Wdrożenie rozwiązań FireEye na **10.000** hostów

Klient oczekiwał, aby po wdrożeniu zespoły ds. bezpieczeństwa potrafiły wykrywać, analizować i wyciągać wnioski z wykrytych incydentów **w czasie znacznie krótszym, niż ten potrzebny przy stosowaniu dotychczasowych metod.** Biorąc pod uwagę wymagania Klienta – zabezpieczenie m.in. 10 000 komputerów (stacjonarne, laptopy), sieci i infrastruktury IT oraz dokumentów w warunkach rozproszonej organizacji, do realizacji projektu **wybrano rozwiązania FireEye** oraz **Mediarecovery**, jako **partnera mającego wysokie kompetencje technologiczne.**

Zaimplementowane rozwiązania

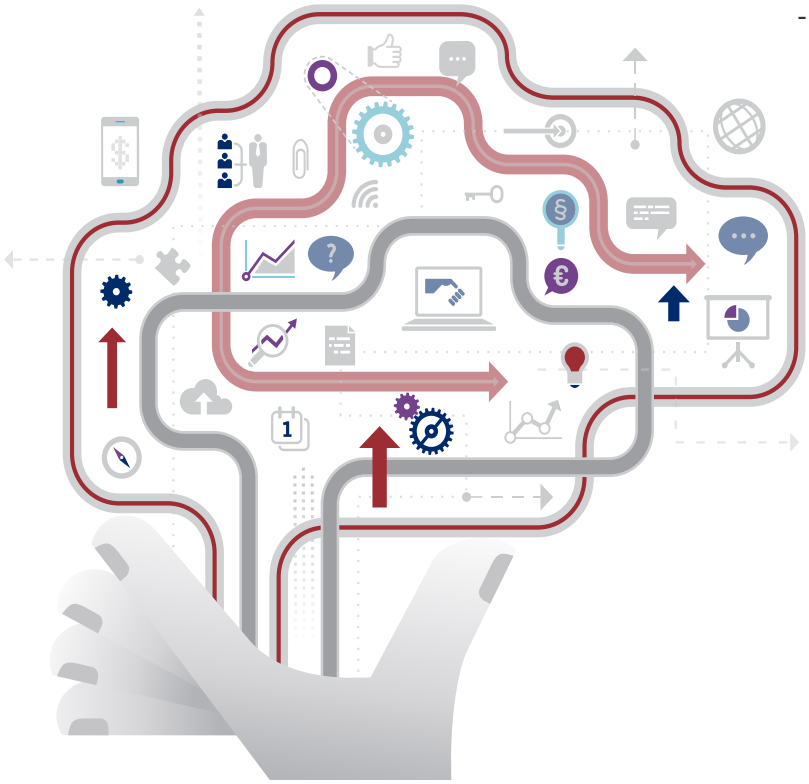
- **FireEye NX** – zabezpiecza infrastrukturę przed zaawansowanymi zagrożeniami, blokuje próby ataku z sieci oraz uniemożliwia komunikację C&C.
- **FireEye EX** – blokuje próby ataku przy zastosowaniu komunikacji mailowej, w tym spear phishing.
- **FireEye HX** – chroni endpointy przed malware, exploitami i umożliwia threat hunting.
- **FireEye CM** - obsługuje wszystkie komponenty FireEye oraz koreluje wykryte zagrożenia.

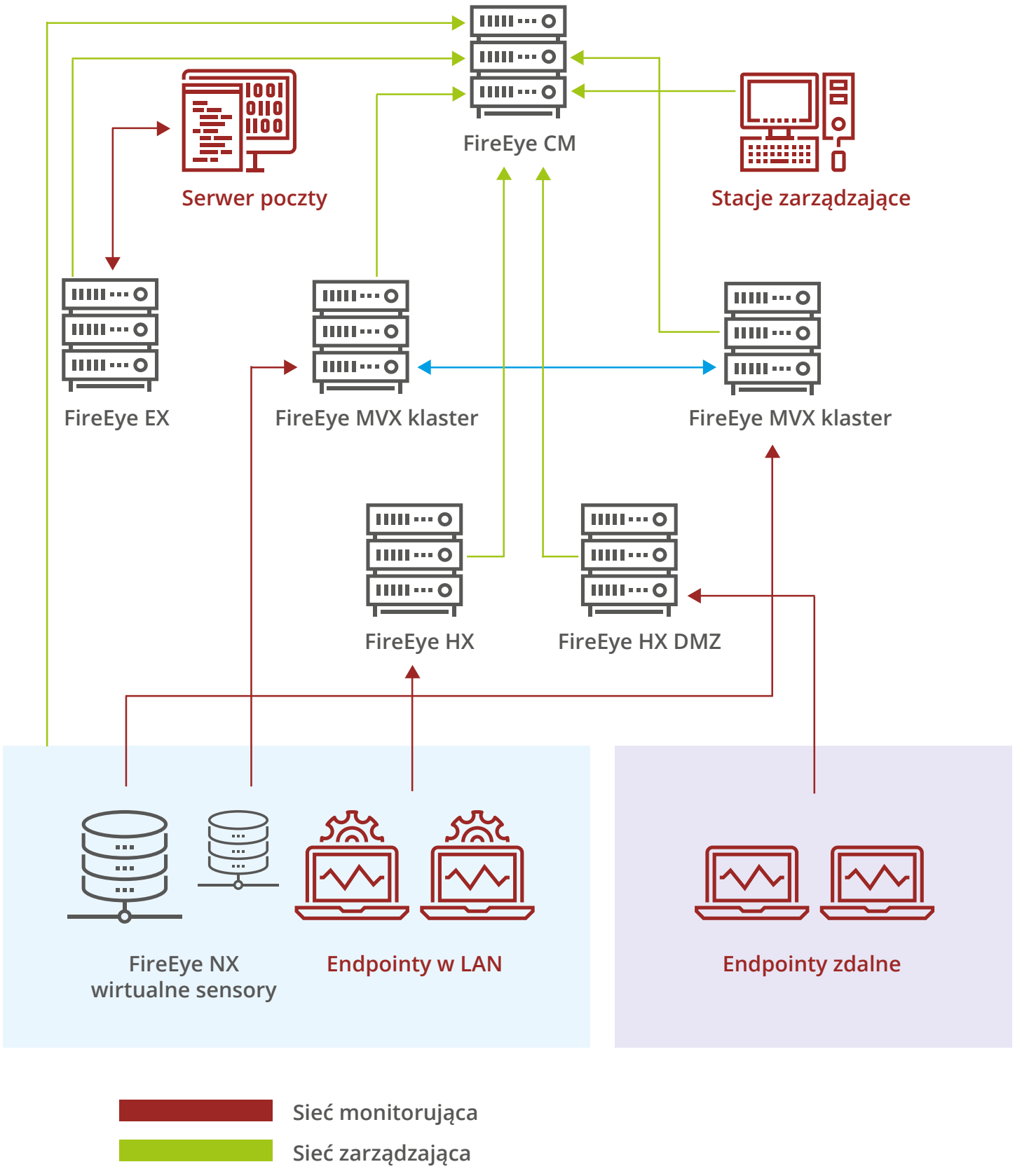
Architektura

FireEye DTI Update Portal posiada kompletny zbiór aktualizacji systemowych oraz definicje nowych zagrożeń.

Realizacja obejmowała wdrożenie dwóch rozwiązań FireEye MVX w klastrze, które znajdują się w centralnym punkcie systemu zabezpieczeń oraz rozwiązania HX i EX. FireEye HX został przygotowany do obsługi **10 000 hostów.** Do rozwiązania MVX zostało dołączonych **100 wirtualnych sensorów NX** rozmieszczonych w różnych lokalizacjach, których zadaniem było przesyłanie próbek do analizy w systemie MVX. Gotowa architektura pozwala na badanie złośliwego oprogramowania pochodzącego z najpopularniejszych źródeł: web, e-mail oraz endpoint.

Rozwiązania FireEye nie muszą mieć stałego dostępu do Internetu, co było kluczowe dla Klienta, gdyż posiada on bardzo rygorystyczne zasady definiujące dostęp do sieci internetowej. W projekcie zastosowano zatem licencję offline, dzięki której wszystkie aktualizacje systemu i sygnatur odbywają się przez dedykowany portal - FireEye DTI Update Portal. Wyznaczony zespół po stronie Klienta otrzymał dostęp do portalu, z którego pobiera aktualne sygnatury, najnowsze obrazy tzw. Guest Image oraz najnowsze wersje systemu bazowego tzw. Base Image. Wszystkie pobierane elementy umieszczane są w centralnym systemie FireEye CM, z którego automatycznie aktualizują się wszystkie elementy architektury, bez ingerencji administratora.




FireEye CM
Serwer poczty
Stacje zarządzające
FireEye EX
FireEye MVX klaster
FireEye MVX klaster
FireEye HX
FireEye HX DMZ
FireEye NX
wirtualne sensory
Endpointy w LAN
Endpointy zdalne
Sieć monitorująca
Sieć zarządzająca

Etapy projektu

1. Etap planowania	Zebranie wymagań oraz informacji o infrastrukturze.
2. Etap realizacji	Dostarczenie sprzętu, oprogramowania oraz licencji. Następnie zainstalowanie, uruchomienie i aktualizacja oprogramowania.
3. Etap stabilizacji	Poddanie wszystkich elementów sprzętowo-programowych testom prawidłowości działania. Wyeliminowanie nieprawidłowości.
4. Etap odbioru	Przekazanie dokumentacji powdrożeniowej, przeprowadzenie szkolenia dla administratorów systemu.
5. Etap wsparcia technicznego	Objęcie wsparciem producenta oraz wsparciem technicznym wszystkich dostarczonych rozwiązań.

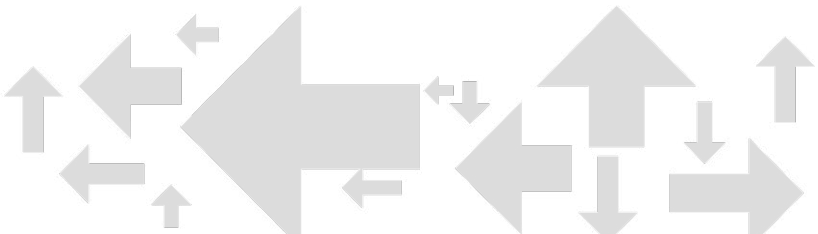
Na co warto zwrócić uwagę w tym projekcie?

Krótki czas wdrożenia

Realizacja pierwszych czterech etapów trwała **10 dni.** Dzięki eksperckiej wiedzy i odpowiedniemu zaplanowaniu prac projektowych przez inżynierów **Mediarecovery** oraz dużemu zaangażowaniu ze strony Klienta w przygotowanie infrastruktury, wdrożenie było możliwe w tak krótkim czasie.

Zastosowanie architektury SMART GRID

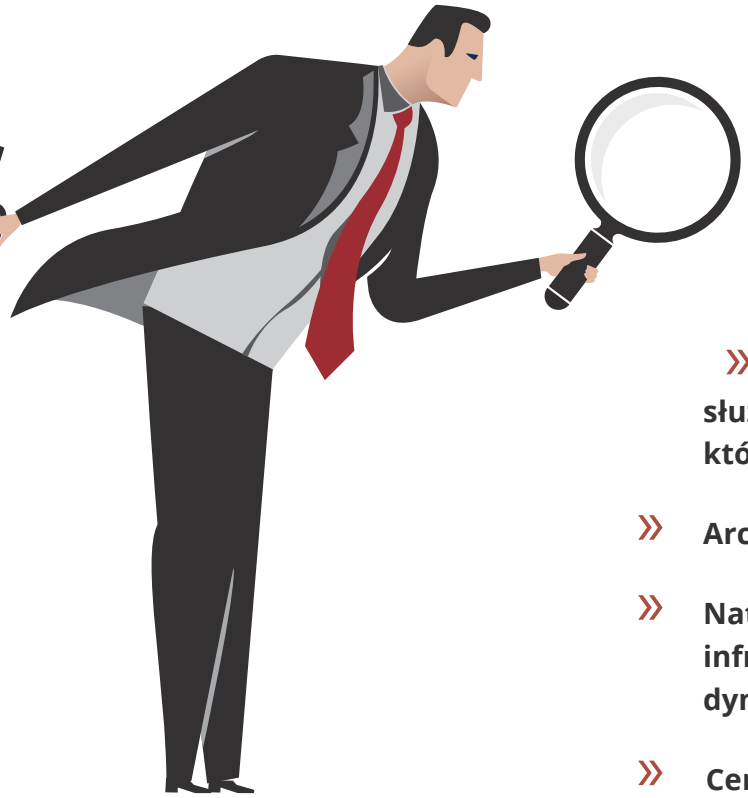
SMART GRID umożliwiała analizę podejrzanych obiektów pochodzących z ruchu internetowego i blokowanie pliku, który sklasyfikowano jako zainfekowany, dzięki wirtualnym sensorom **FireEye NX - SMART NODE** rozporoszonym w różnych lokalizacjach infrastruktury IT. FireEye NX SMART NODE wykonują statyczną analizę obiektów, po czym przekazują pliki do centralnego punktu FireEye MVX, gdzie poddaje się je analizie dynamicznej.



Architekturę SMART GRID można w łatwy sposób dopasować do rozbudowanej infrastruktury Klienta.

Zastosowanie architektury SMART GRID pozwala uniknąć instalacji fizycznych serwerów, gdy Klient dysponuje złożoną infrastrukturą zabezpieczeń. Warto zauważyć, że w tym typie architektury wszystkie wdrożone elementy komunikują się dwukierunkowo i mogą przesyłać informacje do innych elementów FireEye co pozwala na powiązanie zagrożeń wykrytych w FireEye NX, EX oraz HX. Pojedyncze zagrożenia wykrywane przez poszczególne elementy FireEye mogą nie wskazywać na istotę ataku, dopiero po odpowiednim powiązaniu wskazują, iż mamy do czynienia z poważnym zagrożeniem.

Korzyści dla Klienta



- **Zautomatyzowana ochrona przed atakami APT.**
- **Dokładna analiza powłamaniowa tzw. threat hunting.**
- **Zabezpieczenie wszystkich kanałów służących do transferu informacji/komunikacji, którymi malware jest rozpowszechniany.**
- **Architektura odseparowana od Internetu.**
- **Natychmiastowa ochrona nowo powstałego obszaru infrastruktury IT Klienta, dzięki zastosowaniu dynamicznego środowiska.**
- **Centralne zarządzanie wszystkim komponentami.**

Kontakt

Media Sp. z o.o.
ul. Piotrowicka 61, 40-723 Katowice
tel: +48 32 782 95 95

Oddział Warszawa
ul. Nowogrodzka 56A, 00-695 Warszawa
tel. +48 22 719 97 00

e-mail: biuro@mediarecovery.pl