IstroSec

Arkusz danych

Wywiad obronny

W dzisiejszych czasach najcenniejszym dobrem organizacji są dane. Osoby atakujące są również świadome tego faktu, co odzwierciedla się w ekspansji różnych nielegalnych rynków i półpublicznych forów internetowych, które handlują danymi osobowymi i firmowymi. Monitorując te rynki i fora, można dowiedzieć się, na jakich atakach koncentruje się obecnie większość nielegalnej społeczności hakerskiej, jakie luki są atakowane i jakie dane zostały już wykorzystane przez atakujących (dokumenty wewnętrzne, dane użytkownika itp.).

> *Powierzając monitorowanie tych działań i danych o Twojej organizacji ekspertom IstroSec, będziesz informowany o aktualnych atakach istotnych dla Twojej organizacji, podatnościach na zagrożenia i sposobach ograniczania potencjalnego ryzyka.*

Rodzaje wywiadu

Ukierunkowany threat intelligence. Zestaw odpowiedni dla organizacji klienta danych wywiadowczych stanowiących wystarczającą podstawę do działania. Eksperci **Istro**Sec świadczą kompleksowe usługi od analizy wymagań, dostarczania danych o zagrożeniach umożliwiających podjęcie dalszych działań i wdrażania konsumentów w organizacjach docelowych

Monitorowanie wycieków. Eksperci **Istro**Sec będą monitorować clear web, deep web oraz dark web pod kątem wycieków z organizacji klientów.

Briefing dot. zagrożeń Eksperci **Istro**Sec przygotują raport wywiadowczy dla kierownictwa najwyższego i/lub średniego szczebla dotyczący aktualnych zagrożeń i wykorzystywanych podatności istotnych dla profilu zagrożeń organizacji

Usługa obejmuje:

- Monitorowanie wycieków danych do clear, deep oraz dark web
- Zapewnienie kanału informacyjnego istotnego dla organizacji, zawierającego aktualne informacje o zagrożeniach cybernetycznych w odpowiednich wertykałach
- Dostarczanie praktycznych informacji o zagrożeniach umożliwiających podjęcie dalszych działań
- Przygotowanie raportu dla wyższej i średniej kadry zarządzającej, zawierającego listę aktualnych zagrożeń i wykorzystywanych podatności na zagrożenia istotnych dla organizacji

Raport zawiera:

- Informacje o podatnościach na zagrożenia i sposobach ich naprawy, a przynajmniej złagodzenia ryzyka włamania, jeśli poprawka nie jest jeszcze dostępna
- Dane organizacji, które wyciekły do internetu
- Przegląd grup APT skupiających się na branży, w której działa organizacja oraz sposoby ograniczania ryzyka narażenia ze strony tych grup
- Wskaźniki kompromitacji
- Taktyka, techniki i procedury używane przez atakujących
- Rekomendacje narzędzi, konfiguracji i innych środków zapobiegających bieżącym zagrożeniom

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

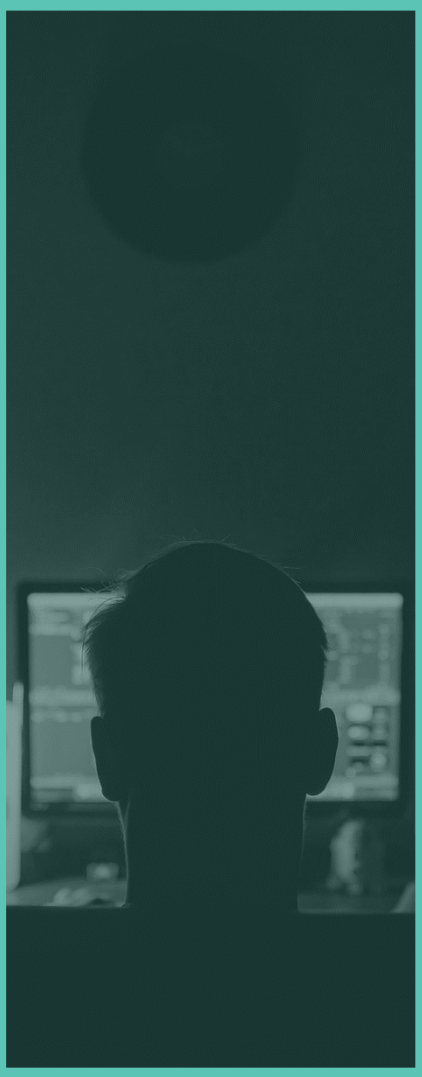
Specjaliści **Istro**Sec mają doświadczenie w wyszukiwaniu, przetwarzaniu i analizie danych dotyczących zagrożeń cyberbezpieczeństwa. Znają taktykę, techniki i procedury atakujących oraz posiadają wiedzę niezbędną do podejmowania decyzji podczas reagowania na incydenty w oparciu o dane o aktualnych cyberzagrożeniach.

Specjalistyczna wiedza z zakresu wywiadu

Specjalistyczna wiedza w zakresie wywiadu 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 zwycięstudniaskim zespole ćwiczenia Locked Shields 2016.

Certyfikowani profesjonaliści

Eksperci IstroSec 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: Producent w branży elektrycznej

Świadczone usługi: Wywiad

Rozwiązanie: Monitorowanie forów hakerskich online

Na GitHubie pojawiła się luka w zabezpieczeniach, która została naprawiona w aktualizacji z poprzedniego tygodnia. Była to luka, dzięki której można było uzyskać uprawnienia na poziomie systemu. Na forum hakerskim opublikowano wpis dotyczący luki, a także listy urządzeń, na których można ją wykorzystać. Zazwyczaj atakujący wybierają ofiary na podstawie stosunku intensywności ataku do potencjalnego zysku. Często zaczynają od przejrzenia listy organizacji, których dane zostały już naruszone i których są swobodnie dostępne w dark webie. Zakładają, że jeśli dane organizacja zostały raz naruszona, jej praktyki w zakresie cyberbezpieczeństwa nie są zbyt dojrzałe. Następnie zaczynają przygotowywać nowo opublikowaną lukę do wykorzystania przeciwko takiej organizacji.

W ramach monitorowania takich forów hakerskich i innych zasobów zespół **Istro**Sec zaobserwował, że liczba zgłoszeń o tej luce oraz liczba potencjalnych ofiar wzrasta. Analityk w **Istro**Sec porównał dane klientów w bazie danych i stwierdził, że jeden z naszych klientów używa systemów podatnych na tego typu ataki.

Klient został powiadomiony, przygotowano również raport o zagrożeniu. Raport zawierał:

- Informacje o podatnościach na zagrożenia i sposobach ich naprawy, a przynajmniej złagodzenia ryzyka włamania, jeśli poprawka nie jest jeszcze dostępna
- Dane organizacji, które wyciekły i pojawiły się na stronie
- Przegląd grup APT skupiających się na branży, w której działa organizacja oraz sposoby ograniczania ryzyka narażenia ze strony tych grup