IstroSec

Arkusz danych

Zarządzanie obroną

W dzisiejszych czasach, podczas rosnącej liczby ransomware, phishingu i innych złośliwych działań, stale rośnie potrzeba systematycznego i ciągłego monitorowania infrastruktury IT organizacji. Nasze usługi monitorowania cyberbezpieczeństwa obejmują czynności, które są zwykle wykonywane przy użyciu rozwiązań z zakresu cyberbezpieczeństwa dostarczających analizy i generujących raporty.

Usługa obejmuje:

- Monitorowanie sieci - IDS i IPS
- Monitorowanie procesów końcowych - EDR
- Zbieranie i korelacja logów - narzędzia SIEM
- Automatyzacja procesów śledczych i reaktywnych - narzędzia SOAR

Dlaczego IstroSec?

Łącznie ponad 70 lat doświadczenia

Dostęp do ekspertów ze wszystkich dziedzinach bezpieczeństwa informacji, w tym testerów penetracyjnych, analityków kryminalistycznych, analityków złośliwego oprogramowania, trenerów i nie tylko

Systematyczna poprawa bezpieczeństwa informacji według frameworków wzbogaconych doświadczeniem ekspertów IstroSec z zaawansowanymi incydentami bezpieczeństwa

Certyfikowani eksperci w celu zapewnienia zgodności z normami i przepisami bezpieczeństwa - eksperci IstroSec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

> *Delegowanie tych działań do wyspecjalizowanego zespołu SOC pozwala skoncentrować się na pracy i podnosi jej jakość oraz sprawia, że operacja monitorowania jest bardziej dostępna.*

Poziomy usług

- **L1** - Monitorowanie i podstawowa analiza raportów generowanych z narzędzi monitorujących
- **L2** - Zaawansowana analiza alertów w ramach narzędzi monitorujących
- **L3** - Dogłębna analiza podejrzanej aktywności bezpośrednio na zaatakowanym urządzeniu, pozyskiwanie i analiza danych ze źródeł spoza narzędzi monitorujących

Możliwe oceny dotyczące analizowanej aktywności

- **Złośliwa** – aktywność została potwierdzona jako złośliwa
- **Podejrzana** – aktywność może zostać zinterpretowana jako złośliwa lub potencjalnie niepożądana w określonych warunkach. Kluczowy jest kontekst aktywności dostarczony przez klienta.
- **Nieszkodliwa** – aktywność była skorelowana z nieszkodliwą, a raport narzędzia do monitorowania był fałszywie pozytywny

IstroSec

Arkusz danych

Warunki wstępne

L1

- Klucze API umożliwiające zbieranie danych z narzędzi monitorujących
- Dostęp do narzędzi monitorowania bezpieczeństwa infrastruktury klienta
- Kontakty eskalacyjne po stronie klienta

L2

- Prawo do wykonywania zapytań, odczytywania i agregowania logów z urządzeń
- Dostęp do narzędzi monitorowania bezpieczeństwa infrastruktury klienta
- Kontakty eskalacyjne po stronie klienta

L3

- Dostęp administratora do punktów końcowych klienta, chyba że wdrożono narzędzie EDR o równoważnej funkcjonalności
- Kontakty eskalacyjne po stronie klienta

Pakiet Usług

Pakiet 1

- Monitorowanie 8/5 i analiza alertów z narzędzi monitorujących na poziomach L1, L2 i L3
- Zgłaszanie klientowi ocen „złośliwa" i „podejrzana"
- Ostrzeganie klienta w przypadku wewnętrznych eskalacji do L3 niezależnie od ostatecznej opinii

Pakiet 2

- Pomoc doraźna 8/5 przy eskalacji L2 i wyższych oraz ich analiza
- Eskalacja wewnętrzna do L3, w razie potrzeby
- Informacja zwrotna dla klienta dotycząca oceny

Pakiet 3

- Pomoc doraźna 8/5 przy eskalacji L3 i wyższych oraz ich analiza
- Informacja zwrotna dla klienta dotycząca oceny

Wszystkie pakiety zawierają:

- Regularne raportowanie aktywności poprzez comiesięczny raport podsumowujący

Opcjonalnie dla każdego pakietu:

- Zarządzanie obsługiwanymi narzędziami programowymi do monitorowania cyberbezpieczeństwa
- Sprawdzenie konfiguracji ad hoc obsługiwanych narzędzi do monitorowania cyberbezpieczeństwa
- Pomoc przy wdrażaniu wspieranych narzędzi do monitorowania cyberbezpieczeństwa
- Regularna rozmowa wideo z analitykiem IstroSec raportującym monitorowaną aktywność
- Rozmowa wideo ad hoc z analitykiem IstroSec w celu omówienia raportu przekazanego klientowi z IstroSec

IstroSec

Arkusz danych

Dlaczego akurat my?

Doświadczenie i wiedza

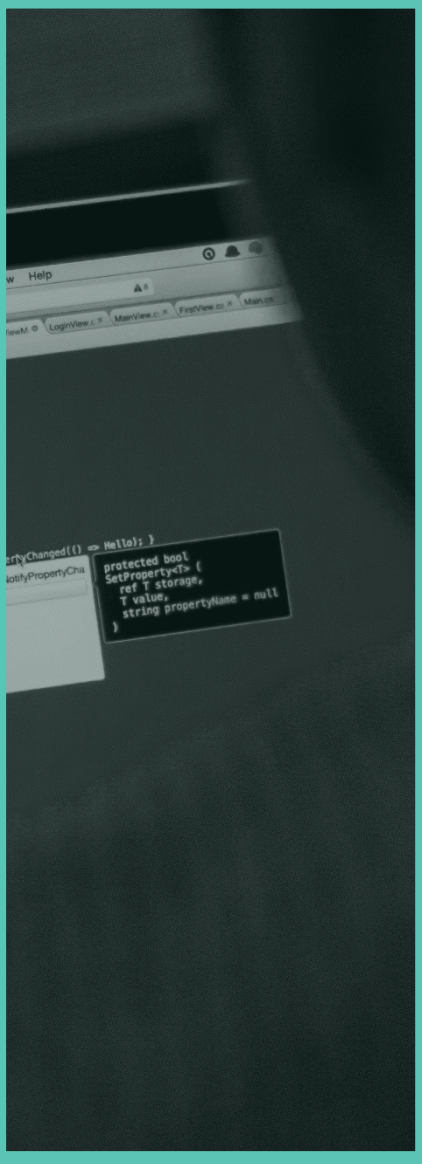
Specjaliści **Istro**Sec mają doświadczenie w zarządzaniu obroną, monitorowaniu bezpieczeństwa i reagowaniu na incydenty związane z bezpieczeństwem zgodnie z aktualnymi najlepszymi praktykami przy użyciu różnych technologii. Znają taktykę, techniki i procedury atakujących oraz mają wiedzę niezbędną do podejmowania decyzji podczas reakcji na incydent w oparciu o analizę działań napastników podczas ataku.

Specjalistyczna wiedza z zakresu zarządzania obroną

Specjalistyczna wiedza w zakresie zarządzania obroną i reagowania na incydenty oraz wielu innych obszarach bezpieczeństwa informacji, takich jak zarządzanie bezpieczeństwem informacji, audyt 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 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), CCFA, CCFR, CCFH i inne.



Studium przypadku

Rodzaj firmy: Organizacja z sektora energetycznego

Świadczone usługi: Zarządzanie obroną

Rozwiązanie: Zarządzanie obroną infrastruktury na poziomie L3, Pakiet 1

Organizacja posiada rozwiązanie EDR wdrożone na wszystkich stacjach roboczych i serwerach. Operator **Istro**Sec wykonujący monitoring L1 odpowiada na komunikat wygenerowany przez funkcję analityczną rozwiązania EDR opisem nietypowego wykonania wiersza poleceń na jednym z serwerów. Wiadomość jest eskalowana do poziomu L2, a operator wykonuje następujące kroki analityczne:

- Analiza polecenia wykonywanego przez proces cmd.exe zawiera dwa kolejne polecenia oddzielone znakami &&. Pierwsza z nich ponownie uruchamia znaną i nieszkodliwą usługę systemową, a druga tworzy zaplanowane zadanie z nazwą wyglądającą na zaufaną, wskazującą na powiązanie z usługą systemową.
- Przegląd ogólnodostępnej dokumentacji nie zawiera żadnej wzmianki o jego istnieniu ani celu zaplanowanego zadania o tej nazwie. Wstępna wewnętrzna ocena dotycząca aktywności - podejrzana lub nawet złośliwa.
- EDR służy do analizy hierarchii procesów, które doprowadziły do wykonania podejrzanego polecenia. Jeden z procesów ma swój plik wykonywalny znajdujący się w folderze AppData\Roaming, w którym często ukrywa się złośliwe oprogramowanie. Alarm zostaje eskalowany do poziomu L3 i rozpoczyna się przygotowanie raportu dla klienta.
- W ramach funkcjonalności EDR wykonywane są zapytania w celu określenia ram czasowych działania:
  - Określanie czasu, w którym podejrzany skrót pliku został po raz pierwszy wyświetlony na urządzeniu generującym alert.
  - Lista wszystkich urządzeń, na których wykryto hash, z datą i godziną. Hash był również widziany kilka godzin wcześniej na serwerze, który jest dostępny z Internetu w celu świadczenia usług organizacji swoim klientom. Lokalizacja pliku jest zgodna z wykorzystaniem luki w aplikacji internetowej.
- Zgłaszany jest incydent bezpieczeństwa, klient otrzymuje raport z aktualnymi ustaleniami i zaleceniami postępowania podczas reakcji na incydent. Zespół monitorujący **Istro**Sec wspiera reakcję i postępowanie za pomocą EDR w celu poszukiwania dodatkowych dowodów odnoszących się do incydentu i pozyskuje dowody i logi do szczegółowej analizy.
- Za pomocą EDR i za zgodą klienta pozyskiwana jest próbka podejrzanego pliku w celu przeprowadzenia analizy złośliwego oprogramowania.
- Bezpośrednio z urządzeń, których dotyczy problem, operator identyfikuje wartości MACB znaczników czasu pliku, a także plik konfiguracyjny podejrzanego zaplanowanego zadania.
- Wszystkie wskaźniki kompromitacji (naruszenia integralności systemu - IoCs) znalezione za pomocą EDR, analizy złośliwego oprogramowania i analizy kryminalistyczne są oznaczone w EDR w celu generowania raportów po ich wykryciu.

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