

Big Data – nástroj k řízení IT?!

22. mezinárodní konference IT pro praxi 2019

Petr Věžník | Sales Director @ Service & Support spol. s r. o.

10. 10. 2019 | Technická univerzita Ostrava, Ostrava-Poruba

Kdo jsme...

a co děláme

- Komplexní integrační projekty
 - Utility, Doprava, Zdravotnictví
- Hlavní oblasti
 - Bezpečnostní řešení (ZoKB, ISO 27000)
 - ITOps optimalizace (ITIL®, ISO 20000)
- 15 let na trhu
- Ocenění za systémovou integraci

itSMF Czech Republic
The IT Service Management Forum

ČIMIB



S&S a Splunk

► Service & Support *Elite Partner* pro CZ/SK

- Silný technický tým
- Integrační projekty (SIEM, ITSI, SecOps)
- Business Analytics (SLA)

► Splunk conf 2017, Washington DC (25.-28.9.)

- 7 000+ účastníků, 70+ partnerů (2 EE)
- Easy Ride: How to Collect Tolls While Keeping Drivers Happy
- <https://conf.splunk.com/sessions/2017-sessions.html#search=Service%20%26%20Support&>



Co chtějí akcionáři

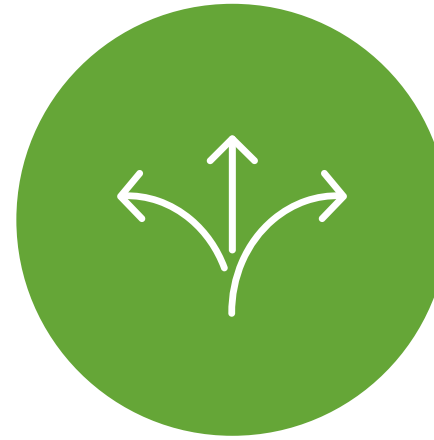
„Svatá čtveřice“ IT?



Zvyšování uživatelské spokojenosti



Efektivně využívat zdroje a snižovat náklady



Stávat se proaktivním



Řídit rizika

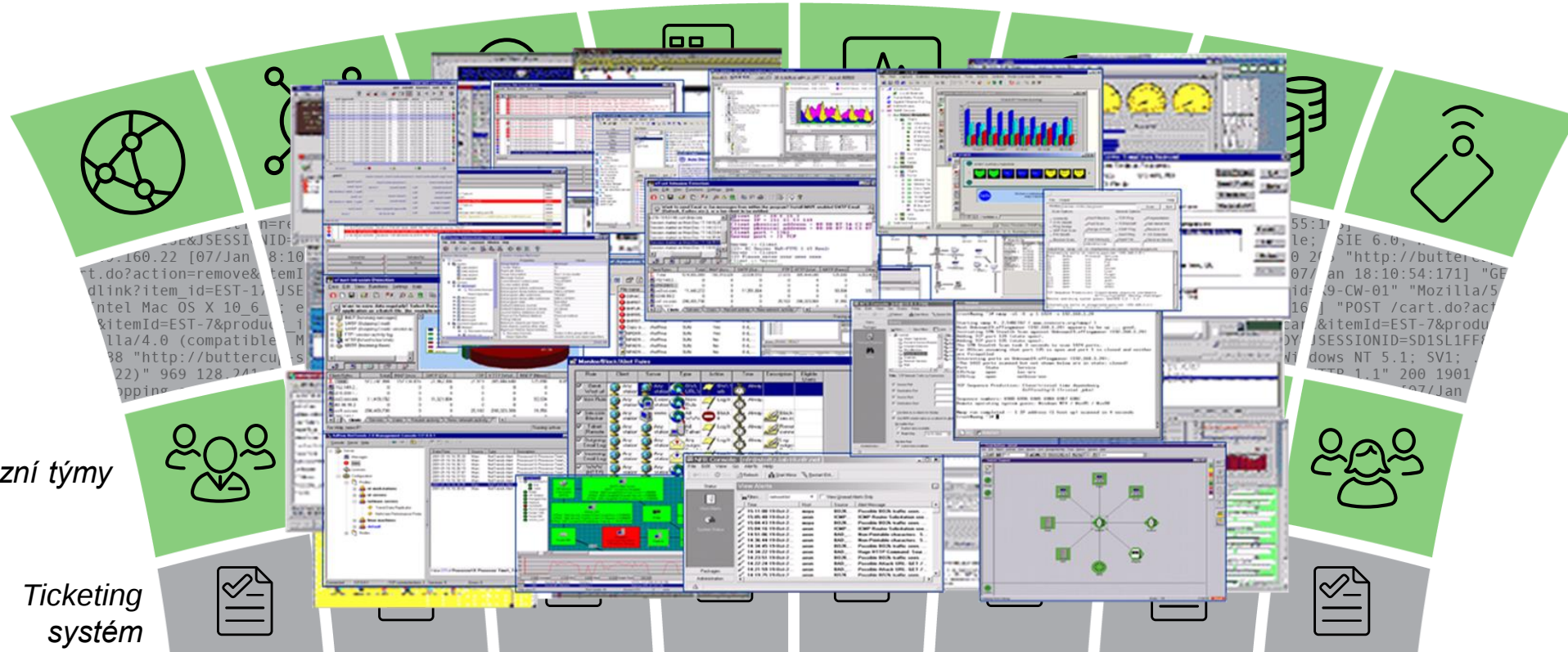
Jak řídíme ITOps

Service Uptime

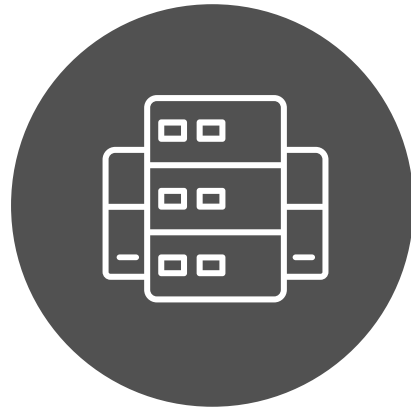
► ITOps

Provozní týmy

Ticketing
systém



Přehodnotit řízení ITOps



Tradiční IT



Data Driven IT

- ▶ Pouze strukturovaná data
- ▶ Různorodé nástroje a integrace
- ▶ „Posedlost“ eventy/alerty
- ▶ **Orientace na Systems Management**

- ▶ Strukturovaná i nestrukturovaná data
- ▶ Robustní datová integrace
- ▶ Přehled v reálné čase
- ▶ **Service Context**
- ▶ využití **ML Analytics**

IT Service Intelligence

Koncept



Získání dat



Definice entit,
služeb, a KPI



Monitoring a
analýza



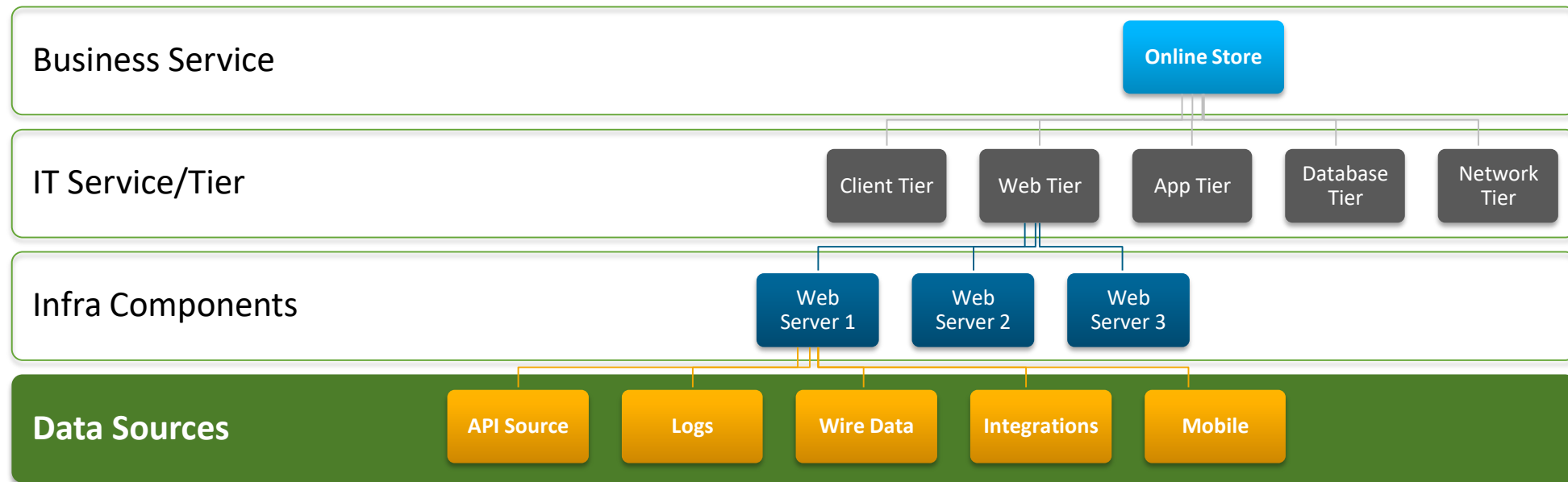
Detekce a
obnova

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
125.17 14.14.14.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&SESSIONID=SD1B5SLBFF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CW-01"
100.100.100.100 - - [07/Jan 18:10:54:100] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1B&product_id=AV-CB-01&SESSIONID=SD1B5SLBFF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CW-01"

IT Service Intelligence

Struktura služeb

► Datové zdroje => Business Service



IT Service Intelligence

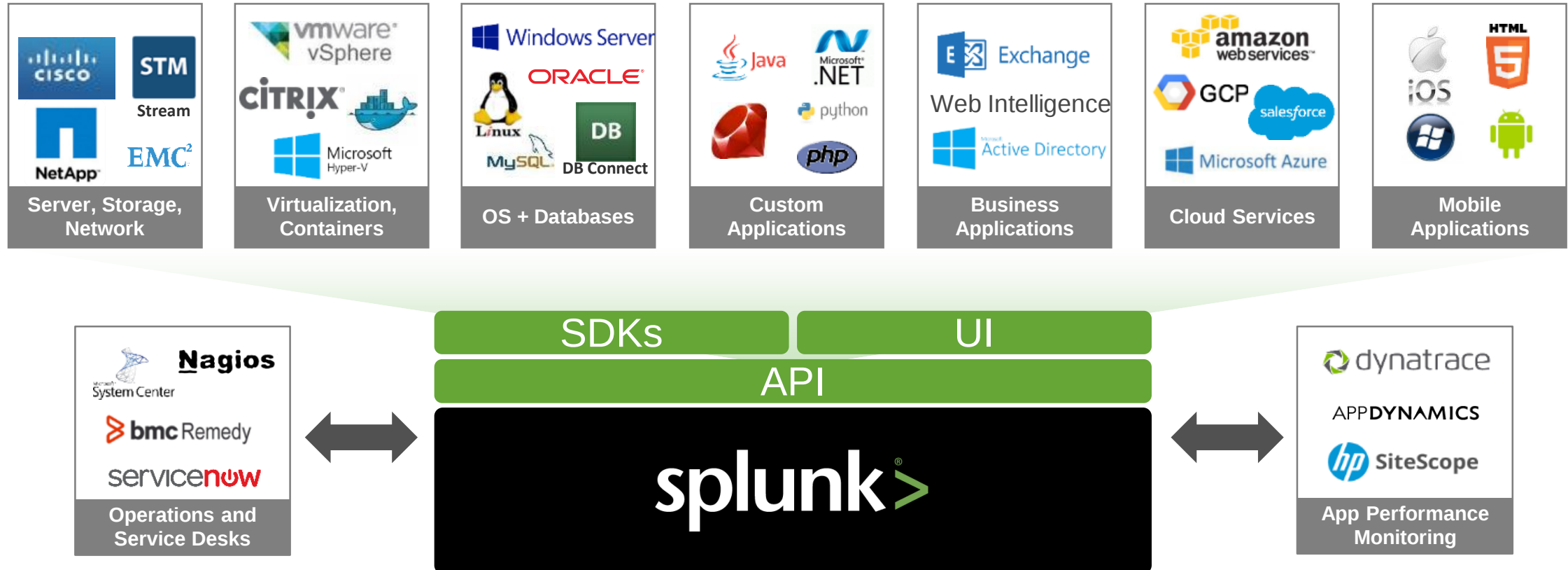


- Přehled o stavu služeb (KPI) v reálném čase na jednom místě
- Zjištění kořenové příčiny zhoršeného stavu služby nebo výpadku



IT Service Intelligence

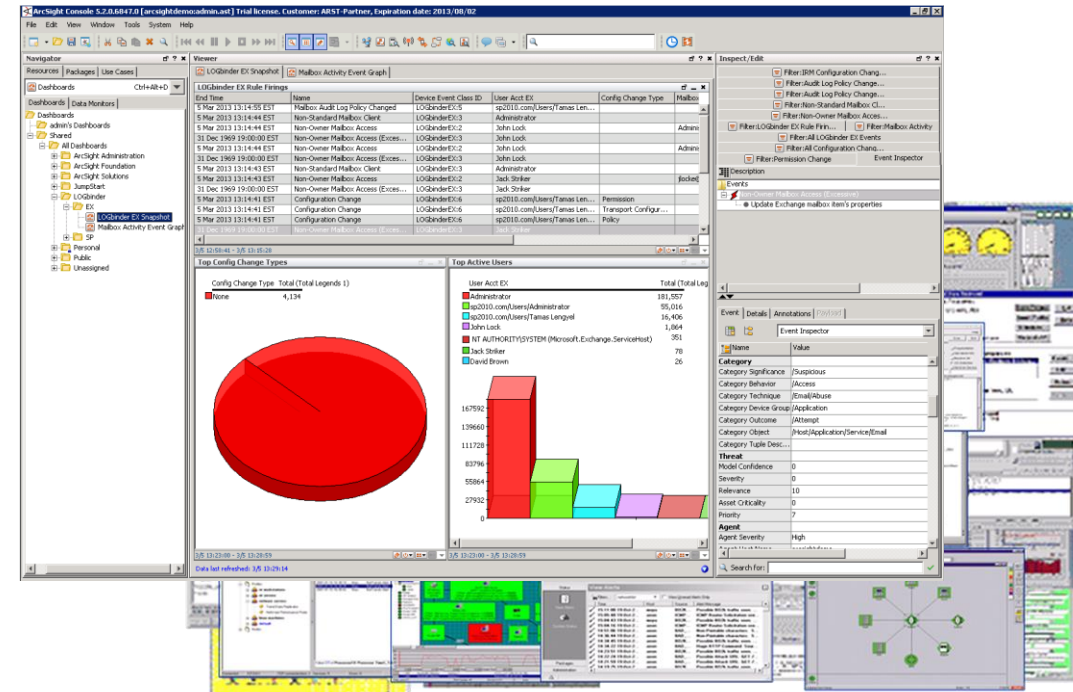
Žádná schémata - data z jakéhokoliv zdroje



Jak řídíme Security

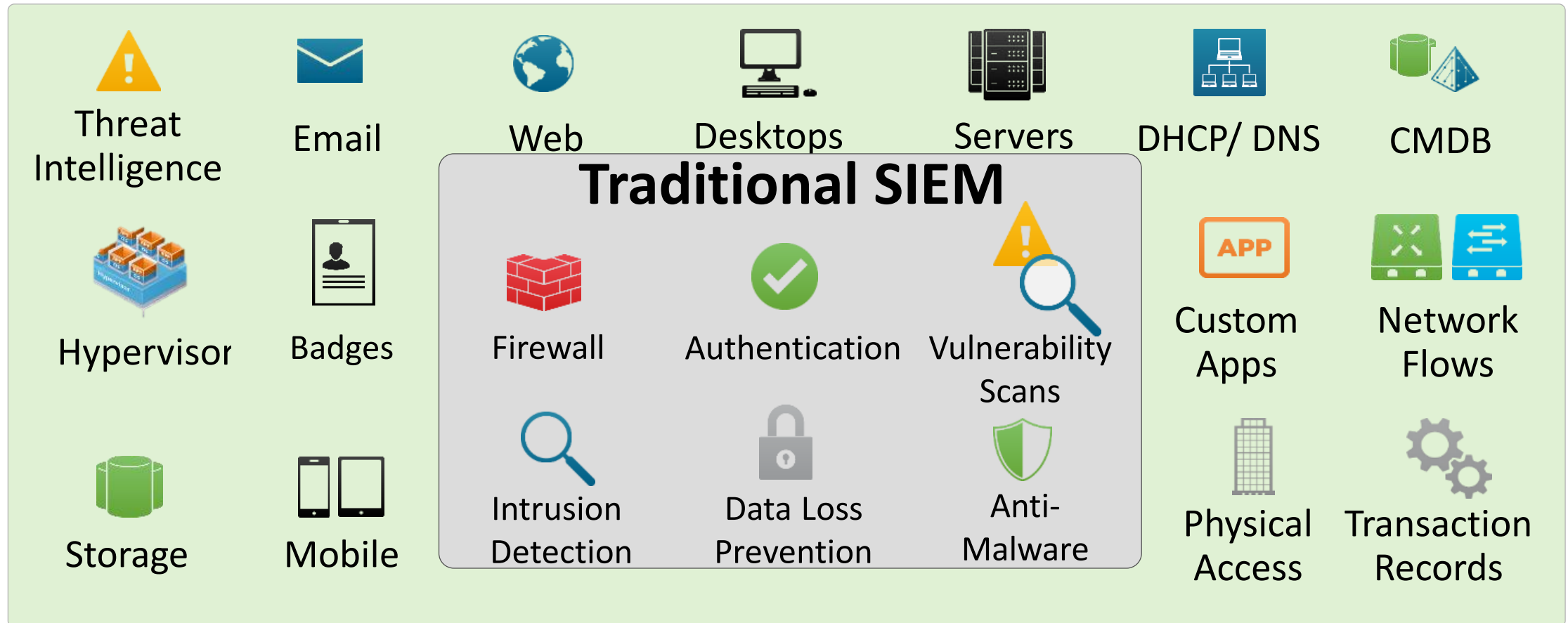
Vývoj konceptu

- ▶ Certifikace ISO 27000
- ▶ Legislativa
 - ZoKB
 - GDPR
- ▶ SOC
 - (Security Operation Center)



Jak řídíme Security

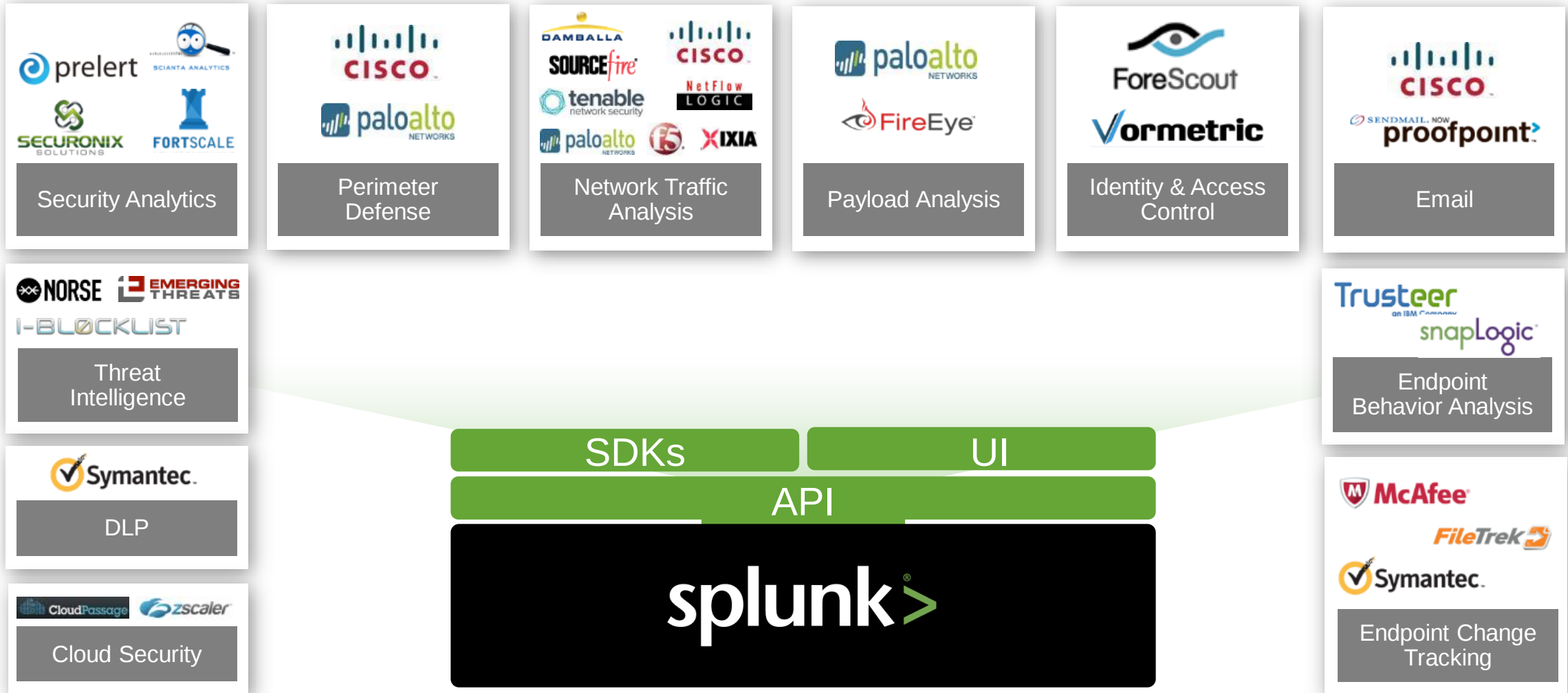
Big Data koncept



Všechna data jsou relevantní a potřebná k detekci a vyšetřování pokročilých hrozeb, podvodů, ztráty dat a zjištění souladu s právními předpisy.

Jak řídíme Security

Security and Compliance



Jak řídíme Security

► SIEM (Security Information and Event Management)

- vývoj na trhu (Gartner)



Synergie SecOps

Synergie SecOpsS

správná data = správné odpovědi = správná rozhodnutí

IT
Operations

Jak predikovat
degradaci
poskytované
služby dřív než se
objeví?

Application
Performance
Analytics

Nízký výkon mé
aplikace je chyba
kódu nebo
infrastruktury?

Security and
Compliance

Jak zrychlit
bezpečnostní
forenzi a snížit
dopad hrozeb?

Business
Analytics

Vytvoří
marketingová
kampaň nové
objednávky přes
portál nebo
mobilní aplikaci?

Internet of
Things

Jak monitorovat a
analyzovat data z
desítek tisíc
senzorů v reálném
čase?

Synergie SecOps

Big Data zdroje...



- ▶ IT infrastruktura
- ▶ Cybersecurity tech
 - IT
 - non IT
- ▶ Aplikace
- ▶ Uživatelé
- ▶ IoT
- ▶ ICS

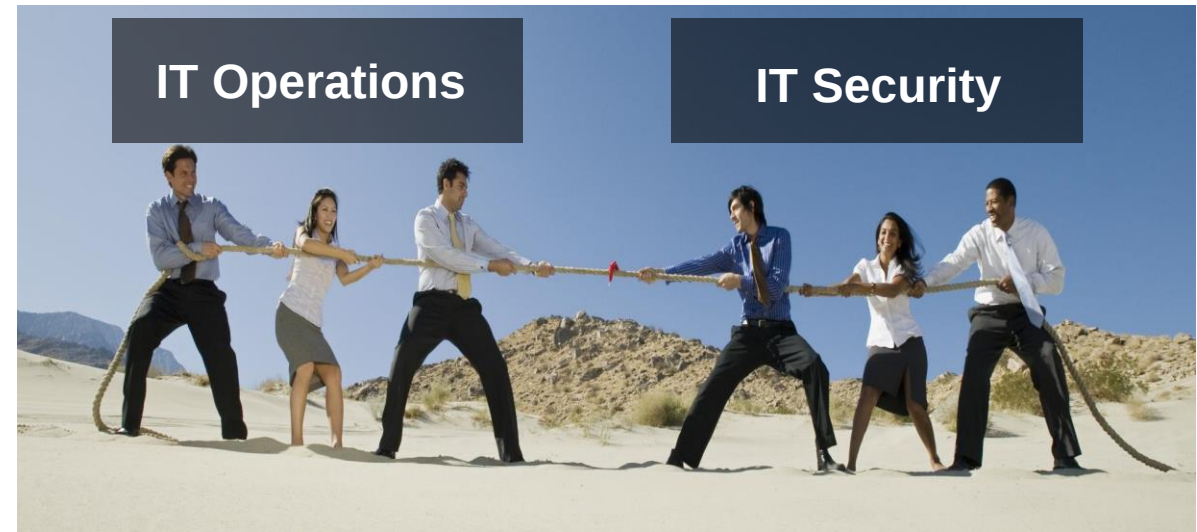
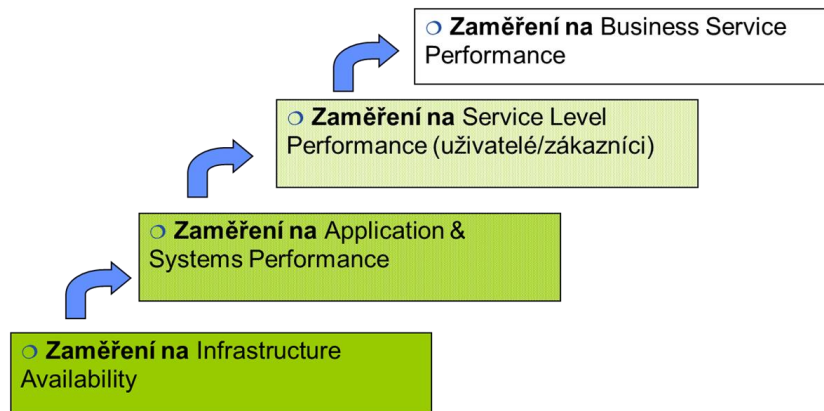
... jakýkoliv digitální záznam

Objem | Rychlost | Rozmanitost | Proměnlivost

Synergie SecOps

Koncept

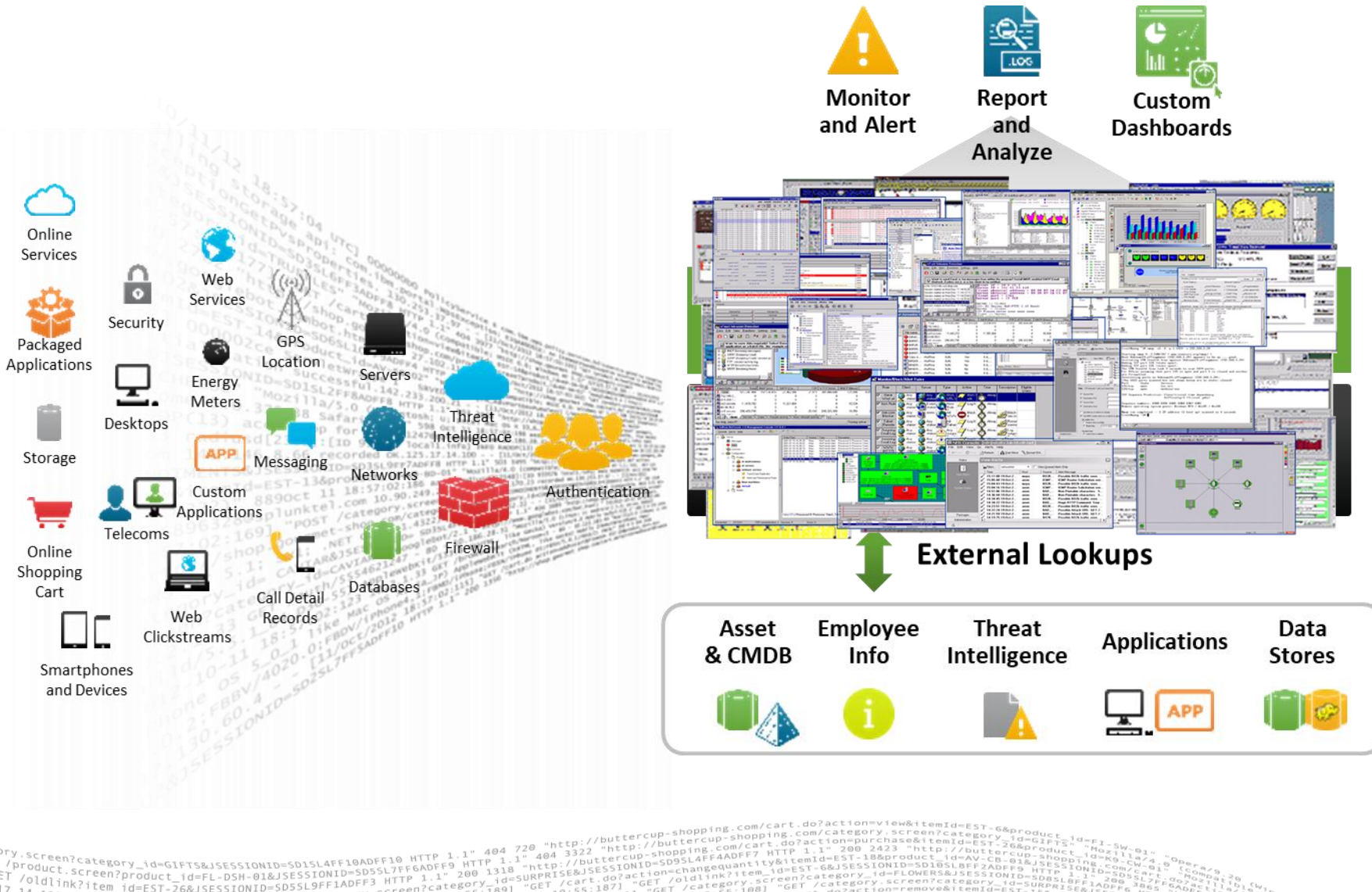
- ▶ IT přímo podporuje business (musí)
 - „... šedé IT...“, Gartner
- ▶ SecOps (IT Security & IT Operations)
 - Mind the Gap ...? No Gap!



Jedny data pro všechny !

Splunk SecOps

IT Security & IT Operation Center



Referenční projekty

Splunk Enterprise, IT Service Intelligence, Enterprise Security

► Vybraní zákazníci



ČESKÁ SPRÁVA
SOCIÁLNÍHO ZABEZPEČENÍ



NÚKIB



Equa bank



PAYWELL

OPENMATICS

Q&A

Děkuji

Petr Věžník, veznik@sands.cz