KARTA DANYCH TECHNICZNYCH

Fidelis Network™

Wykrywanie, badanie i powstrzymywanie zaawansowanych ataków na każdym ich etapie

Niezawodne wykrywanie poważnych ataków

Firmy i instytucje inwestują miliony w budowanie bezpiecznych sieci, aby się chronić 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. Analitycy z tzw. operacyjnych centrów bezpieczeństwa (security operations center, SOC) oraz zespoły ds. bezpieczeństwa otrzymują ogromne ilości alertów. Wskutek tego często zupełnie przeoczają poważne ataki bądź zauważają je długo po kradzieży istotnych danych.

Wykrywanie i analizowanie ruchu na bardzo niskim poziomie — tam, gdzie kryją się atakujący. Można identyfikować ich narzędzia, taktyki oraz zachowania, co pozwala na szybkie badanie charakteru ataku i zapobieganie kradzieży danych.

Informacje ogólne o produkcie

Fidelis Network™ udostępnia dbającym o bezpieczeństwo klientom narzędzia umożliwiające zdecydowane wykrywanie, badanie i powstrzymywanie zaawansowanych ataków na każdym ich etapie. Rozwiązanie to analizuje cały ruch w sieci organizacji nawet przy jego kilkugigabitowej szybkości i rozpoznaje narzędzia oraz taktyki zaawansowanych cyberprzestępców, którym na ogół udaje się pokonać systemy zabezpieczeń w innych sieciach. Fidelis zapewnia wgląd, kontekst i szybkość niezbędne do rozpoznawania zagrożeń i udaremniania prób kradzieży danych.

- **Identyfikacja ataków niewykrywanych przez inne rozwiązania.** Rozwiązanie Fidelis identyfikuje nie tylko zaawansowane złośliwe oprogramowanie, exploity czy komunikację C&C, ale też zachowania atakujących, w tym związane z rekonesansem i przenikaniem do sieci oraz przygotowywaniem danych do wyprowadzenia na zewnątrz.
- **Identyfikowanie i blokowanie ukierunkowanych ataków w zarodku.** Network umożliwia szybkie identyfikowanie złośliwych zachowań — w tym aktywności w metadanych sieciowych, komunikacji C&C oraz działań związanych z rekonesansem i przenikaniem do sieci — oraz zapobieganie kradzieży danych.
- **Korelowanie pozornie niepowiązanych zdarzeń i zachowań w sieci.** Dzięki stosowaniu automatycznych mechanizmów tropiących i analiz zabezpieczeń do retrospektywnych metadanych zbieranych w ramach każdej sesji sieciowej można skutecznie, korelować i weryfikować alerty generowane przez pozornie niepowiązane ze sobą zachowania w sieci.
- **Szybsze wykrywanie incydentów i radzenie sobie z nimi.** W ramach jednego interfejsu można szybko uzyskiwać odpowiednie informacje i analizować dane z sieci pod kątem zagrożeń, a jeśli zostanie zgłoszony alert, analitycy zabezpieczeń mogą błyskawiczne przystąpić do badań.

Najważniejsze zalety

Wykrywanie niewykrywalnego. Unikatowe, czekające na opatentowanie mechanizmy przechwytywania, zapisywania i automatycznego analizowania metadanych rozwiązania Fidelis przyspieszają wykrywanie i analizowanie zaawansowanych ataków ukierunkowanych z użyciem standardowego lub zaawansowanego złośliwego oprogramowania, exploitów oraz komunikacji C&C.

Analizy w czasie rzeczywistym i historyczne w jednym interfejsie. Połączenie dogłębnych analiz zawartości przesyłanych obiektów, analiz historycznych, możliwości wykrywania i badania przeszłych zdarzeń oraz reguł specjalnie opracowanych przez zespół firmy Fidelis ds. badania zagrożeń pozwala szybko wykrywać występujące w danym środowisku zagrożenia.

Kontekst i zawartość. Mechanizm Deep Session Inspection® generuje metadane na poziomie protokołów, aplikacji i zawartości, zapewniając szeroki kontekst nieosiągalny w przypadku innych rozwiązań. Stosując inteligentną analizę na wielu poziomach struktury zawartości, można zwiększyć możliwości wykrywania ataków.

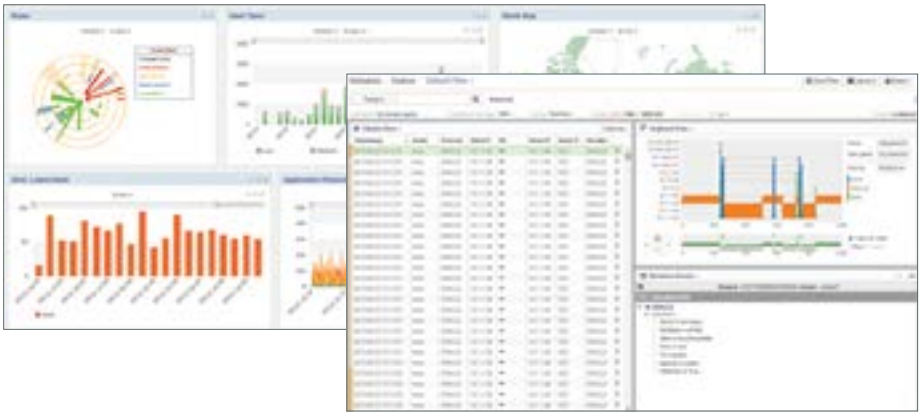
Kompleksowe rozwiązanie sieciowe. Rozwiązanie Fidelis udostępnia szeroką gamę ściśle zintegrowanych funkcji, m.in. analizy złośliwego oprogramowania, wykrywanie zaawansowanych zagrożeń, analizy dochodzeniowo-śledcze sieci, zapobieganie utracie danych oraz analizy zabezpieczeń.

Szybkość i skalowalność. Rozwiązanie obsługuje dogłębną inspekcję sesji przy wielogigabitowej szybkości transmisji i błyskawicznie udostępnia kluczowe informacje, umożliwiając skuteczne identyfikowanie aktywnych zagrożeń w środowisku o każdej wielkości.

Mechanizm Deep Session Inspection oraz wgląd we wszystkie porty i protokoły pozwala identyfikować ataki niewykrywalne dla innych rozwiązań z dziedziny bezpieczeństwa sieci.

Możliwości

- **Szybsze wyjaśnianie incydentów.** Najbardziej czasochłonne zadanie w ramach badań incydentów, tj. zbieranie danych, można uprościć. Dzięki temu eksperci szybciej dotrą do sedna problemu i będą mogli skupić się na tym, co naprawdę ważne.
- **Wykrywanie ataków na każdym etapie.** Ataki są wykrywane na każdym etapie, także wtedy, gdy cyberprzestępcy prowadzą działania związane z rekonesansem i przenikaniem do sieci, tworzą kanały komunikacji C&C i przygotowują kradzież danych.
- **Widoczność wszystkich portów i protokołów.** Wszystkie porty i protokoły w sieci można monitorować z uwzględnieniem niewłaściwego użytkowania protokołów i usług na niestandardowych portach. Poza tym, dzięki przechowywaniu metadanych dotyczących wszystkich sesji sieciowych objętych inspekcją przez rozwiązanie Fidelis, w razie potrzeby można się cofnąć w czasie i prześledzić działania atakującego.
- **Deep Session Inspection®.** Ta funkcja umożliwia dekodowanie i analizowanie zawartości w czasie rzeczywistym — bez względu na to, jak głęboko jest ona zagnieżdżona. Mechanizm Deep Session Inspection wychwytuje każdy pakiet przesyłany przez sieć. Następnie — korzystając z pamięci RAM — łączy pakiety w bufory sesji i rekursywnie dekoduje oraz analizuje dostępne w buforach protokoły, aplikacje i obiekty zawartości w czasie rzeczywistym, tj. podczas trwania sesji. Dzięki temu rozwiązanie Fidelis sięga do głębszych warstw aplikacji, a zwłaszcza zawartości przesyłanej przez sieć.
- **Retrospektywne wykrywanie i badanie incydentów.** W razie potrzeby można badać, co atakujący zrobił w przeszłości. Zbierając i przechowując mnóstwo metadanych na poziomie zawartości zarówno z sieci, jak i urządzeń końcowych, rozwiązanie Fidelis oferuje prostsze, szybsze i mniej kosztowne metody analizowania danych historycznych.
- **Powstrzymywanie ataków w sieci.** Można identyfikować aktywne zagrożenie zewnętrzne lub wewnętrzne w sieci i jednostronnie blokować nieuprawnione transmisje danych w czasie rzeczywistym — na wszystkich portach i z użyciem wszystkich protokołów — bez polegania na serwerach proxy podmiotów zewnętrznych.
- **Stałe monitorowanie zagrożeń związanych z pocztą e-mail.** Sondy Fidelis Mail monitorują wszystkie adresy URL znalezione w e-mailach i dodatkowo kontrolują wszelkie związane z nimi działania w sesjach, lokalnie oraz w chmurze.



W ramach jednego rozwiązania można bezpośrednio przechodzić od wykrywania w czasie rzeczywistym do badań i działań.

Nieustająca koncentracja na zapobieganiu utracie danych w sieci oraz szerokie możliwości obrony przed zaawansowanymi atakami sprawiają, że rozwiązanie Fidelis jest atrakcyjną ofertą i niewątpliwie wyróżnia się na tle konkurencyjnych produktów do analizowania zagrożeń i ochrony przed nimi.

– IDC, Combined Endpoint and Network Visibility Vital to Combating Advanced Threats, sierpień 2015

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_Network_PL_1602