URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

al. Niepodległości 188/192
00-950 Warszawa, skr. poczt. 203
tel.: (+48) 22 579 05 55 | fax: (+48) 22 579 00 01
e-mail: kontakt@uprp.gov.pl | www.uprp.gov.pl

Dyrektor Generalny

Warszawa, 26.02.2026 r.

Dot. postępowania nr BG-PZ.26.3.2026 prowadzonego w trybie przetargu nieograniczonego pn. „Usługa reakcji na incydenty bezpieczeństwa SOC (Security Operations Center)"

Wyjaśnienie i zmiana treści specyfikacji warunków zamówienia (SWZ), przedłużenie terminu składania ofert

Działając na podstawie art. 284 ust. 2, 3 i 6 oraz art. 286 ust. 1 ustawy z 11 września 2019r. – Prawo zamówień publicznych (Dz.U. z 2024 r. poz. 1320 z późn. zmian.) Zamawiający udziela wyjaśnień na zapytania Wykonawców, wprowadza zmiany w treści SWZ oraz przedłuża termin na składanie ofert **do 2 marca 2026 r. do godz.: 11:00.** Termin otwarcia ofert: 2 marca 2026 r. godz.: 11:30. Termin związania ofert: 31 marca 2026 r.

Treść pytania nr #1
Zamawiający w Załączniku nr 1 do SWZ – Opis Przedmiotu Zamówienia w punkcie 5 „Monitorowanie systemów EDR i NDR" specyfikuje:
„Usługa obejmuje całodobowe monitorowanie i analizę zagrożeń z wykorzystaniem systemów klasy EDR i NDR, posiadanych przez Zamawiającego, realizowane przez analityków zespołu SOC w trybie 24/7/365. W ramach monitorowania EDR i NDR wymagane są w szczególności następujące funkcje"
Zwracamy się z prośbą o informację jakiego producenta rozwiązania klasy EDR oraz NDR posiada Zamawiający.

Odpowiedź Zamawiającego na pytanie nr #1
Zamawiający informuje, że posiada rozwiązania klasy EDR SentinelOne oraz NDR Fidelis Security.

Treść pytania nr #2
W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego, zwracamy się z uprzejmą prośbą o udzielenie odpowiedzi na poniższe pytania:
1. Czy Zamawiający posiada obecnie wdrożony system klasy EDR (Endpoint Detection and Response)? Jeśli tak, prosimy o wskazanie producenta i nazwy rozwiązania.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2. Czy Zamawiający posiada obecnie wdrożony system klasy NDR (Network Detection and Response)? Jeśli tak, prosimy o wskazanie producenta i nazwy rozwiązania.

Odpowiedź Zamawiającego na pytanie nr #2
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 1.

Treść pytania nr #3
Czy możemy prosić o wskazanie listy systemów dla usług sklasyfikowanych jako elementy kluczowe?

Odpowiedź Zamawiającego na pytanie nr #3
Zamawiający informuje, że przez systemy kluczowe rozumie w szczególności usługi i systemy teleinformatyczne publikowane do Internetu przez Zamawiającego, a także wewnętrzne systemy informatyczne wspierające bieżącą obsługę urzędu, w tym w szczególności systemy klasy ERP, systemy obiegu dokumentów, systemy finansowo-księgowe, kadrowo-płacowe, oraz inne systemy niezbędne do zapewnienia ciągłości działania jednostki. Łączna liczba systemów zaliczanych do kluczowych nie przekracza 30. Szczegółowa lista systemów kluczowych zostanie uzgodniona z Wykonawcą po rozstrzygnięciu postępowania, na etapie wdrożenia usługi.

Treść pytania nr #4
Prosimy o wskazanie, liczby pracowników wykorzystujących systemy teleinformatyczne,

Odpowiedź Zamawiającego na pytanie nr #4
Zamawiający informuje, że liczba pracowników wykorzystujących systemy teleinformatyczne wynosi około 500.

Treść pytania nr #5
Prosimy o wskazanie liczby aktywnych pracowników (kont) w domenie,

Odpowiedź Zamawiającego na pytanie nr #5
Zamawiający informuje, że liczba aktywnych pracowników (kont) w domenie wynosi około 500.

Treść pytania nr #6
Prosimy o podanie informacji o strukturze środowiska Active Directory, liczbie domen oraz kwestii w zakresie relacji zaufania jedno i dwukierunkowych wobec Spółek zależnych u Zamawiającego,

Odpowiedź Zamawiającego na pytanie nr #6
Zamawiający informuje, że środowisko Active Directory funkcjonujące u Zamawiającego obejmuje pojedynczy las oraz jedną domenę. W związku z powyższym w środowisku nie występują relacje zaufania jedno ani dwukierunkowe, w tym również wobec spółek zależnych. Poziom funkcjonalny domeny Active Directory ustawiony jest na poziomie Windows Server 2016.

Treść pytania nr #7
Wymaganie: 5 c) zasilanie systemów EDR i NDR zewnętrznymi feedami bezpieczeństwa oraz feedami wynikającymi z analiz prowadzonych przez SOC,
Czy Zamawiający w wymaganiu 5 c) oczekuje dostarczania usługi zasilania systemów zewnętrznymi feedami za pomocą integracji lub poprzez dedykowaną platformę udostępniania danych np. missp/opencti

Odpowiedź Zamawiającego na pytanie nr #7
Zamawiający informuje, że nie określa szczegółowego sposobu realizacji zasilania systemów EDR i NDR zewnętrznymi feedami bezpieczeństwa ani feedami wynikającymi z analiz SOC. Wybór metody realizacji, w tym zastosowanie integracji bezpośrednich lub wykorzystanie dedykowanej platformy udostępniania danych, pozostaje po stronie Wykonawcy.

Treść pytania nr #8

Wymaganie: 6. Pozostałe systemy bezpieczeństwa Zamawiającego

Zamawiający posiada również:

- klastry zapór sieciowych nowej generacji (NGFW),
- systemy analizy zdarzeń i logów,
- systemy klasy sandbox, IPS, WAF, DDoS Protection System.

Powyższe systemy mogą stanowić elementy składowe realizacji usługi SOC i być wykorzystywane przez Wykonawcę w procesach monitorowania, analizy oraz reagowania na incydenty bezpieczeństwa.

Czy Zamawiający w odniesieniu do powyższego wymagania posiada agregacje i jedno miejsce przechowywania logów mogące służyć do korelacji logów ze wskazanych systemów bezpieczeństwa?

Odpowiedź Zamawiającego na pytanie nr #8

Zamawiający informuje, że posiada centralny system logów, w którym agregowane są logi z klastrów zapór sieciowych NGFW oraz z lokalnego systemu WAF.

Treść pytania nr #9
Czy Zamawiający oczekuje, że w ramach usługi SOC powinien zostać dostarczony system klasy SIEM umożliwiający monitorowanie, wykrywanie i reagowanie na incydenty uwzględniając korelacje z wszystkich posiadanych incydentów bezpieczeństwa?

Odpowiedź Zamawiającego na pytanie nr #9
Zamawiający informuje, że nie wymaga dostarczenia w ramach usługi SOC systemu klasy SIEM, jednocześnie nie wyklucza możliwości jego zastosowania przez Wykonawcę.
Treść pytania nr #10
Prosimy o informacje czy są opracowane i dostępne scenariusze reakcji na zdarzenia i incydenty w środowisku Zamawiającego?

Odpowiedź Zamawiającego na pytanie nr #10
Zamawiający informuje, że działania w zakresie reakcji na zdarzenia i incydenty w środowisku opierają się na obowiązującej dokumentacji dotyczącej bezpieczeństwa systemów teleinformatycznych zamawiającego, która określa incydenty oraz przewidziane postępowania.

Treść pytania nr #11
Czy możemy prosić o szacunkowe liczby aktualnej biblioteki playbooków czy UC, funkcjonujących w środowisku Zamawiającego?

Odpowiedź Zamawiającego na pytanie nr #11
Zamawiający informuje, że w środowisku funkcjonuje system FortiAnalyzer, który w ramach posiadanej licencji udostępnia gotowe ścieżki reakcji i alerty, które działają i są wykorzystywane w praktyce. Należy podkreślić, że dotyczą one wyłącznie części systemów bezpieczeństwa oraz systemów sieciowych i nie stanowią odrębnej, opracowanej przez Zamawiającego biblioteki playbooków ani Unified Communications (UC) dla wszystkich procesów bezpieczeństwa.

Treść pytania nr #12
Czy Zamawiający posiada opracowany i wykorzystywaną procedurę reagowania na incydenty?

Odpowiedź Zamawiającego na pytanie nr #12
Zamawiający informuje, że procedury reagowania na incydenty bezpieczeństwa są określone i wykorzystywane w ramach obowiązującej dokumentacji dotyczącej bezpieczeństwa systemów teleinformatycznych zamawiającego.

Treść pytania nr #13
Czy Zamawiający posiada klasyfikacje wykorzystywaną do oceny/priorytetyzacji zdarzeń i incydentów?

Odpowiedź Zamawiającego na pytanie nr #13
Zamawiający informuje, że kryteria oceny i priorytetyzacji zdarzeń oraz incydentów bezpieczeństwa są określone w obowiązującej dokumentacji dotyczącej bezpieczeństwa systemów teleinformatycznych zamawiającego. Jednocześnie Zamawiający informuje, że trwają prace nad rozbudową procedur, w tym klasyfikacji incydentów.

Treść pytania nr #14
Czy możemy prosić o informacje jaka ilość incydentów na dzień dzisiejszy jest wykrywana i podlega analizie?

Odpowiedź Zamawiającego na pytanie nr #14
Zamawiający informuje, że w systemie EDR wykrywanych jest około 20 zdarzeń miesięcznie. W przypadku systemów NDR, NGFW oraz WAF liczba zdarzeń podlegających analizie jest znacznie większa i obejmuje setki zdarzeń miesięcznie, z czego duża część to

false positive oraz skany sieci i wykrycia podatności. Rzeczywiste incydenty bezpieczeństwa stanowią pojedyncze przypadki w skali miesiąca.

Treść pytania nr #15
Czy możemy prosić o informacje o potencjalnej liczbie zdarzeń wykrywanych w systemach bezpieczeństwa?

Odpowiedź Zamawiającego na pytanie nr #15
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 14

Treść pytania nr #16
Czy Zamawiający ma opracowane dane/informacje w zakresie - Właścicieli biznesowych, przypisanych Administratorów, określonych zasobów infrastrukturalnych stojących za daną aplikacją czy usługą biznesową:

a) Kluczowe systemy odpowiedzialne za funkcjonowanie podstawowych usług teleinformatycznych w Organizacji (np.: środowisko Active Directory, DNS, DHCP, dostęp zdalny, usługi pracy grupowej, DMZ itp.) oraz systemy odpowiedzialne za monitorowanie i ochronę środowiska (zapory FW/NGFW/WAF/PROXY, systemy teleinformatyczne, systemy/narzędzia bezpieczeństwa itp.),
b) Krytyczne systemy i aplikacje odpowiedzialne za kluczowe usługi i procesy biznesowe w Organizacji, (np. system ERP, CMS, Baza danych z klientami itp.)
c) Urządzenia sieciowe odpowiedzialne za przetwarzanie/ruchu w warstwie L3 lub wyższej odpowiedzialne za realizacje routingu, filtracje ruchu, zmiany w regułach i politykach ACL, (np.: Core switche, FW, VPN, Routery, LB, inne systemy realizujące dodatkowe funkcjonalności),

Odpowiedź Zamawiającego na pytanie nr #16
Zamawiający informuje, że posiada opracowane dane i informacje dotyczące wszystkich właścicieli biznesowych, przypisanych administratorów oraz określonych zasobów infrastrukturalnych odpowiadających za poszczególne aplikacje i usługi biznesowe.

Treść pytania nr #17
Wymaganie 3b: W ramach usługi CTI Wykonawca dostarcza:

- zweryfikowane wskaźniki kompromitacji (Indicators of Compromise – IOC),
- rekomendacje mitigacyjne,
- zalecenia działań korygujących, umożliwiające skuteczne reagowanie na potencjalne zagrożenia i minimalizowanie ryzyka ich wystąpienia,
- Raportowanie w zakresie CTI odbywa się nie rzadziej niż raz w miesiącu.

Czy intencją Zamawiającego jest dostarczanie wskaźników Indicators of Compromise – IOC z przeprowadzanych analiz po incydentach wykrytych w środowisku teleinformatycznym Organizacji oraz ich wzbogaceniu o źródła Threat Intelligence?

Odpowiedź Zamawiającego na pytanie nr #17
Zamawiający informuje, że wskaźniki IOC (Indicators of Compromise) w ramach usługi CTI powinny być opracowywane przede wszystkim w oparciu o zewnętrzne źródła

informacji o zagrożeniach (Threat Intelligence). W przypadku wykrycia incydentów w środowisku Zamawiającego odpowiednie IOC będą również uwzględniane i integrowane w dostarczanych danych CTI.

Treść pytania nr #18
Wymaganie 5 c) zasilanie systemów EDR i NDR zewnętrznymi feedami bezpieczeństwa oraz feedami wynikającymi z analiz prowadzonych przez SOC.
Czy Zamawiający w wymaganiu 5 c) zaakceptuje dostarczanie usługi zasilania systemów zewnętrznymi feedami za pomocą integracji lub poprzez dedykowaną platformę udostępniania danych missp?

Odpowiedź Zamawiającego na pytanie nr #18
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 7

Treść pytania nr #19
Czy Zamawiający posiada platformę XCTI monitorującą darkweb, czy oczekuje dostarczenia platformy XCTI monitorującej darkweb wraz z usługą?

Odpowiedź Zamawiającego na pytanie nr #19
Zamawiający informuje, że w zakresie zamówienia przewidziany jest monitoring widoczności danych Zamawiającego w dark web. Zamawiający nie określa sposobu realizacji tego monitoringu, pozostawiając wybór metody realizacji po stronie Wykonawcy.

Treść pytania nr #20
Prosimy o doprecyzowanie jakie słowa kluczowe Zamawiający poddać monitorowaniu w darkweb?

Odpowiedź Zamawiającego na pytanie nr #20
Zamawiający informuje, że w zakresie monitoringu w dark web jako słowa kluczowe na pewno poddane będą monitorowaniu m.in. „Urząd Patentowy RP” (w różnych wersjach językowych) oraz skrót „UPRP”. Szczegółowe słowa kluczowe zostaną ustalone z Wykonawcą w oparciu o jego doświadczenie w tego typu działaniach, po rozstrzygnięciu postępowania. Zamawiający zakłada wykorzystanie do 5 słów lub nazw kluczowych.

Treść pytania nr #21

Prosimy o doprecyzowanie co zamawiający rozumie przez "nadzór nad zasobami i bazami reputacyjnymi pod kątem domen, adresów IP oraz innych aktywów Zamawiającego."?

Czy zamawiający oczekuje monitorowania baz reputacyjnych pod kątem występowania adresów IP i innych aktywów własnych Zamawiającego w tych bazach? Jakich efektów takiego działania oczkuje się Zamawiający?

Odpowiedź Zamawiającego na pytanie nr #21
Zamawiający informuje, że oczekuje monitorowania baz reputacyjnych pod kątem występowania adresów IP i innych aktywów własnych Zamawiającego w tych bazach. Efektem takiego działania jest informowanie Zamawiającego o wykryciu jego zasobów w bazach reputacyjnych, takich jak np. RBL(Realtime Blacklist), oraz o innych potencjalnych zagrożeniach związanych z reputacją domen, adresów IP i aktywów, co pozwala na szybkie podjęcie działań korygujących lub zabezpieczających.

Treść pytania nr #22

Jaki system analizy zdarzeń i logów posiada zamawiający? Jakie dane są dostępne w tym systemie? Jakie reguły analityczne są uruchomione w tym systemie?

Odpowiedź Zamawiającego na pytanie nr #22
Zamawiający informuje, że w środowisku funkcjonuje system FortiAnalyzer, w którym agregowane są dane z klastrów zapór sieciowych NGFW oraz lokalnego systemu WAF. Większość informacji generowanych przez NGFW jest dostępna w FortiAnalyzer. W zakresie reguł analitycznych system korzysta z dodatkowych licencji Security Automation Service oraz FortiGuard IOC and Outbreak Detection Service, co umożliwia zaawansowaną analizę zdarzeń i detekcję incydentów bezpieczeństwa.

Treść pytania nr #23
Prosimy o informację jaki system sandbox posiada Zamawiający?

Odpowiedź Zamawiającego na pytanie nr #23
Zamawiający informuje, że w środowisku funkcjonuje system FortiSandbox oraz system NDR Fidelis Security posiada funkcjonalność sandbox.

Treść pytania nr #24
Ile osób ma zostać przeszkolonych w zakresie "współpracy z usługą SOC"?

Odpowiedź Zamawiającego na pytanie nr #24
Zamawiający informuje, że zgodnie z zapisami OPZ szkolenia w zakresie „współpracy z usługą SOC” przewidziane są dla minimum dwóch administratorów Zamawiającego.

Treść pytania nr #25
Jakie są oczekiwania zamawiającego w zakresie "zapewnienie narzędzi i oprogramowania wspierającego monitorowanie, analizę i raportowanie incydentów, w tym w razie potrzeby dedykowanych skryptów, szablonów raportów lub aplikacji pomocniczych."?

Odpowiedź Zamawiającego na pytanie nr #25
Zamawiający informuje, że w razie wystąpienia incydentu, w sytuacji gdy dostępne systemy bezpieczeństwa Zamawiającego nie są wystarczające, Wykonawca zapewni dodatkowe skrypty lub narzędzia pomocnicze wspierające monitorowanie, analizę i raportowanie incydentów oraz wykonywanie działań mitygujących i naprawczych.

Treść pytania nr #26
Zamawiający opisuje "[...] maksymalny czas mitygacji zagrożenia spowodowanego incydentem po stronie SOC: do 2 godzin, przy czym maksymalny czas całkowitej obsługi incydentu krytycznego uzależniony jest od stopnia skomplikowania incydentu, ale nie może przekroczyć 72 h [...]"
Oferent posiada duże doświadczenie w zakresie reakcji na krytyczne incydenty cyberbezpieczeństwa w tym również wieloetapowe ataki ransomware i ataki grup APT. Na podstawie doświadczenia stwierdza, że pełna obsługa i reakcja na wiele aspektów wpływających na organizację po wystąpieniu takiego incydentu może zająć kilka tygodni.
Nie jest możliwe przewidzenie i ograniczenie tego czasu. Możliwe jest zagwarantowanie rozpoczęcie aktywnych działań związanych z reakcją na incydent bezzwłocznie po jego zidentyfikowaniu, co spełnia zapis "do 2 godzin". Zapis wymagający zaprzestania wsparcia w zakresie mitygacji do 72 godzin jest zapisem ograniczającym poziom cyberbezpieczeństwa Zamawiającego oraz naraża oferenta na duże straty wizerunkowe.
Oferent wnosi o usunięcie zapisu ograniczającego czas obsługi incydentu krytycznego.

Odpowiedź Zamawiającego na pytanie nr #26 - ZMIANA SWZ
W odpowiedzi na pytanie Zamawiający zmienia treść SWZ w zakresie:

Wzór Umowy, § 3 ust. 3
z:
3. Zgłoszenia i obsługa incydentów objętych Usługą przyjmowane będą przez serwis Wykonawcy drogą telefoniczną lub pocztą elektroniczną:
1) Wszystkie incydenty zgłaszane będą pocztą elektroniczną, poprzez wysłanie wiadomości na adres e-mail…… lub telefonicznie na numer …….. Szczegółowa procedura obsługi incydentów zostanie ustalona i obustronnie zatwierdzona przed uruchomieniem Usługi;
2) Termin realizacji prac związanych z obsługą Incydentu lub Zdarzenia zależy od wagi zgłoszenia:
a) Czas reakcji dla Incydentów Krytycznych wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego incydentem wynosi 2 godziny. Maksymalny czas całkowitej obsługi Incydentu Krytycznego uzależniony jest od stopnia skomplikowania incydentu, ale nie może przekroczyć 72 h,
b) Czas reakcji dla Incydentów Istotnych wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego Zdarzeniem wynosi 4 godziny. Maksymalny czas całkowitej obsługi Incydentu Istotnego uzależniony jest od stopnia skomplikowania incydentu, ale nie może przekroczyć 72 h,
c) Czas reakcji dla Zdarzenia wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego incydentem wynosi 12 godziny. Maksymalny czas całkowitej obsługi Zdarzenia uzależniony jest od stopnia skomplikowania zdarzenia, ale nie może przekroczyć 1 tygodnia;
3) Incydenty i Zdarzenia rejestrowane są w systemie obsługi zgłoszeń Wykonawcy;

4) Niezwłocznie po potwierdzeniu zgłoszenia Incydentu lub Zdarzenia Wykonawca przystąpi do ustalenia przyczyn wystąpienia incydentu;
5) Po ustaleniu przez Wykonawcę przyczyn wystąpienia incydentu, Wykonawca poinformuje Zamawiającego o szacowanym terminie usunięcia incydentu i przystąpi do usuwania jego skutków;
6) Na żądanie, w celu uzyskania dodatkowych informacji, przedstawiciel Wykonawcy może kontaktować się z koordynatorem umowy ze strony Zamawiającego.;
7) Niezwłocznie po usunięciu incydentu, koordynator Zamawiającego zostanie poinformowany o tym fakcie przez Wykonawcę pocztą elektroniczną lub telefonicznie;
8) Po otrzymaniu od Zamawiającego informacji o usunięciu incydentu Wykonawca zamknie Zgłoszenie.

na:
3. Wszystkie Incydenty i Zdarzenia objęte Usługą będą rejestrowane w systemie Wykonawcy bezpośrednio po ich wystąpieniu, a informacja o ich rejestracji (rejestracja Zgłoszenia) będzie przekazywana automatycznie na adres e-mail Zamawiającego: ……..
1) Szczegółowa procedura obsługi incydentów zostanie ustalona i obustronnie zatwierdzona przed uruchomieniem Usługi;

2) Termin realizacji prac związanych z obsługą Incydentu lub Zdarzenia zależy od wagi:
a) Czas reakcji dla Incydentów Krytycznych wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego Incydentem wynosi 2 godziny, przy czym pełna obsługa Incydentu Krytycznego powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Incydentu.

b) Czas reakcji dla Incydentów Istotnych wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego Incydentem wynosi 4 godziny, przy czym pełna obsługa Incydentu Istotnego powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Incydentu.

c) Czas reakcji dla Zdarzenia wynosi 60 minut, maksymalny czas mitygacji zagrożenia spowodowanego Zdarzeniem wynosi 12 godzin, przy czym pełna obsługa Zdarzenia powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Zdarzenia.

4) Niezwłocznie po potwierdzeniu wystąpienia Incydentu lub Zdarzenia Wykonawca przystąpi do jego mitygacji i eliminacji wpływu na środowisko Zamawiającego, a także ustalenia przyczyn jego wystąpienia;

6) Jeżeli wystąpi taka konieczność, w celu uzyskania dodatkowych informacji, przedstawiciel Wykonawcy może kontaktować się z koordynatorem umowy ze strony Zamawiającego;

7) Niezwłocznie po zmitygowaniu Incydentu lub Zdarzenia, koordynator Zamawiającego zostanie poinformowany o tym fakcie przez Wykonawcę pocztą elektroniczną lub telefonicznie;

8) Po przekazaniu Zamawiającemu informacji o zmitygowaniu Incydentu lub Zdarzenia oraz po potwierdzeniu zakończenia wszystkich działań związanych z obsługą Incydentu lub Zdarzenia, w tym po przekazaniu analizy powłamaniowej – jeżeli dotyczy – Wykonawca zamyka Zgłoszenie.

Wzór Umowy, § 7 ust. 4-6
z:
4. Za każdą rozpoczętą godzinę zwłoki w stosunku do maksymalnego czasu całkowitej obsługi Incydentu Krytycznego określonego w § 3 ust. 3 pkt. 2 lit. a) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.
5. Za każdą rozpoczętą godzinę zwłoki w stosunku do maksymalnego czasu całkowitej obsługi Incydentu Istotnego określonego w § 3 ust. 3 pkt. 2 lit. b) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.
6. Za każdy rozpoczęty dzień zwłoki w stosunku maksymalnego czasu całkowitej obsługi Zdarzenia do terminów określonych w § 3 ust. 3 pkt. 2 lit. c) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.

na:
4. Za każdą rozpoczętą godzinę zwłoki w stosunku do maksymalnego czasu mitygacji zagrożenia spowodowanego Incydentem, o którym mowa w § 3 ust. 3 pkt. 2 lit. a) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.
5. Za każdą rozpoczętą godzinę zwłoki w stosunku do maksymalnego czasu mitygacji zagrożenia spowodowanego Incydentem, o którym mowa w § 3 ust. 3 pkt. 2 lit. b) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 150 zł.
6. Za każdy rozpoczęty dzień zwłoki w stosunku maksymalnego czasu mitygacji zagrożenia spowodowanego Zdarzeniem, o którym mowa w § 3 ust. 3 pkt. 2 lit. c) Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 200 zł.

Załącznik nr 1 do SWZ OPIS PRZEDMIOTU ZAMÓWIENIA
w pkt I.9
z:
9. Czasy reakcji i obsługi incydentów (SLA)
Wykonawca zobowiązuje się do przestrzegania czasów reakcji i obsługi incydentów zgodnie z klasyfikacją uzgodnioną z Zamawiającym oraz do bezzwłocznego powiadomienia Zamawiającego o wykryciu incydentu.
a) Incydenty krytyczne - powodujące możliwość przerwy w pracy systemów produkcyjnych, utraty lub modyfikacji danych bądź wystąpienia wymiernych strat wizerunkowych

- czas reakcji: do 60 minut,

- maksymalny czas mitygacji zagrożenia spowodowanego incydentem po stronie SOC: do 2 godzin, przy czym maksymalny czas całkowitej obsługi incydentu krytycznego uzależniony jest od stopnia skomplikowania incydentu, ale nie może przekroczyć 72 h,
- maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego: do 1 godziny.

Dla zdarzeń krytycznych zostanie bezwzględnie ustalona i obustronnie zatwierdzona procedura eskalacji, uruchamiana w przypadku nieskutecznych prób kontaktu z personelem technicznym Zamawiającego przy wykorzystaniu ustalonych kanałów komunikacji.

b) Incydenty istotne - wpływa na działanie systemów lub bezpieczeństwo informacji, ale nie powoduje zatrzymania kluczowych procesów ani wymiernych strat

- czas reakcji: do 60 minut,
- maksymalny czas mitygacji zagrożenia spowodowanego incydentem po stronie SOC: do 4 godzin, przy czym maksymalny czas całkowitej obsługi incydentu krytycznego uzależniony jest od stopnia skomplikowania incydentu, ale nie może przekroczyć 72 h,
- maksymalny czas wykonania trzech prób powiadomienia personelu technicznego Zamawiającego: do 1 godziny.

c) Zdarzenia o niskim poziomie istotności - nie wpływają na działanie kluczowych systemów ani bezpieczeństwo informacji w stopniu powodującym natychmiastowe ryzyko

- czas reakcji: do 60 minut,
- maksymalny czas przy czym maksymalny czas całkowitej obsługi zagrożenia spowodowanego zdarzeniem po stronie SOC: 4 godziny, przy czym maksymalny czas całkowitej obsługi zdarzenia uzależniony jest od stopnia skomplikowania zdarzenia, ale nie może przekroczyć 1 tygodnia
- kontakt z personelem technicznym Zamawiającego: do 12 godzin.

Klasyfikacja poziomów incydentów bezpieczeństwa zostanie szczegółowo uzgodniona w ramach etapu wdrożenia usługi SOC oraz ujęta w procedurach monitorowania i reagowania na incydenty wykonanych prze Wykonawcę.

na:

9. Czasy reakcji i obsługi incydentów (SLA)

Wykonawca zobowiązuje się do przestrzegania czasów reakcji i obsługi incydentów zgodnie z klasyfikacją uzgodnioną z Zamawiającym oraz do bezzwłocznego powiadomienia Zamawiającego o wykryciu incydentu.

a) Incydenty Krytyczne – powodujące możliwość przerwy w pracy systemów produkcyjnych, utraty lub modyfikacji danych bądź wystąpienia wymiernych strat wizerunkowych

- czas reakcji: do 60 minut,

- maksymalny czas mitygacji zagrożenia spowodowanego Incydentem po stronie SOC: do 2 godzin, przy czym pełna obsługa Incydentu Krytycznego powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Incydentu,
- maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego: do 1 godziny.

Dla zdarzeń krytycznych zostanie bezwzględnie ustalona i obustronnie zatwierdzona procedura eskalacji, uruchamiana w przypadku nieskutecznych prób kontaktu z personelem technicznym Zamawiającego przy wykorzystaniu ustalonych kanałów komunikacji.

b) Incydenty Istotne – wpływające na działanie systemów lub bezpieczeństwo informacji, ale nie powodujące zatrzymania kluczowych procesów ani wymiernych strat

- czas reakcji: do 60 minut,
- maksymalny czas mitygacji zagrożenia spowodowanego Incydentem po stronie SOC: do 4 godzin, przy czym pełna obsługa Incydentu Istotnego powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Incydentu,
- maksymalny czas wykonania trzech prób powiadomienia personelu technicznego Zamawiającego: do 1 godziny.

c) Zdarzenia o niskim poziomie istotności - nie wpływają na działanie kluczowych systemów ani bezpieczeństwo informacji w stopniu powodującym natychmiastowe ryzyko

- czas reakcji: do 60 minut,
- maksymalny czas przy czym maksymalny czas całkowitej obsługi zagrożenia spowodowanego Zdarzeniem po stronie SOC: 4 godziny, przy czym pełna obsługa Zdarzenia o niskim poziomie istotności powinna zakończyć się przekazaniem Zamawiającemu informacji zwrotnej przez Wykonawcę potwierdzającej zakończenie wszystkich działań związanych z obsługą Zdarzenia.
- kontakt z personelem technicznym Zamawiającego: do 12 godzin.

Klasyfikacja poziomów incydentów bezpieczeństwa zostanie szczegółowo uzgodniona w ramach etapu wdrożenia usługi SOC oraz ujęta w procedurach monitorowania i reagowania na incydenty wykonanych przez Wykonawcę.

Treść pytania nr #27

Zamawiający w projekcie Umowy dzieli wynagrodzenie na dwie części: wdrożenie i uruchomienie usługi SOC oraz monitorowanie środowiska Zamawiającego. W formularzu oferty występuje jedynie rubryka dotycząca całkowitej wartości zamówienia a także sugestia realizacji zamówienia w terminie od 20 do 30 dni. Treść SWZ wyraźnie określa, że zamówienie składa się z dwóch części: wdrożenia usługi w terminie do 30 dni oraz monitorowania przez 12 miesięcy.

Prosimy o wyjaśnienie, ile części składowych będzie miało wynagrodzenie oraz w jaki sposób będzie wypłacane.

Odpowiedź Zamawiającego na pytanie nr #27 – ZMIANA SWZ

W odpowiedzi na pytanie Zamawiający udostępnia zmieniony wzór Załącznika nr 3 do SWZ - „FORMULARZ OFERTOWY" oraz zmienia treść SWZ w następującym zakresie:

Wzór Umowy
w § 6 ust. 1 pkt 2)
z:
2) wynagrodzenie za Monitorowanie i obsługę incydentów bezpieczeństwa w wysokości: …….. zł netto (słownie złotych:……), powiększone o podatek VAT, co daje kwotę …… zł brutto (słownie: ….).

na:
2) wynagrodzenie za Monitorowanie i obsługę incydentów bezpieczeństwa w wysokości: …….. zł netto (słownie złotych:……), powiększone o podatek VAT, co daje kwotę …… zł brutto (słownie: ….), płatne miesięcznie w dwunastu równych częściach, po zaakceptowaniu przez Zamawiającego miesięcznego raportu z prac SOC, o którym mowa w § 3 ust 4.

w § 6 ust. 3.
z:
3. Wynagrodzenie, Zamawiający zapłaci Wykonawcy na podstawie prawidłowo wystawionej faktury po dokonaniu odbioru i podpisaniu bez zastrzeżeń Protokołu Odbioru Końcowego. Przez prawidłowo wystawioną fakturę Strony rozumieją fakturę wystawioną zgodnie z obowiązującymi przepisami, postanowieniami umowy oraz pozytywnie zweryfikowanym rachunkiem bankowym w wykazie podmiotów, o którym mowa w art. 96b ustawy o podatku od towarów i usług (tj. Dz.U. z 2025 r. poz. 775).

na:
3. Wynagrodzenie, o którym mowa:
1) w ust. 1 pkt 1) Zamawiający zapłaci Wykonawcy na podstawie prawidłowo wystawionej faktury po dokonaniu odbioru i podpisaniu bez zastrzeżeń Protokołu Odbioru Końcowego,
2) w ust. 1 pkt 2) Zamawiający zapłaci Wykonawcy na podstawie prawidłowo wystawionej faktury po zaakceptowaniu przez Zamawiającego miesięcznego raportu z prac SOC.
Przez prawidłowo wystawioną fakturę Strony rozumieją fakturę wystawioną zgodnie z obowiązującymi przepisami, postanowieniami umowy oraz pozytywnie zweryfikowanym rachunkiem bankowym w wykazie podmiotów, o którym mowa w art. 96b ustawy o podatku od towarów i usług (tj. Dz.U. z 2025 r. poz. 775).

Treść pytania nr #28
W §6 Umowy, Zamawiający opisuje warunki na jakich będzie wypłacane Wykonawcy wynagrodzenie. W punkcie 3, Zamawiający piszę, że „zapłaci Wykonawcy na podstawie prawidłowo wystawionej faktury po dokonaniu odbioru i podpisaniu bez zastrzeżeń Protokołu Odbioru Końcowego." Wskazany protokół odbioru końcowego (zał. Nr 3 do Umowy) wyraźnie dotyczy uruchomienia usługi SOC. Nie ma odrębnego protokołu dotyczącego monitorowania.
W kontekście powyższej nieścisłości informujemy, że powszechną praktyką wynagradzania za monitorowanie SOC jest abonament miesięczny, płatny z dołu, na podstawie podpisanej umowy. Dzieje się tak dlatego, że Wykonawca ponosi bieżące koszty utrzymania SOC i musi mieć bieżące środki do ich pokrycia. Jedynym odstępstwem od tej reguły, stosowanym w nielicznych przypadkach jest płatność wynagrodzenia w całości z góry. W takiej sytuacji Zmawiający jest z rozliczony z Wykonawcą co do wynagrodzenia a gwarantem prawidłowego wykonania usługi są zapisy umowy określające zasady współpracy oraz kary umowne w sytuacjach, gdy warunki nie zostaną spełnione.
W związku z powyższym, prosimy o sprecyzowanie w jaki sposób będzie wypłacane wynagrodzenie za monitorowanie infrastruktury Zamawiającego.

Odpowiedź Zamawiającego na pytanie nr #28
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 27.

Treść pytania nr #29
1) Zakres monitorowanych zasobów
1. Prosimy o podanie liczby wszystkich domen głównych organizacji;
2. Czy Zamawiający posiada dodatkowe marki, subdomeny, aliasy, domeny powiązane? Jeśli tak – prosimy o pełny wykaz liczby.
3. Prosimy o przekazanie liczby i zakresów adresów IP / bloków CIDR, które mają być objęte monitoringiem oraz skanowaniem.
4. Czy Zamawiający wymaga monitorowania również:
   - zasobów partnerów / łańcucha dostaw,
   - aplikacji mobilnych,
   - mediów społecznościowych (fałszywe konta, treści)?

Odpowiedź Zamawiającego na pytanie nr #29
Zamawiający informuje, że:

1. Liczba głównych domen organizacji wynosi dwie: uprp.gov.pl oraz uprp.pl.
2. Dodatkowe subdomeny i aliasy obejmują: *.pue.uprp.gov.pl, *.uprp.gov.pl oraz *.uprp.pl. Szczegółowe dane zostaną udostępnione po rozstrzygnięciu postępowania.
3. Zamawiający dysponuje około 100 publicznymi adresami IP, które mogą być objęte monitoringiem i skanowaniem. Szczegółowe dane zostaną udostępnione po rozstrzygnięciu postępowania.

4. Zamawiający dopuszcza objęcie monitorowaniem również mediów społecznościowych, pod kątem fałszywych kont i treści.

Treść pytania nr #30

2) Monitoring Dark Web / Deep Web

5. Jakie typy danych wrażliwych mają być wyszukiwane w dark web (np. e-maile, dane osobowe, loginy, dokumenty, wycieki danych klientów)?
6. Czy Zamawiający oczekuje monitorowania marketplace'ów, for, ransomware leak sites czy tylko ogólnych źródeł?
7. Czy wymagane jest raportowanie incydentów związanych z łańcuchem dostaw wykrytych w Dark Web?

Odpowiedź Zamawiającego na pytanie nr #30

Zamawiający informuje, że w zakresie monitoringu dark web wyszukiwane mają być w szczególności słowa kluczowe, domeny (w tym adresy e-mail), adresy IP oraz inne dane powiązane z Zamawiającym (zakres słów kluczowych został wskazany w odpowiedzi na pytanie nr 20). Zamawiający nie określa sposobu realizacji monitoringu dark web ani konkretnych źródeł, pozostawiając dobór metod po stronie Wykonawcy. Zamawiający nie wymaga raportowania incydentów związanych z łańcuchem dostaw wykrytych w dark web, jednak dopuszcza taką możliwość.

Treść pytania nr #31

3) Skanowanie i analityka

8. Czy Zamawiający dopuszcza aktywne skanowanie (skanowanie portów/podatności).
9. Czy wymagane jest wykrywanie:
   - podatności krytycznych,
   - skanowanie ransomware-based CVE?
10. Czy Zamawiający oczekuje integracji z własnymi systemami SIEM/SOAR? Jeśli tak – prosimy o wskazanie typu: Sigma/YARA/Suricata.

Odpowiedź Zamawiającego na pytanie nr #31

Zamawiający informuje, że dopuszcza prowadzenie aktywnego skanowania, w tym skanowania portów i podatności. W zakresie wykrywania podatności Zamawiający oczekuje identyfikacji podatności krytycznych w sprzęcie i oprogramowaniu Zamawiającego, co wynika z zapisów OPZ. Zamawiający nie wymaga wykrywania ransomware-based CVE, jednak dopuszcza taką możliwość. Zamawiający nie wymaga integracji z własnymi systemami SIEM/SOAR.

Treść pytania nr #32

4) Zakres IOC

11. Jakiego typu Indicators of Compromise mają być dostarczane:

- domeny,
- IP,
- hashe,

- e-maile,
- URL,
- dane malware?

12. Czy Zamawiający wymaga IOC Enrichment (wzbogacania IOC o kontekst)?

Odpowiedź Zamawiającego na pytanie nr #32
Zamawiający informuje, że oczekuje dostarczania wskaźników Indicators of Compromise w szczególności w postaci domen, adresów IP, hashy, adresów e-mail oraz URL. Zamawiający nie wymaga IOC Enrichment, jednak nie wyklucza jego stosowania i dopuszcza jego realizację według podejścia Wykonawcy.

Treść pytania nr #33
5) Raportowanie i tryb pracy

13. Jaka jest oczekiwana częstotliwość raportowania w ramach CTI (miesięczne, tygodniowe, incydentalne)?
14. Czy wymagane są:
    - Raporty okresowe,
    - Raporty z analizy incydentów,
    - Newsletter (Dark Web / ogólny)?
15. Czy Zamawiający oczekuje wsparcia analityka CTI w formie:
    - triage incydentów,
    - rekomendacji mitigacyjnych,
    - szczegółowej analizy incydentu?

Odpowiedź Zamawiającego na pytanie nr #33
Zamawiający informuje, że częstotliwość raportowania w ramach CTI jest określona w OPZ, tj. raportowanie odbywa się nie rzadziej niż raz w miesiącu. W zakresie CTI Zamawiający oczekuje przekazywania rekomendacji mitigacyjnych oraz zaleceń działań korygujących, umożliwiających skuteczne reagowanie na potencjalne zagrożenia i minimalizowanie ryzyka ich wystąpienia.

Treść pytania nr #34
6) Reakcja na incydenty

16. Czy Zamawiający wymaga koordynacji obsługi incydentów, informowania o High/Critical, i rekomendacji działań korygujących?
17. Czy przewidywane jest przekazywanie incydentów do zespołu IR po stronie Zamawiającego?

Odpowiedź Zamawiającego na pytanie nr #34
Zamawiający informuje, że oczekuje koordynacji obsługi incydentów, informowania o incydentach o wysokim i krytycznym poziomie oraz przekazywania rekomendacji działań korygujących, a także przekazywania incydentów do zespołu IR po stronie Zamawiającego. Powyższy zakres wynika z zapisów OPZ, w szczególności z pkt 7 i 8.

Treść pytania nr #35

8) Cele i kryteria sukcesu

18. Jakie są kluczowe kryteria sukcesu dla Zamawiającego?
19. Czy Zamawiający kładzie większy nacisk na:
    a. wykrywanie wycieków,
    b. monitoring reputacji,
    c. wykrywanie podatności,
    d. ochronę VIP,
    e. detekcję phishingu,
    f. monitoring IoC?

Odpowiedź Zamawiającego na pytanie nr #35

Zamawiający informuje, że kluczowym kryterium sukcesu jest podniesienie poziomu bezpieczeństwa środowiska teleinformatycznego oraz zdolność do szybkiego wykrywania i ograniczania zagrożeń. Zamawiający kładzie nacisk w szczególności na ochronę przed szkodliwym oprogramowaniem oraz zagrożeniami wynikającymi z działalności cyberprzestępczej.

Treść pytania nr #36

9) Integracje i środowisko

20. Czy CTI ma integrować się z:
    a. SIEM,
    b. SOAR,
    c. ticketing (JIRA/ServiceNow),
    d. EDR,
    e. Firewall?
21. Czy Zamawiający ma wymogi RODO/sieciowe ograniczające import danych?

Odpowiedź Zamawiającego na pytanie nr #36

Zamawiający informuje, że dopuszcza integrację usługi CTI z systemami EDR, NDR oraz firewallami, umożliwiając przesyłanie i automatyczne zasilanie tych systemów danymi takimi jak adresy IP, hashe i domeny. W zakresie wymogów RODO i bezpieczeństwa sieci Zamawiający nie przewiduje dodatkowych ograniczeń poza obowiązującymi przepisami oraz wewnętrznymi dokumentami bezpieczeństwa, przy czym wszelka komunikacja musi być realizowana w sposób bezpieczny i szyfrowany.

Treść pytania nr #37

10) Zakres dodatkowych funkcji

22. Czy Zamawiający przewiduje wymóg:
    a. Malware Analysis (sandbox),
    b. Takedown Management (zdejmowanie domen phishingowych),
    c. Canary Tokens,
    d. dostęp do baz wycieków / breach datasets?

Odpowiedź Zamawiającego na pytanie nr #37
Zamawiający wyjaśnia, że nie wymaga wskazanych funkcjonalności, jednak dopuszcza ich zastosowanie przez Wykonawcę.

Treść pytania nr #38
Dot. p.5
Czy Zamawiający dopuszcza zmianę zapisów:
"Monitorowanie systemów EDR i NDR
Usługa obejmuje całodobowe monitorowanie i analizę zagrożeń z wykorzystaniem systemów klasy EDR i NDR, posiadanych przez Zamawiającego, realizowane przez analityków zespołu SOC w trybie 24/7/365. W ramach monitorowania EDR i NDR wymagane są w szczególności następujące funkcje:
a) Wzmocnienie konfiguracji bezpieczeństwa systemów
• analiza zdarzeń wykrytych lub zablokowanych przez systemy EDR i NDR w celu identyfikacji luk w konfiguracji lub politykach bezpieczeństwa,
• opracowanie i przekazywanie rekomendacji dotyczących wzmocnienia konfiguracji zabezpieczeń urządzeń końcowych (hardening).
b) Redukcja fałszywych alarmów
• analiza fałszywych alarmów generowanych przez systemy EDR i NDR w celu identyfikacji ich przyczyn,
• wdrażanie korekt w regułach detekcji i mechanizmach alertowania, mających na celu ograniczenie liczby nieuzasadnionych powiadomień.
c) Wzbogacanie detekcji o zewnętrzne źródła danych
• zasilanie systemów EDR i NDR zewnętrznymi feedami bezpieczeństwa oraz feedami wynikającymi z analiz prowadzonych przez SOC,
• przygotowanie szczegółowych informacji o zdarzeniach, w przypadku gdy zagrożenie nie zostało automatycznie zablokowane przez EDR lub NDR (true positive).
d) Raportowanie
• sporządzanie miesięcznego raportu z realizacji usługi monitorowania EDR i NDR."
Na następujący zapis:
"Monitorowanie systemów EDR
Usługa obejmuje całodobowe monitorowanie i analizę zagrożeń z wykorzystaniem systemów klasy EDR, posiadanych przez Zamawiającego, realizowane przez analityków zespołu SOC w trybie 24/7/365. W ramach monitorowania EDR wymagane są w szczególności następujące funkcje:
a) Wzmocnienie konfiguracji bezpieczeństwa systemów
• analiza zdarzeń wykrytych lub zablokowanych przez systemy EDR w celu identyfikacji luk w konfiguracji lub politykach bezpieczeństwa,
• opracowanie i przekazywanie rekomendacji dotyczących wzmocnienia konfiguracji zabezpieczeń urządzeń końcowych (hardening).
b) Redukcja fałszywych alarmów
• analiza fałszywych alarmów generowanych przez systemy EDR w celu identyfikacji ich przyczyn,
• wdrażanie korekt w regułach detekcji i mechanizmach alertowania, mających na celu ograniczenie liczby nieuzasadnionych powiadomień.

c) Wzbogacanie detekcji o zewnętrzne źródła danych
• Dostarczenie zewnętrzych feedów bezpieczeństwa oraz feedów wynikających z analiz prowadzonych przez SOC
• przygotowanie szczegółowych informacji o zdarzeniach, w przypadku gdy zagrożenie nie zostało automatycznie zablokowane przez EDR (true positive).
d) Raportowanie
• sporządzanie miesięcznego raportu z realizacji usługi monitorowania EDR.

Monitorowanie systemów NDR
Usługa obejmuje całodobowe monitorowanie i analizę zagrożeń zwyko rzystaniem systemów klasy NDR, posiadanych przez Zamawiającego, realizowane przez analityków zespołu SOC w trybie 24/7/365. W ramach monitorowania NDR wymagane są w szczególności następujące funkcje:
a) Wzmocnienie konfiguracji bezpieczeństwa systemów
• analiza zdarzeń wykrytych lub zablokowanych przez systemy NDR w celu identyfikacji luk w konfiguracji lub politykach bezpieczeństwa w oparciu o narzędzie SIEM/SOAR
b) Wzbogacanie detekcji o zewnętrzne źródła danych
• Dostarczenie zewnętrzych feedów bezpieczeństwa oraz feedów wynikających z analiz prowadzonych przez SOC
• przygotowanie szczegółowych informacji o zdarzeniach, w przypadku gdy zagrożenie nie zostało automatycznie zablokowane przez NDR (true positive).
c) Raportowanie
• sporządzanie miesięcznego raportu z realizacji usługi monitorowania NDR"

Odpowiedź Zamawiającego na pytanie nr #38
Zamawiający informuje, że nie przewiduje zmiany zapisu. Wymagane pozostaje monitorowanie zarówno systemów EDR, jak i NDR, zgodnie z treścią OPZ.

Treść pytania nr #39
Prosimy o rozwinięcie zapisu – dot. p.3B
"nadzór nad zasobami i bazami reputacyjnymi pod kątem domen, adresów IP oraz innych aktywów Zamawiającego."

Odpowiedź Zamawiającego na pytanie nr #39
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 21.

Treść pytania nr #40
Zwracamy się z uprzejmą prośbą o wskazanie nazw i producentów systemów klasy EDR oraz klasy NDR jakie Zamawiający posiada w swojej infrastrukturze co pozwoli Wykonawcy na odpowiednie zwymiarowanie świadczonej przez niego usługi.

Odpowiedź Zamawiającego na pytanie nr #40
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 1.

Treść pytania nr #41
Czy systemy klasy EDR i klasy NDR są w pełni skonfigurowane?
Czy rozwiązanie EDR posiada zaimplementowane polityki bezpieczeństwa?
Czy rozwiązanie NDR zbiera dane z przepływów sieciowych oraz logów z wszystkich urządzeń sieciowych będących w infrastrukturze Zamawiającego?
Czy system NDR jest zintegrowany z rozwiązaniem EDR?

Odpowiedź Zamawiającego na pytanie nr #41
Zamawiający informuje, że systemy klasy EDR i NDR są skonfigurowane, a rozwiązanie EDR posiada zaimplementowane polityki bezpieczeństwa. Rozwiązanie NDR zbiera metadane z przepływów sieciowych, natomiast logi z urządzeń sieciowych gromadzone są w innych systemach Zamawiającego. System NDR jest zintegrowany z rozwiązaniem EDR.

Treść pytania nr #42
Czy systemy bezpieczeństwa Zamawiającego posiadają minimum 30-dniową retencję logów? Taka retencja jest niezbędna do prowadzenia usługi Threat huntingu.

Odpowiedź Zamawiającego na pytanie nr #42
Zamawiający informuje, że systemy bezpieczeństwa posiadają minimum 30-dniową retencję logów.

Treść pytania nr #43
Czy Zamawiający aktualnie prowadzi samodzielnie monitorowanie swojej infrastruktury?
Jeśli tak to zwracamy się z prośbą o podanie przybliżonej ilość detekcji obsługiwanych w ciągu miesiąca.

Odpowiedź Zamawiającego na pytanie nr #43
Zamawiający informuje, że prowadzi samodzielne monitorowanie swojej infrastruktury, uzupełniane o dane otrzymywane z krajowych CSIRT-ów. Przybliżona liczba detekcji obsługiwanych w ciągu miesiąca została podana w odpowiedzi na pytanie nr 14.

Treść pytania nr #44
Zwracamy się z uprzejmą prośbą o podanie szczegółowego zakresu wdrożenia usługi (realizacji zamówienia) oraz wskazanie co jest konkretnie wymagane od Wykonawcy.
Czy w ramach tego procesu będzie m.in. wymaganym, aby Wykonawca skonfigurował systemy bezpieczeństwa, podłączył źródła itp.?

Odpowiedź Zamawiającego na pytanie nr #44
Zamawiający informuje, że zakres uruchomienia i utrzymania usługi SOC został określone w OPZ. Wykonawca, przy współpracy z Zamawiającym, będzie zobowiązany do podłączenia się do systemów bezpieczeństwa Zamawiającego oraz do zasilania tych systemów danymi i wskaźnikami w celu monitorowania i wykrywania zagrożeń, przy

zachowaniu wszystkich obowiązujących procedur bezpieczeństwa oraz standardów technicznych obowiązujących w środowisku Zamawiającego.

Treść pytania nr #45
Zgodnie z § 2 ust 1 Wykonawca zobowiązuje się do „Uruchomienia i utrzymania usługi SOC" w terminie maksymalnie 20/25/30 dni od dnia zawarcia umowy, w zależności od zadeklarowanego terminu przez Wykonawcę w Formularzu ofertowym.
Czy termin wskazany w § 2 ust 1 dotyczy wyłącznie uruchomienia usługi SOC czy także utrzymania usługi SOC?

Odpowiedź Zamawiającego na pytanie nr #45 – ZMIANA SWZ
W odpowiedzi na pytanie Zamawiający zmienia treść SWZ:

Wzór Umowy
w § 1 ust. 1
z:
1. Przedmiotem umowy jest świadczenie przez okres 12 miesięcy usługi reakcji na incydenty bezpieczeństwa SOC (Security Operations Center) w szczególności:
1) Uruchomienie i utrzymanie usługi SOC;
2) Monitorowanie i obsługa incydentów bezpieczeństwa

na
1. Przedmiotem umowy jest świadczenie przez okres 12 miesięcy usługi reakcji na incydenty bezpieczeństwa SOC (Security Operations Center) w szczególności:
1) Uruchomienie usługi SOC;
2) Utrzymanie usługi SOC, monitorowanie i obsługa incydentów bezpieczeństwa

Załącznik nr 1 do SWZ OPIS PRZEDMIOTU ZAMÓWIENIA
w pkt I.2

z:
2. Uruchomienie i utrzymanie usługi SOC

na:
2. Uruchomienie usługi SOC

Treść pytania nr #46
Czy Zamawiający wyrazi zgodę, aby zgłoszenia i obsługa incydentów objętych Usługą były przyjmowane przez serwis Wykonawcy za pomocą dodatkowego kanału komunikacji, czyli dedykowanego portalu zgłoszeniowego Wykonawcy? Zwracamy się z uprzejmą prośbą o akceptację oraz odpowiednią modyfikację zapisu.

Odpowiedź Zamawiającego na pytanie nr #46
Zamawiający informuje, że zgodnie z zapisami OPZ Wykonawca zobowiązany jest do zapewnienia dedykowanego kanału komunikacji z dyżurem technicznym SOC, obejmującego numer telefonu i adres e-mail do kontaktu, umożliwiającego niezwłoczny kontakt w przypadku wystąpienia zdarzeń lub incydentów bezpieczeństwa. Jednocześnie Zamawiający nie wyklucza możliwości przyjmowania zgłoszeń i obsługi incydentów również za pośrednictwem dodatkowego kanału komunikacji, w tym dedykowanego portalu zgłoszeniowego Wykonawcy.

Treść pytania nr #47
Uprzejmie prosimy o doprecyzowanie jakie informacje ma zawierać miesięczny raport.

Odpowiedź Zamawiającego na pytanie nr #47
Zamawiający informuje, że niezbędne minimum, które powinien zawierać miesięczny raport, obejmuje podsumowanie wykrytych zagrożeń, źródła, celu, czasów: zgłoszenia, reakcji, mitygacji zagrożenia, całkowitej obsługi incydentu, opis incydentów bezpieczeństwa wraz z podjętymi działaniami oraz w przypadku ich występowania, rekomendacje mitigacyjne i zalecenia działań korygujących umożliwiające minimalizowanie ryzyka wystąpienia zagrożeń.

Treść pytania nr #48
Zwracamy się z uprzejmą prośbą o dodanie poniższego zapisu w sytuacji kiedy to będzie dotyczył Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza:
„Wykonawca oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.”

Odpowiedź Zamawiającego na pytanie nr #48
Zamawiający wyraża zgodę na dodatnie powyższego zapisu w przypadku wybrania podmiotu o takim statusie.

Treść pytania nr #49
Pytanie do par. 3 ust. 9
Wnosimy o wykreślenie tego ustępu. Obowiązek jest nieadekwatny w stosunku do charakteru i zakresu usługi SOC, która stanowi przedmiot umowy. Brak uzasadnienia do nakładania na Wykonawcę obowiązku czynnego udziału w tego rodzaju działaniach, zwłaszcza gdy zakres takich działań oraz ich czasochłonność nie zostały określone ani sprecyzowane w umowie.

Odpowiedź Zamawiającego na pytanie nr #49
Zamawiający nie przewiduje zmian SWZ w tym zakresie.

Treść pytania nr #50
Pytanie do par. 5 ust. 7

Proszę o dodanie zastrzeżenia, że zgoda Zamawiającego nie jest wymagana w przypadku zmiany członka personelu z powodów niezależnych od Wykonawcy, takich jak wypowiedzenie umowy przez pracownika, dłuższa nieobecność z powodu choroby czy inne sytuacje losowe, które uniemożliwiają dalsze świadczenie usług przez danego pracownika.

Odpowiedź Zamawiającego na pytanie nr #50
Zamawiający nie przewiduje zmian SWZ w tym zakresie.

Treść pytania nr #51
Pytanie do par. 7 ust. 4-6
Proszę o dostosowanie wysokości kar umownych w zależności od naruszenia terminów obsługi incydentów/zdarzeń. Obecnie kary są jednakowe, niezależnie od tego, czy chodzi o naruszenie obsługi incydentu krytycznego (które powoduje przerwę w pracy systemów produkcyjnych), czy o naruszenie obsługi zdarzenia o niskim poziomie istotności, które nie wpływa na działanie kluczowych systemów ani na bezpieczeństwo informacji. Proponujemy ustalenie kary w wysokości 150 zł za incydent istotny oraz 50 zł za zdarzenie.

Odpowiedź Zamawiającego na pytanie nr #51
Zamawiający dokonał zmiany SWZ w tym zakresie przy odpowiedzi na pytanie nr 26.

Treść pytania nr #52
Pytanie do par. 10 ust. 2 pkt 1
Proszę o zastrzeżenie, że odstąpienie od umowy powinno być możliwe wyłącznie w przypadku zwłoki Wykonawcy, a nie jedynie opóźnienia. Wykonawca nie powinien ponosić negatywnych skutków, takich jak odstąpienie od umowy, z powodu przyczyn od niego niezależnych, w tym przyczyn leżących po stronie Zamawiającego.

Odpowiedź Zamawiającego na pytanie nr #52- – ZMIANA SWZ
W odpowiedzi na pytanie Zamawiający zmienia treść SWZ w zakresie:

Wzór Umowy
w § 10 ust. 2 pkt 1
z:

1) Wykonawca opóźnia się w spełnieniu przedmiotu umowy powyżej 7 dni roboczych;

na

1) W przypadku zwłoki Wykonawcy w spełnieniu przedmiotu umowy powyżej 7 dni roboczych;

Treść pytania nr #53
Pytanie do par. 10 ust. 2 pkt 2
Proszę o wprowadzenie zamkniętego katalogu okoliczności, które będą uprawniały Zamawiającego do odstąpienia od umowy.

Odpowiedź Zamawiającego na pytanie nr #53
Zamawiający nie przewiduje zmian SWZ w tym zakresie.

Treść pytania nr #54
Jakie dane powinien zawierać raport miesięczny?

Odpowiedź Zamawiającego na pytanie nr #54
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 47.

Treść pytania nr #55
Jakiego producenta i wersje EDR i NDR posiada Zamawiający?

Odpowiedź Zamawiającego na pytanie nr #55
Odpowiedz na pytanie została zawarta w odpowiedzi na pytanie nr 1.

Treść pytania nr #56
Jakich producentów i wersje dla pozostałych rozwiązań posiada Zamawiający w przypadku:
- klastry zapór sieciowych nowej generacji (NGFW),
- systemy analizy zdarzeń i logów,
- systemy klasy sandbox, IPS, WAF, DDoS Protection System.

Odpowiedź Zamawiającego na pytanie nr #56
Zamawiający informuje, że w środowisku funkcjonują następujące rozwiązania bezpieczeństwa:
- Klastry zapór sieciowych nowej generacji (NGFW): FortiGate
- Systemy analizy zdarzeń i logów: FortiAnalyzer
- Systemy klasy sandbox: FortiSandbox oraz Fidelis Security
- Systemy IPS: Forcepoint
- Systemy WAF: FortiWeb oraz Imperva
- Ochrona DDoS: Imperva oraz usługa świadczona przez ISP

Treść pytania nr #57
Jakich usług Zamawiający oczekuje w ramach usługi SOC?

Odpowiedź Zamawiającego na pytanie nr #57
Zamawiający oczekuje dostarczenia usługi SOC opisanej w SWZ.

Treść pytania nr #58
Czy Zamawiający w ramach usługi SOC oczekuje, by Wykonawca będzie realizował usługę w oparciu o narzędzia SIEM /SOAR.

Odpowiedź Zamawiającego na pytanie nr #58
Zamawiający informuje, że w ramach usługi SOC dopuszcza stosowanie narzędzi SIEM i SOAR przez Wykonawcę, przy czym ich wykorzystanie nie jest obligatoryjne.

Treść pytania nr #59
W związku ze specyfiką wdrożenia usługi SOC która obejmuje m.in. audyty wstępne oraz ustalenie i wdrożenie procedur, które są pracochłonne i wymagają oddelegowania pracowników po stronie Zamawiającego, wnosimy o zmianę terminu do 60 dni.

Odpowiedź Zamawiającego na pytanie nr #59
Zamawiający nie przewiduje zmian SWZ w tym zakresie.

Treść pytania nr #60
Czy Zamawiający posiada wolne zasoby na potrzeby instalacji rozwiązania SIEM / SOAR:
- vCPU - 24
- RAM – 24GB
- Przestrzeń dyskowa – 300 GB + 2TB vHDD
- OS - Microsoft Windows Server 2022
- Interfejsy sieciowe – 100 Mb/s Ethernet

Odpowiedź Zamawiającego na pytanie nr #60
Zamawiający informuje, że posiada zasoby spełniające wskazane wymagania.

Treść pytania nr #61
Czy Zamawiający dopuszcza połączenie VPN S2S?

Odpowiedź Zamawiającego na pytanie nr #61
Zamawiający informuje, że dopuszcza zestawienie połączenia VPN typu site-to-site.

DYREKTOR GENERALNY

Marcin Dobruk