Labyrinth Deception Platform

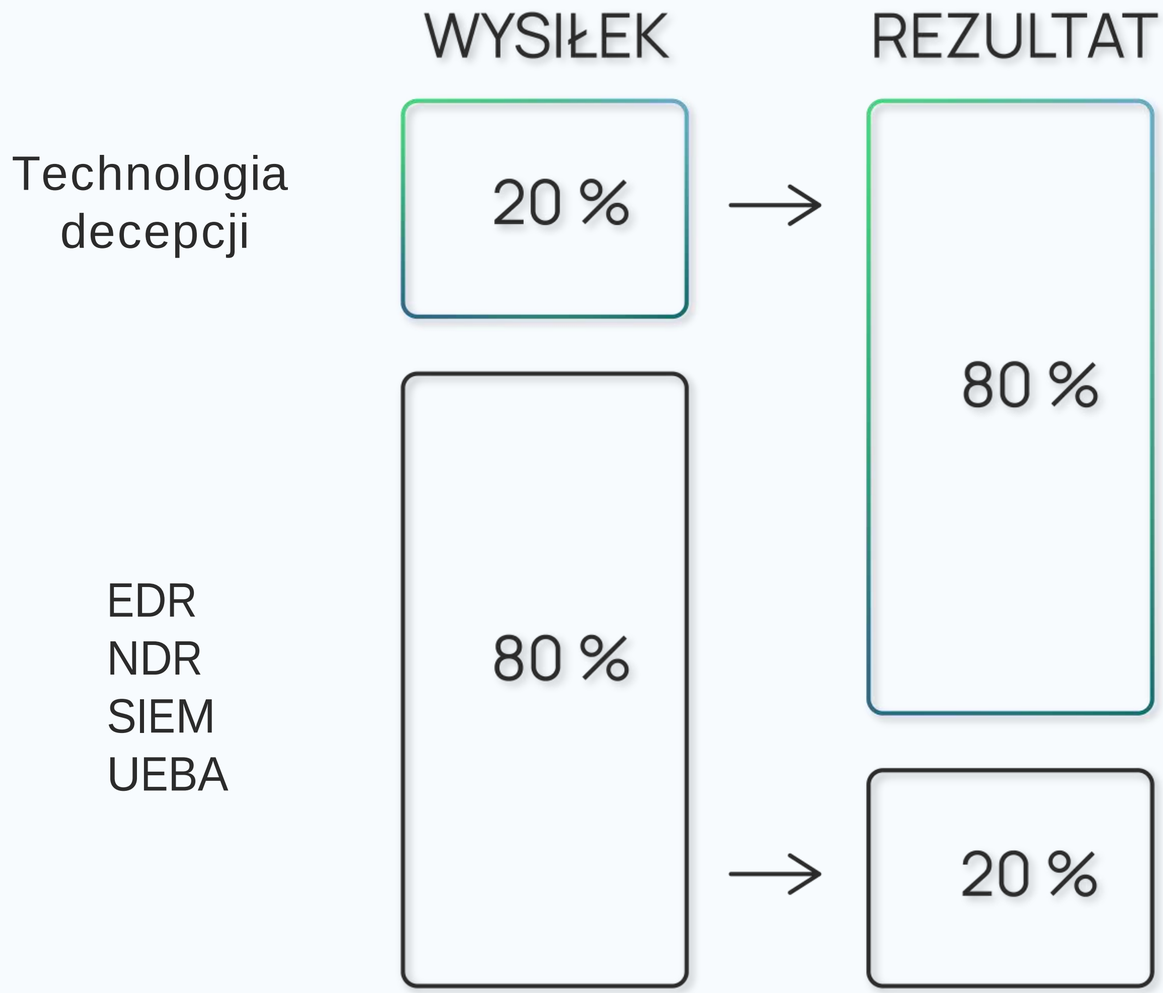
PRZYKŁADY WDROŻEŃ

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

Labyrinth Security Solutions, 2024

LABYRINTH

ROLA DECEPCJI W CYBERBEZPIECZEŃSTWIE



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

LABYRINTH

KORZYŚCI BIZNESOWE PLATFORMY DECEPCJI

POWSTRZYMUJE WYRAFINOWANE ATAKI

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

BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

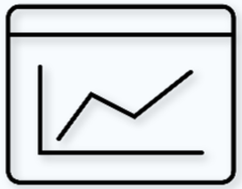
Brak negatywnego wpływu na wydajność urządzeń sieciowych, hostów, serwerów lub aplikacji.

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

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

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 u Klienta.

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

STUDIUM PRZYPADKU 2

Państwowa agencja Ukravtodor została utworzona jako korporacja państwowa w 1990 roku, zastępując Ministerstwo Dróg Ukrainy Radzieckiej jako państwowy organ zarządzający drogami samochodowymi we współczesnej Ukrainie.

Obecnie jest pod nadzorem Państwowej Agencji ds. Odbudowy i Rozwoju Infrastruktury Ukrainy.

Infrastruktura informatyczna klienta składa się z blisko 100 podsieci VLAN z około 750 stacjami roboczymi.

STUDIUM PRZYPADKU 2

Wyzwanie

- Infrastruktura Klienta składa się głównie z serwerów i różnych urządzeń sieciowych. Główną cechą jest to, że krytyczne zestawy hostów są rozproszone geograficznie.
- Wolumen interfejsów web był ogromny: na sprzęcie sieciowym i specjalistycznym oprogramowaniu stworzonym dla tej firmy.
- Klient oczekiwał zwiększenia widoczności działań atakujących w odniesieniu do wszelkiego rodzaju aplikacji / usług sieciowych w jego infrastrukturze.

Realizacja

- Agenty imitujące zostały rozesłane do większości serwerów przy użyciu systemu orkiestracji używanego przez Klienta. Całkowita liczba przynęt plikowych wynosi ponad 4500.
- Utworzono ponad 55 sieci Honeynet do hostowania przynęt sieciowych dla ochrony podsieci VLAN.
- Szczególną uwagę zwrócono na propagację różnych wabików sieciowych w segmencie DMZ. Wabiki sieciowe w tej części sieci są najczęściej regenerowane, aby środowisko nie wyglądało statycznie. Odnawianie to trwa do trzech minut.

STUDIUM PRZYPADKU 2

Rezultaty

- Wabiki sieciowe w segmencie DMZ umożliwiły zbieranie informacji, które pozwoliły poprawić ustawienia ochrony infrastruktury na brzegu sieci firmowej.
- Wdrożenie systemu decepcji znacząco podniosło poziom wykrywalności zdarzeń intranetowych, co potwierdziły testy penetracyjne przeprowadzone po wdrożeniu systemu.
- System wykazał wysoką skuteczność w trakcie testów penetracyjnych, zabierając atakującym dużo czasu i rozpraszając ich wieloma przynętami sieciowymi, rozsianymi po podsieciach Klienta.
- Efektem ubocznym z zastosowania systemu Labyrinth były wykrycia związane z zasobami shadow IT w postaci zapomnianych skanerów bezpieczeństwa i oprogramowania do zarządzania zasobami.

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

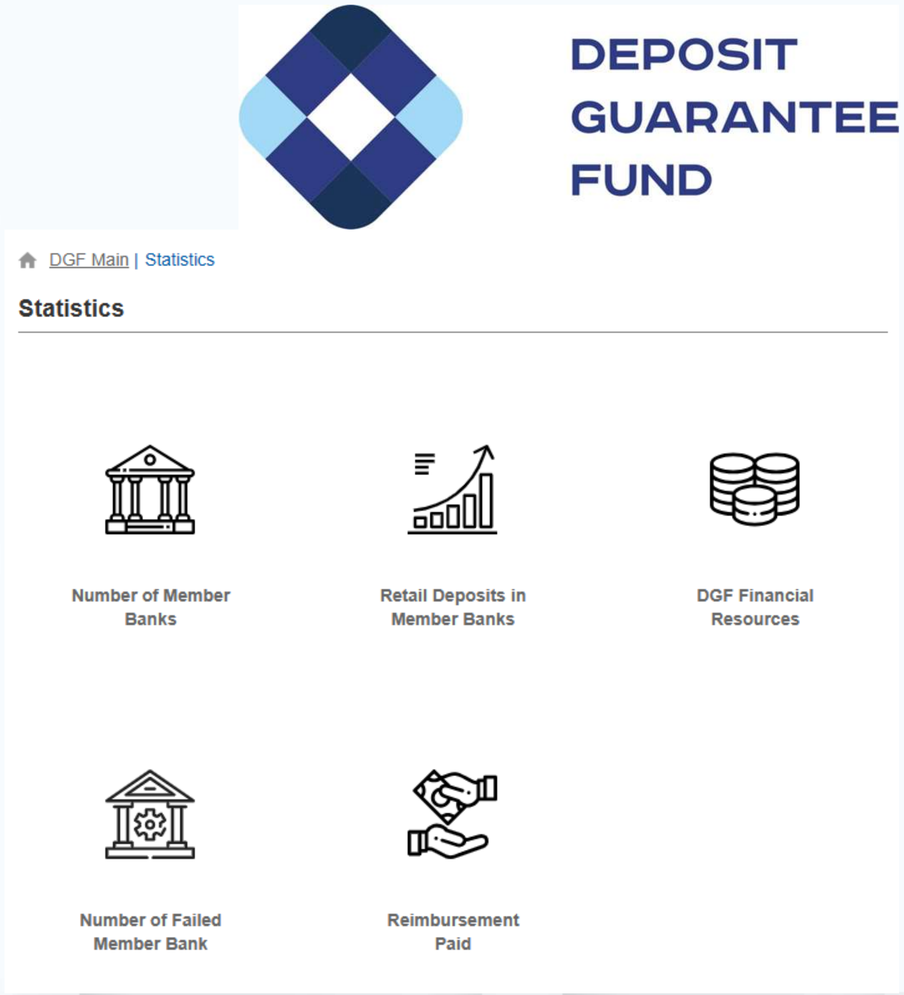
УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

STUDIUM PRZYPADKU 3



Fundusz Gwarancyjny Depozytów (DGF) to instytucja w Ukrainie, która pełni specjalne funkcje w zakresie gwarantowania depozytów osób fizycznych i usuwania niewypłacalnych banków z rynku.

Główne funkcje DGF:

- gromadzi środki oraz monitoruje kompletność i terminowość przekazywania opłat przez każdego członka Funduszu,
- podejmuje działania w celu zorganizowania wypłaty rekompensat depozytowych w przypadku decyzji o cofnięciu licencji bankowej i likwidacji banku,
- reguluje uczestnictwo banków w systemie gwarantowania depozytów,
- podejmuje działania mające na celu ochronę praw i prawnie chronionych interesów deponentów oraz podnoszenie poziomu wiedzy finansowej społeczeństwa.

STUDIUM PRZYPADKU 3

Wyzwania

- Duże ilości danych związanych z informacjami finansowymi wielu banków i podmiotów prawnych stanowią kuszący cel ataku, zwłaszcza w czasie wojny.
- Duża liczba serwerów z systemem MS Windows. Większość stacji roboczych również korzystała z systemu MS Windows w różnych wersjach.
- Oprogramowanie opracowane specjalnie dla Funduszu i współdzielone przez agencje rządowe - Trembita i Ascod.
- Zmniejszenia ryzyka potencjalnych włamań i nieautoryzowanego dostępu do sieci LAN oraz poprawy zdolności wykrywania ataków w sieci.

Realizacja

- Na 25% stacji roboczych i na wszystkich dostępnych serwerach Windows utworzono ok. 10 000 wabików plikowych, które dynamicznie zmieniają się po wprowadzeniu zmian w wabikach sieciowych.
- Stworzono dużą liczbę wabików sieciowych, które imitowały hosty Windows oraz symulowały zachowania użytkowników: surfowanie po sieci, dostęp do udziałów SMB, zapytania DNS, itp.
- W segmencie serwerów wdrożono wabiki imitujące VMware ESXi i Ascod. Oprócz nich stworzono imitacje wszystkich usług sieciowych przy użyciu wabików UniversalWebPoint (w tym interfejsów webowych wszystkich urządzeń Cisco).

STUDIUM PRZYPADKU 3

Rezultaty

- Wdrożenie systemu pozwoliło poprawić wykrywanie prób ataków typu MiTM (man-in-the-middle) i wykorzystania danych uzyskanych z ruchu do przeprowadzenia dalszych ruchów bocznych.
- Wykrywanie ataków na systemie decepcji było znacznie łatwiejsze niż korzystanie z systemu SIEM z wieloma regułami korelacji dla podobnych zadań.
- Po wdrożeniu wabików sieciowych, które emulowały wszystkie istniejące usługi sieciowe, zadanie atakującego, polegające na niezauważonym poruszaniu się po infrastrukturze Klienta, stało się niemożliwe do wykonania.

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

STUDIUM PRZYPADKU 4

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 4

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 4

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.

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

STUDIUM PRZYPADKU 5

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 5

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 dochodzeniowych i reakcji na incydenty.

STUDIUM PRZYPADKU 5

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

STUDIUM PRZYPADKU 6

Ukraińska firma farmaceutyczna.

Portfolio produktów obejmuje zarówno generyczne, jak i oryginalne produkty lecznicze w 11 z 14 grup farmakoterapeutycznych.

Firma zatrudnia ponad 2 300 pracowników w kilku spółkach i zakładach produkcyjnych.

Infrastruktura informatyczna klienta składa się z blisko 80 sieci VLAN z liczbą 900 użytkowników stacji roboczych.

STUDIUM PRZYPADKU 6

Wyzwanie

- U Klienta system antyspamowy przetwarza wiadomości przychodzące w oparciu o sygnatury i konieczne było dodanie kolejnej warstwy ochrony, która byłaby odpowiedzialna za wykrywanie udanych ataków phishing 'owych i nie opierałaby się na sygnaturach.

Realizacja

- Agenty imitujące były dystrybuowane na wszystkich stacjach roboczych przy użyciu systemu orkiestracji używanego przez Klienta. Dla każdej stacji roboczej wygenerowano co najmniej 20 wabików plikowych, z których każdy wskazywał jeden lub więcej wabików sieciowych.
- Imitacje DBMS i aplikacji webowych dla segmentów sieci zawierających krytyczne zasoby IT.
- Zintegrowano platformę decepcji z systemem SIEM w celu wzbogacenia kontekstu wykrywanych zdarzeń oraz dwukierunkowej wymiany informacji.

STUDIUM PRZYPADKU 6

Rezultaty

- Wykryto kilka przypadków obejścia przez atakującego systemu analizy sygnatur wiadomości e-mail i uzyskania dostępu do stacji roboczych.
- Zebrano niezbędne informacje o stacji roboczej, która miała pomóc zdobyć przyczółek i rozwinąć atak w głąb sieci. Intruzi zostali ujawnieni za pomocą informacji z wabików plikowych znalezionych na hostach, które wskazywały na imitacje baz danych.
- Zastosowanie platformy decepcji pozwoliło na uzyskanie dłuższego czasu na reakcję dla zespołu ds. bezpieczeństwa (SOC).

WYBRANI KLIENCI I RECENZJE

softserve

ControlPay

ПОЛІГРАФКОМБІНАТ УКРАЇНА

OKKO

OCTAVA DEFENCE

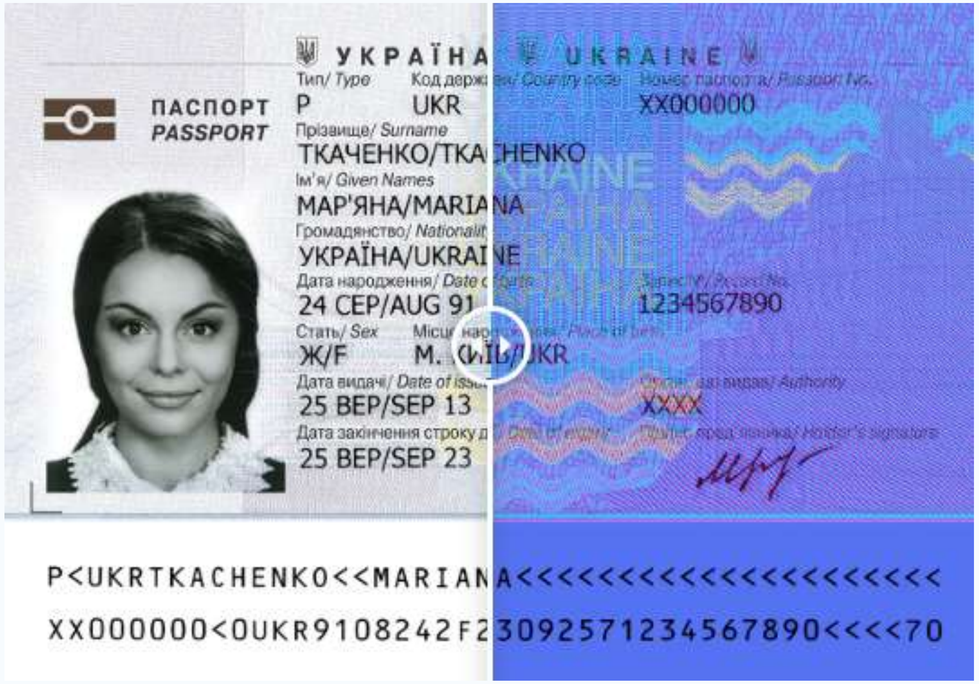
УКРАВТОДОР

RECENZJE

Gartner Peer Insights™

G2

STUDIUM PRZYPADKU 7



Przedsiębiorstwo Państwowe "Kombinat Poligraficzny "Ukraina" do produkcji papierów wartościowych" od wielu lat utrzymuje pozycję lidera w produkcji dokumentów identyfikacyjnych, formularzy papierów wartościowych, bezpiecznych produktów poligraficznych, itp.

Oferuje szeroką gamę produktów: paszporty, dokumenty tożsamości, karty bankowe, wszelkiego rodzaju znaczki (w tym znaczki akcyzowe i pocztowe), dyplomy, certyfikaty i inne dokumenty bezpieczeństwa.

Przedsiębiorstwo Państwowe "Kombinat Poligraficzny "Ukraina" do produkcji papierów wartościowych" jest również oficjalnym przedstawicielem Ukrainy w Katalogu Klucza Publicznego ICAO (ICAO PKD).

STUDIUM PRZYPADKU 7

Wyzwania

- Uzyskanie maksymalnej widoczności zdarzeń w ramach sieci firmowej (brak innych narzędzi w tamtym czasie).
- Wykrywanie anomalii w działaniach pracowników, zwłaszcza łączących się z siecią firmową przez tunele VPN w czasie pandemii.
- Zebranie większej ilości danych o segmencie DMZ i hostach wchodzących w interakcję z nim.
- Istotne było również zabezpieczenie dostępu do systemu elektronicznego zarządzania dokumentami Askod w obrębie sieci Klienta.

Realizacja

ПОЛІГРАФКОМБІНАТ УКРАЇНА

- Wdrożono szereg pułapek typu UniversalWebPoint w strefie DMZ, imitujących prawdziwe usługi w tym segmencie sieci oraz pułapek imitujących usługi zdalnego dostępu: ssh, rdp, rest-api.
- W ramach segmentu zarządzania firmą zastosowano dwa rodzaje pułapek: jeden dla systemu Ascod, a drugi dla symulacji stacji roboczych z użyciem usług rdp, wmi, ssh, netbios, itp.
- Sieć LAN została wypełniona punktami imitującymi różne magazyny plików: ftp, sftp, samba, nfs, webdav. Powstały też symulacje różnych baz danych.
- Na krytycznych hostach ulokowano wiele przynęt (breadcrumbs).

STUDIUM PRZYPADKU 7

ПОЛІГРАФКОМБІНАТ УКРАЇНА

Rezultaty

- Po wdrożeniu systemu można było wykryć anomalne zachowanie oprogramowania w segmencie DMZ, co było wynikiem błędnej konfiguracji.
- Przypadki nieautoryzowanego użycia zasobów sieci LAN przez użytkowników, którzy łączyli się z siecią firmową poprzez VPN z powodu kwarantanny, zostały zidentyfikowane i zbadane.
- Na jednej ze stacji roboczych zostały zidentyfikowane podejrzane skrypty, które skanowały sieć i przeprowadzały ataki typu **bruteforce** na usługach **ssh** i **rdp**.
- Przed wdrożeniem platformy Labyrinth w obrębie sieci Klienta, nie używano żadnego narzędzia zwiększającego widoczność działań użytkowników i oprogramowania sieciowego. Wdrożenie pozwoliło na znaczną poprawę widoczności w tym zakresie i szybszą reakcję na incydenty.

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