LABYRINTH
Developed to stop advanced threats

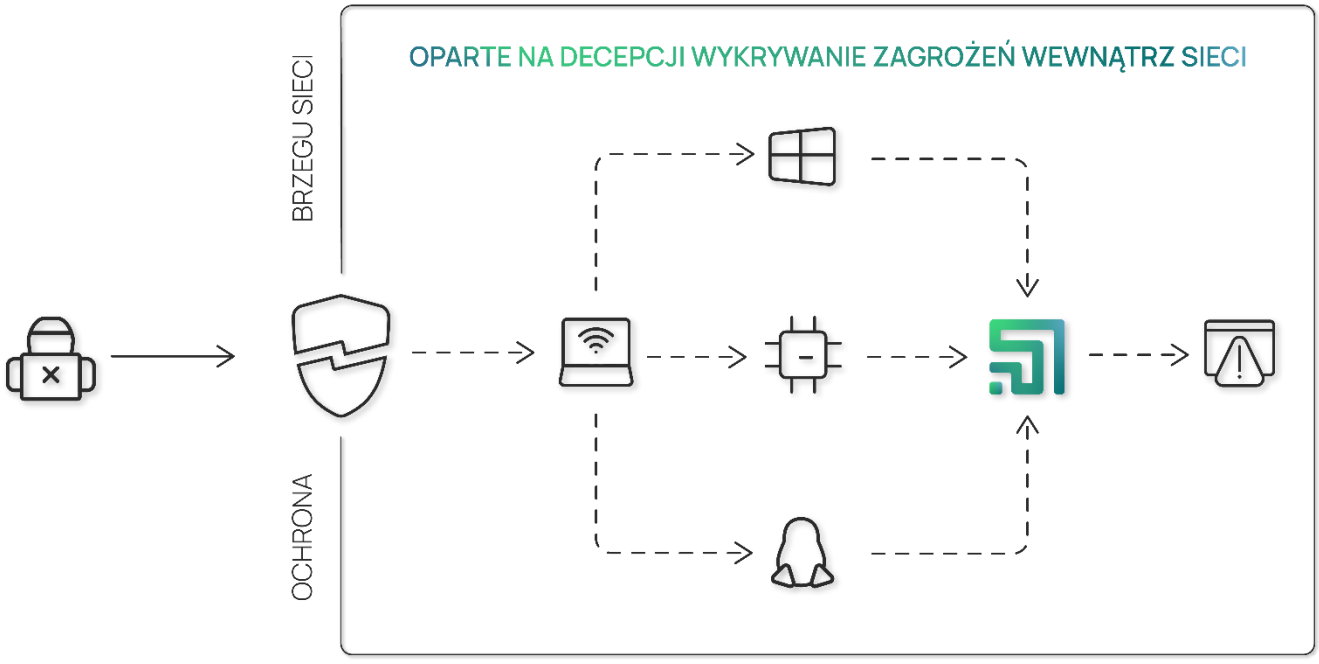
Opis rozwiązania

Labyrinth Deception Platform, 2023

Labyrinth to oparta na decepcji technologia wykrywania zagrożeń, która identyfikuje i blokuje cyberataki w sieci firmowej. Nasze rozwiązanie, oparte na unikalnych technologiach wykrywania zagrożeń, proaktywnie chroni sieci IT / IoT / OT przed ukierunkowanymi atakami, zaawansowanymi i nieznanymi zagrożeniami, botnetami, atakami zero-day i złośliwymi atakami wewnętrznymi.

Platforma zapewnia proste i wydajne narzędzie do jak najwcześniejszego wykrywania intruzów wewnątrz sieci korporacyjnej. Łatwo wdrażana w wirtualnych, fizycznych lub hybrydowych środowiskach IT, wykrywa zagrożenia bez ciągłego monitorowania i generowania nadmiernej ilości danych.

Platforma zapewnia pełną oś czasu ataku z korelacją zdarzeń w celu podejmowania trafniejszych i szybszych decyzji. Labyrinth daje ci pewność, że twoje cenne dane pozostaną chronione przed zagrożeniami, które ominęły korporacyjne zapory sieciowe.



KLUCZOWE MOŻLIWOŚCI

W dziedzinie cyberbezpieczeństwa istnieje dobrze znana asymetria między atakiem a obroną: obrońcy muszą mieć rację w 100% przypadków, a atakujący muszą mieć szczęście tylko raz, aby odnieść sukces.
Platforma decepcji Labyrinth to ofensywna technologia wykrywania, która zmienia równowagę sił na korzyść obrońców. Platforma eliminuje zdolność przeciwnika do rozpoznania sieci, zapobiegając w ten sposób ruchowi bocznemu (wewnątrz sieci korporacyjnej).

WCZESNE WYKRYWANIE ZAGROŻEŃ W SIECI

Labyrinth wykrywa wszelkie ukierunkowane, podejrzane działania na wczesnym etapie ataku. Punkty Labyrinth (wabiki sieciowe) są zaprojektowane tak, aby wychwytywać działania zagrożeń, gdy atakujący próbuje zrozumieć sieć i znaleźć swój cel. Gdy atakujący zaatakuje Punkt, Labyrinth gromadzi wszystkie szczegóły na jego temat: źródła zagrożenia, użyte narzędzia i wykorzystane luki w zabezpieczeniach. Jednocześnie wszystkie rzeczywiste zasoby i usługi działają bez żadnych zakłóceń.

PRECYZYJNE POWIADOMIENIA

Labyrinth wspiera zespoły ds. bezpieczeństwa (SOC) dzięki wysoce niezawodnym alertom, z mniej niż 1% fałszywych alarmów. Z natury Punkty Labyrinth są ciche, dopóki nie zostaną dotknięte. Nikt nie powinien się z nimi kontaktować, więc każda interakcja z punktem jest wyjątkowo podejrzana. Odróżnia to Labyrinth od rozwiązań bezpieczeństwa, które mają na celu analizę wszystkich działań w sieci i wytwarzają dużo cyfrowego "szumu".

SZYBKIE REAGOWANIE NA INCYDENTY

Labyrinth zapewnia inteligentne narzędzie analityczne do badania incydentów i identyfikacji zagrożeń. Wszystkie zebrane zdarzenia są wzbogacane o niezbędne dane bezpieczeństwa z platformy reagowania na incydenty.
Wskaźniki naruszeń (IoC) generowane przez Labyrinth są automatycznie synchronizowane z rozwiązaniami firm trzecich w celu zapobiegania atakom. Pozwala to na natychmiastowe podjęcie działań w przypadku ataku: zrozumienie go, przeprowadzenie analizy kryminalistycznej, pewną reakcję i opracowanie lepszej obrony na przyszłość.

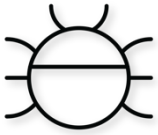
PROAKTYWNA OBRONA

Większość technologii wykrywania zatrzymuje atak po jego wykryciu i nie daje szansy na jego zbadanie. Labyrinth pozwala dowiedzieć się więcej o naturze ataku i lepiej zrozumieć narzędzia i techniki stosowane przez atakujących. Rozwiązanie generuje i instaluje na hostach (stacjach i serwerach) artefakty (fałszywe dane), których celem jest zaangażowanie atakujących z pomocą kuszącego wabika. Zamiast czekać, jaki będzie następny krok atakującego, artefakty kierują go do odizolowanego środowiska, które należy obserwować.

WYKRYWANIE ATAKÓW UKIERUNKOWANYCH

Aby skutecznie przeciwdziałać ukierunkowanym atakom, kluczowe jest zrozumienie technik, narzędzi i celów atakujących.
Platforma decepcji Labyrinth wprawia hakerów lub złośliwych intruzów wewnętrznych w fałszywe poczucie bezpieczeństwa i pozwala poznać ich umiejętności i motywy. Świadomość tego, co atakujący wiedzą o sieciach firmowych, aplikacjach i pracownikach, pomaga stworzyć dokładniejsze profile napastników i zastosować najlepszy, możliwy sposób obrony przed nimi. Ujawnia również słabości korporacyjnych systemów obronnych, które mogą zostać wykorzystane przez napastników w przyszłości.

WYKRYWANIE PO INFEKCJI

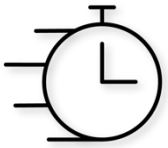


Platforma decepcji Labyrinth zaimplementowana w sieciach firmowych może służyć jako wysoce niezawodny system ostrzegania o atakach, które ominęły zabezpieczenia brzegu sieci.
Agenty Seeder, rozmieszczone na serwerach i stacjach roboczych, imitują najbardziej „smaczne" dla atakującego artefakty. To, co wydaje się być kontem administratora o wysokich uprawnieniach i źle chronionym, jest pułapką, która zwabia atakującego do systemu Labyrinth. Można wtedy monitorować działania atakujących związane z interakcją z Punktami (wabikami systemu), zbierając cenne informacje na temat zagrożeń, które przedostały się przez inne zabezpieczenia sieci firmowej.

ROZPOZNAWANIE RUCHU WEWNĘTRZNEGO

W fazie ruchu bocznego atakujący przemieszcza się w sieci firmowej z jednego zasobu do drugiego. Platforma decepcji Labyrinth została zaprojektowana do wykrywania wczesnego rekonesansu, kradzieży danych uwierzytelniających i ruchu wewnętrznego.
Pozwala firmom uzyskać widoczność takich zagrożeń na ich wczesnym etapie, co jest skomplikowanym zadaniem dla tradycyjnych rozwiązań ochronnych. Labyrinth kieruje następnym krokiem w ataku na ekosystem decepcji i natychmiast ujawnia atakującego.

REDUKCJA CZASU PRZEBYWANIA



Mechanizm wykrywania platformy Labyrinth jest szczególnie skuteczny w zmniejszaniu czasu przebywania (tzw. dwell time), czyli czasu, w którym atakujący pozostaje niezauważony w sieci korporacyjnej. Długi czas przebywania jest kluczowym warunkiem skutecznego przeprowadzenia ataku przez napastnika. Labyrinth skraca czas trwania ataków poprzez konfigurowanie honeypotów, wabików i artefaktów dla atakujących. Platforma decepcji Labyrinth skraca czas i zdolność atakujących do poruszania się w sieciach firmowych i zatrzymuje ich, zanim dotrą do krytycznych zasobów i usług.

KORZYŚCI BIZNESOWE

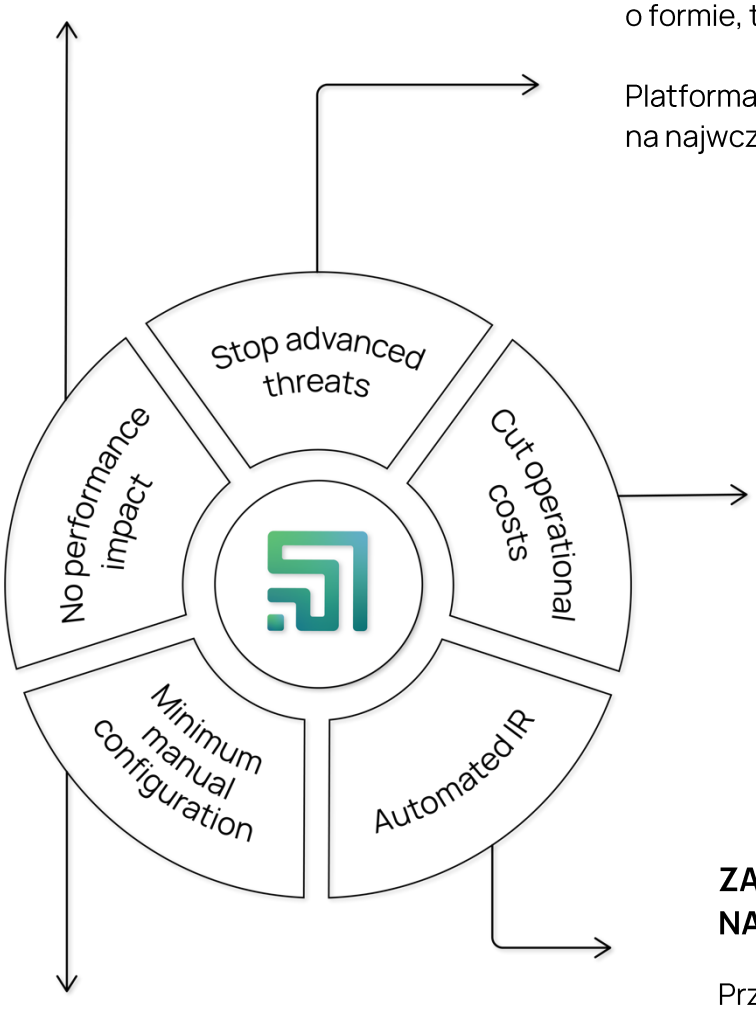
BRAK WPŁYWU NA WYDAJNOŚĆ

Brak negatywnego wpływu na wydajność urządzeń sieciowych, hostów, serwerów lub aplikacji.

POWSTRZYMYWANIE ZAAWANSOWANYCH ZAGROŻEŃ

Wykrywa ukierunkowane i zaawansowane ataki nie wymagając żadnej wcześniejszej wiedzy o formie, typie lub zachowaniu zagrożenia.

Platforma wykrywa znane i nieznane zagrożenia na najwcześniejszym etapie cyklu życia ataku.



REDUKCJA KOSZTÓW OPERACYJNYCH

Nie gromadzi dużych ilości danych, nie generuje fałszywych alarmów, nie wymaga specjalnych umiejętności do obsługi.

Łatwo wdraża się do istniejącej infrastruktury bezpieczeństwa i nie generuje fałszywych alarmów.

ZAUTOMATYZOWANE REAGOWANIE NA INCYDENTY

Przyspiesza reagowanie na incydenty dzięki integracjom z rozwiązaniami innych firm, które automatyzują izolację, blokowanie i wyszukiwanie zagrożeń (threat hunting).

MINIMALNA KONFIGURACJA RĘCZNA

Szybkie i proste wdrożenie bez konfliktów systemowych i minimalna konserwacja systemu: brak baz danych, podpisów lub regułdo konfiguracji i aktualizacji.

WSPARCIE TECHNICZNE 12/7

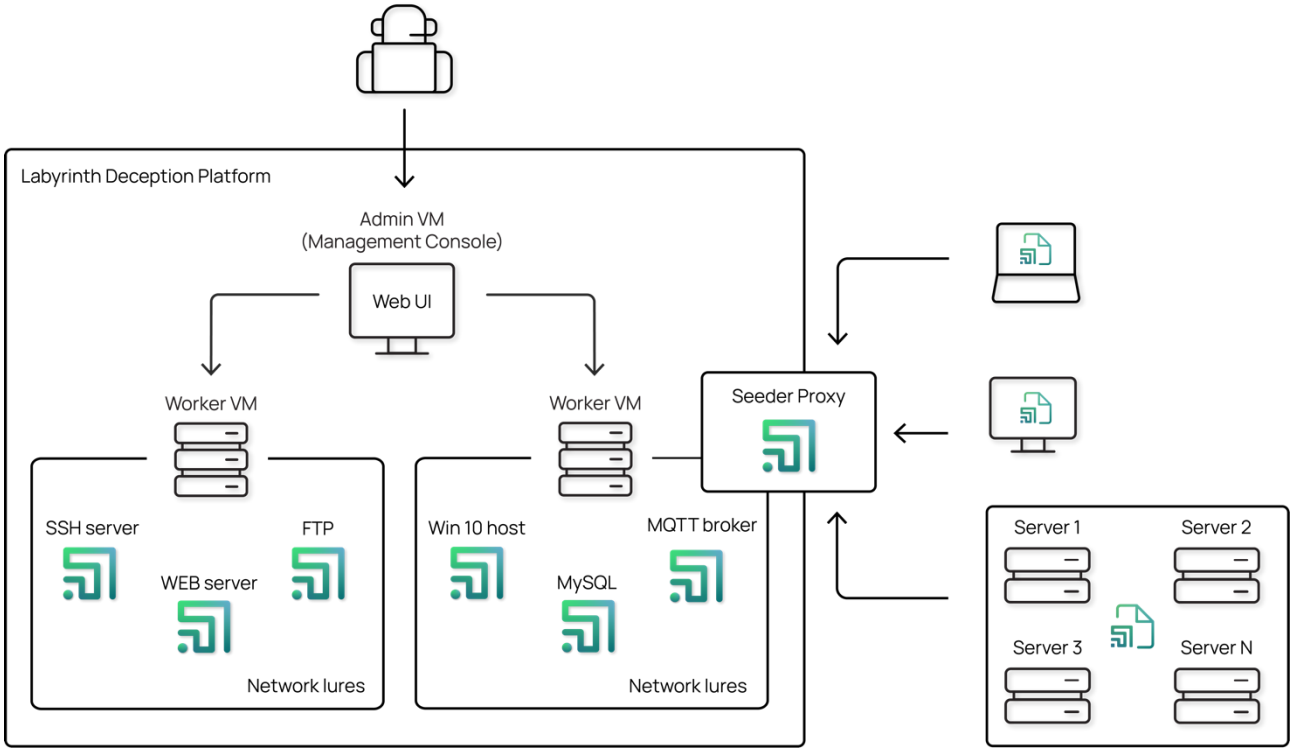
Prawo do aktualizacji, utrzymanie oprogramowania i wsparcie techniczne 12/7 (GMT+2) w cenie subskrypcji.

ARCHITEKTURA PLATFORMY

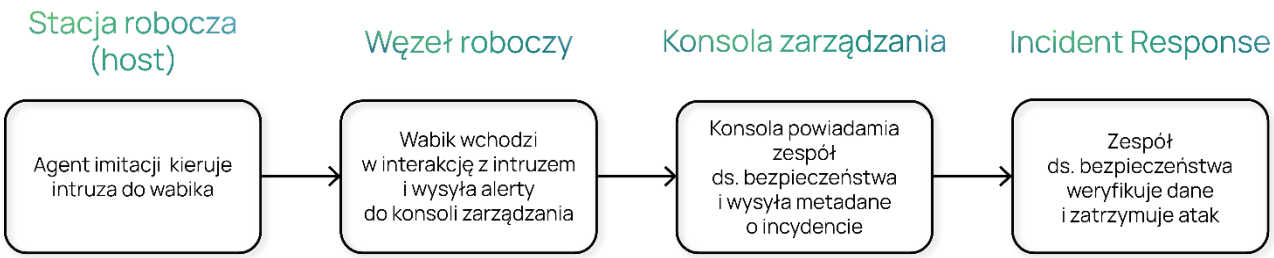
Platforma decepcji Labyrinth automatycznie wdraża sieci imitacji (tzw. Honeynets) na podstawie informacji o środowisku sieciowym i używanych urządzeniach. Wabiki mogą być również wdrażane ręcznie za pośrednictwem konsoli zarządzania.

Daje to firmom potężne narzędzie do rozwijania własnej unikalnej platformy decepcji w oparciu o ich specjalne potrzeby i najlepsze globalne praktyki.

Platforma zapewnia przeciwnikom iluzję słabych punktów usług IT i aplikacji, elementów infrastruktury OT lub IoT, prowokuje ich do działania, wykrywa i monitoruje wszystkie ich działania oraz izoluje ich od prawdziwych sieci IT / OT.



PRZEPŁYW ALERTÓW W RAMACH PLATFORMY



KLUCZOWE FUNKCJE

Platforma decepcji Labyrinth nie naśladuje rzeczywistej infrastruktury IT. Zamiast tego platforma zapewnia atakującym iluzję prawdziwych luk w zabezpieczeniach sieci IT. Zespół techniczny Labyrinth stale aktualizuje rozwiązanie o imitacje nowo odkrytych luk w zabezpieczeniach. Dzięki temu Labyrinth jest bardzo skutecznym narzędziem do wykrywania i reagowania na zaawansowane zagrożenia.

WABIKI O WYSOKIEJ INTERAKCJI

Platforma decepcji Labyrinth opiera się na Punktach - honeypotach o wysokim stopniu interakcji z inteligentnymi funkcjami. Punkty są identyczne z zasobami przedsiębiorstwa i uruchamiają prawdziwe systemy operacyjne, aplikacje i usługi z fałszywymi danymi.

Pozwalają one atakującemu zalogować się i odpowiedzieć na jego żądanie, aby zrozumieć jego intencje. Punkty wabią przez długi czas, obserwując napastników i zbierając cenne dane o ich narzędziach i technikach. Oprócz tego, Punkty tworzą lokalne wskaźniki naruszeń (IoC) i informacje o zagrożeniach do odczytu maszynowego (MRTI).

RÓŻNORODNOŚĆ I WIARYGODNOŚĆ WABIKÓW

Punkty odzwierciedlają luki w zabezpieczeniach sieci produkcyjnych, emulując rzeczywisty system operacyjny/jego obraz, usługi i aplikacje dla IoT, SCADA / OT / ICS, POS, środowisk sieciowych i telekomunikacyjnych. Fałszywe stacje robocze, serwery, urządzenia, aplikacje, usługi i protokoły wyglądają identycznie jak prawdziwe zasoby.

Punkty nie tylko emulują najbardziej atrakcyjne dla atakujących podatności, ale także zachowują się jak prawdziwe hosty. W zależności od typu, mogą wysyłać żądania transmisji, zmieniać adresy IP i łączyć się z witrynami z wiadomościami. Umożliwia to mieszanie wabików w środowisku produkcyjnym i odróżnianie ich od reszty zasobów, aby mogły zostać wybrane jako cel dla atakującego.

WIELOWARSTWOWA OCHRONA

Labyrinth wdraża pełny stos imitacji w celu zapewnienia najwyższego poziomu ochrony swoim klientom. Artefakty o niskim poziomie interakcji na pierwszej linii obrony emulują aplikacje w firmie i są wykorzystywane wyłącznie do podstawowego wykrywania zagrożeń.

Są łatwe do wykrycia i ominięcia oraz informują atakujących, że znajdują się na polu minowym. Odwraca to uwagę oportunistycznych atakujących i daje ukierunkowanym atakującym fałszywą pewność, że odkryli imitacje w sieci. W międzyczasie wabiki o wysokiej interakcji pozostają niezauważone i zapewniają wykrywanie zaawansowanych zagrożeń.

DOSTOSOWANIE POD POTRZEBY KLIENTA

Zespół Labyrinth zapewnia zaawansowane usługi rozwoju platformy Labyrinth w złożonych środowiskach lub dla specjalnych potrzeb branżowych, takich jak IoT, SCADA lub POS. Nasi specjaliści ds. cyberbezpieczeństwa nieustannie pracują nad znajdowaniem i ujawnianiem nowych zagrożeń. Po analizie opracowujemy nowe wabiki, aby zmylić aktywne zagrożenia.

Każda instalacja Labyrinth regularnie aktualizuje swoją mapę o nowe ścieżki i punkty, aby zapewnić najlepsze możliwości wykrywania zagrożeń. Aby wzmocnić obronę, gdy atak jest w toku, można dodać dodatkowe punkty lub zmienić ich typy.

AUTOMATYZACJA

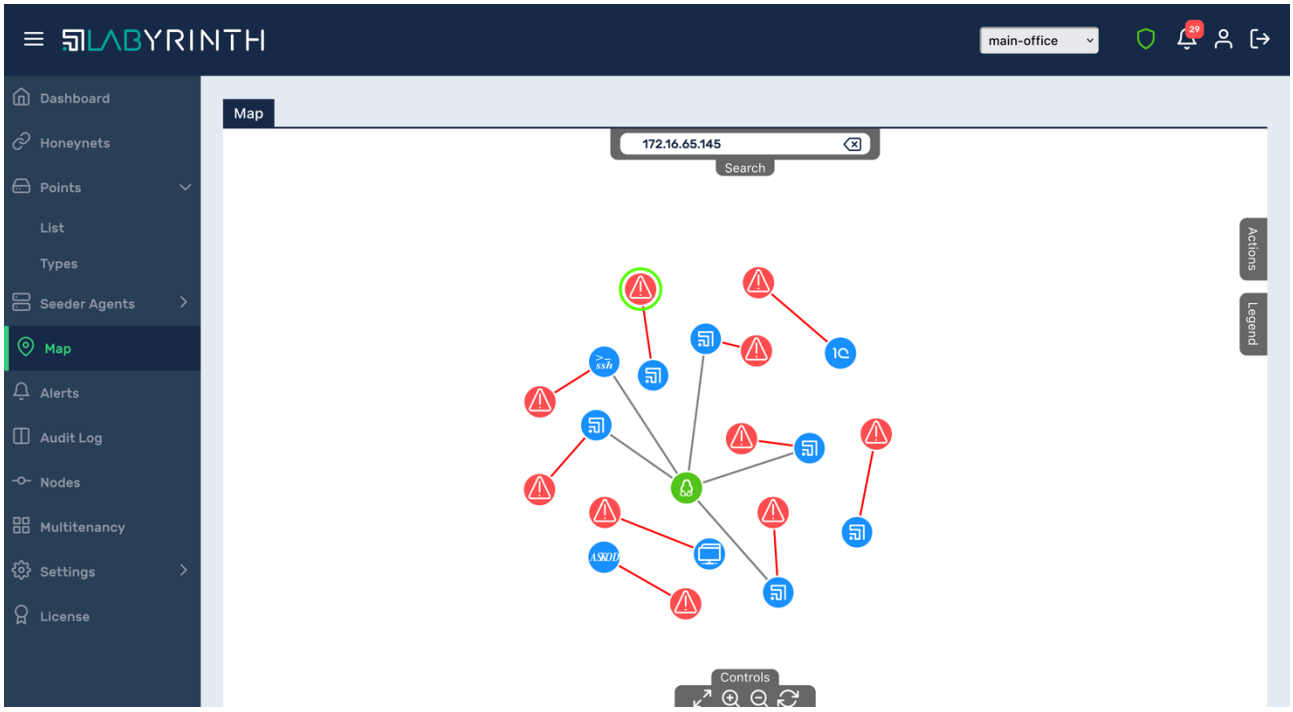
Platforma decepcji Labyrinth automatycznie identyfikuje hosty, usługi i ścieżki połączeń między nimi, aby usprawnić i dostosować tworzenie i wdrażanie wabików i pułapek.

Zaawansowane funkcje sieciowe umożliwiają dynamiczne tworzenie nowych ścieżek w Labyrinth i aktualizację punktów. Labyrinth zapewnia zautomatyzowane zarządzanie i okresowe odświeżanie punktów wdrożonych w środowisku produkcyjnym w celu zachowania ich autentyczności. Lekkie, zautomatyzowane i elastyczne rozwiązanie oszczędza czas i zapewnia wysoki poziom bezpieczeństwa od pierwszego dnia wdrożenia.

SKALOWALNOŚĆ

Labyrinth może być efektywnie skalowany w dużych, rozproszonych sieciach korporacyjnych. Każdy emulowany Punkt jest lekkim procesem działającym na maszynie wirtualnej. Dzięki temu skalowalność nie opiera się na zasobach obliczeniowych, ale na konstruowaniu i wdrażaniu kompleksowego zestawu wabików i pułapek w całym środowisku sieciowym.

Automatyczne tworzenie i wdrażanie Punktów pomaga firmom usprawnić proces skalowania i osiągnąć pełną ochronę wszystkich segmentów sieci.



Platforma decepcji Labyrinth zapewnia najskuteczniejsze narzędzie do wykrywania i powstrzymywania działań hakerów i sabotażystów wewnątrz sieci korporacyjnej.

Aby uzyskać więcej informacji na temat platformy decepcji Labyrinth lub demonstracji produktu, prosimy o kontakt pod adresem **info@labyrinth.tech**