Numer referencyjny postępowania:

**WSZ-EP-57/2022**

**Załącznik nr 1.1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**„Wdrożenie oprogramowania podnoszącego poziom cyberbezpieczeństwa w Wojewódzkim Szpitalu Zespolonym im. dr. Romana Ostrzyckiego w Koninie”**

**WYMAGANIA OGÓLNE**

Przedmiotem zamówienia jest wdrożenie usług i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Szpitalu.

Powyżej wyspecyfikowano minimalne parametry oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z konfiguracją dostarczanego oprogramowania:**

1. Instalacja oraz konfiguracji oprogramowania.
2. Testy rozwiązania.
3. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
4. Dostarczenie dokumentacji powykonawczej, która będzie składała się co najmniej z następujących elementów:
	* Specyfikacja techniczna,
	* Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
	* Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
	* Szczegóły dotyczące instalacji i uruchomienia dostarczonego rozwiązania, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
	* Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis parametrów minimalnych dostarczanego oprogramowania:**

|  |
| --- |
| ***1. System monitoringu infrastruktury IT (SOC) – usługa świadczona do 31.12.2022*** |
| ***Lp.*** | ***Wymagane minimalne parametry techniczne*** |
| ***Użytkownicy*** |
| 1. | * Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.
* Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.
* Ograniczania użytkownikom dostępu do wybranych grup hostów.
 |
| ***Monitorowanie*** |
| 1. | * Monitorowania serwerów fizycznych.
* Monitorowania urządzeń sieciowych.
* Monitorowania stanu połączeń.
* Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
* Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
* Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.
* Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
* Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
* Grupowanie hostów.
* Definiowanie planowanych przerw serwisowych dla hostów i usług.
* Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
* Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
* Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
* Monitorowanie serwerów za pomocą agentów
* Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server .
* Monitorowanie Active Directory.
* Monitorowanie serwerów plików, udziałów sieciowych.
* Monitorowanie statusu serwerów Apache.
* Monitorowanie baz danych:
* ORACLE,
* MySQL,
* Postgress.
* MSSQL Server
* DB2
* Monitorowanie urządzeń przez następujące protokoły:
* SNMP,
* WMI,
* IPMI.
* Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
* Monitorowanie poprawności działania DNS.
* Monitorowanie środowiska VMware.
* Monitorowanie środowiska Hyper-V.
* Monitorowanie działania serwera czasu NTP.
* Monitorowanie offsetu czasu na serwerach.
* Monitorowanie ping - czasy odpowiedzi, straty pakietów.
* Monitorowanie zajętości miejsca na poszczególnych partycjach.
* Monitorowanie obciążenia dysków.
* Monitorowanie wykorzystania pamięci RAM.
* Monitorowanie obciążenia CPU.
* Monitorowanie logów systemowych Windows.
* Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
* Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
* Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
* Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)
* Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
* Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
* Wykrywanie niestabilnie działających usług.
* Monitorowanie dostępności stron internetowych.
* Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
 |
| ***Prezentacja*** |
| 1. | * Prezentację stanu urządzeń na mapie.
* Prezentację danych na dashboardach.
* Elastyczną konfigurację dashboardów, wybór elementów.
* Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
* Tworzenie indywidualnych dashboardów przez użytkowników
 |
| ***Powiadomienia*** |
| 1. | * Globalne wyłączanie powiadomień.
* Powiadamianie użytkownika o problemach przez e-mail.
* Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
* Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.
* Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
 |
| ***Konfiguracja*** |
| 1. | * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW
* Automatyczna konfiguracja i działanie z REST-API
* Centralne zarządzanie agentami
* Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
 |
| ***Monitoring bazy danych systemu HIS*** |
| 1. | Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:* Instance state
* Version
* Jobs
* Locks
* Processes
* Number of active sessions
* Recovery area
* Log switch activity
* General tablespace information
* Tablespaces performance
* Long active sessions
* Undo retention
* Checkpoint and online backup state
* Custom SQLs
* RMAN backup status
* RMAN backups
* ASM disk groups
* Apply and transport lag of Oracle Data-Guard
* Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości
 |
| ***Kolektor logów*** |
| 1. | * System posiada własny kolektor logów syslog
* Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps
* Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event
* Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
 |
| ***Cyberbezpieczeństwo*** |
| 1. | * System monitoruje urządzenia klasy UTM minimum w zakresie:
* wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika
* monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT.
* monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1).
* monitoruje aktualną liczbę sesji na urządzeniu
* monitoruje liczbę dostępnych tuneli IPSec VPN
* monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.
* monitoruje poziom wykorzystania procesora
* Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.
* System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog
* System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.
 |
| ***SOC i NOC*** |
| 1. | * Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty
* W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.
* Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA.
* Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
* Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza
* Reakcji.
* Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
* W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:
* Serwery wirtualne - 65 sztuk
* Serwery fizyczne - 13 sztuk
* Macierze 5 sztuk
* Kontrolery WiFi – 2 sztuki
* UTM – 5 sztuk
* Przełączniki LAN - 113 sztuk
* Serwer Backupu - 2 sztuki
* Bibliotekę taśmowa LTO - 1 sztuka
* UPS 5 sztuk
* W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS:
* Monitorowanie komunikacji z platformą P1
* Monitorowanie komunikacji bramek HL7
* Monitorowanie komunikacji EWUŚ
* Monitorowanie KOWAL
* Monitorowanie komunikacji AP-KOLCE
* Monitorowanie RZM
* Monitorowanie bazy danych systemu HIS
 |

|  |
| --- |
| ***2.*** ***SIEM*** |
| ***Lp.*** | ***Wymagane minimalne parametry techniczne*** |
| ***Wymagania ogólne*** |
| 1. | * System musi wykorzystywać nierelacyjną, rozproszoną bazę danych opartą o Elasticsearch w wersji minimum 7.x/
* System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL"
* System musi pracować w oparciu o architekturę Linux.
* System musi mieć możliwość centralnego zbierania i zarządzania logami
* System działać w trybie zbliżonym do rzeczywistego
* System musi umożliwiać funkcjonowanie bez dostępu do sieci internet
* System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
* Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
* System musi zapewniać efektywną obsługę co najmniej 4000 EPS lub 80  GB danych dziennie
* System musi zapewniać retencję danych w okresie minimum 30  dni.
* Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
* System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
* Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
* Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
* System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
* System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
* Interfejs musi posiadać angielską lub polską wersję językową.
* System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
* System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
* System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
* System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
* System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
* System musi pozwalać na tworzenie parserów z poziomu GUI
* System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
* System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
* System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
* System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
* Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
* System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
* System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
* Syslog,
* WEF,
* Flat file,
* Event log,
* WMI,
* SNMP trap,
* XML,
* JSON,
* JDBC/ODBC
* CSV,
* Email,
* Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
* System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
* System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
* System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
* System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
* Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
* System musi posiadać predefiniowany zestaw parserów zdarzeń.
* System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
* System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
* System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
* System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
* Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
* Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
* System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
* System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
* 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.
* Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
* System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL
* System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
* Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
* System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
* System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
* System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
* Wykrycia dowolnej treści w logach,
* Wykrycia wystąpienia wartości pola na wybranej liście,
* Wykrycia niewystępowania wartości pola na wybranej liście,
* Wykrycia zmiany jednego z kilku pól,
* Wykrycia zdarzeń występujących z zadaną częstotliwością,
* Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
* Wykrycia zaniku Wiadomości,
* Wykrycia nowej wartości pola w zadanym okresie czasu,
* Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
* System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
* Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
* System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
* System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
* System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
* System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
* System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
* System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
* Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
* System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
* Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
* System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
* System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
* System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
* Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
* System musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
* System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 1 roku.
* Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
* System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
* Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.
* Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.
 |
| ***Dostęp do systemu*** |
| 1. | * Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywac się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
* Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protoków TLS w wersji minimum 1.3.
* System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
* Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
* Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP,Radius
* Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
* System musi wspierać mechanizm logowania typu Single Sign On.
* System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
* System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
* System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
 |
| ***Przyjmowanie, identyfikacja i wizualizacja danych*** |
| 1. | * Netflow,
* System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizy formatu Netflow w wersji min. V5, v9 oraz IPFIX z wykorzystaniem oficjalnych modułów dostarczanych przez producenta.
* System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, rentransmisji, Jitter, Server Response Time oraz Round Trip Time.
* Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
* System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
* System posiada natywna integrację z Mitre ATT@CK.
 |
| ***Reguły korelacyjne, alerty i obsługa incydentów*** |
| 1. | * System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
* System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
* System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
* System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
* System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit’u i wykrywania ukrytych procesów, plików, portów
* System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
* System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
 |
| ***Raportowanie i Archiwizacja danych*** |
| 1. | * System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
* Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
* Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
* Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich 0wcześniejszego rozpakowania.
* System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
* Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
* System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
 |
| ***Wdrożenie*** |
| 1. | * Zakres oczekiwanych prac związanych z wdrożenie systemu SIEM:
* Opracowanie harmonogramu wdrożenia systemu SIEM.
* Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.
* Przeprowadzenie instalacji i konfiguracji systemu SIEM.
* Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.
* Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
* Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.
* Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
* Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
* Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.
 |
| ***Wymagania niefunkcjonalne*** |
| 1. | * Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem SIEM dla 5  pracowników zamawiającego w wymiarze 2 dni roboczych (min. 16h roboczych).
* Szkolenie odbędzie się w siedzibie Zamawiającego.
* Szkolenie musi być prowadzone w języku polskim.
* Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
* Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.
 |

|  |
| --- |
| ***3. Wykonanie skanu podatności*** |
| **Lp.** | **Wymagane minimalne parametry techniczne** |
| **1.** | * Wykonanie skanów otwartych portów w całej adresacji publicznej audytowanego podmiotu.
* Wykorzystanie dedykowanego oprogramowania do wykrywania podatności zasilonego
* najnowszą bazą znanych podatności.
* Wykonanie skanów nieuwierzytelnionych.
* Wykonanie raportu końcowego.

**Planowanie (faza I)*** Rekonesans, kolekcja danych i pozyskiwanie informacji, mapowanie

**Testy stabilności i dostępności infrastruktury sieciowej na styku z Internetem (faza II)*** Skan całej puli adresacji publicznej jednostki audytowanej
* Testy ekspozycji systemów na styku z Internetem
* Opcjonalne testy destabilizujące infrastrukturę sieciową typu Denial of Service
* W sytuacji wykrycia mniejszej bądź większej liczby systemów niż w przyjętych w punkcie
* „założenia skali i architektury przyjęte w wycenie”, nastąpi spotkanie między
* zamawiającym, a wykonawcą, które będzie miało na celu doprecyzowanie danych lub
* przekazanie dodatkowych informacji wykonawcy

**Raportowanie (faza III)*** Zebranie wyników testów bezpieczeństwa
* Analiza wyników audytu
* Opisanie podatności wraz z kategoryzacją CVE i CVSS
* Opisanie rekomendacji
* Przekazanie raportu
* Zawartość raportu:
* Executive Summary – główne konkluzje
* Główne rekomendacje
* Przedmiot testów
* Risk Rating
* Metodologia i kryteria testowania
* Wykorzystane narzędzia w trakcie prowadzenia skanów
* Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE
* (Common Vulnerability Enumaration) oraz odnośnikiem do opisu luki.
* Podatności będą pogrupowane według ryzyka, zgodnie ze standardem CVSS
* (Common Vulnerability Scoring System).
* Rekomendacje związane z możliwym usunięciem wykrytych podatności
 |
| **Istotne założenia** |
| **1.** | * Typ prowadzonego audytu: Black Box / Grey Box
* W momencie konieczności przeprowadzenia skanu uwierzytelnionego wykonawca ma prawo uzyskać od jednostki audytowanej poświadczenia dla danego systemu. Będzie to warunkiem

prowadzenia skanu uwierzytelniającego. Brak przekazania poświadczeń uwierzytelniających nie będzie podstawą do wstrzymania audytu.* W ramach testów nie jest przewidziana próba przełamania zabezpieczeń fizycznych lub sprawdzenia reakcji służb bezpieczeństwa zamawiającego na nieautoryzowany dostęp
* Zespół testerów dołoży wszelkich starań w trakcie pozyskiwania informacji i testowania w celu zminimalizowania ingerencji w sieć produkcyjną. Jednak działania testerów mogą być obarczone pewnym prawdopodobieństwem destabilizacji niektórych usług, o czym

wykonawca powiadomi zamawiającego przed wykonaniem danego testu.* Działania audytowe mogą być prowadzone o dowolnej porze dnia i nocy.
* Przed rozpoczęciem prac audytowych niezbędne będzie wypełnienie stosownej deklaracji osób decyzyjnych zamawiającego oraz jednostki audytowanej świadczącej o zgodzie na działania i wiedzy nt. potencjalnych skutków działań testerów.
* Testowanie odbędzie się zdalnie z biura oraz centrum przetwarzania danych wykonawcy
* Audyt danej jednostki zostaje zakończony w momencie przekazania raportu zamawiającemu jako zaszyfrowany załącznik w wiadomości Email
* Tester użyje komputera niepowiązanego z podmiotem audytowanym przy próbach dostępu do zasobów
 |

***Szkolenia***

Przeprowadzenie szkoleń (stacjonarnych oraz w trybie online) skierowanych do:

1. Personelu medycznego – tryb online zakończony uzyskaniem certyfikatu poświadczającego odbycie szkolenia – ilość godzin - 1

w zakresie cyberbezpieczeństwa:

- ochrony przed zaawansowanymi atakami przez pocztę i WWW,

- obrona przed phishingiem i socjotechniką,

1. Kadry zarządzającej, kierowników komórek organizacyjnych i samodzielnych stanowisk pracy – tryb stacjonarny zakończony uzyskaniem certyfikatu poświadczającego odbycie szkolenia – ilość godzin – 4

w zakresie cyberbezpieczeństwa:

- zarządzanie ryzykiem w systemie bezpieczeństwa informacji, omówienie najnowszych wytycznych
w ustawie o KSC.

- tworzenie i utrzymanie polityki ciągłości działania,

- ochrony przed zaawansowanymi atakami przez pocztę i WWW,

- obrona przed phishingiem i socjotechniką.