Battle card

DOTAZY (Q&A)

Otázka: Co je to vlastně ThreatGuard? V čem je lepší?

*Odpověď: **ThreatGuard = Bezpečnostní hrozby = Služba = Webový portál!***

Nabízíme Vám buď pomoc pro stávajícího IT security managera, nebo tak získáte částečně virtuálního! Jakou pomoc?

- *Za měsíční poplatek získáte tým **9 stálých zaměstnanců** - bezpečnostních specialistů, kteří průběžně aktualizují hrozby na webovém portálu.*
- *Máte přehled o **kritických a nebezpečných zranitelnostech a hrozbách** pro Vaše technologie.*
- ***Obdržíte rady a doporučení,** jak se správně bránit a jaká máte učinit bezpečnostní opatření.*

ŽE VÁM TO UŽ NĚKDO NABÍDNUL? A umí toto?

- *Poskytujeme konsolidované informace z až **55 nezávislých informačních zdrojů**.*
- *ThreatGuard je postaven tak, aby uživatel viděl po přihlášení **pouze svoje technologie** a případně/volitelně byl na novinky **upozorňován mailem** pouze pokud nějaká v jeho zájmové oblasti nastane!*
- *ThreatGuard na rozdíl od podobných služeb např. od vendorů má **přesně stanovený proces**, jak se informace přidávají a posuzuje se průběžně i kvalita a rychlost = zdroje se přidávají i vyřazují, a to i od renomovaných bezpečnostních firem, protože jejich informace jsou bohužel často týdny až měsíce zastaralé.*

Otázka: Na co potřebuji ThreatGuard, když mám Skener zranitelnosti?

Odpověď: Jsou to dva jiné světy!

"SKENER ZRANITELNOSTÍ" primárně testuje Vaši vnitřní síť a kontroluje, zda byly aplikovány patche na známé zranitelnosti a zda jsou všechny OS a firmware aktuální.

"ThreatGuard" hlídá BEZPEČNOSTNÍ HROZBY:

- *Tedy zranitelnosti jsou podmnožinou jeho zaměření.*
- *O hrozbě skener zranitelnosti ani nemůže vědět a nemůže ani v mnoha případech pomoci! - Reakce na hrozbu není „jen" patchování, ale soubor komplexních opatření od personálních např. neotevírat mail, až po nastavení konkrétních zařízení = to Vám skener nikdy nezajistí!*

"ThreatGuard" je ZDROJ INFORMACÍ o:

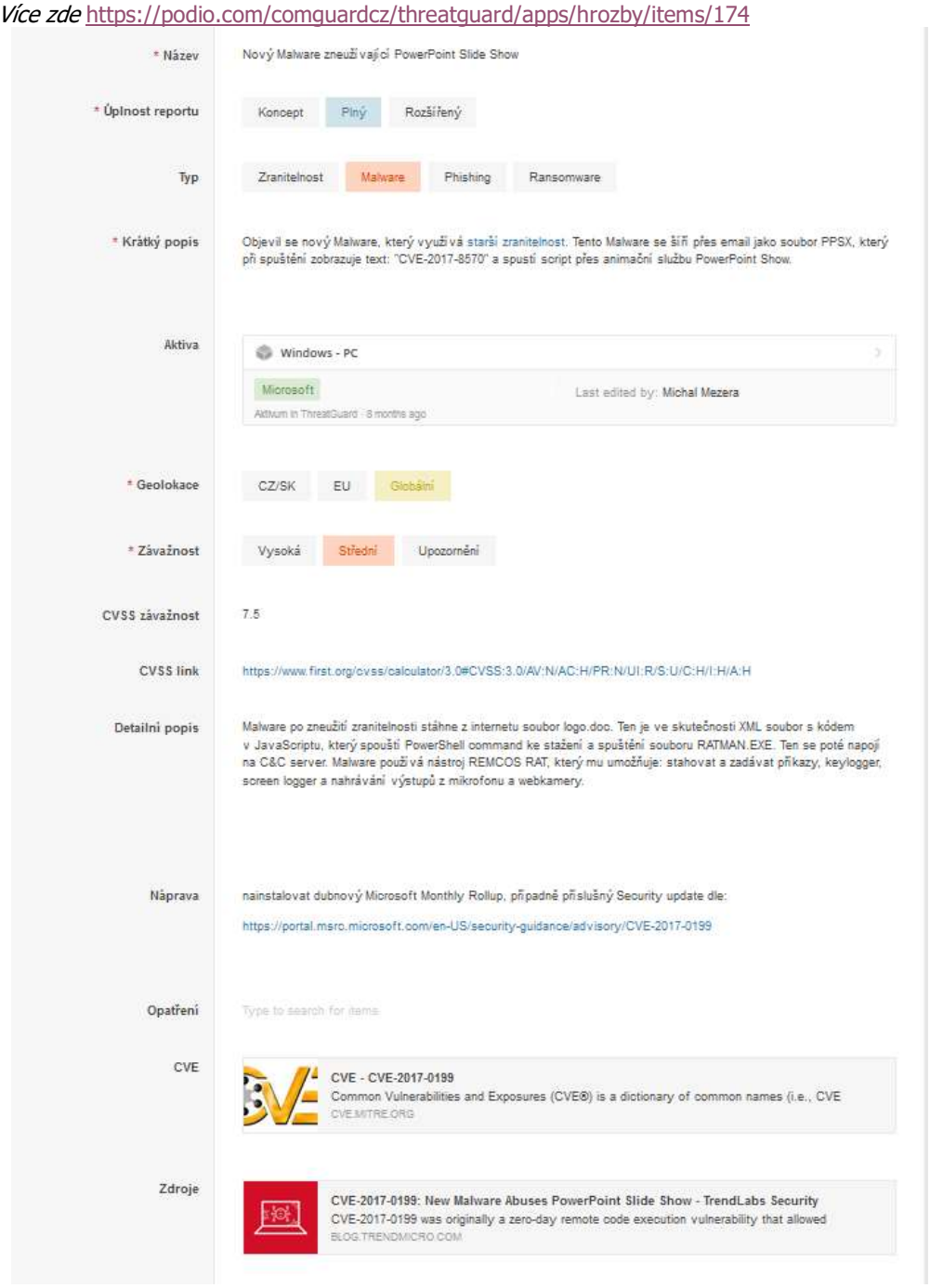
- *Všech hrozbách v ICT, mimo zranitelností systémů také malware, phishing, ransomware, HW i SW vč. různých rozšíření, neopomínaje např. rozšíření webových prohlížečů, atd.*
- *Opatřeních pro reálně uplatnitelné hrozby v ICT, opatření nejen typu instalace patche, ale i úprava konfigurace či designu systému anebo celé sítě.*
- *Proto tuto službu nazýváme také "VIRTUÁLNÍ BEZPEČNOSTNÍ MANAŽER".*

Otázka: Mám pocit, že vy pod linkem hrozby popisujete zranitelnosti, které odhalím Skenerem zranitelností, nebo se mýlím?

*Odpověď: Souhlasíme s Vámi, že některé zranitelnosti lze síťovým skenerem odhalit, je jich však zlomek ve srovnání se všemi hrozbami. Pro Vaši představu o informacích zveřejněných na ThreatGuard, připojujeme několik vybraných hrozeb (včetně souvisejících opatření, tyto detaily uvidíte v EVAL verzi ZDARMA na 14 dní), na <u>které síťový skener zranitelností **nedokáže reagovat**</u>:*

- *Nový Malware zneužívající PowerPoint Slide Show*

- *Objevil se nový Malware, který využívá starší zranitelnost. Tento Malware se šíří přes email jako soubor PPSX, který při spuštění zobrazuje text: "CVE-2017-8570" a spustí script přes animační službu PowerPoint Show.*
- *Více zde* https://podio.com/comguardcz/threatguard/apps/hrozby/items/174



- *Zraniteľnosť vo Foxit reader*
  - *Zraniteľnosti vo Foxit pdf reader umožňujú útočníkový spustiť vlastný kód. Výrobca nebude zraniteľnosti opravovať.*
  - *Více zde* https://podio.com/comguardcz/threatguard/apps/hrozby/items/180
- *Remote code execution v Mozille Firefox verzie < 45*
  - *Mozilla Firefox vo verzii staršej ako 45 obsahuje zraniteľnosť, ktorá umožňuje vzdialené spustenie kódu. Zraniteľnosť je známa už od 2/2016. Momentálne je dostupný exploit. Odporúčame používať aktuálnu verziu.*

- *Více zde* https://podio.com/comguardcz/threatguard/apps/hrozby/items/179
- *PostgreSQL zranitelnost v pg_user_mappings*
  - *PostgreSQL má zranitelnost v pg_user_mappings, díky které může vzdálený útočník se základními právy získat hesla z user mappingu bez příslušných oprávnění.*
  - *Více zde* https://podio.com/comguardcz/threatguard/apps/hrozby/items/177

Otázka: Lze službu ThreatGuard PORTAL používat i v ANGLICKÉM jazyce?

Odpověď: ANO, portál je na tuto alternativu připraven (může být multijazyčný). Cena za anglickou mutaci (příplatek) je zatím předmětem individuálního jednání a podle zájmu klientů může být v budoucnu zahrnuta do ceníku. Odhadujeme fixní příplatek, pouze ke službě ThreatGuard PORTAL, ve výši 1.000 Kč/měsíc za AJ.

Otázka: Je možné službu ThreatGuard provázat na řešení SIEM nebo McAfee ePO?

Odpověď: Služba ThreatGuard PORTAL nabízí opatření proti vybraným hrozbám formou exportu politik pro ePO v ceně služby. Forma předpřipravených konfiguračních exportů pro nastavení doporučených úprav v ePO je velmi efektivní způsob, jak aplikovat doporučení a zkušenosti analytiků ThreatGuard ve vlastní síti.
Napojení do SIEM řešení ThreatGuard aktuálně nenabízí. Kontaktujte obchodního zástupce a s popisem vašich požadavků na integraci, služba je stále vyvíjena a zlepšována.

Otázka: Jaká jsou kritéria pro výběr sledovaných hrozeb?

Odpověď: Kritéria jsou interně v týmu analytiků stanovena následovně:

- *Musí se jednat o hrozbu, která je v danou chvíli reálná a ne pouze teoretická*
  - *Existence zranitelnosti, pro kterou není známá forma aplikovatelného zneužití, nepovažujeme za podstatnou a zranitelnost do ThreatGuard nezařadíme.*
  - *Zveřejnění exploitu nebo zdokumentované pokusy o zneužití určité zranitelnosti je pro nás signál, že je nutné hrozbu do TG zařadit.*
- *Hrozba se musí týkat našeho regionu*
  - *Jakákoliv globální hrozba nebo lokální malwarová/phishingová kampaň je relevantní.*
  - *Phishingová/malwarová kampaň mířící velmi specificky na region mimo CZ/SK je pro ThreatGuard irelevantní*
- *Hrozba se musí týkat aktiv, která jsou relevantní pro firemní použití*
  - *Nezabýváme se např. zranitelnostmi domácích routerů, soukromých blogovacích platforem, herních systémů, apod.*
  - *Velmi vážně bereme hrozby týkající se aplikačních serverů, Active Directory, Linuxových serverů, aktivních prvků apod.*

Ze všech zpracovávaných zdrojů projde našimi filtry cca 10% všech možných zpráv, upozornění, novinek, apod., takže odfiltrujeme zbytečný šum irelevantní pro ochranu infrastruktury.

Otázka: Proč např. zranitelnost NetBackup CVE-2017-885[6-9] není v ThreatGuard uvedena?

Odpověď: Důvodem je, že pro zmíněné zranitelnosti neexistuje zatím veřejně dostupný exploit ani zmínka o tom, že by zranitelnost byla zneužívána některými útočníky nebo malwarem.

Otázka: S jakým zpožděním se objeví nová hrozba ve službě ThreatGuard?

Odpověď: Jedná se o best-effort aktivitu. Vyhodnocování probíhá v pracovní dny 8:00-17:00 a proces je nastaven tak, aby informace o existenci hrozby byly zveřejněny co nejrychleji po ověření podmínek uvedených výše. Analytik hrozbu zveřejňuje samostatně, abychom eliminovali zpoždění způsobené zavedením schvalovacího procesu. Hrozby jsou kontrolovány zpětně dalším členem týmu, který případně může navrhnout jejich stažení nebo přepracování.

Otázka: Lze službu ThreatGuard přizpůsobit konkrétním požadavkům, tedy budu sledovat pouze technologie, které mám v infrastruktuře nasazeny?

Odpověď: Filtrace je možná již dnes na základě dostupných aktiv.