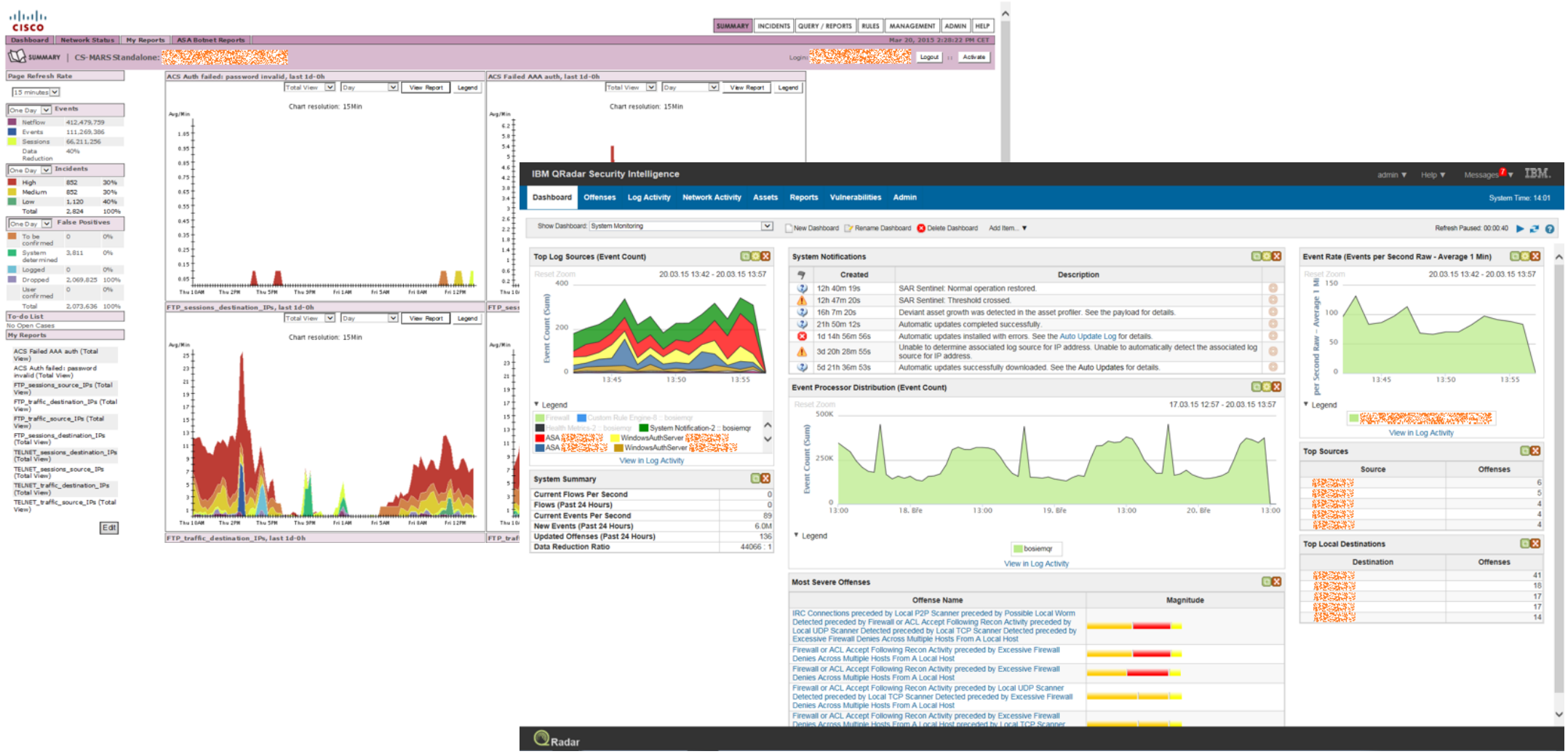
COMPLIANCE

65%	Compliant with Check Point Best Practices
58%	Compliant with Regulatory Requirements



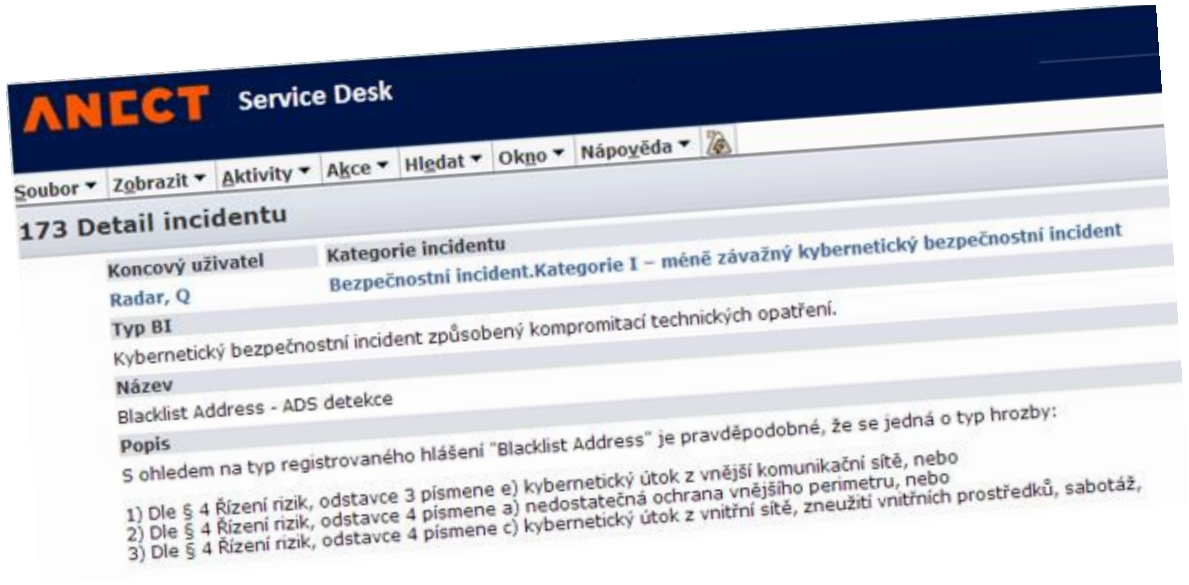
technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace



technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace

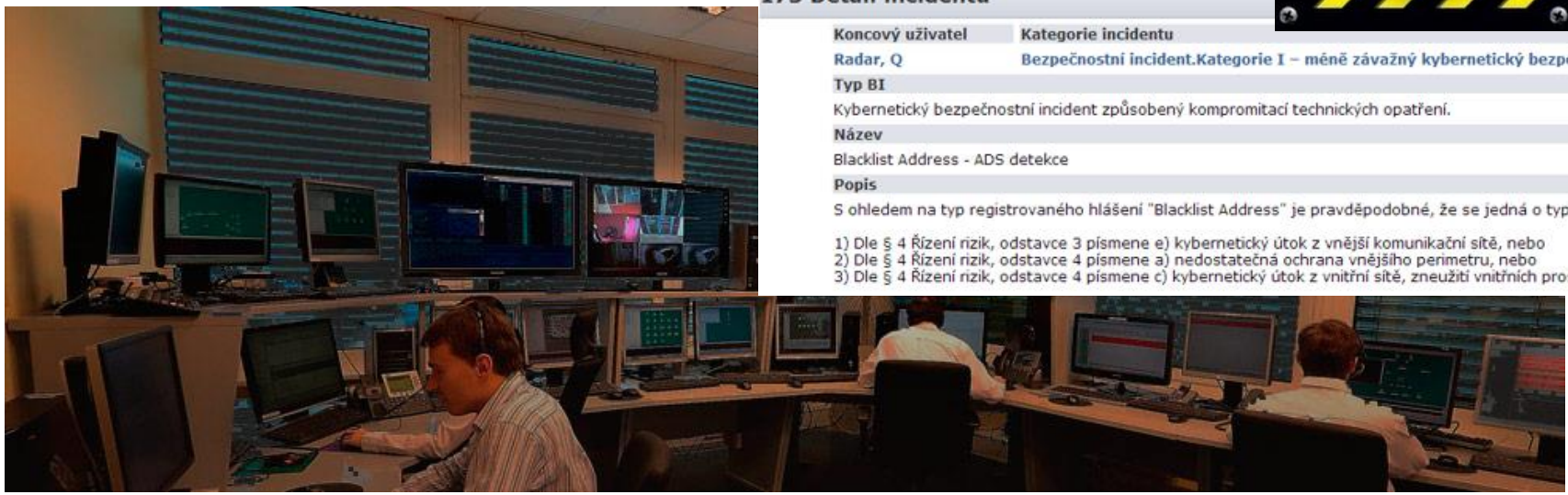


start SOCA

technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace

premium SOCA



active SOCA

start SOCA

technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace

Potřebujete pomoc se ZKB ?

Chcete zjistit, co vám konkrétně hrozí ?

Potřebujete technologie, procesy, role, lidi ?

Chcete trvale vidět, rozumět a reagovat ?

SOCA

SOC powered by ANECT

Ivan.Svoboda@anect.com

Děkuji za pozornost

Ivan.Svoboda@anect.com