LABYRINTH

CASE STUDY

O Kliencie

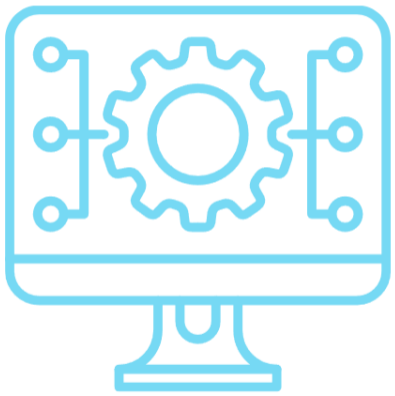
Klientem jest miejskie centrum informatyczne o ugruntowanej pozycji, które specjalizuje się w świadczeniu kompleksowych usług informatycznych i wsparcia dla różnych departamentów rządowych i instytucji publicznych w gminie. Obecnie firma zatrudnia prawie 50 osób i posiada ponad 800 urządzeń.

Infrastruktura klienta:

- do 520 hostów LAN
- do 100 podsieci VLAN

Wyzwanie

Po przeprowadzeniu audytu IT wyraźnie wskazano na niski poziom zarządzania zasobami i słabą widoczność w sieci LAN. Infrastrukturę IT dodatkowo komplikowała obecność sprzętu należącego do powiązanych struktur i organizacji. Proces monitorowania, wykrywania i reagowania na nietypowe zdarzenia w sieci LAN był skomplikowany ze względu na duże obciążenie pracowników i brak dedykowanych specjalistów bezpośrednio do tych zadań, ponieważ kierownictwo klienta zdecydowało się na reorganizację infrastruktury na dużą skalę.



Realizacja

Maszyna wirtualna Labyrinth Admin i 2 maszyny wirtualne Worker zostały wdrożone w segmencie zarządzania LAN na hiperwizorze VMware vSphere.

Agenci imitacji (Seeder) byli używani tylko z krytycznymi zasobami. Łączna liczba wabików plikowych przekroczyła 500.

Utworzono ponad 100 sieci Honeynet w celu hostowania wabików sieci Points odpowiedzialnych za określone sieci VLAN.

Rozwiązanie

Infrastruktura klienta została wypełniona wieloma różnymi typami wabików, aby stworzyć dużą liczbę wektorów ataku dla potencjalnego napastnika.

System cyber decepcji Labyrinth został zintegrowany z IPS i skonfigurowany do automatycznego izolowania hosta, z którego wykryto atak. Znacznie skraca to czas reakcji na atak i minimalizuje negatywne konsekwencje braku całodobowego monitorowania przez zespół SOC.

Rezultaty

Po wdrożeniu systemu Labyrinth wykryto i sklasyfikowano dużą ilość anomalnego ruchu. Źródło tego ruchu zostało zidentyfikowane i wyeliminowane z sieci. W oparciu o wyniki tych alertów stworzono kilka dodatkowych typów wabików sieciowych, aby pomóc w jeszcze szybszym wykrywaniu podobnych przypadków w przyszłości. Ogólnie rzecz biorąc, zarządzanie zasobami IT w sieci uległo znacznej poprawie.

O firmie Labyrinth

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

Platforma decepcji Labyrinth zmienia powierzchnię ataku, zapewniając iluzję rzeczywistej podatności infrastruktury.

Oparte na Punktach - inteligentnych imitacjach, które naśladują usługi, treści, routery, urządzenia, itp., rozwiązanie zapewnia kompleksową ochronę wszystkich możliwych wektorów ataku.

Platforma Labyrinth wabi atakujących w celu zaangażowania ich w tę fałszywą infrastrukturę, rejestrując każdy szczegół ich działań.

KLUCZOWE KORZYŚCI

- WCZESNE WYKRYWANIE ZAGROŻEŃ
- SPOWOLNIENIE CYBERATAKU
- ŁATWOŚĆ WDROŻENIA I UTRZYMANIA
- ELASTYCZNE OPCJE LICENCJONOWANIA

KLUCZOWE CECHY

- WDROŻENIE LOKALNE (ON-PREMISE)
- CENTRALNIE ZARZĄDZANE WABIKI IT/OT
- INTEGRACJE Z ROZWIĄZANIAMI FIRM TRZECICH
- OBSŁUGA WIELU PLATFORM
- MULTI-TENANCY DLA DUŻYCH LUB ROZPROSZONYCH ARCHITEKTUR

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

CISO CHOICE AWARD 2025
FINALIST