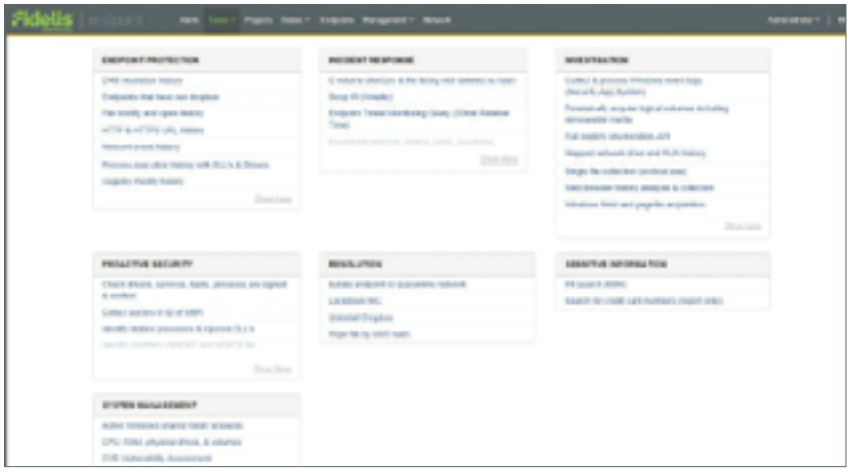
KARTA DANYCH TECHNICZNYCH

Fidelis Endpoint™

Rozpoznawanie zaatakowanych punktów końcowych oraz automatyzacja badań i reakcji

Koncentracja na istotnych incydentach

Firmy i instytucje inwestują miliony w budowanie bezpiecznych sieci i ochronę przed nieraz bardzo zmotywowanymi atakującymi. Mimo to zdeterminowanym hakerom często udaje się wtargnąć do z pozoru bezpiecznych sieci firm i wykraść własność intelektualną, poufne dane oraz informacje finansowe. Przytłoczeni liczbą zgłoszeń analitycy z operacyjnych centrów bezpieczeństwa (security operations center, SOC) i zespołów ds. bezpieczeństwa, którym powierzono zadanie kontrolowania i klasyfikowania podejrzanych incydentów, otrzymują ogromne ilości alertów. Nie są więc w stanie szybko sprawdzić, czy podejrzany incydent stanowi faktyczne zagrożenie, i nie dysponują wystarczającą ilością informacji, aby określić możliwe skutki wykrytego zagrożenia.



Zespoły ds. bezpieczeństwa mogą szybko weryfikować podejrzane incydenty i zdobywać informacje na temat ich potencjalnych skutków.

Informacje ogólne o produkcie

Fidelis Endpoint™ udostępnia dbającym o bezpieczeństwo klientom narzędzia umożliwiające zdecydowane reagowanie na przypadki naruszenia zabezpieczeń, ich weryfikację i neutralizację w czasie wielokrotnie krótszym niż w przypadku stosowania tradycyjnych rozwiązań. Fidelis Endpoint zapewnia zespołom ds. bezpieczeństwa wgląd, kontekst i automatyzację, które są potrzebne do osiągnięcia następujących celów:

- **Identyfikowanie i blokowanie ukierunkowanych ataków w zarodku.** Fidelis Endpoint umożliwia szybką identyfikację złośliwej aktywności, weryfikację i proaktywne tropienie zagrożeń na podstawie wielu kryteriów oraz automatyzację procesów naprawy i analizy.
- **Synchronizacja działań z innymi narzędziami bezpieczeństwa.** Teraz można skutecznie oceniać i weryfikować alerty generowane przez istniejące systemy zabezpieczeń, jak rozwiązania sieciowe czy SIEM, skupiać się na faktycznych zagrożeniach i natychmiast na nie reagować.
- **Podejmowanie szybszych i trafniejszych decyzji.** Jest to możliwe dzięki automatyzacji procesów reagowania, stosowaniu analiz zagrożeń i dostępowi do szczegółowych informacji na temat zidentyfikowanej złośliwej aktywności bez względu na miejsce jej występowania.
- **Szybsze neutralizowanie incydentów.** Fidelis Endpoint umożliwia automatyzację skomplikowanych i czasochłonnych procesów ręcznych, weryfikację alertów z uwzględnieniem zebranych informacji i kontekstu oraz wykorzystywanie kluczowych wskaźników skuteczności zabezpieczeń, takich jak średni czas weryfikacji (MTV) czy średni czas reakcji (MTR) do śledzenia i raportowania przypadków naruszenia zabezpieczeń.

Najważniejsze zalety

Zaawansowane możliwości dochodzeniowo-śledcze. Rejestrowanie i analiza dynamicznych danych dotyczących reakcji, obrazów pamięci lub pełnych obrazów dysku i szczegółowa analiza przez agenta w celu zebrania wszystkich danych śledczych.

Alerty o zagrożeniach w punktach końcowych. Automatyczne wykrywanie wskaźnika zagrożenia (np. adresu IP, DNS, nazwy procesu, URL czy MD5) w punkcie końcowym i samoczynne uruchomienie skonfigurowanej procedury reakcji.

Ochrona poza siecią. Monitorowanie punktów końcowych — bez względu na to, czy znajdują się w sieci, czy poza nią — w celu ochrony wszystkich punktów końcowych klienta.

Integracja z istniejącymi narzędziami do ochrony bezpieczeństwa. Płynna integracja z rozwiązaniami SIEM, zaporami nowej generacji, narzędziami do generowania alertów i innymi urządzeniami monitorującymi w celu automatycznej weryfikacji alertów oraz przystępowania do likwidacji zagrożeń.

Zarządzanie systemami. Szybka dystrybucja oprogramowania, wykonywanie określonych zadań w punktach końcowych oraz wykrywanie niezarządzanych urządzeń.

Analiza zagrożeń. Importowanie danych o zagrożeniach ze źródeł komercyjnych, danych open source i własnych danych dotyczących zagrożeń w celu automatycznego wykrywania i weryfikacji zagrożeń w punktach końcowych.

Szybsze klasyfikowanie i weryfikowanie podejrzanych incydentów przez eliminację czasochłonnych badań ręcznych wymagających udziału wysoce wykwalifikowanych i trudno dostępnych specjalistów.

O Fidelis Endpoint

- **Eliminacja tzw. martwych punktów.** Można natychmiast rozpoznawać zagrożenia bez względu na to, czy występują w sieci, czy w punkcie końcowym (w sieci lub poza nią).
- **Natychmiastowa reakcja.** Zintegrowanie rozwiązań SIEM, zapór nowej generacji i narzędzi do generowania alertów z punktami końcowymi umożliwia automatyczne łączenie osobnych informacji, uzyskanie pełnego wglądu w środowisko i skuteczną reakcję na zagrożenie.
- **Identyfikowanie punktów końcowych, w których doszło do naruszenia zabezpieczeń.** Rozwiązanie automatycznie szuka oznak naruszenia zabezpieczeń we wszystkich punktach końcowych w przypadku pozytywnej weryfikacji wskaźnika naruszenia zabezpieczeń (Indicator of Compromise, IOC).
- **Proaktywne tropienie zagrożeń.** Korzystając z szerokiej gamy narzędzi do analizy — od prostych rozwiązań po bardzo rozbudowane — działających na hoście lub w sieci, można błyskawicznie zidentyfikować naruszenie zabezpieczeń w punktach końcowych i automatycznie przystąpić do jego neutralizacji.
- **Szybsze klasyfikowanie i weryfikowanie podejrzanych incydentów.** Szczegółowe dane systemowe z punktów końcowych można zbierać automatycznie i korelować z danymi generowanymi przez usługi określania reputacji i analizy zagrożeń oraz zaawansowane detektory zagrożeń w celu weryfikacji naruszenia zabezpieczeń w punktach końcowych — bez użycia wielu oddzielnych produktów i angażowania analityka.

Kluczowe wskaźniki skuteczności zabezpieczeń, takie jak średni czas weryfikacji (MTV) i średni czas reakcji (MTR), umożliwiają monitorowanie i raportowanie incydentów.

- **Rekonstrukcja wydarzeń za pomocą funkcji Playback.** Nawet długo po wystąpieniu incydentu wciąż można dokładnie ustalić, jak doszło do ataku, co zostało skradzione i kto jeszcze był w to zamieszany. Fidelis Endpoint rejestruje (nagrywa) najważniejsze zdarzenia (dotyczące np. plików, procesów, rejestru, sieci, DNS i adresów URL), a następnie automatycznie generuje oś czasową odzwierciedlającą działania związane z potencjalnym incydentem oraz alerty z przypisanymi priorytetami.
- **Automatyczna naprawa i reakcja w zaatakowanych punktach końcowych.** Fidelis Endpoint umożliwia niezwłoczne blokowanie wyprowadzania danych oraz rekonesans i przenikanie atakujących z punktów końcowych do sieci przez izolację punktów końcowych, zatrzymywanie procesów, czyszczenie plików, uruchamianie skryptu wywołującego skanowanie antywirusowe lub uruchamianie wywoływanych przez skrypty niestandardowych procedur w punktach końcowych.
- **Automatyzacja procedur reagowania na incydenty.** Fidelis Endpoint ułatwia tworzenie i modyfikowanie obowiązujących w organizacji procedur reagowania na ataki. Zdefiniowanie reguł wyzwalania i podejmowanych działań w mechanizmie procedury reagowania umożliwia automatyczne uruchamianie procedur naprawczych lub szczegółowych analiz.

„Największą korzyścią z wdrożenia rozwiązania Fidelis Endpoint jest to, że wreszcie jesteśmy w stanie własnymi siłami reagować na złamania zabezpieczeń. Dzięki temu znacznie skróciliśmy nasz czas reakcji na cyberprzestępstwa: z 10 dni do zaledwie 5 godzin".

– Dyrektor ds. informatyki śledczej i eDiscovery jednego z pięciu największych banków świata

Korzyści

- **Skuteczniejsza ochrona przed kradzieżą zasobów i własności intelektualnej**
- **Niższe całkowite koszty reakcji na incydenty**
- **Mniejsze zakłócenia działalności firmy**
- **Mniejsze ryzyko utraty reputacji i wiarygodności**

Aby dowiedzieć się więcej o rozwiązaniach Fidelis, skontaktuj się z nami

Fidelis Cybersecurity | +48-22-275-5955 | emea@fidelissecurity.com

Fidelis Cybersecurity chroni najbardziej poufne dane świata Pomagamy klientom w szybszym wykrywaniu i neutralizacji incydentów. Współpracując z Fidelis, dowiesz się o wystąpieniu ataku, zidentyfikujesz ślady pozostawione przez atakującego i zapobiegniesz kradzieży danych.

 DS_Fidelis_Endpoint_PL_1602