

SECURITY OPERATIONS CENTER

TÜV SÜD Slovakia



Add value.
Inspire trust.



150+
ROKOV KVALITY,
BEZPEČNOSTI A
UDRŽATEĽNOSTI



1,000+
ZASTÚPENÍ
VO SVETE



€2.6
MILIARDY
ROČNÝCH
TRŽIEB



24,500+
ZAMESTNANCOV*



41%
TRŽIEB MIMO
NEMECKA



574,000
CERTIFIKÁTOV



100%
NEZÁVISLOSTI A
NESTRANNOSTI



1
POSKYTOVATEĽ

Poznámka: Údaje boli zaokrúhlené.

OBSAH PREZENTÁCIE

Zacielenie na sektor

Poskytovatelia
zdravotnej
starostlivosti

Súčasná situácia
v sektore

Výsledky auditov
v sektore

Kritické oblasti

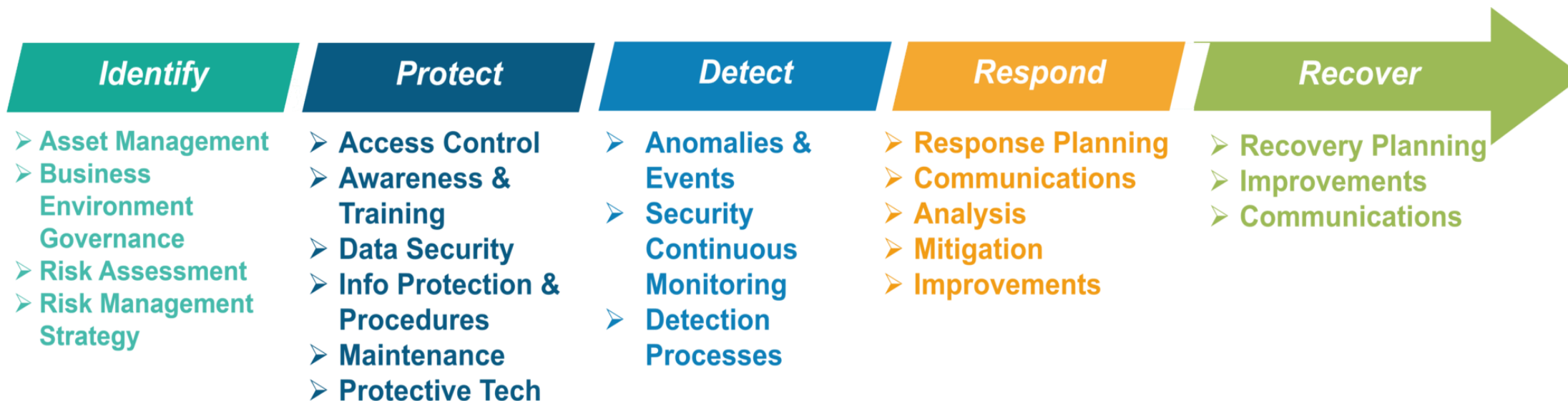
Riešenia

SEKTOR POSKYTOVATELIA ZDRAVOTNEJ STAROSTLIVOSTI - ŠPECIFIKÁ

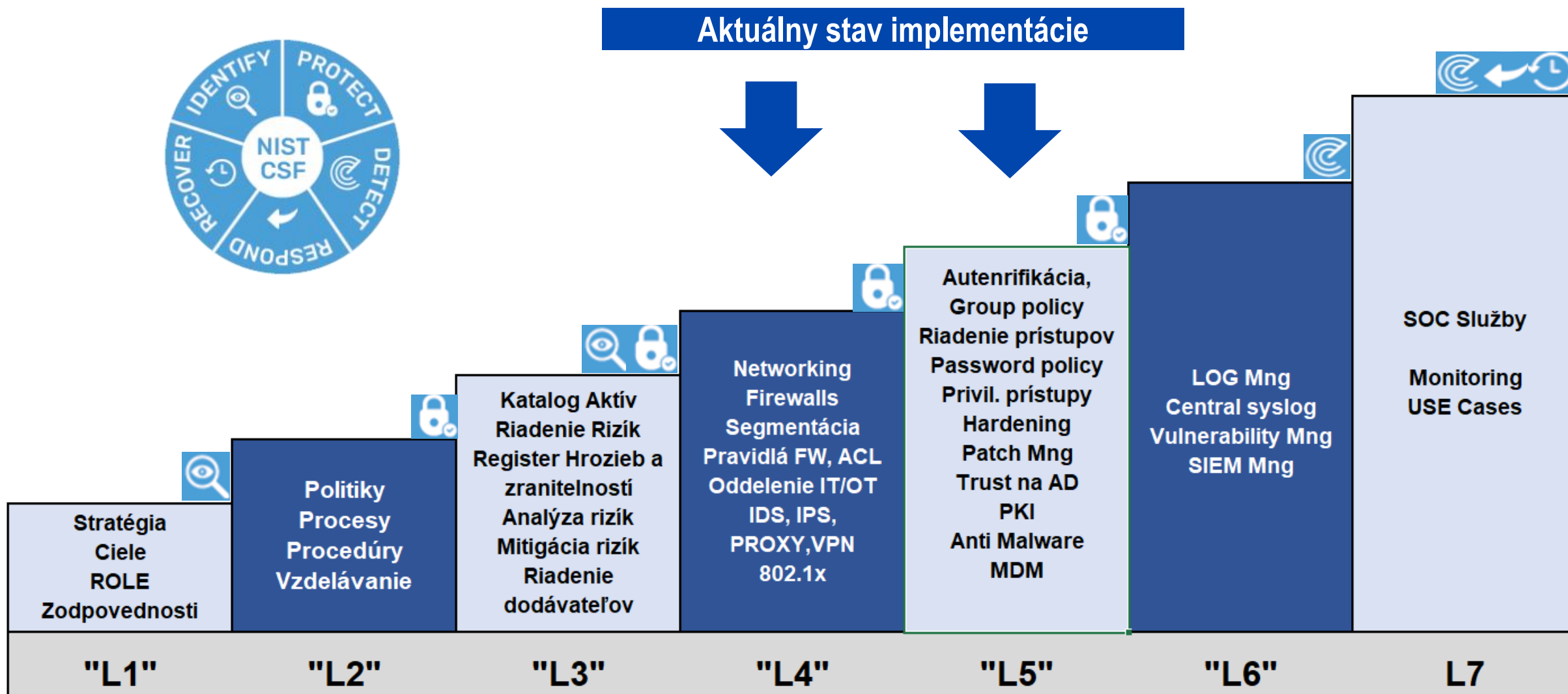
- Cieľ č.1 pre hackerov
- Chránené hodnoty – život a zdravie
- Údaje – Osobitná kategória osobných údajov
- Dva rozdielne svety IT vs. OT



NIST – METRIKY PRE CS – INÝ POHLAD

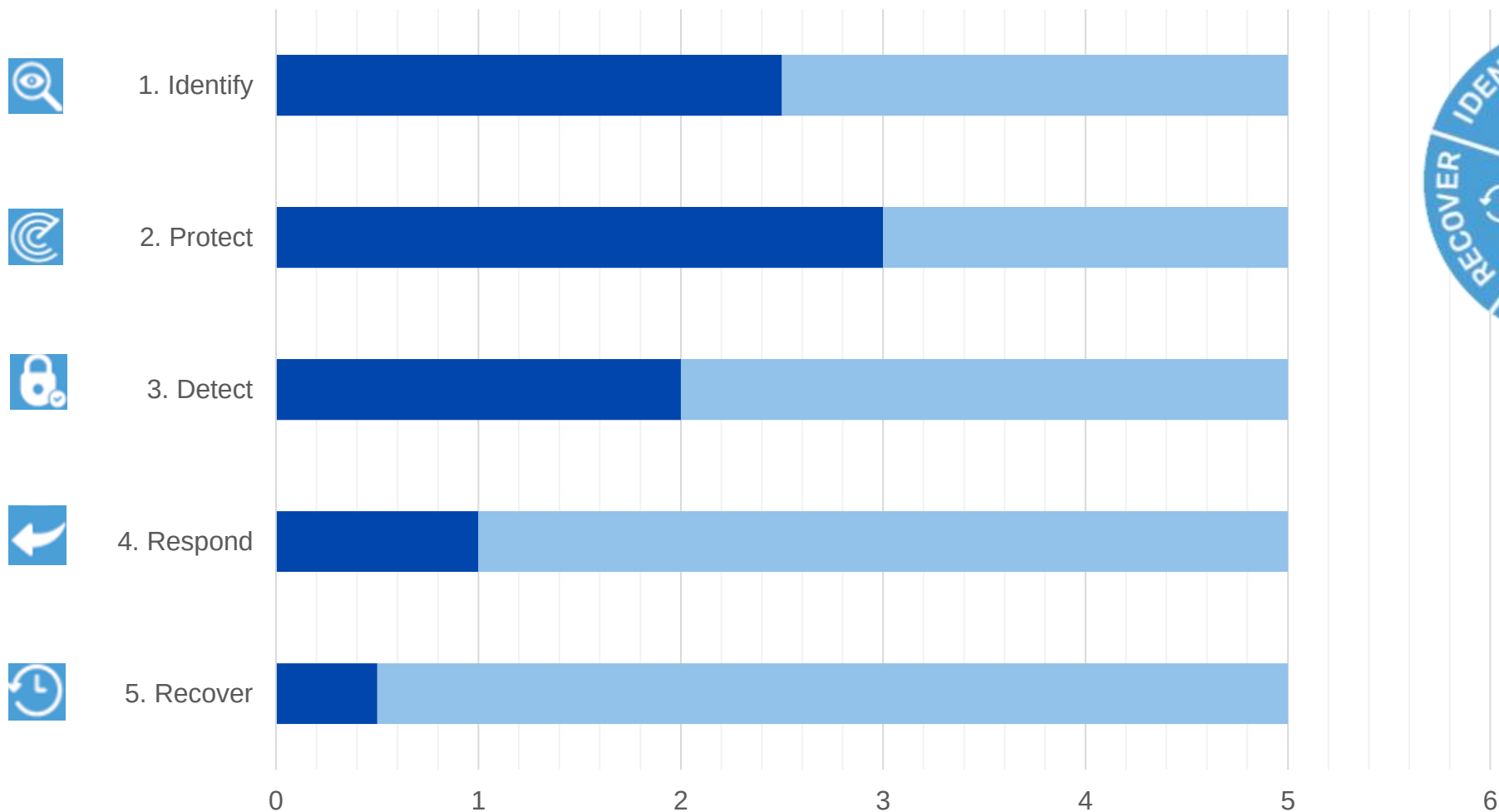


AKTUÁLNY STAV



SÚČASNÝ STAV V SEKTORE CEZ VÝSLEDKY AUDITU KB

■ Plnenie ■ Plán



PROBLÉMOVÉ OBLASTI V SEKTORE – RIADENIE RIZÍK

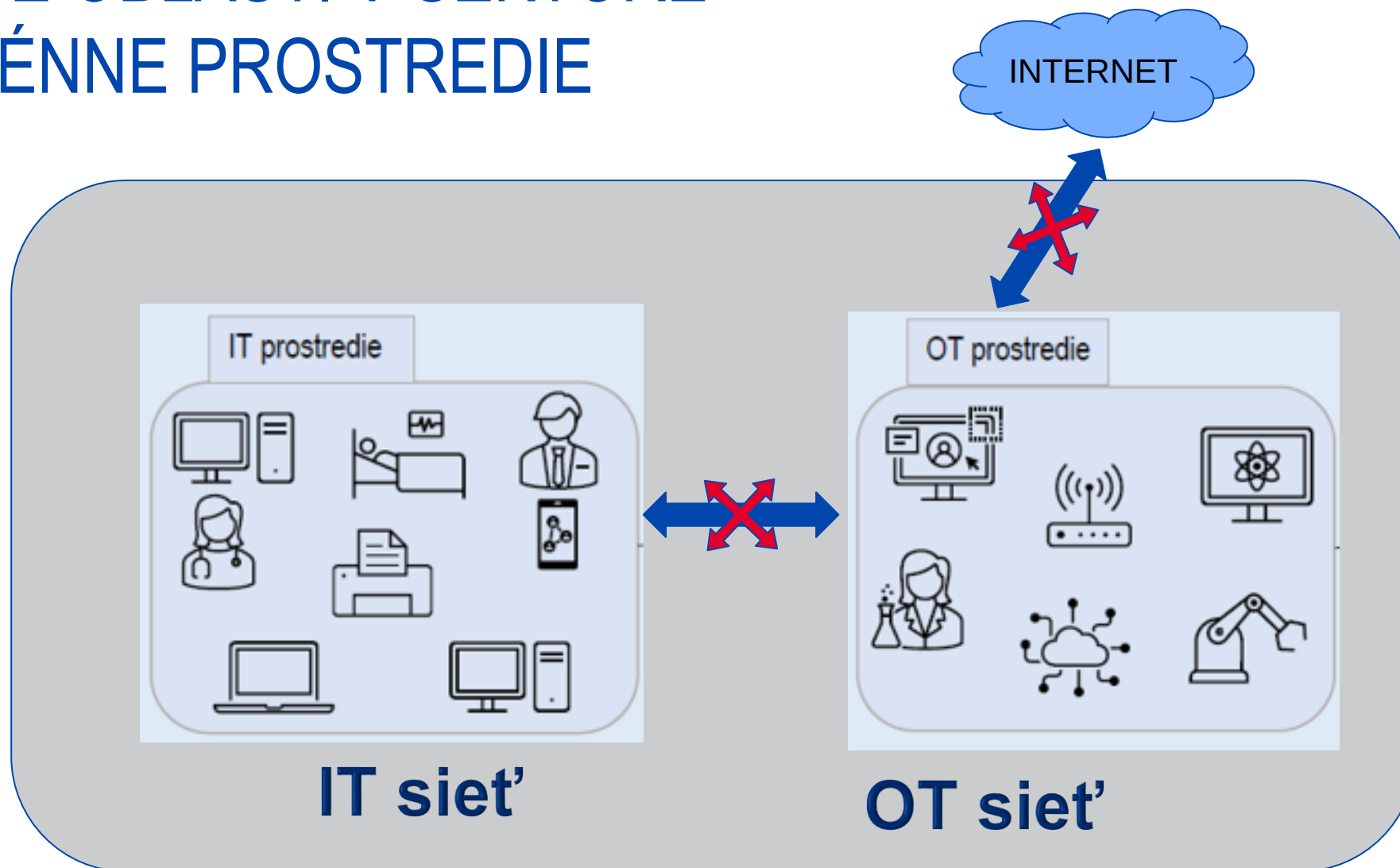
Metodika analýzy rizík kybernetickej bezpečnosti

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

- Ver.01 účinnosť od 1. januára 2022
- Možnosť používať kvalitatívnu metódu hodnotenia rizík
- Metodika nerieši oblasť PRIVACY podľa ISO 29100

PROBLÉMOVÉ OBLASTI V SEKTORE – NEHOMOGENNÉ PROSTREDIE

- Prestupy
- Privilegované prístupy
- Modemy v OT
- Patch Mng
- Nepodporované OS



PROBLÉMOVÉ OBLASTI – DETECT, RESPOND, RECOVERY

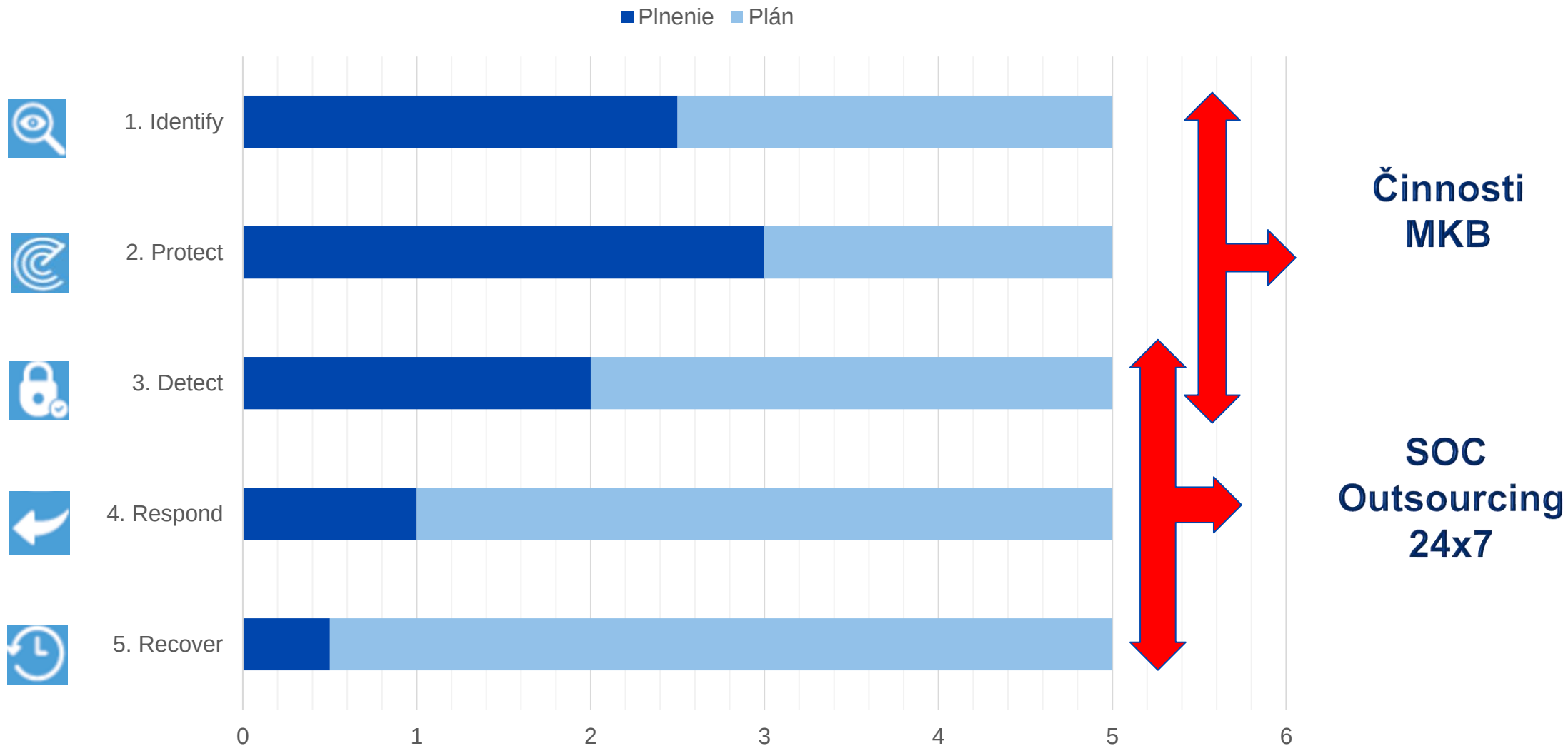
- Nie je vybudovaný Log Mng
- Nie je vybudovaný SIEM Mng
- Nie sú zavedené SOC Služby
- Nie sú definované scenáre pre rôzne vektory útokov (Runbook)
- Nie sú vybudované Respond tímy
- Nie je zavedené BCM

PROBLÉMOVÉ OBLASTI – PRÍČINY

- NIE JE DOSTUPNÝ KOMPETENTNÝ PERSONÁL A POTREBNÉ INVESTÍCIE

- | | |
|------------------------------------|--|
| - Nie je vybudovaný LOG, SIEM Mng- | Vysoké investície, Drahý a nedostupný personál |
| - Nie sú zavedené SOC Služby | Drahý a nedostupný personál |
| - Nie sú scenáre (Runbooks) | Drahý a nedostupný personál |
| - Nie sú vybudované Respond tímy | Drahý a nedostupný personál |
| - Nie je zavedené BCM | Nie je definovaná rola BCO |

NÁVRH RIEŠENIA V OBLASTI ROZDELENIA ČINNOSTÍ



NÁVRH RIEŠENIE TÜV SÜD

- ZÁKLADNÉ ŠKOLENIA A CERTIFIKÁCIE

- Základy informačnej bezpečnosti
- Interný audítor systémov manažérstva podľa ISO/IEC 27001
- DPO - Data Protection Officer: GDPR a ochrana osobných údajov podľa 18/2018 Z.z.
- TISAX (Trusted Information Exchange Assessment Security)
- Manažér riadenie rizík v IT
- Manažér kontinuity v podnikaní (manažér BCMS) / interný audítor podľa ISO 22301
- Manažér kybernetickej bezpečnosti (Cyber Security Manager)
- Informačné technológie vo verejnej správe podľa zákona č. 95/2019 Z.z.
- Riadenie kvality softvéru podľa noriem radu ISO/IEC 25000

NÁVRH RIEŠENIE TÜV SÜD - EXTENDED ŠKOLENIA A CERTIFIKÁCIE

Extended školenia:

Penetračné testovanie
Odozva na incident (Incident response)
Forenzná analýza kybernetického bezpečnostného incidentu

Extended Certifikácie:

Certifikačná skúška: Audítor kybernetickej bezpečnosti
Certifikačná skúška: Manažér kybernetickej bezpečnosti – v procese akreditácie

Všetky školenia sú vedené kvalifikovanými odborníkmi s dlhoročnými skúsenosťami v oblasti forenznej analýzy a riešenia incidentov, threat huntingu, etického hackingu a bezpečnostného monitoringu, čo dokazujú aj získané certifikácie, ako napríklad CISA, CGFE, GCPN, OSCP, OSWP, CHFI a mnohé ďalšie.



RIEŠENIE TÜV SÜD - Prvý OT-IT SOC na Slovensku, 24X7

Pre koho je nevyhnutná služba SOC

Služba SOC je určená predovšetkým pre spoločnosti, ktoré sú povinné splniť zákonné požiadavky zákonom 69/2018 o kybernetickej bezpečnosti ale aj pre spoločnosti, ktoré si uvedomujú potrebu riadenia kybernetických hrozieb.

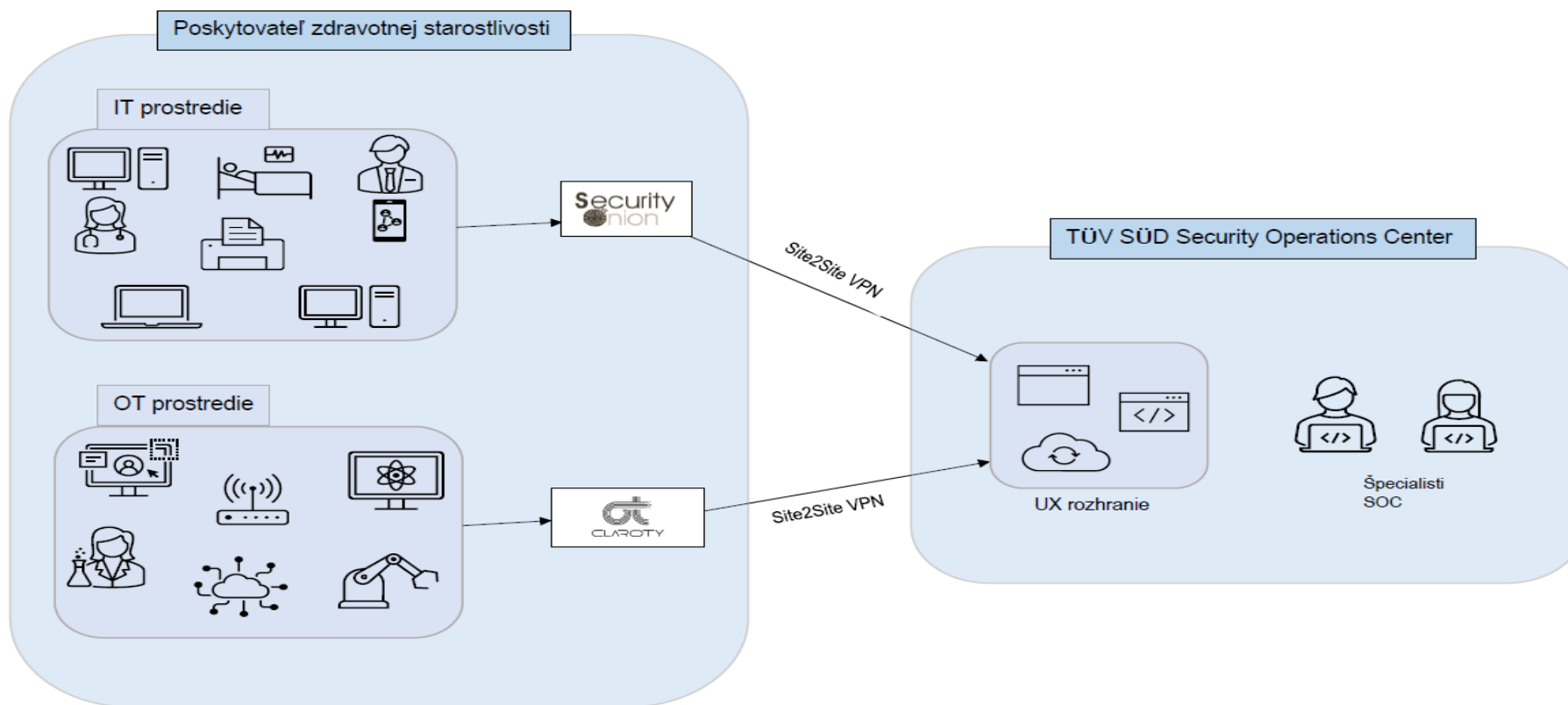
- Voda a atmosféra
- Energetika
- **Zdravotníctvo**
- Priemysel
- Digitálna infraštruktúra
- Doprava
- Prvky kritickej infraštruktúry

Poskytované služby SOC 24x7

- Aktívna podpora zákazníka pri riešení incidentov a implementácií nápravných opatrení,
- Služby bezpečnostného spravodajstva pre konkrétny sektor zákazníka,
- Hĺbková analýza prostredia a infraštruktúry zákazníka v rámci "threat huntingu", odhaľovania APT hrozieb,
- Forenzné analýzy.

RIEŠENIE TÜV SÜD - SOC SLUŽBY 24X7

TÜV SÜD SOC monitoring deteguje, analyzuje a vyhodnocuje kybernetické udalosti alebo incidenty v prostredí zákazníka, a spoločne v spolupráci so zákazníkom sa snaží minimalizovať dopad bezpečnostného incidentu na prevádzku zákazníka.



ZHRNUTIE

- Problém nedostatku kompetentného personálu (MKB)
- Problém chýbajúcich technológií a personálu pre SIEM a SOC služby
- Nedostatok finančných zdrojov

Akčný plán – akcelerácia KB

- Prenesenie časti činností MKB na externý SOC
- Vzdelávanie MKB L1
- Vzdelávanie poskytovateľov SOC Služieb L2, L3
- Podpora budovania externých SOC tímov
- Hľadanie zdrojov



Ing. Igor Straka

Business Area Manager

Cyber Security

TÜV SÜD Slovakia

+421 910 925 318

Igor.Straka@partner.tuvsud.com



Add value.
Inspire trust.

Napredujte s TÜV SÜD

www.tuvsud.com/sk

Všetky naše novinky sú na sociálnych sieťach:

 @tuvsud

 [linkedin.com/company/tuvsud](https://www.linkedin.com/company/tuvsud)

 @tuvsud

 [xing.com/companies/tuvsud](https://www.xing.com/companies/tuvsud)

 [youtube.com/tuvsud](https://www.youtube.com/tuvsud)