*ZAŁĄCZNIK nr 1 do SWZ*

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

**wraz z oświadczeniem o spełnianiu przez oferowane dostawy wymagań**

**ZADANIE NR 1**

**Oprogramowanie do monitorowania ruchu w sieci**

|  |  |
| --- | --- |
|  | **PRZEDMIOT ZAMÓWIENIA** |
|  | Zakup i dostawa oprogramowania do monitorowania sieci oraz systemów IT pod kątem podatności wraz ze wsparciem na okres 12 mies. |
|  | **WYMAGANE PARAMETRY TECHNICZNE:** |
|  | 1. **Wymagania funkcjonalne** |
|  | * 1. **Zarządzanie Logami i Zdarzeniami:**  1. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą m.in. gromadzenie i korelacja zdarzeń zbieranych, odbieranych lub wgrywanych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco, wyszukiwanie zależności między różnymi zdarzeniami, agregację oraz wzbogacanie, na podstawie zdefiniowanych reguł, danych. 2. System musi mieć możliwość centralnego zbierania i zarządzania logami. 3. Instancje systemu muszą mieć możliwość wgrywania logów z nośników zewnętrznych. 4. System musi umożliwiać prezentację zdarzenia, w interfejsie użytkownika, w formie, w jakiej został przesłany do systemu (RAW) przed przetwarzaniem. 5. System musi umożliwiać przyjmowanie zdarzeń poprzez mechanizmy agentowe i bezagentowe. 6. System musi umożliwiać przeszukiwanie danych wejściowych z uwzględnieniem filtracji po zdefiniowanych atrybutach. 7. System musi umożliwiać anonimizację danych wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzne procedury bezpieczeństwa. 8. System musi umożliwiać funkcjonalność eksportu danych o zdarzeniach, incydentach i raportach do formatów m.in. CSV, HTML, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC. 9. System musi umożliwiać dodawanie innych formatów eksportu danych w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego. 10. System musi przechowywać logi na czas określony przez prawo i regulaminy wewnętrzne, na zasadach gwarantujących ochronę ich integralności. 11. System zapewnia mechanizmy rozliczalności pracowników i innych użytkowników infrastruktury teleinformatycznej. 12. System musi umożliwiać pobieranie logów/zdarzeń, z co najmniej z następujących rodzin systemów i aplikacji:   - Windows Server 2012-2022, oraz Windows 10,11,  - Systemu poczty elektronicznej Microsoft Exchange,  - Serwerów usługowych opartych na platformie Windows Server,  - Systemów Linux,  - Systemy wirtualizacji wiodących vendorów,  - urządzeń sieciowych L2, L3,  - baz danych,  - urządzania bezpieczeństwa sieciowego tj. NGFW, IDS, IPS itd. |
|  | * 1. **Analiza i Korelacja Zdarzeń:**  1. System musi umożliwiać korelację danych w czasie rzeczywistym. 2. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących. 3. System musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być dostępne, co najmniej w formatach PDF, CSV. 4. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. 5. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. 6. System musi posiadać bazę reguł spełniającą wymagania Zamawiającego w zakresie posiadanych systemów IT. 7. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. 8. System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL. 9. System SIEM musi utrzymywać repozytorium logów z możliwością ich przeglądania  w formie surowej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). 10. Wyszukiwanie danych i zdarzeń musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący, jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól. 11. System musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia czy dnia tygodnia). 12. System w swoim działaniu powinien korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników  i komputerów. |
|  | * 1. **Wizualizacja i Raportowanie:**  1. System musi zapewniać wizualizację danych w postaci oryginalnych logów, list, wykresów i diagramów. 2. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP. 3. System musi generować raporty w formatach PDF i JPEG, z możliwością dodawania logo i komentarzy. 4. System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres  i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika. 5. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa. 6. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu. 7. System powinien udostępniać automatyczny raport z wszystkich podjętych działań  w ramach incydentu. 8. System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji  z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej  o wartości pochodzące ze zgromadzonych w systemie danych. 9. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IOC. |
|  | * 1. **Bezpieczeństwo i Zgodność:**  1. System musi zapewniać pełen audyt aktywności użytkowników, w tym logowania, operacje, zmiany uprawnień. 2. System musi posiadać funkcjonalność badania integralności plików i rejestrów na monitorowanych hostach. 3. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń. 4. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników. 5. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych. 6. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokół TLS w wersji minimum 1.3. 7. Komunikacja pomiędzy komponentami systemu musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3. 8. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem. 9. Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. 10. Komunikacja pomiędzy wszystkimi komponentami Systemu musi być szyfrowana. |
|  | * 1. **Integracja i Rozbudowa:**  1. System musi umożliwiać integrację z bazą MISP oraz z Mitre ATT&CK. 2. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska. 3. System musi posiadać predefiniowany zestaw parserów zdarzeń. 4. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól oraz zastosowanie różnych metod parsowania, takich jak REGEX, JSON, XML. 5. Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na dashboardach systemu. 6. System SIEM musi umożliwiać korzystanie z zewnętrznych źródeł tzw. wskaźników kompromitacji (ang. IOC Indicator of compromise). 7. System ma umożliwiać aktualizację (oprogramowania) w sposób ręczny z poziomu systemu operacyjnego. 8. Funkcjonowanie rozwiązania musi być oparte w całości o architekturę „on-premise”, w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego. |
|  | * 1. **Interfejs i Użyteczność:**  1. Interfejs musi posiadać angielską lub polską wersję językową. 2. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej (min. Firefox, Chrome, EDGE). 3. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami. |
|  | * 1. **Bezpieczeństwo:**  1. System musi umożliwiać funkcjonalność badania integralności plików i rejestrów na monitorowanych hostach. 2. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym. 3. System musi posiadać wbudowany moduł tworzenia i edycji elektronicznej dokumentacji. |
|  | 1. **Wymagania niefunkcjonalne:** |
|  | * 1. **Architektura i Wydajność:**  1. System musi pracować w oparciu o system operacyjny Linux. 2. System musi umożliwiać funkcjonowanie bez dostępu do sieci internet. 3. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania. 4. System dostarczony w środowisku wirtualnym powinien być integrowalny z narzędziami: MS Hyper-V lub Proxmox. 5. Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych np.: Adobe Flash, Java lub Microsoft Silverlight. 6. System będzie zaimplementowany na środowisku Zamawiającego. |
|  | * 1. **Licencjonowanie:**  1. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu. 2. Zamówienie zawiera licencje na 2 instancje systemu. 3. Oferowana licencja nie może być abonamentowa. 4. Oferowana licencja na system klasy SIEM pozwoli na obsługę min. 800 zdarzeń na sekundę. 5. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów. |
|  | **WYMAGANIA GWARANCYJNE ORAZ W ZAKRESIE SERWISOWANIA:** |
|  | 1. **Wsparcie techniczne:** |
|  | * 1. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.   2. Wsparcie nie może być limitowane ilością zgłoszeń, musi być realizowane zdalnie oraz w siedzibie Zamawiającego.   3. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować również to narzędzie.   4. Dostarczone rozwiązanie musi być objęte 12 mies. wsparciem producenta lub producentów.   5. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego). |
|  | 1. **Wdrożenie i szkolenie:** |
|  | * 1. **Szkolenie:**  1. Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem SIEM dla pracowników Zamawiającego. 2. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim. 3. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania, potwierdzający ich kompetencje w zakresie użytkowania  i administrowania systemem. |
|  | * 1. **Wdrożenie:**  1. Wykonawca opracuje harmonogram wdrożenia systemu SIEM. 2. Wykonawca przeprowadzi instalację i konfigurację systemu w siedzibie Zamawiającego. 3. Wykonawca skonfiguruje reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem. 4. Wykonawca przedstawi do akceptacji listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych. 5. Wykonawca przedstawi Zamawiającemu w terminie do 7 dni kalendarzowych po podpisaniu umowy projekt techniczny zawierający w szczególności:   - Plan i opis architektury logicznej Systemu,  - Opis funkcji Systemu SIEM do zaimplementowania w infrastrukturze Zamawiającego,  - Szczegółowy opis zakresu integracji Systemu SIEM z innymi systemami eksploatowanymi w infrastrukturze Zamawiającego,  - Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do dostosowania Systemu do potrzeb Zamawiającego  i konfiguracji środowiska produkcyjnego,  - Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego. |

**ZADANIE NR 2**

**Oprogramowanie do zarządzania urządzeniami mobilnymi (MDM)**

|  |  |
| --- | --- |
|  | **PRZEDMIOT ZAMÓWIENIA** |
|  | Zakup, dostawa i wdrożenie oprogramowania do zarządzania urządzeniami mobilnymi wraz ze wsparciem powdrożeniowym na okres 36 mies. |
|  | **WYMAGANE PARAMETRY TECHNICZNE:** |
|  | 1. **Wymagania niefunkcjonalne** |
|  | * 1. przygotowanie planu przedwdrożeniowego.   2. licencja/licencje pozwalające na wieczystą obsługę 500 urządzeń mobilnych(android/iOS).   3. prace wdrożeniowe na infrastrukturze w siedzibie Zamawiającego.   4. wsparcie producenta w języku polskim przez dedykowanych inżynierów.   5. oprogramowanie musi umożliwiać jego instalację na systemie operacyjnym MS Windows.   6. dopuszczalny język interfejsu polski lub angielski.   7. system musi pracować w architekturze on-premise.   8. żadna funkcjonalność nie może być czasowa/abonamentowa. |
|  | 1. **Wymagania funkcjonalne** |
|  | * 1. system posiada:  1. wbudowany mechanizm vpn. 2. możliwość dostarczania konfiguracji apn. 3. instalację w sieci zamkniętej. 4. wsparcie dla backupu maszyn wirtualnych. 5. możliwość konfiguracji firewalla serwera. 6. wsparcie dla implementacji high availability. 7. wbudowane narzędzie do wykonywania kopi zapasowych. 8. możliwość grupowania użytkowników. 9. dynamiczne przypisywanie konfiguracji. 10. logi audytowe, monitorowanie zdarzeń w systemie, logi sieciowe. 11. możliwość logowania do systemu klasy siem. 12. możliwość dodania aplikacji z zasobu zewnętrznego. 13. możliwość instalacji aplikacji własnych z pliku .apk. 14. możliwość aktualizacji aplikacji z pliku. 15. zarządzanie uprawnieniami aplikacji. 16. wsparcie dla android enterprise. 17. wsparcie dla ldap. 18. możliwość ustawienia dedykowanej tapety ekranu głównego. 19. możliwość konfiguracji whitelist/blacklist aplikacji. 20. ustawienie wymagań minimalnych hasła. 21. wymuszanie ustawienia skomplikowanego hasła. 22. wyświetlanie geo-lokalizacji aktywnych urządzeń końcowych. 23. wyświetlanie atrybutów użytkownika. 24. możliwość połączenia zdalnego z urządzeniem końcowym (android). 25. zdalny pulpit z możliwością kontroli urządzenia. 26. manualne aktualizacje serwera. 27. możliwość zarzadzania aktualizacjami systemu operacyjnego android. 28. możliwość zablokowania ekranu. 29. wysyłania notyfikacji. 30. wyświetlanie komunikatów na urządzeniu zdalnym. 31. zdalne wysyłanie alarmu. 32. zdalny restart urządzenia. 33. eksport logów audytowych. 34. wyświetlać lokalizację urządzenia na żądanie. 35. wyświetlać lokalizację urządzenia w interwałach czasowych. 36. wyświetlać lokalizację urządzenia w ruchu. 37. możliwość zablokowanie/odblokowanie aplikacji na urządzeniu.     1. system nie może wymagać połączenia do sieci internet, w celu realizacji dowolnej funkcjonalności.     2. oprogramowanie musi umożliwiać zarządzanie urządzeniami mobilnymi typu smartphone z zainstalowanym systemem operacyjnym: Android v.12 i wyższym.     3. system musi oferować wbudowane centrum certyfikacji.     4. system będzie w stanie pobierać z urządzeń końcowych informacje np: Informacja o producencie, modelu, systemie operacyjnym, wersji systemu, stanie baterii, numery IMEI, numer seryjny itd.     5. system loguje próby połączenia nieautoryzowanego urządzenia.     6. system umożliwia generowanie raportów.     7. system ma możliwość definiowania i dystrybucji masowej zdefiniowanych polityk bezpieczeństwa na urządzenia końcowe.     8. rejestracja urządzeń końcowych na serwerze musi odbywać się bez połączenia na serwery zewnętrzne.     9. system musi posiadać możliwość zdalnego usuwania danych z telefonu i całej konfiguracji (Wipe urządzenia).     10. System musi oferować co najmniej możliwość: 38. zablokowania tetheringu i mobilnych hotspotów. 39. zablokowania dodawania nowych konfiguracji Wi-Fi. 40. zablokowania podłączania nośników fizycznych. 41. zablokowania połączeń wychodzących. 42. zablokowania SMS. 43. zablokowania transferu plików przez USB. 44. ustawiania metod wprowadzania danych. 45. zarządzania usługami lokalizacji. 46. zablokowania dodawania użytkowników nowych użytkowników do urządzenia. 47. zablokowania zrzutów ekranu. 48. zablokowania opcji deweloperskich. 49. zablokowania trybu awaryjnego. 50. zablokowania przywracania urządzeń do ustawień fabrycznych przez użytkownika. 51. zablokowania mikrofonu. 52. zablokowania zmian tapety. 53. zablokowania przeglądarki.     1. system ma możliwość uruchomienia urządzenia końcowego Android w trybie Kiosku[[1]](#footnote-1) (telefon de facto służy tylko jako terminal dostępowy do wgranej aplikacji).     2. system ma możliwość zdalnego blokowania urządzania.     3. system ma możliwość wykonania zdjęcia podczas blokady urządzenia.     4. system ma możliwość uruchomiania funkcjonalności obszarowego ograniczania wykorzystania urządzeń końcowych.     5. system musi rejestrować udane i nieudane próby logowania na koncie administratora.     6. system musi oferować wbudowany audyt integralności danych i bezpieczeństwa serwera.     7. rollout urządzenia końcowego odbywa się w architekturze on-premise z wykorzystaniem loginu i hasła lub kodu QR lub równoważne. |
|  | **DOKUMENTACJA TECHNICZNA** |
|  | Dokumentacja Systemu musi zawierać wszystkie niezbędne informacje odnośnie procedur i polityk dotyczących systemu, zastosowanych konfiguracji, instrukcji realizacji wymaganych funkcjonalności oraz uzgodnionych w trybie roboczym, nie ujętym w niniejszym dokumencie, informacji. Dokumentacja powdrożeniowej powinna być napisana w języku polskim (wersja elektroniczna w formacie MS Word, docx oraz .pdf). |
|  | **WYMAGANIA GWARANCYJNE ORAZ W ZAKRESIE SERWISOWANIA:** |
|  | 1. Wykonawca zapewni usługę wsparcia powdrożeniowego dla oprogramowania do zarządzania urządzeniami mobilnymi. 2. Usługa wsparcia powdrożeniowego musi uprawniać Zamawiającego przez okres 36 mies. liczonych od dnia podpisania Protokołu Odbioru bez zastrzeżeń do: 3. Telefonicznego i mailowego wsparcia w języku polskim przez 5 dni w tygodniu (od poniedziałku do piątku z wykluczeniem dni ustawowo wolnych od pracy), od godziny 8.00 do 16.00. 4. W przypadku zgłoszeń wad o wysokim priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 4 godziny, czas rozwiązania problemu maksymalnie w 2 dni robocze liczone od dnia zgłoszenia. 5. W przypadku zgłoszeń wad o normalnym priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 48 godzin, czas rozwiązania problemu maksymalnie w 7 dni roboczych liczone od dnia zgłoszenia. 6. Dodatkowych konsultacji telefonicznych i mailowych w zakresie działania systemu. 7. Instruktażu telefonicznego i mailowego lub online dotyczącego oprogramowania. 8. Konsultacji telefonicznych i mailowych lub online w zakresie konfiguracji zaoferowanego rozwiązania w celu usprawnienia jego działania. 9. Aktualizacji oprogramowania do najnowszych wersji wykonywanych przez Wykonawcę w siedzibie Zamawiającego lub zdalnie/online. 10. Obsługi zgłoszeń w siedzibie Zamawiającego lub zdalnie/online. 11. Szkolenie z wystawieniem certyfikatu producenta oprogramowania dla wyznaczonych administratorów w zakresie administracji, obsługi oraz utrzymania dostarczonego oprogramowania. 12. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim. 13. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz w siedzibie Zamawiającego. 14. System będzie zaimplementowany na środowisku serwerowym Zamawiającego. |

**ZADANIE NR 3**

**Oprogramowanie do skanowania podatnościami (VM)**

|  |  |
| --- | --- |
|  | **PRZEDMIOT ZAMÓWIENIA** |
|  | Zakup i dostawa oprogramowania do skanowania sieci oraz systemów IT pod kątem podatności wraz ze wsparciem na okres 12 mies. |
|  | **WYMAGANE PARAMETRY TECHNICZNE:** |
|  | 1. **Wymagania niefunkcjonalne** |
|  | * 1. przygotowanie planu przedwdrożeniowego.   2. licencja/licencje pozwalające na wieczystą obsługę 2 maszyn wirtualnych realizujących funkcjonalność skanowania podatności.   3. prace wdrożeniowe na infrastrukturze w siedzibie Zamawiającego.   4. wsparcie producenta w języku polskim przez dedykowanych inżynierów.   5. dopuszczalny język interfejsu polski lub angielski.   6. system musi pracować w architekturze on-premise.   7. żadna funkcjonalność nie może być czasowa/abonamentowa.   8. możliwość aktualizacji bazy podatności w trybie offline (z zewnętrznych zasobów).   9. system będzie zaimplementowany na środowisku serwerowym Zamawiającego. |
|  | 1. **Wymagania funkcjonalne** |
|  | * 1. system posiada konfigurowalny moduł odpowiadający za wyświetlanie zdefiniowanych przez administratora Dashboardów.   2. system umożliwia zarządzanie użytkownikami.   3. system posiada możliwości przeprowadzanie wstępnego skanowania, określającego dostępne zasoby sieciowe które system może zbadać w skanowaniu właściwym.   4. system umożliwia generowanie reportów w formatach min. XML, PDF.   5. system w wersji wirtualnej powinien zostać dostarczony w postaci predefiniowanej maszyny wirtualnej, kompatybilny z hypervisorem tj. Hyper-V.   6. wykonawca dostarczy oprogramowanie w języku polskim lub angielskim.   7. system musi umożliwiać uruchomienie różnych trybów skanowania: natychmiastowego, zaplanowanego, częściowego.   8. system musi wykorzystywać protokoły i/lub technologie kolekcjonujące kluczowe metryki i zdarzenia, takie jak SNMP lub NETFLOW lub równoważne.   9. po połączeniu do wybranej sieci, system nie może wymagać instalacji dodatkowego oprogramowania (agentów) do przeprowadzenia badania podatności.   10. rozwiązanie musi zapewnić możliwość skanowania w trybie bez autentykacji i/lub autoryzacji   11. wykorzystywane podczas skanowania podatności testy, powinny być zależne od przeprowadzonego wcześniej wstępnego rozpoznania sieci.   12. mechanizm rozpoznania sieci musi mieć możliwość wykrywania dostępnych hostów do przeskanowania. Co najmniej z wykorzystaniem następujących technologii:   - ICMP Ping,  - TCP-ACK Service Ping,  - TCP-SYN Service Ping,  - ARP Ping,  - ACK Service ping,  - równoważne.   * 1. system powinien zapewnić możliwość automatyzacji procesów.   2. system musi mieć możliwość obsługi jednorazowo do 250 adresów IP podczas jednego skanowania.   3. ogólna liczba adresów IP, które system będzie skanował w ciągu miesiąca musi być nieograniczona. Ograniczeniu nie mogą podlegać również inne funkcjonalności oferowane przez system.   4. system powinien obsługiwać automatyczny/zaplanowany transfer logów z konsoli w celu archiwizacji.   5. system zapewni możliwość śledzenia zmian ryzyka związanego z konkretnym hostem (np. Adres MAC).   6. system powinien posiadać możliwość logowania do systemów klasy SIEM, poprzez rsyslog, syslog lub równoważne.   7. wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone.   8. System musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:   - podanie listy adresów IP,  - wskazanie zakresu adresów IP,  - podanie listy adresów IP podsieci,  - tworzenie dynamicznie lub statycznie grup systemów,  - wskazanie nazw domenowych systemów.   * 1. wykryte podatności powinny wyświetlać się w formie pozwalającej na szybkie odniesienie do otwartych baz podatności.   2. system musi pozwalać na wybór konkretnych podatności, jakie będą sprawdzane podczas skanowania co najmniej na podstawie wskazanego CVE.   3. podczas pracy w sieci system musi umożliwiać ciągłe monitorowanie ruchu w sieci w celu wykrycia podejrzanych przepływów sieciowych z lub do podatnych usług oraz podatnych urządzeń.   4. system musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów z następujących rodzin:   - Windows,  - Unix,  - Linux,  - HyperV  - Cisco,  - MySQL,  - SQL Server,  - PostgreSQL.   * 1. system musi zawierać implementacje mechanizmu oceny skali zagrożenia, które generuje wykryta podatność, co najmniej w skali CVSS 2.0.   2. dla wykrytych podatności system musi być w stanie wygenerować listę możliwych środków, które administrator będzie mógł podjąć, aby zlikwidować podatność bądź ograniczyć ryzyko związane z ich występowaniem.   3. system musi pozwalać na wykonanie ręcznej oraz zaplanowanej kopii zapasowej konfiguracji.   4. interfejs zarządzania funkcjonalnością skanowania musi być dostępny w formie aplikacji internetowej, obsługiwanej minimum przez przeglądarki Chrome, Firefox i MS Edge.   5. system musi oferować możliwość konfiguracji zarówno za pośrednictwem interfejsu graficznego jak i tekstowego.   6. system musi oferować skanowanie sieci minimum dla następujących protokołów i technologii:   - WMI,  - LDAP,  - RADIUS,  - http,  - SMB,  - SSH,  - TCP,  - UDP,   * 1. system dla odkrytych podatności musi mieć możliwość oznaczenia ich jako tzw. false-positive.   2. system musi oferować możliwość integracji ze skanerami innych producentów przynajmniej przy użyciu protokołu OSP (Open Scanner Portocol).   3. system musi oferować co najmniej następujące silniki skanowania:   - OpenVAS,  - Notus. |
|  | **DOKUMENTACJA TECHNICZNA** |
|  | Dokumentacja Systemu musi zawierać wszystkie niezbędne informacje odnośnie procedur i polityk dotyczących systemu, zastosowanych konfiguracji, instrukcji realizacji wymaganych funkcjonalności oraz uzgodnionych w trybie roboczym, nie ujętym w niniejszym dokumencie, informacji. Dokumentacja powdrożeniowej powinna być napisana w języku polskim (wersja elektroniczna w formacie MS Word, docx oraz .pdf). |
|  | **WYMAGANIA GWARANCYJNE ORAZ W ZAKRESIE SERWISOWANIA:** |
|  | 1. Wykonawca zapewni usługę wsparcia powdrożeniowego dla oprogramowania. 2. Usługa wsparcia powdrożeniowego musi uprawniać Zamawiającego przez okres 12 mies. liczonych od dnia podpisania Protokołu Odbioru bez zastrzeżeń do: 3. Telefonicznego i mailowego wsparcia w języku polskim przez 5 dni w tygodniu (od poniedziałku do piątku z wykluczeniem dni ustawowo wolnych od pracy), od godziny 9.00 do 17.00. 4. W przypadku zgłoszeń wad o wysokim priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 4 godziny, czas rozwiązania problemu maksymalnie w 2 dni robocze liczone od dnia zgłoszenia. 5. W przypadku zgłoszeń wad o normalnym priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 48 godzin, czas rozwiązania problemu maksymalnie w 7 dni roboczych liczone od dnia zgłoszenia. 6. Dodatkowych konsultacji telefonicznych i mailowych w zakresie działania systemu. 7. Instruktażu telefonicznego i mailowego lub online dotyczącego oprogramowania. 8. Konsultacji telefonicznych i mailowych lub online w zakresie konfiguracji zaoferowanego rozwiązania w celu usprawnienia jego działania. 9. Aktualizacji oprogramowania do najnowszych wersji wykonywanych przez Wykonawcę w siedzibie Zamawiającego lub zdalnie/online. 10. Obsługa zgłoszeń w siedzibie Zamawiającego lub zdalnie/online. 11. Szkolenie z wystawieniem certyfikatu producenta oprogramowania dla wyznaczonych administratorów w zakresie administracji, obsługi oraz utrzymania dostarczonego oprogramowania. 12. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim. 13. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz w siedzibie Zamawiającego. |

|  |
| --- |
| **Oświadczenie**  **o spełnianiu przez oferowane dostawy wymagań określonych w OPZ** |
| Składając ofertę w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym - art. 275 ustawy Pzp.,  **oświadczam, że**  **oferowany przedmiot zamówienia** **pozostaje w zgodności z opisem przedmiotu zamówienia** ze wszystkimi parametrami określonymi przez Zamawiającego i spełnia minimalne wymagane parametry.   |  |  |  | | --- | --- | --- | | ***zadanie nr*** | ***nazwa*** | ***pełna nazwę handlowa, model i/lub typ, marka oraz nazwa producenta*** | | ***1*** |  |  | | ***2*** |  |  | | ***3*** |  |  | |

|  |
| --- |
|  |
| *Imię i nazwisko osoby uprawnionej do reprezentacji Wykonawcy lub pełnomocnika* |

1. Tryb kiosk rozumiany jako, maksymalne ograniczenia funkcjonalności urządzenia, zgodnie z wcześniej ustawionymi politykami bezpieczeństwa, wyłączenie większości funkcji telefonu m.in.. brak możliwości wejścia do ustawień telefonu, brak możliwości wykonywania połączeń, wysyłania smsów, brak sklepu aplikacyjnego. Umożliwienie tylko włączenia wybranych aplikacji). [↑](#footnote-ref-1)