GREYCORTEX

NIS2
z pohledu nástroje GCX Mendel

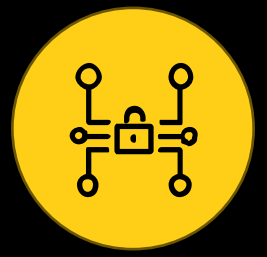
| ITAPA 2023 |

Ondřej Hubálek

Kde můžeme pomoci

Řízení aktiv

- Discovery aktiv a vaze mezi nimi.
- Podklad pro analýzu rizik.



Bezpečnost komunikačních sítí

- Segmentace a dodržování politik.
- Detekce nové nebo zakázané služby.
- Využívání nepovolených aplikací a služeb.

Kryptografické algoritmy

- Neaktuální, slabé, kryptogr. algoritmy.
- Přenos hesel v plain-text formě.

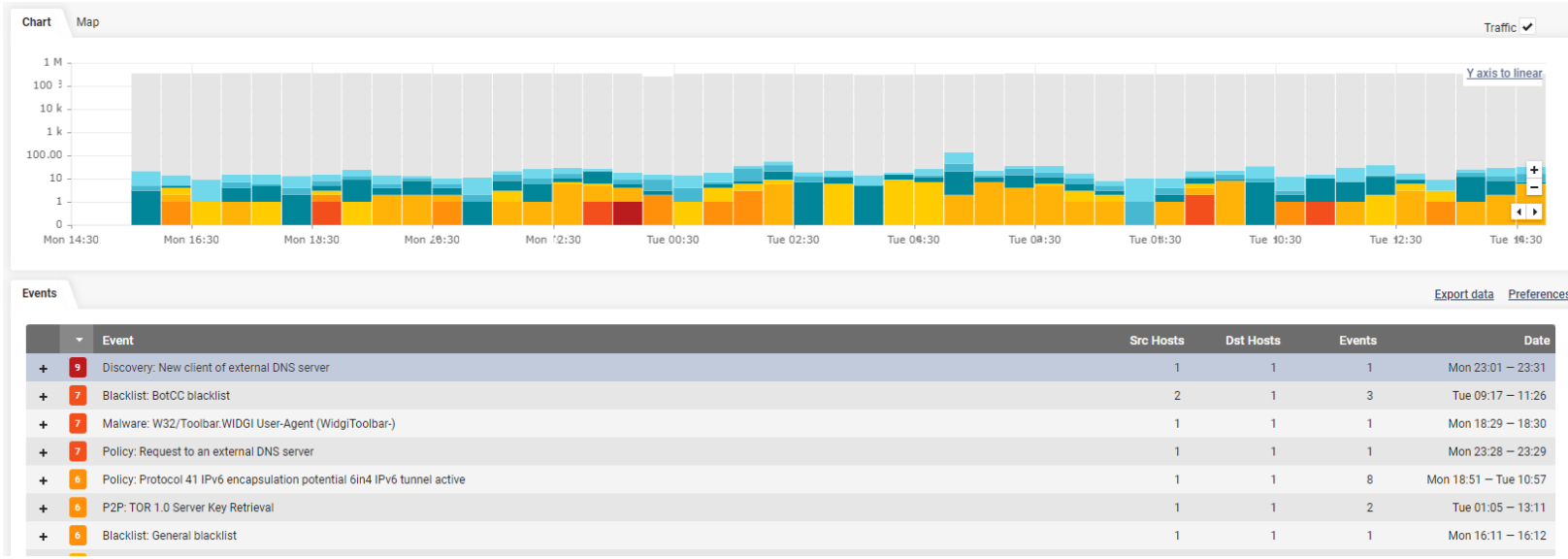
Řízení přístupu

- Komunikace na oprávněné systémy.
- Přístupy externistů.

Detekce kybernetických bezpečnostních událostí

… je tedy požadováno nasazení nástrojů, které jsou schopny detekovat kybernetické bezpečnostní události, které mohou vést ke kybernetickým bezpečnostním incidentům a tyto události buď detekovat, nebo jim současně mohou účinně čelit.

- Kategorizace dle MITRE ATT&CK security framework
- Detekce bezpečnostních událostí na základě síťového provozu.



GREYCORTEX

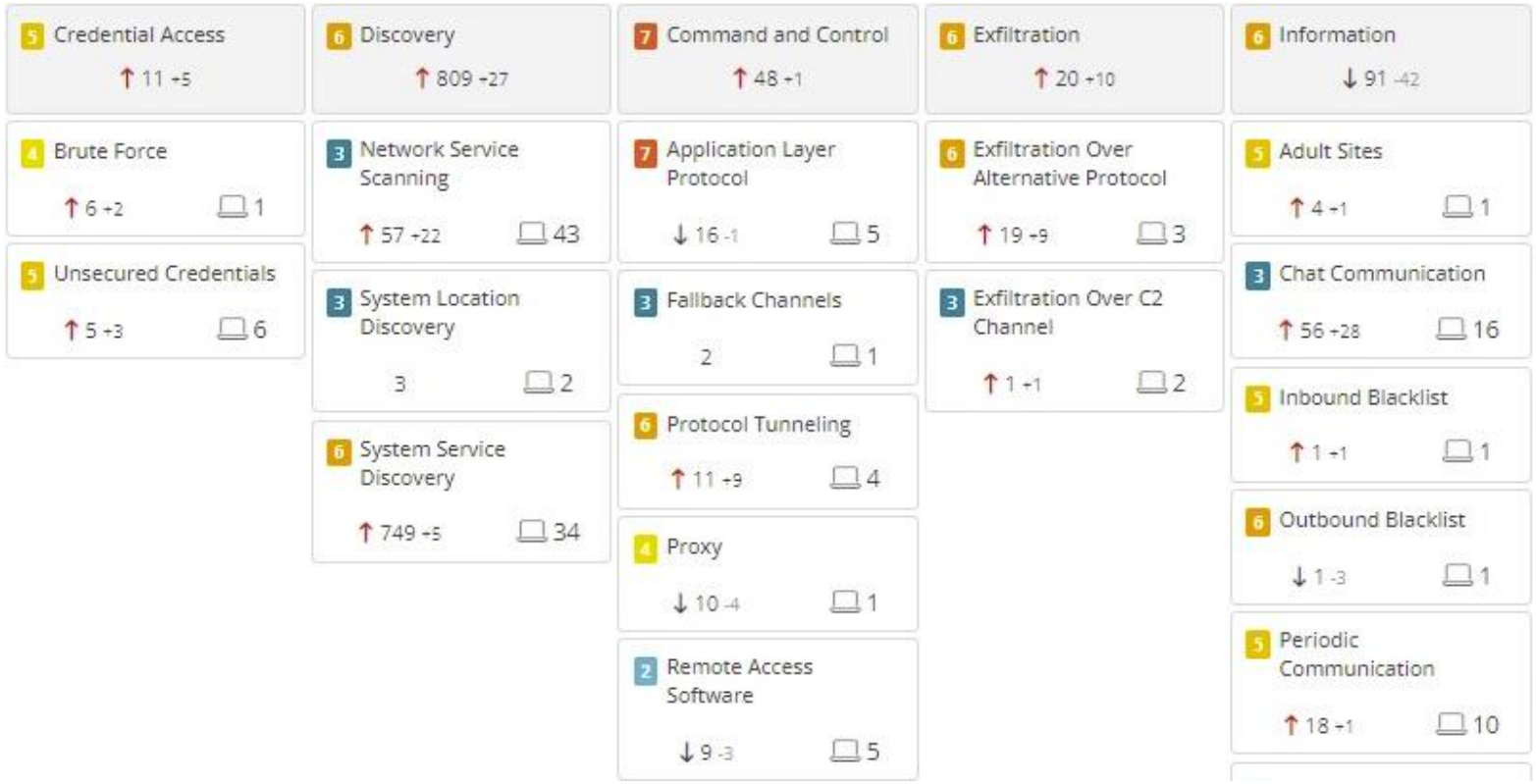
Vyhodnocení kybernetických bezpečnostních událostí

… disponovaly nástroji umožňujícími provádět kontinuální a centralizované vyhodnocování kybernetických bezpečnostních událostí…

Známé hrozby

Projevy nebezp. chování

- C&C odchozí komunikace
- Útoky hrubou silou
- Skeny
- Tunely

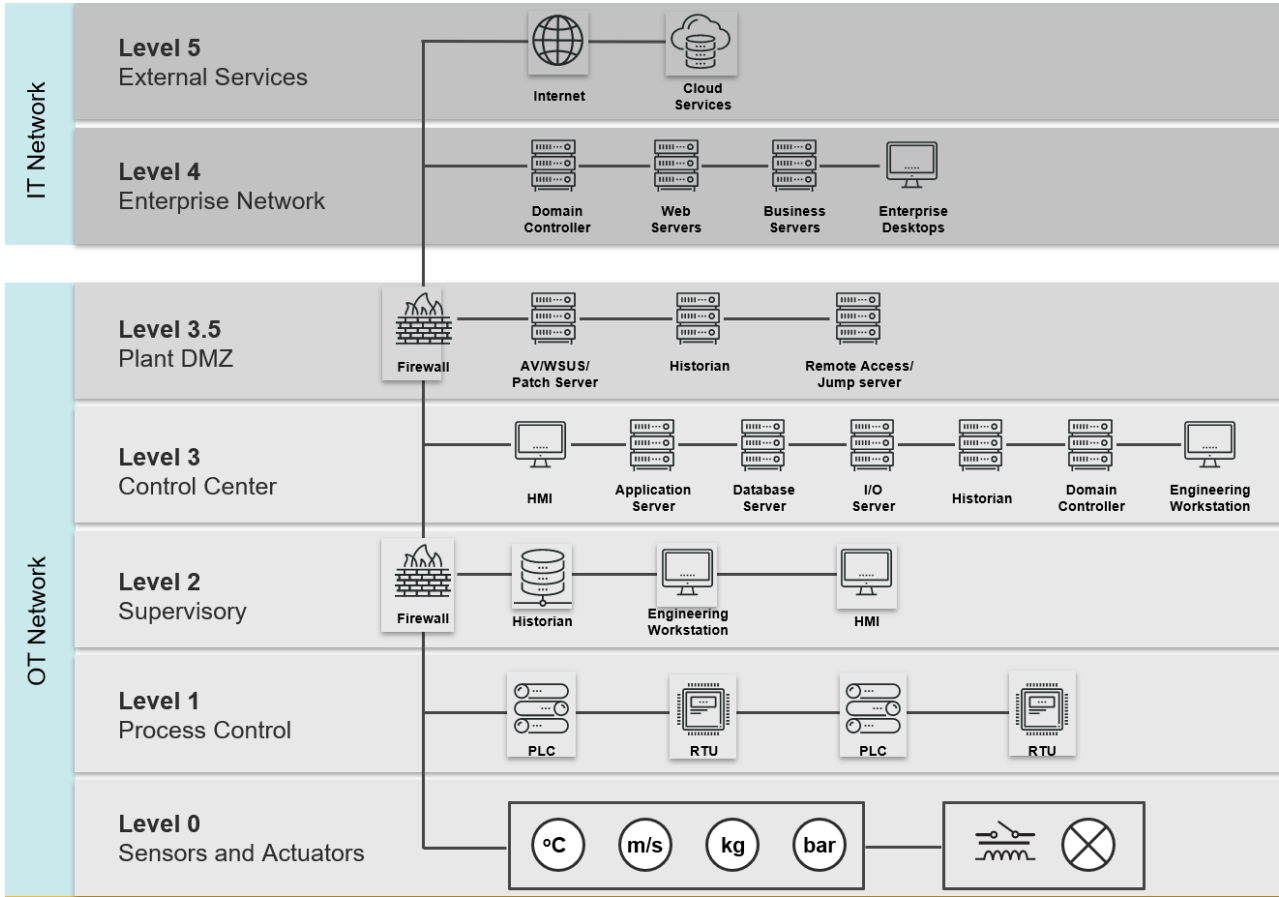


GREYCORTEX

Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

… zajistí ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých hrozeb a zranitelností a

- Viditelnost do provozu průmyslových sítí.
- Podpora průmyslových protokolů mnoha renomovaných výrobců.
- Detekce změny firmware.
- Detekce aktuálních CVE



GREYCORTEX

www.greycortex.com