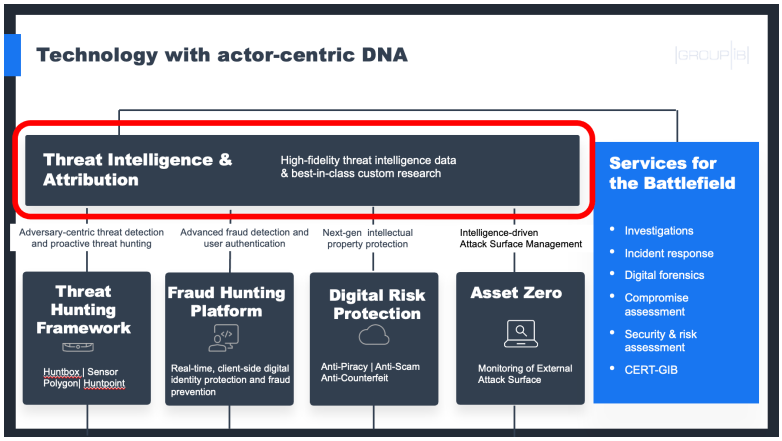
THREAT INTELLIGENCE & ATTRIBUTION System analizy i atrybucji cyberataków, proaktywnego wykrywania zagrożeń oraz ochrony infrastruktury sieciowej w oparciu o dane dotyczące taktyki, narzędzi i działań przeciwnika.



Możliwości platformy TI&A

Wykrywa i powstrzymuje ataki Zapobiega szkodom wyrządzanym firmie przez zagrożenia, które nie są wykrywane przez tradycyjne narzędzia bezpieczeństwa

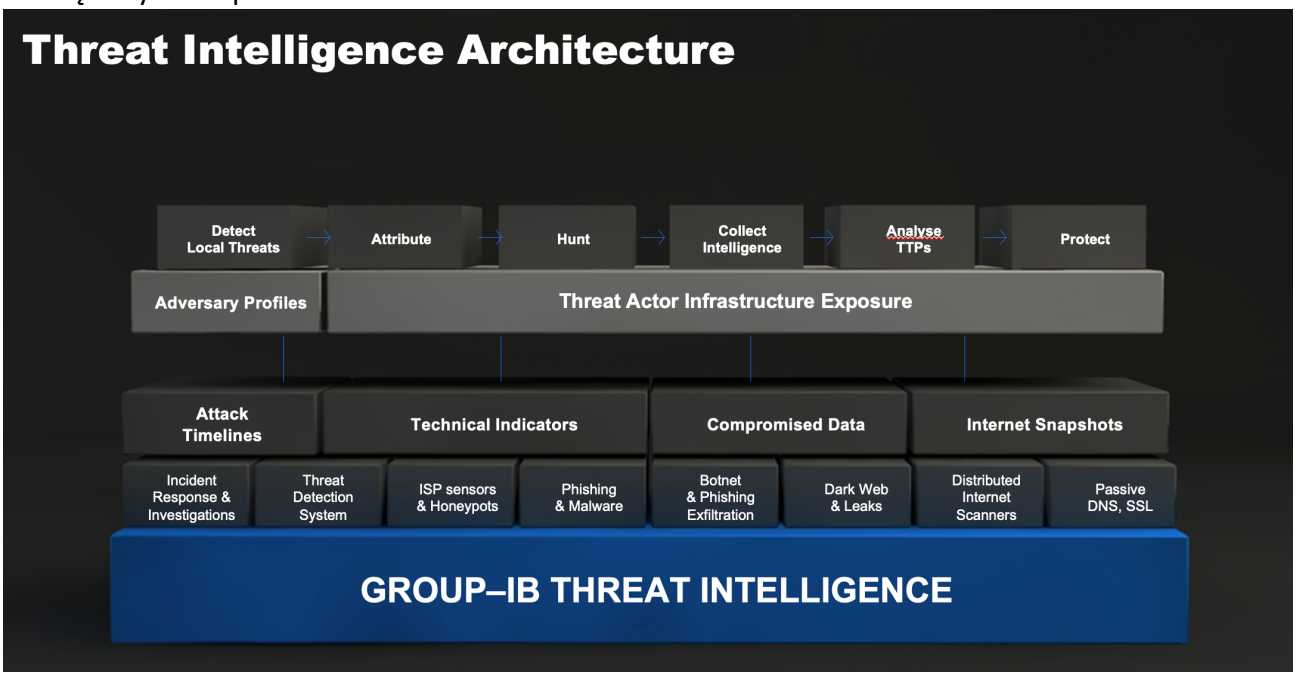
Identyfikuje i blokuje strony phishingowe Powstrzymuje aktorów zagrażających firmie lub klientom poprzez nadużywanie marki

Zna metody działania zaawansowanych grup hakerskich Określa, czy chroniona infrastruktura może przeciwdziałać odpowiednim TTP

Analizuje i przypisuje zagrożenia Uzupełnia i wzbogaca o unikalne dane wskaźniki uzyskane z innych systemów

Wykrywa insiderów lub przecieki Uzyskuje z zamkniętych źródeł informacje o możliwym naruszeniu danych lub aktywności osób z wewnątrz działających na szkodę organizacji

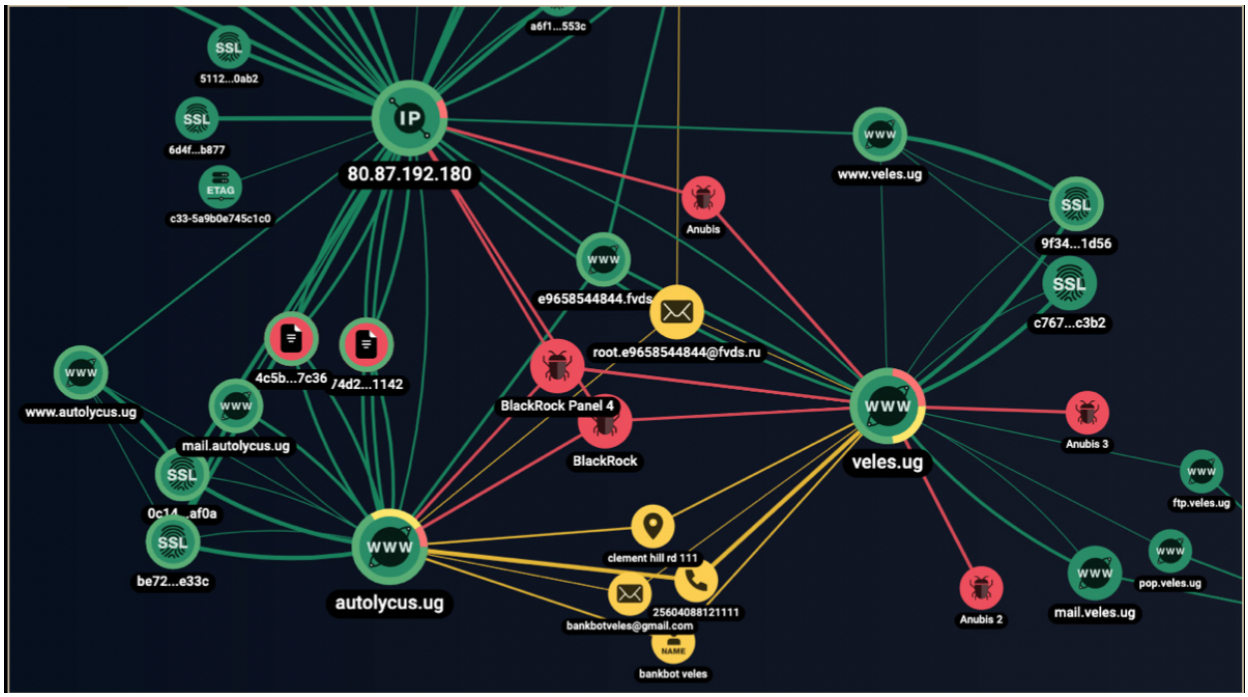
Wzmacnia i usprawnia Twój zespół Zwiększa efektywność o 30%, redukuje koszty i angażuje zewnętrznych ekspertów



Główne cechy

- Tworzenie i zarządzanie spersonalizowanym interfejsem do wizualizacji zagrożeń i ataków
- Zaawansowane profilowanie uczestników zagrożeń, w tym cyberprzestępców i grup hakerskich
- Dostęp do unikalnych zestawów danych i szerokiego zakresu zamkniętych źródeł
- Dostosowane i spersonalizowane dane dla każdej konkretnej firmy i branży
- Ekstrakcja i odzyskiwanie danych firmowych po ataku phishingowym lub złośliwym oprogramowaniu
- Gotowa integracja z systemami SIEM, TIP i innymi poprzez API/STIX

Wykorzystaj potężne narzędzia analityczne TI&A



Największa baza danych dark web Zbieranie wiadomości i analiza profili napastników.

Platforma wykrywania złośliwego oprogramowania Detonowanie i analiza złośliwego oprogramowania i złośliwych linków w środowisku wirtualnym, dostosowywanym do potrzeb każdego klienta.

Zautomatyzowana analiza wykresów Korelacja i badanie zdarzeń; wskaźniki parametry usprawniające aktywne polowanie na zagrożenia oraz ich atrybucja dzięki wiodącej technologii.

Źródła danych i unikalne cechy Niezrównany pakiet rozwiązań, który wyszukuje, ekstrahuje, gromadzi i analizuje dane, z których 90% znajduje się w zamkniętych źródłach.
Analitycy (Human Intelligence) Aktywność hakerów, TTP, dochodzenia IR, raporty, DarkWeb
System (Data intelligence) C&C analiza śledcza, skompromitowane dane kart, skompromitowane konta, wykorzystanie komputerów tzw. mules.
Wywiad w zakresie szkodliwego oprogramowania Analiza szkodliwego oprogramowania, zasoby phishingowe, urządzenia, wycieki danych

Wywiad w zakresie otwartego oprogramowania Media społecznościowe, repozytoria kodu, kontekst, haktywizm itp.

Najważniejsze informacje

- Własne narzędzia analityczne + Big Data + Machine Learning
- Najwyższej klasy własne środowisko wirtualne typu sandbox (detonacja złośliwego oprogramowania)
- Network Graph (wizualizacja i wyszukiwanie zagrożeń)
- Monitorowanie i usuwanie nadużyć związanych z marką Digital Risk Protection
- Łatwa integracja poprzez API/STIX/TAXII
- Szybkie wsparcie techniczne 24/365