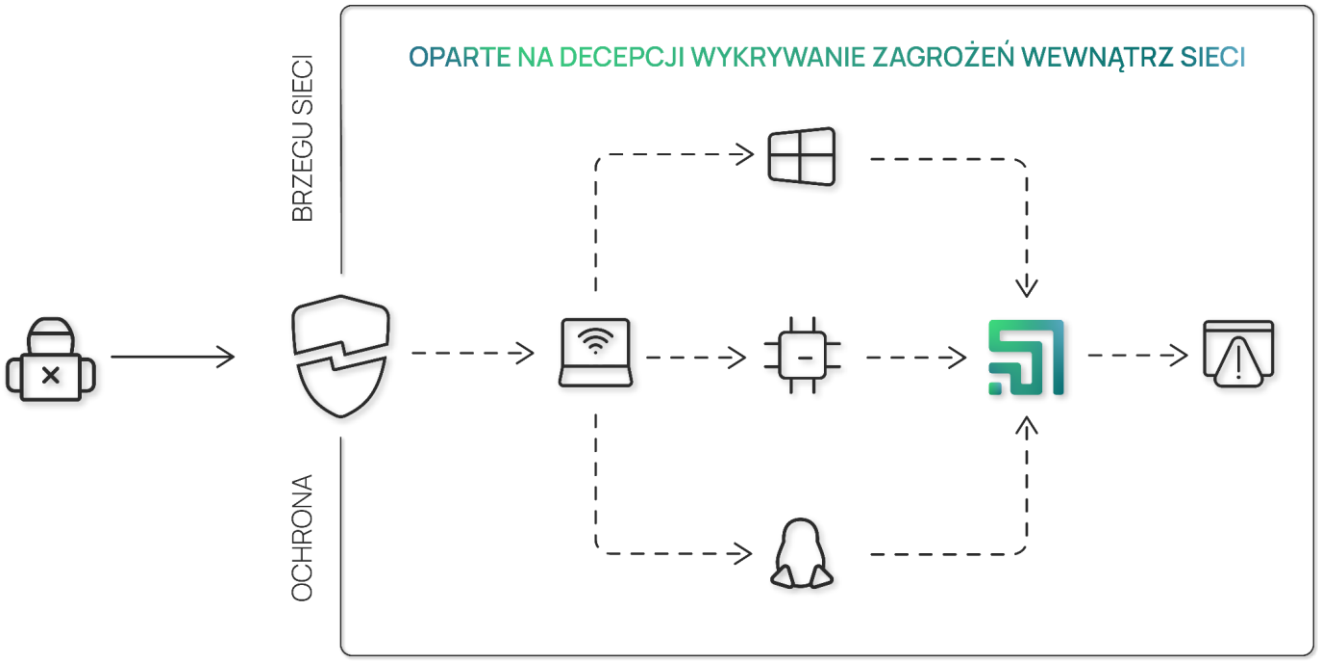
1. TECHNOLOGIA DECEPCJI

Cyberataki nie ustępują, ponieważ wyrafinowani napastnicy wciąż znajdują sposoby na przenikanie przez zabezpieczenia brzegowe. Z każdym naruszeniem, specjaliści ds. bezpieczeństwa stają w obliczu rosnącej presji, aby szybko wykryć i powstrzymać zagrożenia, zanim zostaną wyrządzone szkody. Oprócz oczekiwań związanych ze zgodnością, proponowane są nowe przepisy dotyczące powiadamiania o naruszeniach, które przewidują znaczne grzywny i potencjalną karę więzienia, jeśli oczekiwania dotyczące powiadomień nie zostaną spełnione.

Organizacje każdej wielkości i we wszystkich branżach poszukują innowacji, aby udoskonalić swoje modele bezpieczeństwa, zlikwidować luki w wykrywaniu, lepiej zrozumieć swoich przeciwników i być przygotowanym na przestrzeganie wymogów dotyczących śledzenia i ujawniania naruszeń. Organizacje zmieniają obecnie swoje strategie bezpieczeństwa z reaktywnego modelu bezpieczeństwa na podejście aktywnej obrony (active defense), które nie opiera się wyłącznie na reagowaniu na ataki, ale zamiast tego stosuje wczesne wykrywanie i szybką reakcję na zagrożenia.

Technologia decepcji (deception technology) zapewnia innowacje wymagane do niezakłóconej ewolucji do modelu bezpieczeństwa opartego na aktywnej obronie. Wdrażając strukturę wykrywania opartego na decepcji w całym stosie sieciowym, firmy są w stanie osiągnąć skuteczne wykrywanie dla każdego wektora zagrożeń i śledzić cykl życia ataku. Wykorzystując wabiki i przynęty o wysokim stopniu interakcji, decepcja przymusza napastników do ujawnienia się, co pozwala na wczesne ostrzeganie i identyfikuje luki w wykrywaniu zagrożeń, które ominęły inne zabezpieczenia.



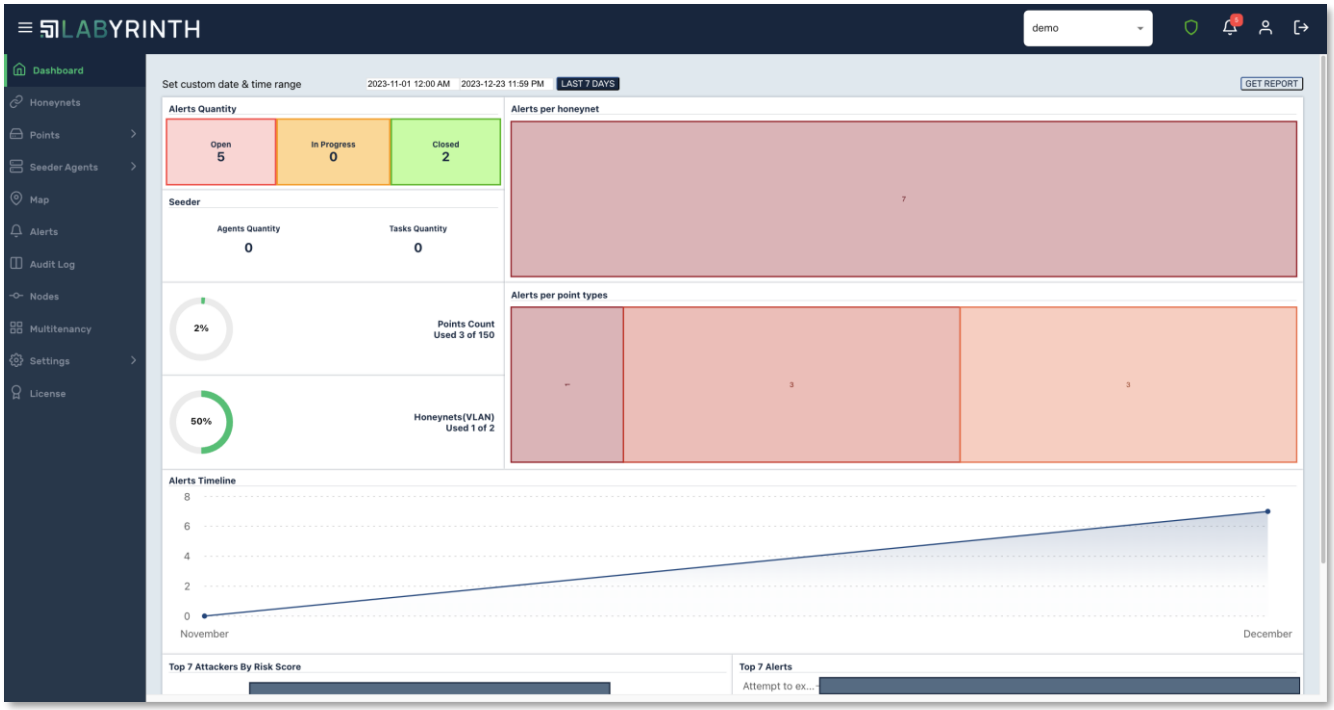
Dzięki widoczności w sieci zagrożeń na wczesnym etapie i alertom umożliwiającym podejmowanie działań w celu obsługi incydentów, rozwiązania typu „deception" szybko stają się preferowanym podejściem do proaktywnego wykrywania i reagowania na zagrożenia zewnętrzne, wewnętrzne i ze strony dostawców. Organizacje na wszystkich poziomach dojrzałości w zakresie bezpieczeństwa, agresywnie wdrażają technologie decepcji w celu ograniczenia ryzyka związanego z kradzieżą danych uwierzytelniających pracowników, eksfiltracją danych, oprogramowaniem ransomware, wydobywaniem kryptowalut i atakami mającymi na celu zakłócenie usług lub wpłynięcie na bezpieczeństwo publiczne. Dokładność i łatwość użycia technologii decepcji do wykrywania zagrożeń była głównym motorem jej przyjęcia i szerokiego zastosowania.

2. PLATFORMA DECEPCJI OD LABYRINTH

Rozwiązanie Labyrinth zapewnia atakującemu iluzję prawdziwych podatności infrastruktury. Podstawą rozwiązania są tzw. punkty (Points) - inteligentne imitacje (wabiki). Każda część środowiska imitującego odtwarza usługi i zawartość prawdziwego segmentu sieci IT / OT.

Labirynt prowokuje napastnika do działania i jednocześnie uczy się podejrzanej aktywności. Nasi doświadczeni specjaliści pomagają skonstruować najlepszy „labirynt" dla złożonych środowisk. Jego funkcje zapewniają potężne możliwości wykrywania ataków ukierunkowanych, sieci BOTNET, ataków typu 0-day i złośliwych użytkowników wewnętrznych..

Punkty naśladują specjalne usługi oprogramowania, treści, routery, urządzenia IoT, itp. Każdy punkt wykrywa wszystkie ukierunkowane i podejrzane działania. Podczas, gdy napastnik przechodzi przez fałszywą infrastrukturę swojego celu ataku, platforma Labyrinth przechwytuje wszystkie szczegóły dotyczące wroga. Firma otrzymuje informacje o źródłach zagrożenia, narzędziach, które zostały użyte, a także o wykorzystanych podatnościach i zachowaniu atakującego. W międzyczasie cała prawdziwa infrastruktura kontynuuje pracę bez żadnego wpływu na jej wydajność.



3. KORZYŚCI DLA KLIENTÓW I ZASTOSOWANIE

KORZYŚCI:	PRZYKŁADY ZASTOSOWANIA:
- Dokładne i wczesne wykrywanie zagrożeń w sieci dla dowolnego wektora ataku - Kompleksowe rozwiązanie z możliwością skalowania dla ewoluujących obszarów ataków - Łatwe wdrożenie, obsługa i skalowalność - Możliwość zyskania dodatkowego czasu na reakcję na incydent, gdy napastnik znajduje się wewnątrz „labiryntu” - Szczegółowe informacje o ataku, w tym taktyki i narzędzia ataku - Mniejsza ilość danych do analizy i mniej cyfrowego „szumu” - Wysoce wiarygodne alerty, z mniej niż 1% fałszywych alarmów	- Wykrywanie ruchu bocznego (lateral movement) i wewnętrznego rekonesansu - Wykrywanie kradzieży poświadczeń - Dokładny wgląd w zagrożenia ze strony: przeciwników zewnętrznych, osób wewnątrz organizacji i dostawców - Usprawnienie reakcji na zagrożenia i weryfikacja niezawodności istniejących zabezpieczeń - Szczegółowa analiza ataku i pierwotnej przyczyny wraz z uzasadnionymi alarmami i raportami kryminalistycznymi - Przyspieszona reakcja na incydenty dzięki integracji z rozwiązaniami firm trzecich, które automatyzują izolację, blokowanie i wyszukiwanie zagrożeń - Wykrywanie złośliwego oprogramowania i spowalnianie jego rozprzestrzeniania się

4. WYMAGANIA SYSTEMOWE

Instalacja na VMware vSphere 6.5 lub wyższym, Microsoft Hyper-V 2016 lub wyższym, Microsoft Azure Cloud oraz Proxmox 8.2 i wyższym jest oficjalnie wspierana.

Komponenty platformy	Wymagania sprzętowe
Admin VM (konsola cetralnego zarządzania)	4 vCPU (rdzenie), 16 GB RAM, 500 GB HDD
Worker VM (węzeł roboczy dla Punktów)	8 vCPU (rdzeni), 16 GB RAM, 200 GB HDD

W CELU UZYSKANIA DALSZYCH INFORMACJI O PLATFORMIE LABYRINTH LUB DEMONSTRACJI PRODUKTU, PROSIMY O KONTAKT Z FIRMĄ LABYRINTH POD ADRESEM: INFO@LABYRINTH.TECH