IstroSec

Arkusz danych

Threat Hunting oraz ocena zagrożenia

Threat Hunting polega na aktywnym wyszukiwaniu podejrzanej aktywność lub pozostałości jakiejkolwiek potencjalnej złośliwej aktywności w infrastrukturze klienta. Obecnie atakujący i ich wysiłki zmierzające do penetracji docelowej infrastruktury są coraz bardziej wyrafinowane. Ich ataki są często pomijane przez nowoczesne rozwiązania komercyjne, takie jak EDR czy AV, aż w końcu będzie za późno.

> *Skupiamy się na działaniach, które mogą sygnalizować obecność złośliwych podmiotów, potencjalnych słabościach systemów, złych nawykach IT, takich jak niepotrzebne uprawnienia administratora, hasła w postaci zwykłego tekstu itp.*

Warunki wstępne

- Dostęp do SIEM, EDR lub innych kolektorów logów
- Możliwość wykonywania zapytań o dane dotyczące punktów końcowych
- Dostęp do odczytu i możliwość pracy z logami urządzeń końcowych
- Opcjonalnie: Wcześniejsze wyniki testów penetracyjnych, audytów, incydentów itp.

Podstawowe usługa Threat Hunting zawiera:

- Sprawdzanie IoC w komunikacji sieciowej (jeśli to możliwe).
- Zautomatyzowana kontrola kluczowych systemów klientów, jeżeli zawierają niektóre IOC z bazy danych IstroSec.
- Opracowanie planu Threat Hunting w oparciu o standardowe ataki na dany rodzaj organizacji klienta, dodatkowa usługa - rozwój Customer Threat Landscape.
- Identyfikacja i analiza możliwych źródeł danych istotnych dla opracowanego planu.
- Automatyczna kontrola dzienników punktów końcowych i określanie podejrzanych zdarzeń.
- Tworzenie i inwentaryzacja programów Klienta, ich wersji, podatności dla tych wersji (jeśli jest to możliwe za pomocą narzędzi Klienta).
- Dostęp do odpowiednich źródeł danych (w ramach wdrożonych technologii lub wdrożenie naszych narzędzi).
- Podstawowa identyfikacja outlierów w infrastrukturze Klienta.

Pełna usługa Threat Hunting zawiera również:

- Konsultacje w oparciu o możliwości klientów i zaproponowanie wdrożenia darmowych/komercyjnych narzędzi do monitoringu.
- Pomoc we wdrożeniu narzędzi monitorujących w infrastrukturze Klienta oraz ich początkowym ustawieniu w oparciu o potrzeby Klienta.
- Szczegółowa ręczna analiza wyników narzędzia monitorującego.

Elementy dostarczane:

- Raport zawierający streszczenie, szczegóły techniczne i zalecane działania dotyczące zidentyfikowanych problemów
- Kwerendy używane do aktywnego poszukiwania zagrożeń.

IstroSec

Dlaczego my?

Doświadczenie i wiedza

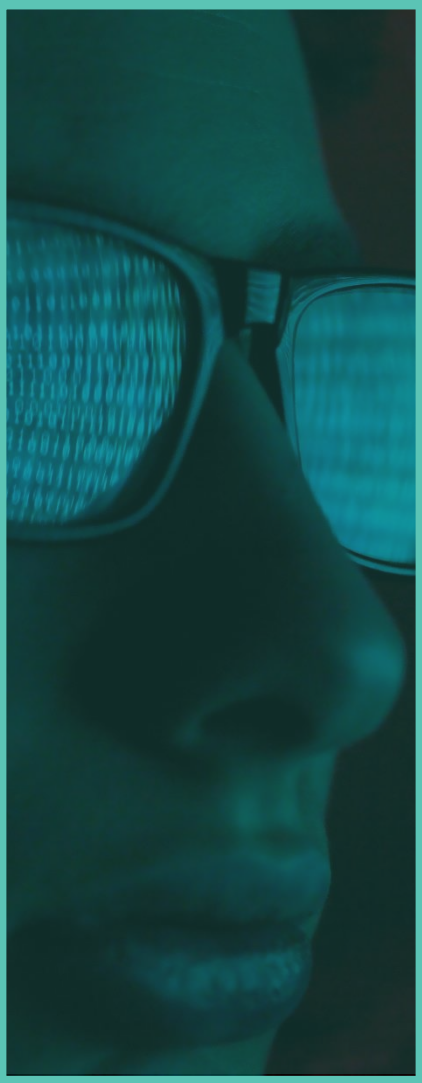
Specjaliści IstroSec mają doświadczenie w aktywnym poszukiwaniu zagrożeń przy użyciu różnych komercyjnych, bezpłatnych i zastrzeżonych narzędzi. Ponadto mają doświadczenie z atakującymi od poziomu script kiddie aż po państwowe grupy APT. Znają taktykę, techniki i procedury atakujących oraz posiadają wiedzę niezbędną do podejmowania decyzji w oparciu o dane o aktualnych cyberzagrożeniach.

Ekspertyza w threat huntingu

Specjalistyczna wiedza w zakresie threat hunting oraz wielu innych obszarach, takich jak reakcja na zdarzenia, analiza kryminalistyczna czy światowej klasy analiza złośliwego oprogramowania, którą wielokrotnie wykazali się nasi specjaliści podczas radzenia sobie z cyberatakami wspieranymi przez państwo, atakami na organizacje z listy Fortune 500, a także udział czterech ekspertów IstroSec w zwycięskim zespole ćwiczenia Locked Shields 2016.

Certyfikowani profesjonaliści

Eksperci **Istro**Sec są również posiadaczami uznanych na całym świecie certyfikatów w tych dziedzinach. Posiadamy certyfikaty takie jak Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) i inne.



Studium przypadku

Rodzaj firmy: Organizacja działająca w sektorze wrażliwym na ataki

Świadczone usługi: Threat hunting

Rozwiązanie: Ocena zagrożenia i wprowadzenie threat hunting po opublikowaniu informacji o luce typu zero-day.

Producent jednego z wdrożonych produktów oprogramowania wydał ostrzeżenie o poważnej luce zero-day. Istnieją oznaki bieżącego wykorzystywania tej luki przez atakujących w celu naruszenia infrastruktury. Zespół zajmujący się aktywnym wyszukiwaniem zagrożeń **Istro**Sec został poinstruowany, aby zweryfikować, czy organizacja została naruszona. W związku z tym zespół zebrał dostępne dane dotyczące luk w zabezpieczeniach od dostawcy oraz ze źródeł w społeczności zajmującej się bezpieczeństwem IT, aby określić strategię poszukiwania zagrożeń i wskaźniki kompromitacji, które były punktem wyjścia do poszukiwania zagrożeń. Zespół zmapował środowisko klienta z naciskiem na identyfikację dostępnych źródeł informacji o tym, co dzieje się w infrastrukturze, takich jak logi podatnych aplikacji, logi ruchu sieciowego, logi z lokalnego serwera DNS, logi systemowe urządzeń oraz logi wdrożonych rozwiązań SIEM. W logach aplikacji zawierającej lukę znaleziono zapisy błędów zgodne z próbami wykorzystania luki.

Na podstawie korelacji czasu w dziennikach komunikacji sieciowej zidentyfikowano podejrzane połączenia. Reputacja źródłowych adresów IP została sprawdzona pod kątem źródeł analizy zagrożeń, ale żaden zapis nie był jeszcze dostępny. Pełny zapis (full-packet capture) komunikacji sieciowej nie był dostępny. Jednocześnie analiza statystyczna ruchu sieciowego wykazała, że urządzenie zaczęło wykonywać więcej zapytań DNS niż przed momentem podejrzanej aktywności, co mogło wskazywać na beaconing i utworzony kanał C2 przez atakującego. Rozwiązanie EDR zostało operacyjnie zainstalowane na urządzeniu z podejrzaną aktywnością, aby pomóc zidentyfikować proces beacon i uzyskać próbki powiązanych plików.

Zespół zalecił zgłoszenie incydentu związanego z bezpieczeństwem i wezwanie analityków kryminalistycznych i złośliwego oprogramowania. Usługa threat hunt nadal odgrywała pomocniczą rolę w rozwiązaniu incydentu. Podejrzane adresy IP zostały zablokowane w zaporze obwodowej (firewall). Analiza złośliwego oprogramowania zidentyfikowała próbki jako sygnał nawigacyjny DNS z pakietu CobaltStrike. Analiza kryminalistyczna ujawniła działania mające na celu kradzież danych logowania sprzed wdrożenia na urządzeniu rozwiązania EDR. W ramach trwającego threat hunting sprawdzano w dziennikach SIEM aktywność wszystkich kont użytkowników znalezionych na zabezpieczonym urządzeniu. Okazało się, że jedno konto administratora logowało się po włamaniu na kilka serwerów wewnętrznych, a sam użytkownik nie potwierdził takiej aktywności. Na tej podstawie zalecono zmianę wszystkich haseł użytkowników i zresetowanie usługi Kerberos w fazie przechowawczej incydentu.

IstroSec | Černyševského 10 | 851 01 Bratysława | Słowacja| +421 917 699 002 | info@istrosec.com | www.istrosec.com