COMGUARD
communication security

Gytpol Validator

Unikátní technologie pro detekci a nápravu konfiguračních závad

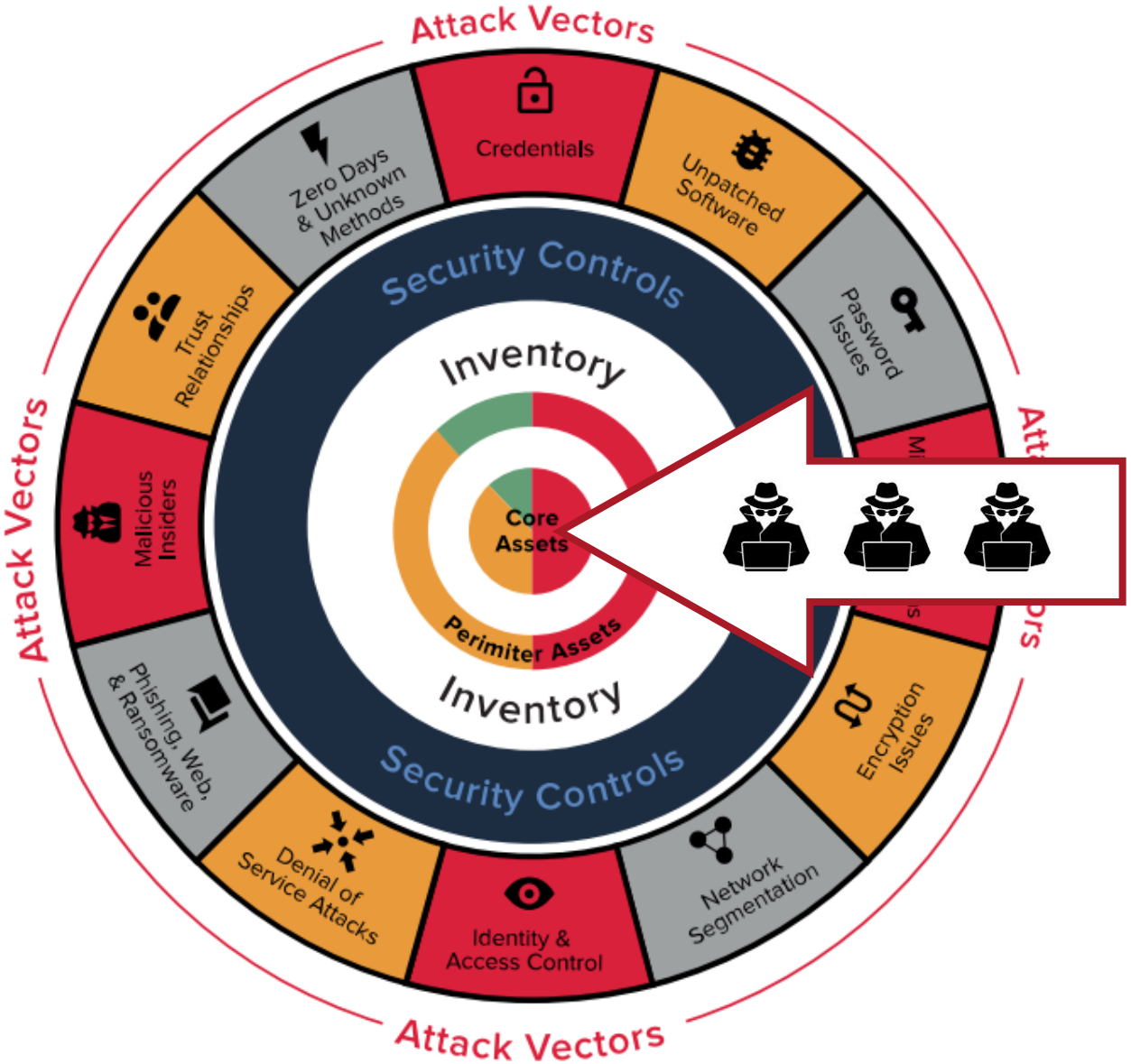
Lukáš Babčický
lukas.babcicky@comguard.cz

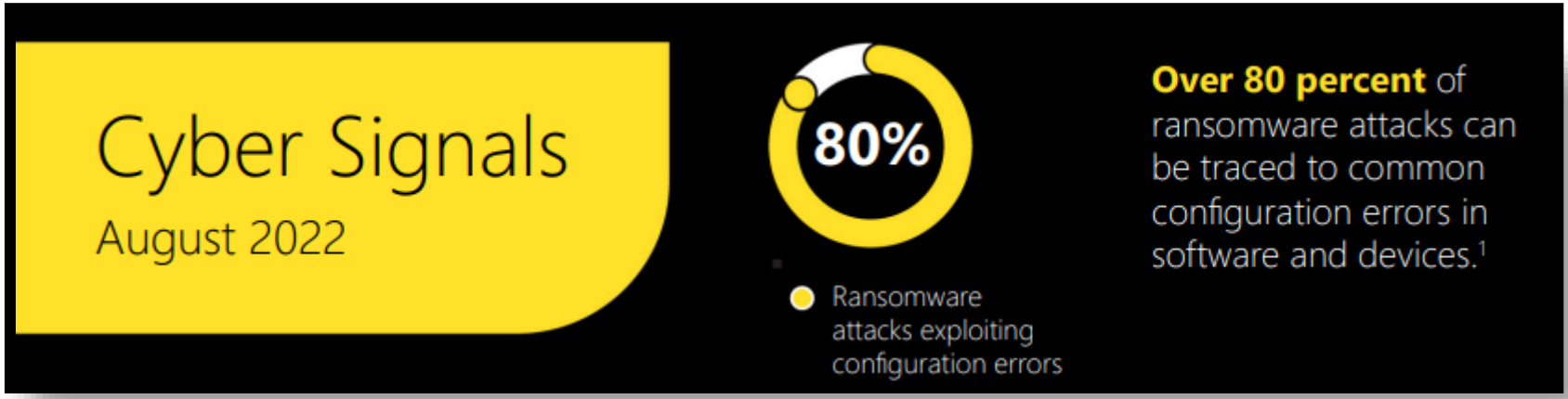
GYTPOL

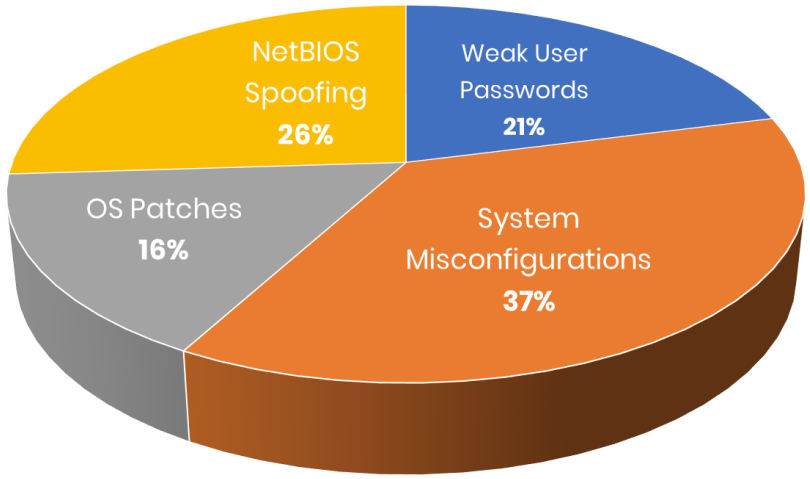
Konfigurační závady

Zneužití konfiguračních závad je běžný vektor útoku.

Narůstající četnost zneužívání tohoto vektoru může z vašich endpointů udělat entry-pointy.





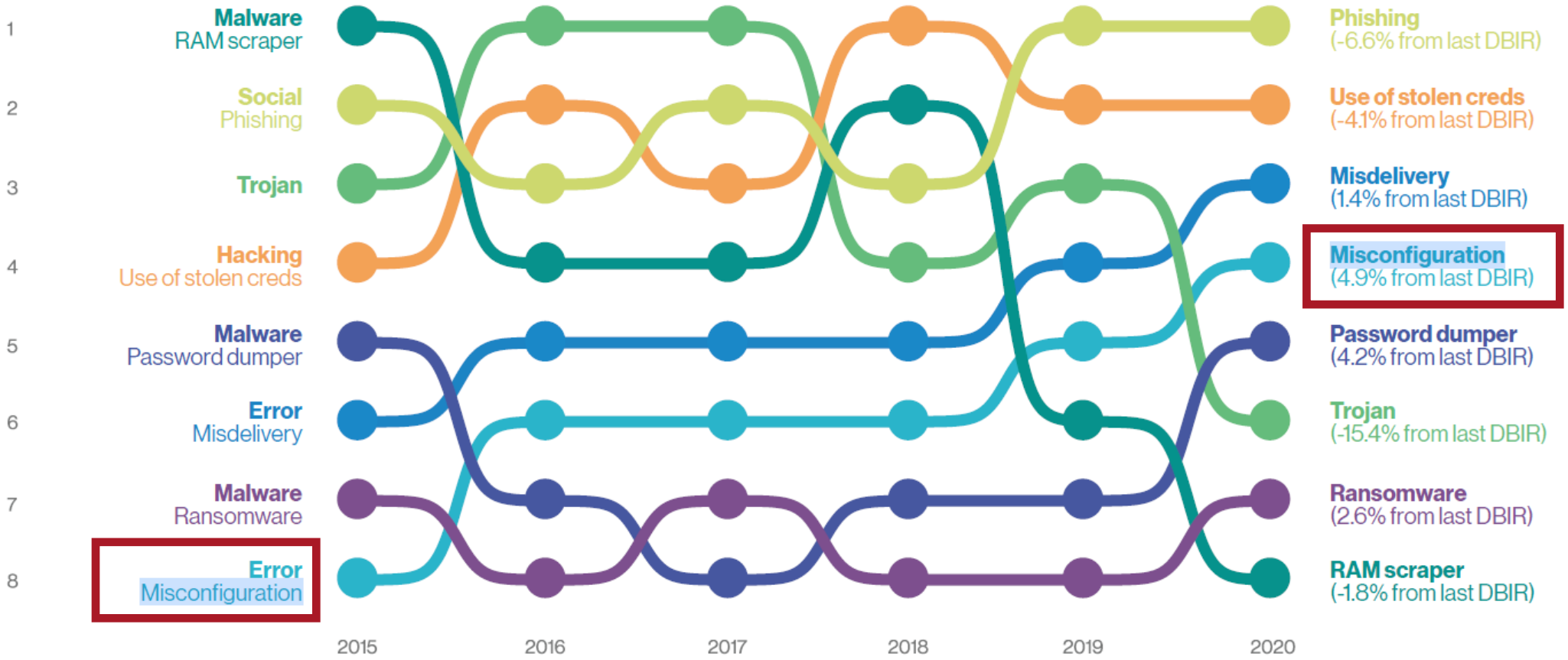


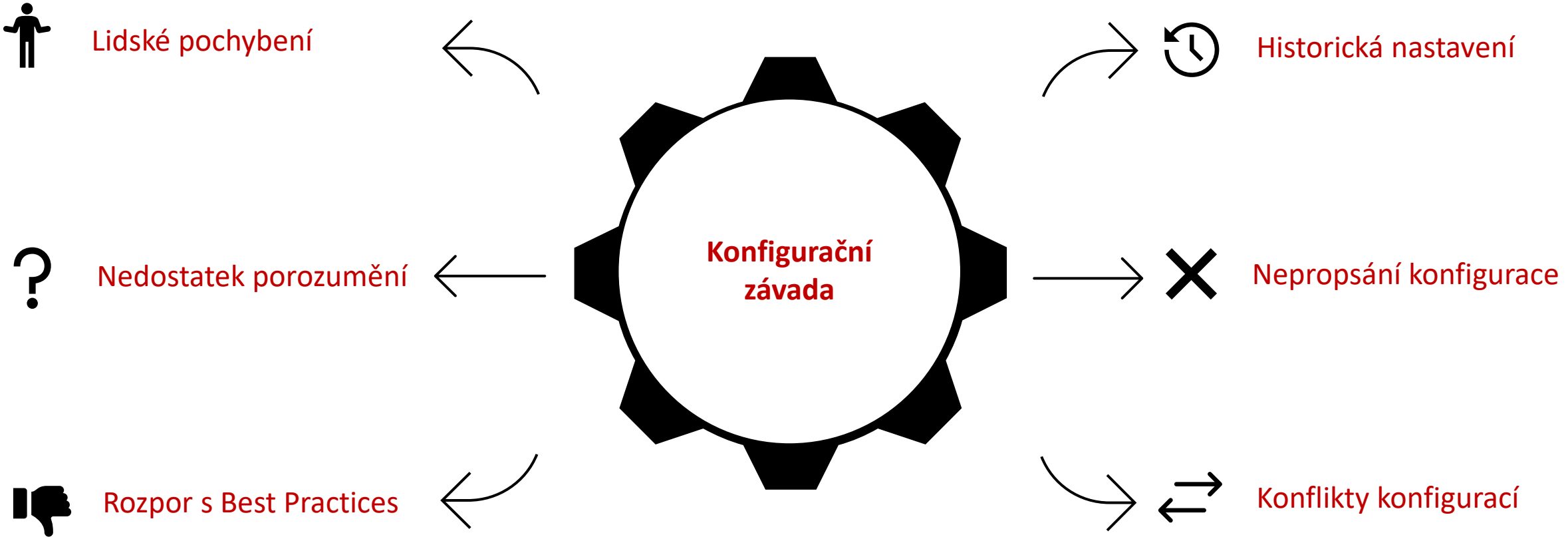
RSM Attack Vectors - Report 2020

"**Misconfigurations** made up of **37%** of all successful attacks over the last two years. These exposures provide multiple pathways to compromise"

Data Breach Investigations Report 2020, Verizon

Figure 6. Select action varieties in breaches over time




Lidské pochybení
Historická nastavení
Konfigurační závada
Nedostatek porozumění
Nepropsání konfigurace
Rozpor s Best Practices
Konflikty konfigurací

7/2018
Založení společnosti

11/2018
1. BETA zákazník

2/2019
Product Launch (Izrael)
1. Zákazník

3/2020
Mezinárodní rozšiřování působení společnosti

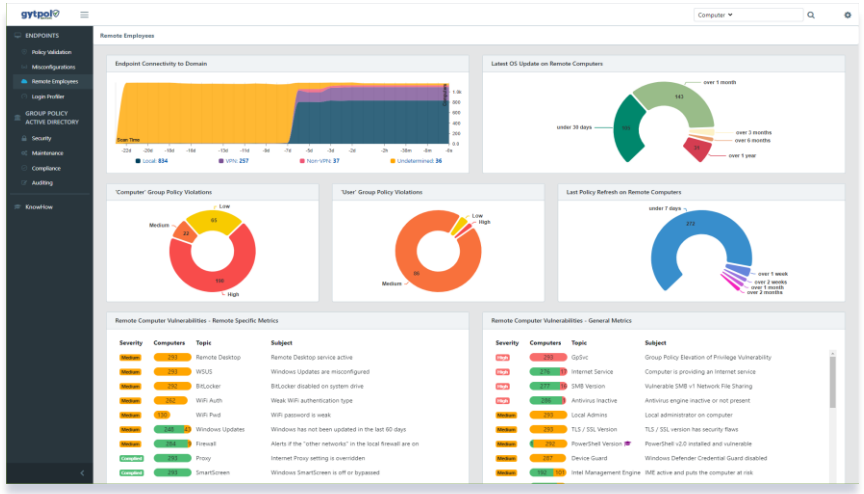
9/2022
Globální působnost,
2M+ chráněných zařízení

... a desítky dalších společností napříč obory

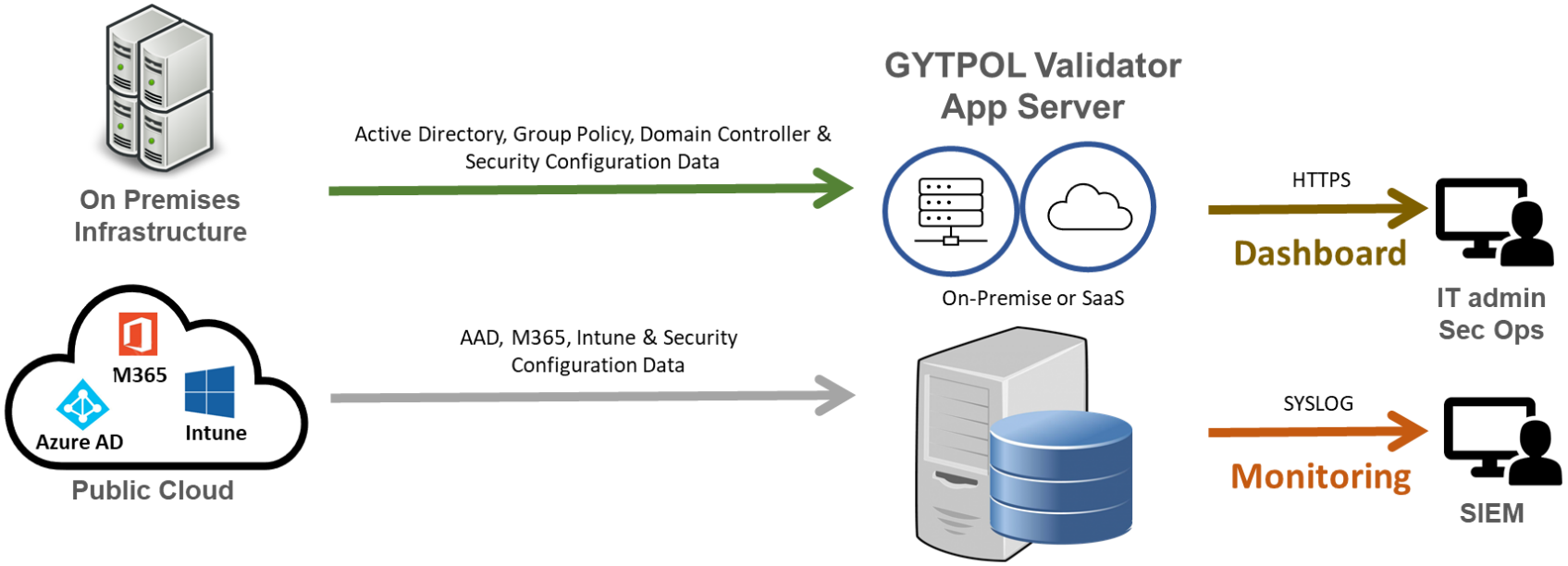
- Finance & Banking
- Zdravotnictví
- Výroba a služby
- Vládní organizace a ozbrojené složky

GYTPOL VALIDATOR

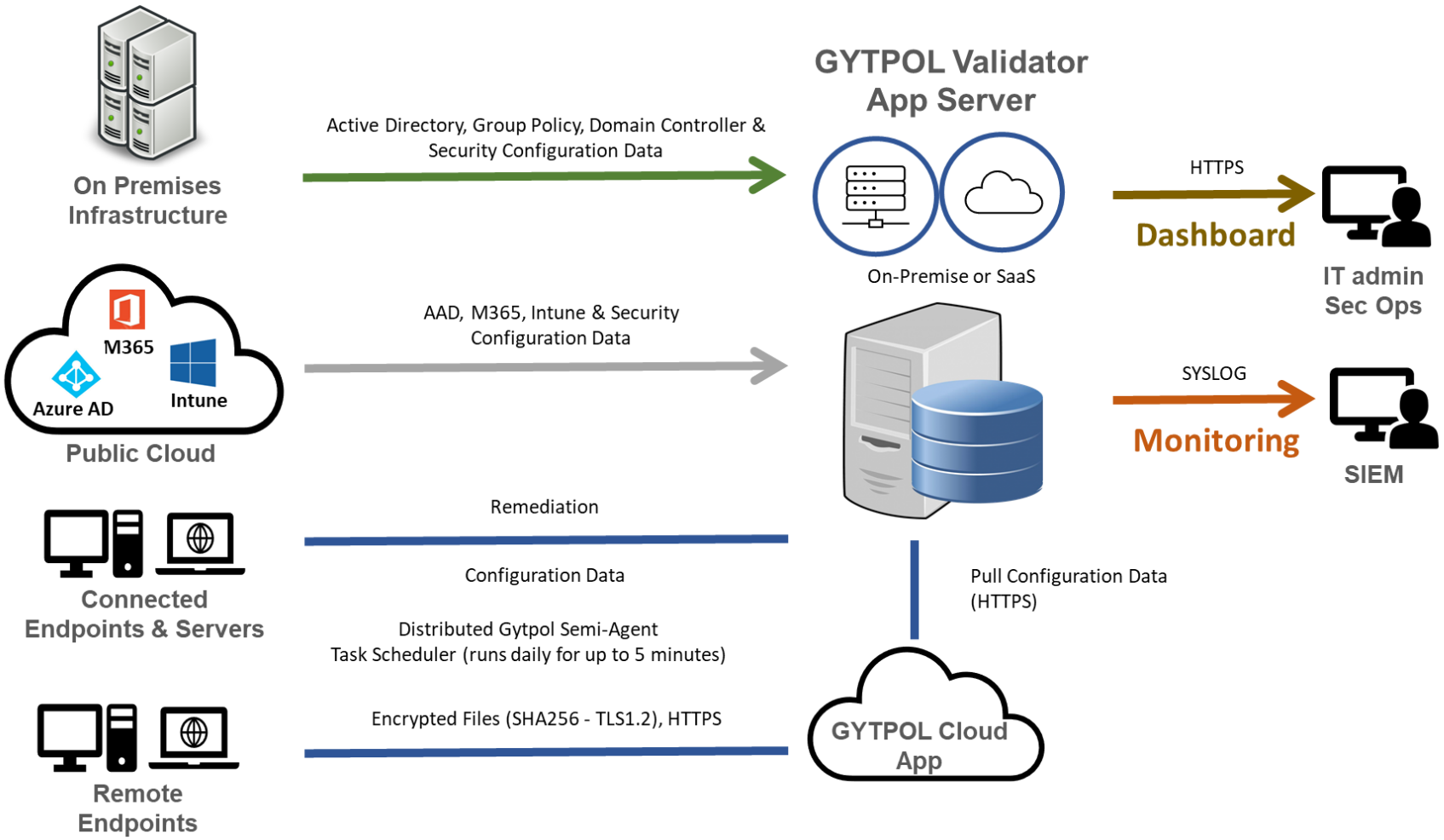
- **Unikátní technologie.** Monitoruje, detekuje a napravuje bezpečnostní rizika plynoucí z konfiguračních zranitelností a nekorektně prosazených politik.
- **Prosvětluje temná zákoutí**. Poskytuje kompletní náhled na rizika spojená s konfigurační bezpečností nehledě na to, jestli se monitorované zařízení nachází v podnikové síti, či patří zaměstnanci pracujícímu z domova.
- **Kompletní pokrytí**. Pracovní stanice a servery, On-Premise infrastruktura, cloud či hybridní prostředí.



ARCHITEKTURA



ARCHITEKTURA



Detekční schopnosti

- **Vyhledávání rizik v rámci AD / AAD / O365 / GPO / Intune / Windows / Linux**
  - Nesoulad politik – DC vs. Koncový bod / Uživatel
  - Konflikty konfigurací / Orphaned policies u zařízení i uživatelů
  - Odchylky od Best Practices
  - Rozpor s ISO 27001 / PCI-DSS
  - Cachovaná hesla
  - Neaktivita Endpoint Security
  - Detekce lokálních administrátorů a konfigurací
  - Prověření úrovní oprávnění, detekce eskalace privilegií

- Prezentace via Web-UI či SIEM
- Kategorizace dle závažnosti a postižených aktiv

MOŽNOSTI REMEDIATIONS

- Úprava konfigurace
- Aktualizace SW
- Změny hodnot v registru
- Spuštění aktualizace OS
- Kontrola a aplikace skupinové politiky

ZPŮSOBY VYUŽITÍ

- **Hodnocení rizik v oblasti konfigurační bezpečnosti**
  - Definice a zapečetění bezpečného standardu konfigurací
  - Bezpečnostní monitoring Active Directory
  - Prověřování konfigurací Group Policy
  - Detekce zranitelností pracovních stanic a serverů
  - Dohled nad hybridním prostředím
  - Analýza vzdálených PC
- **Reakce na incidenty**
  - Detekce bočního pohybu
  - Detekce přípravných fází kybernetického útoku
  - Nápravné procesy

REAKCE NA AKTUÁLNÍ HROZBY

- **Velice pohotový a flexibilní přístup k vydání updatů adresujících aktuální hrozby**
  - Log4J / Log4Shell vulnerability
    - Detekce neaktualizovaných instancí napříč koncovými body
    - Automatizovaný mechanismus nápravy – Virtual patch
  - Folina
    - Do 24h Detect & Remedy

  - Která témata se uživatelů Gytpol vůbec netýkala?
    - Supply Chain útoky skrze SolarWinds
    - Petit Potam (NTLM)
    - Print Nightmare
    - Microsoft Exchange (3/2021)

SHRNUTÍ NA ZÁVĚR

- Detekce širokého souboru doposud přehlížených hrozeb
- Minimální překryvy s ostatními prvky zabezpečení
- Usnadnění a automatizace nápravných procesů
- Využití nejen v oblasti bezpečnosti
  - AD admin — kontrola politik, účtů apod.
  - Security manager/CIO — kontrola zranitelností
  - Compliance — ověření souladu s normami
  - Endpoint admin — sledování startup time, login time
  - SOC Team — propojení na SIEM

COMGUARD
communication security

Děkuji za pozornost!

Lukáš Babčický
lukas.babcicky@comguard.cz

GYTPOL