

# Řešení zranitelností pomocí ThreatGuard

Bc. Petr Staněk  
architekt kybernetické bezpečnosti

# Kdo jsem?

*CV, životopis*

## **2000-2016**

Armáda ČR, Voják z povolání

## **2016-2017**

Mark2Corporation, bezpečnostní manažer

## **2017-2019**

Státní tiskárna cenin s.p., vedoucí oddělení ochrany informací a ISO

## **2019-2021**

AERO Vodochody Aerospace a.s., manažer kybernetické bezpečnosti

## **2021 – dosud**

Krajský úřad Středočeského kraje, architekt kybernetické bezpečnosti

## **Certifikace, kurzy:**

auditor kybernetické bezpečnosti

Ethical Hacker Foundation



**m2c** | CONNECT  
FUTURE

  
STÁTNÍ TISKÁRNA CENIN,  
státní podnik

**Aero** | VODOCHODY

Středočeský kraj



Středočeský kraj



# Proč zrovna ThreatGuard?

*důvody k implementaci*

- update, aktualizace pracovních stanic zajištěny centrálním nástrojem
- switche, routery a další zařízení aktuálně nemají centrální nástroj pro řešení update atd.
- nedostatek času procházet denně všechny výrobce, zda nemají nový update atd.
- jednoduchost, možnost filtrování dle výrobců atd.

A diagram for ThreatGuard Cyber Threat Intelligence. At the top, the ThreatGuard logo is followed by 'CYBER THREAT INTELLIGENCE' in white, bold, sans-serif font. Below this is a circular radar chart with a red glow and a central red shield icon. The chart is divided into four quadrants, each with text describing a benefit. The text is in white and red. The quadrants are: top-left (Přehledná a aktuální databáze IT hrozeb včetně návrhů a nápravných opatření), top-right (Návrhy a opatření před nejnovějšími IT hrozbami), bottom-left (Podpora zkušených IT expertů), and bottom-right (Relevantní informace k Vaší IT infrastruktuře díky aktivním filtrům).

**ThreatGuard**  
**CYBER THREAT**  
**INTELLIGENCE**

Přehledná a aktuální  
databáze IT hrozeb  
včetně návrhů a  
nápravných opatření

Podpora zkušených  
IT expertů

Návrhy a opatření  
před nejnovějšími IT  
hrozbami

Relevantní informace  
k Vaší IT infrastruktuře  
díky aktivním filtrům

# A jak to vypadá v reálu?

dashboard

- na úvodní straně okamžitý přehled zranitelností dle mého filtru
- možnost otestování podezřelých domén a souborů v nezávislém Sandboxu



The screenshot shows the ThreatGuard dashboard for user Petr Staněk. It features a grid of six vulnerability cards:

- Eskalace práv pomocí Dell aplikací**: Vendor: Dell, Štítky: Závažnost: vysoká, Typy: zranitelnost, Aktualizováno 14.4.2022
- Code injection v produktech Microsoft Office**: Vendor: Microsoft, Štítky: Závažnost: vysoká, Typy: zranitelnost, Aktualizováno 14.4.2021
- Eskalace práv ve Windows Error Reporting**: Vendor: Microsoft, Štítky: Windows Server, Windows Desktop, Závažnost: střední, Typy: zranitelnost, Aktualizováno 16.10.2020
- Spuštění závadného kódu skrze Python Extension v Microsoft Visual Studio Code**: Vendor: Microsoft, Štítky: Windows aplikace, Závažnost: střední, Typy: zranitelnost, Aktualizováno 20.3.2020
- Vzdálené spuštění kódu v Microsoft Excel**: Vendor: Microsoft, Štítky: Windows Server, Windows Desktop, Závažnost: vysoká, Typy: zranitelnost, Aktualizováno 2.3.2020
- Zranitelnost ve Windows Installer umožňující zvýšení oprávnění uživatele**: Vendor: Microsoft, Štítky: Windows 10, Windows Server, Windows 7, Windows Desktop, Závažnost: střední, Typy: zranitelnost, Aktualizováno 17.2.2020

The screenshot shows the Trellix Intelligent Sandbox interface. It includes a header with the Trellix logo and a main section for uploading files for analysis. The interface is in Czech and includes the following text:

Otestujte si podezřelé soubory nebo webové stránky pomocí dynamické analýzy v Trellix Intelligent Sandbox. Vyberte soubor z vašeho počítače nebo zadejte URL odkazující na soubor nebo stránku k otestování. Testování nahraného souboru nebo URL může trvat i několik minut.

Podporované typy souborů

**Výsledné skóre**

- probíhá analýza
- nepodařilo se
- čistý
- neověřeno
- informační
- nízké
- střední
- velké
- velmi vysoké

Při nahrání souboru prostřednictvím ThreatGuard souhlasí uživatel s testováním a uložení souboru v datacentru společnosti COMGUARD a.s. V případě zájmu o detailnější analýzu vzorku, kontaktujte Vašeho obchodního garanta za společnost COMGUARD a.s.

Metoda odeslání

- Soubor (Přímý upload souboru)
- URL souboru (Odkaz na stažení souboru k analýze)
- URL (Dynamická analýza webové stránky)

Soubor (Přímý upload souboru)  není vybrán žádný soubor



# A jak to vypadá v reálu?

## detail zranitelnosti



ThreatGuard

Přehled hrozeb CVE Můj ThreatGuard Novinky Analýza Žádost o funkcionalitu Petr Staněk CS

Vyzkoušejte vyšší level Aktivovat přístup do ThreatManageru

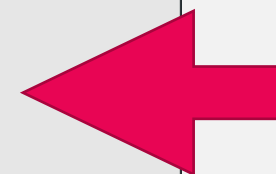
< Zpět Export do PDF

### Zranitelnosti v produktech Microsoftu z 12. 9. 2023

Základní údaje			
ID	2800	Přidáno	13.9.2023 13:15
Úplnost reportu	plný	Aktualizováno	13.9.2023 14:10
Typy	získání citlivých informací, vzdálené spuštění kódu, navýšení oprávnění, spuštění kódu	Geolokace	global
Závažnost	informativní, vysoká	Autor	COMGUARD a.s.
CVSS závažnost	8.8		
CVSS	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
CVE	CVE-2023-36804 CVE-2023-36756 CVE-2023-27909 CVE-2023-36744 CVE-2023-36777 CVE-2023-36770 CVE-2023-36773 CVE-2023-36771 CVE-2023-36772 CVE-2023-38144 CVE-2023-38155		
Zdroje	<a href="https://www.zerodayinitiative.com/blog/2023/9/12/the-september-2023-security-update-review">https://www.zerodayinitiative.com/blog/2023/9/12/the-september-2023-security-update-review</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-23-1421/">https://www.zerodayinitiative.com/advisories/ZDI-23-1421/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-23-1419/">https://www.zerodayinitiative.com/advisories/ZDI-23-1419/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-23-1409/">https://www.zerodayinitiative.com/advisories/ZDI-23-1409/</a>		

Krátký popis
Několik zranitelností bylo objeveno v Microsoft produktech Word, Exchange, 3D Builder, Windows a Azure, jež umožňují útočnickovi provádět na napadených instalacích škodlivou činnost.

Detailní popis
Jedná se o následující zranitelnosti:
<b>CVE-2023-36804</b> Uvedená zranitelnost existuje v ovladači win32kfull z důvodu nedostatečné validace existence objektu, před jeho zpracováním, čehož může útočník zneužít k navýšení svých oprávnění a spuštění libovolného kódu v kontextu uživatele SYSTEM.
<b>CVE-2023-36756</b> Tato zranitelnost se projevuje v nedostatečné ochraně proti deserializaci třídy ApprovedApplicationCollection, kvůli nesprávné validaci uživatelem zadaných dat, což má za následek deserializaci nedůvěryhodných dat, což může útočník zneužít ke spuštění kódu v kontextu uživatele SYSTEM.
<b>CVE-2023-27909</b> Daná zranitelnost existuje v parsingu FBX souborů kvůli nedostatečné validaci uživatelem zadaných dat, což má za následek vyvolání zápisu za konec alokovaného bufferu, čehož může útočník zneužít ke spuštění kódu v kontextu probíhajícího procesu.



Export do PDF, který je přiložen k ticketu pro IT

# Shrnutí

*Proč zrovna ThreatGuard?*

- snadné nasazení
- přehledné výstupy, PDF dokument s informací pro IT
- možnost nezávislého Sandbox Trellix
- možnost filtrování dle výrobců, atd. používaných ve společnosti
- úspora času





Děkuji za Váš čas