

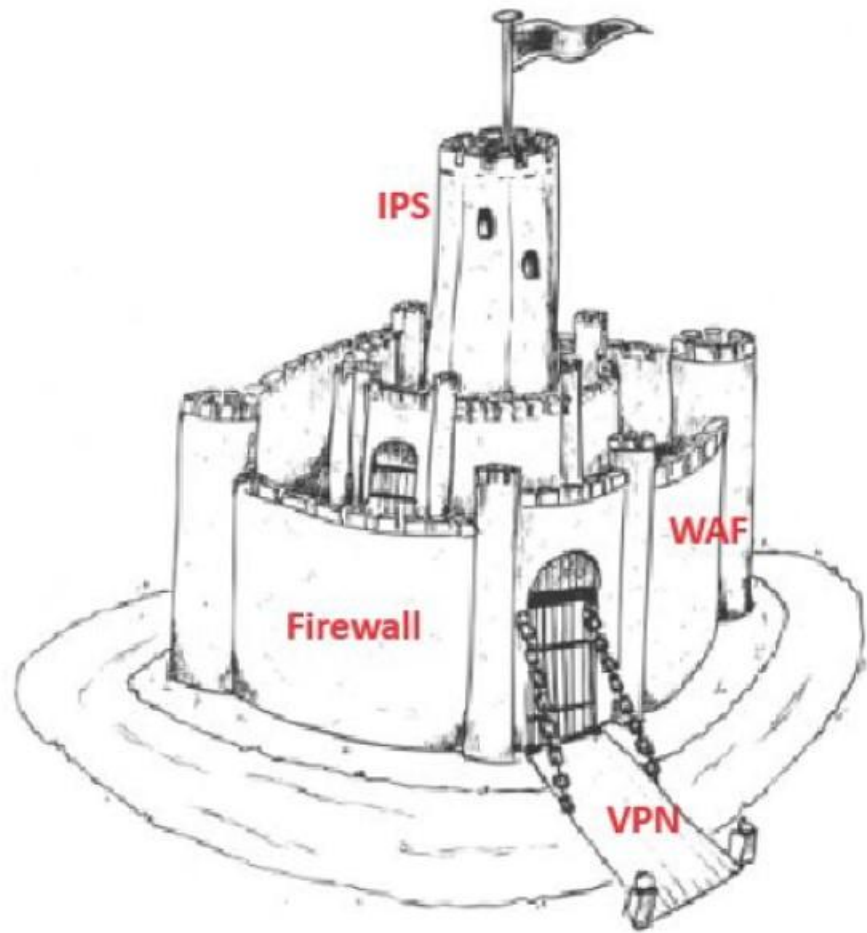
A hand is pointing towards a complex network diagram. The diagram consists of numerous nodes connected by lines, with nodes colored in shades of blue, cyan, pink, and red. Several nodes are labeled with alphanumeric codes: LL-092, KP-805, BT-960, TR-603, 56935, VA-770, and SO-209. The background is dark blue with some blurred light effects.

# INOVATÍVNE RIEŠENIA V BOJI S KYBERNETICKÝMI HROZBAMI

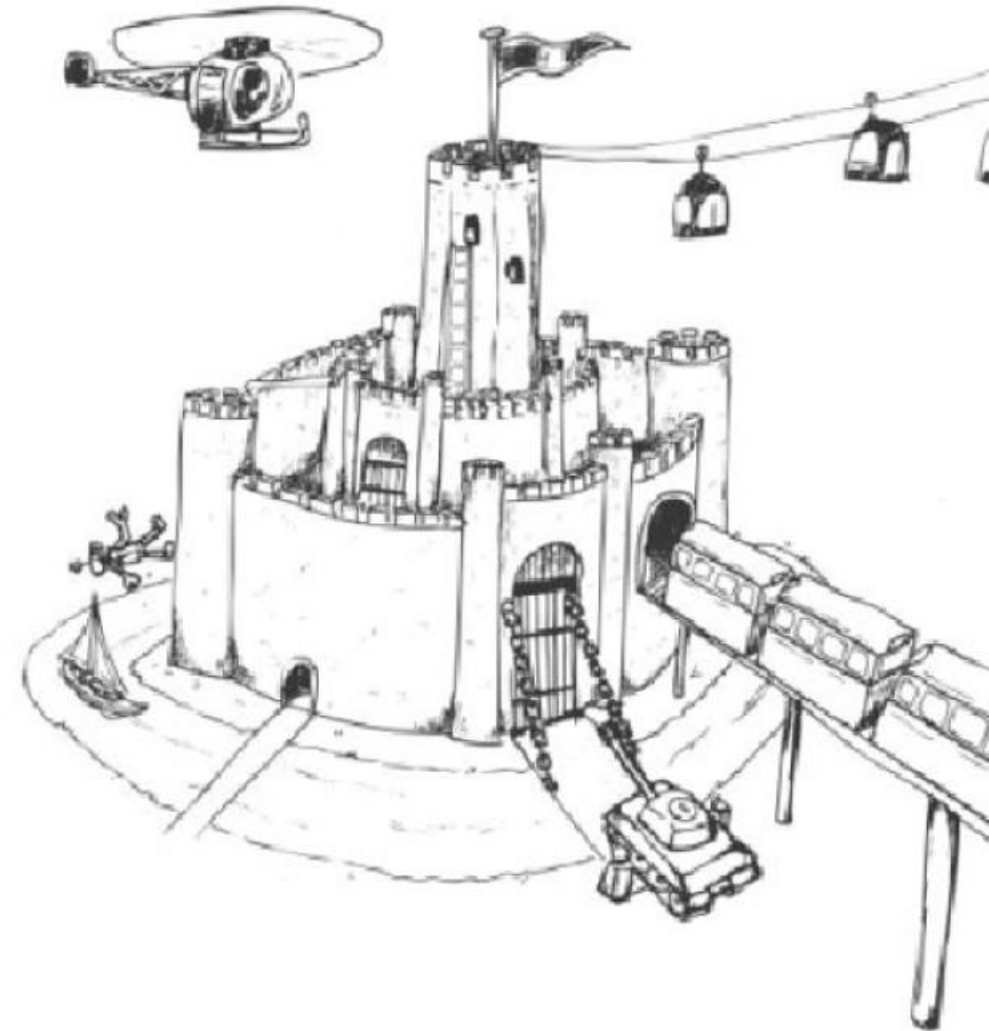
Alanata

IBM

Castle Model of Security



Castle Model in Reality





# 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 23, 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**

- Kawing Hacker Group Exploits More Flaws to Expand Botnet for Cryptjacking
- 4 Mistakes Organizations Make When Deploying Advanced Authentication
- Remoteless Attacks Exploit VMware ESX Vulnerabilities in Alarmign Pattern
- Researchers Warn of Chinese-Aligned Hackers Targeting South China Sea Countries
- Rockwell Advises Disconnecting Internet-Facing ICS Devices Amid Cyber Threats

**Popular Resources**

SECURITY WEEK

Networks & Threats Security Operations Security Architecture Risk Management CISO Strategy ICS/OT Fueling ML

## 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 Issel Argon October 18, 2023



**Trending**

- Rockwell Automation Urges Customers to Disconnect ICS From Internet
- Critical Veem Vulnerability Leads to Authentication Bypass
- VMware Abused in Recent MITRE Hack for Persistence, Evasion
- User Outcry as Slack Scrapes Customer Data for AI Model Training
- Chrome 125 Update Patches High-Severity Vulnerabilities
- 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.

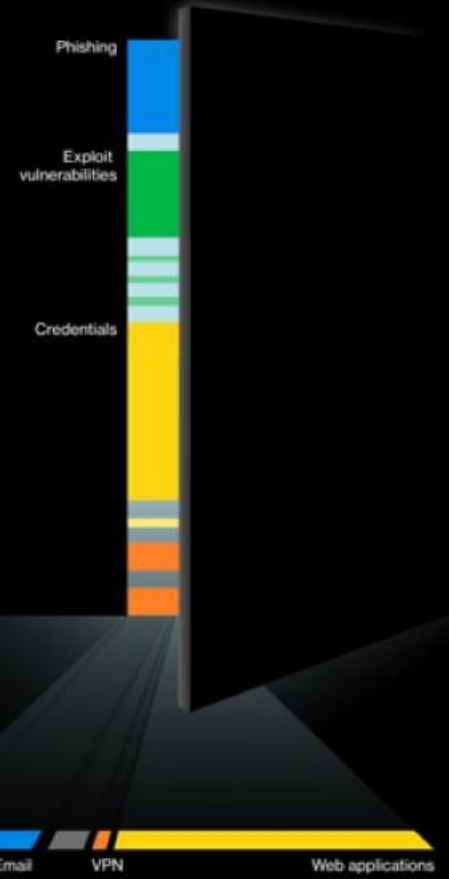
Ako sa brániť proti neznámym hrozbám?

VPN

security gateway

2FA

firewall



# Riešenie je monitoring a rýchla reakcia na hrozby

## Technológie:

SIEM – monitoring kybernetickej bezpečnosti  
SOAR – orchestrácia, automatizácia a odpoveď  
a veľa ďalších nástrojov ...

## Ľudia:

Špecialisti kybernetickej bezpečnosti

## Procesy:

Incident response plány  
Zadefinované procesy  
Kontinuálne zlepšovanie



# In house alebo outsourcing?

- Ak máte interné kapacity a know how, vyplatí sa vybudovať interný SOC tím
- V opačnom prípade je odpoveď:

Hybridný SOC = kontaktná osoba/tím na vašej strane a SOC špecialisti u dodávateľa

# Alanata

Technology Meets Business

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

[www.alanata.sk](http://www.alanata.sk)