www.4sync.pl
sales@4sync.pl tel.:22 299 17 00

KARTA DANYCH TECHNICZNYCH

Fidelis Elevate™

Platforma do automatycznego wykrywania i tropienia zagrożeń oraz reagowania na nie

Wyzwanie

Ataki są coraz bardziej zaawansowane i często pozostają niezauważone przez mechanizmy obrony prewencyjnej, przez co wykrywanie i tropienie zagrożeń oraz reagowanie na nie — jako ostatnia linia obrony — jest obecnie niezwykle istotne. Hakerski rekonesans i przeniknięcie do środowiska jest kwestią kilku godzin od złamania zabezpieczeń, po czym następuje faza poznawania nowego środowiska mająca na celu szybkie i głębokie ukrycie ataku. Systemowe dzienniki i monitory zdarzeń nie wykrywają tych zaawansowanych zagrożeń, a używane platformy nie udostępniają szybkich, interaktywnych i iteracyjnych funkcji wykrywania i badania ataków. Ponadto scentralizowana infrastruktura monitorowania alertów zaprojektowana z myślą o rozwiązywaniu problemów ze zgodnością z przepisami nie jest w stanie sprostać obecnym potrzebom w zakresie wykrywania, badania, reagowania i tropienia.

W rozwiązaniach tych brakuje szczegółowych metadanych z zawartością i kontekstem umożliwiających wykrywanie oraz tropienie zagrożeń, w czasie rzeczywistym i retrospektywnie, przy użyciu wielu sensorów i punktów końcowych, a także wielu kanałów informacji o zagrożeniach. Metadane są też podstawą modeli uczenia maszynowego i zastosowań nauki o danych w obszarze bezpieczeństwa.

Platforma Fidelis Elevate

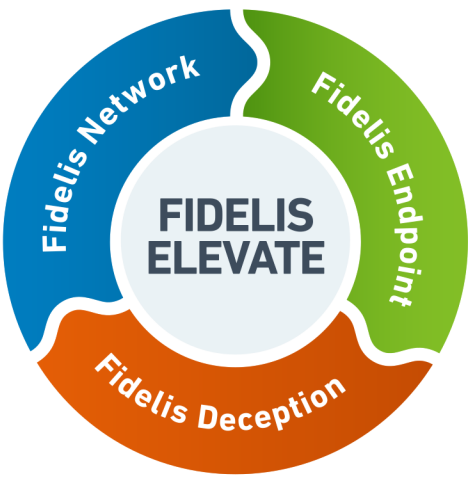
Platforma Fidelis Elevate udostępnia sensory dla bram, sieci wewnętrznych, maszyn wirtualnych w chmurze, poczty e-mail i bram WWW, a także funkcje wykrywania zagrożeń w punktach końcowych oraz reagowania na nie (EDR). Platforma zbiera z sensorów wartości ponad 300 atrybutów metadanych, niestandardowe tagi, a także dane procesów i zdarzeń w punktach końcowych. Udostępnia też zoo plików wykonywalnych i skryptów, prowadzi inwentaryzację oprogramowania i znanych luk w zabezpieczeniach oraz pozyskuje materiały dowodowe. Aby zwiększyć skuteczność wykrywania, analiz śledczych i reagowania, udostępniliśmy na tej platformie aktywowane w tych fazach zaawansowane mechanizmy obronne, a także zwiększającą wydajność pracy automatyzację większości zadań analiz zabezpieczeń warstwy 1.

W przypadku platformy Fidelis Elevate obrona skupia się na zapobieganiu, wykrywaniu i reagowaniu, oferując m.in.:

- Zapobieganie i wykrywanie w czasie rzeczywistym z zastosowaniem wielowymiarowych reguł, sygnatur, emulacji i heurystyki oraz oznak włamań
- Wykrywanie w czasie rzeczywistym na podstawie zachowań w punktach końcowych i sieci oraz analiz w środowisku sandboxingu
- Wykrywanie retrospektywne na podstawie oznak, sygnatur i anomalii w uczeniu maszynowym w ramach analiz szczegółowych metadanych z sensorów, metadanych punktów końcowych oraz zoo plików
- Technologia Deep Session Inspection® (DSI) umożliwia odtwarzanie całych sesji, dekodowanie protokołów i aplikacji, rekurencyjne dekodowanie zaszytej zawartości oraz analizowanie całej zawartości w celu wykrywania zagrożeń i kradzieży danych
- Warstwy dezinformacji zawierające „okruszki chleba", które przyciągają ataki do wabików w postaci maszyn VM z prawdziwym systemem operacyjnym, zasobów i usług IT, firmowej infrastruktury IoT oraz maszyn VM w chmurze, zapewniając wysoką precyzję alertów
- Informacje o zagrożeniach z Fidelis Insight, reguł OpenIOC, YARA i Suricata oraz od innych firm
- Usługi zarządzanego wykrywania i reagowania (MDR) oparte na platformie Elevate, które pozwalają zorganizować całodobowe czuwanie nad danym środowiskiem
- Proaktywne umowy o dyspozycyjności do reagowania na incydenty — dla firm i instytucji państwowych

Korzyści zapewniane przez Fidelis Elevate

- **Mapowanie zasobów i usług środowiska cyfrowego** oraz inwentaryzacja oprogramowania i znanych luk w zabezpieczeniach
- **Lepsze wykrywanie i reagowanie** dzięki uzupełnieniu infrastruktury zabezpieczeń o szczegółowe metadane
- **Aktywacja mechanizmów obronnych** opartych na uczeniu maszynowym obejmujących wiele sensorów, punktów końcowych i warstw dezinformacji
- **Zwiększająca wydajność pracy automatyzacja podstawowych zadań analiz zabezpieczeń** pod kątem wykrywania, analiz śledczych i reagowania
- **Weryfikacja alertów z sensorów** do punktów końcowych i zbieranie materiału dowodowego, w tym wykonywanie obrazów całych dysków
- **Sprawniejsze tropienie zagrożeń** obejmujące metadane z sensorów, zoo plików z punktów końcowych oraz dane procesów i zdarzeń
- **Wsparcie zespołów ds. bezpieczeństwa** w ramach usług MDR i IR



Najważniejsze cechy wyróżniające

Fidelis Network®

- **Deep Session Inspection® —** umożliwia odtwarzanie całych sesji, dekodowanie protokołów i aplikacji, rekurencyjne dekodowanie zaszytej zawartości oraz analizowanie całej zawartości w celu wykrywania zagrożeń i wycieków danych.
- **Wiele sensorów —** do bram, sieci wewnętrznych, maszyn wirtualnych w chmurze, poczty e-mail i bram WWW. Zapewniają pełny wgląd w dane i umożliwiają zbieranie metadanych ponad 300 atrybutów i niestandardowych tagów na potrzeby analiz w czasie rzeczywistym i retrospektywnych.
- **Profilowanie i klasyfikacja zasobów —** sensory w sieci mapują całe środowisko, z uwzględnieniem firmowej infrastruktury IoT, „shadow IT" i starszych systemów. Obsługiwany jest też import ze źródeł zewnętrznych, w tym rozwiązania Fidelis Endpoint.
- **Zapobieganie i wykrywanie —** przy użyciu statycznych, dynamicznych i retrospektywnych mechanizmów obronnych, w tym anomalii uczenia maszynowego, analiz zachowań, sandboxingu, wielowymiarowych reguł, emulacji i heurystyki, sygnatur i kanałów informacji o zagrożeniach (Fidelis Insight, źródła innych firm, udostępnione oraz wewnętrzne).
- **Zapobieganie kradzieży i utracie danych —** przy użyciu predefiniowanych zasad, profilowania danych, atrybutów metadanych i niestandardowych tagów w ramach mechanizmów ochrony danych przed utratą w sieci, sensorów WWW i sensorów poczty e-mail, w tym analiz OCR tekstu w obrazach.
- **Automatyzacja —** zadań analiz zabezpieczeń warstwy 1 w zakresie zapobiegania, wykrywania, analiz śledczych i reagowania w jednym interfejsie użytkownika, co ma na celu sprawne działanie mechanizmów obrony sieci i punktów końcowych oraz dezinformacji.

Fidelis Endpoint®

- **Zapobieganie —** ochrona przed złośliwym oprogramowaniem w systemach Windows oparta na narzędziu BitDefender lub oprogramowaniu antywirusowym wybranym przez klienta. Blokowanie zachowań procesów i procesów przy użyciu reguł IOC lub YARA działa niezależnie od rozwiązań antywirusowych.
- **Wykrywanie i reagowanie —** niezawodna ochrona punktów końcowych dla systemów Windows, macOS i Linux, w tym monitorowanie zachowań i wykrywanie na podstawie oznak (IOC, YARA), działająca zarówno przy aktywnym połączeniu z siecią, jak i jego braku, a ponadto izolowanie systemów, integralność sprawdzana metodą analiz śledczych przez zapisywanie obrazów całych dysków, zbieranie wybranych plików i folderów oraz rejestrowanie zawartości pamięci.
- **Zoo plików i metadane —** dane procesów i zdarzeń z 30, 60 lub 90 dni, umożliwiające automatyczne oraz ręczne wykrywanie i tropienie zagrożeń, a także obsługa niestandardowych operacji wyszukiwania oraz zbieranie nowych plików wykonywalnych i skryptów w celu analizy.
- **Zainstalowane oprogramowanie i znane luki w zabezpieczeniach —** sposób na zachowanie higieny zabezpieczeń punktów końcowych dzięki zestawieniom zainstalowanego oprogramowania z linkami do raportów MITRE CVE i Microsoft KB na temat luk, informacjom o stanach systemów operacyjnych i zastosowanych poprawek, możliwościom raportowania oraz zmian stanów zapory i oprogramowania antywirusowego, a także alertom o podłączeniach urządzeń do portu USB.
- **Biblioteka skryptów —** z setkami gotowych do użycia skryptów do automatycznego gromadzenia artefaktów, reagowania na zagrożenia lub przywracania punktów końcowych, a także możliwością dostosowywania do doraźnych potrzeb lub szczególnych wymagań klienta.
- **Informacje o zagrożeniach —** m.in. Fidelis Insight, sandboxing w chmurze, analizy oparte na uczeniu maszynowym, reguły oznak behawioralnych oraz badanie zagrożeń. Oprócz tego obsługiwane są niestandardowe reguły zachowań oraz otwarte kanały dla oznak IOC, reguł YARA oraz zewnętrznych źródeł informacji o zagrożeniach.

Fidelis Deception™

- **Precyzyjne alerty —** do badań cyberbezpieczeństwa w celu poznawania taktyk, technik i procedur ataków, analizowania plików z zastosowaniem prawdziwych wabików OS lub inteligentnego systemu alarmowego opartego na wabikach emulujących, co eliminuje ryzyko. Rolę wabików mogą też pełnić firmowa infrastruktura IoT oraz niestandardowe urządzenia.
- **Automatyzacja i skala —** możliwość wykrywania elementów środowisk w celu automatycznego generowania wabików, dystrybucji, testowania dostępu i anonsowania wabików, a także automatycznego generowania „okruszków chleba" przeznaczonych do umieszczania w rzeczywistych systemach w charakterze przynęt.
- **Duży wybór wabików —** wabiki w postaci prawdziwych maszyn VM z systemem operacyjnym, wabiki oparte na złotych obrazach OS, wabiki emulujące zasoby i usługi IT, wabiki VM w chmurze, wabiki w formie firmowej infrastruktury IoT, a także ładowanie stron internetowych do wabików HTTP i obsługa przesyłania plików do analiz w chmurowym środowisku sandboxingu.
- **Analizy ruchu —** skalowanie do poziomu korporacyjnego w celu odróżnienia ruchu powodowanego przez ludzi od zautomatyzowanego ruchu generowanego przez złośliwe oprogramowanie, wykrywanie anomalii i komunikacji C&C, a także profilowanie i klasyfikacja zasobów oraz usług wykorzystywane do ciągłego mapowania środowiska w celu wykrywania zmian.
- **Adaptacja i świeżość —** warstwy dezinformacji automatycznie dostosowują się do zmian w środowisku, a także obsługują częste operacje logowania do wabików, publikacje w tabelach ARP, zapytania do serwerów DNS i fałszywe konta z dużą aktywnością w usłudze Active Directory.

Wdrożenie lokalne

- Klient zajmuje się konserwacją wszystkich urządzeń, punktów końcowych i narzędzi administracyjnych oraz zarządzaniem nimi
- Profesjonalne usługi Fidelis stanowią pomoc we wdrożeniu i szkoleniach
- Dostępne sensory: Direct, Mail, Internal, Cloud VM i Web
- Usługi konserwacji obejmują aktualności o zagrożeniach dostarczane przez zespół firmy Fidelis ds. badania zagrożeń
- Licencje na dodatkowe urządzenia i sensory w miarę wzrostu potrzeb

Wdrożenie w chmurze

- Infrastruktura jest utrzymywana przez firmę Fidelis, w tym metadane, dzięki czemu klient może się skupić na kwestiach bezpieczeństwa
- Szybkie wdrożenie i błyskawiczna implementacja sensorów, warstw dezinformacji i punktów końcowych
- Rozbudowa w miarę rozwoju środowiska oraz udostępnienie dowolnie dużej wymaganej liczby sensorów programowych i punktów końcowych
- Niezakłócone działanie podczas przejścia ze środowiska testowego do produkcyjnego
- Uproszczony model subskrypcyjny na podstawie zapotrzebowania na przepustowość i pamięć masową

Aby dowiedzieć się więcej, skontaktuj się z nami

Fidelis Cybersecurity | 800 652 4020 | info@fidelissecurity.com

Fidelis Cybersecurity jest czołowym dostawcą rozwiązań do wykrywania i tropienia zagrożeń oraz reagowania na nie. Fidelis zwalcza całą gamę cyberprzestępstw, w tym kradzież danych i szpiegostwo, zapewniając pełny obraz środowisk hybrydowych z infrastrukturą chmurową i lokalną, automatyzując wykrywanie zagrożeń i kradzieży danych, wspomagając tropienie zagrożeń i optymalizując reakcje na incydenty dzięki kontekstom, szybkości i dokładności. Rozwiązania Fidelis są używane jako ostatnia linia obrony przez wiele firm z grupy Global 1000 oraz władz państwowych. Zapraszamy na wspólne łowy. Więcej informacji: www.fidelissecurity.com.

