LABYRINTH

PLATFORMA DECEPCJI LABYRINTH W MODELU MSSP

Labyrinth Deception Platform, 2023

https://labyrinth.tech

info@labyrinth.tech

Labyrinth Development

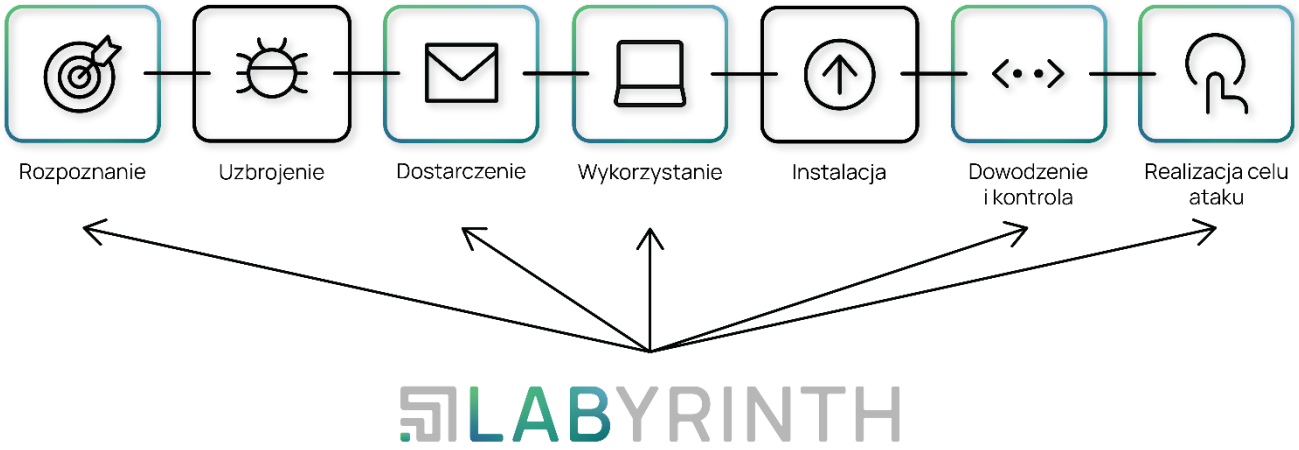
1. OGÓLNY OPIS SYSTEMU

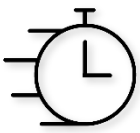
Labyrinth Deception Platform to platforma do wykrywania cyberzagrożeń, która celowo chroni sieć przed ukierunkowanymi atakami, nieznanymi zagrożeniami, botnetami, atakami „dnia zerowego" i złośliwymi intruzami, wykrywając i blokując cyberataki w sieci korporacyjnej.

Rozwiązanie nie wymaga instalacji dodatkowego oprogramowania i posiada intuicyjny interfejs. Platforma zapewnia proste i skuteczne narzędzie do jak najszybszego wykrywania intruzów oraz pełny wgląd w przebieg ataków, z korelacją zdarzeń w celu podejmowania prawidłowych i szybkich decyzji.

1.1. Funkcjonalność systemu

Labyrinth Deception Platform obejmuje pięć z siedmiu etapów metodologii Cyber kill chain.





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

1.1.1. Wczesne wykrywanie zagrożeń w sieci

System wykrywa wszelkie ukierunkowane, podejrzane działania na wczesnym etapie ataku. Pułapki są zaprojektowane do wykrywania działań atakującego, gdy próbuje on zbadać sieć i znaleźć swój cel. Gdy tylko atakujący zacznie wchodzić w interakcje z wabikami (tzw. Punktami), system zbiera wszelkie szczegóły na jego temat: źródła zagrożeń, używane narzędzia i słabe strony. Jednocześnie wszystkie rzeczywiste zasoby i usługi działają bez żadnych zakłóceń.

1.1.2. Szybka reakcja na incydent

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 naruszenia (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 i przeprowadzenie analizy, pewną reakcję i opracowanie lepszej obrony na przyszłość.

1.1.3. Ujawnianie 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. Platforma ujawnia również słabości korporacyjnych systemów obronnych, które mogą zostać wykorzystane przez napastników w przyszłości.

1.1.4. Wykrywanie po infekcji

Platforma decepcji Labyrinth zastosowana w sieciach firmowych może służyć jako wysoce niezawodny system ostrzegania o atakach, które ominęły zabezpieczenia brzegu sieci. Agenty, rozmieszczone na serwerach i stacjach roboczych, imitują bardzo atrakcyjne dla atakującego artefakty. To, co wydaje się być kontem administratora o wysokich uprawnieniach i źle chronionym, jest pułapką, która zwabia atakującego do systemu Labyrinth, w której można śledzić działania atakującego, gromadząc cenne informacje na temat zagrożeń, które przeniknęły do sieci.

1.1.5. 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. Platforma decepcji Labyrinth skraca czas i zdolność atakujących do poruszania się w sieciach firmowych i zatrzymuje ich, zanim dotrą do krytycznych zasobów i usług.

1.2. Korzyści z użytkowania

1.2.1. Redukcja kosztów operacyjnych

Platforma zmniejsza koszty operacyjne cyberbezpieczeństwa nawet o 30% - nie gromadzi dużych ilości danych, nie generuje fałszywych alarmów i nie wymaga specjalnych umiejętności do obsługi.

1.2.2. Automatyzacja reakcji na incydenty

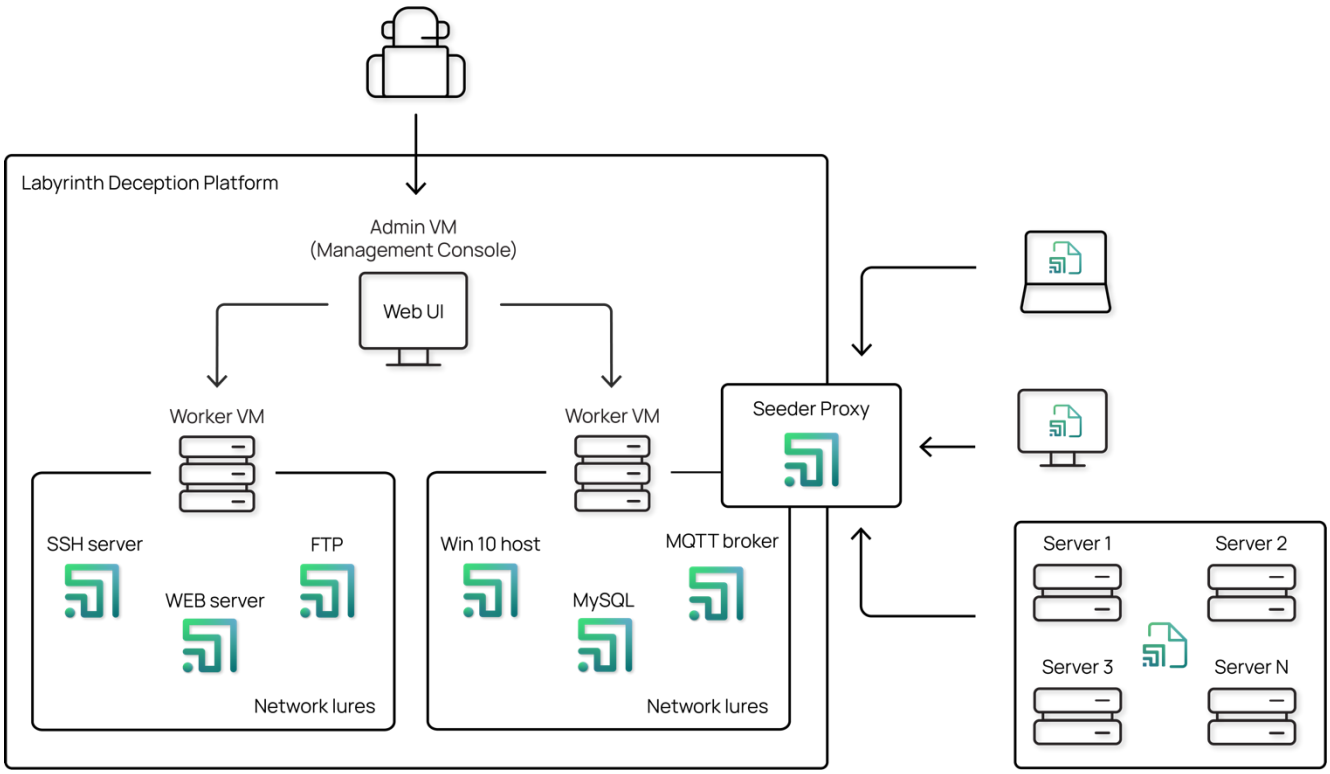
Przyspiesza reagowanie na incydenty poprzez nawet 12-krotne skrócenie średniego czasu: wykrywania oraz reagowania na zagrożenia (MTTD, MTTR).

1.2.3. Łatwość wdrożenia

Szybkie i proste wdrożenie bez konfliktów systemowych i minimalna konserwacja systemu: brak baz danych, podpisów lub reguł do konfiguracji i aktualizacji.
Labyrinth wykrywa i zatrzymuje ukierunkowane i zaawansowane cyberataki bez konieczności wcześniejszego poznania formy, typu lub zachowania zagrożenia oraz bez wpływu na wydajność urządzeń sieciowych, hostów, serwerów lub aplikacji.

1.3. Architektura logiczna

Ogólna architektura platformy została przedstawiona na rysunku:



Komponenty systemu:

1. **Admin VM** (konsola zarządzania) to główny moduł, który wykonuje funkcje zarządzania systemem, zapewnia interfejs sieciowy, zbiera i przechowuje informacje o incydentach bezpieczeństwa, generuje alerty, itp. Obejmuje również izolację środowiska (Multitenancy).

   Admin VM komunikuje się z węzłami roboczymi (Worker node) za pośrednictwem szyfrowanych kanałów.

2. **Worker Node** (węzeł roboczy) to oparta na systemie Linux maszyna wirtualna przeznaczona do tworzenia, przechowywania i uruchamiania wabików sieciowych (Points). System może zawierać jedną lub więcej maszyn wirtualnych Worker w zależności od wymagań skalowalności lub funkcji infrastruktury sieciowej klienta.

   W węźle Worker należy podłączyć TRUNK z listą sieci VLAN, w których planowane jest wdrożenie wabików sieciowych, aby każda maszyna wirtualna mogła jednocześnie obsługiwać jedną i kilka sieci VLAN.

3. **Point** (Punkt) to wabik sieciowy imitujący określoną/e usługę/usługi. Obiekty systemowe tego typu mogą zawierać imitacje różnych luk w zabezpieczeniach, które wygenerują powiadomienie o ataku (Alert), gdy atakujący spróbuje je wykorzystać.

   Punkty zatrzymują atakującego wewnątrz platformy decepcji Labyrinth do momentu zebrania wszystkich niezbędnych informacji.

4. **Seeder Agent** to plik binarny dla systemów Windows i Linux, który zapewnia logiczne połączenia między rzeczywistą i wygenerowaną infrastrukturą. Po uruchomieniu na prawdziwym hoście, Seeder Agent komunikuje się z maszyną wirtualną administratora i otrzymuje zadania do utworzenia nawigacji okruszkowej

   Może działać w dwóch trybach:
   a. jako jednorazowe uruchomienie i zatrzymanie swojego procesu po utworzeniu wszystkich artefaktów,
   b. działać jako stały proces z połączeniem do konsoli zarządzania (Admin VM).

   Agenci Seeder znajdują się na serwerach i stacjach roboczych i imitują najbardziej atrakcyjne artefakty dla hakerów. Po uruchomieniu przez atakujących, agent kieruje ich do Punktów.

5. **Seeder Proxy Point** - cała interakcja między Seeder-Agent i maszyną Admin VM (konsolą zarządzającą) przechodzi przez usługę Seeder-Proxy, która jest zaimplementowana jako oddzielny typ Punktu (Point). W tym przypadku Seeder-Agent łączy się z portem 443/tcp w Seeder-Proxy.

   W ten sposób ten typ przynęty sieciowej pełni jednocześnie dwie funkcje:
   a. imituje podatną na ataki aplikację internetową,
   b. pośredniczy między Seeder-Agentami na rzeczywistych hostach w określonej sieci VLAN a maszyną wirtualną administratora (Admin VM).

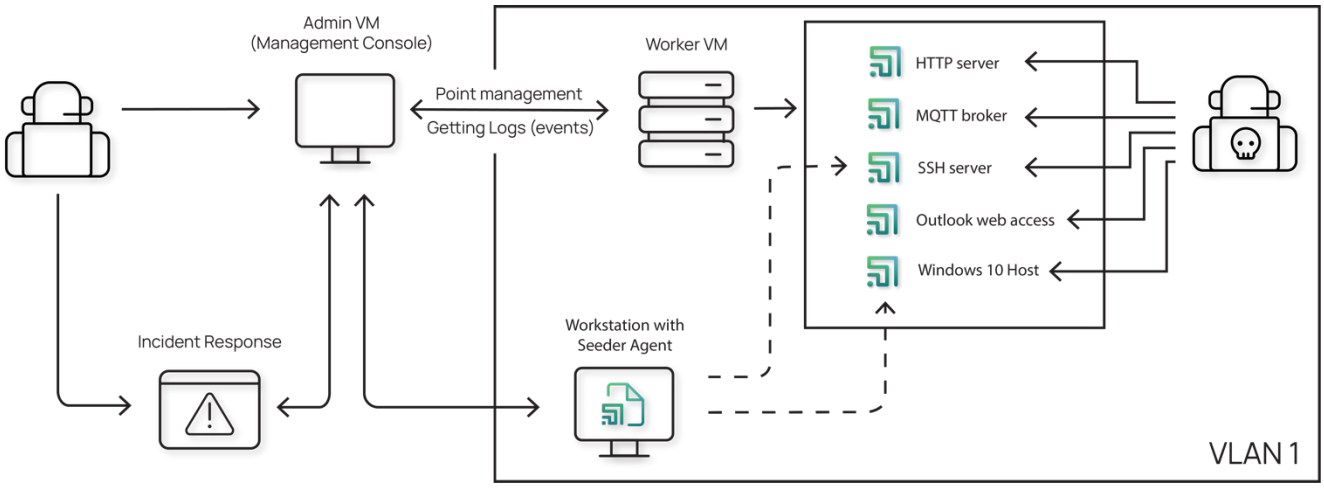
1.3. Opis systemu wielu najemców (Multitenancy) i uwierzytelniania (RBAC)

Dla usługodawców MSSP krytyczne jest posiadanie narzędzi, które pozwolą im świadczyć usługi klientom przy niskich kosztach sprzętu i minimalnym czasie na wdrożenie niezbędnych komponentów/modułów. Jest to ułatwione dzięki funkcjonalności multitenancy i elastycznemu modelowi ról dla użytkowników systemu.

Mówiąc najprościej, multitenancy (model wielu najemców) to zdolność różnych użytkowników lub firm do korzystania z odizolowanych od siebie zasobów w ramach tej samej usługi (jednej instalacji lub wdrożenia).

Dzisiejsza architektura modelu wielu najemców jest zatem jednym z najbardziej wydajnych modeli dostarczania usług IT i podstawowym sposobem oszczędzania zasobów obliczeniowych i pamięci dyskowej. Pojedyncza instancja aplikacji, działająca na pojedynczej infrastrukturze serwerowej, ale dostępna dla wielu użytkowników i firm jednocześnie, pozwala zminimalizować koszty świadczenia usług IT i zmaksymalizować ich jakość.

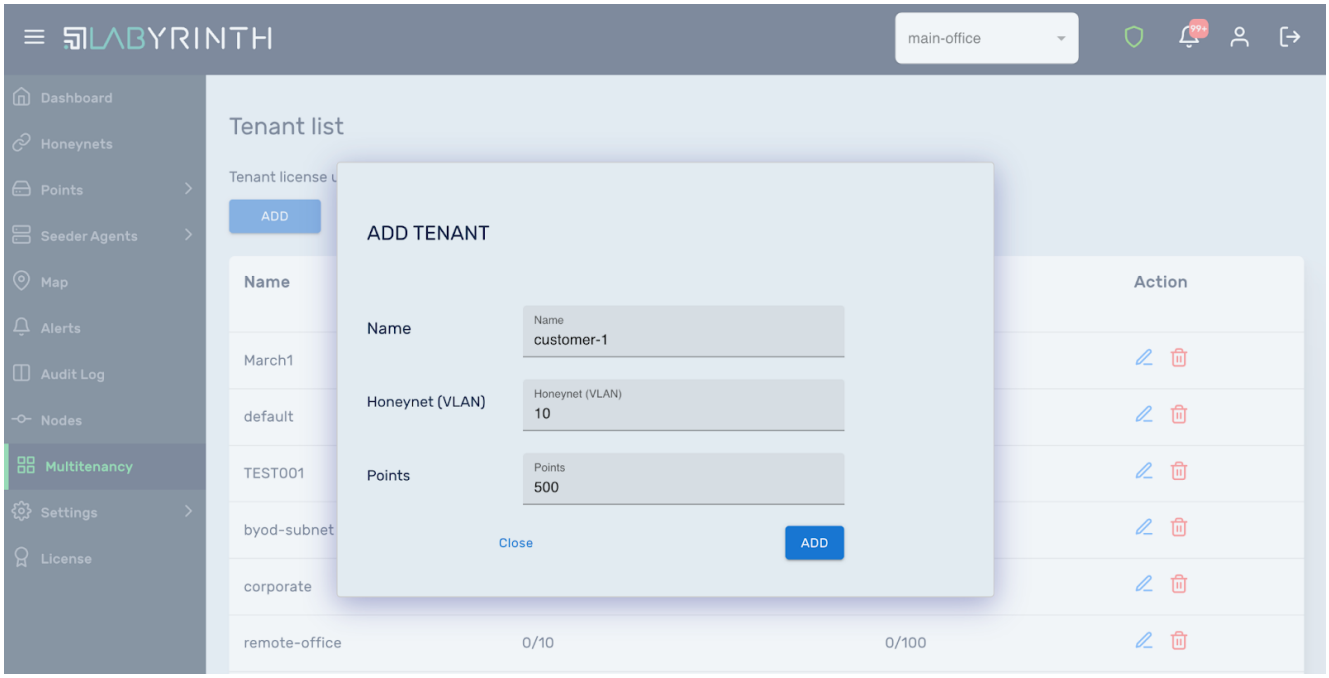
Platforma decepcji Labyrinth obsługuje wielu najemców, co pozwala na zapewnienie odizolowanych środowisk dla różnych działów lub oddziałów firmy lub klientów firmy MSSP w ramach tej samej instalacji. Oznacza to, że dzierżawy są całkowicie odizolowane od siebie, tj. użytkownicy, alerty, sieci honeynet, itp. są dostępne w ramach danej dzierżawy, a nie w innych dzierżawach.



Admin VM (konsola zarządzania) znajduje się w centralnym biurze firmy MSSP lub w głównym centrum danych. Dostęp do jej interfejsu sieciowego na porcie sieciowym **443/tcp(https)** jest ograniczony do segmentu zarządzania siecią.

Worker VMs (węzły robocze) są umieszczane w sieciach klientów firmy MSSP, którzy używają systemu Labyrinth do wykrywania ataków. Węzły te są synchronizowane z Admin VM (konsolą zarządzania) na porcie sieciowym **20202 (tcp/udp)**. Kanał między systemami wirtualnymi jest szyfrowany. Do transmisji danych wykorzystywany jest algorytm kryptograficzny ChaCha20.

Podczas tworzenia lub edytowania najemcy należy określić liczbę sieci Honeynet (VLAN) i Punktów przypisanych do tego najemcy z licencji ogólnej:



Zapewnia to oczekiwany podział licencji między najemców i eliminuje niepożądaną możliwość, że jeden najemca może wykorzystać pełną licencję.

Ustawienia konfiguracji i inne działania związane z zarządzaniem dzierżawami są wykonywane **przy użyciu poświadczeń z uprawnieniami Superużytkownika**. Po utworzeniu jednego lub więcej najemców, Superużytkownik może przełączać się między najemcami.

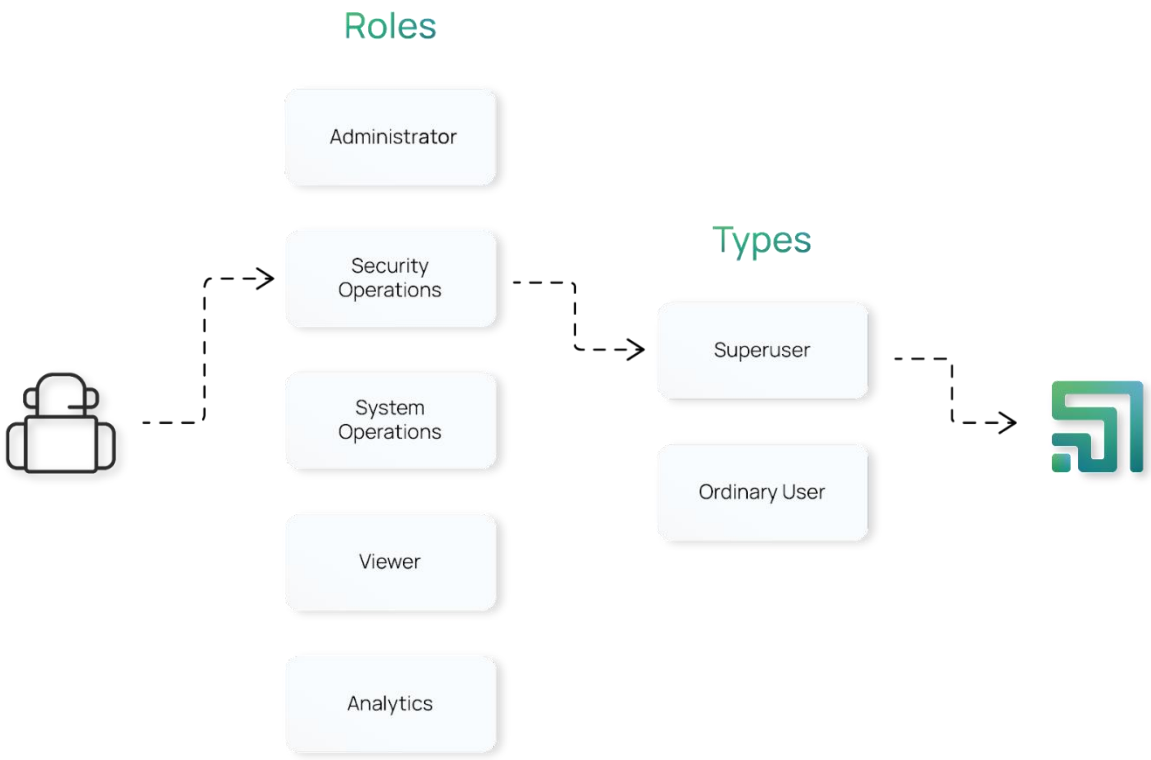
Użytkownicy utworzeni w ramach najemcy, w tym użytkownicy ze statusem administratora, mogą utworzyć zarówno superużytkownika, jak i użytkownika z uprawnieniami administratora w bieżącej dzierżawie. Role użytkowników są regulowane przez RBAC.

Istotą podejścia RBAC (Role-based access control) jest tworzenie ról odzwierciedlających role biznesowe w firmie i przypisywanie ich użytkownikom. Na podstawie tych ról sprawdzana jest zdolność użytkownika do wykonania określonej akcji.

Rola jest szablonem uprawnień i dostępów w systemie definiowanym podczas tworzenia użytkownika. Później może być zmieniona przez superużytkownika lub użytkownika tego najemcy z rolą Administratora.

Istnieje pięć możliwych ról dla użytkowników najemcy dla nowo utworzonego użytkownika:

1. **Administrator** to rola z pełnymi uprawnieniami w ramach najemcy. Użytkownik z tą rolą może tworzyć innych użytkowników w ramach najemcy, w tym użytkowników z rolą Administratora.
2. **Operacje systemowe** to rola, która ma dostęp do komponentów systemu w celu konfiguracji. Dane dotyczące incydentów bezpieczeństwa nie są dostępne.
3. **Operacje bezpieczeństwa** to rola przeznaczona do obsługi incydentów bezpieczeństwa. Rola ma dostęp do danych o wykrytych atakach (Alerts) oraz zarządzania Honeynet, Point i Seeder, ale nie ma dostępu do ustawień systemowych w ramach najemcy.
4. **Widz** to rola podobna do roli Administratora, ale w trybie do odczytu.
5. **Analityka** to rola, która ma dostęp tylko do danych o incydentach bezpieczeństwa.



Inżynierowie IT/IS firmy klienta są wyznaczani jako użytkownicy w dzierżawie. Umożliwia to przeniesienie niektórych funkcji konfigurowania i monitorowania zdarzeń w dzierżawie na użytkowników lokalnych.

1.4. Licencjonowanie

System jest licencjonowany na podstawie liczby segmentów sieci (VLAN) i wabików (Punktów). Artefakty (breadcrumbs) i liczba użytkowników/adresów IP w sieci nie są licencjonowane oddzielnie.

Aby uzyskać licencję, należy upewnić się, że serwer licencjonowania jest dostępny - https://update.labyrinth.tech/

Dostarczona, pełna licencja może zostać podzielona pomiędzy najemców według uznania MSSP.

2. PROGRAMY WSPARCIA TECHNICZNEGO

Wszyscy testujący / istniejący klienci mają pełny dostęp do naszego zespołu inżynierów wsparcia. Chociaż prośba o wsparcie może zostać zgłoszona 24 godziny na dobę, 7 dni w tygodniu, ważne jest, aby pamiętać o godzinach dostępności wsparcia dla konkretnego programu.

Program	Dostępność wsparcia	Kanały kontaktu
Wsparcie dla klientów (Full support)	Pon-Nd 8:00 – 20:00 (GMT+2)	Phone / Web / Email
Wsparcie dla testujących (Evaluation)	Pon-Pt 9:00 – 18:00 (GMT+2)	Web / Email

Każdy program, po uzgodnieniu, może być dostosowany do potrzeb klienta.

W celu zapewnienia wzorcowego, ogólnego doświadczenia wszystkim naszym obecnym i przyszłym klientom (testującym rozwiązanie), ustaliliśmy pewne wytyczne dotyczące wagi problemu, aby zapewnić, że im wyższa waga problemu, tym szybszy będzie początkowy docelowy czas reakcji.

Poziomy ważności zgłoszeń

Waga	Opis / przykład problemu	First Response Time (FRT) czas pierwszej reakcji	
		Evaluation Support	Full Support
Wysoka	Krytyczny problem, w którym rozwiązanie nie działa lub ma wpływ na środowisko sieciowe, w którym zostało wdrożone.	24 godziny	12 godzin
	Na przykład: kolizja adresów IP lub negatywny wpływ na wydajność infrastruktury.		
Średnia	Nie ma wpływu na infrastrukturę produkcyjną, rozwiązanie działa poprawnie, ale jego działanie nie jest właściwe.	48 godzin	24 godziny
	Na przykład: dostosowanie konfiguracji i dostrajanie raportów.		
Niska	Drobny problem, który nie ma wpływu na funkcjonalność rozwiązania lub środowiska sieciowego, w którym zostało ono wdrożone.	72 godziny	48 godzin
	Na przykład: ogólne pytanie dotyczące konfiguracji, opinia, sugestia lub prośba o funkcję.		

Więcej informacji można znaleźć w Przewodniku referencyjnym obsługi klienta.

3. WYMAGANIA TECHNICZNE

3.1. Wymagania wobec klienta (firmy MSSP)

Niezbędne warunki obejmują następujące elementy:

1. Zatwierdzenie przydziału pojemności serwera. Parametry podano w sekcji "3.2 Zasoby obliczeniowe".
2. Zatwierdzenie konfiguracji wymaganych dostępów:
    1. Wymagany jest dostęp sieciowy do interfejsu sieciowego hiperwizora, na którym system zostanie wdrożony, oraz dostęp przez HTTPS i SSH do maszyn wirtualnych Labyrinth.
    2. Wymagania dotyczące konfiguracji portów sieciowych.

3. Dostępność wirtualnych uplinków dla operatorów użytkownika.
4. Podanie adresów IP i nazwy hosta dla węzła roboczego, aby zarządzać sieciami VLAN.
5. Konieczne jest zapewnienie łączności sieciowej między AdminVM (w sieci firmy MSSP) a węzłami roboczymi (Worker Nodes) w sieciach firm klienckich (najemców).
6. Należy uzyskać listę adresów IP dla każdej sieci VLAN, która ma być chroniona. Te adresy IP będą używane do generowania wabików sieciowych (Punktów), jeśli do tworzenia wabików sieciowych używane jest adresowanie statyczne.

3. Zapewnienie konfiguracji niezbędnych otwartych portów i protokołów zgodnie z sekcją „3.3 Zasady dostępu do sieci".

3.2. Zasoby obliczeniowe

Komponenty Labyrinth Deception Platform są dystrybuowane jako obraz maszyny wirtualnej w formacie OVA (dla VMware) lub archiwum Zip (dla Hyper-V). Są one obecnie oficjalnie obsługiwane przez następujące platformy wirtualizacji/chmury:

- VMWare vSphere 6.0/6.5/7.0;
- Microsoft Hyper-V z minimalną wersją Hyper-V 2008 R2;
- Microsoft Azure Cloud;
- Rozwiązania oparte na KVM (Proxmox, OpenStack itp.) dla Admin VM (konsoli zarządzania).

Firmy klienckie (najemcy) obsługiwane przez firmę MSSP instalują komponent Worker Node (jeden lub więcej, w zależności od potrzeb).

Komponenty	Do 150 Punktów (Points) Do 15 segmentów VLAN	Do 300 Punktów (Points) Do 50 segmentów VLAN	Do 500 Punktów (Points) Do 100 segmentów VLAN	Powyżej 500 Punktów (Points) Powyżej 100 segmentów VLAN
	vCPU (ilość rdzeni), RAM(GB),HDD(GB)	vCPU (ilość rdzeni), RAM(GB),HDD(GB)	vCPU (ilość rdzeni), RAM(GB),HDD(GB)	vCPU (ilość rdzeni), RAM(GB),HDD(GB)
Admin VM (konsola zarządzania)	4 vCPU(rdzenie) 28 GB RAM 500 GB HDD	4 vCPU(rdzenie) 28 GB RAM 500 GB HDD	4 vCPU(rdzenie) 32 GB RAM 800 GB HDD	Skontaktuj się z przedstawicielem producenta.
Worker Node (węzeł roboczy)	8 vCPU(rdzeni) 16 GB RAM 200GB HDD	12 vCPU(rdzeni) 24 GB RAM 250GB HDD	16 vCPU(rdzeni) 40 GB RAM 500GB HDD	
Sumarycznie	12 vCPU(rdzeni) 44 GB RAM 700 GB HDD	16 vCPU(rdzeni) 52 GB RAM 750 GB HDD	20 vCPU(rdzeni) 72 GB RAM 1300 GB HDD	

W przypadku instalacji Proof of Concept (wdrożenie nieprodukcyjne/testowe) można nieznacznie zmniejszyć przydzielone zasoby:

Admin VM (konsola zarządzania)	4 vCPU (rdzenie), 24 GB RAM, 200 GB HDD lub większy
Worker Node VM (węzeł roboczy)	4 vCPU (rdzenie), 8 GB RAM, 200 GB HDD

3.3. Zasady dostępu do sieci

Aby Platforma działała poprawnie, konieczne jest zapewnienie dostępności między różnymi komponentami systemu na określonych portach sieciowych (TCP, UDP):

Z ↓ / do →	Admin VM	Worker Node	update.labyrinth.tech	ntp.labyrinth.tech	Seeder Proxy	SIEM
Admin VM (konsola zarządzania)		20202 UDP	443 TCP	123 TCP 123 UDP		514 TCP 514 UDP
Worker Node (węzeł roboczy)	20202 UDP 20202 TCP					
PC Operator	22 TCP 443 TCP	22 TCP				
Realne hosty z agentami Seeder					443 TCP	

4. WDROŻENIE I URUCHOMIENIE SYSTEMU

Pilotażowy plan wdrożenia systemu dla potrzeb MSSP można przedstawić następująco:

№	Nazwa działania	Liczba dni roboczych
1	**Prace przygotowawcze do rozpoczęcia projektu pilotażowego**	**4**
1.1	Przydzielanie pojemności serwera	1
1.2	Dostosowywanie ustawień sieciowych	1
1.3	Konfigurowanie wymaganych dostępów dla komponentów Labyrinth	1
1.4	Zatwierdzenie planu projektu pilotażowego	1
2	**Wdrożenie systemu Labyrinth**	**1-3**
2.1	Konfigurowanie maszyn wirtualnych	
2.2	Przeprowadzenie procedury uzyskania licencji (subskrypcji)	

2.3	Sprawdzenie dostępności aktualizacji i aktualizacja systemu (w razie potrzeby)	
2.4	Dołączenie "niestandardowych" plików przez operatora systemu, które będą używane przez system jako dodatkowe wabiki plikowe (wordlists)	
2.5	Wdrożenie agenta Seeder na rzeczywistych hostach	
2.6	Konfigurowanie niestandardowych typów Punktów (opcjonalnie)	
2.7	Konfigurowanie sieci Honeynet	
2.8	Generowanie wabików (Points), w tym: Universal Web Points do emulacji istniejących w sieci usług internetowych oraz wabików SCADA/OT (w razie potrzeby u klienta)	
2.9	Weryfikacja utworzonych wabików sieciowych (Points) oraz wabików plikowych (Seeder-Tasks/Breadcrumbs) dystrybuowanych na rzeczywistych hostach	
3	**Wdrażanie integracji w zależności od dostępnych rozwiązań infrastrukturalnych (np. integracja z systemem SIEM)**	**1**
4	**Uruchomienie systemu Labyrinth w pilotażowej eksploatacji i przeprowadzenie testów za pomocą instrukcji dostarczanych przez zespół inżynierów Labyrinth (gotowy przewodnik)**	**3-5**
4.1	Symulacja wykorzystania przez atakującego informacji ze standardowych wabików plikowych (Seeder-Tasks / Breadcrumbs) na rzeczywistych hostach w sieci klienta MSSP	
4.2	Przeprowadzenie serii ataków na wygenerowane Punkty (Points), np. utworzenie punktu symulującego usługi RDP i WMI oraz próba ich przeskanowania i bezpośredniego połączenia przy użyciu odpowiedniego oprogramowania klienckiego.	
4.3	Testowanie scenariuszy I działania skonfigurowanych integracji	
5	**Wygenerowanie raportu na temat wyników projektu pilotażowego**	**1**
6	**Prezentacja wyników**	**1**
Całkowity czas pilotażu		11-15

Liczba dni roboczych na wdrożenie i uruchomienie systemu jest przybliżona i w dużej mierze zależy od zasad stosowanych w Twojej firmie.

Można ją dostosować do własnych potrzeb.