

Opis Przedmiotu Zamówienia

Zakres usługi SOC

1. Cel usługi

Celem usługi jest zapewnienie ciągłego monitorowania bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego, wykrywania zagrożeń, reagowania na incydenty, wspierania działań naprawczych oraz podnoszenia poziomu odporności cyberbezpieczeństwa systemów IT, OT i systemów specjalistycznych Zamawiającego.

Usługa SOC powinna być świadczona w trybie 24/7/365, z zachowaniem ciągłości działania również w dni wolne od pracy i święta.

2. Zakres organizacyjny usługi

Zakres usługi obejmuje:

Obszar	Zakres prac
Monitoring SOC 24/7	ciągły nadzór nad zdarzeniami bezpieczeństwa
Reagowanie na incydenty	klasyfikacja, eskalacja, analiza, rekomendacje, izolacja
Obsługa EDR/XDR/endpoint security	współzarządzanie i nadzór nad systemami ochrony stacji, serwerów i urządzeń mobilnych
Threat Hunting	aktywne poszukiwanie zagrożeń w sieci i systemach
Attack Surface Management	monitoring zewnętrznej powierzchni ataku
Zarządzanie podatnościami	skanowanie, analiza CVE, rekomendacje naprawcze
Patch Management Windows Server	wdrażanie poprawek bezpieczeństwa dla serwerów Microsoft
Informatyka śledcza	zabezpieczanie dowodów, analiza powłamaniowa, malware analysis
Raportowanie	raporty miesięczne, incydentalne, podatności, compliance
Transfer wiedzy	konsultacje, warsztaty, rekomendacje bezpieczeństwa

[Handwritten signatures and initials in blue ink]

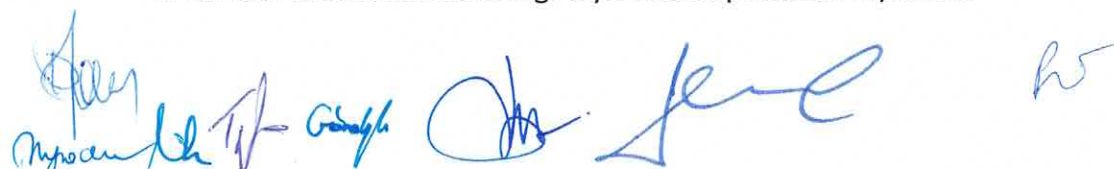
3. Systemy objęte usługą SOC

Usługą SOC powinny zostać objęte co najmniej następujące środowiska:

Lp.	System / obszar	Zakres monitorowania
1	INFLOT – system monitorów informacyjnych	serwery, stacje sterujące, komunikacja LAN, dostęp administracyjny
2	System łączności TETRA	sieć TCP/IP, urządzenia komunikacyjne, zdarzenia bezpieczeństwa
3	System odpraw biletowo-bagażowych	AD, serwery, stacje check-in/gate, aplikacje odprawowe, urządzenia peryferyjne
4	SCADA bagażowni	stacje operatorskie, serwery, komunikacja sieciowa, anomalie OT
5	Serwery sortowania bagażu	zdarzenia systemowe, aplikacyjne, komunikacja z systemami zależnymi
6	Sieć przeglądarek rentgenowskich	stacje analizy, urządzenia LAN, dostęp administracyjny
7	System kontroli dostępu	serwery, stacje operatorskie, zdarzenia dostępu
8	System monitoringu wizyjnego CCTV	serwery, rejestratory, stacje operatorskie, dostęp zdalny
9	Systemy administracyjno-biurowe	AD, poczta, stacje robocze, serwery, usługi sieciowe
10	Firewalle, VPN, urządzenia sieciowe	logi bezpieczeństwa, ruch zewnętrzny, zmiany konfiguracji
11	Endpointy i serwery	EDR/XDR, alerty, polityki, izolacja, malware
12	Zasoby publiczne	domeny, DNS, certyfikaty, usługi publiczne, podatności

4. Etap I – uruchomienie usługi SOC

W ramach uruchomienia usługi Wykonawca powinien wykonać:



1. Inwentaryzację systemów, źródeł logów i punktów integracji.
2. Uzgodnienie architektury technicznej SOC.
3. Integrację narzędzi Wykonawcy z infrastrukturą Zamawiającego.
4. Integrację z narzędziami Zamawiającego, w szczególności endpoint security (EDR/XDR).
5. Uzgodnienie katalogu monitorowanych źródeł logów.
6. Uzgodnienie klasyfikacji incydentów zgodnie z procedurami Zamawiającego.
7. Uzgodnienie procedur eskalacji zgodnie z procedurami Zamawiającego.
8. Opracowanie matrycy kontaktów i odpowiedzialności.
9. Przygotowanie reguł korelacyjnych i scenariuszy detekcji.
10. Przeprowadzenie audytu konfiguracji endpoint security.
11. Uruchomienie raportowania operacyjnego.
12. Przeprowadzenie testu gotowości usługi SOC.

5. Monitoring w trybie ciągłym (24/7/365) systemów teleinformatycznych oraz sieci Zamawiającego oraz reagowanie na pojawiające się zdarzenia (SOC)

Usługa w zakresie cyberbezpieczeństwa będzie świadczona na Infrastrukturze Zamawiającego, z wykorzystaniem zarówno narzędzi Wykonawcy, jak i narzędzi Zamawiającego obsługiwanych przez jego zespół, zgodnie z obowiązującymi wymaganiami. Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r. poz. 2479).

Wykonawca powinien zapewnić ciągły monitoring:

1. zdarzeń bezpieczeństwa,
2. zdarzeń systemowych,
3. zdarzeń aplikacyjnych,
4. zdarzeń urządzeń sieciowych,
5. zdarzeń firewall/VPN,
6. alertów EDR/XDR/endpoint security,
7. działań użytkowników,
8. działań administratorów,
9. działań kont uprzywilejowanych,
10. zdarzeń nietypowych i anomalii,
11. prób nieautoryzowanego dostępu,
12. prób eskalacji uprawnień,
13. komunikacji z adresami C2,
14. złośliwego oprogramowania,
15. ataków brute-force,
16. phishingu,



17. botnetów,
18. podejrzanych zmian konfiguracji,
19. zdarzeń w systemach OT/SCADA,
20. incydentów dotyczących systemów krytycznych.

6. Trzy linie obsługi SOC

a. I linia SOC

I linia SOC odpowiada za:

Obszar	Zakres działań
Monitoring	bieżąca obserwacja alertów i zdarzeń
Triage	wstępna analiza i odrzucanie false-positive
Klasyfikacja	klasyfikacja zdarzeń według poziomu istotności
Rejestracja	ewidencja zdarzeń i incydentów
Eskalacja	przekazanie incyduentu do GTL i/lub II linii SOC
Raportowanie	raporty bieżące i cykliczne

b. II linia SOC

II linia SOC odpowiada za:

Obszar	Zakres działań
Analiza techniczna	pogłębiona analiza incyduentu
Reagowanie	ograniczanie skutków, izolacja, containment
Dowody	zabezpieczenie logów i danych technicznych
Rekomendacje	działania korygujące i zapobiegawcze
Wsparcie zgłoszeń	dane niezbędne do zgłoszeń do CSIRT GOV / właściwego CSIRT
Raport końcowy	opis przyczyn, skutków i zaleceń



c. III linia SOC

III linia SOC odpowiada za:

Obszar	Zakres działań
Informatyka śledcza	zabezpieczenie śladów cyfrowych
Malware analysis	analiza kodu złośliwego
Analiza powtórzeniowa	ustalenie wektora ataku i zakresu kompromitacji
Identyfikacja TTP	mapowanie działań atakującego
Wsparcie dowodowe	przygotowanie materiału dla organów ścigania
Red Team / Pentest	wsparcie eksperckie przy analizie podatności i ataków

7. Obsługa EDR/XDR/Endpoint Security

Wykonawca powinien zapewnić:

1. przejęcie nadzoru nad systemami endpoint security,
2. współzarządzanie konsolami EDR/XDR,
3. analizę alertów z istniejących konsol Zamawiającego,
4. tworzenie niestandardowych reguł detekcji,
5. konfigurację polityk bezpieczeństwa,
6. konfigurację kontroli urządzeń USB,
7. konfigurację ochrony przeglądarek,
8. konfigurację SSL/TLS inspection lub polityk kontroli SSL/TLS, jeśli technicznie uzasadnione,
9. ochronę przed phishingiem, botnetami i malware,
10. blokowanie brute-force,
11. wykrywanie niepożądanych aplikacji,
12. identyfikację najbardziej narażonych urządzeń,
13. izolację endpointów w sytuacjach krytycznych,
14. rekomendacje hardeningu stacji i serwerów,
15. raportowanie stanu ochrony endpointów.
16. odtwarzanie danych po ataku cryptolockera



8. Threat Hunting

W ramach Threat Huntingu Wykonawca dostarczy rozwiązanie (na własny koszt) do realizacji usługi tak aby zapewnić:

1. aktywne poszukiwanie zagrożeń niewykrytych przez EDR/XDR,
2. analizę ruchu sieciowego bez konieczności instalacji agentów,
3. analizę ruchu ARP,
4. możliwości wykrywania ataków warstwy drugiej modelu OSI realizowanych poza protokołem ARP,
5. wykrywanie manipulacji protokołem Spanning Tree (Rogue Root Bridge, Topology Change Notification),
6. wykrywanie przejęcia bramy redundantnej w protokołach HSRP i VRRP,
7. wykrywanie ataków typu VLAN hopping (double-tagged 802.1Q frames na porcie access)
8. wykrywanie ataków typu MAC flooding prowadzących do przepełnienia tablicy CAM przełącznika,
9. wykrywanie sekwencyjnej iteracji adresów MAC charakterystycznej dla narzędzi automatyzacji ataków,
10. wykrywanie ataków Rogue Router Advertisement, w tym z wykorzystaniem opcji DNSSL przekierowującej rozwiązywanie nazw DNS,
11. wykrywanie ataków typu mitm6 (Rogue DHCPv6 Server) skutkujących przejęciem konfiguracji DNS klientów,
12. wykrywanie spoofingu pakietów Neighbor Advertisement (NA spoofing),
13. wykrywanie zalewu pakietów Neighbor Discovery (ND flood),
14. wykrywanie skanów ICMPv6 Echo Request oraz Neighbor Solicitation,
15. wykrywanie fałszywych pakietów ICMPv6 Redirect,
16. wykrywanie MiTM, ARP poisoning i skanowania podsieci,
17. wykrywanie LLMNR, NBNS, mDNS poisoning,
18. analizę DHCP, w tym rogue DHCP, race condition, badWPAD,
19. wykrywanie ataku Web Proxy Auto-Discovery (WPAD) poisoning realizowanego równocześnie na czterech warstwach wykrywania nazw:
 - a. opcji DHCP numer 252,
 - b. protokole Link-Local Multicast Name Resolution (LLMNR),
 - c. protokole NetBIOS Name Service (NBNS),
 - d. protokole Multicast DNS (mDNS), wraz z identyfikacją hosta odpowiadającego fałszywie na zapytania o nazwę „wpad”
20. wykrywania konkretnych narzędzi ofensywnych po sygnaturach behawioralnych oraz fingerprintach protokołowych:
 - a. narzędzi klasy LLMNR/NBT-NS poisoner (po unikalnej liście opcji DHCP Option 55 oraz po wzorcu hostname klienta),



- b. frameworków typu Adversary-in-the-Middle (po charakterystycznych zapytaniach mDNS oraz nagłówkach SSDP User-Agent),
 - c. miniaturowych urządzeń atakujących podłączanych fizycznie do sieci (po prefiksach OUI producenta),
 - d. dystrybucji systemów operacyjnych przeznaczonych do prowadzenia testów penetracyjnych (po hostname zgłaszanym w trakcie autentykacji SMB/NTLMSSP),
 - e. narzędzi DHCP-spoofingu,
 - f. alternatywnych systemów operacyjnych routerów (po identyfikatorze vendor class).
- 21. wykrywanie password spraying,
 - 22. wykrywanie prób podszywania się pod hosty,
 - 23. identyfikację usług po ruchu multicast/broadcast,
 - 24. analizę lateral movement,
 - 25. wykrywanie skanów Nessus, Nexpose lub podobnych narzędzi,
 - 26. analizę komunikacji pomiędzy stacjami,
 - 27. przygotowanie raportów z obserwacji,
 - 28. redukcję false-positive,
 - 29. rekomendacje poprawy segmentacji VLAN.

9. Attack Surface Management

Wykonawca powinien dostarczyć i utrzymywać rozwiązanie ASM obejmujące:

- 1. identyfikację zasobów publicznych,
- 2. wykrywanie zapomnianych usług i subdomen,
- 3. wykrywanie ryzyka subdomain takeover,
- 4. monitoring nowych otwartych portów,
- 5. monitoring zmian bannerów usług,
- 6. monitoring DNS,
- 7. monitoring certyfikatów SSL/TLS,
- 8. wykrywanie wygasających certyfikatów,
- 9. wykrywanie błędów SPF, DKIM, DMARC,
- 10. wykrywanie ujawnionych adresów IP za usługami typu Cloudflare,
- 11. automatyczną analizę aplikacji webowych,
- 12. rekonesans zasobów internetowych,
- 13. raportowanie zmian powierzchni ataku,
- 14. rekomendacje ograniczenia ekspozycji.



10. Zarządzanie podatnościami

Zakres zarządzania podatnościami powinien obejmować:

1. cykliczne skanowanie podatności,
2. monitoring publicznej klasy adresowej,
3. analizę podatności CVE,
4. klasyfikację podatności według krytyczności,
5. ocenę wpływu podatności na środowisko Zamawiającego,
6. opracowanie rekomendacji naprawczych,
7. wskazanie priorytetów remediacji,
8. walidację usunięcia podatności,
9. raporty podatności,
10. raporty trendów i ryzyka.

11. Patch Management Windows Server

Wykonawca powinien realizować proces aktualizacji systemów Windows Server obejmujący:

1. monitoring biuletynów Microsoft,
2. analizę Patch Tuesday i aktualizacji out-of-band,
3. ocenę wpływu aktualizacji na środowisko Zamawiającego,
4. klasyfikację aktualizacji: 0-day / Critical / Important / Moderate,
5. opracowanie harmonogramu wdrożeń,
6. uzgadnianie okien serwisowych,
7. weryfikację backupu przed aktualizacją,
8. rekomendację wykonania snapshotów,
9. wdrażanie aktualizacji na środowisku testowym lub pilotażowym,
10. instalację poprawek bezpieczeństwa,
11. rozpoczęcie wdrażania poprawek bezpieczeństwa typu 0-day nie później niż 12h po opublikowaniu
12. instalację Servicing Stack Updates,
13. instalację Cumulative Updates,
14. restart serwerów zgodnie z ustaloną procedurą Zamawiającego,
15. weryfikację działania usług po aktualizacji,
16. analizę logów Windows po wdrożeniu,
17. diagnostykę błędów,
18. raport patch compliance.

12. Reagowanie na incydenty

Wykonawca powinien realizować obsługę incydentów obejmującą:



1. wykrycie incydentu,
2. rejestrację incydentu,
3. klasyfikację incydentu,
4. ocenę wpływu na ciągłość działania,
5. ocenę wpływu na dane osobowe,
6. eskalację do Zamawiającego,
7. analizę techniczną,
8. izolację systemów w sytuacjach krytycznych,
9. ograniczanie skutków incydentu,
10. zabezpieczenie logów,
11. zabezpieczenie dowodów,
12. analizę przyczyn źródłowych,
13. rekomendacje naprawcze,
14. rekomendacje zapobiegawcze,
15. raport końcowy z incydentu,
16. wsparcie przy komunikacji z CSIRT GOV / właściwym CSIRT,
17. wsparcie przy analizie obowiązku zgłoszenia naruszenia ochrony danych osobowych.

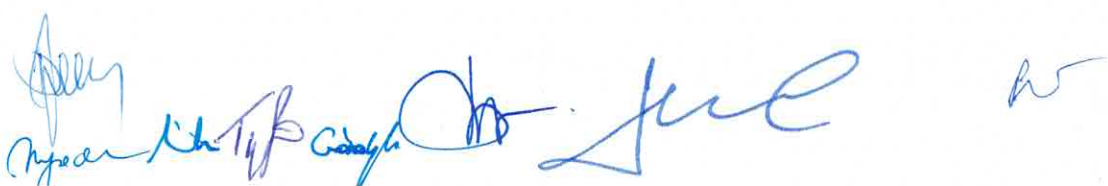
13. Informatyka śledcza i analiza powłamaniowa

Wykonawca powinien zapewnić możliwość realizacji:

1. zabezpieczenia materiału dowodowego,
2. zabezpieczenia obrazów dysków,
3. zabezpieczenia pamięci operacyjnej,
4. zabezpieczenia logów,
5. zabezpieczenia urządzeń w terenie,
6. analizy powłamaniowej,
7. analizy malware,
8. analizy ransomware / cryptolocker,
9. wsparcia przy odzyskiwaniu danych,
10. przygotowania raportu technicznego,
11. wsparcia przy współpracy z organami ścigania,
12. zachowania łańcucha dowodowego.

14. Raportowanie

Wykonawca powinien dostarczać co najmniej:



Raport	Częstotliwość	Zakres
Raport operacyjny SOC	miesięcznie	liczba alertów, incydentów, klasyfikacja, trendy
Raport incydentu	po każdym incydencie lub na wezwanie	opis, oś czasu, skutki, działania, rekomendacje
Raport podatności	miesięcznie / kwartalnie	podatności, ryzyko, priorytety naprawy
Raport ASM	miesięcznie	zmiany powierzchni ataku, nowe zasoby, certyfikaty
Raport endpoint security	miesięcznie	stan ochrony, urządzenia ryzykowne, alerty EDR/XDR
Raport patch compliance	miesięcznie	status aktualizacji serwerów, braki, ryzyka
Biuletyn bezpieczeństwa	Miesięcznie lub w razie konieczności	najważniejsze podatności, zagrożenia, rekomendacje
Raport roczny	rocznie	podsumowanie trendów, dojrzałość SOC, plan doskonalenia

15. Minimalne wymagania SLA

Kategoria incydentu	Przykład	Czas reakcji SOC	Eskalacja
Krytyczny	ransomware, aktywny atak, kompromitacja AD, zatrzymanie systemu krytycznego	do 30 min	natychmiast do Zamawiającego i II/III linii
Wysoki	malware, brute-force, podejrzenie przejęcia konta uprzywilejowanego	do 60 min	do II linii
Średni	podejrzana aktywność, skanowanie, nietypowy ruch	do 2 h	według procedury



Kategoria incydentu	Przykład	Czas reakcji SOC	Eskalacja
Niski	zdarzenie informacyjne, pojedyncze nieudane logowania	do 8 h	raport miesięczny / eskalacja według oceny

[Handwritten signatures and initials]