COMGUARD

ThreatGuard

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

Proč zrovna ThreatGuard?

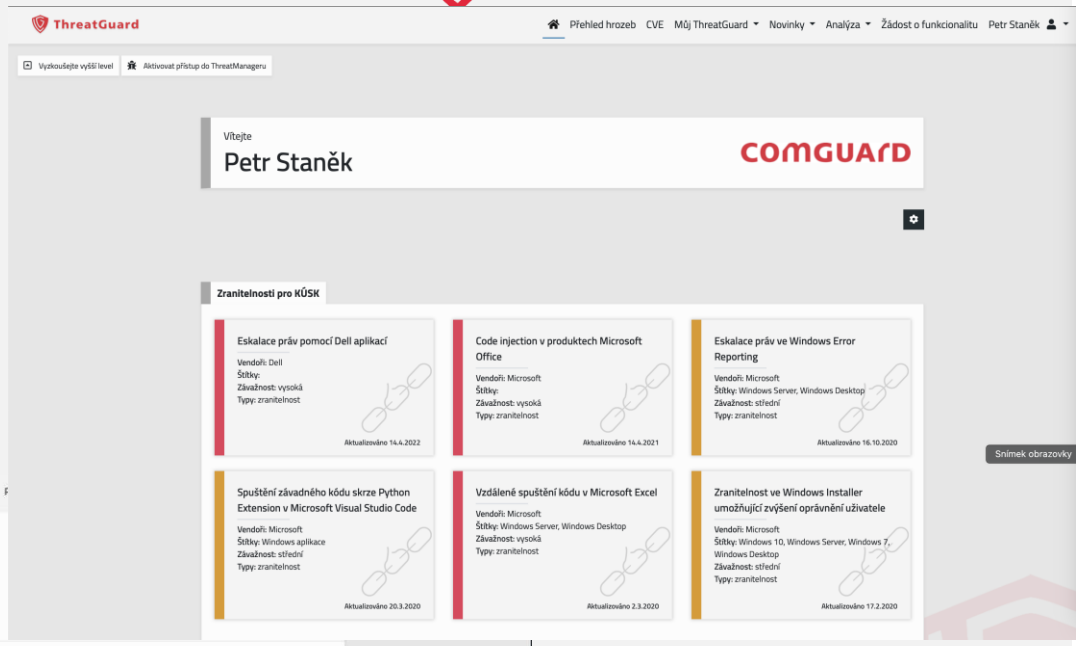
důvody k implementaci

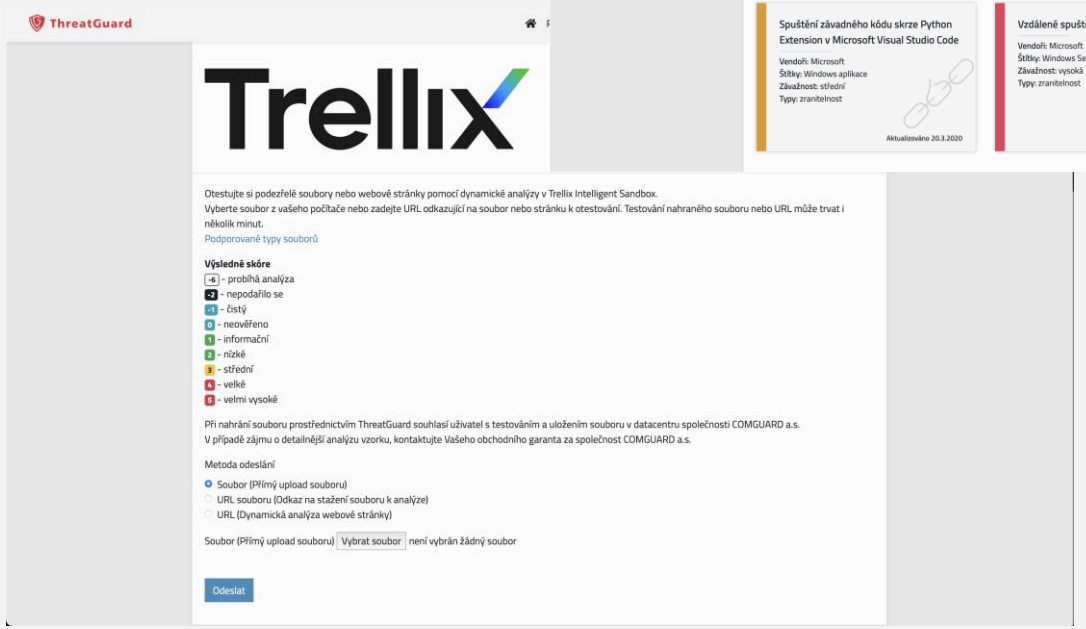
- update, aktualizace pracovních stanic zajištěny centrálním nástrojem
- switche, routery a další zařízení aktuálně nemají centrální nástroj pro řešení update atd.
- nedostatek času procházet denně všechny výrobce, zda nemají nový update atd.
- jednoduchost, možnost filtrování dle výrobců atd.

A jak to vypadá v reálu?

dashboard

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

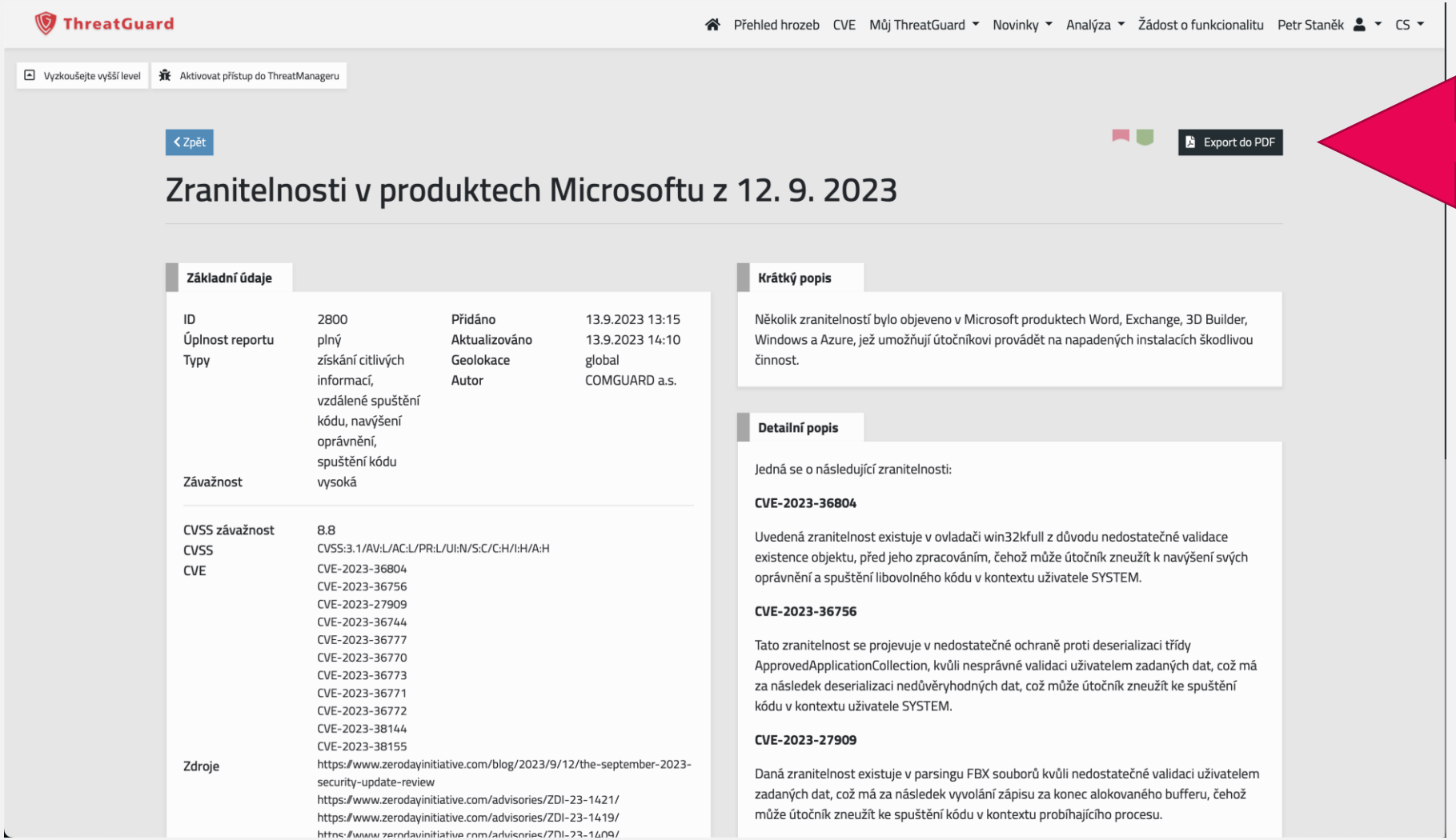




A jak to vypadá v reálu?

detail zranitelnosti

COMGUARD ThreatGuard



Export do PDF, který je přiložen k tiketu 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