DATASHEET

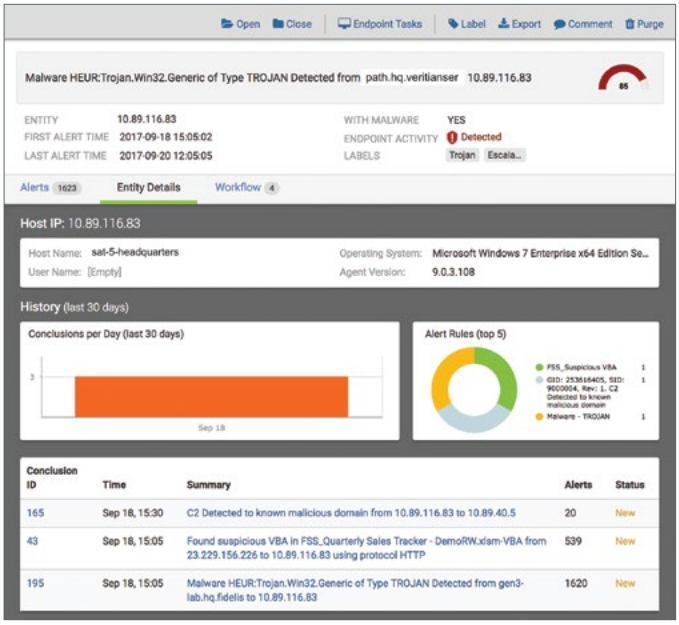
Modul Fidelis Network™

Komplexní automatická detekce a reakce ve vaší síti

Nikdy neponechte žádný závažný útok bez povšimnutí

Moderní útoky se neustále vyvíjejí ve snaze obelstít firewally a proniknout za ochranný perimetr sítě. Bezpečnostní týmy nemají dostatečný přehled a automatizované technologie, aby tyto moderní pokročilé hrozby dokázaly detekovat a včas na ně reagovat. Místo toho používají různé „tzv. propojené" nesourodé systémy, které jim spíš přidávají práci a zvyšují složitost místo toho, aby poskytovaly řešení bezpečnosti.

Práce s těmito izolovanými a nesourodými systémy bezpečnostní týmy přetěžuje, protože musí pracovat v různých prostředích, na různých obrazovkách, na což nemají dostatek času. To vede k zahlcení alarmy, pomalejšímu prošetřování incidentů a opožděné reakci. Útočníci tak mají více času na působení v napadené síti. Vaše data i finance jsou vystaveny zvýšenému riziku, pokud prošetřování, reakce a následně i pobyt útočníka ve vašem systému trvají déle, než je přípustné.



Automatická validace a obohacování alarmů

Vlastnosti produktu

Modul Fidelis Network je zásadní součástí platformy Fidelis Elevate, která byla navržena speciálně pro automatizovanou detekci a reakci, jako odpověď na rostoucí nároky vyplývající z dnešních pokročilých kybernetických hrozeb, jimž čelí bezpečnostní týmy. Pokročilé technologie zajišťují komplexní vizibilitu sítě, validaci alarmů a rychlejší reakce v dnešních složitých infrastrukturách.

Fidelis Network eliminuje fragmentované činnosti prošetřování IT teamů. Řeší problém zahlcení alarmy automatickým vyhodnocováním alarmů a seskupováním souvisejících alarmů. Analytikové reagují s využitím účinných rad a automatizace. Díky prošetření na jedno kliknutí a vestavěné automatizované reakci z jediného a jednotného uživatelského rozhraní, dokáže i méně zkušený analytik reagovat na incident jako zkušený profesionál.

Fidelis Network skládá kompletní historii hrozeb, napadení a průniků. Veškeré informace z alarmu, obsah i souvislosti, popis chování i výsledek exekuce na sandboxu, včetně relevantních informací z koncových bodů, jsou zobrazovány na jedné obrazovce. Kompletní vizibilita znamená, že alarmy jsou viditelné v časových souvislostech a napříč různými pohledy. Vyhodnocení jsou rychlá. Reakce jsou okamžité. Zabezpečení již nezávisí na dalších týmech.

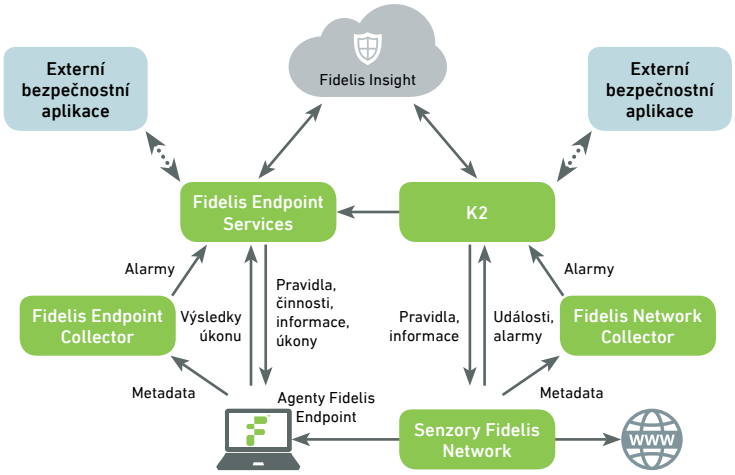
- **Síťová řešení:** Modul Fidelis Network byl od základu navržen s ohledem na zvýšení efektivity a účinnosti. Poskytuje komplexní vizibilitu, detekci a automatickou reakci z jediné praktické zastřešující platformy.
- **Integrace v síti i na koncových bodech:** Automatické validace, korelace a sběr dat týkajících se hrozeb pro vhodnou odezvu. Zajišťuje reakci na napadení za výrazně kratší dobu. Významně zkracuje čas působení útočníka v síti.
- **Automatická detekce, reakce a obohacení informací:** Zjednodušuje posloupnost kroků a šetří čas i úsilí bezpečnostních týmů, takže i méně zkušení analytici mají k dispozici prostředky a informace zkušených profesionálů včetně smysluplného kontextu a pokynů pro nápravu.
- **Automatická validace alarmů:** Poskytněte analytikům přehled o tom, na kterých koncových bodech dochází ke škodlivé činnosti. Odlišením ověřených alarmů od nevalidovaných získají analytici čas a prostředky, které mohou věnovat událostem vyžadujícím pozornost.
- **Vizibilita na všech portech a protokolech:** Neselektivní vizibilita a aplikace bezpečnostních politik znamená lepší detekci a efektivnější využití informací o hrozbách.

Základní funkce síťového modulu

- **Celá síťová spojení, nikoliv jen pakety:** Naše inspekce síťových spojení a paketů je mnohem důkladnější než pouhé prověřování paketů. Sledujeme celý tok příchozí i odchozí komunikace, včetně hluboko vnořeného obsahu. Fidelis seskupuje a analyzuje síťová spojení v paměti, což je zárukou bezkonkurenční vizibility, a rychlosti detekce a vyhodnocení.
- **Dokážeme detekovat to, co jiní ne, protože vidíme, co oni nemohou:** Kromě pokročilého škodlivého kódu (malwaru), exploitů a spojení typu command & control dokáže Fidelis odhalit chování útočníků i během jejich pohybu po vnitřní síti a během jejich přípravy na exfiltraci dat.
- **Zastavte útočníky, zabraňte průniku:** Identifikujte útočníka nebo aktivní vnitřní hrozbu ve vaší síti a zablokujte neautorizované přenosy informací v reálném čase, a to na všech portech a protokolech bez závislosti na proxy serverech jiných dodavatelů.
- **Snadno využívejte informací o hrozbách:** Modul Fidelis Network umožňuje importovat informace o hrozbách založené na síťových spojeních i paketech, a to včetně pravidel Snort, ke zvýšení schopnosti detekce a ochrany proti pokročilým hrozbám.
- **Vizibilita na všech portech a protokolech:** Sledujte síťový provoz na všech portech a protokolech, včetně zneužití protokolů a služeb na nestandardních portech. Kromě toho, uložením síťových metadat všech síťových spojení analyzovaných systémem Fidelis se můžete vrátit v čase a rekonstruovat stopy útočníka.

Pokročilé funkce s integrací modulu Fidelis Endpoint

- **Automatizujte reakce na incident:** Snadno konfigurujte posloupnost kroků reakce automaticky spouštějící nápravná opatření nebo hloubkové analýzy podle definovaných pravidel, která vyvolávají akce nástroje workflow reagujícího na alarmy.



Architektura platformy Fidelis s moduly Network a Endpoint

- **Automatizované obohacování alarmů:** Fidelis automatizuje sběr, korelaci a integraci forenzních dat, přičemž u každého alarmu ukazuje, co se stalo před ním i po něm. Fidelis zkracuje čas na detekci, vyhodnocení a třídění alarmů ze dnů na minuty.
- **Automatizujte nápravu koncových bodů:** Okamžitě zabraňte exfiltraci dat a rozšiřování nákazy v síti prostřednictvím izolace koncových bodů, zastavením procesů, smazáním souborů, spuštěním skriptů nebo použitím uživatelských programů na koncových bodech.
- **Zvyšte účinnost se sdružováním souvisejících událostí – tzv.** Conclusions: Fidelis spouští validaci na každém koncovém bodu v infrastruktuře a generuje alarmy v případě zjištění hrozby. Fidelis automaticky seskupuje související alarmy, které prezentuje v kontextu jako tzv. Conclusions. Conclusions identifikují alarmy, které v průběhu času vznikly na stejném napadeném systému (hostiteli nebo e-mailové adrese).

Výhody

- Omezení krádeží aktiv a IP
- Snížení celkových nákladů na reakci
- Menší a kratší narušení chodu podniku
- Menší ohrožení reputace/ integrity podniku
- Zvýšení efektivity SOC

Obraťte se na nás ještě dnes a získejte další informace o společnosti Fidelis

Fidelis Cybersecurity | +420 222 191 918 | emea@fidelissecurity.com

Fidelis je jediná integrovaná platforma pro automatizovanou detekci a reakci na sítích i koncových bodech. Platforma Elevate™ společnosti Fidelis zvyšuje efektivitu i účinnost práce bezpečnostních týmů soustředěním dat alarmů do akčních souhrnů útoků s následnými automatickými akcemi reakce a prošetřování. Řešení Fidelis jsou vyvíjena s cílem zvýšit vizibilitu a zajistit rychlou reakci. Nabízejí automatizovanou validaci, prošetřování a prevenci útoků. Spoléhají se na ně přední světové společnosti.

