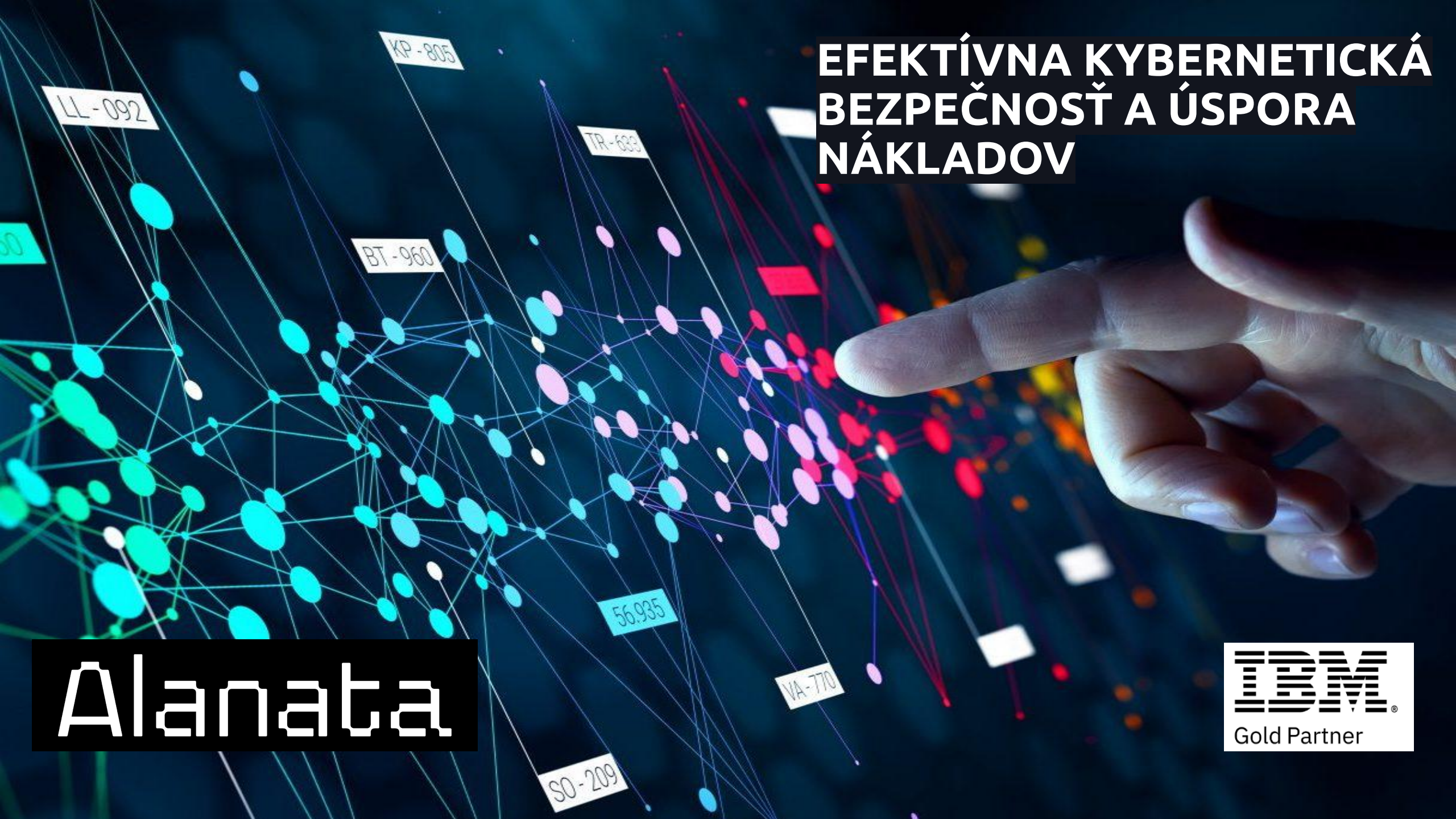
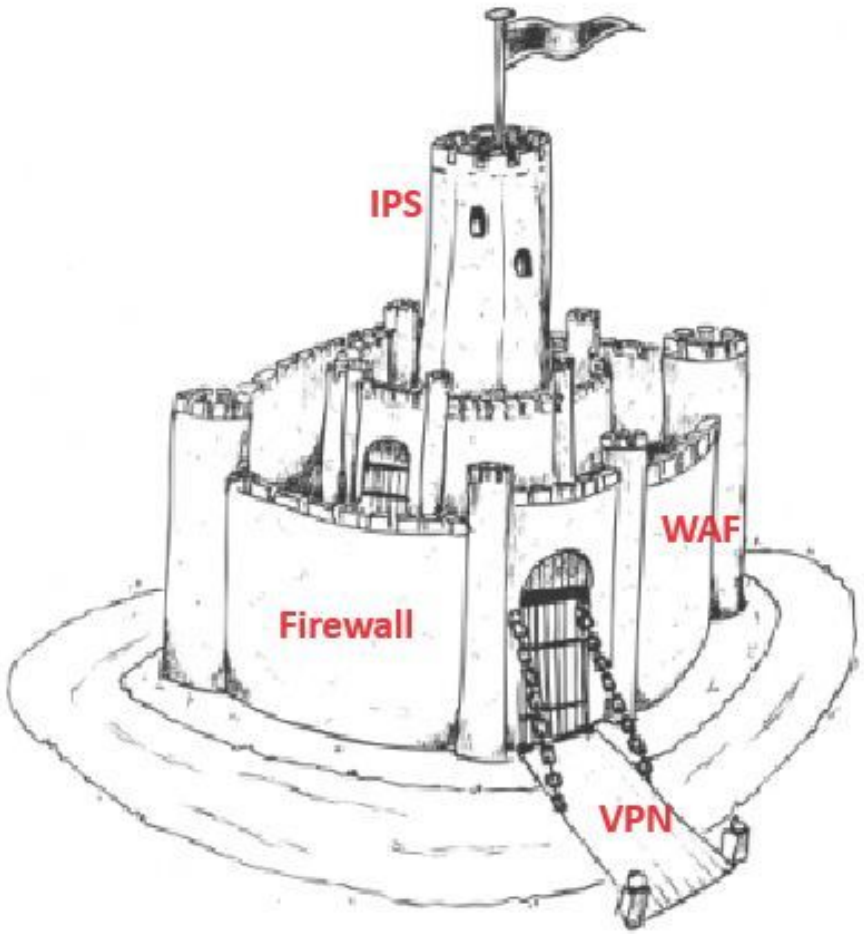
EFEKTÍVNA KYBERNETICKÁ BEZPEČNOSŤ A ÚSPORA NÁKLADOV



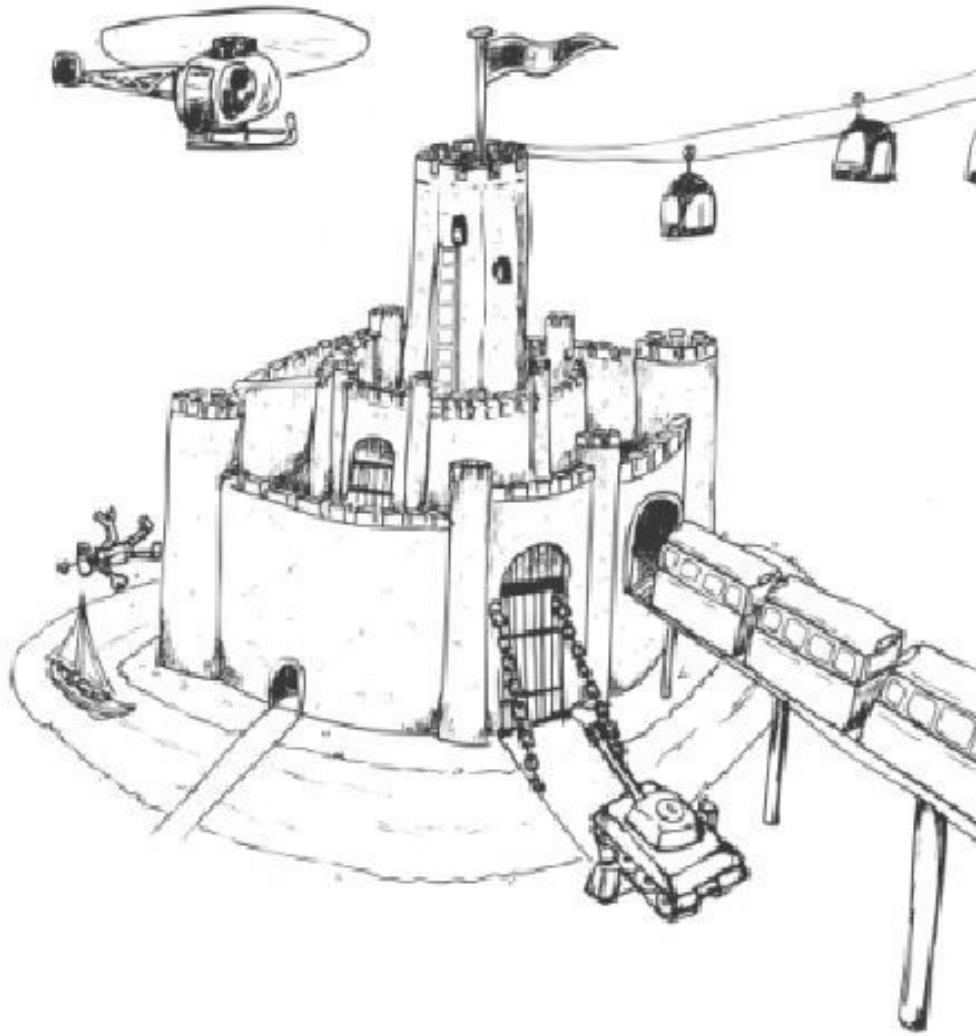
Alanata

IBM Gold Partner

Castle Model of Security



Castle Model in Reality



Ako sa brániť proti neznámym hrozbám?

The Hacker News

Subscribe – Get Latest News

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Store Contact

MITRE Corporation Breached by Nation-State Hackers Exploiting Ivanti Flaws

Apr 22, 2024 The Hacker News Network Security / Cybersecurity

The MITRE Corporation revealed that it was the target of a nation-state cyber attack that exploited two zero-day flaws in Ivanti Connect Secure appliances starting in January 2024.

The intrusion led to the compromise of its Networked Experimentation, Research, and Virtualization Environment (NERVE), an unclassified research and prototyping network.

Trending News

- Kinsing Hacker Group Exploits More Flaws to Expand Botnet for Cryptojacking
- 6 Mistakes Organizations Make When Deploying Advanced Authentication
- Ransomware Attacks Exploit VMware ESXi Vulnerabilities in Alarming Pattern
- Researchers Warn of Chinese-Aligned Hackers Targeting South China Sea Countries
- Rockwell Advises Disconnecting Internet-Facing ICS Devices Amid Cyber Threats

Popular Resources

SECURITYWEEK

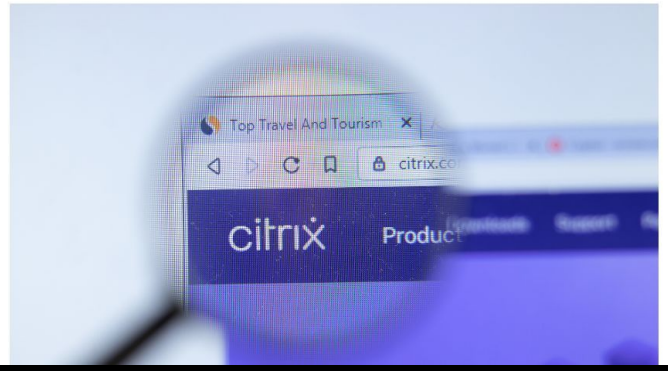
Malware & Threats Security Operations Security Architecture Risk Management CISO Strategy ICS/OT Funding/M&A

VULNERABILITIES

Recent NetScaler Vulnerability Exploited as Zero-Day Since August

Mandiant says the recently patched Citrix NetScaler vulnerability CVE-2023-4966 had been exploited as zero-day since August.

By Ionut Arghire
October 18, 2023



TRENDING

1. Rockwell Automation Urges Customers to Disconnect ICS From Internet
2. Critical Veeam Vulnerability Leads to Authentication Bypass
3. VMware Abused in Recent MITRE Hack for Persistence, Evasion
4. User Outcry as Slack Scrapes Customer Data for AI Model Training
5. Chrome 125 Update Patches High-Severity Vulnerabilities
6. Ivanti Patches Critical Code Execution Vulnerabilities in Endpoint Manager

Bug Highlights

The following are some examples of impactful bugs that we awarded under our new guidelines:

Account Takeover and Two-Factor Authentication Bypass Chain: We received a report from Yaala Abdellah, who identified a bug in Facebook's phone number-based account recovery flow that could have allowed an attacker to reset passwords and take over an account if it wasn't protected by 2FA. We've fixed this bug and found no evidence of abuse. We rewarded the researcher our highest bounty at $163,000, which reflects its maximum potential impact and program bonuses. While we were investigating, the researcher was able to build on an earlier find to chain it to a separate 2FA bypass bug. We've fixed this issue and rewarded the researcher an additional a bounty of $24,700, including program bonuses.

2FA Bypass: We also fixed a bug reported by Gtm Mänôz of Nepal, which could have allowed an attacker to bypass SMS-based 2FA by exploiting a rate-limiting issue to brute force the verification pin required to confirm someone's phone number. We awarded a $27,200 bounty for this report.

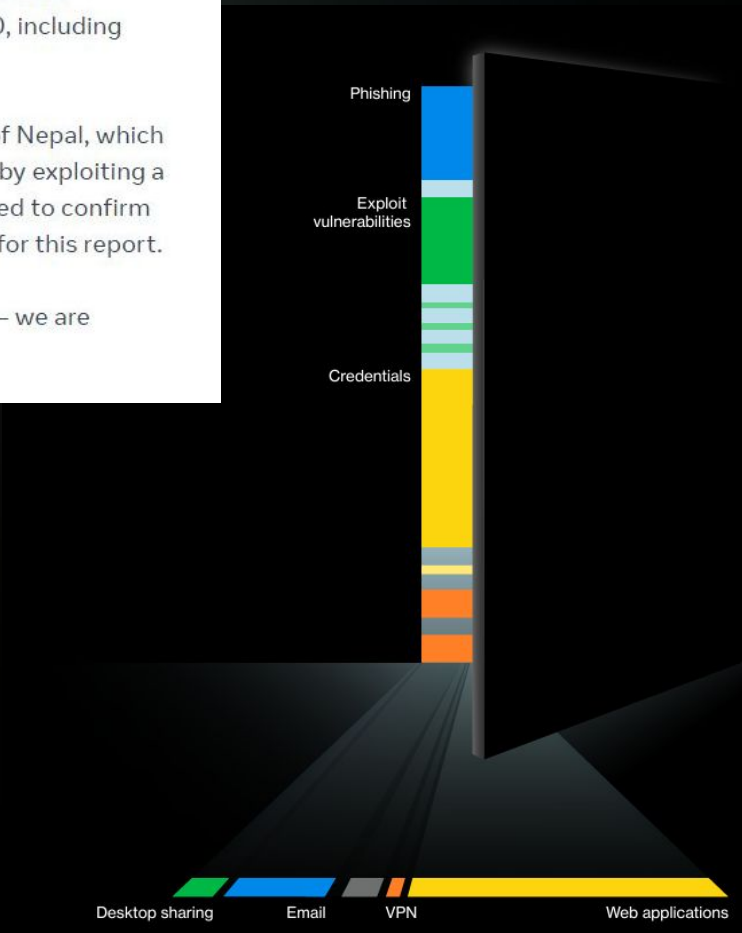
Thank you to the bug bounty community for a great year — we are excited to work together again in 2023.

VPN

security gateway

2FA

firewall



Na čo mi ten SIEM bude?

Vysvetli to laikovi

- Realtime monitoring kybernetickej bezpečnosti
- Prečo potrebujem realtime monitoring?
- IBM report Cost of a Data Breach 2023 hovorí:

277 dní

máte útočníka v sieti do jeho odhalenia

- IBM report Cost of a Data Breach 2024 hovorí:

Priemerné nákladzy spojené s únikom údajov sú až

$ 4,88 mil

Problém s financovaním

Ako zdôvodniť nákup?

- Neprináša zisk
- Potrebujete zdôvodniť nákup a prevádzku riešenia
- SIEM so SOC je niečo ako poistka na auto
- Pri poistnej udalosti rátate škody – buď zaplatíte drobné opravy, alebo to dáte na totálku
- Pomôže vám analýza dopadov na podnikanie?

Ako na to?

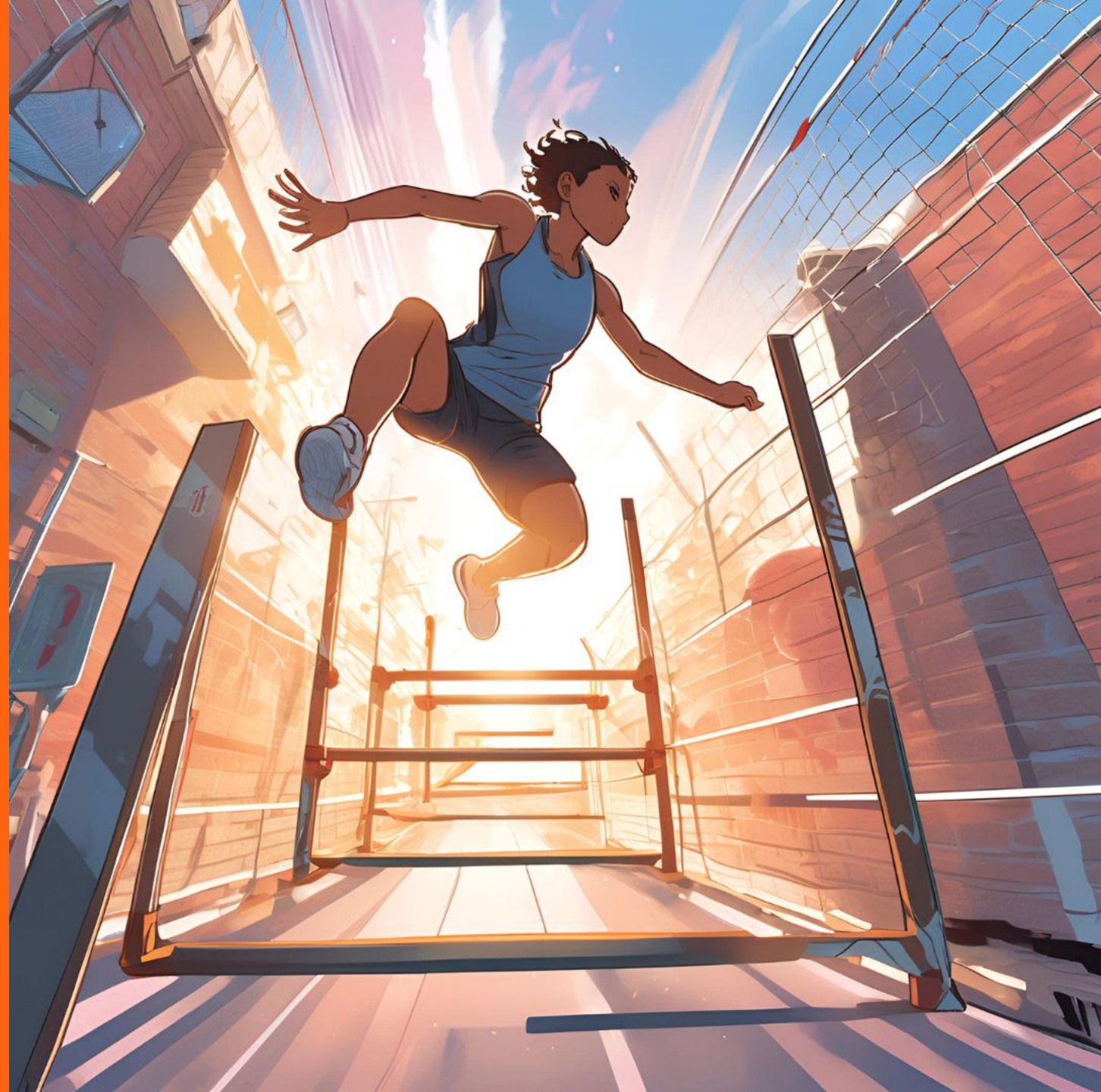
Cez Čísla

- Aká je hodnota vašich zákazníkov?
- Čo sa stane ak prídem o veľkého zákazníka?
- Akú veľkú pokutu zaplatím?
- Koľko ma bude stáť zotavenie z incidentu?
- Koľko ma bude stáť následná investícia do zabezpečenia infraštruktúry a dát?
- O koľko budúcich zákazníkov prídem v dôsledku bezpečnostného incidentu?
- Koľko ma bude stáť obnova reputácie?

Ďalšie prekážky

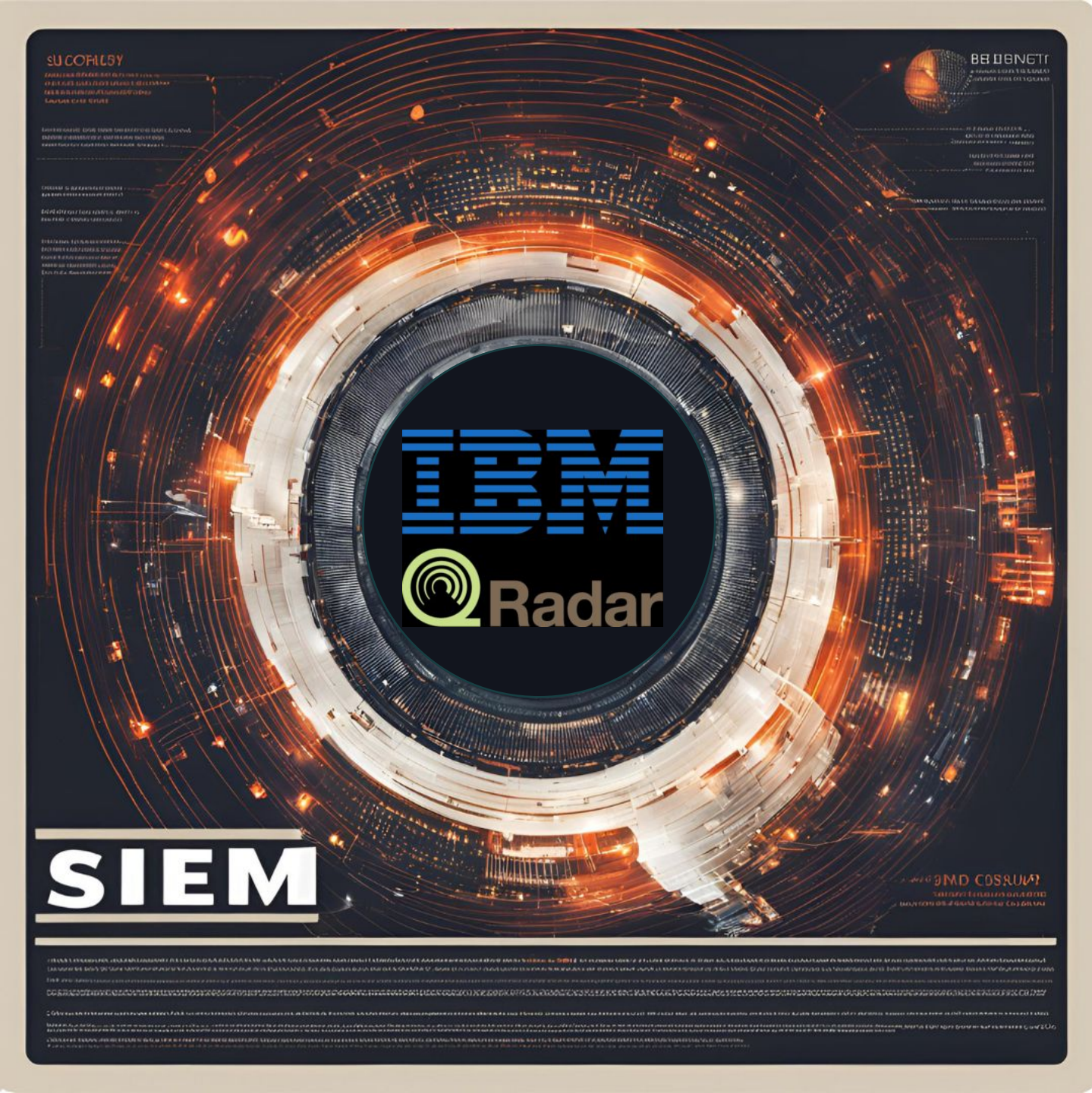
Ako pripraviť tender a ušetriť?

- Nastavte jednoduché kritériá
- Tendrujte jeden produkt
- Optimalizujte budúcu prevádzku
- Keep it simple
- Ak nemáte Špecialistov, outsoursujte
- Nechajte si poradiť od odborníkov



Neobjavené benefity SIEM platformy

- **IBM QRadar** je 2.5x lacnejší ako konkurencia (MVS licenčný model)
- Zlepšuje úroveň manažmentu aktív spoločnosti. Núti vás udržiavať databázu aktuálnu.
- Objaví skryté problémy v predstihu
- Zmapuje za vás nedostatky a chýbajúce prvky kybernetickej bezpečnosti
- Odhalí nepokryté časti infraštruktúry
- Zlepší vizibilitu prostredia
- Pomáha prioritizovať investície



Alanata

Technology Meets Business

Alanata a.s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

www.alanata.sk