Labyrinth Deception Platform

Czy technologia decepcji ochroni Twój biznes?

Wybierz innowacyjność. Wybierz proaktywną obronę.
Wybierz technologię cyber decepcji.

Labyrinth Security Solutions, 2024

AGENDA

- Wyzwania dotyczące bezpieczeństwa w cyberprzestrzeni
- **Technologia decepcji i jej zalety**
- Platforma decepcji firmy Labyrinth w pigułce
- Kluczowe korzyści i przykłady zastosowania platformy
- Przykładowe wdrożenia u klientów

WYZWANIA

RAPORT ATSummit Holistyczna perspektywa cyberbezpieczeństwa https://www.atsummit.pl/raport-ats/

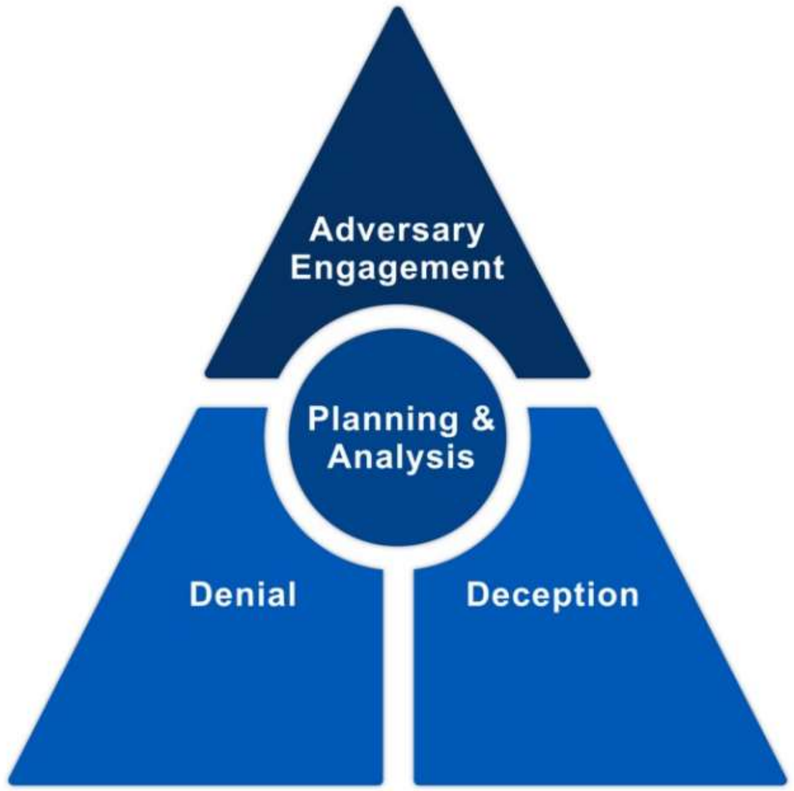
DECEPCJA

Technologia decepcji (podstępu/oszustwa) zapewnia innowację niezbędną w ewolucji strategii bezpieczeństwa organizacji do postaci aktywnej obrony, która stosuje wczesne wykrywanie i szybką reakcję na zagrożenia.

Według ekspertów MITRE, model **Engage** ma stymulować dyskusję na temat aktywnej obrony:

„Włączenie decepcji do **cyberobrony** może być wykorzystywane do wykrywania złośliwej aktywności, kontrolowania przeciwników, gdy znajdą się w środku, **oraz zbierania informacji na temat ich taktyk i metod.**

Strategiczne wykorzystanie decepcji w cyberprzestrzeni i wymiana uzyskanych w ten sposób danych **cyberwywiadowczych** może zwiększyć skuteczność ochrony i poziom odporności.”



https://engage.mitre.org/

ZALETY TECHNOLOGII DECEPCJI

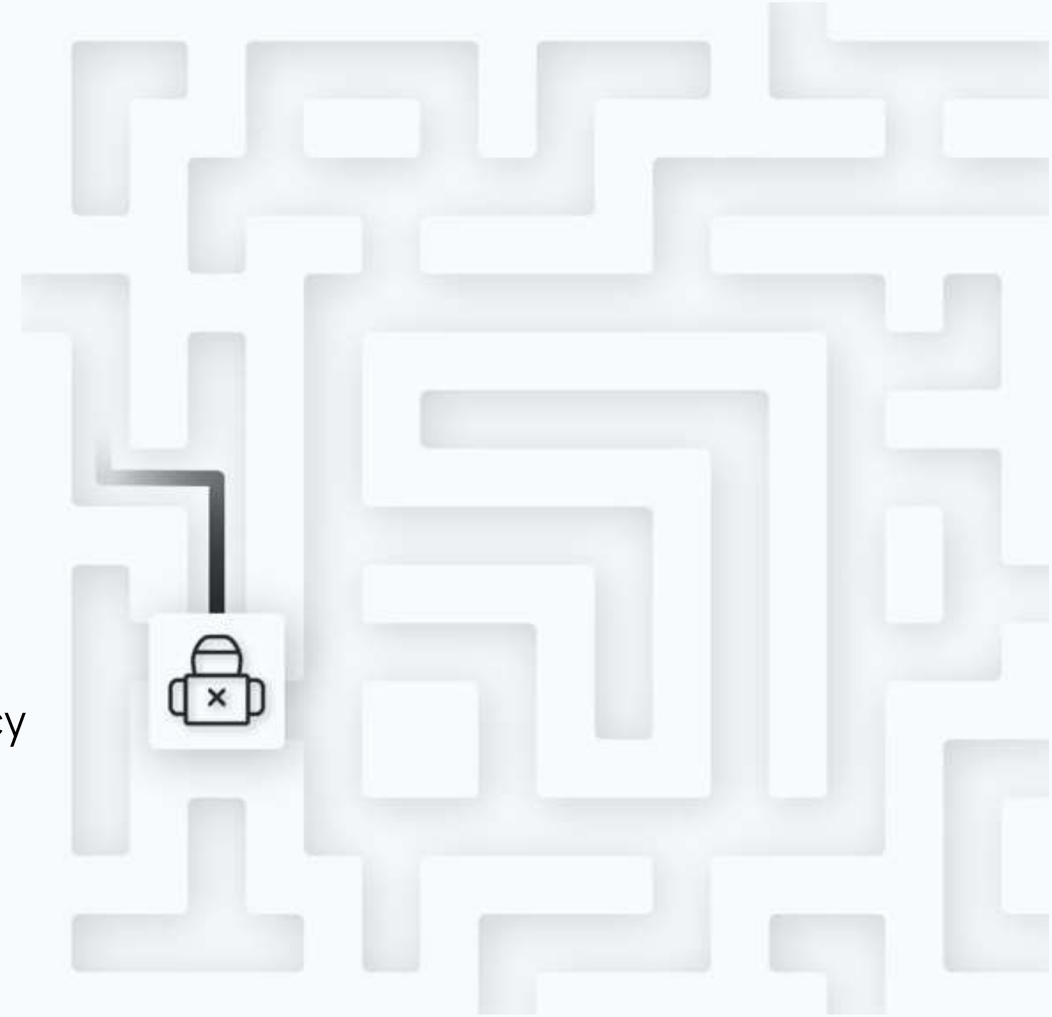
Natychmiastowe wykrywanie

Dokładność wykrywania

ZALETY TECHNOLOGII DECEPCJI

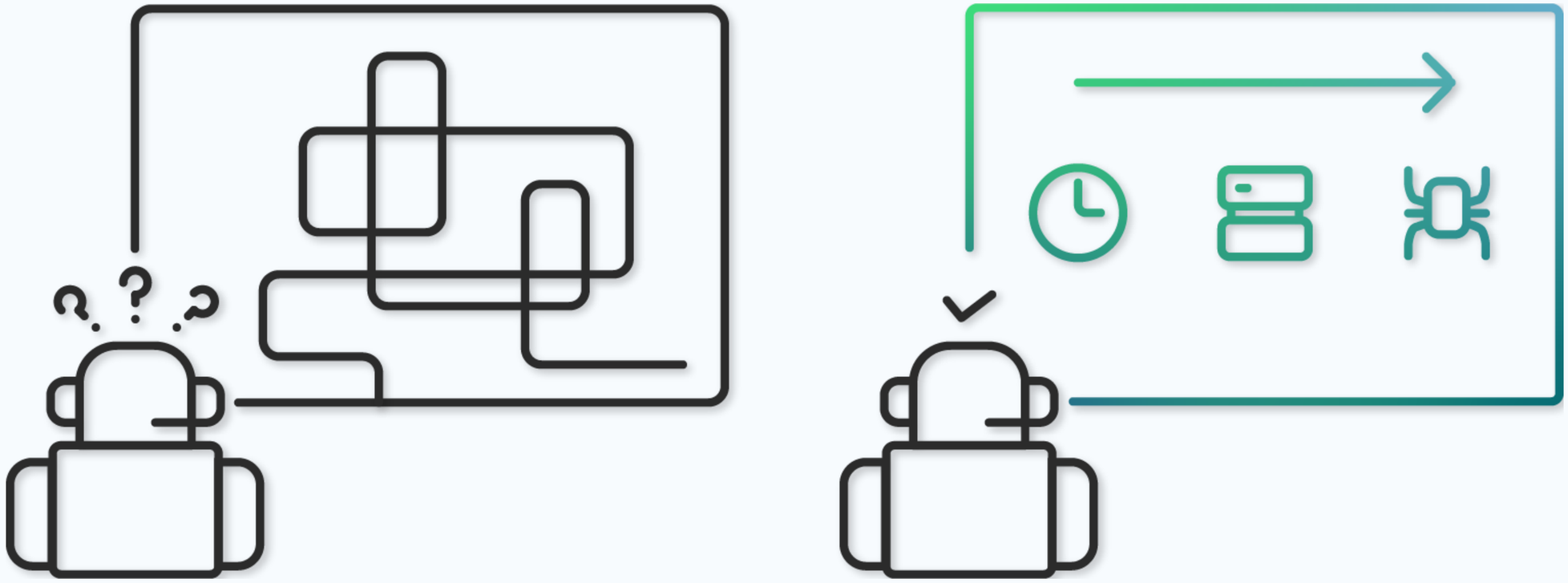
Dwell Time

tzw. współczynnik przebywania, czyli czas jaki atakujący spędzi w naszym imitowanym środowisku, zamiast atakować realne systemy w organizacji – im dłuższy, tym lepiej dla zespołów ds. bezpieczeństwa (SOC)



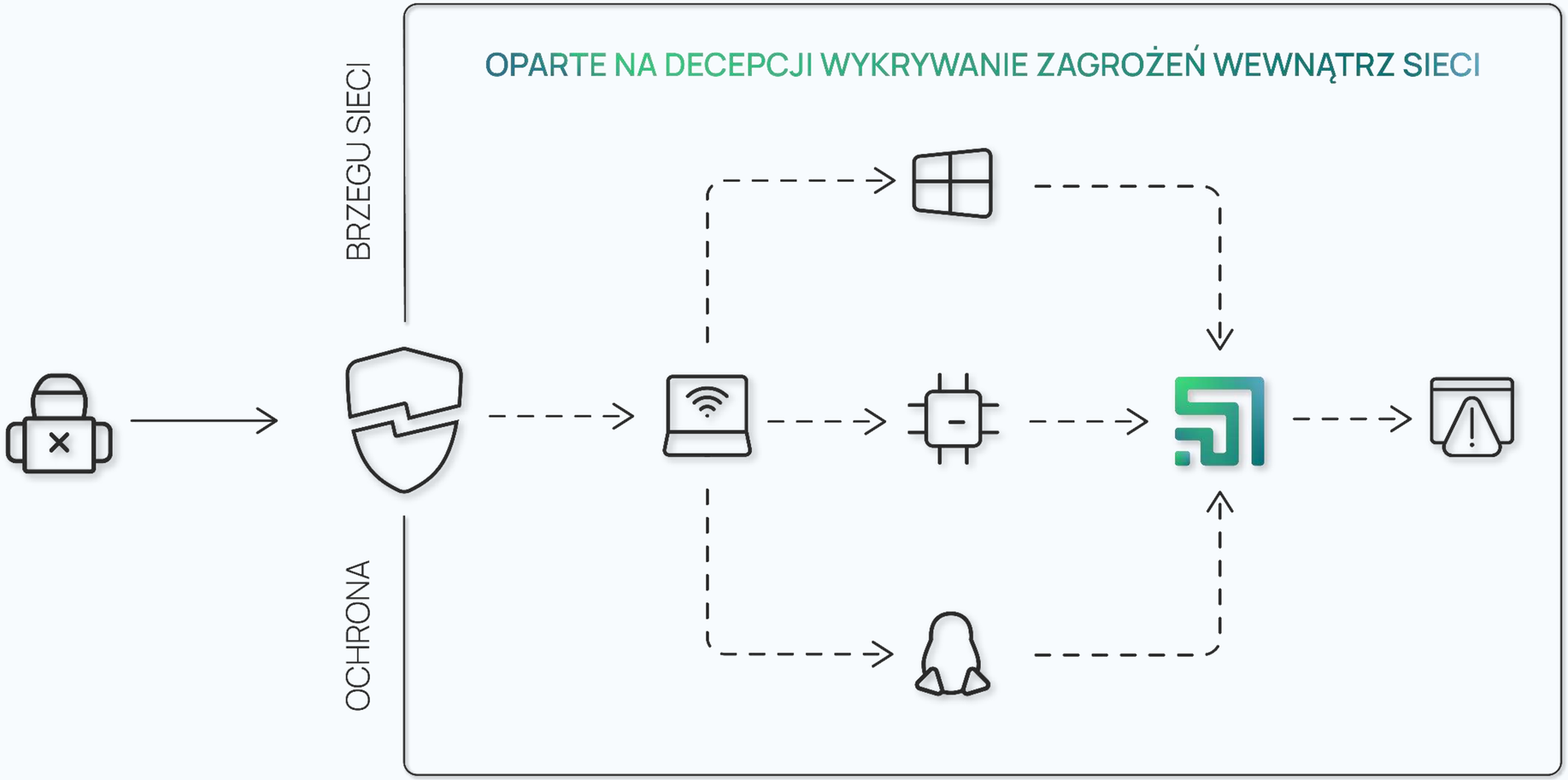
ZALETY TECHNOLOGII DECEPCJI

Technologia decepcji usprawnia proces badania incydentów, ponieważ gromadzi tylko dane związane z incydentami bezpieczeństwa i zapewnia widoczność ataku w czasie rzeczywistym.



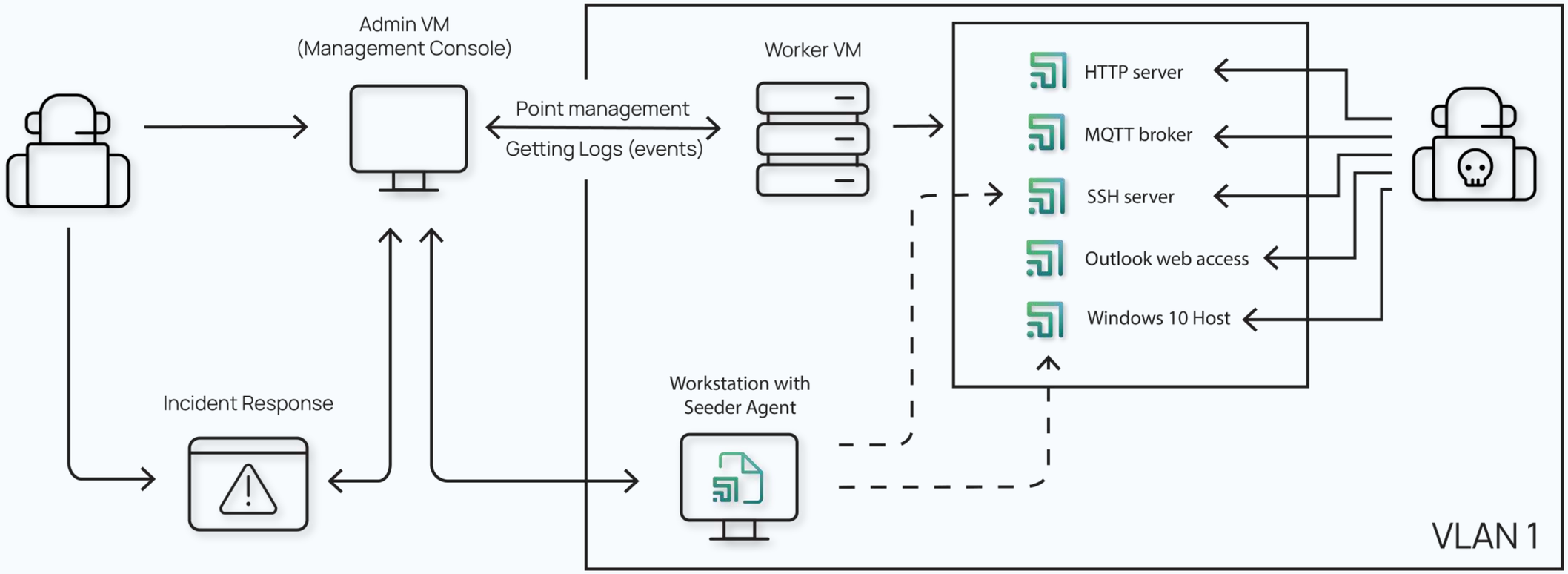
WYKRYWANIE ZAGROŻEŃ ZA POMOCĄ DECEPCJI

Labyrinth zmienia paradygmat cyberbezpieczeństwa poprzez proaktywne podejście do wykrywania zagrożeń.



PLATFORMA DECEPCJI OD LABYRINTH

Platforma imituje podatne na ataki usługi i aplikacje, zwiększając powierzchnię ataku i dezorientując napastników. Labyrinth prowokuje napastników do działania, wykrywa i śledzi wszystkie ich działania oraz izoluje ich od rzeczywistych sieci IT/OT.



SKŁADOWE PLATFORMY LABYRINTH

Seeder Agent

Agenty imitacji, zainstalowane na rzeczywistych hostach, rozmieszczają atrakcyjne artefakty (dane).
Odkryte przez intruzów artefakty kierują ich do przygotowanych Punktów.

Worker Node

Węzeł roboczy jest hostem dla wszystkich wabików w systemie Labyrinth. Działa jednocześnie w wielu sieciach VLAN.
Może występować wiele węzłów w jednej instancji Labyrinth.

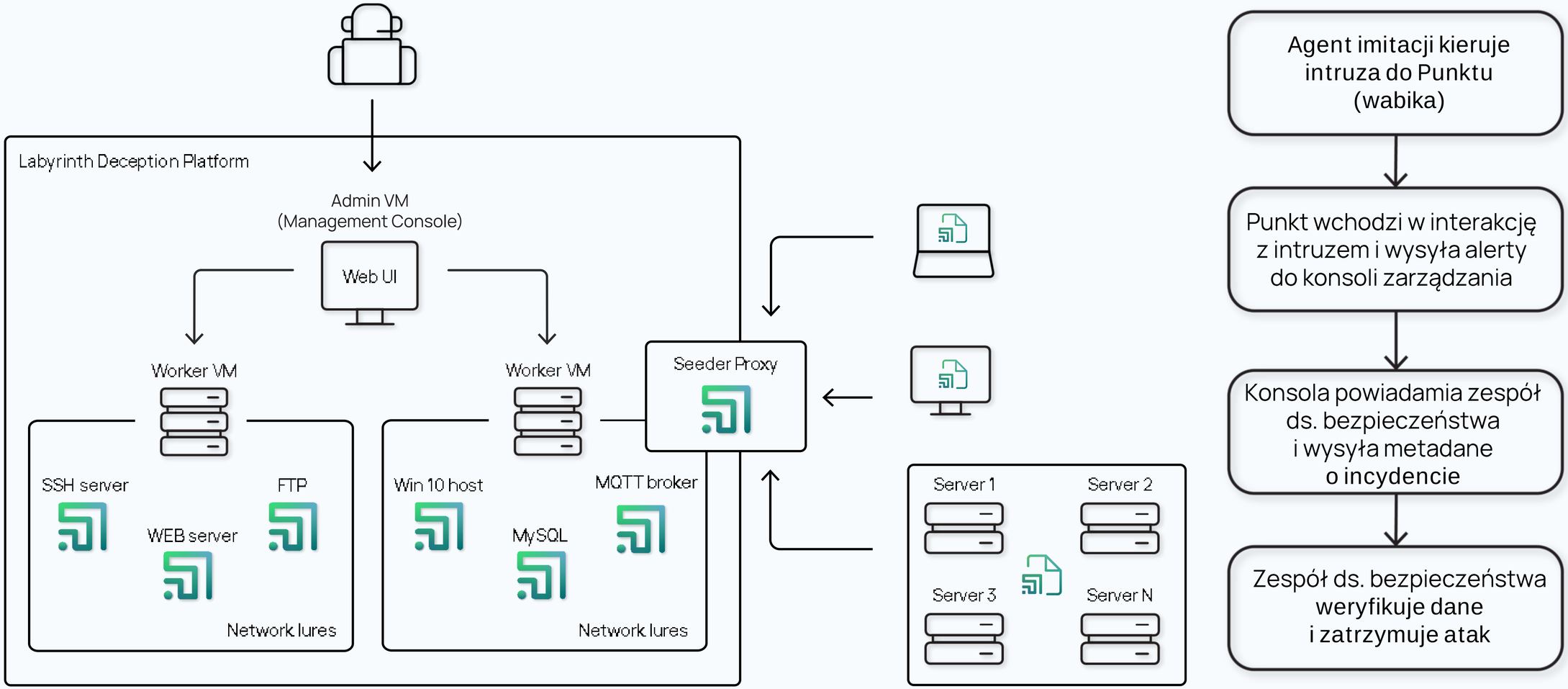
Point

Punkty to wabiki, które naśladują aplikacje i usługi w rzeczywistym środowisku IT/OT i wchodzą w interakcję z intruzem, utrzymując go w systemie Labyrinth.

Management Console

Wszystkie informacje zebrane z wabików poprzez węzeł trafiają do konsoli zarządzania w celu analizy i reagowania na incydenty.

ARCHITEKTURA PLATFORMY



Agent imitacji kieruje intruza do Punktu (wabika)

Punkt wchodzi w interakcję z intruzem i wysyła alerty do konsoli zarządzania

Konsola powiadamia zespół ds. bezpieczeństwa i wysyła metadane o incydencie

Zespół ds. bezpieczeństwa weryfikuje dane i zatrzymuje atak

LABYRINTH

DOSTĘPNE INTEGRACJE Z POZIOMU PLATFORMY

TheHive

CROWDSTRIKE

splunk>

Radar

FORTINET

State	Name	Edit
	CrowdStrike	
	Cuckoo Sandbox	
	Fortigate	
	Microsoft Teams Notifications	
	IBM-Qradar	
	Slack Notification	
	SMTP Notification	
	Splunk	
	SIEM Integration (Syslog forwarder)	
	TheHive	

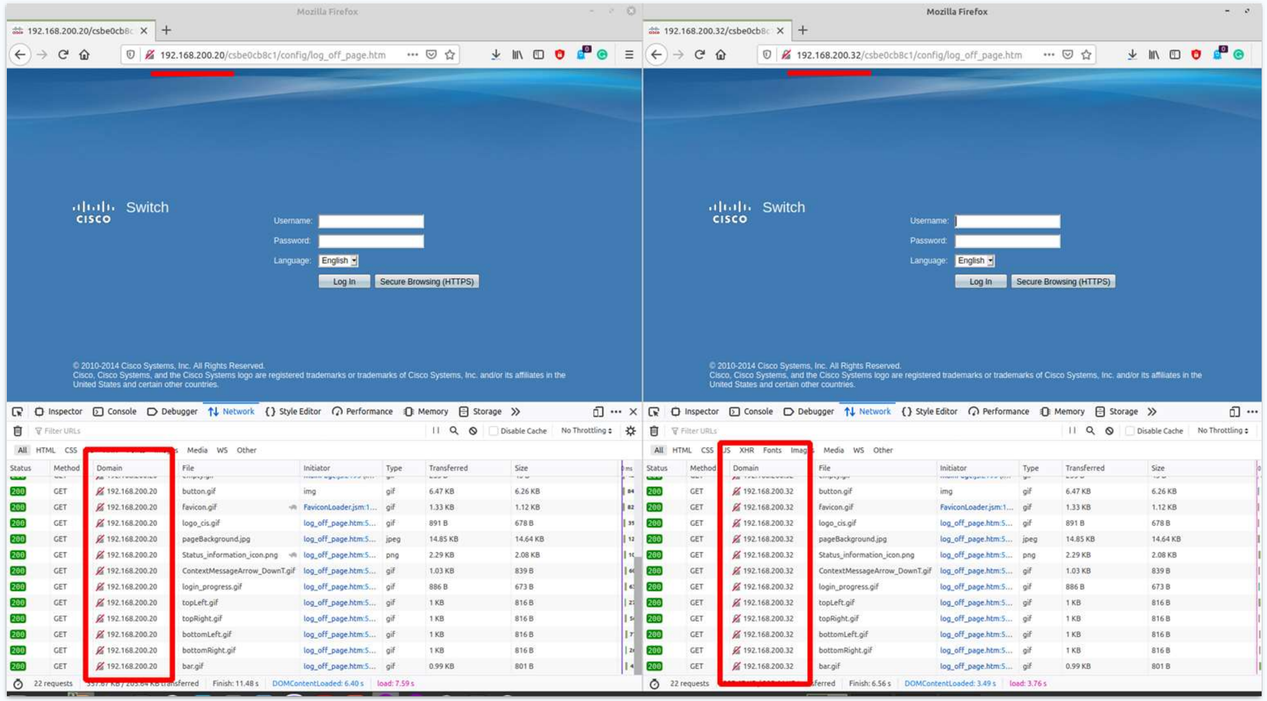
WIARYGODNOŚĆ PUŁAPEK

Każdy wabik to unikalna wirtualna instancja z możliwością interakcji z intruzem.

Wszystkie symulacje tworzone w ramach platformy Labyrinth to wabiki o wysokiej interakcji - zapewniają interaktywność na poziomie co najmniej reagowania na skanowanie, monitowania o poświadczenia, wyświetlania interfejsu graficznego i/lub tekstowego.

Każdy wabik jest unikalny, ma jeden adres IP, nie jest używany żaden alias IP. Zapewnia to najlepszą w branży wiarygodność tworzonych symulacji.

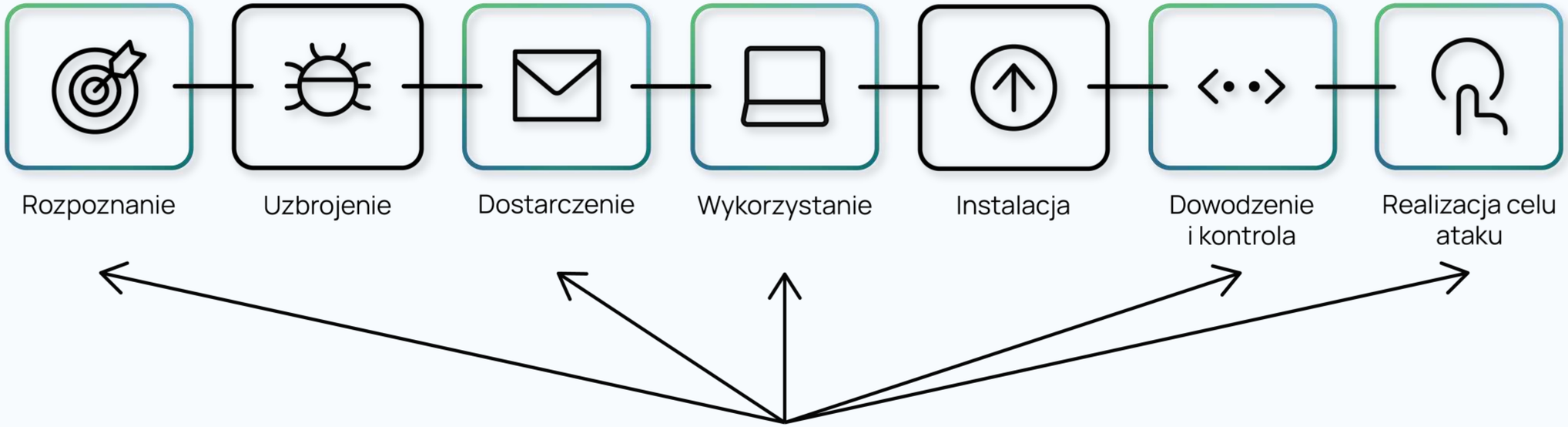
UNIVERSAL WEB POINT



Firma Labyrinth wdrożyła unikalną technologię, która zapewnia dodatkową ochronę najczęściej wykorzystywanych przez hakerów celów - aplikacji i usług internetowych.

Platforma Labyrinth automatycznie wykrywa wszystkie aplikacje internetowe w sieci firmowej i tworzy uniwersalne punkty internetowe (wabiki), które naśladują wykryte aplikacje i osadzają w nich dodatkowe luki (podatności), aby uczynić je bardziej atrakcyjnymi dla atakujących.

ZASTOSOWANIE PLATFORMY



LABYRINTH

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

KLUCZOWE KORZYŚCI

Imitacje o wysokim stopniu interakcji

Każdy wabik to unikalna wirtualna instancja z możliwością interakcji z intruzem. Do wabika można dodać znane podatności.

Aktywne wabiki

Labyrinth nie tylko czeka na działania atakującego, ale także symuluje ruch pochodzący z wabików.

Universal WEB Point (fałszywe aplikacje WWW)

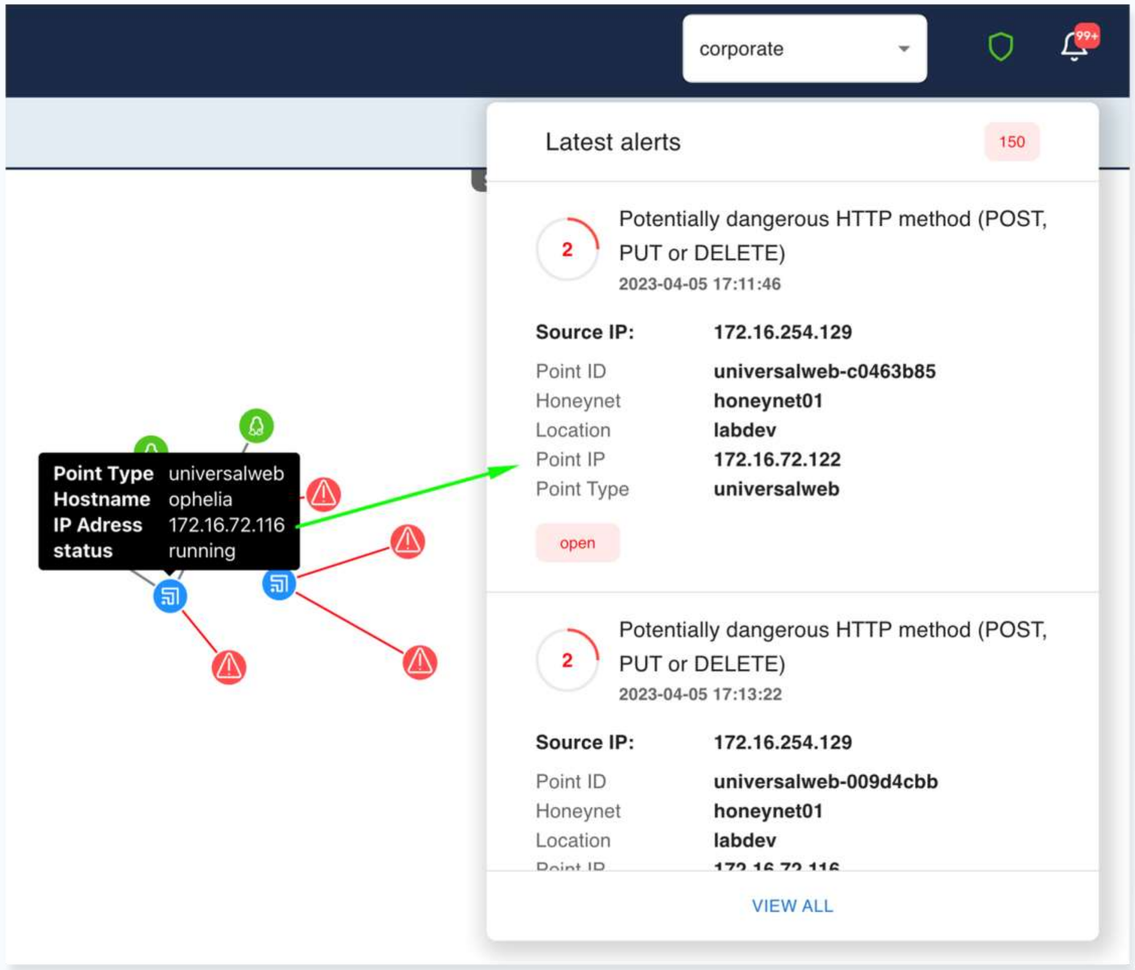
Kilka minut na stworzenie interaktywnej symulacji złożonej, wieloskładnikowej aplikacji internetowej.

Dostosowanie pod klienta

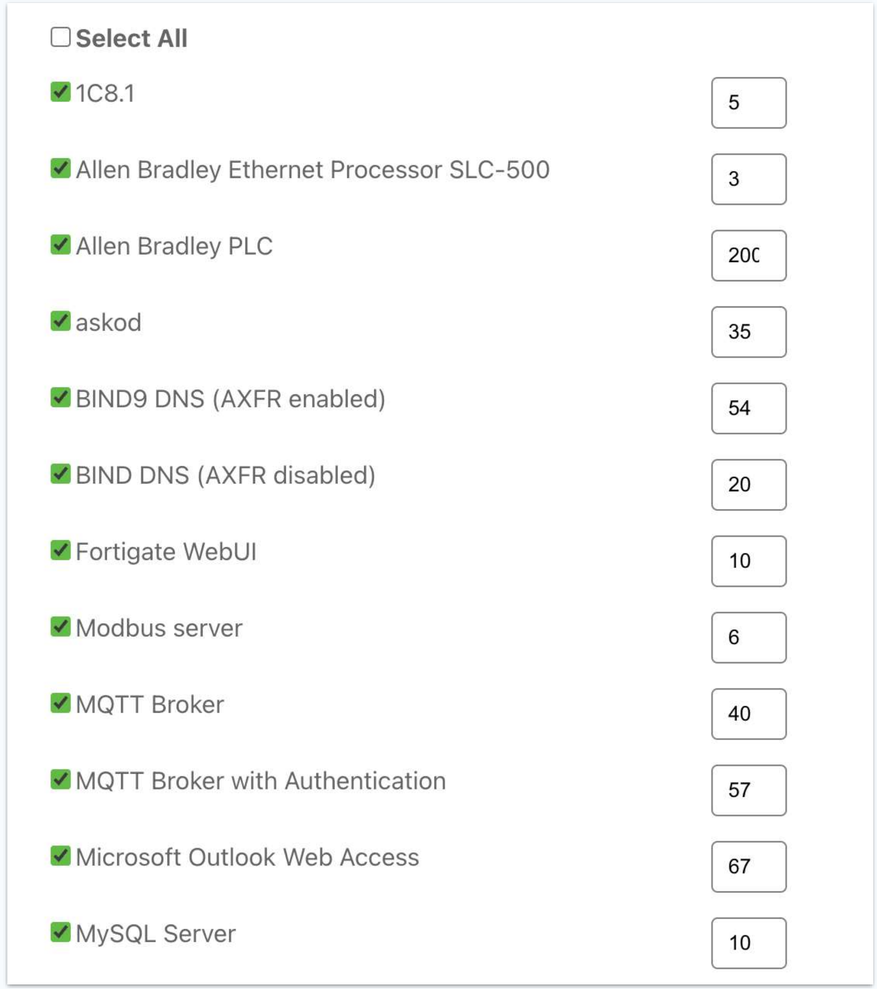
Różne opcje dostosowania wabików i nawigacji okruszkowej (breadcrumbs) – język, branża, domena, itp.

Multitenancy (model wielu najemców)

W pełni izolowanymi od siebie dzierżawcami można zarządzać z poziomu pojedynczej konsoli zarządzania, z obsługą RBAC.



KLUCZOWE KORZYŚCI



Nie tylko obraz istniejącej infrastruktury IT

Wabiki imitują podatne na ataki usługi i aplikacje, a nie tylko powielają prawdziwe zasoby IT / OT.

Nie wymaga dedykowanego urządzenia

Platforma oparta jest na maszynach wirtualnych, które można wdrożyć w dowolnym miejscu.

Nie opiera się na podejściu Full OS

Brak dodatkowych kosztów licencji na oprogramowanie firm trzecich, brak aliasów IP, lepsze imitacje wabików.

Brak osobnych alertów dla każdej interakcji

Labyrinth zapewnia zagregowane alerty pozwalające obniżyć liczbę zdarzeń do analizy.

Minimalizacja ręcznej konfiguracji

Wysoce zautomatyzowane procesy wdrażania i konfiguracji z minimalną liczbą czynności ręcznych.

KORZYŚCI BIZNESOWE

POWSTRZYMUJE WYRAFINOWANE ATAKI

Wykrywa i powstrzymuje ukierunkowane i zaawansowane ataki bez konieczności wcześniejszej znajomości formy, rodzaju lub zachowania zagrożenia.

BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

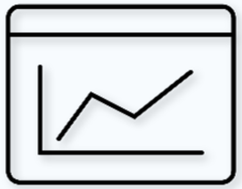
Brak negatywnego wpływu na wydajność urządzeń sieciowych, hostów, serwerów lub aplikacji.

PROSTE WDROŻENIE

Szybkie i łatwe wdrożenie, bez konfliktów systemowych i konieczności prac konserwacyjnych: brak baz danych, sygnatur lub reguł, które trzeba stale konfigurować i aktualizować.

WSPARCIE TECHNICZNE 12/7

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



REDUKCJA KOSZTÓW OPERACYJNYCH NAWET O 30% [1]

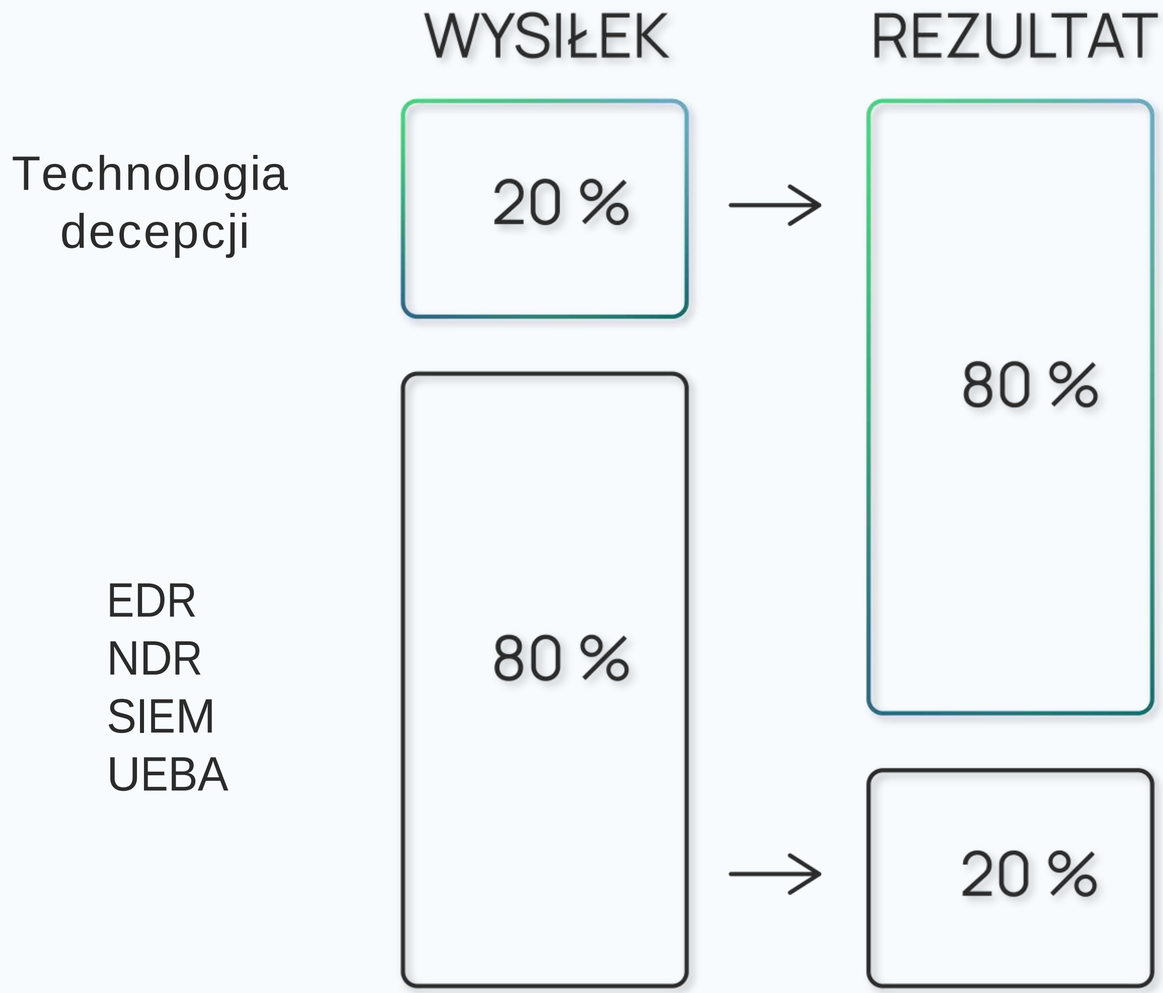
Nie gromadzi dużych ilości danych, nie generuje fałszywych alarmów i nie wymaga specjalnych umiejętności do obsługi.

ZAUTOMATYZOWANA REAKCJA

Przyspiesza reakcję na incydenty, skracając średni czas wykrywania zagrożeń i reagowania na nie (MTTD, MTTR) nawet 12-krotnie [2].

[1] https://www.enterprisemanagement.com/news/press_release.php?p_id=2659
[2] https://www.bloomberg.com/press-releases/2020-09-14/cyber-deception-reduces-data-breach-costs-by-over-51-and-soc-inefficiencies-by-32

KORZYŚCI BIZNESOWE



Natychmiastowe wykrywanie wszelkich działań atakującego

Przyjmuje atak, jednocześnie zyskując czas na podjęcie akcji dla zespołu ds. bezpieczeństwa (SOC)

Jasne i szczegółowe informacje o ataku i atakującym

Przetwarzanie logów, informacje o ruchu i przepływie danych w sieci

Dodatkowy kontekst

PRZYKŁADY WDROŻEŃ

STUDIUM PRZYPADKU 1

softserve

SoftServe to globalna firma informatyczna o ukraińskim rodowodzie. W portfolio posiada szeroką gamę usług świadczonych dla swoich klientów – inżynieria oprogramowania, big data i analityka, AI i ML, internet rzeczy, cyberbezpieczeństwo, platformy doświadczeń, rozszerzona rzeczywistość, robotyka, badania i rozwój.

SoftServe zatrudnia ponad 13 000 pracowników w 55 centrach rozwojowych, biurach i siedzibach klientów na całym świecie, z czego najwięcej w Europie Środkowej i Wschodniej.

Infrastruktura informatyczna SoftServe jest skoncentrowana na chmurze, a usługi świadczone są z rozproszonych centrów danych w Unii Europejskiej, Europie Środkowo-Wschodniej oraz USA.

STUDIUM PRZYPADKU 1

softserve

Wyzwania

- obniżenie ryzyka potencjalnych naruszeń i niechcianego dostępu
- zapewnienie i wdrożenie prawidłowego zestawu narzędzi reagowania dla wewnętrznego Cybersecurity Operation Center, aby poradzić sobie z potencjalnymi intruzami, którzy mogli już wejść do sieci (np. poprzez skompromitowaną maszynę wirtualną zainstalowaną na punkcie końcowym użytkownika korporacyjnego)

Realizacja

- platforma decepcji została wybrana do wdrożenia jako dodatkowy zestaw narzędzi ochrony
- pułapki zostały wdrożone na setkach serwerów w segmentach DMZ i LAN z tysiącami hostów
- skonfigurowanie zdarzeń detekcji oraz opracowanie scenariuszy dla zespołu CSOC w celu zapewnienia reakcji na potencjalne incydenty
- zbudowanie modelu behawioralnego dla usług i użytkowników w sieci, aby dopracować procedury reagowania i zmniejszyć liczbę fałszywych alarmów

STUDIUM PRZYPADKU 1

softserve

Rezultaty

- zaliczone zewnętrzne testy penetracyjne w połączeniu z działaniami purpurowych i niebieskich zespołów SoftServe – przyspieszona reakcja i odpowiedź zespołu CSOC na nieautoryzowany dostęp złośliwych podmiotów do zasobów korporacyjnych
- znaczna poprawa widoczności w odizolowanych segmentach sieci
- poprawa wykrywania błędów w konfiguracji sieci
- zidentyfikowanie istniejących naruszeń "polityki użytkowania sieci" i poprawa postawy bezpieczeństwa
- dostarczenie zestawu narzędzi do zbudowania typowego modelu behawioralnego i dostępu do różnych usług w sieci korporacyjnej
- poprawa możliwości analizy działań szpiegowskich
- łatwiejsze podejmowanie realnych decyzji podczas zarządzania incydentami i redukcja ilości fałszywych alarmów na platformie SIEM klienta

STUDIUM PRZYPADKU 2

ControlPay is now
Transporeon Freight Audit

Grupa Transporeon jest międzynarodowym przedsiębiorstwem logistycznym, zatrudniającym ponad 1000 pracowników w 21 lokalizacjach na całym świecie.

Aplikacje logistyczne oparte na chmurze zapewniają kompleksowe rozwiązania w zakresie zarządzania logistyką transportu – pełne portfolio usług dla załadowców, dostawców, sprzedawców detalicznych, odbiorców towarów i przewoźników.

STUDIUM PRZYPADKU 2

Wyzwania

- Usługa Transporeon Freight Audit usprawnia audyt frachtu i proces finansowania, umożliwiając uczestnikom uzyskanie prawdziwego obrazu ich operacji logistycznych w oparciu o jedno źródło zweryfikowanych i niepodważalnych danych. Ochrona danych jest kluczową kwestią dla tego typu działalności.

- ControlPay oczekiwał natychmiastowego zwiększenia widoczności infrastruktury firmy w zakresie bezpieczeństwa informacji, a także rozszerzenia możliwości wykrycia potencjalnie zaistniałego ataku, który mógł się przedrzeć przez zabezpieczenia brzegu sieci.

Realizacja

- Wdrożenie kilku pułapek typu UniversalWebPoint w strefie DMZ obok prawdziwych serwerów produkcyjnych i otwarcie dostępu do pułapek z poziomu sieci Internet (wektor pierwszy).

- Integracja zestawu pułapek (Points) w segmentach sieci: serwery deweloperskie i testowe oraz VLANy używane przez komputery kadry zarządzającej i działu finansowego spółki (wektor drugi).

- Całe wdrożenie systemu decepcji w infrastrukturze klienta zajęło mniej niż dwie godziny.

STUDIUM PRZYPADKU 2

Rezultaty

- Dla pierwszego wektora (DMZ) starania atakujących były nakierowane na bazę danych transakcji niedokończonych, podczas gdy klient zakładał, że głównym celem będzie baza danych firm korzystających z ich usług. W związku z tym przeprowadzono niezwłoczny przegląd kodu dla aplikacji internetowej powiązanej z bazą danych transakcji niedokończonych.

- Dla drugiego wektora odkryto, że skanowanie sieci LAN odbywa się z domowej stacji roboczej jednego z twórców oprogramowania u klienta, łączącego się przez VPN w czasie wolnym od pracy i przeprowadzającego rozpoznanie hostów znajdujących się w segmencie **dev/test.**
  Ponadto wykryto ataki siłowe (**bruteforce**) i próby wykorzystania luk (**exploity**) na usługi sieciowe, z dalszym działaniem wskazującym na eskalację uprawnień.
  Stacja robocza tego pracownika została odizolowana i przekazana do analizy kryminalistycznej.

- Wysoka skuteczność systemu decepcji Labyrinth w zakresie ochrony przed różnorodnymi cyberatakami.

STUDIUM PRZYPADKU 3

Otwarta Spółka Akcyjna „Koncern Galnaftogaz” jest właścicielem ponad 400 stacji paliw pod marką OKKO. Spółka zarządza również największą w kraju siecią zajazdów, obejmującą 35 restauracji, które działają pod markami A la minute, Pasta Mia i Meiwei.

Jednostki sieci OKKO prowadzą sprzedaż towarów poprzez sklepy na stacjach paliw, sprzedaż hurtową i detaliczną produktów naftowych oraz świadczą usługi w zakresie badania jakości paliw, magazynowania i transportu produktów naftowych.

Holding OKKO Group zrzesza ponad 10 przedsiębiorstw o różnych profilach działalności - produkcja, handel, budownictwo, ubezpieczenia, usługi. Europejski Bank Odbudowy i Rozwoju jest akcjonariuszem i inwestorem instytucjonalnym w spółkach holdingu.

STUDIUM PRZYPADKU 3

Wyzwania

- W wyniku testowania i modelowania zagrożeń, zastosowanego w różnych segmentach infrastruktury Klienta, zidentyfikowano słabe punkty w wykrywaniu zdarzeń w obrębie sieci firmowej.
- Ustalono, że wymagana jest dodatkowa warstwa ochrony na poziomie stacji roboczych w postaci wabików plikowych dla napastników, którzy już wcześniej uzyskali dostęp do stacji, na przykład poprzez atak phishingowy.
- Aby poprawić jakość badania incydentów, należało m.in. zmniejszyć czas reakcji SOC, przy jednoczesnym odwróceniu uwagi atakujących od rzeczywistych zasobów IT.

Realizacja

OKKO

- Zidentyfikowano krytyczne procesy biznesowe i wewnętrzne aplikacje internetowe, dla których stworzono na bazie UniversalWebPoint po kilka wabików sieciowych (honeypot'ów).
- Na hostach zaimitowano wiele różnych typów plików wabików w celu wykrycia atakującego na etapie poeksploatacyjnym (jeśli intruz uzyskałby dostęp do rzeczywistego hosta za pomocą phishing 'u, dostępu fizycznego, itp.).
- Skonfigurowano dwustronną integrację systemów SIEM i Labyrinth. Na podstawie tej integracji zostały opracowane dodatkowe procedury, rozmieszczone i sformalizowane do wykorzystania przez zespół SOC w procesach dochodzeniowym i reakcji na incydenty.

STUDIUM PRZYPADKU 3

OKKO

Rezultaty

- Zwiększenie widoczności w obrębie sieci firmowej w celu zidentyfikowania ewentualnych prób nieautoryzowanego dostępu oraz rozeznawania struktury i zawartości hostów w segmentach sieci.
- Ze względu na wykorzystanie funkcji imitacji aplikacji internetowych na bazie UniversalWebPoint, sekwencje działań atakujących na wewnętrznych aplikacjach web zostały wykryte i dokładnie sklasyfikowane.
- Na podstawie danych zebranych na platformie decepcji Labyrinth, znacznie wzrosła wartość informacyjna wykrytych incydentów, co doprowadziło do podjęcia szybszej decyzji zespołu ds. bezpieczeństwa (SOC) dla każdego z badanych przypadków.

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

LABYRINTH

Labyrinth to zespół doświadczonych inżynierów cyberbezpieczeństwa i testerów penetracyjnych, który specjalizuje się w opracowywaniu rozwiązań do wczesnego wykrywania cyberzagrożeń i zapobiegania im.

Znajdź nas:

Labyrinth Security Solutions

Labyrinth Deception Platform

https://labyrinth.tech

info@labyrinth.tech

LABYRINTH

DZIĘKUJEMY ZA UWAGĘ

ZAPRASZAMY DO BEZPŁATNYCH TESTÓW