COMGUARD
communication security

Gytpol

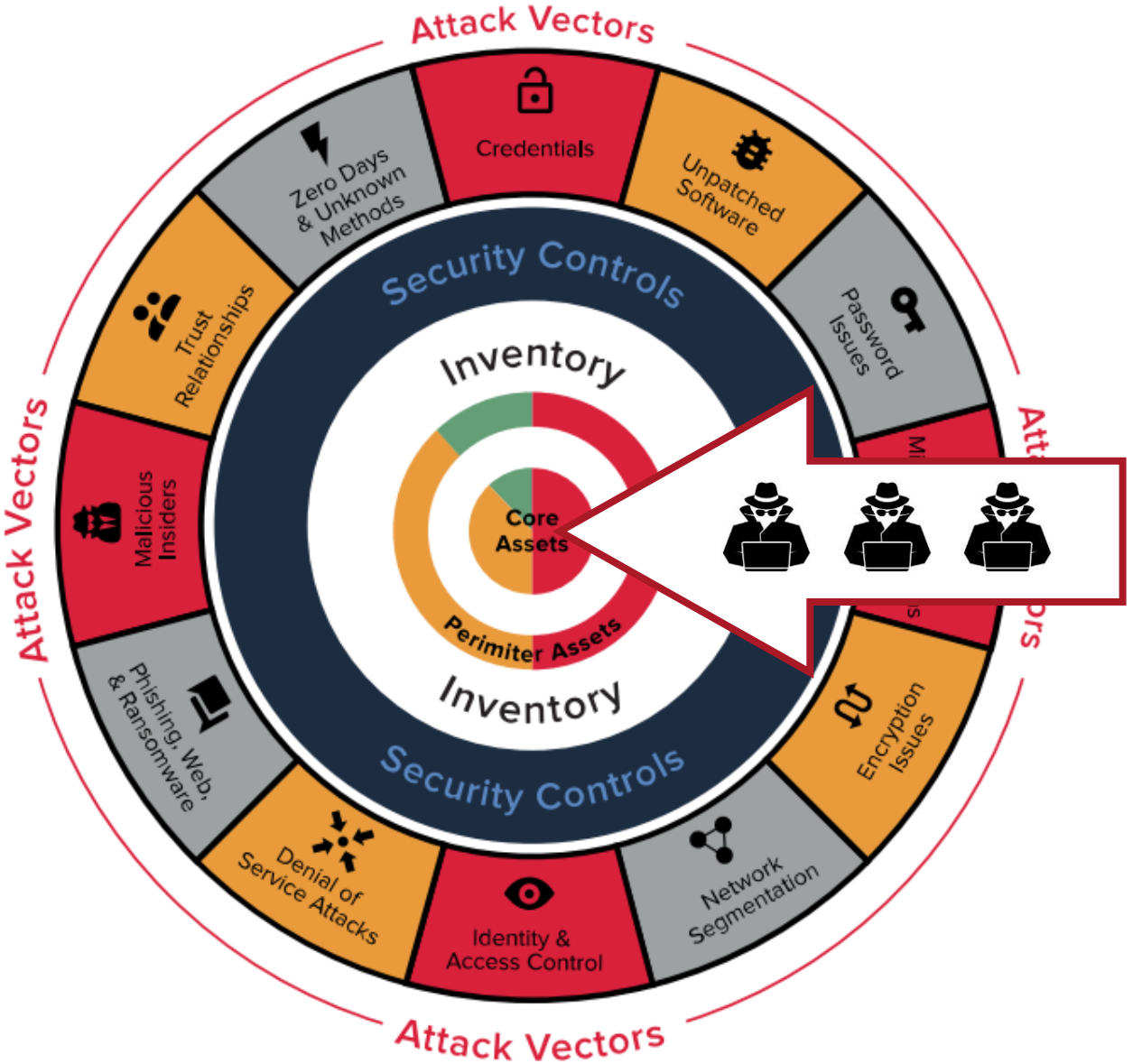
Konfigurační závady jako Achillova pata kybernetické bezpečnosti

Lukáš Babčický | Account & Vendor Manager

Konfigurační závady

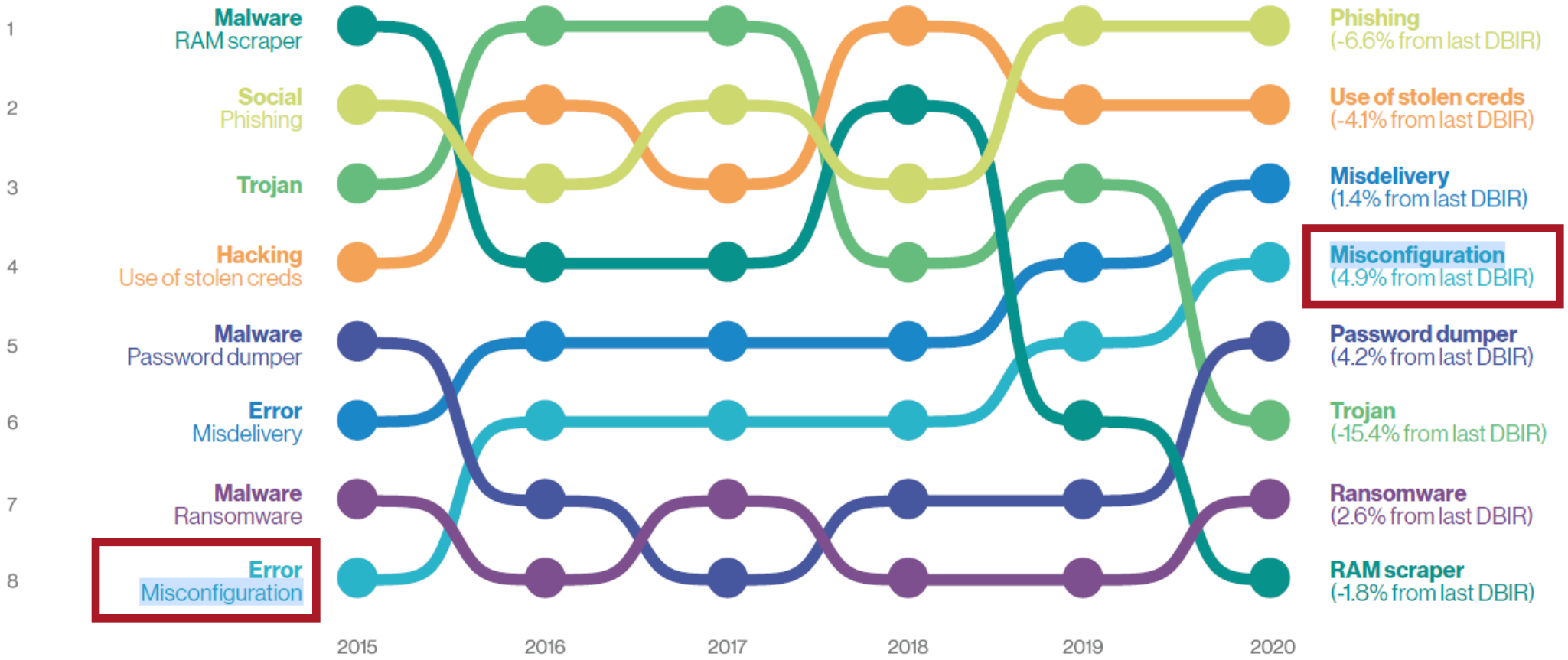
Zneužití konfiguračních závad je běžný vektor útoku.

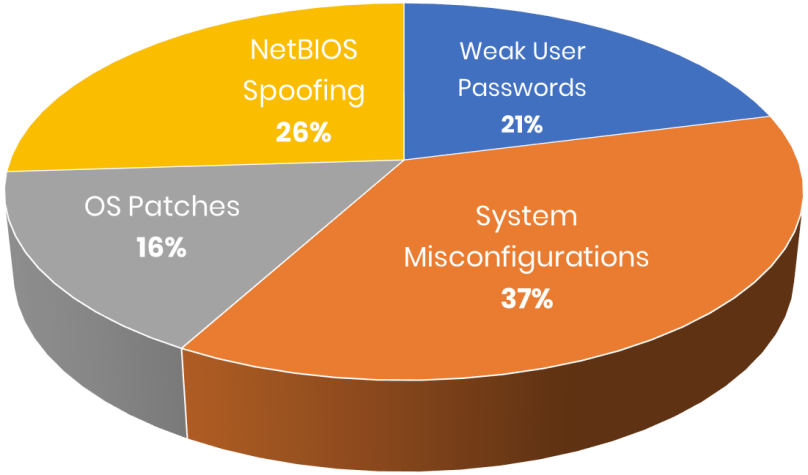
Narůstající četnost zneužívání tohoto vektoru může z vašich endpointů udělat entry-pointy.



Data Breach Investigations Report 2020, Verizon

Figure 6. Select action varieties in breaches over time





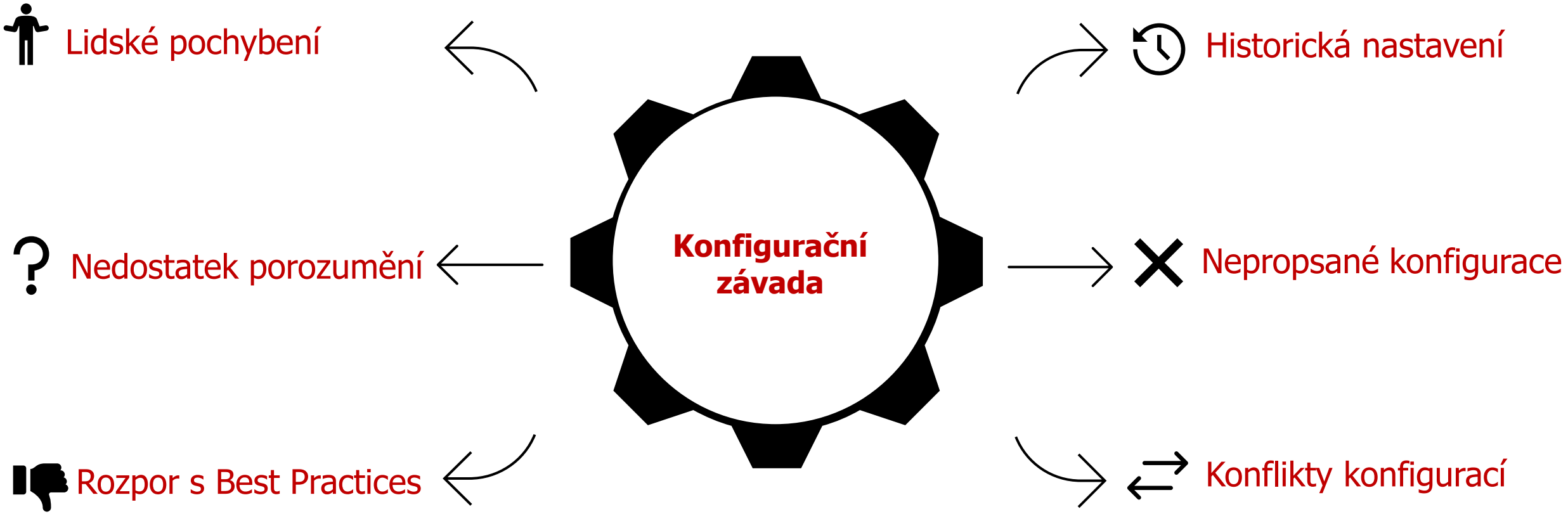
RSM Attack Vectors - Report 2020

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

DARK Reading

DARK Reading- Říjen 2020

"**Endpoint misconfigurations** are responsible for a **third** of all security incidents, and poor remote management policies account for hundreds of thousands of vulnerable systems"


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

GYTPOL

- Izraelská společnost s kořeny v armádních kybernezpečnostních jednotkách
- Spoluzakladatelé stáli u zrodu prvního CheckPoint Firewallu a Symantec antiviru
- „Think like a hacker“
- Gytpol Validator je komerčně dostupný 2 roky a chrání více než 2 miliony zařízení

Check Point SOFTWARE TECHNOLOGIES LTD

INCIDENT RESPONSE TEAM
CHECK POINT

NVIDIA

CYBERARK

salesforce

UPS

… a desítky dalších společností

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

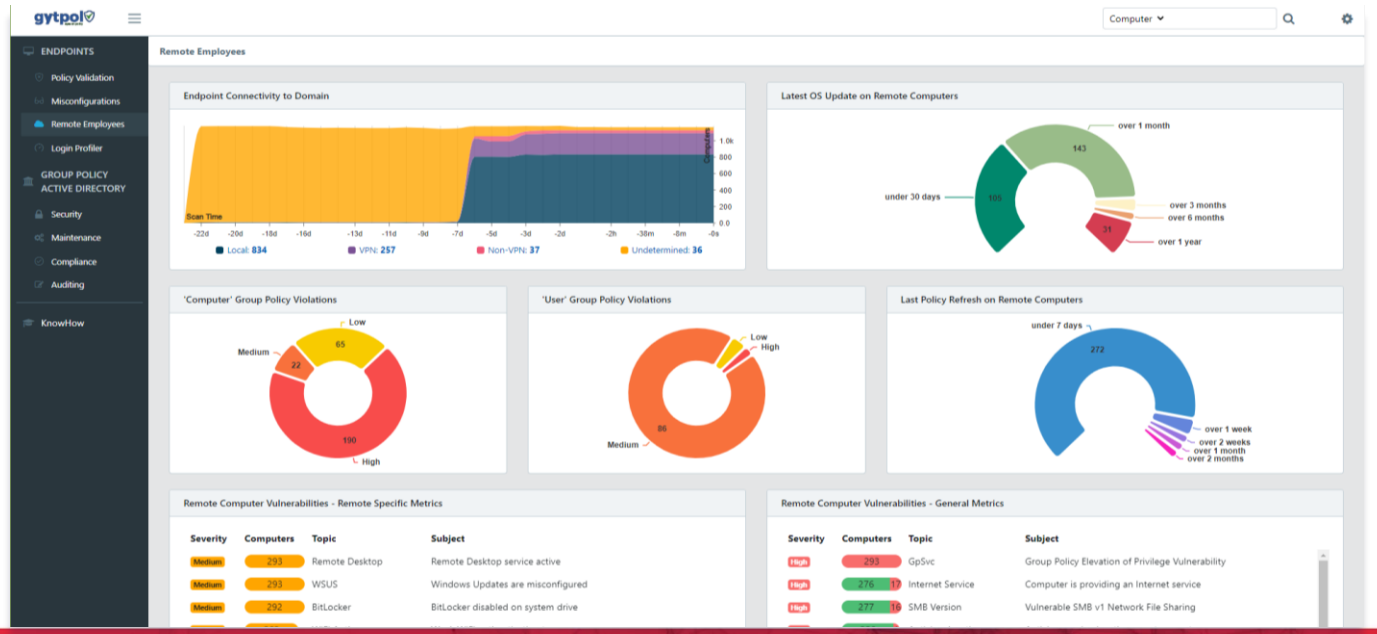
GYTPOL

- Izraelská společnost s kořeny v armádních kybernezpečnostních jednotkách
- Spoluzakladatelé stáli u zrodu prvního CheckPoint Firewallu a Symantec antiviru
- „Think like a hacker“
- Gytpol Validator je komerčně dostupný 2 roky a chrání více než 2 miliony zařízení

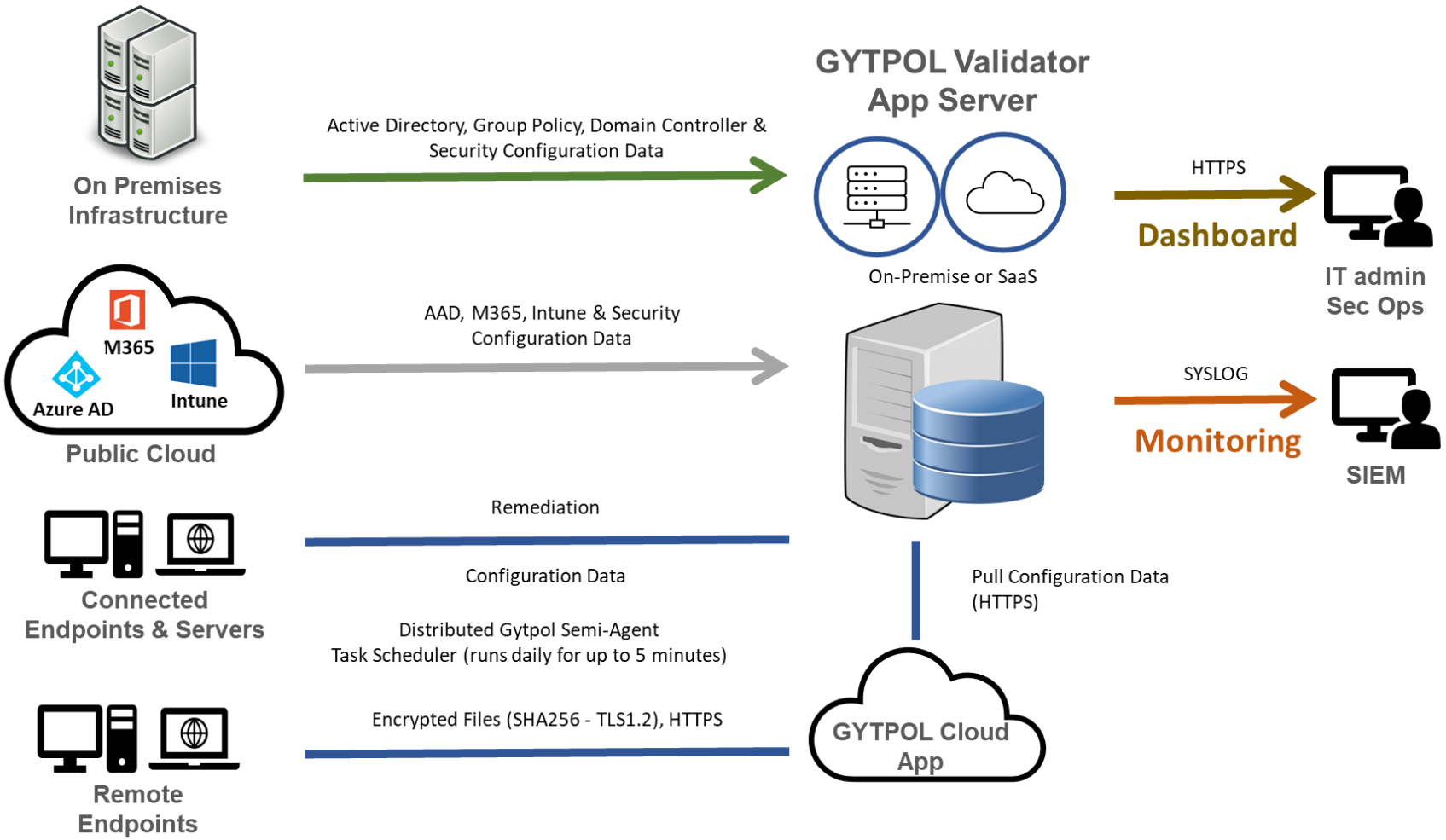
- 5 bezpečnostních manažerů
- Přes 50 tis. chráněných zařízení

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.



GYTPOL VALIDATOR - Architektura



Detekční schopnosti

- **Vyhledávání rizik v rámci AD / AAD / O365 / GPO / Intune /Windows**
  - Nesoulad politik – DC vs. Koncový bod
  - Konflikty konfigurací / Orphaned policies
  - Odchylky od Best Practices
  - Rozpor s ISO 27001 / PCI-DSS
  - Cachovaná hesla
  - Neaktivita Endpoint Security
  - Detekce lokálních administrátorů a konfigurací
- Podpora Linux / MacOS v dalším release

Nápravná opatření

- **Automatizované procesy dostupné u 90% objemu nálezů**
  - Snadné a bezpečné a persistentní
  - Plně v režii administrátorů

  - Kde chceme opravit? PC, uživatel, organizační jednotka, plošně?
  - Chceme opravu zafixovat, resp. zapečetit bezpečný stav?
  - Nebude mít oprava dopady na služby / procesy?

  - Forma nápravy:
    - Úprava konfigurace
    - Změny hodnot v registru
    - Kontrola a aplikace GPO
    - Spuštění aktualizace OS / SW

Způsoby využití

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

- **Reakce na aktuální hrozby**
  - Log4J, Solar Winds Exploits, PrintSpooler Nightmare, NTLM Relay

PoC

- **21 serverů, 5 pracovních stanic**
- **1678 závažných a 2649 středně závažných nálezů**

Alerts

Module	Type	Alerts	High	Med	Low	Passed	Filtered
Validator	Endpoints	42	5	37	0	0	0
	Servers	100	34	17	49	0	0
	Users	30	0	12	18	0	0
Misconfigurations	Servers	1331	638	578	115	612	0
	Endpoints	360	81	252	27	202	0
Miscon. RE	General Metrics	1634	719	773	142	786	0
	Remote Metrics	57	0	57	0	28	0
GP AD	Security	1147	198	908	41	250	0
	Maintenance	4106	0	6	4,100	19	0
	Compliance	0	0	0	0	0	0
	Auditing	18	3	15	0	28	0

Shrnutí na závěr

- **Unikátní nástroj, aktuálně neexistuje alternativa**
- **Minimální funkční překryvy s konvenčními technologiemi**
- **Nálezy a nápravy doposud neviditelných závad**
- **Široká paleta využitelnosti – Nejen bezpečnost, ale i provoz**

COMGUARD
communication security

Děkuji za pozornost