Załącznik nr 1 do Informacji	Wstępny opis przedmiotu zamówienia

Subskrypcja systemu SIEM wraz z wdrożeniem

Przedmiotem zamówienia jest subskrypcja systemu SIEM wraz z wdrożeniem, który będzie spełniał wymagania konfiguracyjne i parametrowe zgodne z poniższą tabelą:

LP.	PARAMETRY I FUNKCJE	WYMAGANIA
1.	Wymagania ogólne	- dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), którego celem jest gromadzenie i korelacja zdarzeń systemowych (w tym zdarzeń bezpieczeństwa), przesyłanych lub pobieranych z innych systemów i urządzeń teleinformatycznych; - oprogramowanie zostanie dostarczone w formie subskrypcji rocznej (minimum 1 rok) w ramach której Wykonawca zapewnieni gwarancję w trakcie trwania subskrypcji oraz licencje dla liczby użytkowników określonych w niniejszym opisie; - niedopuszczalne są rozwiązania darmowe/open source oraz rozwiązania składające się z wielu osobnych modułów różnych producentów, dodatkowo wszystkie komponenty muszą być w wersji produkcyjnej; - system musi działać zachowując wszystkie funkcje w modelu on premises (lokalnie) w infrastrukturze Zamawiającego – niedopuszczalne jest rozwiązanie w modelu chmurowym; - instalacja systemu musi być możliwa w wirtualnym środowisku VMware VSphere posiadanym przez Zamawiającego; - system musi posiadać graficzny interfejs użytkownika, który będzie możliwy do uruchomienia przez przeglądarki internetowe minimum Chrome, Firefox, Edge, Opera, Safari - bez konieczności instalowania dodatkowego oprogramowania; - system musi umożliwić jednoczesne przetwarzanie zdarzeń w ilości minimum 30 000 zdarzeń/sekunda i objęcie monitoringiem minimum 250 zasobów IT (sprzęt oraz systemy posiadane w infrastrukturze Zamawiającego)

		- system musi umożliwić prezentację danych w postaci dostosowanego dashboardu przez administratora/użytkownika - system SIEM musi zawierać mechanizm integracji z minimum 3 skanerami podatności: 1) co najmniej dwóch różnych producentów; 2) co najmniej jednym dostępnym na zasadach open source. - system SIEM musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej, uwzględniając schematy architektury zabezpieczeń sieci; - system SIEM musi być wyposażony w mechanizmy zautomatyzowanego, dynamicznego uzupełniania elektronicznej dokumentacji na podstawie danych pozyskanych z logów i informacji o ruchu sieciowym (Netflow), protokołów SNMP, WMI, SSH, skanerów podatności oraz skryptów PowerShell, za pomocą których musi istnieć możliwość precyzyjnego określenia zakresu danych, które mają zostać uzupełnione. System musi posiadać repozytorium gotowych skryptów oraz graficzny interfejs pozwalający na tworzenie nowych skryptów, obejmujący możliwość przekazywania do nich parametrów wejściowych; - mechanizmy automatycznego uzupełniania dokumentacji elektronicznej muszą uwzględniać informacje o typach zasobów (np. serwer WWW, baza danych, serwer plików, stacja robocza) oraz zależnościach między tymi zasobami (np. połączenie stacji z serwerem baz danych) - elektroniczna dokumentacja infrastruktury teleinformatycznej systemu SIEM musi pozwalać na wprowadzenie informacji o procesach biznesowych oraz technicznych oraz określania powiązań procesów z elementami infrastruktury - system musi pozwalać na definiowane własnych parametrów dla wszystkich typów obiektów gromadzonych w elektronicznej dokumentacji sieci - system SIEM musi współpracować z posiadaną przez Zamawiającego subskrypcją VirusTotal
2.	Użytkownicy	- tworzenie wielu użytkowników administracyjnych/tylko monitorowania – minimum 10 kont

		- równoległy dostęp do systemu dla wielu użytkowników – minimum 10 użytkowników korzystających z systemu typu SIEM jednocześnie (konta z równoważną rangą uprawnień) - możliwe nadawanie różnych uprawnień dla poszczególnych użytkowników
3.	Analiza logów systemowych związanych z aplikacjami/ systemami Zamawiającego	- monitorowanie plików konfiguracyjnych - skanowanie integralności plików - analiza integralności rejestru - analiza logów aplikacji systemowych - analiza logów serwera poczty elektronicznej - analiza logów aplikacji internetowych - analiza logów aplikacji na poziomie użytkownika - analiza logów związanych z bazami danych - analiza logów związanych z sieciami VPN - analiza logów związanych z kontami użytkowników - analiza logów związanych z kontami serwisowymi - analiza logów związanych z kontami administratorów
4.	Detekcja i reagowanie na ataki i zagrożenia dotyczące aplikacji/ systemów Zamawiającego	- wykrywanie i reagowanie w czasie rzeczywistym zgodnie z wymaganiami opisanymi w module obsługi incydentów i powiadomieniami/alertami - wykrywanie i reagowanie na próby włamania się (brute-force) - wykrywanie i reagowanie na próby typu Man-in-the-Middle - wykrywanie i reagowanie na próby zmiany lub ataku na pliki systemowe - wykrywanie i reagowanie na próby wykorzystania podatności - wykrywanie i reagowanie na próby ataku typu SQL injection, Cross-Site Scripting (XSS), zero-day, buffer overflow, DNS poisoning, DDoS (Denial-of-Service) - wykrywanie i reagowanie na zmiany w konfiguracji firewalla - wykrywanie i reagowanie na próby ataku typu ransomware, eavesdropping, cryptojacking, data manipulation
5.	Zbieranie logów z aplikacji/	- zbieranie danych z systemów wirtualizacji

	systemów Zamawiającego	- zbieranie danych z systemów monitorowania chmury - zbieranie danych z platform wirtualizacyjnych - zbieranie danych z platform chmurowych
6.	Monitorowanie aktywności użytkowników aplikacji/ systemów Zamawiającego	- monitorowanie aktywności użytkowników - monitorowanie aktywności na poziomie portów i usług - monitorowanie aktywności na poziomie interfejsów - monitorowanie na poziomie protokołów
7.	Monitorowanie urządzeń sieciowych Zamawiającego	- monitorowanie aktywności na poziomie protokołów sieciowych - monitorowanie aktywności na poziomie protokołów aplikacji - monitorowanie aktywności na poziomie protokołów transportowych - monitorowanie aktywności na poziomie protokołów internetowych - monitorowanie ruchu sieciowego - monitorowanie dostępów SSH - monitorowanie aktywności sieciowych na poziomie interfejsów
8.	Integracja z systemami monitorowania posiadanych przez Zamawiającego	- integracja z systemami monitorowania logów - integracja z systemami monitorowania zachowań użytkowników - integracja z systemami monitorowania aplikacji - integracja z systemami monitorowania chmury
9.	Zdalne monitorowanie agentów	- zdalne monitorowanie agentów w różnych środowiskach - zdalne monitorowanie agentów w chmurze
10.	Wykrywanie nieautoryzowanego dostępu do aplikacji/ systemów Zamawiającego	- wykrywanie prób nieautoryzowanego dostępu - wykrywanie prób podmiany tokenów uwierzytelnienia - wykrywanie prób podważenia integralności plików

11.	Ostrzeganie przed atakami na systemy/ aplikacje Zamawiającego i moduł obsługi incydentów	- ostrzeganie przed próbami włamania się na konta - ostrzeganie przed próbami łamania haseł metodą bruteforce - ostrzeganie przed próbami ataku typu SQL tampering, formjacking, clickacking, domain hijacking, URL poisoning, click injection, zero-click exploit - dla zarejestrowanych zdarzeń/incydentów system musi wskazywać ścieżkę ataku i zaprezentować ją na schemacie sieci organizacji - system musi zapewniać narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa na działalność organizacji (wyszukiwanie i prezentowanie informacji na temat procesów i informacji, które mogły zostać naruszone w wyniku incydentu oraz wyświetlenie przewidywanych konsekwencji) - narzędzia systemu muszą umożliwiać wyznaczanie o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń oraz wskazywanie zasobów IT o krytycznym znaczeniu, które nie posiadają odpowiednich zabezpieczeń - moduł obsługi incydentów systemu musi zawierać proces ich obsługi tj. selekcja, analiza, ocena wpływu i reakcja. W ramach procesu każdy incydent przyjmuje odpowiedni status, np.: nowe zdarzenie, incydent, fałszywy alarm, incydent poddany do analizy, incydent zamknięty - moduł obsługi systemu musi być wyposażony w mechanizm scenariuszy obsługi incydentów, które będą automatycznie dopasowywane uwzględniając: priorytet incydentu wynikający z działania reguł korelacji, ważność zasobu, typ zasobu i aktualny status zdarzenia - moduł obsługi incydentów systemu musi być wyposażony w graficzny interfejs umożliwiający tworzenie i testowanie scenariuszy obsługi incydentów - moduł obsługi incydentów systemu musi być wyposażony w mechanizm automatycznego powiadamiania wskazanych adresatów o nowych incydentach, zmianach statusów, przekroczeniach czasów reakcji i obsługi
12.	Integracja z posiadanymi systemami Zamawiającego	- integracja z narzędziami do analizy ruchu sieciowego, zachowań użytkowników, zarządzania incydentami, analizy zachowań aplikacji

13.	Powiadomienia i alerty	- system generuje alerty w czasie rzeczywistym, informując o potencjalnych zagrożeniach. Możliwa konfiguracja komunikatu (np. za pomocą email) dla wskazanych użytkowników
14.	Reguły korelacji	- system SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE - możliwość definiowania reguł korelacji, które określają, jakie zdarzenia i logi mają być analizowane oraz w jaki sposób mają być powiązywane, aby wykrywać zaawansowane ataki - możliwość powiązania wielu zdarzeń i logów w celu identyfikacji bardziej złożonych aktywności i etapów ataków, które mogą obejmować różne komponenty infrastruktury - silnik korelacji wykorzystuje wiedzę zawierającą informacje o znanych zagrożeniach i atakach, co pozwala na lepsze wykrywanie i identyfikację nowych incydentów - silnik korelacji wykorzystuje zaawansowane heurystyki, aby identyfikować podejrzane aktywności i zachowania, nawet jeśli nie są to znane zagrożenia - możliwość budowania profili aktywności użytkowników oraz zasobów IT poprzez wielowartościowe listy referencyjne i wykorzystywanie ich w regułach korelacyjnych
15.	Raporty i dane	- przechowywanie zgromadzonych danych przez minimum 90 dni oraz zapewniać archiwizację do oprogramowania funkcjonującego w infrastrukturze Zamawiającego po upływie tego terminu - pozyskane przez system dane muszą być dostępne w wersji pierwotnej i znormalizowanej - raporty na żądanie w oparciu o zapytanie i dane z logów, uwzględniające:a) automatyczne generowanie raportów w oparciu o interwały czasowe; b)wybór zakresu czasowego: możliwość wyboru zakresu czasowego dla raportu; c) raportowanie anomalii systemów/aplikacji/zachowań użytkowników; d) raporty dotyczące wydajności i dostępności infrastruktury;

		e) dostępny eksport danych do formatów PDF lub CSV; f) wykresy i diagramy ułatwiające wizualizację i analizę danych; g) narzędzie umożliwiające dodatkowo raportowanie określonego zestawu danych bez użycia języka przetwarzania wyszukiwania (czyli poleceń, argumentów i klauzul) poprzez „przeciągnij i upuść", aby móc zagregować dane w formie przestawnych tabel oraz wykresów i innych wizualizacji.
16.	Parser logów systemów	- zbieranie logów i proces normalizacji (parsowania) w czasie rzeczywistym na etapie rejestrowania danych w systemie - normalizacja logów z różnych źródeł do jednolitego formatu, na podstawie którego może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych, system musi posiadać predefiniowany zestaw reguł normalizacji logów dla źródeł logów takich jak: urządzenia sieciowe, systemy bezpieczeństwa, systemy Windows, Active Directory - wykorzystanie reguł i detekcja w czasie rzeczywistym - skalowalność – możliwe rozbudowanie do obsługiwania dużych ilości logów z różnych źródeł w czasie rzeczywistym

Dodatkowo Wykonawca zobowiązany jest:

1. Zapewnić wdrożenie systemu SIEM uwzględniając całą infrastrukturę i konfigurację poszczególnych systemów Zamawiającego. Przez wdrożenie Zamawiający rozumie:
   a) dostarczenie licencji na oprogramowanie systemu SIEM,
   b) przygotowanie infrastruktury Zamawiającego do instalacji systemu SIEM,
   c) instalacja i konfiguracja niezbędnego oprogramowania oraz serwerów wirtualnych,
   d) instalacja systemu SIEM,
   e) zestawienie połączenia zdalnego dostępu,
   f) aktywacja licencji,
   g) aktualizacja oprogramowania – najnowsza wersja oprogramowania dostępna na dzień instalacji,
   h) konfiguracja systemu SIEM i uzyskanie akceptacji jej przez Zamawiającego
   i) przeprowadzenie testów potwierdzających poprawne wdrożenie systemu i jego konfigurację
2. Zapewnić podłączenie wskazanych przez Zamawiającego źródeł zdarzeń.
3. Zapewnić uruchomienie i konfigurację parserów dla niestandardowych źródeł danych, w przypadku wymagania integracji ich przez Zamawiającego.
4. Zapewnić uruchomienie i konfigurację reguł korelacyjnych, ustawień i obszarów bezpieczeństwa infrastruktury i sieci, mechanizmów oceny ryzyka, powiadamiania oraz obsługi incydentów.

5. Zapewnić dostrojenie i skalibrowanie reguł korelacji.
6. Dostarczyć dokumentację powdrożeniową oraz dokumentację systemu SIEM (techniczną oraz dla użytkownika) – dokumentacja w formie edytowalnej (.docx, .xlsx) i wersji .pdf:
   a) projekt wdrożenia rozwiązania w infrastrukturze Zamawiającego,
   b) dokumentacja powdrożeniowa systemu SIEM,
   c) dokumentacja techniczna i użytkownika,
   d) dokumentacja zostanie sporządzona w języku polskim
7. Udzielić gwarancji na okres trwania subskrypcji dostarczonego systemu SIEM, która liczona będzie od dnia podpisania protokołu odbioru zamówienia:
   a) wykonawca w ramach gwarancji pokryje wszystkie koszty związane z naprawą systemu SIEM
   b) wykonawca zapewni elektroniczny dostęp do informacji na temat posiadanego oprogramowania oraz biuletynów technicznych, poprawek, aktualizacji.
8. W ramach subskrypcji Wykonawca jest zobowiązany świadczyć usługi wsparcia technicznego, które będą realizowane poprzez dodatkowe zlecenia lub zgłoszenia w trakcie eksploatacji systemu:
   a) zgłoszenia będą dokonywane przez Zamawiającego w trybie NBD (następny dzień roboczy),
   b) zgłoszenia będą obsługiwane w ramach zdefiniowanych parametrów SLA i kategorii zgłoszenia: high - zgłoszenie krytyczne, przez co rozumie się brak działania systemu/niepoprawne działanie systemu/brak możliwości zalogowania się – usunięcie awarii usługi/systemu lub zaproponowanie obejścia nastąpi do 6h od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego z zastrzeżeniem, że w przypadku zaproponowania obejścia Wykonawca przywróci prawidłowe działanie usługi/systemu w terminie do 24h od momentu zgłoszenia awarii przez Zamawiającego, medium przez co rozumie się zgłoszenie inne niż high polegające na zmienieniu konfiguracji/sprawdzeniu poprawnego działania funkcji systemu w razie wątpliwości lub naprawie ich awarii - usunięcie awarii usługi/systemu lub zaproponowanie obejścia nastąpi do 8h od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego z zastrzeżeniem, że w przypadku zaproponowania obejścia Wykonawca przywróci prawidłowe działanie usługi/systemu w terminie do 48h od momentu zgłoszenia awarii przez Zamawiającego, low) przez co rozumie się pozostałe nieprawidłowości działania usług/systemu niewyszczególnione jako high i medium - usunięcie nieprawidłowości lub zaproponowanie obejścia nastąpi do 2 dni roboczych od momentu przekazania zgłoszenia do Wykonawcy; , none - zgłoszenie dodatkowe dotyczące udzielenia przez Wykonawcę informacji lub dokonania zmiany w konfiguracji usług/systemu. Udzielenie odpowiedzi lub konfiguracja usług/systemu nastąpi do 3 dni roboczych od momentu przesłania zgłoszenia do Wykonawcy przez Zamawiającego,
   c) w przypadku braku rozwiązania zgłoszenia z innej przyczyny niż awaria systemu SIEM, Wykonawca wskaże element, który powoduje nieprawidłowość działania systemu,
   d) usługi wsparcia technicznego będą składane za pośrednictwem poczty elektronicznej/systemu wskazanego przez Wykonawcę,

e) czasy reakcji Wykonawcy na zgłoszenia i zlecenia dodatkowe zostaną określone w odrębnej umowie.

9. Zapewnić bezpłatne 4 dniowe certyfikowane warsztaty dla 6 osób (4 dni x 8h) w zakresie użytkowania i administrowania wdrożonym systemem SIEM w siedzibie Zamawiającego – ul. Józefa Lewartowskiego 6, 00-190 Warszawa. Wykonawca przygotuje wszystkie potrzebne do przeprowadzenia szkolenia materiały. Szczegółowy plan zostanie przedstawiony w umowie.

Procedura odbioru zamówienia będzie obejmowała:

1. Dostawę licencji na oprogramowanie systemu SIEM.
2. Wdrożenie i konfigurację systemu SIEM.
3. Dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej i użytkownika, dokumentacji powdrożeniowej.
4. Warsztaty z obsługi systemu SIEM.

Odbiór każdego z elementów realizacji musi być potwierdzony protokołem odbioru.

Zespół Obsługi Informatycznej
Kryštian Pac
Kryštian Pac
REFERENT

Zespół Obsługi Informatycznej
Marcin Dziadosz
Referent

Zespół Obsługi Informatycznej
Kaczyński
Rafał Kaczyński
SAMODZIELNY REFERENT

Zespół Obsługi Informatycznej
Łukasz Walczak
REFERENT