

ANECT

SOCA & Zákon o kybernetické
bezpečnosti

od teorie **k praxi**

Ivan Svoboda & **SOCA**



SOCA
SOC powered by ANECT

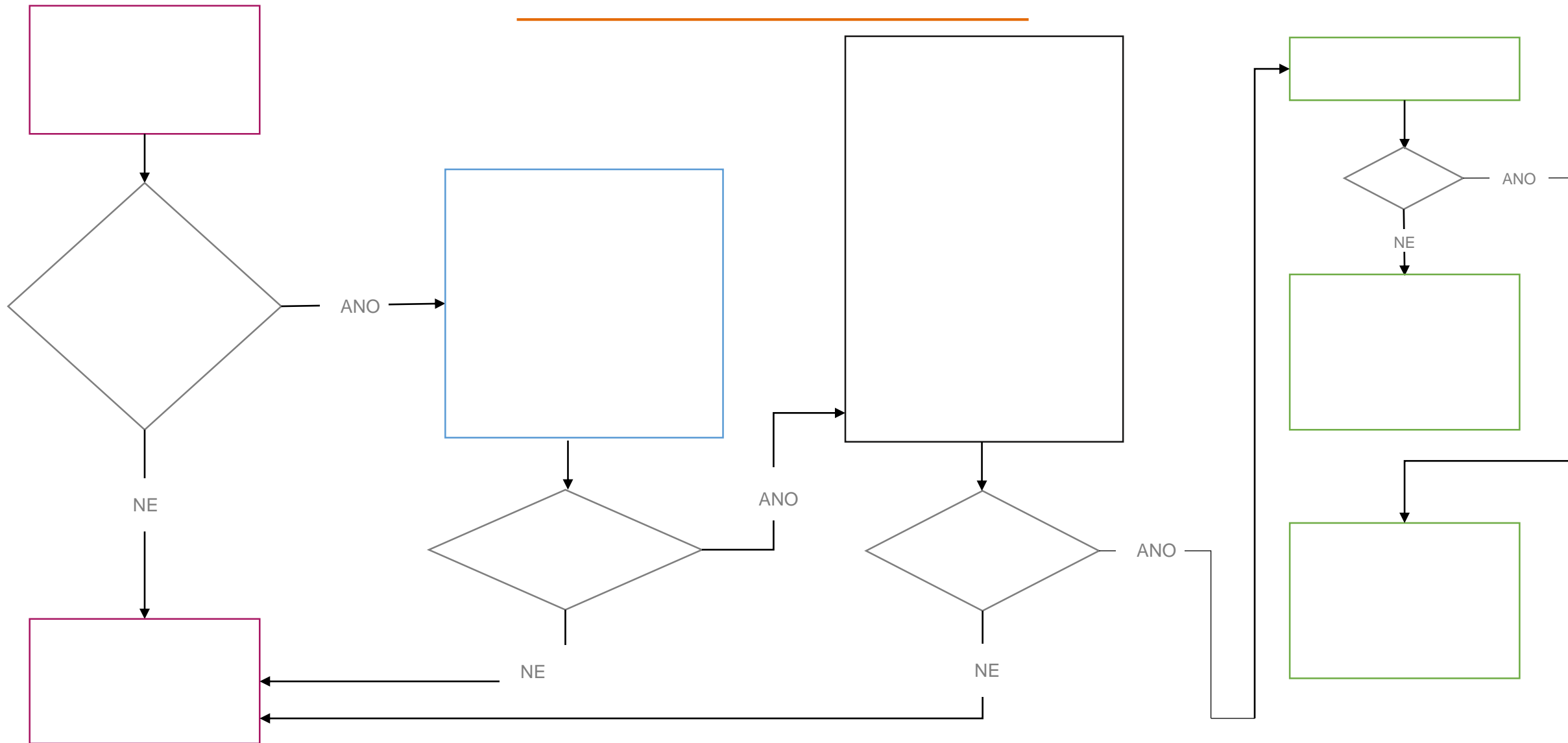


Týká se vás **ZKB**?



Nebojte se zeptat

Provedeme vás ...



Ne pro zákon, pro **bussines**

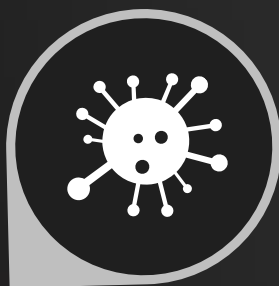
Ochráníte, co vás **živí** ...

... a současně **splníte** požadavky zákona



Zajímáte ale hackera ...

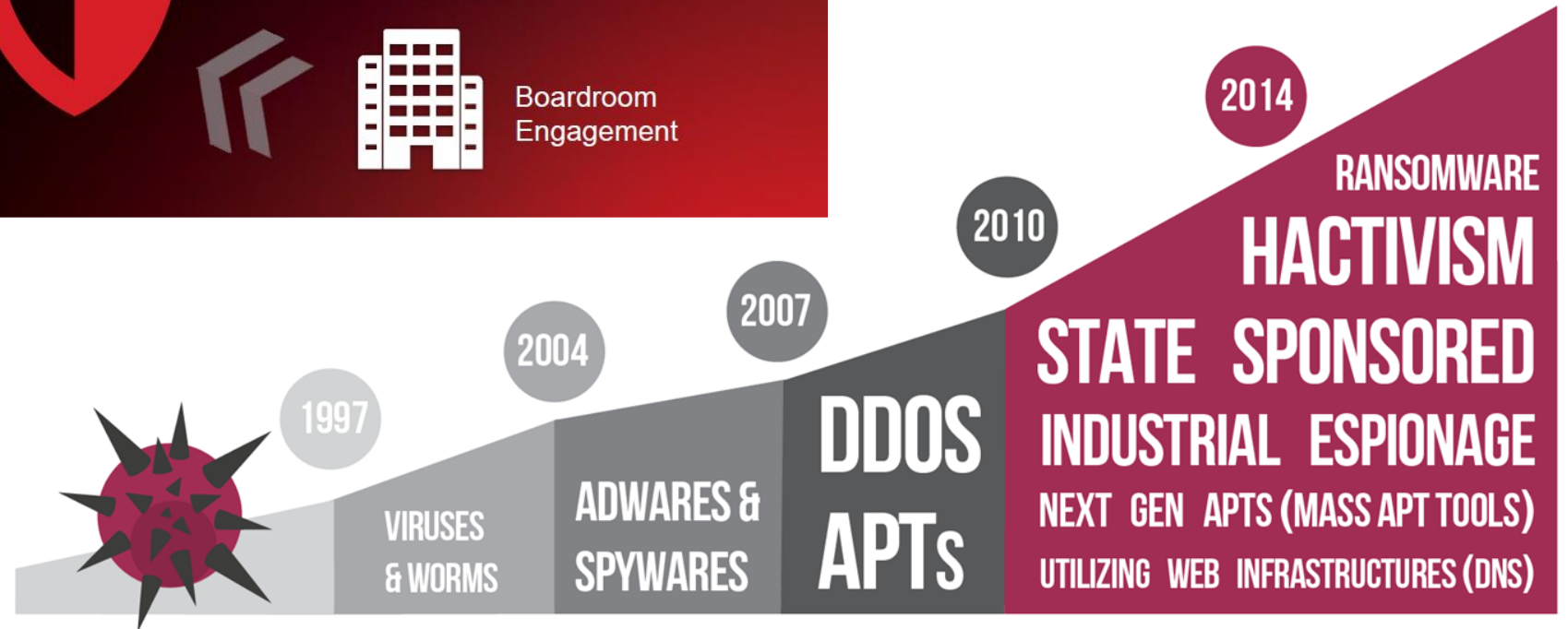
... z druhého konce světa?



Cisco Annual Security Report Summary



THREATS



globální reporty můžete mít

české reporty byste měli mít

Hrozby, reporty - ČR

MojeID | Jak na Internet | Doménový prohlížeč | Edice | Akademie | Laboratoře | Dobrá doména | Háčky čárky | CSIRT.CZ | Turris | Katalog routerů

CSIRT.CZ powered by CZ.NIC

AKTUÁLNĚ Z BEZPEČNOSTI

- HLÁŠENÍ INCIDENTU
- RADY A NÁVODY
- ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

ENGLISH / ČESKY

Hledat...

Aktuálně z bezpečnosti (RSS)
Další informace k bezpečnosti najdete také na webu NCKE

OpenSSL oznámilo vydání záplaty pro vysoce kritickou zranitelnost
17.03.2015 16:44
Nová verze OpenSSL, která má vyjít ve čtvrtek, bude opravovat několik závažných bezpečnostních zranitelností a jednu, která je označována jako **velmi nebezpečná**.

Qualys spustila API rozhraní služby SSL Labs pro automatické testování webových stránek
17.03.2015 16:35
Společnost Qualys **oznámila** dostupnost API rozhraní pro svou službu SSL Labs. Toto rozhraní je zdarma dostupné pro nekomerční využití. Dostupná je také open source aplikace pro příkazovou řádku, která slouží jako referenční klient pro toto API.

Microsoft znovu záplatuje chybu LNK, která umožňovala šíření Stuxnetu
13.03.2015 13:13
Bezpečnostní bulletin nedávno vydaný společností Microsoft **řeší chybu v zobrazování LNK souborů**, která byla využívána Stuxnetem, a kterou jsme mylně považovali od roku 2010 za opravenou. Nová záplata byla již vydána a doporučuje se ji co nejdříve aplikovat.

Společnost Adobe opravuje další kritické zranitelnosti Flash Playeru
13.03.2015 12:44
Společnost Adobe **uvolnila bezpečnostní záplaty** pro bezmála deset závažných bezpečnostních problémů týkajících se verzi Flash Playeru pro Windows, Mac i Linux.

Pozor na nový virus vydávající se za Seznam E-mail aplikaci
12.03.2015 18:21
Počítačová piráta **zkoušejí novou taktiku**, která by jim pomohla otevřít cestu k cizím bankovním účtům. Šíří internetem počítačový virus, který se vydává za oficiální aplikaci Seznam E-mailu. Díky němu se dokážou vypořádat i s procesem ověřování plateb prostřednictvím SMS zpráv. Hrozbu by proto lidé neměli v žádném případě podceňovat.

Zranitelnost pluginu 'WordPress SEO by Yoast' se týká milionů stránek

ACCREDITED BY TRUSTED INTRODUCEE

Úvodní stránka | Mapa serveru | Textová verze | English

národní centrum kybernetické bezpečnosti

ÚVOD | VLÁDNÍ CERT | RKB | **INFORMAČNÍ SERVIS** | LEGISLATIVA | KII / VIS | ODKAZY | KONTAKTY

Úvodní stránka » Informační servis » Zranitelnosti

Zranitelnosti

- Akce a události
- Publikace
- Strategie a Akční plán
- Pracovní příležitosti
- RSS
- Informace CSIRT.CZ
- Výkladový slovník

Zranitelnosti

- 11.03.2015 [FREAK – Společnosti Apple a Microsoft vydaly opravy zranitelnosti](#)
- 06.03.2015 [FREAK – nová zranitelnost SSL/TLS](#)
- 02.03.2015 [JetLeak – zranitelnost v zabezpečení webového serveru Jetty](#)
- 23.02.2015 [Samba - kritická zranitelnost](#)
- 18.02.2015 [Zranitelnosti v návrhovém prostředí Siemens TIA Portal \(Step 7\) a systému WinCC](#)
- 09.02.2015 [Podvodné e-maily s nebezpečnou přílohou](#)
- 05.02.2015 [Internet Explorer 11 ohrožen XSS zranitelností nultého dne](#)
- 30.01.2015 [Upozornění na možné riziko zvýšeného zatížení webových serverů](#)
- 29.01.2015 [Ghost - kritická zranitelnost linuxové knihovny glibc](#)
- 23.01.2015 [Adobe vydal opravu zranitelnosti Flash Playeru](#)
- 22.01.2015 [Angler Exploit Kit útočí na zranitelnost nultého dne Flash Playeru](#)
- 12.01.2015 [Další vlna podvodných e-mailů](#)
- 06.01.2015 [Zranitelnost ve Windows 8.1](#)
- 17.12.2014 [SoakSoak – malware kampaň využívající zranitelnosti WordPress](#)
- 10.12.2014 [POODLE v2.0 – nová zranitelnost využívá protokol TLS 1.2](#)
- 05.12.2014 [WordPress Download Manager - vážná zranitelnost](#)
- 24.11.2014 [DoubleDirect - nový typ útoku Man-in-the-Middle](#)
- 14.11.2014 [Windows Secure Channel \(Schannel\) - kritická zranitelnost](#)
- 07.11.2014 [Rootpipe - kritická zranitelnost Mac OS X](#)
- 03.11.2014 [Drupal - kritická chyba umožňuje SQL injection](#)
- 23.10.2014 [Worm Koler - nová varianta ransomwaru pro mobilní telefony](#)
- 17.10.2014 [POODLE - zranitelnost využívá SSL 3.0 protokol](#)

<https://www.govcert.cz/cs/informacni-servis/zranitelnosti>

<https://www.csirt.cz/news/security>

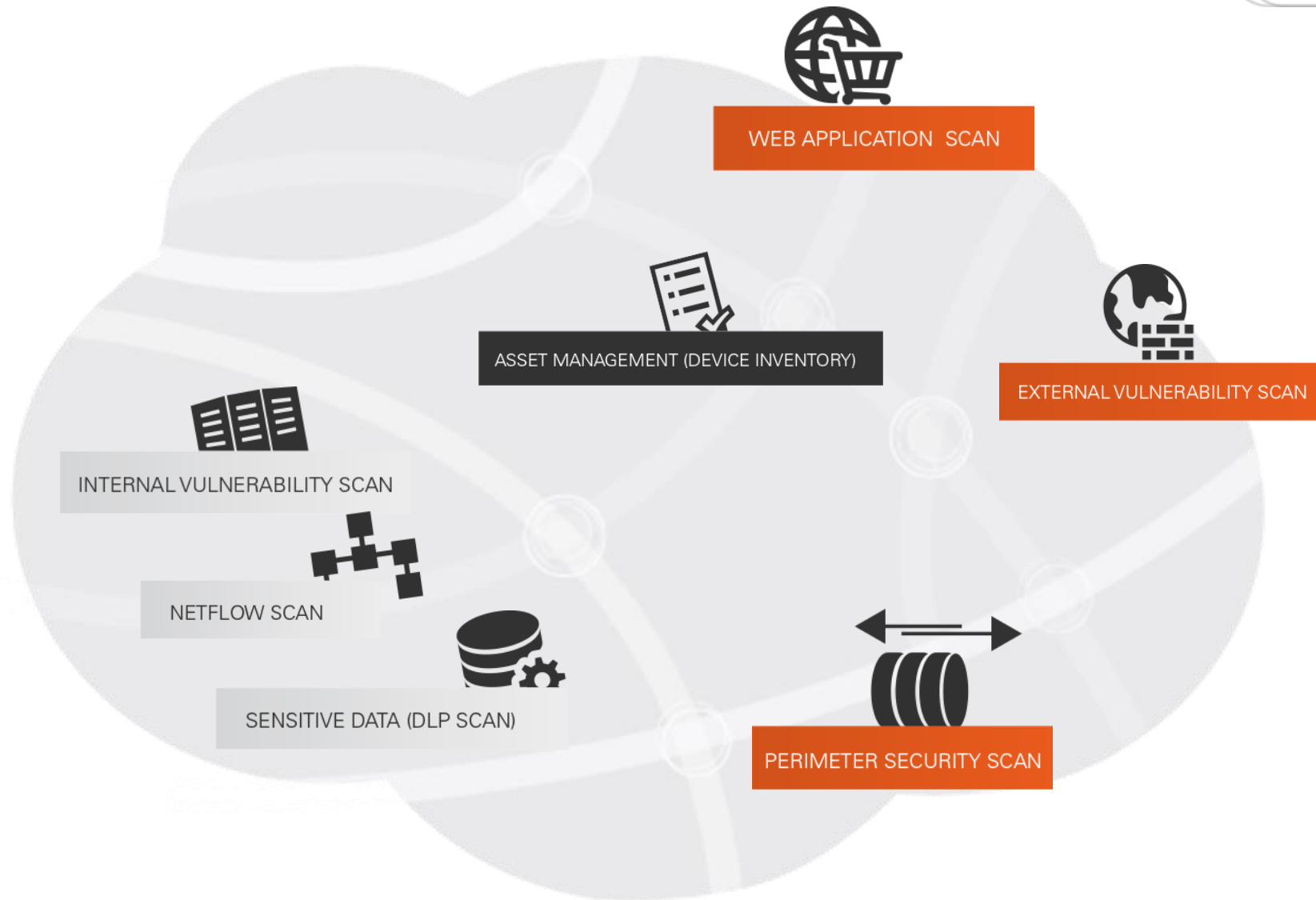
globální reporty **můžete** mít

české reporty **byste měli** mít

vlastní měření **musíte** mít!

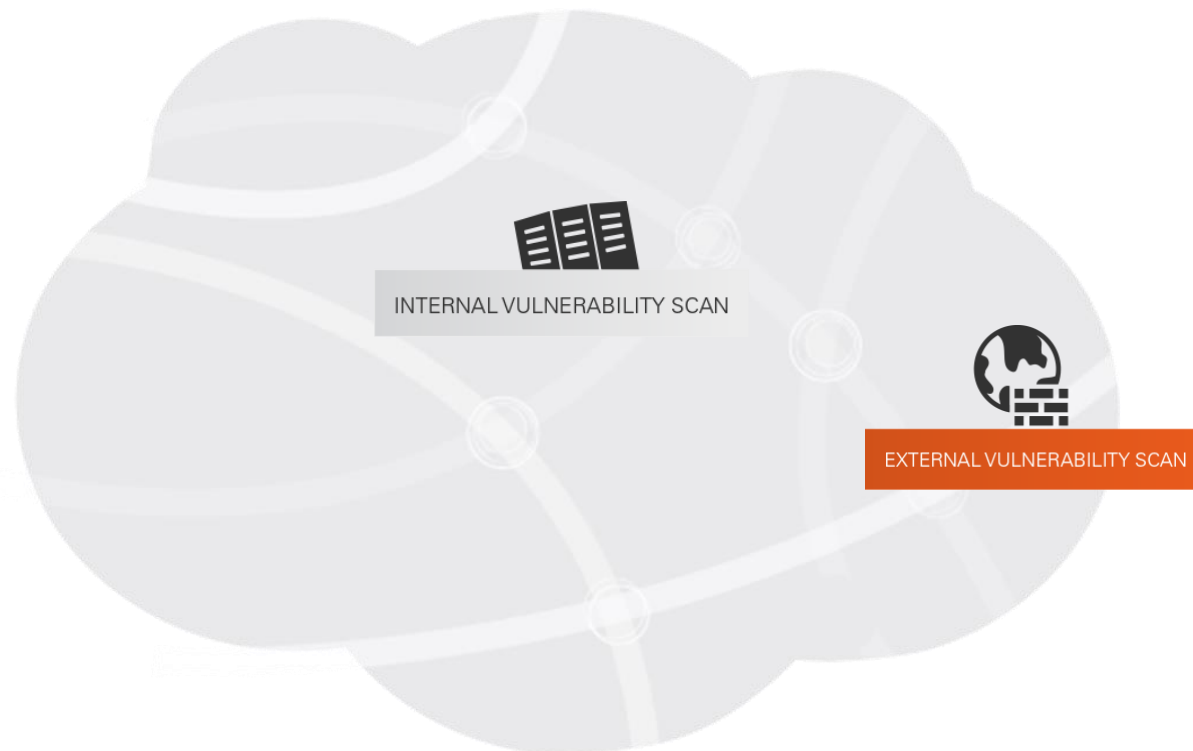
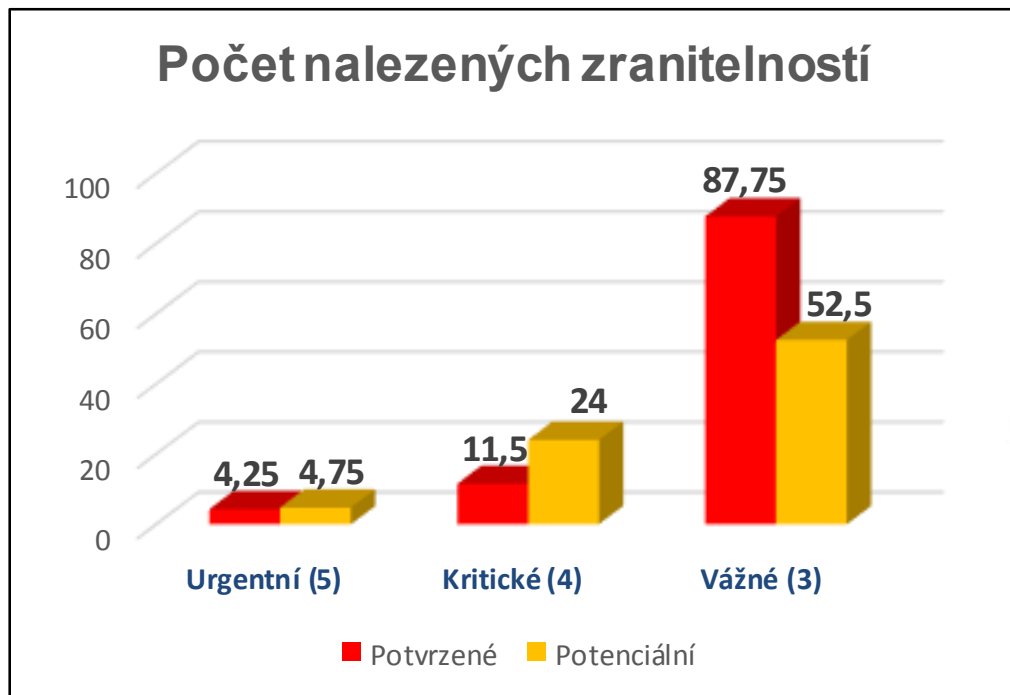
měřte vlastním testováním

SOCA Scan

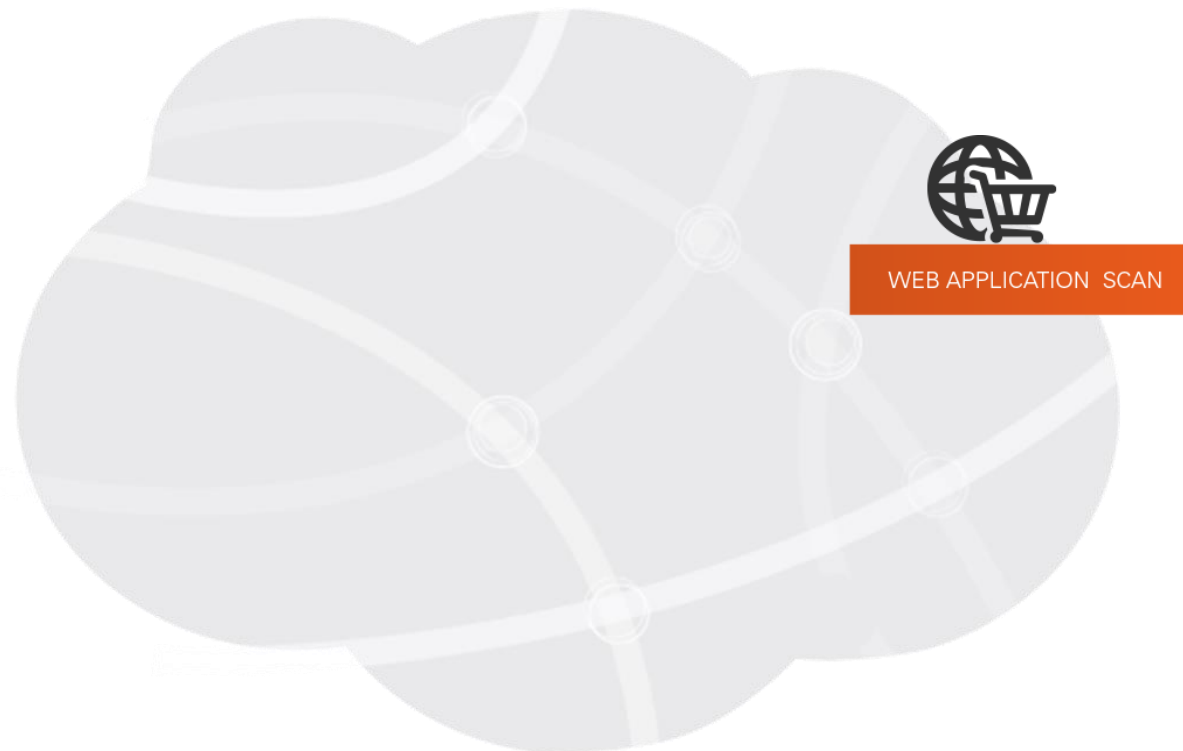
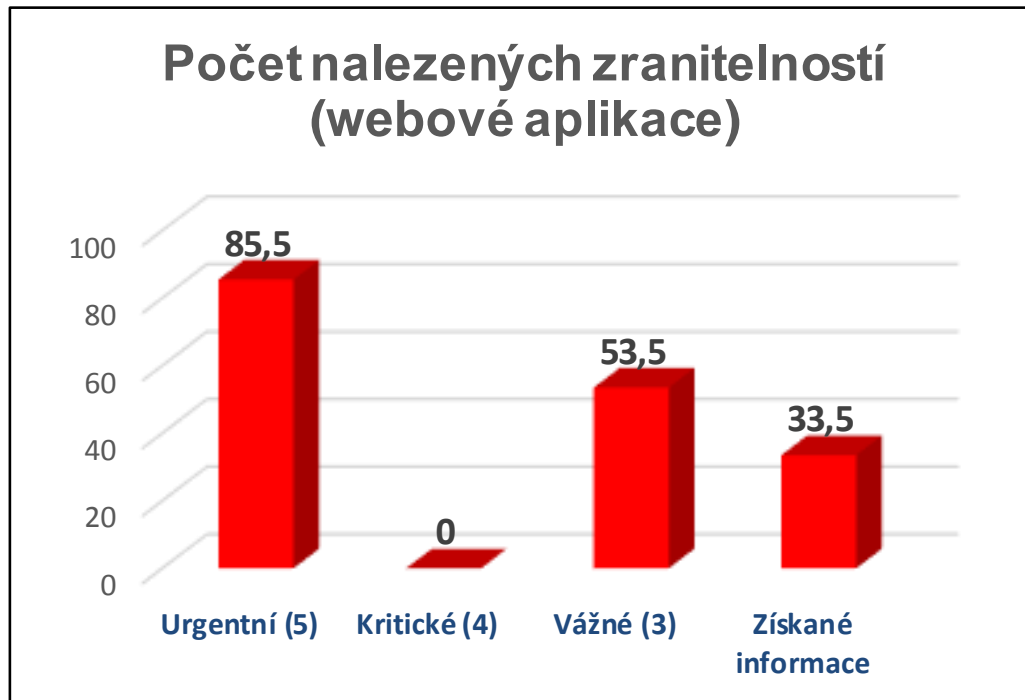


Výsledky testů zranitelnosti

Testy zranitelností: externí & interní



Testy zranitelností webových aplikací



Testy zranitelností: bezpečnost perimetru



otestujte se zdarma

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

Test zranitelnosti zdarma

celé jméno:

e-mail:

pozice:

firma:

velikost firmy: zaměstnanců

IP adresa: [použít moji IP adresu](#)

čas scanu:

SPUSTIT TEST 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“

PREVENENCE

„doufám“

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

Vaše technologická základna

Korelace

SIEM

Detekční nástroje

LOGY

FLOW

MALWARE

VM

NG-IDS

Preventivní nástroje

FW

NGFW

IPS

AV

URL

WAF

DDOS

Cenná aktiva

DATA

SERVERY

APLIKACE

SÍŤE

Vaše technologická základna

Korelace

SIEM 

Detekční nástroje

LOGS



FLOW



MALWARE



QUALYS

NET



Preventivní nástroje



FW



IPS

AV

URL

WAF



DDOS

Cenná aktiva

DATA

SERVERY

APLIKACE

SÍŤ

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 Zvládnání 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

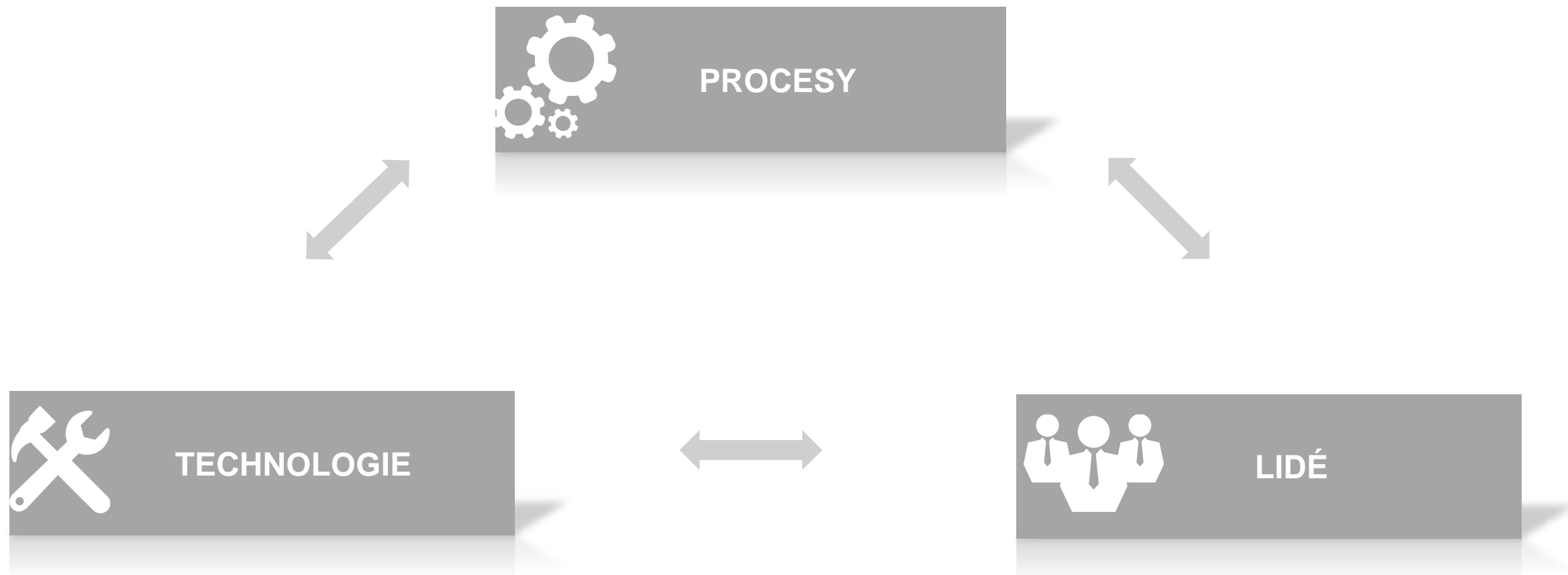
§25 Kryptografické prostředky

§26 Nástroj pro zajišťování úrovně dostupnosti

§27 Bezpečnost průmyslových a řídicích systémů



Bezpečnost obecně



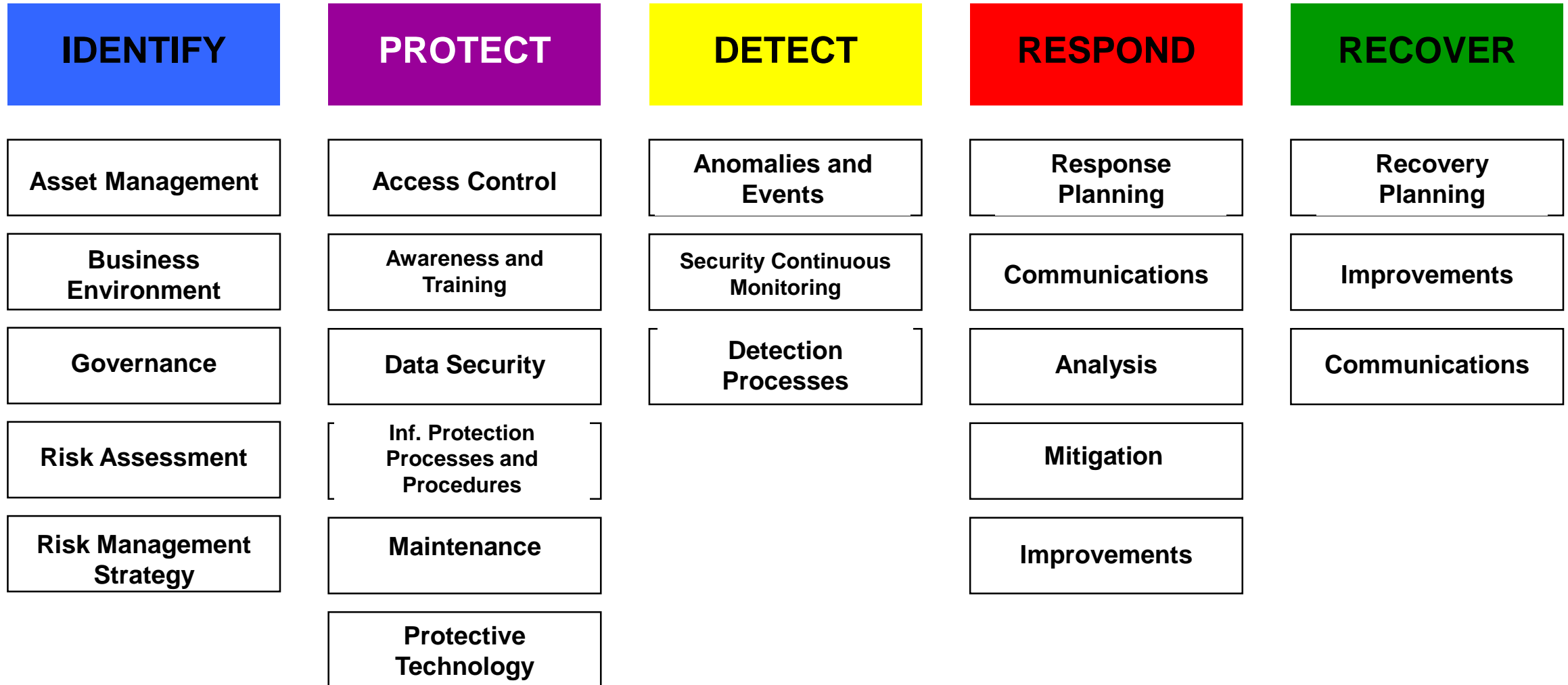
Security Intelligence, Analytics & GRC		
Identity & Access Management	Data Security	Application & Fraud Security
Perimeter / Network Security	Data Center / Server Security	Endpoint / Device security
High Availability		
Physical Security		



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

NIST CyberSecurity Framework



Znáte svůj **business**

Víte, co vám **konkrétně** hrozí

Víte, **jaké** potřebujete technologie

Jak to dát do vzájemné **souvislosti**?

BUSINESS

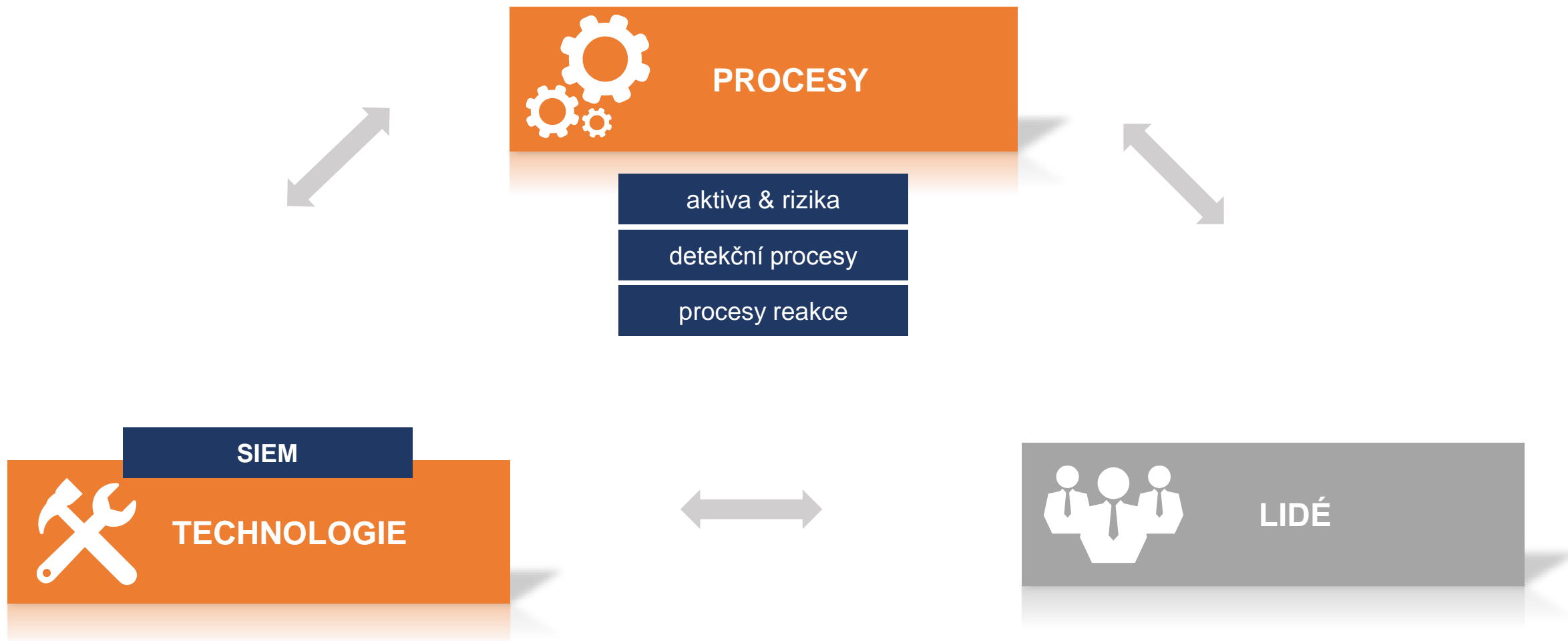
HROZBY

ZKB

SIEM

TECHNOLOGICKÁ ZÁKLADNA

Spojení technologií a procesů

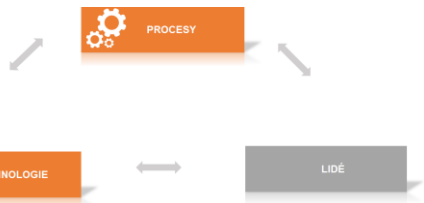


Spojení technologií a procesů

aktiva & rizika

detekční procesy

procesy reakce



Aktiva a rizika

Business -> Aktiva

ZKB -> návod na jejich ohodnocení

Aktiva -> Podpůrná aktiva -> Komponenty

Statistiky, skeny, zkušenosti -> Hrozby

ZKB -> návod na analýzu hrozeb

ZKB -> návod na vyhodnocení rizika

Hodnota rizika -> Kritičnost události v SIEM

Důvěrnost

Dostupnost

Integrita

Pravděpodobnost

Zranitelnost

Dopad

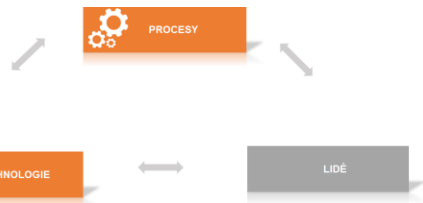
Managed SIEM

Spojení technologií a procesů

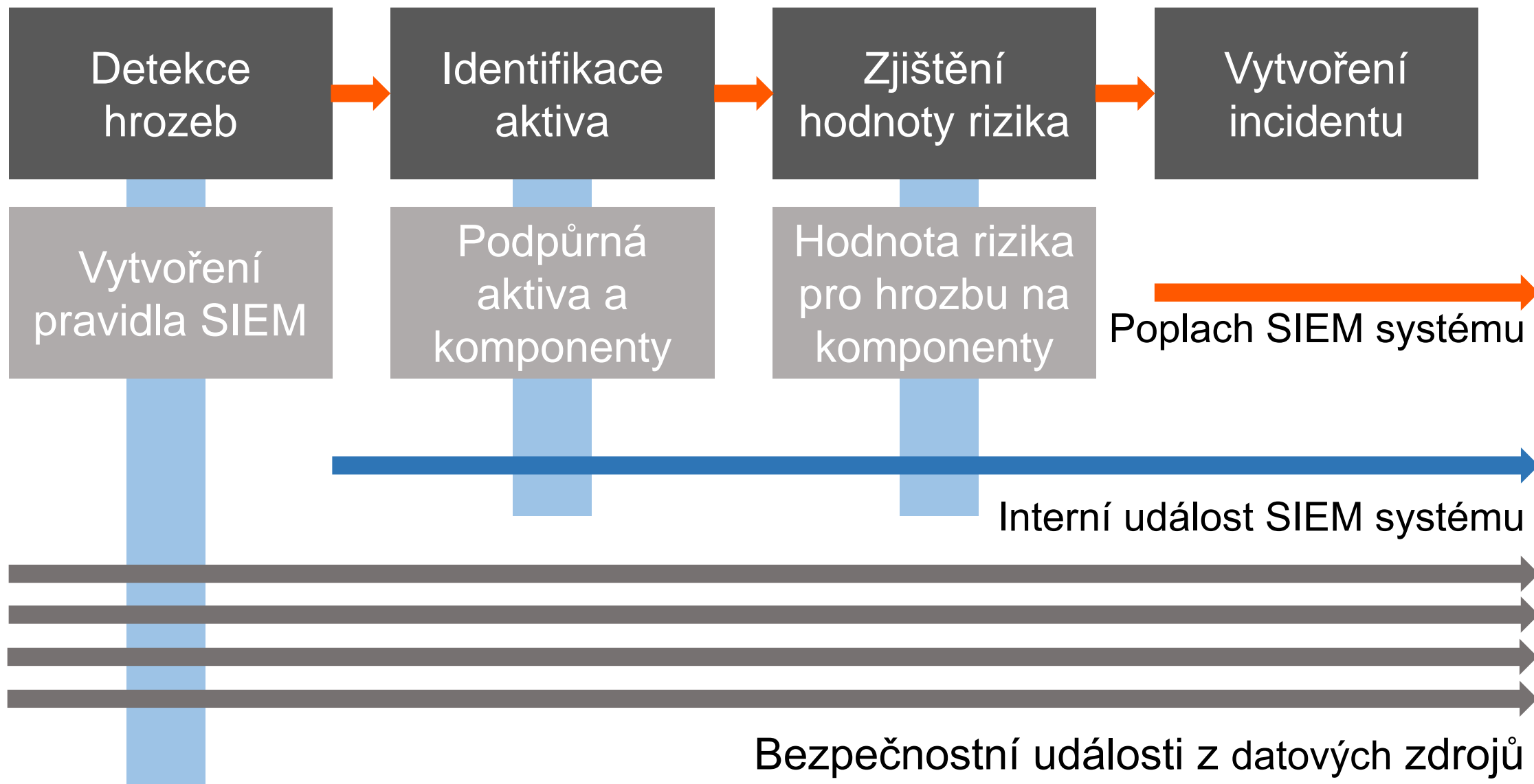
aktiva & rizika

detekční procesy

procesy reakce



Detekční procesy

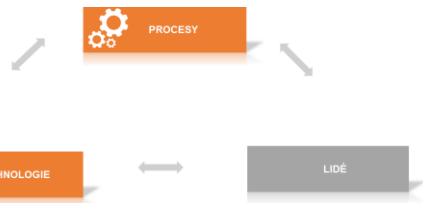


Spojení technologií a procesů

aktiva & rizika

detekční procesy

procesy reakce



Procesy reakce a lidé

Procesní podpora

SOCA používá provozní procesy podle ITIL a Servicedesk

Role

Manažer KB

Administrátor

Architekt KB

Operátor

Auditor KB

Analytik

Vlastníci aktiv

Manažer

Všechny role můžete outsourcovat ! **SOCA** je připravena ...



SOC A



Služby SOCA

premium
SOCA

mějte vše pod kontrolou

active
SOCA

bud'te aktivní

start
SOCA

nebojte se začít

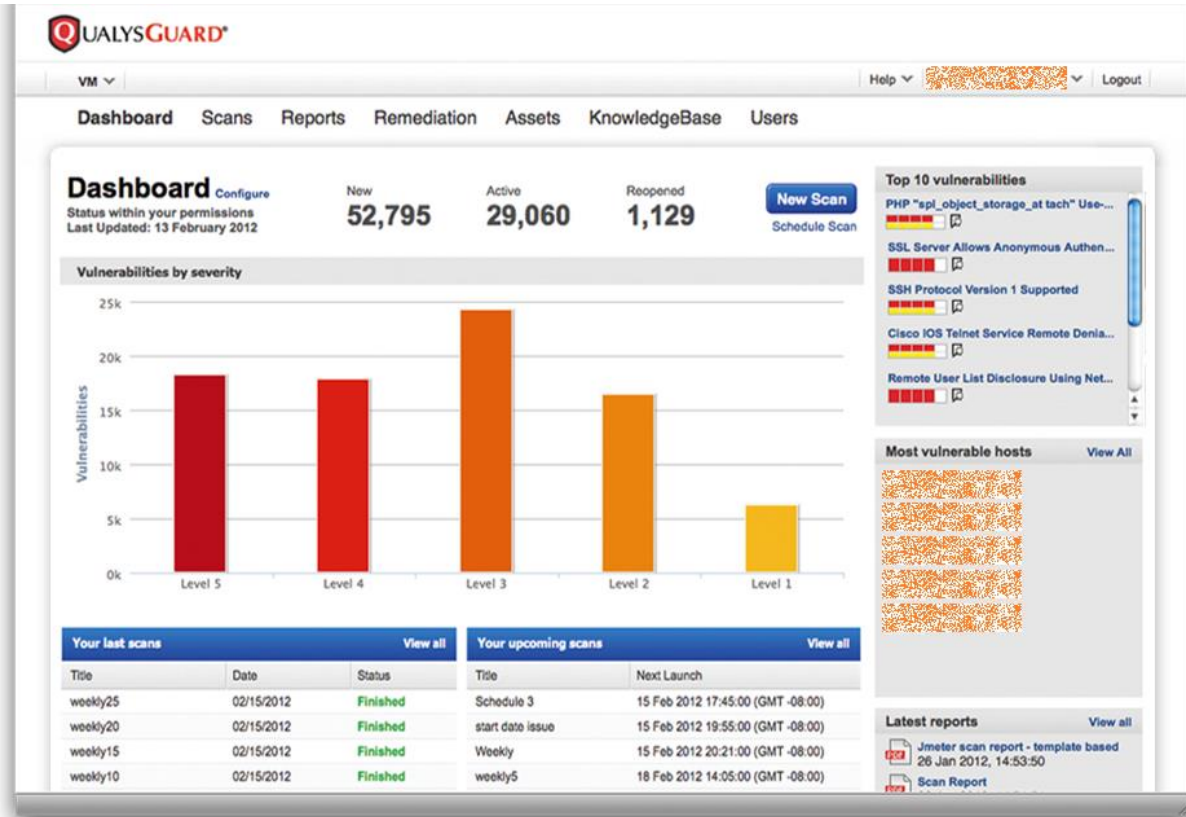
scan
SOCA

zjistěte, jak jste na tom

technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace

SOC**A** v praxi



ACCESS CONTROL & DATA PROTECTION

- 30,670 High Risk Applications Events
- 22 Data Loss Events

THREAT PREVENTION

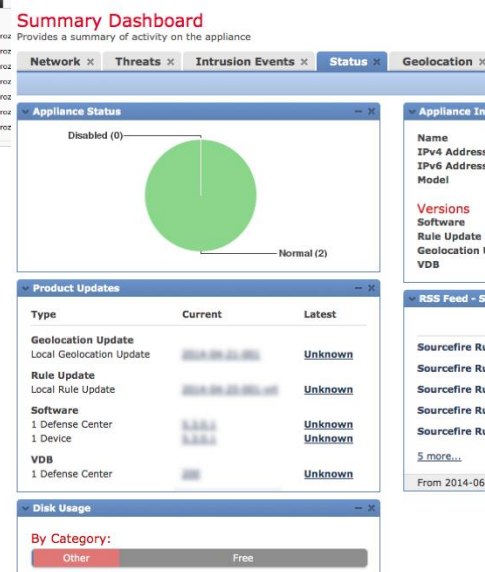
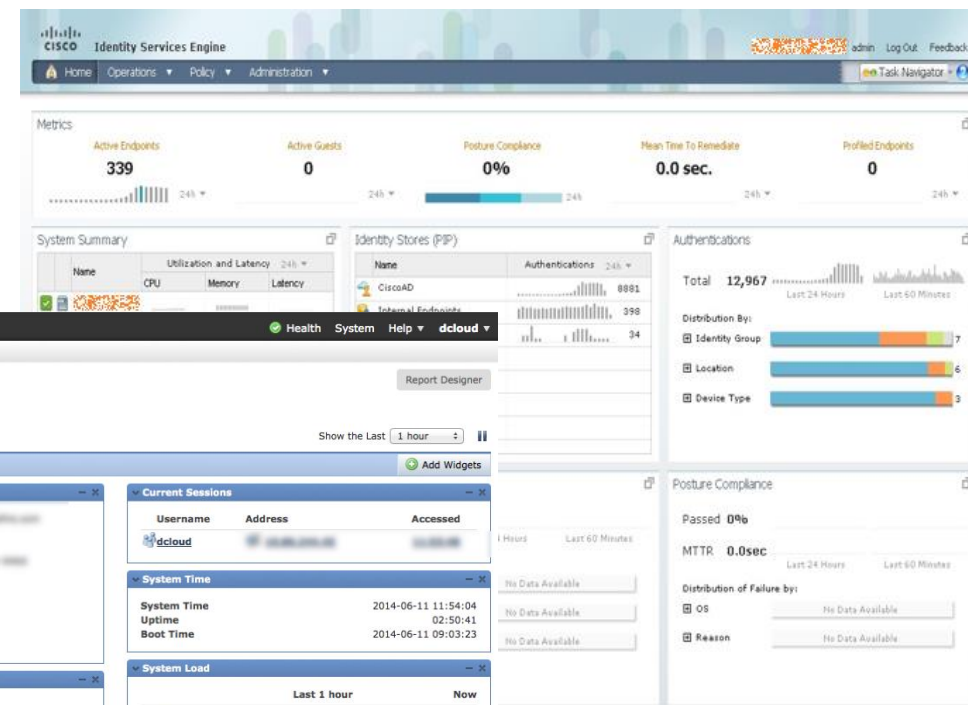
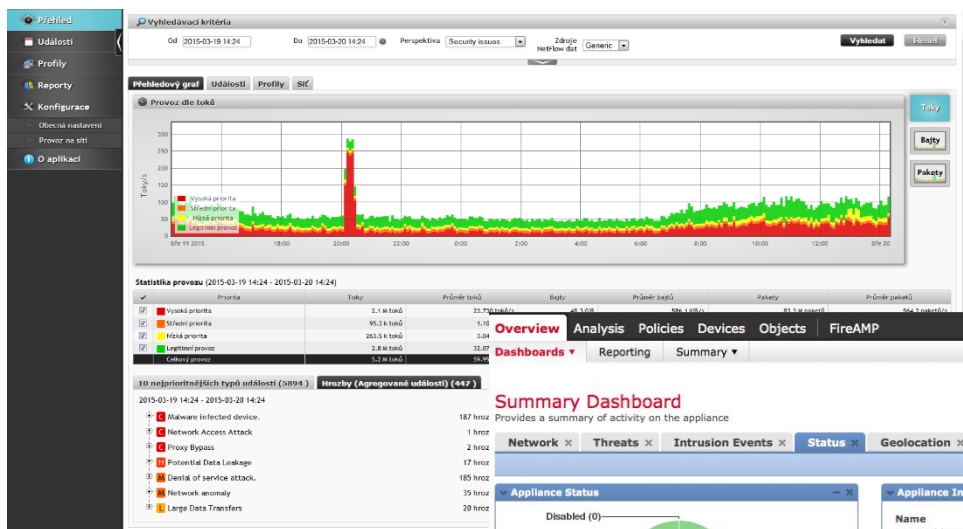
- 9 Bot Events
- 5 Viruses Events
- 16 Zero-day Events
- 18 Intrusions & Attacks Events

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

The screenshot displays a comprehensive security dashboard with the following components:

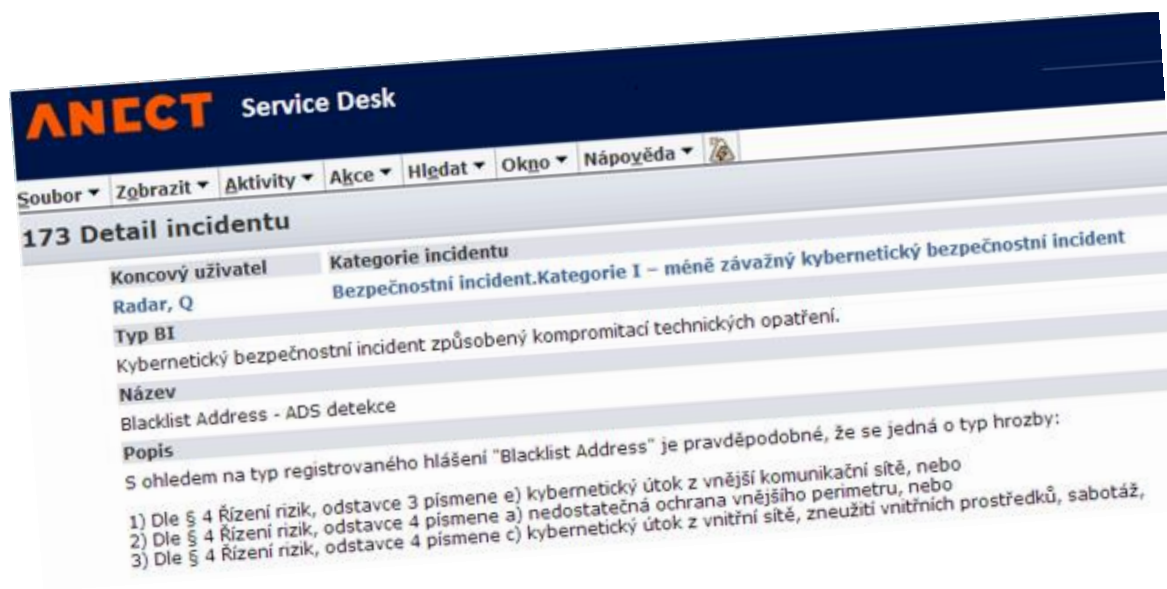
- Navigation and Status:** Includes a top navigation bar with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The current date is Mar 20, 2015, 2:28:22 PM CET.
- Left Sidebar:** Contains a 'Page Refresh Rate' set to 15 minutes, 'Events' summary (NetFlow: 412,479,739; Events: 111,269,386; Sessions: 66,211,256; Data Reduction: 40%), 'Incidents' summary (High: 852, 30%; Medium: 852, 30%; Low: 1,120, 40%; Total: 2,824, 100%), and 'False Positives' summary (To be confirmed: 0, 0%; System determined: 3,811, 0%; Logged: 0, 0%; Dropped: 2,069,823, 100%; User confirmed: 0, 0%; Total: 2,073,636, 100%).
- Main Content Area:**
 - ACS Auth Failed:** Two line charts showing 'ACS Auth Failed: password invalid, last 1d-0h' and 'ACS Failed AAA auth, last 1d-0h' with a 15-minute resolution.
 - IBM QRadar Security Intelligence:** A central dashboard with tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Vulnerabilities, and Admin. It includes a 'System Notifications' table and an 'Event Processor Distribution' chart.
 - System Notifications Table:**

Created	Description
12h 40m 19s	SAR Sentinel: Normal operation restored.
12h 47m 20s	SAR Sentinel: Threshold crossed.
16h 7m 20s	Deviant asset growth was detected in the asset profiler. See the payload for details.
21h 50m 12s	Automatic updates completed successfully.
1d 14h 56m 56s	Automatic updates installed with errors. See the Auto Update Log for details.
3d 20h 28m 55s	Unable to determine associated log source for IP address. Unable to automatically detect the associated log source for IP address.
5d 21h 36m 53s	Automatic updates successfully downloaded. See the Auto Updates for details.
 - Event Processor Distribution:** A line chart showing 'Event Count (Sum)' over time for various processors like Firewall, Custom Rule Engine-6, Health Monitor-2, System Notification-2, ASA, and WindowsAuthServer.
 - System Summary Table:**

Metric	Value
Current Flows Per Second	0
Flows (Past 24 Hours)	0
Current Events Per Second	89
New Events (Past 24 Hours)	6,081
Updated Offenses (Past 24 Hours)	156
Data Reduction Ratio	44066 : 1
 - Other Charts:** 'Top Log Sources (Event Count)', 'Event Rate (Events per Second Raw - Average 1 Min)', and 'Most Severe Offenses' table.

technologická základna

cenná aktiva | preventivní nástroje | detekční nástroje | korelace





ANECT Service Desk

Soubor ▾ Zobrazit ▾ Aktivita ▾ Akce ▾ Hledat ▾ Okno ▾ Náp

173 Detail incidentu

Koncový uživatel	Kategorie incidentu
Radar, Q	Bezpečnostní incident.Kategorie I – méně závažný kybernetický bezpečnostní incident

Typ BI
Kybernetický bezpečnostní incident způsobený kompromitací technických opatření.

Název
Blacklist Address - ADS detekce

Popis
S ohledem na typ registrovaného hlášení "Blacklist Address" je pravděpodobné, že se jedná o typ hrozby:

- 1) Dle § 4 Řízení rizik, odstavce 3 písmene e) kybernetický útok z vnější komunikační sítě, nebo
- 2) Dle § 4 Řízení rizik, odstavce 4 písmene a) nedostatečná ochrana vnějšího perimetru, nebo
- 3) Dle § 4 Řízení rizik, odstavce 4 písmene c) kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž,

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