Załącznik nr 5b do SWZ

Opis przedmiotu zamówienia - Część II

Zamawiający zastrzega sobie prawo sprawdzenia zgodności oferowanego oprogramowania w oparciu o informacje zamieszczone na stronie internetowej producenta, w przypadku braku takiej możliwości, Zamawiający będzie wymagał przedstawienia dokumentacji producenta potwierdzającej wymagania minimalne.

Przedmiotem zamówienia jest zakup i dostawa wraz z wdrożeniem oprogramowania klasy **SIEM (Security Information and Event Management)** do monitorowania infrastruktury informatycznej ze wsparciem serwisowym i aktualizacjami do 17.04.2026 r., na potrzeby Starostwa Powiatowego w Radomsku, o parametrach nie gorszych niż wskazane poniżej:

Parametr	**Wymagania minimalne**
Licencja	Bezterminowa
Liczba urządzeń	200
Serwis/wsparcie techniczne	Oferowane oprogramowanie musi posiadać aktywne wsparcie producenta do 17.04.2026 r., umożliwiające bezpłatne aktualizacje (bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji) w tym do najnowszych wersji oprogramowania oraz wsparcie w zakresie zgłaszania ewentualnych problemów drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia.
Wdrożenie	W ramach wdrożenia wymagane jest aby Wykonawca wykonał następujące czynności: a) instalację i konfigurację wszystkich komponentów oprogramowania na infrastrukturze Zamawiającego, b) szkolenie z funkcjonalności oprogramowania dla 2 osób wskazanych przez Zamawiającego w zakresie użytkowania i

	administrowania wdrożonego oprogramowania. Szkolenie musi zakończyć się przyznaniem certyfikatu wydanym przez Certyfikowanego Inżyniera systemu. Usługa może być wykonana zdalnie lub na miejscu przez pracownika posiadającego wiedzę potwierdzoną aktualnym certyfikatem/dokumentem producenta – wymagane przedstawienie przed przystąpieniem do wdrożenia aktualnego certyfikatu/dokumentu osoby potwierdzającego jej kwalifikacje do wdrożenia wydanego przez producenta oprogramowania lub oficjalnego przedstawiciela w Polsce. Koszty wdrożenia należy ująć w cenie oprogramowania. Wykonawca zapewni usługę konsultacji powdrożeniowej w formie spotkań zdalnych z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu Proces wdrożenia systemu powinien zostać przeprowadzony w porozumieniu z Zamawiającym. Wymagane jest podłączenie wszystkich źródeł logów wskazanych przez Zamawiającego do górnej granicy licencji. Należy uruchomić wszystkie niezbędne funkcjonalności umożliwiające korelację zdarzeń i logów z podłączonych źródeł. W ramach wdrożenia rozwiązania SIEM Zamawiający wymaga, aby Wykonawca wdrożył rozwiązanie SIEM na minimum 2 maszynach wirtualnych przygotowanych przez Zamawiającego. Wymaga się, aby Wykonawca przygotował i przekazał przed przystąpieniem do wdrożenia harmonogram wdrożenia uwzględniający 4 etapy wdrożenia: 1 etap - analiza przedwdrożeniowa, określenie istotnych informacji które SIEM powinien wykrywać z podłączonych źródeł logów, 2 etap - instalacja systemu, 3 etap - konfiguracja systemu, implementacja wcześniej opracowanych reguły bezpieczeństwa wraz z weryfikacją ich działania,

	4 etap - dostrojenie systemu, wykluczenie nadmiernej ilości fałszywych alarmów. Zamawiający wymaga wdrożenia kompletnego systemu w ramach którego zostanie podłączonych do 200 źródeł logów z systemów takich jak serwery fizyczne, serwery wirtualne, urządzenia sieciowe, rozwiązania AV, systemów backupu. Nie dopuszcza się sytuacji, w której jedno źródło logów spowoduję destabilizację działania całego systemu SIEM w krótkim okresie czasu np. 10minut.
Stacje robocze	Pełne wsparcie dla posiadanych przez Zamawiającego stacji roboczych z systemami Windows 10/11.
Baza danych	Jeżeli system SIEM wymaga do swego działania bazy danych, musi ona być wkalkulowana w cenę systemu lub posiadać bezpłatną licencję.
Interfejs użytkownika	W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim.
Funkcjonalność	System SIEM przeciwdziałający cyberzagrożeniom oferujący możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności, spełniający minimalne wymagania: 1. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. 2. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach. 3. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 4. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.

	5. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 6. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware. 7. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 8. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji. 9. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych. 10. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. 11. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

	12. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. 13. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. 14. Ze względu na możliwość wygenerowania dużej ilości danych system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. 15. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. 16. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. 17. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. 18. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki

	wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. 19. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. 20. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów. 21. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej. 22. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług. 23. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły. 24. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej

	kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 25. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: a) nowe zasoby wykryte w sieci, b) typy wykrytych zasobów (np.: serwer lub stacja robocza), c) zastosowane na nich zabezpieczenia, d) usługi z którymi się komunikują, e) nowe usługi wykryte na zasobie f) komunikację do usług wykrytych na zasobie. 26. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. 27. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy. 28. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji do incydentów. 29. System musi umożliwiać integrację z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

	30. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. 31. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. 32. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. 33. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 34. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, b) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, 35. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów. 36. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. 37. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

	38. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. 39. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: a) wykrycie dowolnej treści w logach, b) wykrycie zmiany jednego z kilku pól, c) wykrycie zaniku wiadomości, d) wykrycie nowej wartości pola w zadanym okresie czasu, e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu, m) wykrycie skanowania portów. 40. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: a) wykrycie wystąpienia wartości pola na wybranej liście, b) wykrycie niewystępowania wartości pola na wybranej liście,

	c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony), d) wykrycie niewystąpienia pary wartości na wybranej liście e) np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył). 41. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. 42. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. 43. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;

	b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji; 44. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, c) wykrycie nieautoryzowanej usługi na serwerze, d) wykrycie nieautoryzowanego połączenia do usługi na serwerze, e) wykrycie nieautoryzowanego połączenia z serwera usług, f) wykrycie nieautoryzowanego połączenia do sieci Internet. 45. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN. 46. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,

	b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach. 47. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, c) wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, d) wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności. 48. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 49. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. 50. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć

	wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a) identyfikację celu i źródła zagrożenia, b) nazwę oraz adres IP źródła zagrożenia, c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d) lokalizację z które pochodzi zagrożenie np.: Internet, e) strefę bezpieczeństwa z której pochodzi zagrożenie, f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h) nazwę oraz adres IP celu zagrożenia, i) zabezpieczenia lokalne chroniące cel zagrożenia, j) strefę bezpieczeństwa w której znajduje się cel zagrożenia. 51. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: a) nazwy zasobu, b) rodzaj przetwarzanych informacji, c) usług, które ten zasób świadczy, d lokalizację użytkowników, którzy z niego korzystają, e) usługi z których zasób korzysta. 52. System powinien powiadamiać operatora o przypisanych mu zdarzeniach poprzez min. e-mail, SMS. 53. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, b) segregacja – segregacja i kwalifikacja zdarzeń,

	c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, e) zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa" do statusu „zdarzenie zamknięte", ale zablokować zmianę ze statusu „incydent bezpieczeństwa" na status „fałszywy alarm". 54. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. 55. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: a) podgląd aktywności zagrożonego zasobu na linii czasu, b) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d) podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, f) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g) gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o: • listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,

	• listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, f) gotowe i proste w użyciu filtry rozszerzajcie analizę logów o: • listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, • listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym. 56. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień, • zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • zdarzeń o przekroczonych czasach SLA o definiowalny okres, • zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • zdarzeń, których priorytet osiągnął określoną wartość, • zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, • Zdarzeń, na których doszło do naruszenia bezpieczeństwa, • zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu zostało przydzielone zdarzenie, • właściciela zasobu, na którym wystąpiło zdarzenie, • zespół obsługi, który odpowiada za obsługę zdarzeń, • właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.

	c) kanały powiadomień, m.in. e-mail, sms, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości. 57. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: a) aktualnym statusie obsługi, b) adresie IP tego systemu, c) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, 58. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji. 59. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 5 tyś zdarzeń na sekundę w trybie ciągłym. 60. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta. 61. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym

	ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej. 62. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. 63. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych. 64. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych. 65. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI). 66. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI). 67. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; d) zdolność do monitorowania integralności plików; e) zdolność do monitorowania rejestru systemowego; f) zdolność do monitorowania urządzeń zewnętrznych (removable devices); g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;

	h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu. 68. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI 69. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM. 70. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). 71. W celach weryfikacji zgodności produktu z wymaganiami, musi być oferowany przez autoryzowanego dystrybutora na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego,

	związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. 72. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. 73. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać min. 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. 74. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów. 75. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. 76. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server (minimum Server 2022) lub Redhat/Oracle Linux (minimum 7.x).
Wymagania sprzętowe	Oprogramowanie musi poprawnie funkcjonować i nie może mieć wymagań większych niż posiadany przez Zamawiającego serwer o parametrach: - dwa procesory 8-rdzeniowe, klasy serwerowej x86, - pamięć 64 GB, - macierz dyskowa 4 TB, - system operacyjny Windows Server Standard 2022 x64.

Gwarancja	1. Wykonawca zapewni prawidłowe i sprawne działanie oferowanego oprogramowania - systemu jako całości, jak również każdego z elementów tego systemu oddzielnie i udzieli gwarancji do 17.04.2026 roku na system i wszystkie jego elementy. 2. Wykonawca zapewni również wsparcie serwisowe dla dostarczonego rozwiązania, które będzie świadczone przez Producenta oprogramowania w ramach wynagrodzenia przysługującego Wykonawcy na podstawie umowy. 3. Zgłoszenia dotyczące wystąpienia wad, awarii mogą być przyjmowane drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego Producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia. 4. Bieg terminu gwarancji rozpoczyna się od daty odbioru przedmiotu umowy. 5. W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia stwierdzonych wad. 6. Gwarancja obejmuje wszelkie wady z wyjątkiem wad spowodowanych niewłaściwym lub niezgodnym z instrukcją obsługi użytkowaniem produktu oraz wad spowodowanych zdarzeniami losowymi. 7. Jeżeli usunięcie ujawnionej wady wdrożonego systemu jest możliwe wyłącznie w drodze dokonania zakupu jakichkolwiek udoskonaleń (w tym: unowocześnień, aktualizacji, dodatków sprzętowych, wszelkiego rodzaju usług, serwisów, licencji i uprawnień), Wykonawca jest zobowiązany dokonać tego zakupu na własny koszt i zainstalować przedmiot zakupu we wdrożonym systemie.

	8. Wykonawca pokrywa w ramach gwarancji wszelkie koszty napraw i wymiany elementów systemu, w tym koszty dojazdu, transportu, demontażu, montażu, odinstalowania lub zainstalowania. 9. Udzielona przez Wykonawcę gwarancja nie wyłącza uprawnień Zamawiającego wynikających z rękojmi za wady oraz uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producenta oprogramowania. 10. Wykonawca do oprogramowania dostarczonego Zamawiającemu na podstawie umowy dołącza Licencje oraz wszelkie inne dokumenty konieczne do prawidłowego korzystania z Systemu. 11. Dla oprogramowania wymaga się dostarczenia wsparcia technicznego producenta tego oprogramowania do 17.04.2026 roku z możliwością jego odnawiania po tym czasie.