Budovanie digitálnej odolnosti

Komplexné monitorovanie bezpečnosti a prevádzky Business Services

Ing. Miloslava Gábrišová | CTO @ Energotel
Ing. et Mgr. Marek Solařík | CCO @ Service & Support
CISA, CRISC

ITAPA 2024 | 18. 6. 2024, Bratislava

Budujeme bezpečnejší a odolnejší digitálny svet

Rastúcie nároky na digitálnu odolnosť

Odstávky sú škodlivé

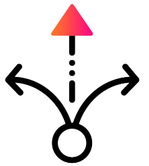
Spoločnosti prichádzajú ročne o 200 miliónov dolárov kvôli neplánovaným výpadkom

Kybernetické riziko je podnikateľské riziko

Kybernetické riziko je teraz #1 a vďaka umelej inteligencii je čoraz väčším problémom

Digitálna odolnosť je regulovaná

Vlády zaviedli prísne sankcie za ich nedodržiavanie. Dodržiavanie právnych predpisov je nevyhnutné



Rýchlosť inovácií má zásadný význam

Rýchlejšie uvedenie produktov na trh je konkurenčnou výhodou

Je ťažké zostať odolný

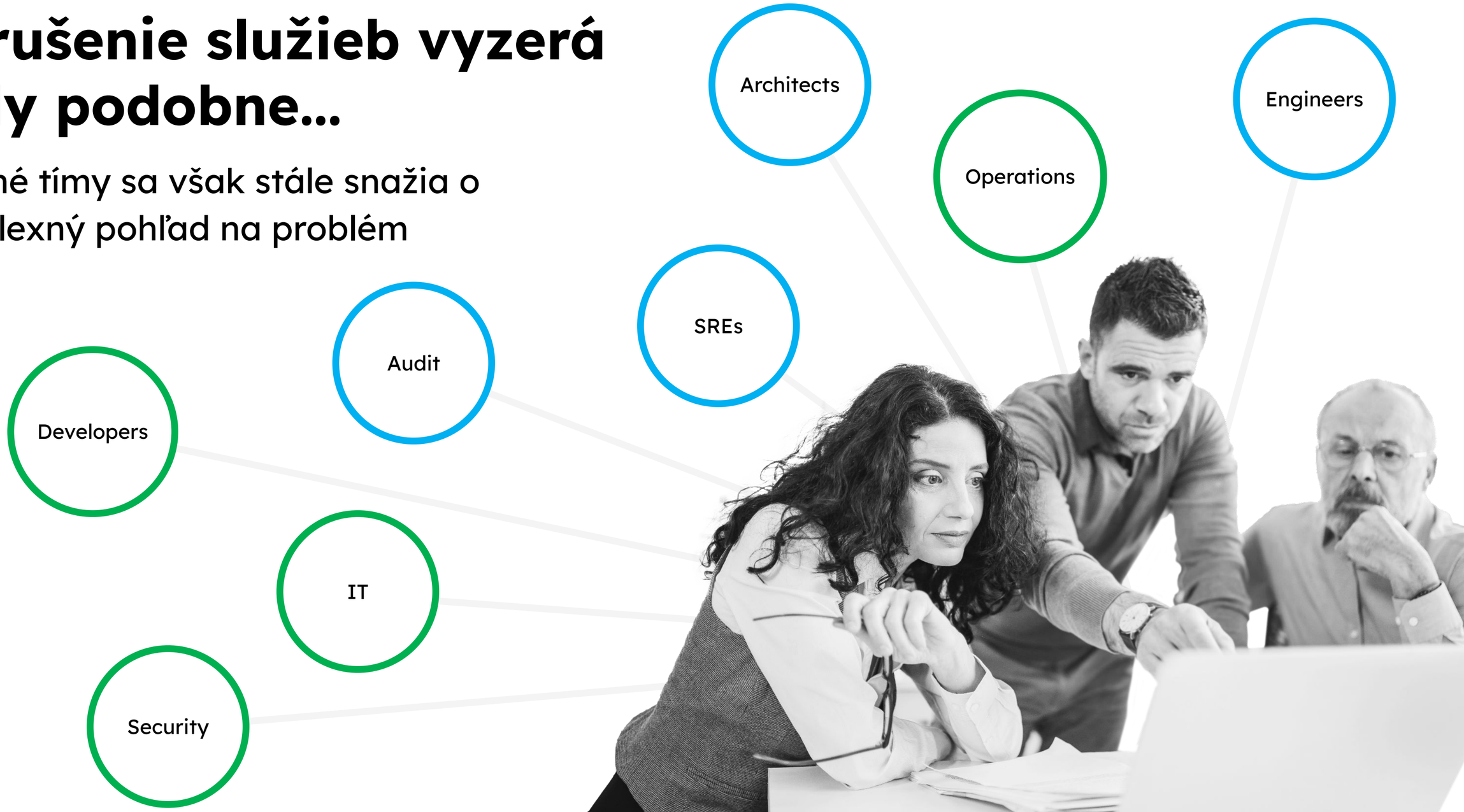
Komplexné hybridné prostredie rozširuje priestor pre útoky a provozné zlyhania

Rastúce objemy dát sú uložené v silách a je čoraz ťažšie ich spravovať

Právne požiadavky vyžadujú hodnotenie rizík v reálnom čase

Narušenie služieb vyzerá vždy podobne...

Interné tímy sa však stále snažia o komplexný pohľad na problém



Ako sa pripraviť na neočakávané výpadky a rýchlo sa z nich zotaviť?

Budovanie digitálnej odolnosti pomocou Splunku

Splunk spája SecOps, ITOps a Engineering, aby ...

Predchádzanie závažným problémom

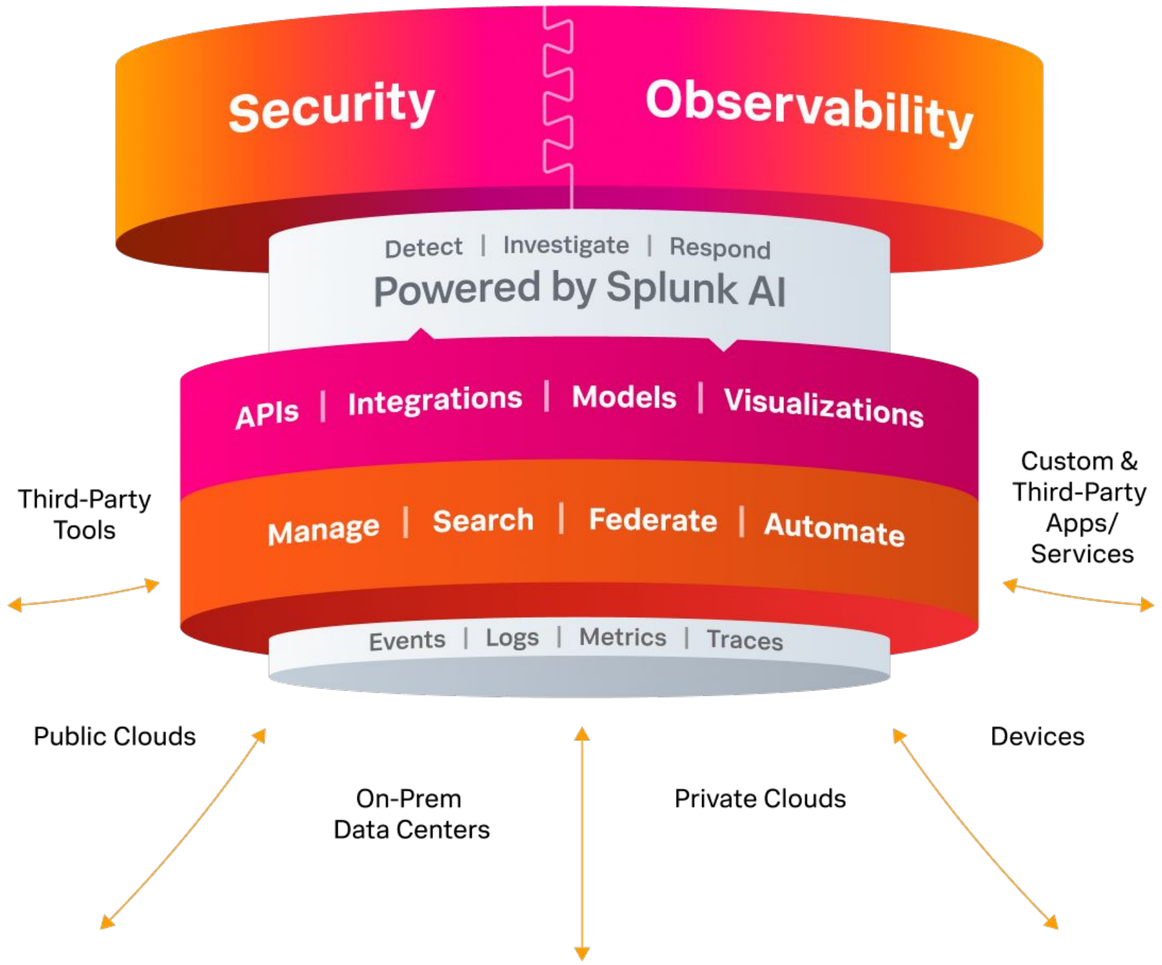
Rýchlejšia obnova provozu

Rýchla adaptácia na zmeny

energotel

Service & Support

Splunk™ Jednotná platforma pre bezpečnosť a observabilitu



Splunk zabezpečuje digitálnu odolnosť jedinečným spôsobom

Komplexná viditeľnosť v akomkoľvek prostredí

Rozsiahla analytika, ktorá urýchľuje MTTx

Technologický líder v oblasti bezpečnosti a observability

Jednotná platforma na správu veľkých dát v akomkoľvek kontexte

energotel

Service & Support

Pomáhame odpovedať na otázky ako...

Ako môžem efektívnejšie spravovať svoje rozsiahle dátové zdroje?

Ako môžu tímy SecOps, ITOps a Engineering lepšie spolupracovať, keď to potrebujú?

Ako môžem dodržiavať neustále sa vyvíjajúce predpisy?

Na čo sa zamerať pri konsolidácii nástrojov a dodávateľov?

Ako môžem byť digitálne odolnejší?

Ako zabrániť výpadkom v akomkoľvek prostredí?

Ako môžem bezpečne a efektívne používať generatívnu AI?

Ako môžem vybudovať SOC budúcnosti?

Cesta k posilneniu digitálnej odolnosti

Security
SecOps

Observability
ITOps, Engineering

Základná viditeľnosť

Videnie naprieč prostrediami

Vyhľadávanie, monitorovanie a vyšetrovanie na sledovanie bezpečnosti v reálnom čase

Riešenie problémov kritických aplikácií a infraštruktúry

Riadený vhľad

Odhaľovanie hrozieb a problémov v kontexte

Zníženie šumu, odhalenie väčšieho počtu hrozieb a identifikácia rizík pomocou detekcie založenej na AI/ML

Stanovenie priorít na základe vplyvu na podnikanie

Proaktívna reakcia

Predchádzajte problémom

Urýchlenie vyšetrovania incidentov a reakcie na ne prostredníctvom automatizácie

Zabezpečenie spoľahlivosti kritických aplikácií a predchádzanie výpadkom

Jednotné pracovné postupy

Bezproblémová spolupráca

Maximalizácia efektívnosti SOC prostredníctvom integrovanej detekcie, vyšetrovania a reakcie na hrozby

Štandardizácia postupov observability v rámci tímov

Akcelerované pomocou Splunk AI

Splunk jediný dodávateľ označený v aktuálnych Gartner Magic Quadrant™ pro SIEM, APM a Observability označený ako leader

Gartner

A Leader

Gartner® Magic Quadrant™ for Security Information and Event Management

A Leader

Gartner® Magic Quadrant™ for APM and Observability

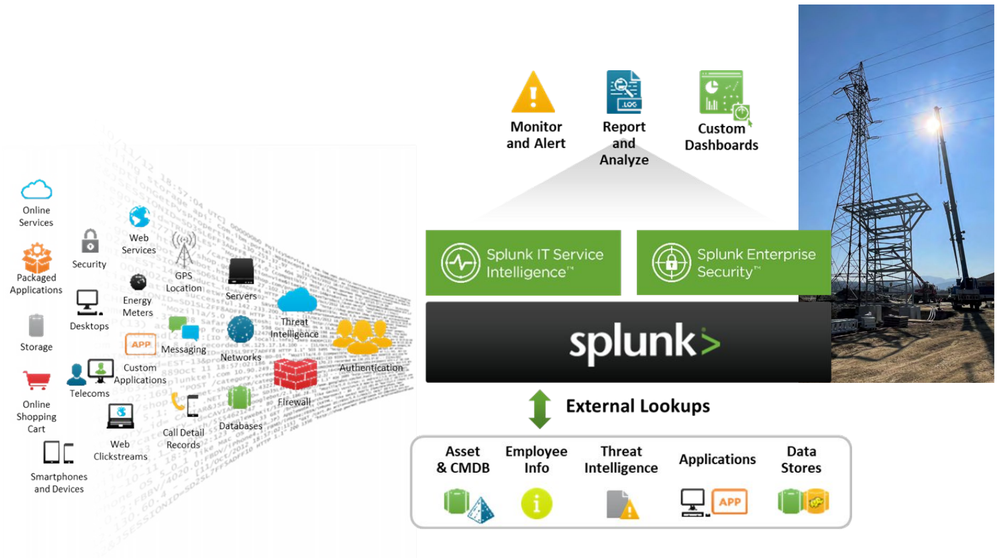
Gartner, Magic Quadrant for Security Information and Event Management, October 2022

Gartner, Magic Quadrant for Application Performance Monitoring and Observability, July 2023

Stredoslovenská distribučná, a. s.

Koncept SecOps

- Pôsobnosť
  - Distribúcia elektrickej energie a súvisiace činnosti, 780 000 prípojných miest
- Kritická infraštruktúra
  - Úzké prepojenie Distribúcia <=> Billing
- Prínosy
  - Vidiťelnosť **Asset – Udalosť**
  - Jedna platforma pre **forenziu** Sec/ITOps - **RCA**
  - Priamy **reporting súladu** so ZKB
- Poskytovanie služby
  - **24/7 SOC**

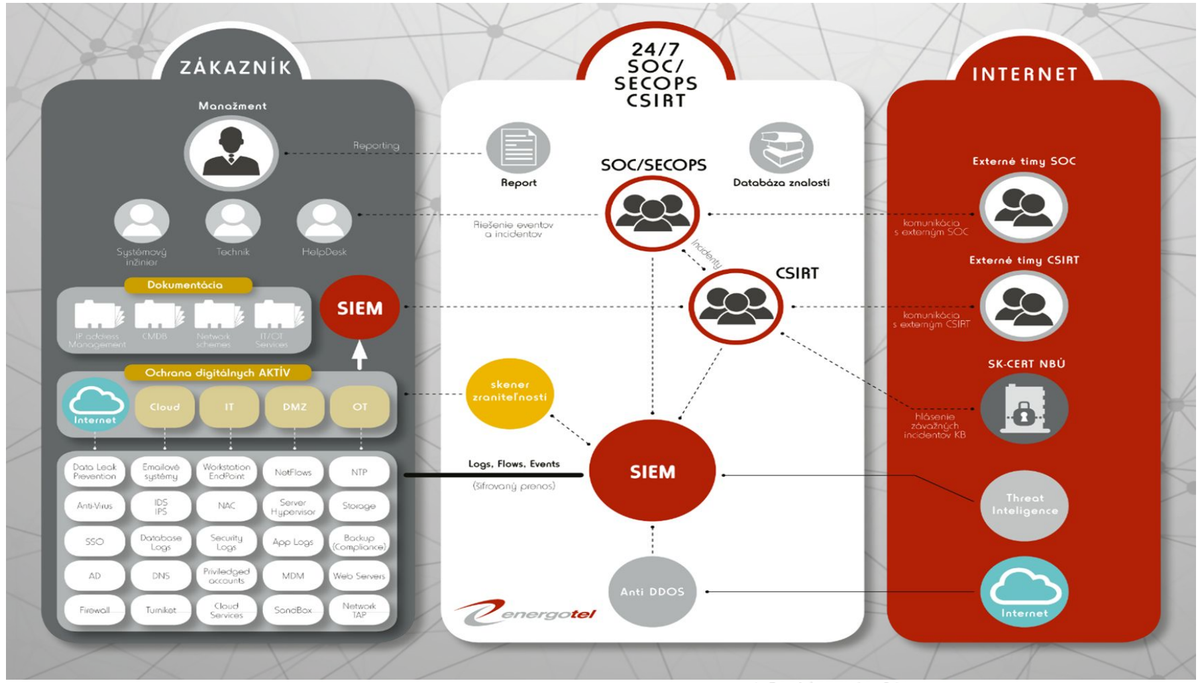


Service & Support

Energotel, a.s.

Kto sme a čo dokážeme

- 20-ročné skúsenosti s prevádzkovaním telco, IT a bezpečnostných služieb, IT a SCADA prostredie
- Komplexné IT a bezpečnostné riešenia



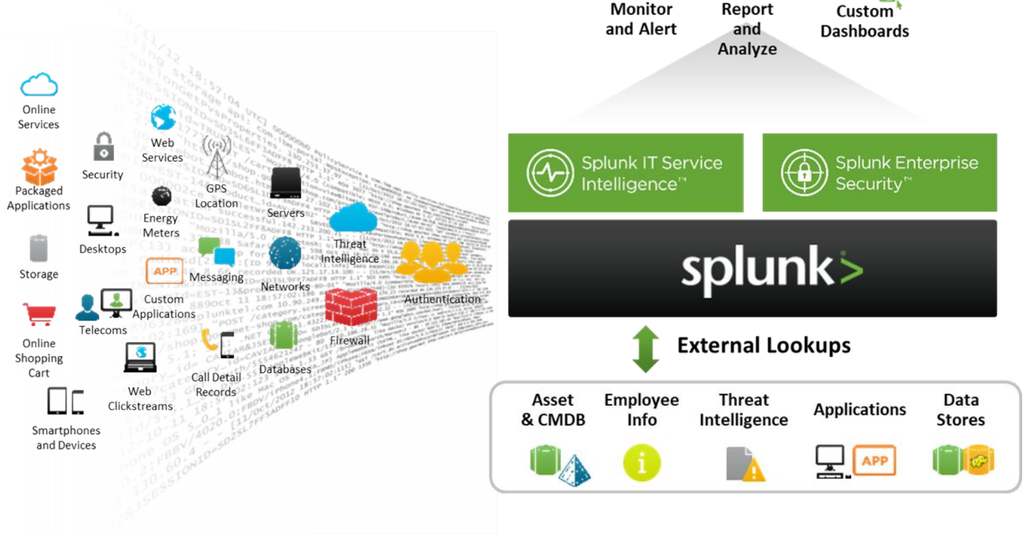
Service & Support, spol. s r. o.

Kdo jsme a co umíme

- 20+ let na trhu komplexních integračních projektů v CZ/SK/EU
- První Splunk Elite Partner v CZ/SK
- Jeden ze 2 CEE partnerů prezentujících na
  - splunk> .conf2017 Washington DC, US
- Ocenění

itSMF Czech Republic
The IT Service Management Forum

ČIMIB



Service & Support

Ďakujeme

Miloslava Gábrišová, miloslava.gabrisova@energotel.sk
Marek Solařík, solarik@sands.cz