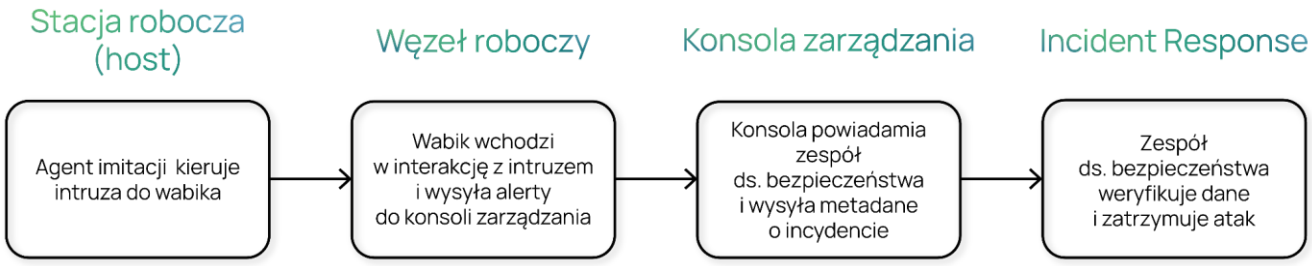
Platforma Labyrinth Deception imituje potencjalne cele cyberataku, zapewniając intruzom iluzję podatności infrastruktury. Każda część imitowanego środowiska odtwarza usługi i zawartość prawdziwego segmentu sieci IT/OT. Architektura rozwiązania opiera się na rozmieszczeniu różnych typów wabików na hostach, imitujących usługi sieciowe, aplikacje, routery, urządzenia IoT, itd. Wabiki wykrywają złośliwe działania wewnątrz sieci korporacyjnej, zapewniając kompleksowe monitorowanie wszystkich możliwych wektorów ataku.

Labyrinth prowokuje intruza do działań i wykrywa podejrzane aktywności. Podczas infiltracji podstawionej infrastruktury, platforma rejestruje wszystkie szczegóły działań intruza. Zespół ds. bezpieczeństwa otrzymuje informacje o źródłach zagrożenia, użytych narzędziach oraz o wykorzystanych podatnościach i zachowaniu intruza. W tym samym czasie produkcyjna infrastruktura sieciowa działa bez żadnych zakłóceń.

Labyrinth symuluje szeroki zakres rzeczywistych usług (poczta, aplikacje webowe, itp.). Dodatkowo system naśladuje łączność sieciową użytkownika oraz wszelkiego rodzaju wabiki (pliki, linki, klucze ssh, itp.), aby zwiększyć prawdopodobieństwo dostania się atakującego do symulowanych usług.

Do ochrony infrastruktury SCADA/OT opracowano nowe typy wabików, które mogą emulować interfejsy Web PLC oraz protokoły Siemens S7COMM, SNMP, Modbus. Dla ochrony IoT dodano imitację serwera MQTT.

PRZEPŁYW ALERTÓW W RAMACH PLATFORMY LABYRINTH



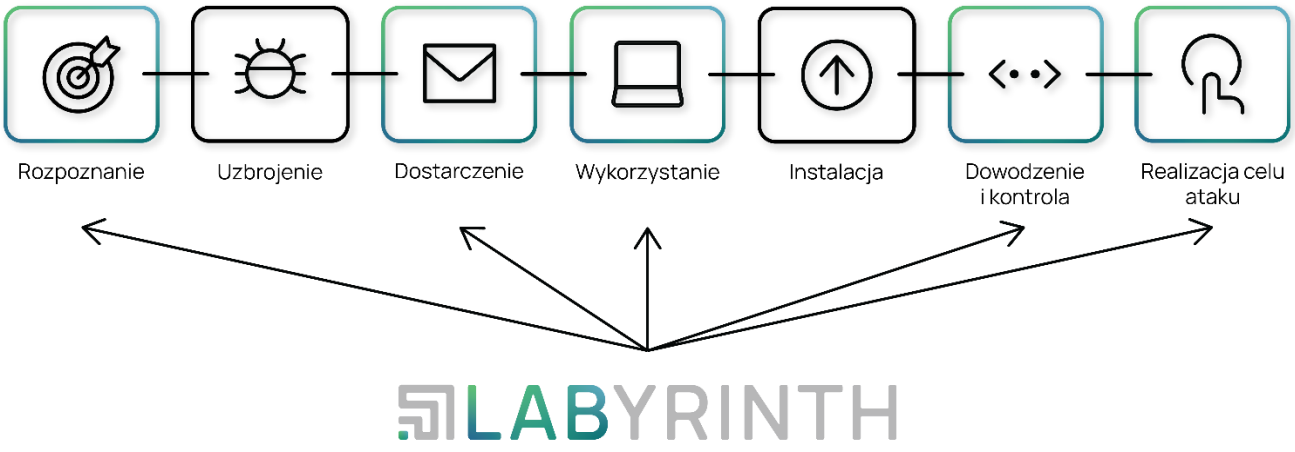
INTEGRACJE Z INNYMI ROZWIĄZANIAMI

Wykrywanie

Działania naprawcze

Reagowanie

ZASTOSOWANIE PLATFORMY



- Wczesne wykrywanie zagrożeń
- Ochrona proaktywna
- Wykrywanie ataków typu ATP
- Szybsze wykrywanie ataków

- Wykrywanie ataków Man-In-the Middle
- Wykrywanie ruchu pobocznego
- Szybka reakcja na incydenty
- Informatyka śledcza incydentów

ZAAWANSOWANE FUNKCJE

Rozszerzona integracja z systemami SIEM

Dwukierunkowa integracja z rozwiązaniami SIEM, która pozwala nie tylko przesyłać dane do SIEM, ale także odbierać od nich niezbędne informacje.

Zaawansowana ochrona aplikacji internetowych

Labyrinth zawiera unikalną technologię, która pozwala zapewnić dodatkowe zabezpieczenie dla najbardziej pożądanego przez hakerów celu – aplikacji i usług internetowych.

Multitenancy

Dostępny model wielu najemców i obsługa RBAC pozwalają na izolowanie i obsługę klientów z różnych organizacji w ramach jednej instalacji (podejście MSSP).

WYMAGANIA SYSTEMOWE

VMware vSphere 6.0/6.5/7.0, Microsoft Hyper-V 2008 R2 lub wyższy, Microsoft Azure Cloud.
Instalacja AdminVM na platformach opartych na KVM (Proxmox, OpenStack itp.) jest oficjalnie wspierana.

AdminVM (Konsola zarządzania)	4 vCPU (rdzenie), 32 GB RAM, 800 GB HDD
Worker Node (Węzeł roboczy)	8 vCPU (rdzeni), 24 GB RAM, 500 GB HDD

Szczegóły procesu instalacji opisane są w Deployment and Configuration Guide.