LABYRINTH

CASE STUDY

O Kliencie

Klientem jest globalna firma informatyczna, która 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.

Klient z powodzeniem zrealizował ponad 20 000 projektów na całym świecie i świadczy usługi dla wiodących na rynku podmiotów, takich jak Cisco, IBM, Allscripts, Atlassian, Coupa, Panasonic, Logitech i wielu innych.

Wyzwanie

Klient zatrudnia ponad 10 000 pracowników w ponad 50 centrach rozwojowych, biurach i siedzibach klientów na całym świecie, z czego najwięcej w Europie Środkowej i Wschodniej, i nie jest uzależniony od jednej konkretnej lokalizacji biura lub kraju, w którym prowadzi działalność. Infrastruktura informatyczna i bezpieczeństwa Klienta jest skoncentrowana na chmurze, a usługi świadczone są z rozproszonych centrów danych w Unii Europejskiej, Europie Środkowo-Wschodniej oraz USA.

W obliczu rosnących zagrożeń w cyber-przestrzeni na całym świecie, powinniśmy utrzymywać nasze standardy bezpieczeństwa na najwyższym poziomie, aby chronić nasze aktywa, dane współpracowników i klientów.

Wyzwaniem dla nas jest obniżenie ryzyka potencjalnych naruszeń i niechcianego dostępu.

Wymagane jest również 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

Funkcjonalność decepcji została wybrana do wdrożenia jako dodatkowy zestaw narzędzi ochrony. Konfiguracja pułapek powinna być zbliżona do istniejących zasobów dostępnych w sieci korporacyjnej.

Labyrinth Admin VM i Labyrinth Worker VM zostały wdrożone na setkach serwerów SoftServe w segmentach DMZ i LAN z tysiącami hostów.

Rozwiązanie

Wdrożenie systemu decepcji odbyło się zaledwie w kilku krokach:

1. Zidentyfikowanie odpowiedniej liczby pułapek na podstawie liczby aktywnych hostów w każdym segmencie sieci.
2. Zidentyfikowanie i zbadanie wszystkich rodzajów usług w każdym segmencie sieci.
3. Wdrożenie i skonfigurowanie pułapek (honeypots) na podstawie powyższych analiz.
4. Ustanowienie właściwego wykrywania i reagowania na incydenty w trybie 24/7. Skonfigurowanie wymaganych zdarzeń detekcji oraz opracowanie scenariuszy dla wewnętrznego zespołu CSOC w celu zapewnienia reakcji na potencjalne incydenty.
5. Zmniejszenie liczby fałszywych alarmów na naszej platformie SIEM. Zbudowaliśmy model zachowań usług i użytkowników w sieci, aby dopracować nasze procedury reagowania.

Rezultaty

Najważniejszym potwierdzonym rezultatem były zewnętrzne testy penetracyjne w połączeniu z działaniami purpurowych i niebieskich zespołów. Profesjonalni pentesterzy z jednej z najlepszych firm konsultingowych nie byli w stanie wykryć pułapek sieciowych, a nasz zespół CSOC miał możliwość przeanalizować odpowiednie zdarzenie bezpieczeństwa demonstrujące udaną pułapkę dla "hakerów".

Dodatkowo, wdrożenie technologii decepcji od Labyrinth okazało się realnym dodatkiem do istniejącego u nas zestawu narzędzi bezpieczeństwa:

- Znacznie poprawiliśmy naszą widoczność w odizolowanych segmentach sieci.
- Pomogło nam to zidentyfikować istniejące naruszenia "polityki użytkowania sieci" i poprawić naszą postawę bezpieczeństwa.
- Poprawiło nasze wykrywanie błędów w konfiguracji sieci.
- Przyspieszyło reakcję i odpowiedź zespołu CSOC na nieautoryzowany dostęp złośliwych podmiotów do zasobów korporacyjnych. Zostało to potwierdzone na podstawie wyników niezależnych testów penetracyjnych przeprowadzonych przez stronę trzecią.
- Dostarczyło nam zestawu narzędzi do zbudowania typowego modelu behawioralnego i dostępu do różnych usług w naszej sieci.
- Poprawiło nasze możliwości analizy działań szpiegowskich.

Na podstawie danych zebranych przez Labyrinth Deception Platform znacząco wzbogaciliśmy nasze możliwości reagowania na incydenty. Zebrane informacje przez Labyrinth stanowiły realne uzupełnienie dla naszego zespołu CSOC w zakresie wykrywania i zapobiegania incydentom cyberbezpieczeństwa. Łatwiejsze stało się podejmowanie realnych decyzji podczas zarządzania incydentami i nastąpiła redukcja fałszywych alarmów.