Fidelis Elevate

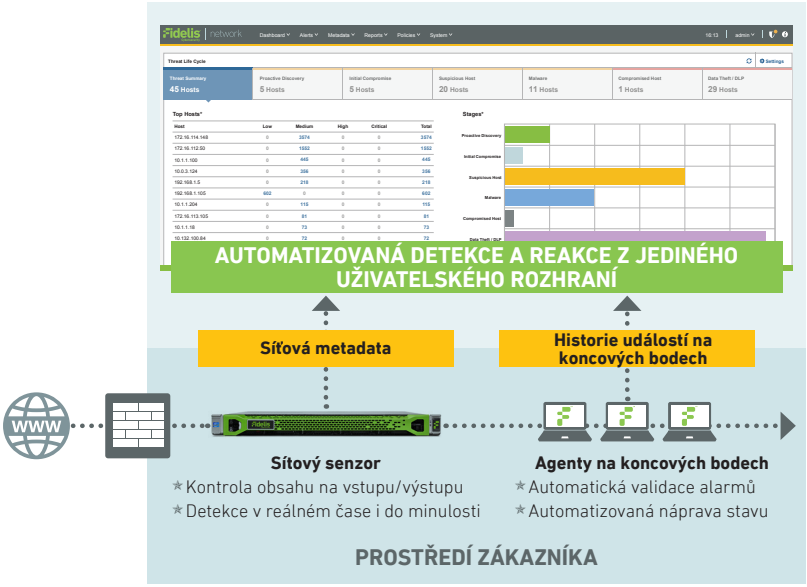
Platforma pro automatizovanou detekci a reakci

Problém

Moderní útoky se neustále vyvíjejí, snaží se překonat firewally a proniknout do vnitřní sítě. Podniky na to reagují zaváděním různých nekoncepčních opravných systémů, které jsou dohromady komplikovanější než problémy, které řeší. Bezpečnostní týmy nemají dostatečnou vizibilitu o dění v síti a na koncových bodech – chybí automatizace zajišťující maximální využití prostředků a schopnost detekce a reakce na dnešní kyberhrozby je nedostatečná. Nám se to vše podařilo změnit.

Řešení Fidelis

Fidelis Elevate je řešení vytvořené za účelem automatizované detekce a reakce na síti i koncových bodech. Bylo vyvinuto tak, aby poskytovalo maximální vizibilitu, podporu vyhodnocování a validaci alarmů a vylepšenou reakci v reálném čase i do minulosti, a tím zvýšilo efektivitu a účinnost bezpečnostních týmů.



- **Integrace.** Řešení Fidelis Elevate bylo navrženo s cílem zajistit dokonalý přehled o celé síti i o všech koncových bodech a provádět kompletní analýzu hrozeb včetně odpovídající reakce.
- **Vizibilita.** Fidelis Elevate nabízí unikátní vizibilitu paketů i síťových spojení v síti i na koncových bodech, v reálném čase i retrospektivně, známých i neznámých hrozeb a schopnost detekce útoků v průběhu všech fází jejich životního cyklu.
- **Automatizace.** Platforma Fidelis využívá automatizačních technologií k výraznému zvýšení efektivity a účinnosti práce bezpečnostních týmů

AUTOMATIZOVANÁ DETEKCE

Navrženo pro pochopení a akci

- **Integrovaná a automatizovaná** statická, dynamická i historická detekce
- **Triangulace místa útoku** pro přesnější analýzu
- **Multifaktorová detekce a determinace** zahrnuje strojové učení | atomické signatury| detekci anomálního chování | analýzu hrozeb přes historická metadata | sandbox

AUTOMATICKÁ REAKCE

Pomáháme bezpečnostním týmům snížit úsilí a čas nutný k reakci na bezpečnostní incident

- Automatizujte vyhledání, validaci a reakci na pokročilé útoky
- Automatizujte workflow reakcí, izolování, vyčištění a analýzy
- Automatizujte jednotlivé kroky Vaší práce s informacemi o hrozbách a zajistěte tak lepší bezpečnost

Pilíř platformy: Fidelis Network 9

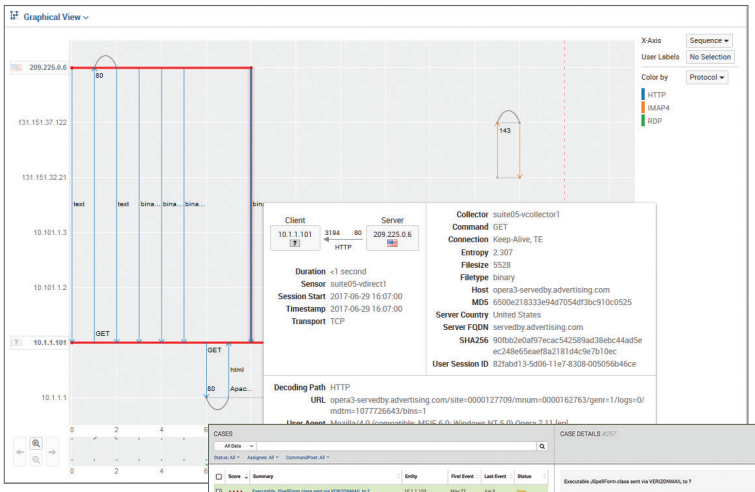
Fidelis Network™ zastavuje moderní útoky, které snadno projdou perimetrem.

Řeší problém zahlcení alarmy (alert fatigue) díky automatizovanému vyhodnocování alarmů a seskupování souvisejících alarmů tak, aby mohl bezpečnostní tým efektivně reagovat na větší množství bezpečnostních hrozeb v kratším čase.

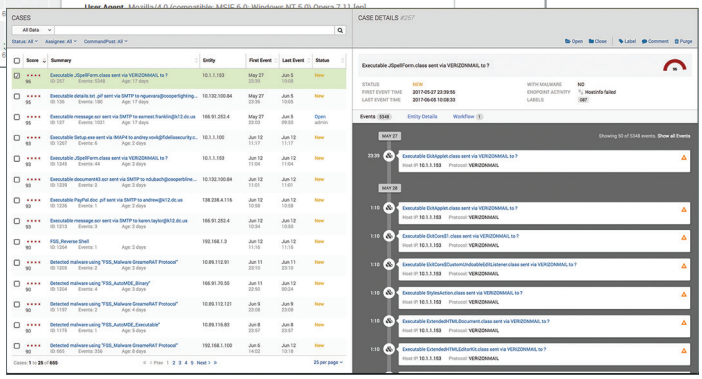
Fidelis eliminuje zdlouhavé prošetřování ve spolupráci s IT týmy díky investigaci na jedno kliknutí a vestavěné automatizované reakci v jednotném uživatelském rozhraní.

Fidelis Network ukládá kompletní historii hrozeb. Veškeré informace o alarmu, obsah i souvislosti, popis chování i výsledek exekuce v sandboxu včetně relevantních informací z koncových bodů jsou doručovány na jednu obrazovku.

Dokonalá vizibilita umožňuje rychlé rozhodování. Reakce jsou okamžité.



Fidelis sestavuje vícefaktorová data útoku do jediného sjednoceného, kompletního zobrazení.



Fidelis seskupuje veškeré související alarmy do skupin, které zobrazuje na centrálního panelu alarmů, takže analytici mohou snadno a rychle reagovat.

Schopnosti

Dokážeme detekovat to, co jiní ne, protože vidíme, co oni nemohou
Kromě pokročilého škodlivého kódu (malwaru), exploitů a převzetí kontroly (command & control spojení) dokáže Fidelis odhalit chování útočníků i během jejich pohybu po síti (lateral movement) a během jejich přípravy dat k exfiltraci.

Automatizované obohacování alarmů
Fidelis automatizuje sběr, korelaci a integraci forenzních dat, přičemž každý alarm ukazuje i to, co se stalo před ním a po něm. Fidelis zkracuje čas na detekci, vyhodnocení a třídění alarmů ze dnů na minuty.

Celá síťová spojení, nikoliv jen pakety
Naše inspekce síťových spojení a paketů je mnohem důkladnější než pouhé prověřování paketů. Sledujeme celý tok příchozí a odchozí komunikace včetně hluboko vnořeného obsahu. Fidelis Network jedinečným způsobem sestavuje a analyzuje síťová spojení v paměti, čímž je dosahováno nebývalé vizibility a přesné detekce.

Detekce v minulosti a přítomnosti
Ukládaná metadata z vaší sítě i koncových bodů jsou automaticky analyzována a porovnávána s nově popsanými hrozbami, signaturami a pravidly, takže dokážete odhalovat i minulé útoky a připravit se na budoucnost.

Fidelis Cloud
Spravováno Fidelisem

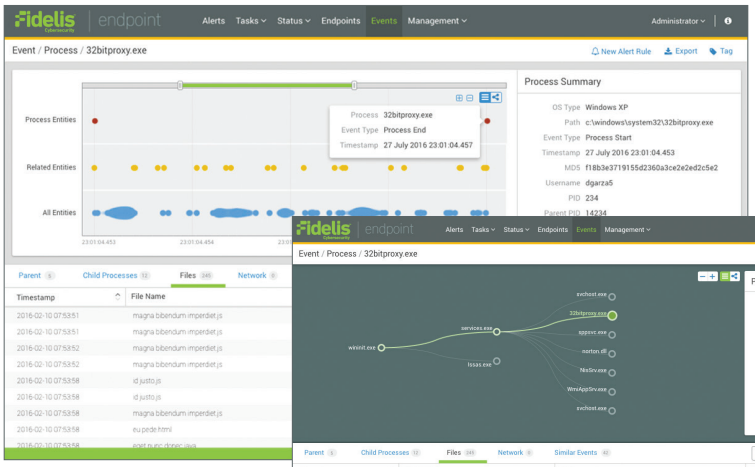
Získejte všechny výhody řešení Fidelis Network a Fidelis Endpoint prostřednictvím cloudu. Prostřednictvím platformy Fidelis Cloud pečuje Fidelis o vaši celou infrastrukturu, takže vy se můžete soustředit na svoji hlavní činnost – ochranu své organizace.

- ★ Infrastrukturu spravuje Fidelis, takže vy se můžete soustředit na užívaní systému a zabezpečení svých výpočetních prostředků.
- ★ Rychlé nasazení a okamžitá implementace
- ★ Škálujete průběžně podle svého růstu s tolika softwarovými senzory, kolik jich potřebujete
- ★ Nepřerušená služba při přechodu ze zkušební verze na ostrou
- ★ Zjednodušený cenový model předplatného na základě vašeho skutečného provozu a potřebné úložné kapacity metadat

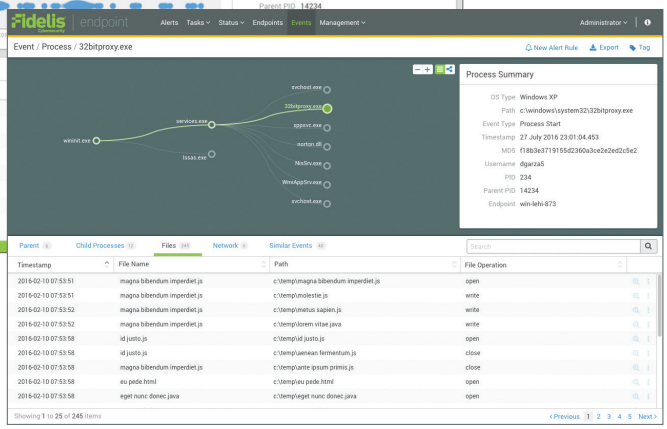
Pilíř platformy: Fidelis Endpoint 9

Fidelis Endpoint™ je naše kombinované řešení pro detekci a reakci na koncových bodech (EDR) i ochranu koncových bodů (EPP) vybavující bezpečnostní organizace schopností spolehlivě odhalovat bezpečnostní incidenty, reagovat na ně i jim předcházet a řešit je za zlomek času oproti tradičním koncepcím. Endpoint 9 byl od počátku vyvíjen tak, aby spolehlivě spolupracoval se síťovou částí Fidelis Network. Automatizuje jednotlivé činnosti reakce na incident, které dříve trvaly dny nebo týdny.

Bezpečnostní analytici jsou schopni provádět úkony, které dříve prováděli SOC analytici a IR týmy.



Interaktivní časová osa útoku umožňuje přesnou identifikaci jeho fází a zařízení, kde je třeba reagovat.



Interaktivní vizualizace stromu procesů a cest útoku.

Schopnosti

Detekce útoků v okamžiku, kdy k nim dojde
Neustále monitoruje a zaznamenává klíčové aktivity na koncových bodech včetně souborových manipulací, spouštění procesů, síťových spojení, práce s registry, otevíraných URL a DNS překladů i připojování USB paměťových médií. Automaticky aplikuje aktuální informace o hrozbách na všechny koncové body a poskytuje téměř okamžitou odezvu.

Zjistěte, co se dělo, díky možnosti zpětného přehrání
Kompletní přehled o tom, jak útok probíhal, čeho se útočník zmocnil, a kdo ještě byl napaden prostřednictvím alarmů s přiřazenou prioritou a automaticky generované časové osy pro každé podezření na incident.

Automatizovaná náprava stavu koncových bodů
Okamžité zastavení exfiltrace dat a další šíření útoku po síti prostřednictvím izolace koncových bodů, ukončení procesů, smazání souborů, spuštění skriptů nebo s použitím uživatelsky naskriptovaných akcí na koncových bodech.

Automatická reakce na incident
Snadno nakonfigurujete posloupnost kroků jako reakci na incident, která se automaticky spustí a provede nápravná opatření, nebo hloubkovou analýzu podle definovaných spouštěcích pravidel a následných činností.

Citace zákazníka

„Díky společnosti Fidelis jsme nyní o **60 %** úspěšnější při odhalování narušení bezpečnosti. Snížili jsme náklady na reakci na incidenty o **17 %** a zotavení po incidentu jsme zrychlili o **50 %**."

~ CISO, společnost finančních služeb

Fidelis Enterprise
Implementace u zákazníka

Řešení Fidelis Enterprise bylo navrženo pro organizace, které preferují implementaci ve své infrastruktuře. Nabízí jim kompletní kontrolu nad aplikacemi a zařízeními Fidelis Endpoint a Fidelis Network.

- ★ Udržujete a spravujete si veškerá zařízení a software
- ★ Profesionální služby Fidelis vám pomohou s implementací a zaškolením
- ★ K dispozici jsou následující síťové senzory: Direct, Internal, Mail a Web
- ★ Poplatky za údržbu zahrnují i aktualizaci analytických nástrojů prováděnou týmem Fidelis Threat Research
- ★ Možnost dokoupení dalších licencí na zařízení dle potřeby

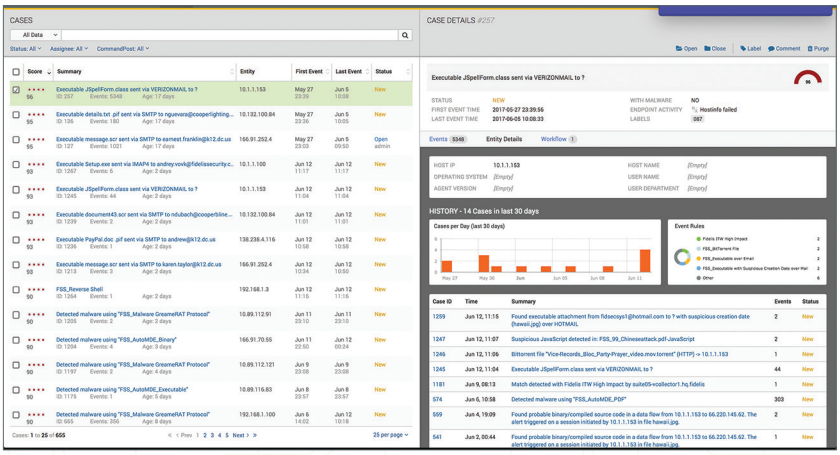
Přechod od alarmů k akci

Fidelis Elevate nabízí bezpečnostním týmům vizibiltu celé jejich sítě i všech koncových bodů. Díky kombinaci této vizibility s automatizovanou prevencí, detekcí a reakcí v počáteční fázi odhalení hrozby má podnik první obrannou linii a bezpečnostní týmy mohou profitovat z mnohem detailnějších bezpečnostních alarmů. Mohou se tak rychleji rozhodovat a rychle dosahovat výsledků.

Klíčovými otázkami zodpovězenými systémem jsou:

- ★ Dosáhl útok svého cíle?
- ★ Byl útok aktivován?
- ★ Co ještě se stalo před útokem a po něm?
- ★ Vyskytla se tato aktivita i v nějakém dalším systému v našem prostředí?

Fidelis Elevate poskytuje odpovědi. Díky validaci na každém koncovému bodu v infrastruktuře Fidelis automaticky generuje alarmy v případě zjištění hrozeb. Několik alarmů může představovat jedinou událost, která indikuje hrozbu. K pochopení celého rozsahu hrozby je nutno sdružit mnoho alarmů. Fidelis automaticky seskupuje související alarmy a prezentuje je v jejich kontextu jako tzv. Conclusions. Tyto Conclusions identifikují související alarmy, které v průběhu času vznikají na stejném napadeném systému (hostiteli nebo e-mailové adrese). Výsledky poskytují kritické informace, které pomáhají analytikům rychleji pochopit celkový rozsah a životní cyklus útoku.



Fidelis automatizuje sběr, korelaci a analytiku složitých útoků v sítích a na koncových bodech v průběhu času.

PŘÍPADOVÁ STUDIE

FINANČNÍ SLUŽBY

Pozadí

- ★ 10 000 zaměstnanců
- ★ Přes 450 miliard spravovaného majetku
- ★ Zkušený tým SOC a reakce na incidenty

Výzva

- ★ V současnosti rozšířený vyděračský software, tzv. ransomware, vytváří potřebu přehodnotit postoj k zabezpečení
- ★ Obava o bezpečnost značky v důsledku vážného bezpečnostního incidentu
- ★ Stávající IPS a anti-malwarová řešení vytvářely hodně „šumu“
- ★ Prošetřování kritických alarmů trvalo v průměru dva dny a déle

Výsledky

- ★ O 60% efektivnější při identifikaci průniků
- ★ Snížení nákladů na odezvu o 17 %
- ★ Zkrácení času na vyřešení incidentu o 50 %
- ★ Nové řešení pro IPS a pokročilou detekci škodlivého kódu

Podívejte se, o co přicházíte. Vyžádejte si demo ještě dnes **www.fidelissecurity.com/demo**

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

Fidelis Cybersecurity | +44 203 021 2500 | emea@fidelissecurity.com

Fidelis je jediná integrovaná platforma pro automatizovanou detekci a reakci na sítích i koncových bodech. Fidelis zvyšuje efektivitu i účinnost práce bezpečnostních týmů seskupením souvisejících alarmů a následnou automatizovanou reakcí a prošetřováním. Řešení Fidelis jsou vyvíjena s cílem zvýšit vizibilitu a zajistit rychlou reakci. Nabízejí automatizované vyhodnocování, prošetřování a prevenci útoků. Spoléhají se na ně přední světové společnosti.

