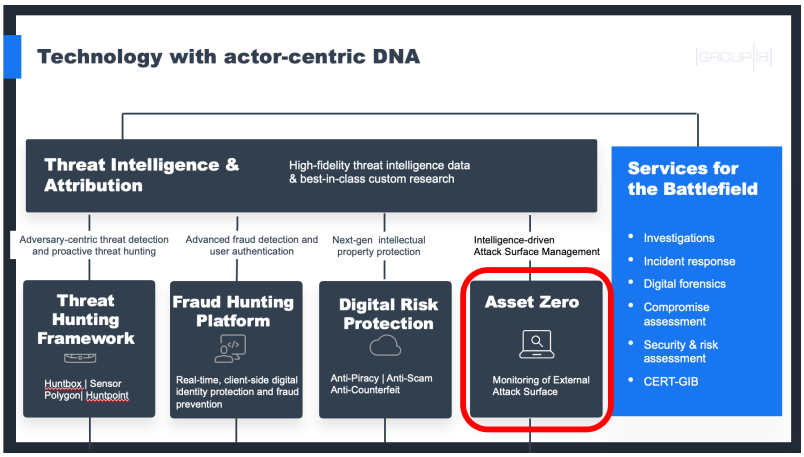
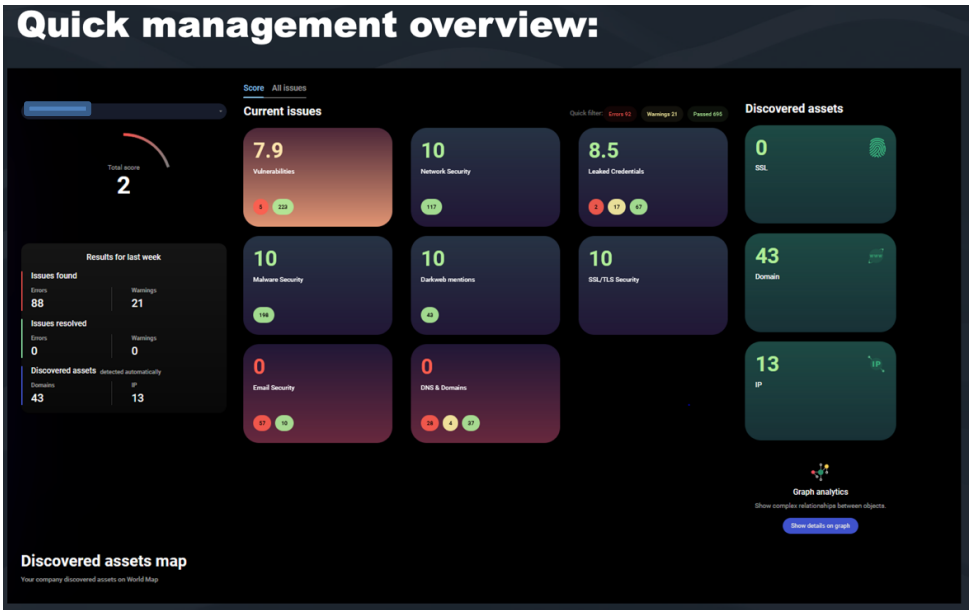
Asset Zero – Ochrona zasobów firmy, czyli organizacja widziana z perspektywy hakerów



AssetZero jest kompleksowym, opartym na inteligencji rozwiązaniem SaaS, zaprojektowanym w celu oceny i pomocy w zarządzaniu powierzchnią ataku. Narzędzie zapewnia pełny wgląd w zasoby komunikujące się z otoczeniem zewnętrznym, identyfikując te, które mogą być potencjalnymi wektorami ataku oraz dając możliwość podjęcia działań w kierunku ograniczenia ryzyka i naprawy podatności

Zarządzanie zadaniami realizowane jest dzięki przejrzystemu i łatwemu w użyciu interfejsowi użytkownika.



AssetZero to prosta i elegancka platforma, realizująca ważne zadania, mające na celu ochronę każdej firmy w dowolnej branży przed niepożądanymi naruszeniami: od dużych korporacji, które mają najszersze i najmniej wyraźnie zdefiniowane powierzchnie ataku (a także najwięcej do stracenia), po mniejsze firmy z ograniczonymi zasobami, które często mają trudności z efektywnym zarządzaniem i śledzeniem swojej infrastruktury IT.

AssetZero wykorzystuje informacje o głównej domenie organizacji, aby zidentyfikować jej zasoby w sieci. System skanuje całą przestrzeń IPv4, zapewniając, że żaden krytyczny zasób nie zostanie pominięty.

Zbierane dane obejmują:

- Adresy IP
- Nazwy domen
- Certyfikaty SSl/TlS
- Zasoby chmurowe
- Oprogramowanie publiczne

System testuje każdy zasób (powiązany z główną domeną) narażony na zewnętrzny atak, aby określić, czy należy on do jednej z następujących ośmiu kategorii:

- podatności
- bezpieczeństwo sieci
- wyciek danych uwierzytelniających
- bezpieczeństwo złośliwego oprogramowania
- wzmianki o ciemnej sieci
- Bezpieczeństwo SSl/TlS
- Bezpieczeństwo poczty elektronicznej
- DnS i domeny

System wzbogaca wszystkie zidentyfikowane zasoby i potencjalne problemy o bogaty kontekst pochodzący z Group-IB Threat Intelligence & Attribution. Pozwala to na efektywną priorytetyzację zagrożeń i określenie potencjalnego ryzyka biznesowego oraz pomaga zrozumieć, czy wykryta luka lub technika ataku jest obecnie wykorzystywana.

Alerty mogą mieć jeden z trzech rezultatów:
- Błąd: Krytyczny problem, który wymaga natychmiastowego działania
- Ostrzeżenie: Potencjalny problem, który wymaga dalszej analizy
- Zaliczony: nie wykryto żadnego problemu

Wszystkie alerty mogą być dostarczane za pomocą interfejsu użytkownika, poprzez natywne funkcje współdzielenia zgłoszeń i alertów lub poprzez API w ramach integracji z systemami zgłoszeń, SIEM, SOAR i innymi zestawami narzędzi, aby umożliwić efektywne zarządzanie i remediację. Alerty zawierają również rekomendacje dotyczące rodzaju zagrożenia i zalecanych procedur zaradczych.
System codziennie monitoruje wszystkie zmiany zasobów zewnętrznej powierzchni ataku, aby zapewnić dynamiczną informację na temat aktualnego stanu bezpieczeństwa.
Jeśli zostaną zidentyfikowane nowe zagrożenia, system natychmiast generuje nowy wynik i odpowiedni alert.