Systém pro detekci a vyšetřování kybernetických událostí Fidelis Elevate

2.11.2021

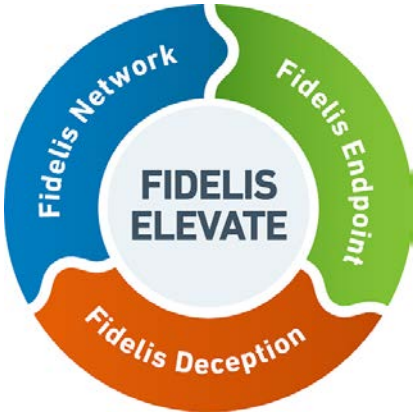
Technologie Fidelis Elevate

Platforma pro automatizovanou detekci, vyšetřování, reakci a hunting

(integrovaná platforma, mnoho forem a způsobů použití)

Fidelis Elevate – ADR – Automated Detection and Response :

- platforma pro **prevenci, detekci a vyšetřování kybernetických incidentů**
- nástroj pro **hlubokou vizibilitu dění na síti i koncových bodech**
- Poskytuje **komplexní pohled, kontext a automatizovanou analýzu**, popř. reakci na kybernetické hrozby a události (incidenty)



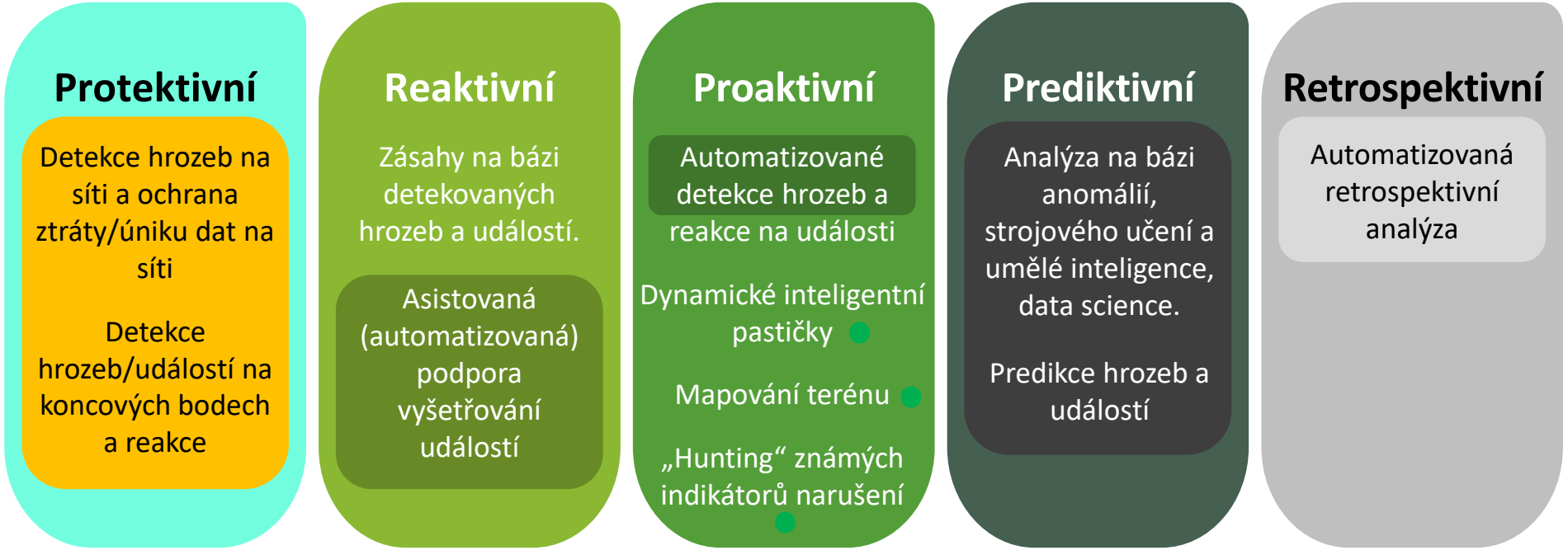
Obsahuje tři základní moduly

- **Fidelis Network** – detekce a prevence na síťovém provozu *(hloubková analýza síťového provozu)*
- **Fidelis Endpoint** – EDR – ochrana koncových bodů *(detekce, reakce, remediace, vyšetřování)*
- **Fidelis Deception** – inteligentní pasti a návnady *(proaktivní „post-breach“ detekce)*

XDR - Extended Detection and Response *(implementováno na MHMP)*

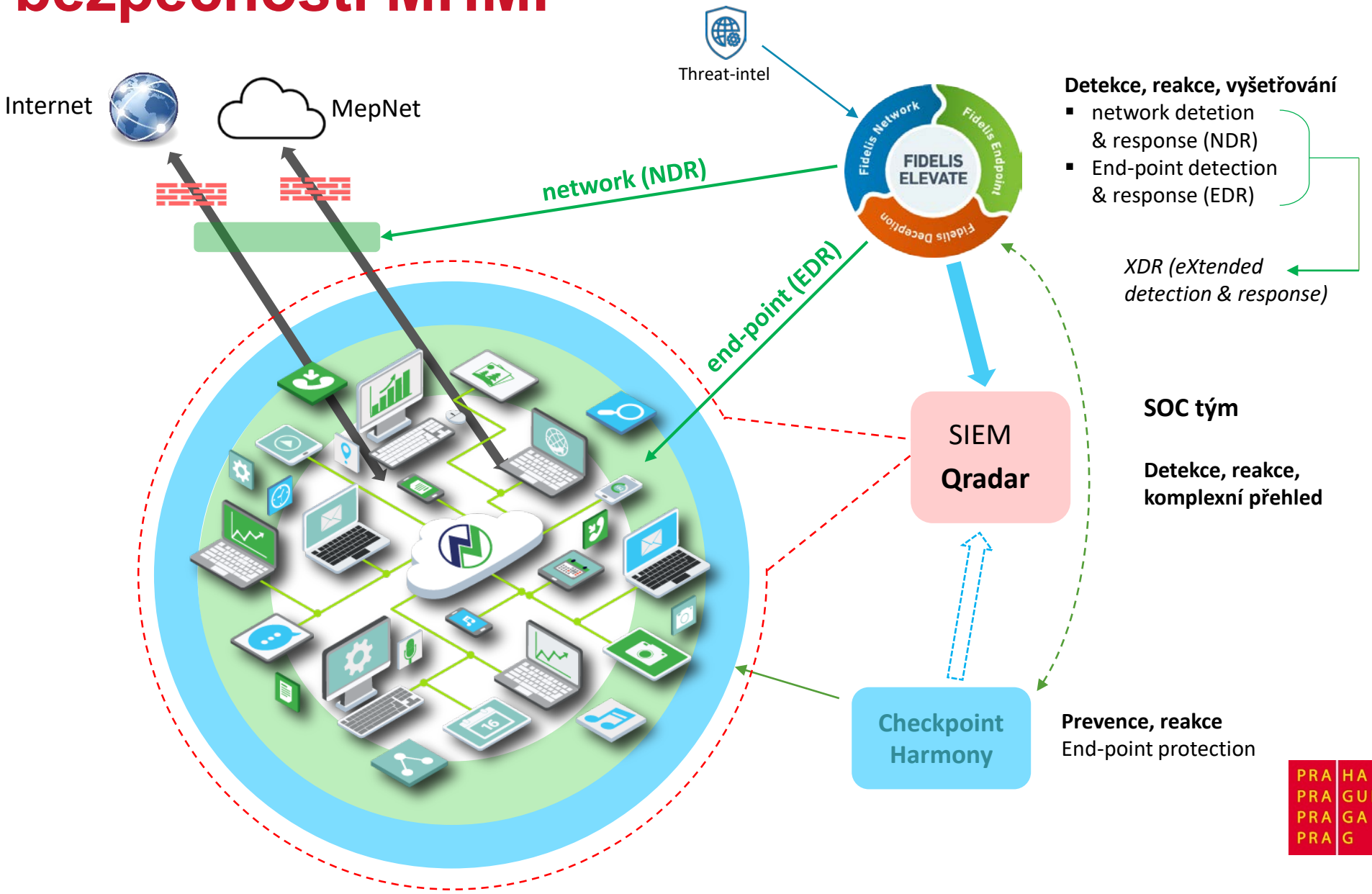
Základní vlastnosti Fidelis Elevate

Schopnosti systému Active XDR implementované v rámci platformy Elevate



Pro provoz systém využívá hardwarové prostředky (servery a sondy) umístěné ve dvojici datových center magistrátu.

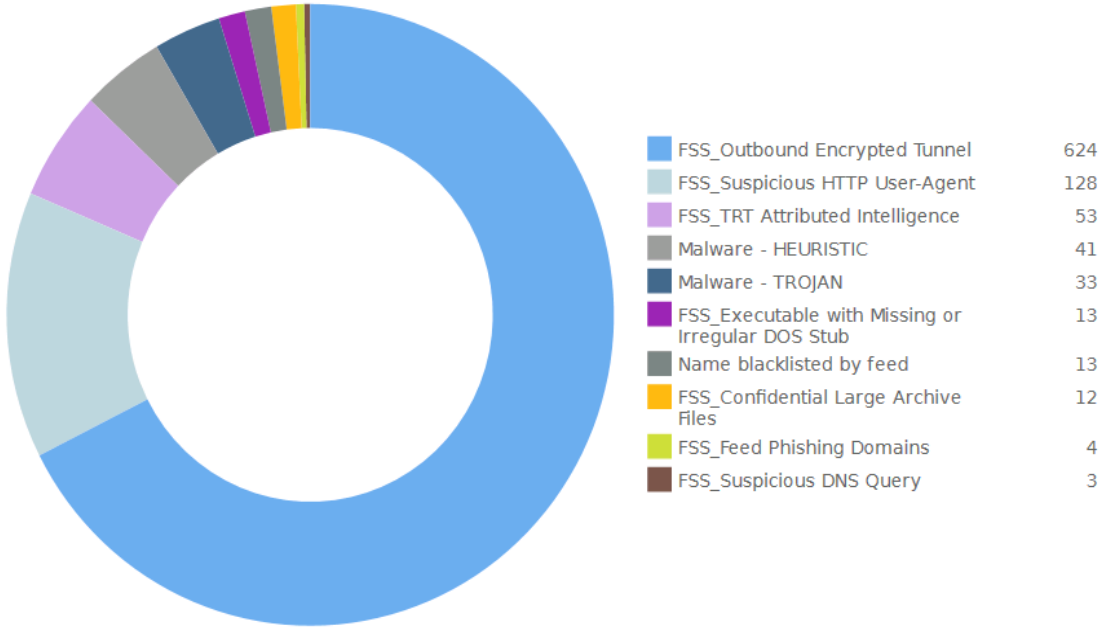
Pozice v architektuře systémů kybernetické bezpečnosti MHMP

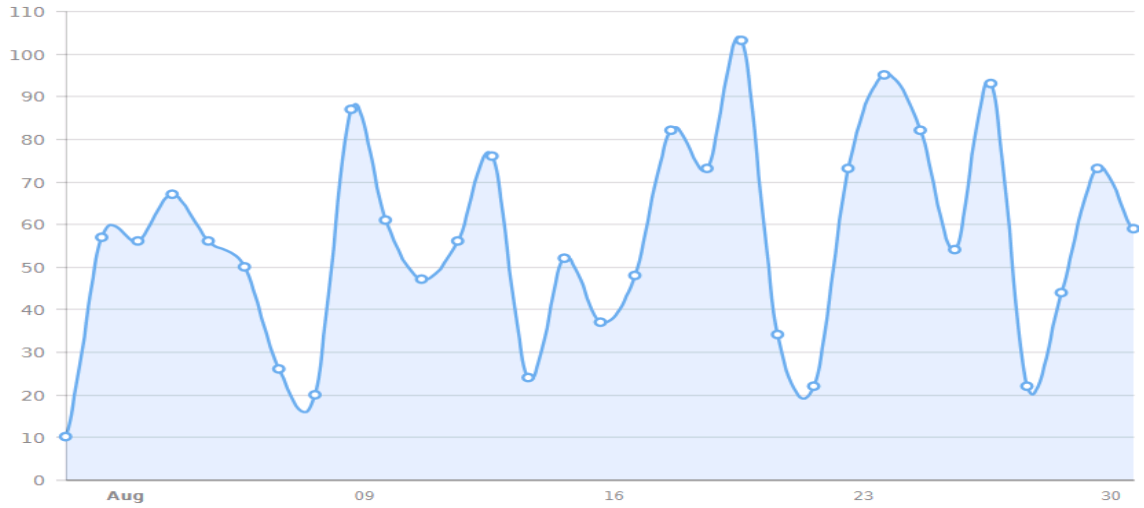


Analýza a statistiky provozu Fidelis Elevate

Analýza síťového provozu na vstupních bodech perimetru:

- průměrný analyzovaný provoz 800 Mbps
- systém je po celou dobu provozu „laděn“ – tj. bezpečnostní události jsou lépe filtrovány a jejich analýza je přesnější
- v srpnu 2021 bylo zaznamenáno a vyšetřeno celkem **1 739** bezpečnostních událostí
- tyto události jsou dále tříděny a vyhodnoceny
- na grafu 1 je uvedeno top 10 detekcí
- graf 2 zobrazuje počty denních detekcí v srpnu 2021

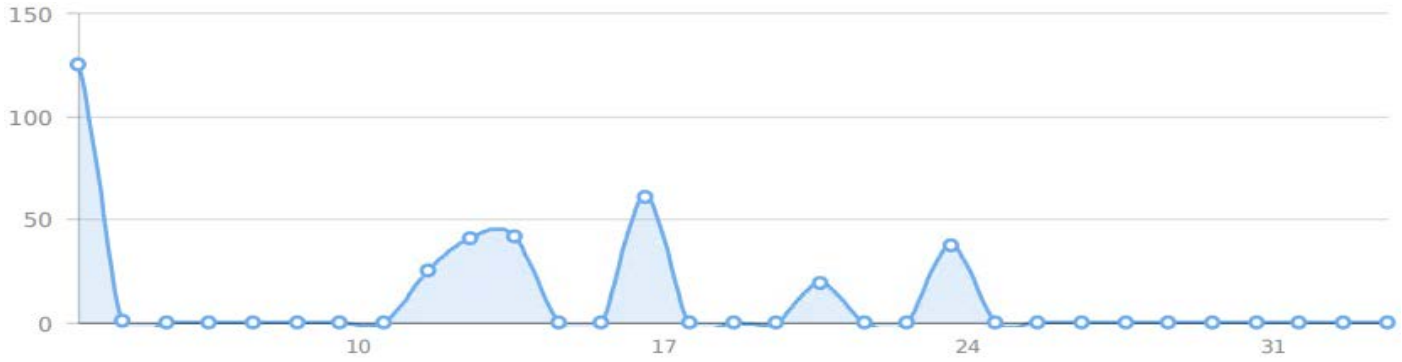




Analýza a statistiky provozu Fidelis Elevate

Analýza provozu koncových bodů:

- Aktuálně je do dohledu napojeno cca 2 800 koncových bodů - stanic a serverů (v rámci probíhajícího projektu je dokončováno kompletním pokrytí koncových bodů)
- Tato část je využita zejména pro došetření a analýzu nežádoucích aktivit na koncových stanicích.
- Postupným dopřesňováním detekčních pravidel jsou analyzovány jednotky až desítky událostí denně – viz grafy níže 351 bezpečnostních událostí / měsíc květen.
- Nejčastější detekce jsou: ransomware, komunikace na podezřelé IP, šifrovaná komunikace přes DNS, torrent, komunikace na CnC, pokus o zajištění persistence nežádoucího SW, vypnutí AV ochrany na koncové stanici, podezřelý soubor v systémovém adresáři, těžba kryptoměn, přenosy velkých archivů, Nobelium.



Analýza a statistiky provozu Fidelis Elevate

Příklad řešeného masivního kybernetického útoku (kampaně) – NOBELIUM

- Jedná se o celosvětový útok prostřednictví tzv. phising techniky
- Hlavní část útoku probíhala počátkem července 2021
- Celkem bylo systémem Elevate v červenci 2021 zaznamenáno a zablokováno celkem **84 140** pokusů o aktivitu v rámci útoku
- Útok byl dořešen a jsou blokovány komunikace s CnC servery využitými k útoku NOBELIUM
- graf ukazuje denní počty řešených událostí kampaně NOBELIUM

Diskuze.

Děkujeme za pozornost.