OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiot zamówienia**

Świadczenie usługi SOC (Security Operation Center) polegającej na monitorowaniu, analizowaniu i reagowaniu na incydenty związane z cyberbezpieczeństwem w modelu usługowym (dostawca usługi zapewnia po swojej stronie wymaganą infrastrukturę, oprogramowanie i niezbędne zasoby) wraz z uruchomieniem i utrzymaniem systemu klasy SIEM (Security Information and Event Management).

1. **Realizacja Usługi**
	1. W ramach usługi Wykonawca zapewni monitorowanie bezpieczeństwa infrastruktury teleinformatycznej, systemów i działań użytkowników Zamawiającego w trybie 24/7/365.
	2. Wykonawca oświadcza spełnienie wymagań zawartych w „Rozporządzeniu 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”. Obiekty, które będą miejscem świadczenia usługi, muszą stanowić własność Usługodawcy.
	3. Monitorowanie bezpieczeństwa infrastruktury Zamawiającego oznacza co najmniej:
		1. Analizę logów w czasie rzeczywistym.
		2. Reagowanie na incydenty – realizację uzgodnionych scenariuszy (w tym zamykanie zdarzeń typu False Positive).
		3. Raportowanie.
		4. Identyfikowanie i zarządzanie podatnościami.
		5. Aktualizację narzędzi bezpieczeństwa.
	4. Wykonawca zapewni dostęp do wykwalikowanych analityków cyberbezpieczeństwa pracujących w SOC w trybie pracy 24/7/365.
	5. Wykonawca zapewnia informowanie Zamawiającego o wykrytych incydentach krytycznych w ciągu 1 godziny, oraz o wykrytych innych incydentach w ciągu 4 godzin od momentu ich wykrycia oraz o podjętych działaniach za pośrednictwem ustalonych w umowie kanałów komunikacji (telefon, e-mail).
	6. Usługa SOC musi być świadczona w siedzibie wykonawcy
	7. Zamawiający wymaga, aby usługa SOC świadczona przez Wykonawcę spełniała wskaźniki efektywności obsługi incydentów. Jako poprawne wartości przyjmuje się:
		1. Czas reakcji na incydent – 15 minut bez względu na typ incydentu (krytyczny, istotny, niski). Czas reakcji rozumiany jest jako czas pomiędzy wykryciem incydentu bezpieczeństwa do momentu podjęcia działań po stronie zespołu SOC Usługodawcy.
		2. Czas obsługi incydentu: krytycznego – 2 godziny, istotnego 4 godziny, niskiego 16 godzin. Czas obsługi rozumiany jest jako czas potrzebny na zakończenie incydentu, usunięcie zagrożenia i przywrócenie normalnego funkcjonowania systemu lub infrastruktury.
2. **Wymagania ogólne dla Usługi**
	1. Wykonawca musi legitymować się ważnym certyfikatem ISO 27001 dla świadczonej usług bezpieczeństwa, wystawionym na Usługodawcę i ważnym w całym okresie świadczenia usługi.
	2. Wykonawca musi posiadać wdrożone procedury ciągłości działania określone normą ISO:22301 ważne w całym okresie świadczenia usługi.
	3. Wykonawca musi posiadać certyfikaty w ilości minimum **:** 2 CEH oraz 1 CompTIA Security +.
	4. Wykonawca musi posiadać certyfikat 9001 ważny w całym okresie świadczenia usługi.
	5. Wykonawca musi posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF).
	6. Wykonawca powinien posiadać minimum dwa certyfikaty z zarządzania platformą vendora SIEM ważne w całym okresie świadczenia usługi.
	7. Wykonawca powinien posiadać ubezpieczenie OC działalności na kwotę minimum 2 mln złotych ważną w całym okresie świadczenia usługi.
	8. Wykonawca musi posiadać zespół SOC, wszyscy pracownicy Wykonawcy zaangażowani bezpośrednio w świadczenie usługi powinni być zatrudnieni przez Wykonawcę na zasadach umowy o pracę minimum 8 osób etatowych zatrudnionych w SOC.
	9. System SIEM musi być objęty wsparciem technicznym producenta przez cały okres na jaki zostały kupione licencje. Wsparcie to w szczególności musi pozwalać na nieodpłatne instalowanie wszelkich poprawek, aktualizacji i najnowszych wersji oprogramowania.
	10. Środowisko, na którym realizowana jest usługa SOC oraz SIEM musi być uruchomione na środowisku wysokiej dostępności HA w profesjonalnym Data Center (wymagane spełnienie TIER minimum III). Usługi bezpieczeństwa teleinformatycznego operatora powinny posiadać certyfikat na zgodność z normą PN-EN ISO 9001:2015 i PN-EN ISO/IEC 27001. Data Center w którym odbywa się przetwarzanie danych musi znajdować się na terenie Polski.
	11. Zestawienie, zabezpieczenie i obsługa połącznia w relacji Zamawiający do SOC poprzez uruchomienie łącza szyfrowanej transmisji danych w technologii MPLS o przepustowości wymaganej do prawidłowej pracy systemu, realizowane na koszt Wykonawcy.
	12. Oferowany przez Usługodawcę w celu świadczenia Usługi system SIEM musi być dojrzałym produktem a miarą dojrzałości będzie zakwalifikowanie oferowanego systemu w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM, w obszarze liderów.
	13. Wykonawca będzie przetwarzał dane Zamawiającego w ramach standardowych działań operacyjnych, w związku z czym zabezpieczy je przed utratą poufności, integralności, dostępności oraz rozliczalności. Zamawiający może wymagać podpisania dodatkowych, wymaganych prawem umów dotyczących przetwarzania danych.
3. **Instalacja i Wdrożenie**
	1. Wykonawca rozpocznie świadczenie usługi nie później niż w ciągu 90 dni od daty zawarcia Umowy. Rozpoczęcie usługi oznacza podłączenie drugiego źródła do SIEM.
	2. Wykonawca zapewni możliwość rozbudowy licencji oraz elastycznego zwiększania przestrzeni na logi i rozbudowę systemu.
	3. Wykonawca zapewni obsługę minimum 500 EPS (Events Per Second) pochodzących z co najmniej 50 źródeł logów wskazanych przez Zamawiającego.
	4. System SIEM będzie uruchomiony na zasobach własnych Usługodawcy. System będzie miał wsparcie producenta przez cały okres świadczenia Usługi.
	5. Kolektor SIEM zbierający logi z infrastruktury Zamawiającego będzie posadowiony na zasobach serwerowych Zamawiającego. Wykonawca określi wymagania dla tych zasobów.
	6. Wykonawca przeprowadzi analizę przedwdrożeniową, określającą gotowość Zamawiającego do wdrożenia SOC oraz omówi z Zamawiającym wnioski wynikające z tej analizy.
	7. Wykonawca przeprowadzi analizę potencjalnych źródeł logów (systemy, serwery, adresacje, itp.), oraz określi sposób ich normalizacji, parsowania i korelacji w SIEM w celu identyfikacji incydentów bezpieczeństwa.
	8. Wykonawca będzie wykorzystywać w ramach swoich działań zewnętrzne źródła informacji

o globalnych zagrożeniach (Threat Inteligence) w efekcie czego Incydenty Bezpieczeństwa odnotowywane przez SOC na bieżąco będą wzbogacane o opis ich źródeł a także analizę ich szkodliwości.

* 1. Zamawiający zapewni połączenia niezbędne do komunikacji pomiędzy monitorowaną infrastrukturą (źródłami logów) a uruchomionym Kolektorem.
	2. Wykonawca zapewni połączenie niezbędne do komunikacji pomiędzy Kolektorem a systemem SIEM oraz uruchomi przesyłanie logów do SIEM.
	3. Wykonawca wraz z Zamawiającym ustalą i wdrożą mechanizmy uwierzytelnienia oraz mechanizmy szyfrowania danych w czasie transmisji w sieci prywatnej i publicznej.
	4. Wykonawca określi wykonalności scenariuszy na podstawie dostępnych danych oraz analizę potencjalnych dodatkowych scenariuszy, wstępnie określi sposób reagowania na poszczególne podejrzenia incydentów.
	5. Wykonawca ustali z Zamawiającym klasyfikację incydentów, przedstawi propozycję minimum 30 scenariuszy reagowania na wykryte incydenty oraz dostarczy opis sposobu obsługi tych scenariuszy. Jako podstawową kwalifikację incydentów przyjmuje się:
		1. Incydent krytyczny: incydent wygenerowany na bazie logów pochodzących
		ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego
		w zgłoszeniu jako uniemożliwiający prowadzenie podstawowej działalności operacyjnej,
		2. Incydent istotny: incydent wygenerowany na bazie logów pochodzących ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego jako utrudniający prowadzenie podstawowej działalności operacyjnej,
		3. Incydent niski: incydent wygenerowany na bazie logów pochodzących ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego jako naruszający funkcjonującą u Zamawiającego politykę bezpieczeństwa.
	6. Wykonawca usługi przeprowadzi strojenie systemu SIEM w celu zmniejszenia ilości fałszywych alarmów, przez cały okres świadczenia usługi.
	7. Wykonawca przygotuje protokół zakończenia okresu wdrożenia, zawierający wykaz źródeł logów z systemu Zamawiającego oraz wykaz przygotowanych scenariuszy reagowania na wykryte incydenty.
	8. Wykonawca gwarantuje składowanie logów otrzymanych od Zamawiającego oraz dostęp do nich w ramach zasobów Wykonawcy przez czas nie krótszy niż 3 miesięcy w sposób umożliwiający ich wykorzystanie w celu dokonania analizy powłamaniowej lub przekazanie organom prowadzącym postępowanie związane z wystąpieniem incydentu.
	9. Wykonawca przekaże Zamawiającego informacje o sposobie dostępu po składowanych logów.
1. **Wymagania do platformy**
	1. Wykonawca zapewni licencjonowanie zależne od ilości wysyłanych logów bez względu na ilość źródeł z których te logi są wysyłane.
	2. Zastosowany SIEM będzie wyposażony w automatyczne pozyskiwanie, analizowanie i normalizację danych dotyczących bezpieczeństwa.
	3. Zastosowany system będzie wyposażony w mechanizmy uczenia maszynowego, umożliwiającego wykrywanie zagrożeń w oparciu o dane dotyczące aktywności sieciowej

i odchylenia od historycznych danych dotyczących tej aktywności.

* 1. Zastosowany system będzie miał funkcjonalność samodzielnego uczenia maszynowego w celu automatycznego reagowania na podatności typu Zero-Day, wspomagania przy powtarzających się działaniach decyzyjnych o niskiej wartości i wspieraniu przy wykrywaniu nieznanej, złośliwej aktywności.
	2. SIEM umożliwi dynamiczne łączenie wielu jednowątkowych analiz (alertów) w jedno zdarzenie o wysokim priorytecie w celu ograniczenia liczby incydentów analizowanych przez analityków, redukcji fałszywych alarmów oraz poprawnej priorytetyzacji wykrytych incydentów.
	3. Zastosowany SIEM będzie miał wsparcie producenta w dostarczaniu aktualnych informacji dla Advanced Threat Intelligence.
	4. System SIEM musi być wskazany jako lider zgodnie z najnowszą klasyfikacją systemów SIEM wg Gartnera. Producent musi posiadać wysoką zdolność do realizacji (ability to execute) oraz wysoką kompletność wizji (completeness of vision).
1. **Linie wsparcia**
	1. Wykonawca gwarantuje w ramach opłaty za świadczenie Usługi dostęp do Pierwszej i Drugiej Linii Wsparcia, a w ramach odrębnych zamówień dostęp do Trzeciej Linii Wsparcia.
		1. Zadania realizowane w ramach 1 linii wsparcia:
			1. monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24/7/365, zgodnie z określonymi warunkami SLA (zarządzanie incydentami),
			2. reakcja na wykryte incydenty zgodnie z przygotowanymi scenariuszami i warunkami określonymi w SLA,
			3. priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa,
			4. weryfikacja alertów,
			5. odbieranie zgłoszeń telefonicznych i mailowych od Zamawiającego,
			6. analiza wykrywanych incydentów,
			7. przekazywanie Zamawiającemu informacji o wykrytych incydentach, zgodnie z ustalonym kanałem informacji (telefon, e-mail),
			8. przekazywanie incydentów do Drugiej Linii Wsparcia, zgodnie z scenariuszami.
		2. Zadania realizowane w ramach 2 linii wsparcia:
			1. obsługa incydentów przekazanych z 1 linii, w szczególności incydentów krytycznych,
			2. przygotowywanie rekomendacji zmian w następstwie zaobserwowanych incydentów,
			3. troubleshooting,
			4. strojenie systemów,
			5. przygotowywanie scenariuszy,
			6. zaawansowane skanowanie podatności systemów i usług Zamawiającego,
			7. zgłaszanie incydentów poważnych do właściwego CSIRT w ciągu 24 godz. godzin od momentu ich wykrycia oraz udzielanie odpowiedzi na ewentualne pytania CSIRT,
			8. komunikacja pomiędzy pracownikami Wykonwacy i Zamawiającego,
		3. Zadania realizowane w ramach 3 linii wsparcia:
			1. analizę malware,
			2. reverse engineering,
			3. analizy powłamaniowe,
			4. informatykę śledczą,
			5. cykliczne skanowanie podatności systemów i usług Zamawiającego.
	2. Zamawiający dopuszcza inny podział zadań pomiędzy Pierwszą i Drugą Linią Wsparcia z zachowaniem pełnego ich zakresu i czasów reakcji (SLA).
	3. Dostawca usługi zapewni dostęp do usług specjalistycznych 3 linii wsparcia SOC, które realizowane będą dodatkowym zamówieniem, uwzględniając: analizę malware, analizę powłamaniową, informatyka śledczą, cykliczne podatności systemów i usług Zamawiającego, reverse engineering. Zamawiający rozważy również inne usługi specjalistyczne w ramach 3 linii wsparcia oferowane przez Wykonawcę.
	4. Wykonawca zapewni wsparcie personelu Zamawiającego we wdrożeniach rekomendacji po wystąpieniach incydentów.
	5. Wykonawca deklaruje gotowość do realizowania dodatkowych testów oraz analiz w zakresie Cyberbezpieczeństwa.
2. **Raportowanie**
	1. Wykonawca zapewni sprawne przekazywanie informacji o wykrytych incydentach do wyznaczonych pracowników Zamawiającego z użyciem uzgodnionych kanałów informacji: telefon, e-mail.
	2. Wykonawca zapewni przekazywanie Zamawiającemu uzgodnionych co do treści i częstotliwości wykonywania, generowanych automatycznie cyklicznych raportów dotyczących wykrytych incydentów
	3. W raportach Wykonawca będzie przedstawiał ogólne rekomendacje z zakresu cyberbezpieczeństwa dla Zamawiającego, wynikające z obsłużonych incydentów i mające na celu zapobieżenie powstaniu takich incydentów w przyszłości.
	4. Wykonawca zapewnia raportowanie poważnych incydentów (kwalifikacja incydentów zgodnie w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa) do właściwego CSIRT w ciągu 24 godzin od momentu ich wykrycia.
3. **Wsparcie eksperckie**
	1. W ramach świadczonej Usługi Wykonawca ma za zadanie zapewnić (poprzez przedstawienie stosownych rekomendacji oraz zaleceń) optymalne działania systemów bezpieczeństwa, wykorzystywanych do świadczenia tej usługi. W przypadku identyfikacji nieprawidłowości Wykonawca w porozumieniu z Zamawiającym podejmie stosowne działania korygujące,
	2. Wykonawca powinien aktywnie wspierać rozwój systemów bezpieczeństwa, które posiada Zamawiający.
	3. Wykonawca zapewni cykliczne spotkania podsumowujące (raz na miesiąc) w celu wykonania transferu wiedzy oraz omówienia istotnych zdarzeń bezpieczeństwa, podatności czy problemów technicznych**.**
4. **Dokumentacja**
	1. Wykonawca przygotuje i przedstawi Projekt Techniczny powstały na podstawie przeprowadzonej wcześniej wraz z Zamawiającym analizy przedwdrożeniowej.
	2. Dokument będzie zawierał co najmniej analizę potencjalnych źródeł logów (systemów i aplikacji), sposób ich normalizacji, parsowania i korelacji w SIEM w celu identyfikacji incydentów bezpieczeństwa, klasyfikację incydentów oraz listę scenariuszy.
	3. Po zakończeniu wdrożenia Wykonawca przedstawi Dokumentację zawierającą co najmniej:
5. ostateczny kształt infrastruktury informatycznej wykorzystywanej do świadczenia usługi,
6. architekturę,
7. listę źródeł logów,
8. listę scenariuszy,
9. listę uzgodnionych sposobów komunikacji,
10. sposób powiadamiania o incydentach,
11. listę raportów przedstawianych Zamawiającemu podczas świadczenia Usługi.