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

KARTA DANYCH TECHNICZNYCH

Fidelis Network®

Niezastąpiona architektura zabezpieczeń z funkcjami analiz ruchu sieciowego, WWW i e-mail oraz ochrony przesyłanych danych przed utratą

Znacznie więcej, niż wskazuje nazwa

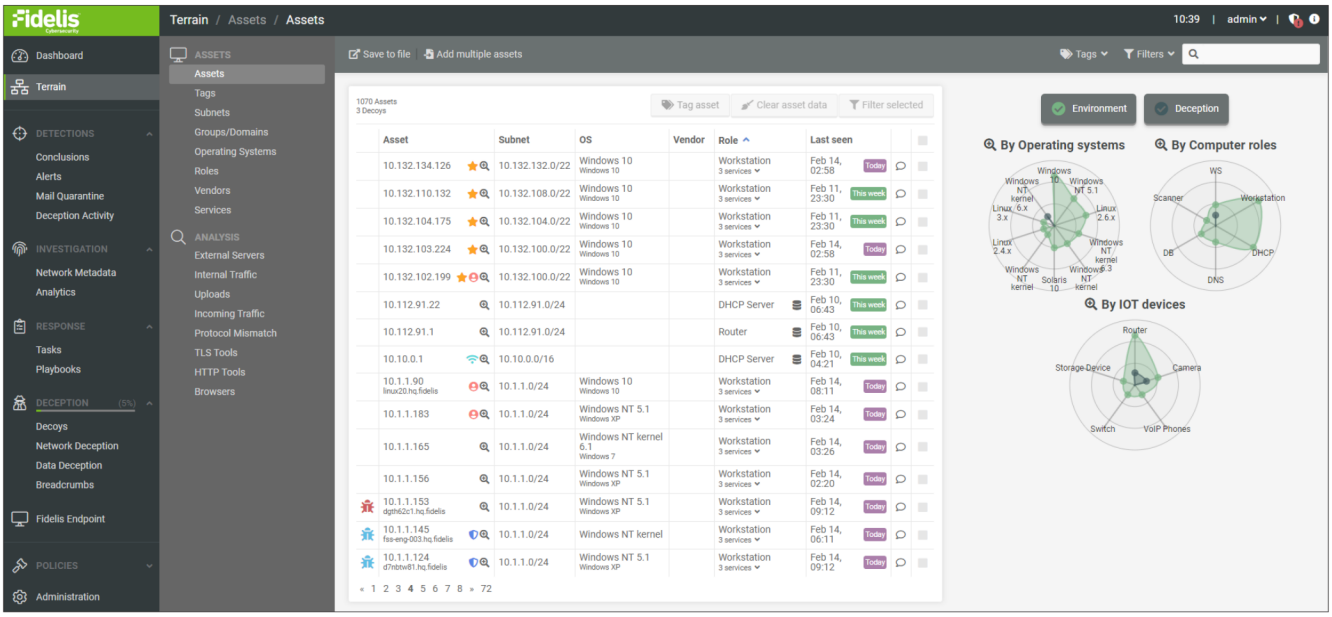
Zakres działania rozwiązania Fidelis Network znacznie wykracza poza to, co sugeruje jego nazwa. Łączy ono funkcje wykonywanych w czasie rzeczywistym analiz danych z pięciu lokalizacji sensorów (bram, sieci wewnętrznych, poczty e-mail, WWW i chmury), ochronę przed utratą danych ruchu sieciowego, e-mail i WWW oraz zabezpieczenia poczty e-mail, m.in. przez OCR obrazów. Ponadto bogate w kontekst metadane umożliwiają wykrywanie i tropienie zagrożeń w całym środowisku cyfrowym, które jest stale mapowane przez Fidelis Network z zastosowaniem profilowania i klasyfikacji zasobów. Rozwiązanie to, będąc z założenia otwarte dla kanałów informacji o zagrożeniach, jest nowoczesnym rdzeniem dla każdej infrastruktury zabezpieczeń.

Metadane jako DNA infrastruktury zabezpieczeń

Diagnozowanie stanu bezpieczeństwa na podstawie dzienników, zdarzeń i alertów jest nieco ograniczone. Przyszłość uczenia maszynowego i nauki o danych z perspektywy ochrony bezpieczeństwa leży w szczegółowych metadanych dostępnych na poziomie zawartości i kontekstu. A skoro zależy nam na zapobieganiu zagrożeniom i ich wykrywaniu w czasie rzeczywistym lub analizie retrospektywnej z uwzględnieniem nowo odkrytych oznak zagrożeń, metadane muszą być generowane stale, a nie całe godziny czy dni później. W Fidelis Network zastosowano opatentowaną technologię Deep Session Inspection® (DSI), która umożliwia odtwarzanie całych sesji, dekodowanie protokołów i aplikacji, dekodowanie zaszytej zawartości oraz analizowanie zawartości, zagrożeń i mechanizmów ochrony przed utratą danych w czasie rzeczywistym.

Identyfikacja, klasyfikacja, wykrywanie, blokowanie i reagowanie w jednym rozwiązaniu

- Możliwość oceny stanu w ramach jednego rozwiązania dzięki zagregowanym ostrzeżeniom, kontekstom i materiałom dowodowym
- Automatyzacja zapobiegania, wykrywania, analiz śledczych oraz reakcji przy użyciu gotowych procedur i specjalnie dostosowanych skryptów
- Ujawnianie przypadków niewłaściwego użytkowania zasobów i szyfrowania oraz obchodzenia serwerów proxy i zabezpieczeń
- Wykrywanie niestandardowych protokołów, usuwanie maskowania oraz wykrywanie ścieżek ataku i zagrożeń wewnętrznych
- Ocena ryzyka na podstawie analiz behawioralnych i historycznych oraz zarządzanie zasadami i alertami
- Wielodostępne sensory VLAN z uprawnieniami tworzenia zasad obsługujące wiele zespołów
- Otwarty interfejs zasad oraz wysyłanie alertów i danych do rozwiązań SIEM lub SOAR
- Zgodność ze standardem FIPS 140-2



Wykrywanie i mapowanie elementów środowiska sieciowego

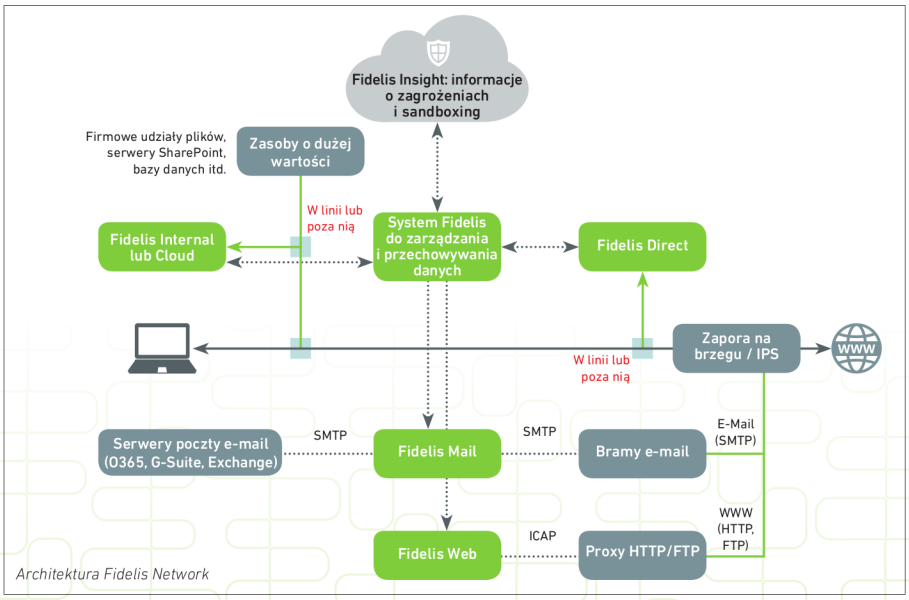
Konsolidacja zapobiegania, wykrywania i reagowania

Budowanie infrastruktury zabezpieczeń zaczyna się od rdzenia zapewniającego wgląd w czasie rzeczywistym obejmujący:

- Wszystkie porty i protokoły przy użyciu technologii DPI, DSI (Layer7) oraz PCAP
- Analizy dwukierunkowe z odtwarzaniem całych sesji
- Dekodowanie protokołów, aplikacji i zaszytej zawartości z rekurencyjnym wyodrębnianiem obiektów
- Sensory ruchu bezpośredniego, wewnętrznego, e-mail, WWW i chmurowego zapewniające szeroko zakrojony wgląd
- Profilowanie i klasyfikacja zasobów środowiska cyfrowego, w tym import źródeł zewnętrznych
- Ustrukturyzowane metadane ponad 300 atrybutów, zindeksowane w celu szybkiej obsługi zapytań
- Rozszerzone metadane (np. alerty, informacje o zagrożeniach, geolokalizacja, tagowanie zasad, ID2IP)
- Niestandardowe tagi z zawartości dekodowanych obiektów (np. autor, stopka czy słowo kluczowe)
- Przechowywanie metadanych lokalnie lub w chmurze przez 360 dni lub dłużej na potrzeby analiz retrospektywnych

Wgląd w czasie rzeczywistym umożliwia uruchamianie wielu mechanizmów obronnych w architekturze Fidelis Network, takich jak:

- **Zapobieganie zagrożeniom** przy użyciu statycznych podpisów, wielowymiarowych reguł zachowań, kanałów informacji o zagrożeniach oraz emulacji i heurystyki
- **Ochrona przed utratą danych** z zastosowaniem profilowania i klasyfikacji danych przy użyciu wbudowanych zasad dotyczących znanych wymogów zgodności na wszystkich sensorach sieci, poczty e-mail i WWW w celu generowania alertów o naruszeniach zasad
- **Zapobieganie wyciekom/kradzieży danych** — sensory bezpośrednie i wewnętrzne zrywają sesje, sensory e-mail poddają kwarantannie, odrzucają, przekierowują lub usuwają załączniki, a sensory WWW przekierowują do stron internetowych lub zrywają sesje
- **Zabezpieczenia poczty e-mail,** w tym blokowanie wewnętrznych ataków dyspersyjnych (ang. spray attack) na chmurową lub lokalną pocztę e-mail za pomocą analiz adresów URL przed kliknięciem, analiz załączników i OCR obrazów pod kątem ewentualnego wycieku danych
- **Analizy zabezpieczeń** na podstawie dużej i małej częstości zdarzeń oraz analizy sekwencji
- **Wykrywanie zagrożeń** dzięki zastosowaniu sandboxingu w chmurze, analizom zachowań w sieci, automatycznemu uwzględnianiu nowych informacji o zagrożeniach w analizach metadanych retrospektywnych oraz wykrywaniu anomalii przy użyciu mechanizmów uczenia maszynowego
- **Profilowanie zaszyfrowanego ruchu TLS** na podstawie metadanych i certyfikatów, rozróżnianie operacji przeglądania dokonywanych przez człowieka i ruchu generowanego przez urządzenia, a także rozwijanie modeli nauki o danych w celu wykrywania ukrytych zagrożeń
- **Otwarte kanały informacji o zagrożeniach** (Fidelis Insight, Reputation, STIX/ TAXII, YARA, Suricata) oraz wewnętrzne źródła informacji tego rodzaju, w tym własne, niestandardowe reguły i oznaki włamań
- **Tropienie zagrożeń** przy użyciu analiz zawartości w czasie rzeczywistym lub zindeksowanych metadanych retrospektywnych obsługujących szybkie iteracyjne i interaktywne zapytania w celu sprawdzania hipotez tropów



Architektura Fidelis Network

Oprzyj środowisko na niezastąpionym rozwiązaniu Fidelis Network, płynnie zintegrowanym z Fidelis Endpoint® i Fidelis Deception®.

Połączenie produktów Network, Endpoint i Deception w celu stworzenia platformy Fidelis Elevate zapewnia niezrównany wgląd w środowisko cyfrowe firmy, w tym podatne na ataki obszary. Rozwiązanie Fidelis w pełni integruje, automatyzuje i koordynuje niezawodne mechanizmy obsługujące m.in. wykrywanie i klasyfikację zasobów, ochronę przed utratą danych w sieci, wykrywanie zagrożeń i reakcje na nie, wykrywanie i reakcje w punktach końcowych oraz dezinformację.

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.

