COMGUARD

cyber security masters

# Gytpol Validator

## Chybovat je lidské, odpouštět je božské (hacker není bůh)

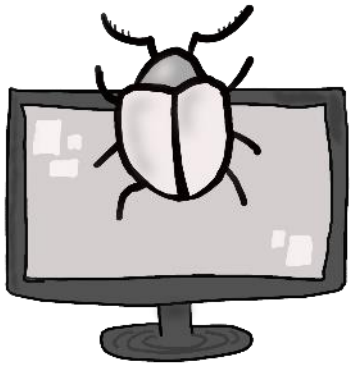
Lukáš Babčický

18.09.2023

COMGUARD

# Teorie miskonfigurací

# Zranitelnost vs. Miskonfigurace



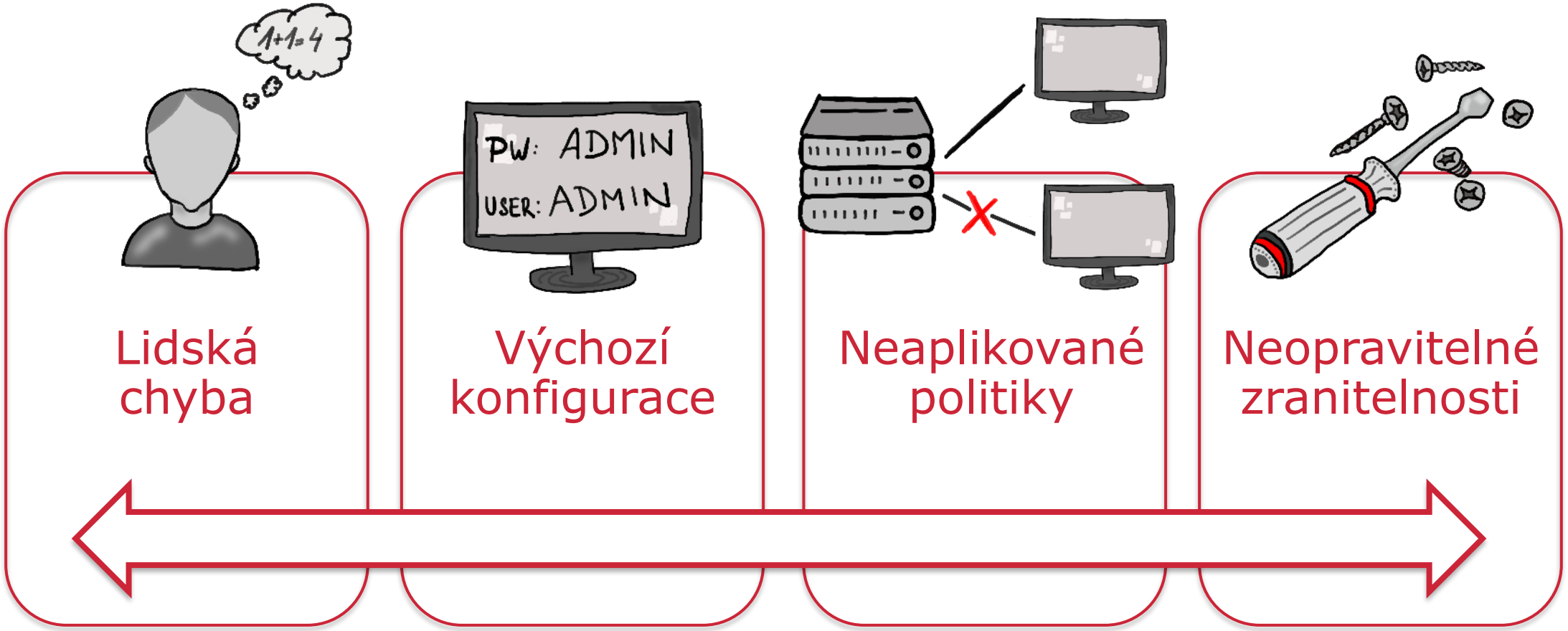
**Zranitelnost** je bezpečnostní chyba přímo v software

Oprava je přímo závislá na vendorovi

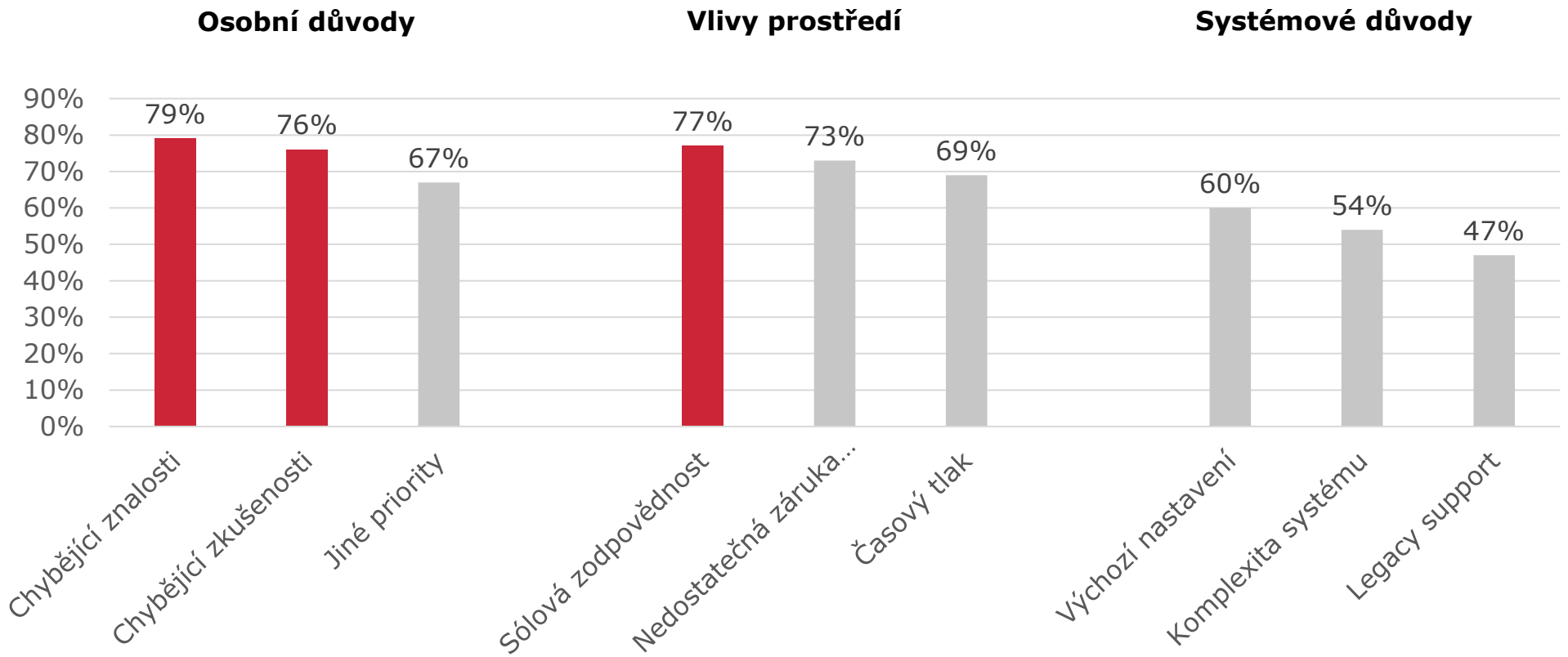
**Miskonfigurace** je bezpečnostní chyba vytvořená konfiguraci software

Oprava je závislá na operátorovi

# Typy miskonfigurací

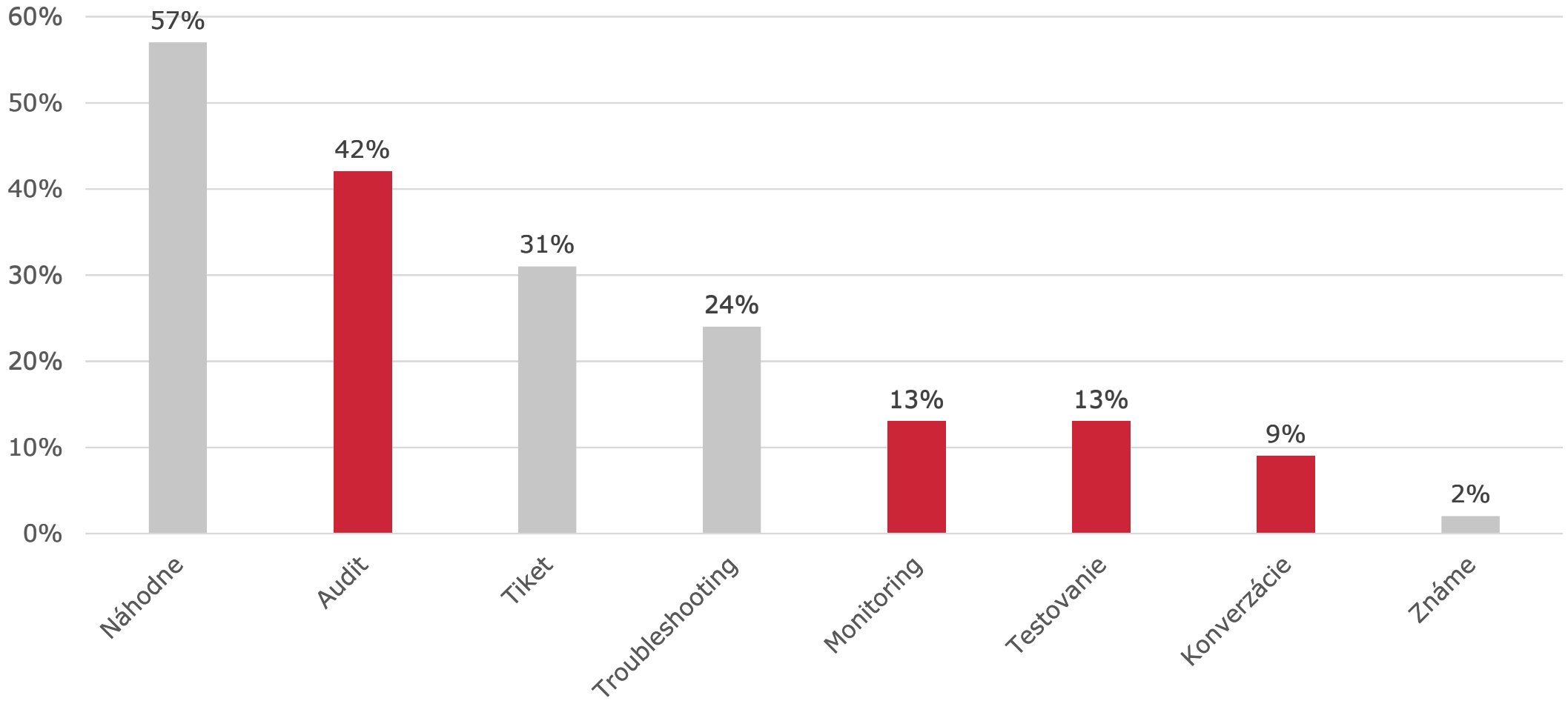


# Jak miskonfigurace vznikají?



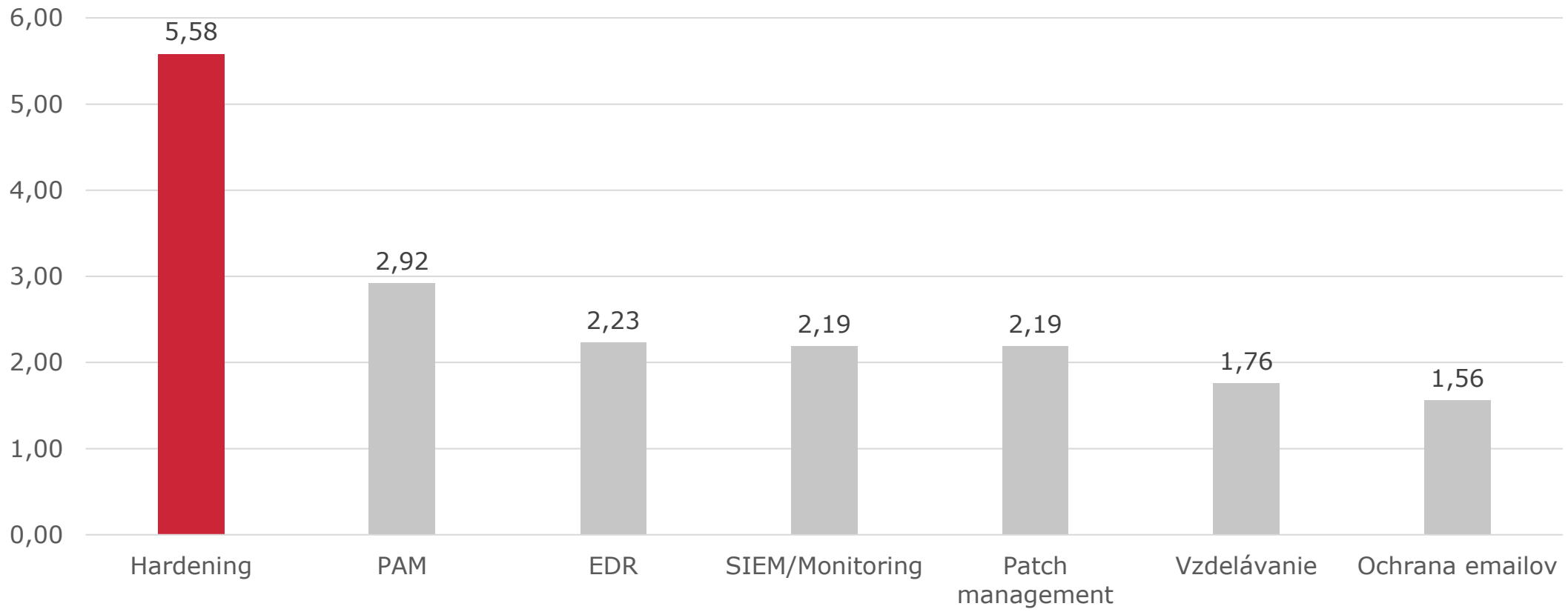

Zdroj: Moving Fast and Breaking Things: Security Misconfigurations
Prof. Dr. Kevin Borgolte, Princeton University

# Jak dojde k jejich nálezu?



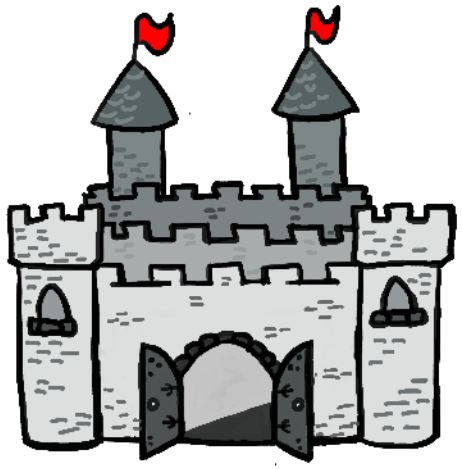

Zdroj: Moving Fast and Breaking Things: Security Misconfigurations
Prof. Dr. Kevin Borgolte, Princeton University

# Hardening – doplnok alebo priorita?

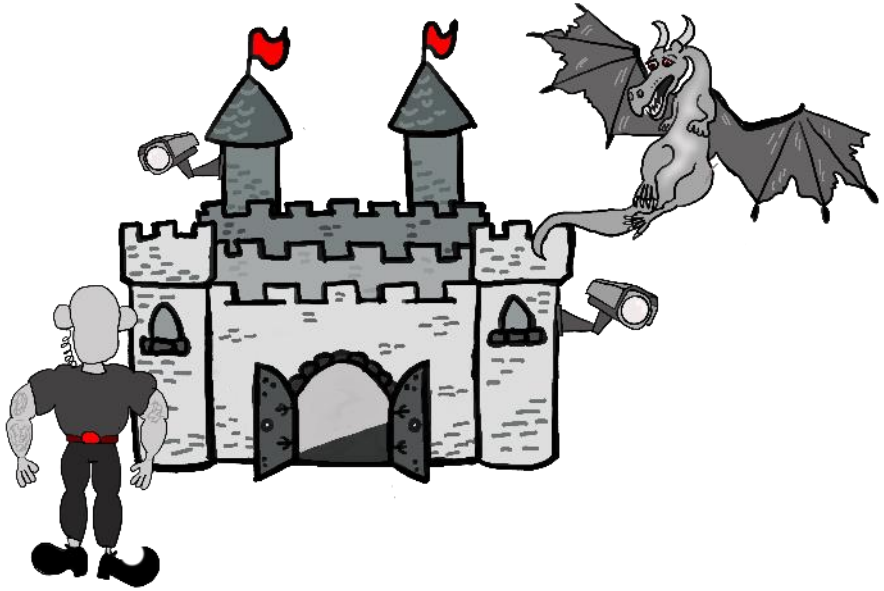



Zdroj: Marsh McLennan – Using data to prioritize cybersecurity investments

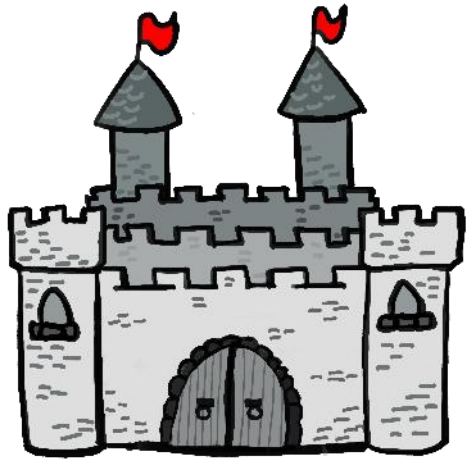
# Hardening – doplnok alebo priorita?



**Bez ochrany**



**PAM, EDR, SIEM,...**



**Hardening**

# Příklady miskonfigurací

# Sdílené složky

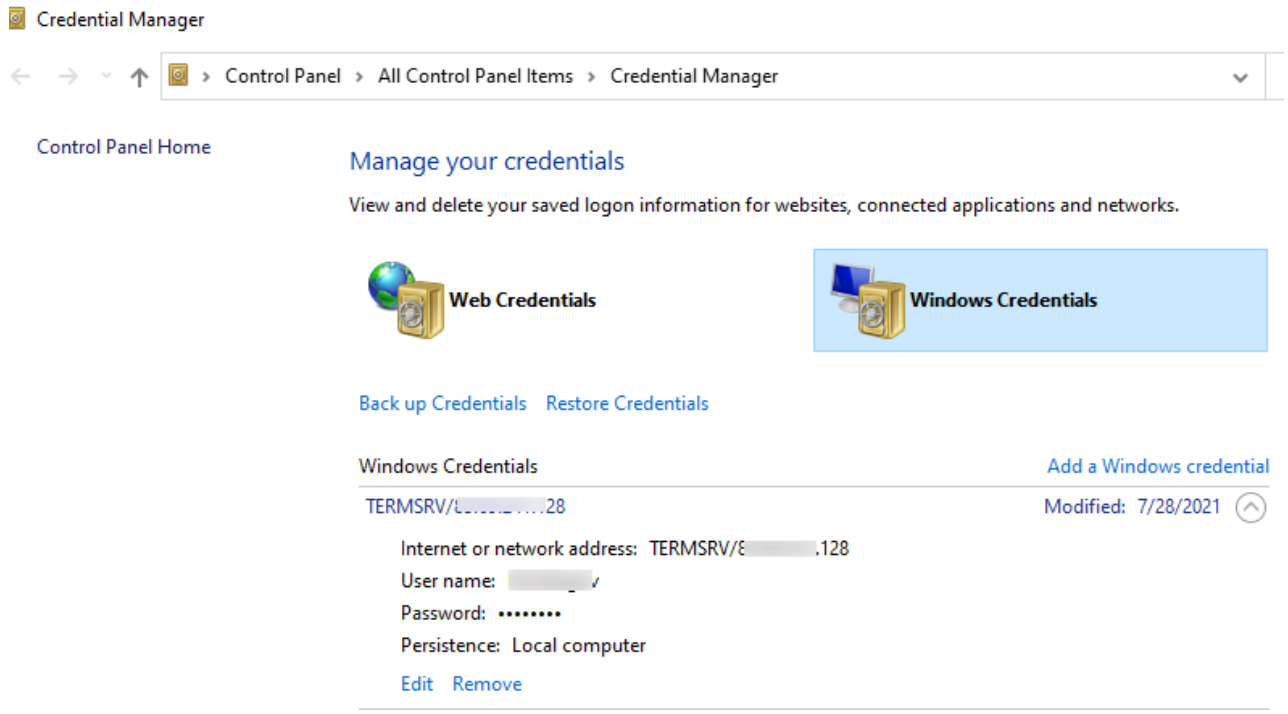

*McDonalds unikla data o 4,8 mil. uživatelích z verejného SMB share. (2023)*


*Microsoft uniklo 2.4 TB dat z nekorektně nakonfigurovaného Azure Blob Storage bucket. (2022)*

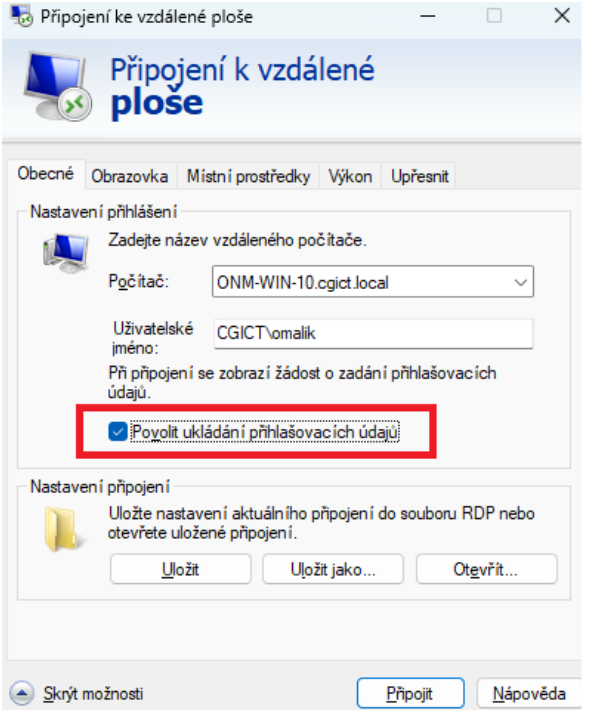

*V rámci Lateral Movement odhalil útočník hardcoded credentials v powershell skriptu, ve veřejně dostupném sSMB sharu. (2022)*

# Windows credential manager

## Uložené credentials




## RDP klient



# New Technology LAN Manager (NTLM)

- Ve větších / starších AD je velmi obtížné se této konfigurace zbavit
- **Útoky:** Pass-the-Hash, Net-NTLMv2 relay

COMGUARD

# Eliminace miskonfigurací

Prevence, detekce, výzvy

# Detekce

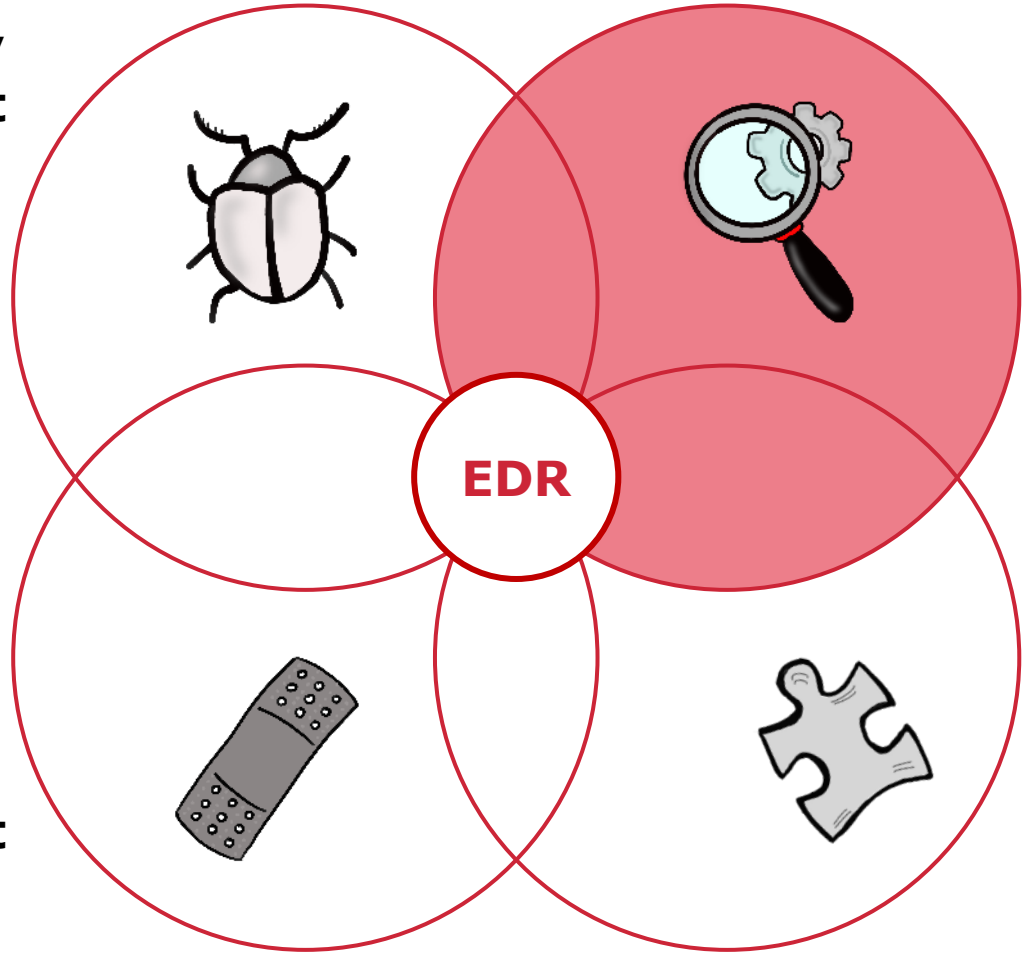
- Auditní nástroje?
  - AD checker, Policy Auditor etc.
  - Jedná se primárně o compliance checkery

- Co nám dají?
  - Jednorázový report
  - Health score z klíčových ukazatelů
  - Okrajový náhled na miskonfigurace

# Běžně užívané nástroje

**Vulnerability Management**

**Secure Configuration**
Formou manuálních procesů




**Patch Management**

**Configuration Management**

# Mitigace

- Jak napravit?
  - Co je ideální stav? Google / dokumentace / info od komunity

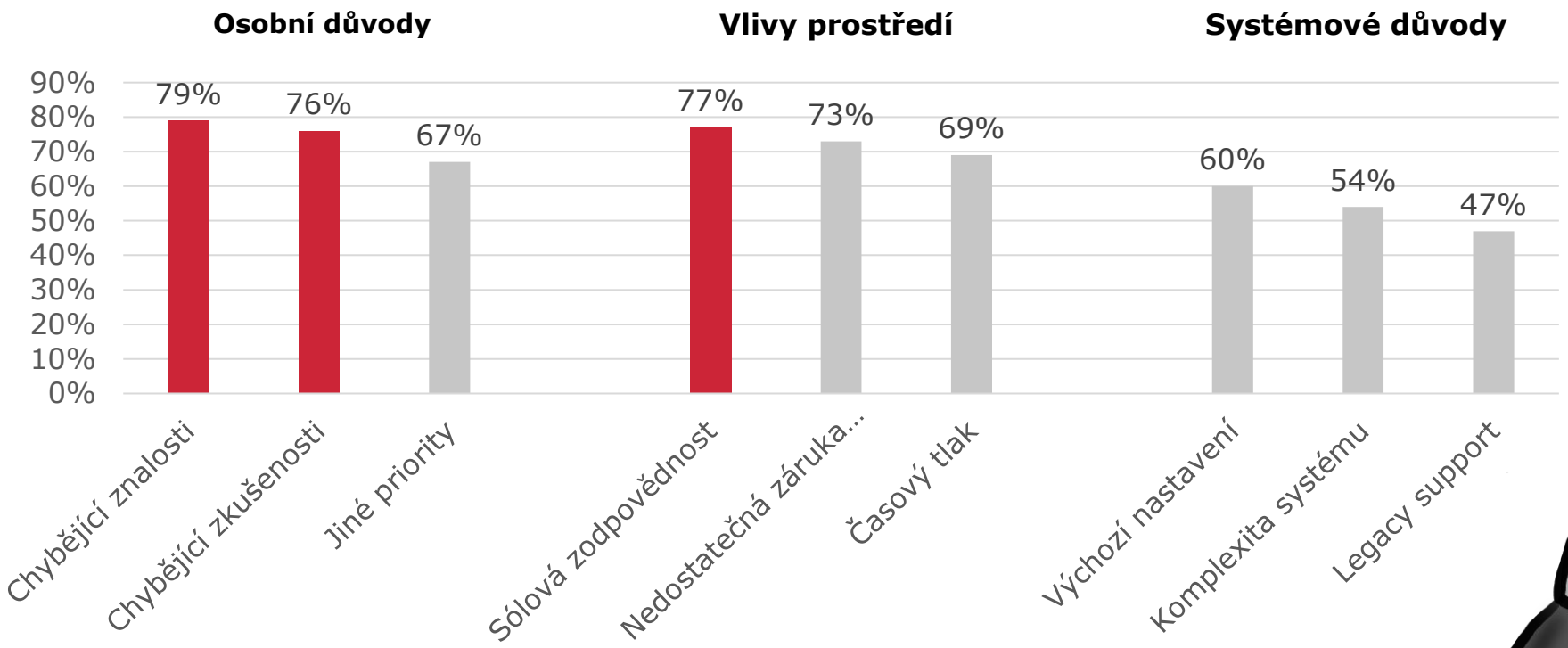
- Budeme fungovat? Miskonfigurace ~ Feature
  - Kdy a jak zjistíme nefunkčnost?

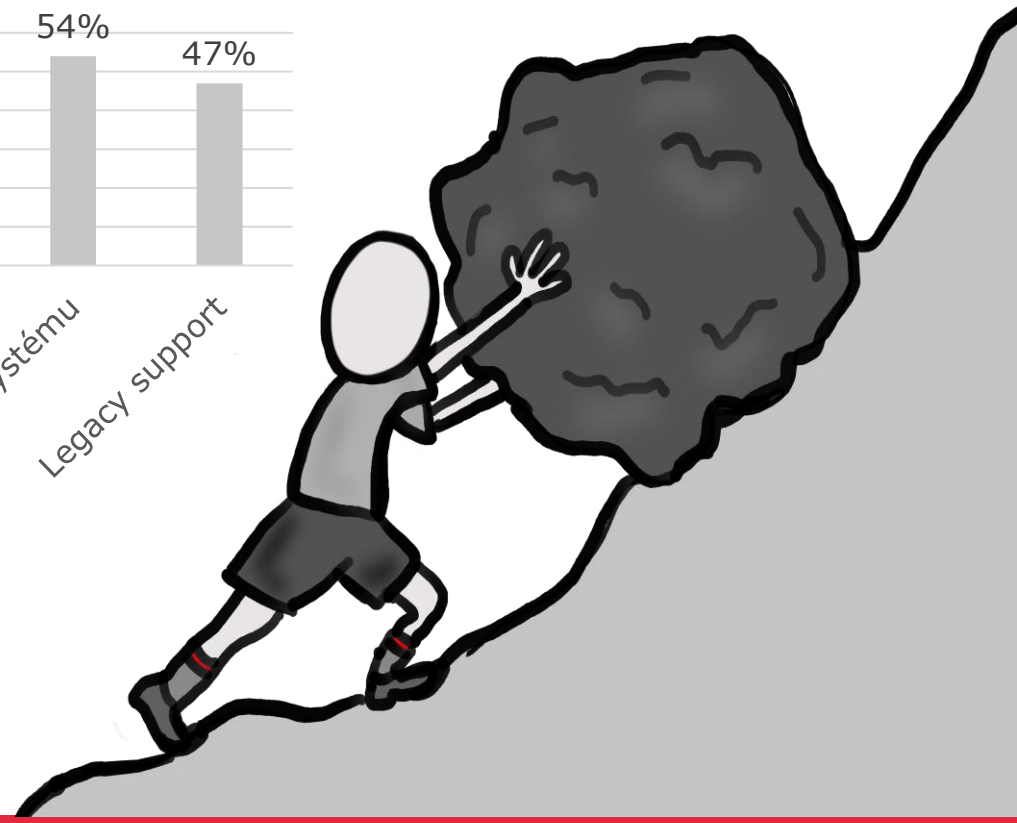

- Nefungujeme – Jak zpět?

# Udržení baseline

- Sdílená odpovědnost
- Dodržování best practices
- Podrobná dokumentace

# Udržení baseline?



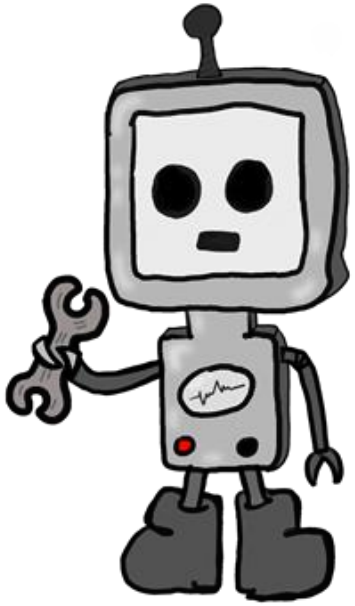
COMGUARD

# Automatizace – Gytpol Validator

Robotu robotům!

# Gytpol Validator - Detekce

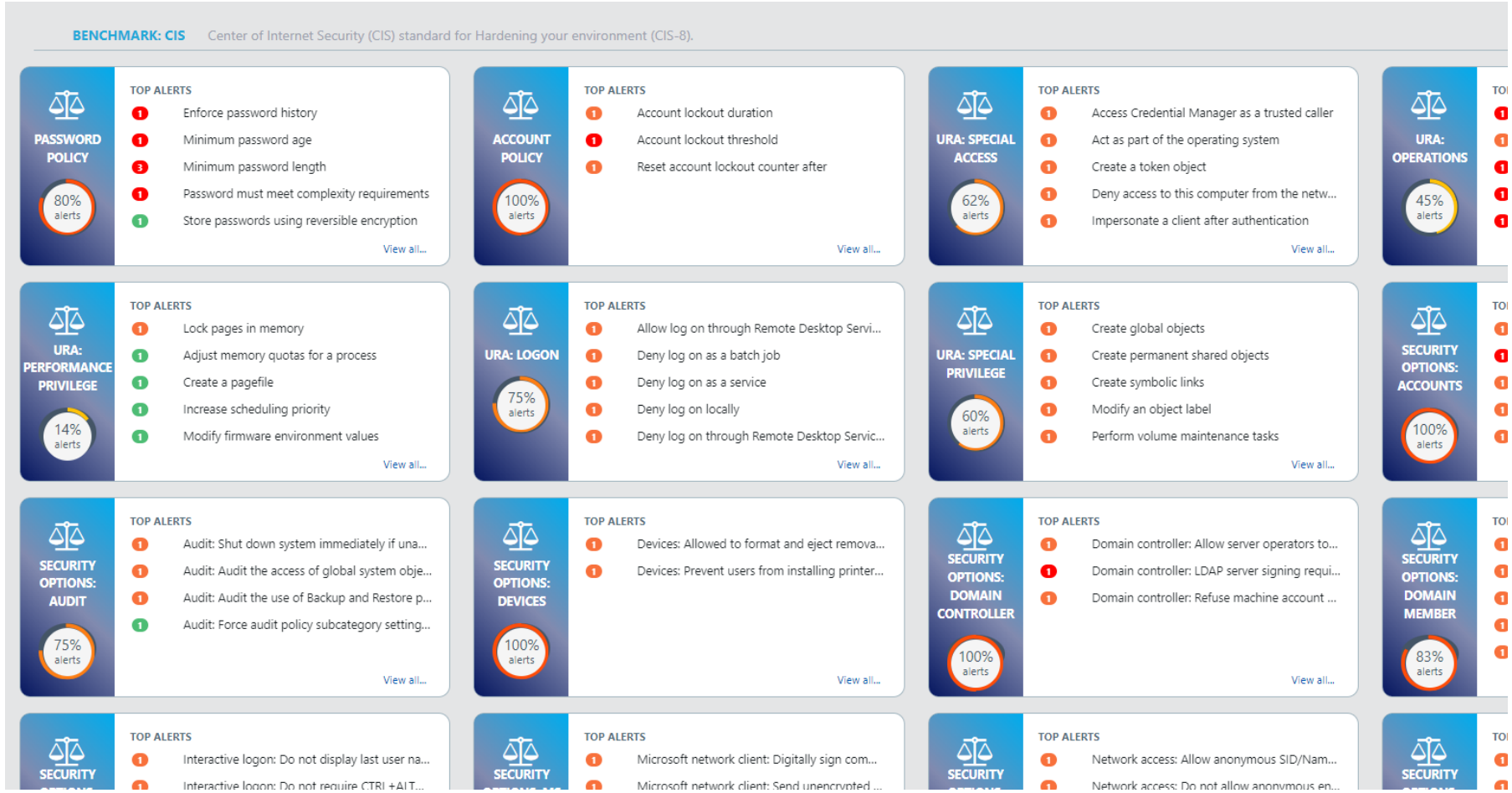
- Neustálý, podrobný dohled až na koncové body
- Dodání kontextu k nálezům
- Široká know-how knihovna



# Gytpol Validator - Mitigace

- Lidský faktor pro informované rozhodnutí
- Prověření dopadu náprav
- Automatizované provedení + rollback

# Mitigace Gytpolem



# Mitigace Gytpolem

**Topic:** SMB Version 1

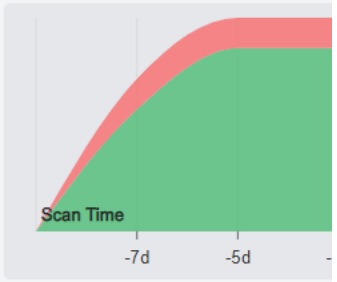
**Subject:** Vulnerable SMB v1 Network File Sharing

**Viewing:** Non-VDI endpoints

**Description:** The computer has SMB v1 installed, which lacks important protection mechanisms offered by later SMB protocol versions. It is a well known security risk, exploited by various ransomware worms, Denial-of-Service and Remote Code Execution attacks. Bear in mind that some legacy software and network printers require SMB v1 to function. less

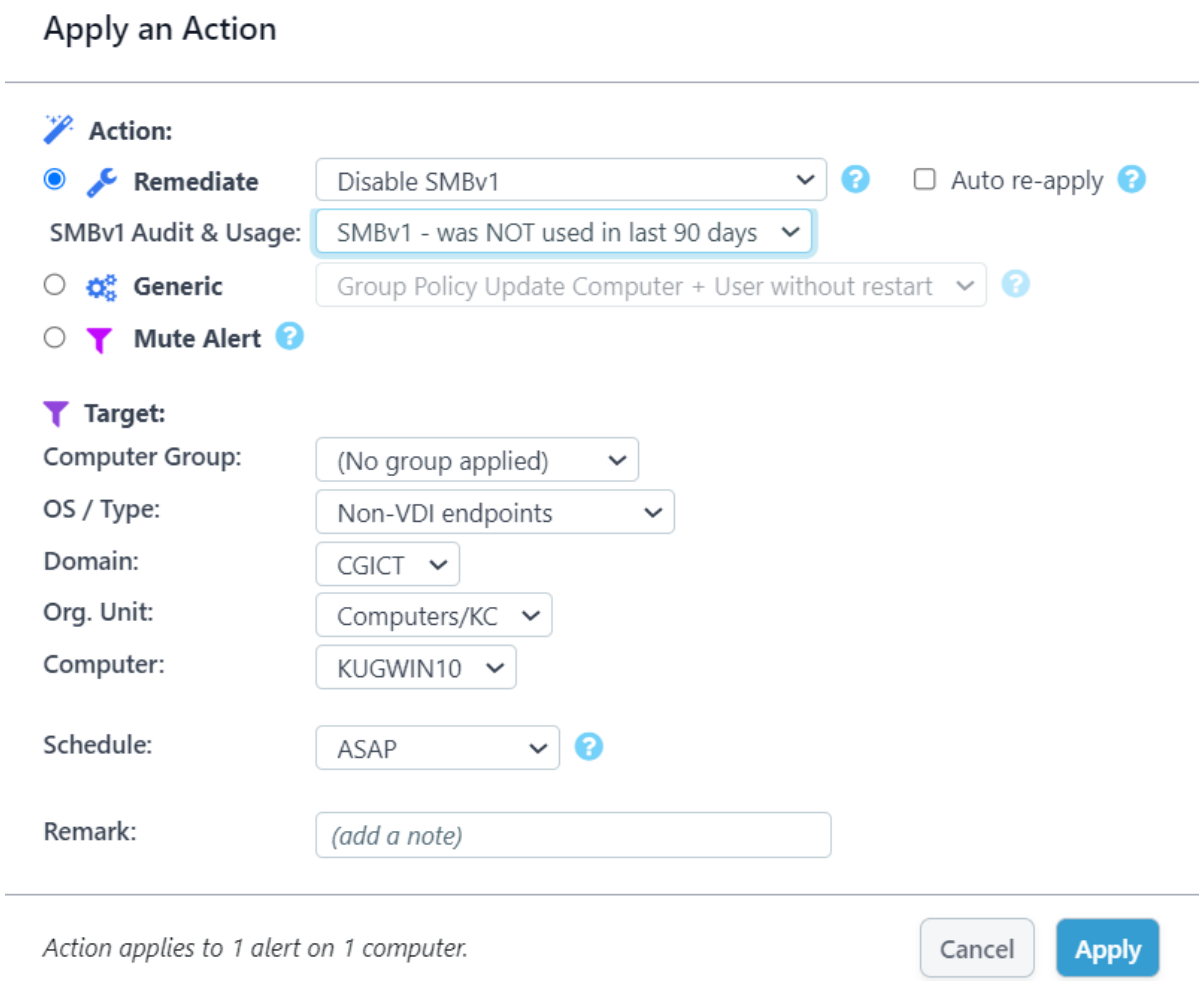
**Suggestion:** It is highly recommended to remove SMB v1 via GYTPOL. Do verify that there's no legacy software or network printers that requires SM more

**Related:** SMB Client Audit, SMBv1 Client Audit, SMBv1 Client Events, Anonymous - Shares Enumeration, Anonymous - Shares&SAM, Everyone to




| Computer | Alerts by Severity | OS | Domain | Org. Unit |
|---|---|---|---|---|
| KUGWIN10 | 1 | Win 10 Pro | CGICT | Computers/KC |
| JAB-PC | 1 | Win 10 Pro | CGICT | Computers/KC |
| KUG-GYTPOLTEST | 1 | Win 10 Pro | CGICT | CN=Computers |
| NB23075 | 1 | Win 11 Pro | comguard.cz | SBSComputers/Compu |
| MCAFEE5 | 1 | Win 10 Pro | CGICT | McAfee/Computers/K( |
| MCAFEE1 | 1 | Win 10 Pro | CGICT | McAfee/Computers/K( |
| MCAFEE2 | 1 | Win 10 Pro | CGICT | McAfee/Computers/K( |

# Mitigace Gytpolem



# Zamyšlení závěrem

- Kontinuální vs. ad-hoc řešení?
- Manuální procesy vs. Gytpol?

COMGUARD

cyber security masters

# Děkujeme za pozornost!