DATASHEET

Modul Fidelis Endpoint™

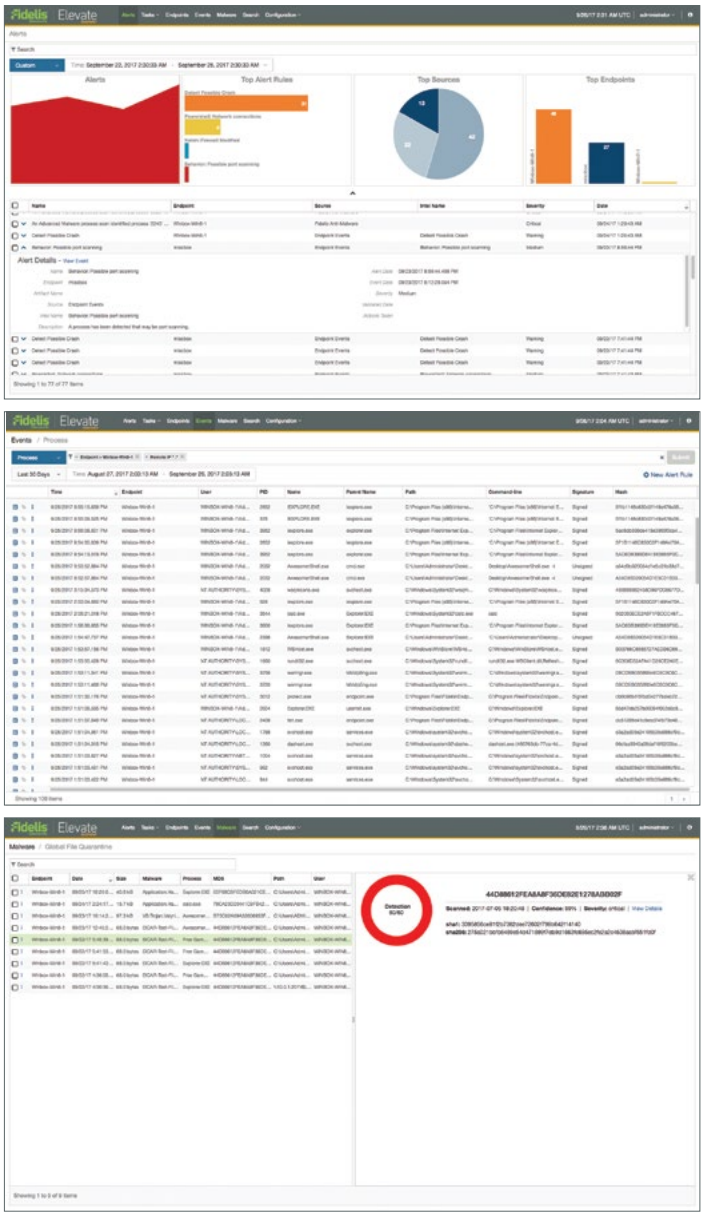
Komplexní automatizovaná detekce a reakce na vašich koncových bodech.

Moderní útoky jsou složité a často jsou tvořeny automatizovanou řadou procesů, kroků a vzájemně provázaných činností zaměřených na překonání perimetru kybernetického zabezpečení. Až příliš často jsou bezpečnostní týmy nuceny spoléhat se na poslepované ochranné systémy, které zvyšují provozní náročnost a složitost místo skutečného řešení aktuálních problémů. Chybí jim sjednocená a automatizovaná technologie pro detekci na koncových bodech, reakci a prevenci, takže nemohou tyto typy útoků včas identifikovat a reagovat na ně.

Vlastnosti produktu

Modul Fidelis Endpoint™ je zásadní součástí platformy Fidelis Elevate, která byla navržena pro automatizovanou detekci a reakci dnešních pokročilých kybernetických hrozeb. Umožňuje organizacím s jistotou detekovat bezpečnostní incidenty, řešit je a reagovat na ně za zlomek času oproti tradičním způsobům.

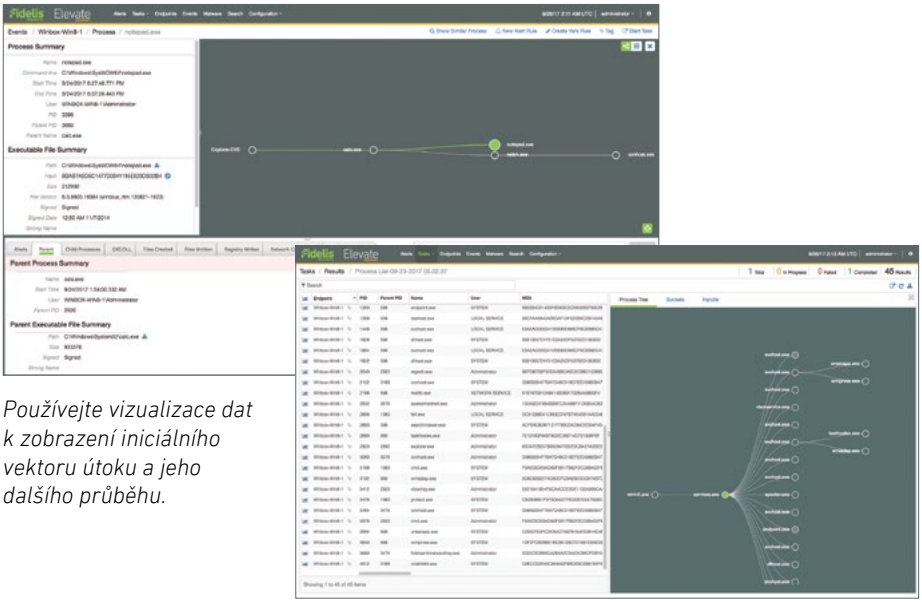
- **Integrace v síti i na koncových bodech:** Automatické validace, korelace a sběr dat týkajících se hrozeb do rozhodné akce. Umožňuje reagovat zásadně rychleji. Významně zkracuje čas působení útočníka v síti.
- **Automatická retrospektivní detekce:** Identifikujte první „oběť" společně s velikostí a rozsahem útoku. Umožní vám poznat hloubku a závažnost incidentu a okamžitě zahájit nápravu.
- **Identifikujte a zastavujte cílené útoky:** Rychle identifikujte záškodnické jednání, validujte hrozby podle mnoha různých kritérií, automatizujte nápravná opatření a posloupnost kroků analýz, proaktivně vyhledávejte hrozby.
- **Korelujte aktivitu s dalšími bezpečnostními nástroji:** Posuzujte a ověřujte alarmy generované stávajícími bezpečnostními produkty jako jsou síťová bezpečnostní řešení či SIEM, takže se budete moci zaměřit na skutečné hrozby a zavádět opatření okamžik po zjištění hrozby.
- **Rychlejší a informovanější rozhodnutí:** Automatizujte procesy reakce na incidenty, používejte analýzy hrozeb a získejte dokonalou vizibilitu každé škodlivé aktivity, která se vyskytne.



Identifikujte hrozby v reálném čase a získávejte kontext týkající se jejich závažnosti a dopadů.

Schopnosti:

- **Okamžitě reagujte:** Integrujte SIEM, firewally nové generace, výstražné nástroje a další instrumenty k automatickému propojení různorodých informací a zajištění vertikální vizibility a účinné reakce.
- **Detekujte útoky v okamžiku, kdy k nim dojde:** Neustále analyzujte události, identifikujte škodlivé aktivity jakmile k nim dojde a generujte alarmy v reálném čase.
- **Proaktivně vyhledávejte hrozby:** Používejte popisy síťových hrozeb nebo hrozeb na koncových bodech v libovolném formátu, od jednoduchých po složité, k rychlé identifikaci napadených koncových bodů a automatické reakci.
- **Urychlete třídění a vyhodnocování podezřelých incidentů:** Automaticky sbírejte bohaté systémové informace z koncových bodů a korelujte je s reputačními službami, pokročilými detektory hrozeb a informacemi o známých hrozbách, abyste dokázali identifikovat napadení koncových bodů – bez použití více úzce zaměřených produktů či nehospodárného využití času analytiků.
- **Mějte přehled o minulých událostech díky zpětnému přehrávání – automatická retrospektivní detekce:** Plně odhalte, jak došlo k útoku, co bylo ztraceno a koho ještě se týkal – i po uplynutí značné doby od původního úspěšného napadení – zaznamenáváním klíčových událostí (týkajících se např. souborů, procesů, registrů, sítí, DNS a URL) a automatickým vypracováním jejich časové sousledností společně se zahrnutím prioritních alarmů.
- **Automaticky provádějte nápravná a jiná opatření na napadených koncových bodech:** Okamžitě zastavte exfiltraci dat a rozšiřování nákazy na koncové body díky izolaci již nakažených koncových bodů, zastavením procesů, vyčištěním souborů, spuštěním skriptu, který zahájí vyhledávání virů, nebo uživatelských programů na koncových bodech.
- **Automatizujte posloupnost kroků reakce na incident:** Snadno vytvářejte a upravujte posloupnost kroků reakce na incident specifickou pro vaši organizaci.



Používejte vizualizace dat k zobrazení iniciálního vektoru útoku a jeho dalšího průběhu.

Automaticky spouštějte nápravná opatření nebo hloubkové analýzy podle definovaných spouštěcích pravidel a činností prostřednictvím workflow reagujících na alarmy.

„Hlavní výhodou zavedení Fidelis Endpoint je, že nyní jsme schopni zajistit reakci na incident vlastními silami. To nám umožnilo významně zkrátit časy reakce na incident z deseti dní na pět hodin."

– ředitel pro Forensics and eDiscovery, přední světové banky

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.

