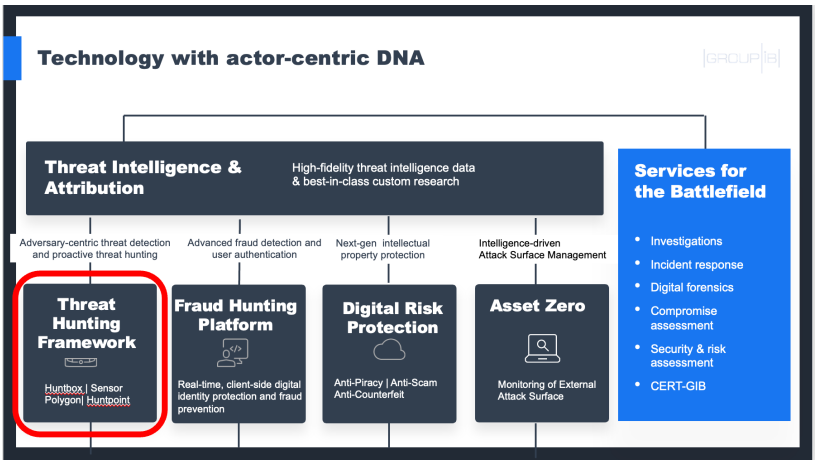
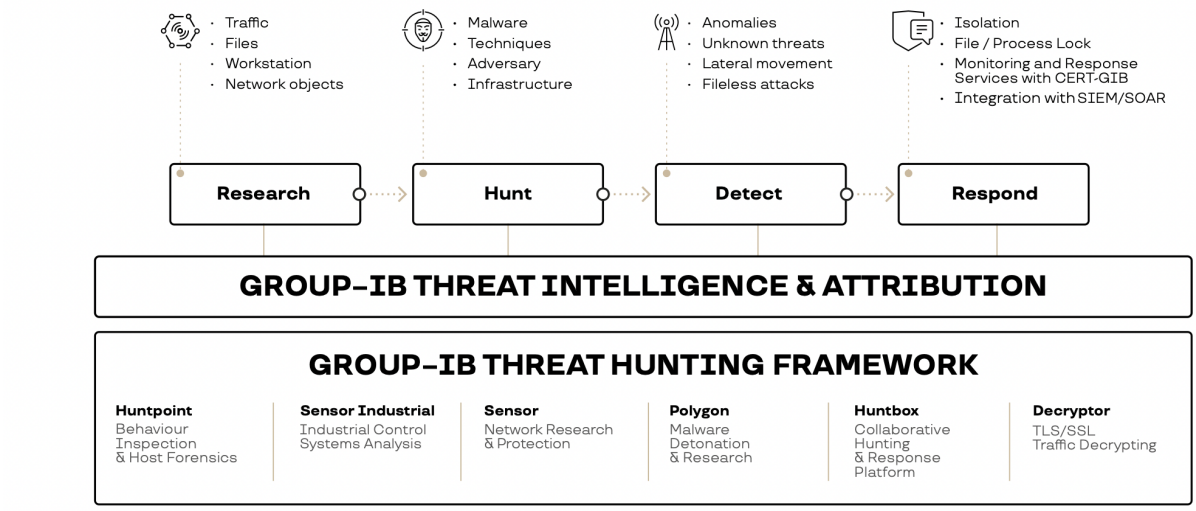
Threat Hunting Framework (THF) – Wykrywanie ataków ukierunkowanych i nieznanych zagrożeń w sposób skoncentrowany na przeciwniku. Proaktywne polowanie na lokalne i globalne zagrożenia. Własne, opatentowane technologie. Kompleksowa ochrona



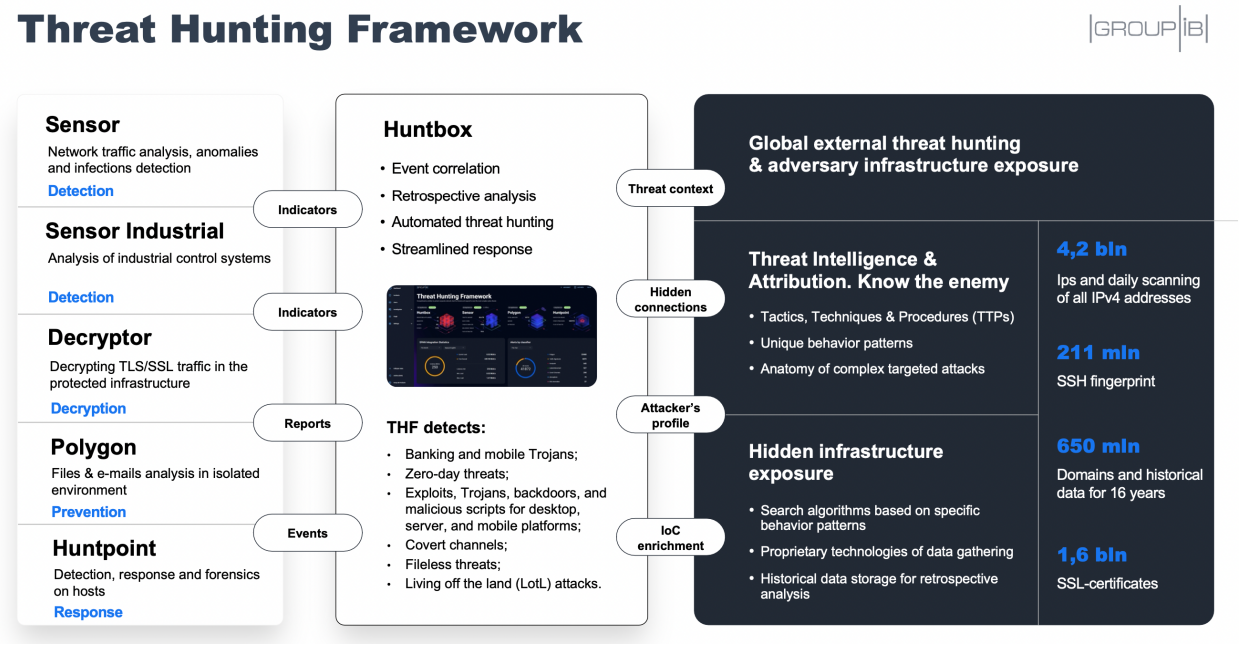
Threat Hunting Framework architecture



Funkcjonalność platformy Threat Hunting Framework

- Zarządzanie złożonymi incydentami poprzez wykrywanie anomalii oraz ukrytych kanałów komunikacji. Analiza behawioralna oprogramowania i użytkowników oraz korelacja zdarzeń.
- Detonacja i analiza złośliwego oprogramowania - opatentowana własna technologia przeprowadza dynamiczną analizę złośliwego oprogramowania na maszynach wirtualnych, a także w pełni wykonuje złośliwy kod i wyodrębnia incydenty tzw. IoC.

- Proaktywne wyszukiwanie zagrożeń poprzez analizę hostów i ruchu sieciowego w obrębie i poza obrębem sieci organizacji (analizując jednocześnie infrastrukturę i techniki potencjalnych atakujących).
- Dostęp do pełnej informacji o zagrożeniach dzięki portalowi „Threat Intelligence& Attribution", który umożliwia przypisywanie rozproszonych zdarzeń do konkretnych typów i rodzin złośliwego oprogramowania lub określonych grup cyberprzestępców w celu zrozumienia procesu ataku i jego skutecznego zakończenia.
- Automatyzacja i wydajność - automatyczne badanie incydentów oszczędza czas na rutynowe zadania uwalniając niezbędne zasoby do analizy prawdziwych incydentów
- Precyzja rozwiązania - niski wskaźnik fałszywych alertów umożliwia skupienie się na realnych incydentach i zapobiega zatrzymaniu ważnych procesów biznesowych.
- Współpraca z ekspertami - ekosystem Group-IB zapewnia współdzielone środowisko, zdalne reagowanie na incydenty, cyfrową kryminalistykę oraz dostęp do analityków i społeczności.
- Ujednolicone rozwiązanie bezpieczeństwa dla IT i OT - system zawiera wszystkie niezbędne narzędzia do adaptacyjnej automatyzacji wyszukiwania zagrożeń i działań umożliwiających ich efektywne usunięcie.
- Integracja - dostosowanie do szybkiej współpracy z systemami typu SIEM



Huntbox

Zarządza infrastrukturą detekcji; wykonuje automatyczną analizę, korelację zdarzeń i proaktywne wykrywanie zagrożeń. Huntbox jest platformą, która dostarcza zestaw narzędzi do monitorowania, reagowania na incydenty oraz wykrywania zagrożeń w obrębie chronionej infrastruktury oraz w Internecie.

Sensor

Analizuje ruch sieciowy i wykrywa zagrożenia na poziomie sieci. Integruje się z podsystemami firmy.

Sensor OT Czujnik przemysłowy
Analizuje protokoły sieci przemysłowych w celu zapewnienia ochrony przed ukierunkowanymi atakami na sieci technologiczne oraz monitoruje integralność przemysłowego systemu sterowania.
Polygon
Detonuje złośliwe oprogramowanie (w postaci załączników e-mail, plików i linków z treścią) w izolowanym środowisku w celu przeprowadzenia analizy behawioralnej
Huntpoint
Rozwiązanie typu EDR. Chroni stacje robocze przed zaawansowanymi atakami umożliwiając jednocześnie sprawdzanie i zbieranie danych istotnych z punktu widzenia analizy śledczej.
Decryptor
Deszyfruje ruch TLS/SSL w chronionej infrastrukturze.
CERT-GIB
Usługa bezpieczeństwa zarządzana dla rozwiązań Group-IB przez analityków ds. cyberbezpieczeństwa i złośliwego oprogramowania. CERT-GIB jest autoryzowany przez Carnegie Mellon University i jest członkiem FIRST, Trusted Introducer oraz IMPACT.

Funkcje bezpieczeństwa informacji objęte THF

- Ochrona firmowej poczty elektronicznej przed ukierunkowanym phishingiem i mailami zawierającymi złośliwe oprogramowanie
- Ochrona sieci, usług i stacji roboczych użytkowników przed oprogramowaniem ransomware, trojanami, wirusami, keyloggerami i programami szpiegującymi
- Ochrona infrastruktury przed kontrolą przez zewnętrznych napastników
- Zabezpiecza transfer plików z niezaufanych do zaufanych magazynów plików
- Przeprowadza analizę złośliwego oprogramowania
- Wykorzystuje API do ochrony systemu klienta przed złośliwym oprogramowaniem
- Chroni stacje robocze i serwery przed potencjalnie niechcianymi aplikacjami i niezaufanymi urządzeniami
- Gromadzi dane kryminalistyczne na potrzeby dochodzeń
- Proaktywne wykrywanie zagrożeń
- Zdalne reagowanie na incydenty
- Identyfikuje i bada infrastrukturę napastników w celu przewidywania nowych ataków
- Odtwarza pełną linię czasu ataku
- Kontrola artefaktów przesyłanych za pośrednictwem zaszyfrowanego ruchu sieciowego
- Kontrola zaszyfrowany ruchu sieciowego
- Ochrona sieci technologicznych OT przed nieuprawnionymi urządzeniami do transferu danych
- Ochrona sieci technologicznych OT przed modyfikacjami sterowników PLC
- Ochrona sieci technologicznych OT przed manipulacjami technicznych funkcji protokołów sieciowych
- Zabezpiecza sieci technologiczne przed zniszczeniem urządzeń