IstroSec

Data Sheet

Manažovaná obrana infraštruktúry

Pri súčasnom globálnom stave kybernetického priestoru sa stále výraznejšie prejavuje potreba systematického a priebežného dohľadu nad stavom bezpečnosti IT infraštruktúry organizácie. Pod monitoring kybernetickej bezpečnosti spadajú činnosti, ktoré sú spravidla zastrešené konkrétnymi bezpečnostnými riešeniami schopnými analýzy a generovania hlásení.

Táto služba obsahuje:

- Monitoring sieťovej komunikácie – Nástroje IDS a IPS
- Monitoring procesov na koncových zariadeniach – Nástroje EDR
- Zber a korelácia logov – Nástroje SIEM
- Automatizácia vyšetrovacích a reakčných procesov – Nástroje SOAR

Prečo IstroSec?

Kombinované skúsenosti expertov viac ako 70 rokov

Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane penetračných testerov, forenzných analytikov, analytikov malvéru, školiteľov a ďalších

Systematické zlepšenie informačnej bezpečnosti v zmysle štandardov a na základe skúseností s riešením pokročilých bezpečnostných incidentov

Zaistenie súladu s bezpečnostnými štandardmi a legislatívou - skúsenosti z verejnej správy (zákon o kybernetickej bezpečnosti, zákon o ITVS a iné) ako aj zo súkromného sektora (ISO 27001, NIST, HIPAA a iné)

> *Zverenie týchto činností špecializovanému tímu SOC zaručuje kvalitu a zároveň robí zavedenie a prevádzkovanie monitoringu dostupnejším.*

Úrovne služby:

- **L1** – Dohľad a základná analýza hlásení generovaných z monitorovacích nástrojov
- **L2** – Pokročilá analýza hlásení v rámci monitorovacích nástrojov
- **L3** – Hĺbková analýza podozrivej aktivity priamo na zasiahnutom zariadení, zaistenie a analýza dát aj zo zdrojov mimo monitorovacích nástrojov

Možné verdikty o analyzovanej aktivite:

- **Škodlivá** – Aktivita bola potvrdená ako škodlivá
- **Podozrivá** – Aktivitu je možné za určitých podmienok interpretovať ako škodlivú alebo potenciálne nežiadúcu, pričom rozhodujúci je kontext aktivity dodaný klientom
- **Neškodná** – Aktivita bola stotožnená s neškodnou aktivitou a hlásenie z monitorovacieho nástroja bol falošný poplach

IstroSec

Data Sheet

Predpoklady vykonávania služby:

L1

- API kľúče umožňujúce zber dát z monitorovacích nástrojov
- Prístup ku nástrojom na monitorovanie bezpečnosti infraštruktúry klienta
- Kontakt na zodpovednú osobu na strane klienta pre eskalácie

L2

- Práva na vykonávanie dopytov, čítanie a agregáciu logov zo zariadení
- Prístup ku nástrojom na monitorovanie bezpečnosti infraštruktúry klienta
- Kontakt na zodpovednú osobu na strane klienta pre eskalácie

L3

- Administrátorský prístup na koncové systémy klienta, pokiaľ nie je nasadený nástroj EDR s ekvivalentnou funkcionalitou
- Kontakt na zodpovednú osobu na strane klienta pre eskalácie

Balíky služieb:

Balík 1

- 8/5 monitoring a analýza hlásení zo zverených bezpečnostných nástrojov na úrovni L1, L2 a L3
- Upovedomenie klienta v prípade verdiktu Škodlivá a Podozrivá
- Upovedomenie klienta v prípade dosiahnutia úrovne L3 v rámci internej eskalácie bez ohľadu na to či už je finalizovaný verdikt

Balík 2

- 8/5 pohotovosť pre príjem eskalácií L2 a vyššie od klienta a ich analýza
- V prípade potreby interná eskalácia na úroveň L3
- Spätná väzba klientovi s verdiktom analýzy

Balík 3

- 8/5 pohotovosť pre príjem eskalácií L3 a vyššie od klienta a ich analýza
- Spätná väzba klientovi s verdiktom analýzy

Všetky balíky zahŕňajú:

- Pravidelný reporting o aktivite a činnosti formou mesačnej súhrnnej správy

Voliteľné ku každému balíku:

- Správa podporovaných softvérových nástrojov na kyberbezpečnostný monitoring
- Ad-hoc kontrola konfigurácie podporovaných nasadených nástrojov na kyberbezpečnostný monitoring
- Podpora pri nasadzovaní podporovaných nástrojov na kyberbezpečnostný monitoring
- Pravidelný videohovor s analytikom **Istro**Sec s podaním hlásenia o monitorovanej aktivite
- Ad-hoc videohovor s analytikom **Istro**Sec kvôli prediskutovaniu hlásenia eskalovaného smerom od **Istro**Sec ku klientovi

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

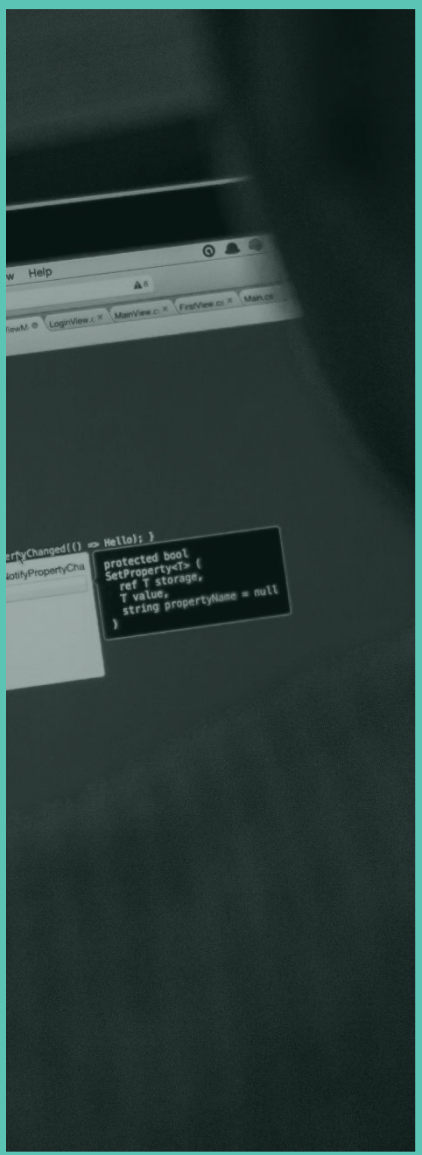
Špecialisti **Istro**Sec majú skúsenosti s manažovanou obranou, bezpečnostným monitoringom a reakciou na bezpečnostné incidenty v zmysle aktuálnych best practices a s využitím širokého spektra technológií. Poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na efektívnu identifikáciu, vyhodnotenie a eskaláciu bezpečnostných incidentov.

Expertíza v manažmente

Expertíza v oblasti manažovanej obrany a mnohých ďalších oblastiach, ako napr. reakcia na incidenty, forenzná analýza a analýza malvéru na svetovej úrovni, ktorú viackrát preukázali pri riešení štátmi sponzorovaných kybernetických útokov, útokov vedených voči organizáciám FORTUNE 500 ako aj účasťou 4 expertov spoločnosti **Istro**Sec vo víťaznom tíme cvičenia LockedShields 2016.

Certifikovaní profesionáli

Experti **Istro**Sec sú držiteľmi medzinárodne uznávaných certifikátov v mnohých oblastiach. Držíme certifikáty, ako napríklad 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 a ďalšie.



Prípadová štúdia

Typ organizácie: Organizácia z energetického sektora

Poskytnutá služba: Manažovaná obrana infraštruktúry

Riešenie: Manažovaná obrana infraštruktúry úrovne L3, Balík 1

Organizácia má nasadené EDR riešenie na všetkých pracovných staniciach a serveroch. Operátor **Istro**Sec vykonávajúci L1 dohľad reaguje na hlásenie vygenerované analytickou funkcionalitou EDR riešenia s popisom o nezvyčajnom spustení príkazového riadku na jednom zo serverov. Hlásenie je eskalované na úroveň L2 a operátor vykoná nasledovné analytické kroky:

- Analýza príkazu vykonaného procesom cmd.exe obsahuje dva za sebou nasledujúce príkazy, oddelené znakmi &&. Prvý reštartuje známu a neškodnú systémovú službu a druhý vytvára plánovanú úlohu s dôveryhodne vyzerajúcim názvom naznačujúci súvis so systémovou službou.
- Prieskum voľne dostupnej dokumentácie neobsahuje žiadne zmienky o existencii alebo o účele plánovanej úlohy s týmto názvom. Predbežný verdikt o aktivite je interne určený ako podozrivá s výhľadom na škodlivá.
- Pomocou EDR je analyzovaná hierarchia procesov, ktorá viedla ku vykonaniu podozrivého príkazu a jeden z procesov má svoj spustiteľný súbor v priečinku AppData\Roaming, čo je lokalita do ktorej sa malvér často skrýva. Hlásenie je eskalované na úroveň L3 a je začatá príprava hlásenia pre klienta.
- V rámci funkcionality EDR sú vykonané dopyty na zodpovedanie otázok, vedúce ku ohraničeniu danej aktivity:
  - Určenie času kedy bol haš podozrivého súboru prvýkrát videný na zariadení, ktoré vygenerovalo hlásenie.
  - Zoznam všetkých zariadení, na ktorých bol daný haš detegovaný spolu s časmi. Haš bol taktiež videný o niekoľko hodín skôr na serveri, ktorý je prístupný z internetu kvôli poskytovaniu služieb organizácie svojim zákazníkom. Umiestnenie súboru je konzistentné so zneužitím zraniteľnosti vo webovej aplikácii.
- Je vyhlásený bezpečnostný incident, klientovi je odoslané hlásenie s aktuálnymi nálezmi a odporúčaniami ako postupovať ďalej v rámci reakcie na incident. Monitorovací tím **Istro**Sec podporuje reakciu a vyšetrovanie použitím EDR na hľadanie ďalších stôp pri ohraničovaní incidentu a zaisťovaní stôp a logov pre podrobnú analýzu.
- Pomocou EDR je so súhlasom klienta zaistená vzorka daného podozrivého súboru kvôli vykonaniu analýzy malvéru.
- Priamo zo zasiahnutých zariadení operátor zaistí hodnoty MACB časových značiek daného súboru a taktiež konfiguračný súbor podozrivej plánovanej úlohy.
- Všetky nájdené indikátory kompromitácie (IOC) nájdené pomocou EDR, analýzy malvéru a forenznej analýzy sú označené v rámci EDR na generovanie hlásení, v momente ako sú detegované v zbieraných dátach.

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