Miejscowość: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Załącznik nr 1**

**FORMULARZ OFERTOWY**

**ZAPYTANIE OFERTOWE nr 26/** **System do zarządzania informacjami i zdarzeniami bezpieczeństwa typu SIEM (Security Information and Event Management)**

Nazwa Wykonawcy:

Adres:

NIP:

Nr telefonu:

Adres e-mail:

Dane osoby do kontaktu:

W odpowiedzi na zapytanie ofertowe pn. *ZAPYTANIE OFERTOWE nr 26/ System do zarządzania informacjami i zdarzeniami bezpieczeństwa typu SIEM (Security Information and Event Management)* oferuję wykonanie przedmiotu zamówienia, zgodnie z wymogami i zakresem określonym w zapytaniu ofertowym, za:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Waluta oferty**  **(PLN / EUR)** | **Ogółem wartość NETTO we wskazanej walucie** | **Wartość podatku VAT we wskazanej walucie** | **Ogółem wartość BRUTTO we wskazanej walucie** |
| System do zarządzania informacjami i zdarzeniami bezpieczeństwa typu SIEM (Security Information and Event Management) |  |  |  |  |

**Całkowita wartość zamówienia brutto słownie:**

1. **Ceny wskazane w tabeli uwzględniają wszystkie koszty związane z wykonaniem przedmiotu zamówienia i są cenami stałymi w okresie obowiązywania umowy.**
2. Cały przedmiot zamówienia będzie posiadał aktualne atesty i certyfikaty bezpieczeństwa poświadczające zgodność z normami obowiązującymi w Unii Europejskiej oraz zgodności i certyfikaty określone w zapytaniu ofertowym.
3. Zobowiązujemy się do wykonania przedmiotu zamówienia z zastosowaniem następujących urządzeń i materiałów:

(***W każdym wierszu tabeli należy podać informację czy/jak oferowany sprzęt spełnia wymagania Zamawiającego. Dopuszcza się wypełnienie wierszy w formule TAK/NIE. W przypadku braku zamieszczenia informacji (braku wypełnienia) w którymkolwiek z obowiązkowych pól, oferta zostanie odrzucona. Wykonawca tam gdzie jest to możliwe wskazuje również „Typ/model oferowanego urządzenia” oraz „Producenta”).***

|  |  |  |
| --- | --- | --- |
| **Lp** | **Parametry techniczne przedmiotu zamówienia** | **Potwierdzenie spełnienia /**  **Parametry oferowane[[1]](#footnote-2)** |
| **1.** | **System do zarządzania informacjami i zdarzeniami bezpieczeństwa typu SIEM (Security Information and Event Management)** | Typ:  Model:  Producent: |

|  |  |
| --- | --- |
| System musi udostępniać mechanizmy pozwalające na integracje urządzeń źródłowych nie znajdujących się w powyższej liście, z wykorzystaniem graficznego kreatora reguł parsowania. |  |
| Graficzny kreator reguł parsowania musi obsługiwać co najmniej formaty: JSON, CEF, LEEF, lista, lista par "klucz-wartość", XML. |  |
| Graficzny kreator reguł parsowania musi umożliwiać tworzenie reguł z wykorzystaniem wyrażeń regularnych. |  |
| Graficzny kreator reguł parsowanie musi mieć możliwość podpowiadania użytkownikowi wzorca wyrażenia regularnego dla wskazanego łańcucha w payloadzie. |  |
| Mechanizmy integracji źródeł, zarówno tych wskazanych przy wdrożeniu, jak i integrowanych w przyszłości przez Zamawiającego, nie mogą być w żaden sposób ograniczane licencyjnie przez producenta ani wymagać dodatkowych opłat ze strony Zamawiającego. |  |
| System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu i pozwalać na równoległe używanie różnych sposobów normalizacji logów. |  |
| System musi posiadać możliwość automatycznego rozpoznawania źródeł logów, które są przekierowane do SIEM (zakładając, że posiada parser dla technologii tego źródła danych). Musi automatycznie rozpoznać typ logu i dobrać odpowiedni parser, tak aby nie była wymagana żadna aktywność ze strony administratora systemu |  |
| System musi umożliwiać pobieranie i analizę przepływów co najmniej w formatach: Netflow w wersji 1, 5, 7 i 9, IPFIX, sFLow w wersji 2, 4 i 5, J-Flow i Packeteer. |  |
| System musi posiadać możliwość zainstalowania natywnego komponentu generującego dane o przepływach na podstawie analizy ruchu sieciowego. |  |
| System musi mieć możliwość przeprowadzenia zarówno bez agentowej jak i agentowej akwizycji danych. W przypadku stosowania agentów, system nie może ograniczać licencyjnie ilości wykorzystywanych agentów. |  |
| Zbierane informacje muszą być poddane w systemie korelacji, na podstawie których administratorzy systemu będą informowani o stanie bezpieczeństwa infrastruktury Zamawiającego oraz ostrzegani o ewentualnych incydentach bezpieczeństwa |  |
| System musi zawierać bazę co najmniej 100 predefiniowanych reguł korelacyjnych, których wykorzystanie przez Zamawiającego nie wymaga ponoszenia dodatkowych nakładów z tym związanych. |  |
| System musi umożliwiać budowanie reguł korelacyjnych bazujących na zdarzeniach, przepływach, jednocześnie zdarzeniach i przepływach, a także na innych korelacjach |  |
| System umożliwia wykorzystanie reguł korelacyjnych jako bloków do wykorzystania w nadrzędnych regułach korelacyjnych. |  |
| System, oprócz prezentowania informacji o alertach w tablicach, musi posiadać możliwość powiadamiania o zdarzeniach co najmniej przez: powiadomienie ekranowe, e-mail, syslog, SNMP, wywołanie skryptu |  |
| System musi umożliwiać zastosowanie w regułach korelacyjnych testów logicznych na wartościach pól bazy danych zdarzeń i przepływów |  |
| System musi umożliwiać zastosowanie w regułach języka zapytań bazy danych zdarzeń i przepływów |  |
| System musi umożliwiać zastosowanie w regułach testów zawartości payloadu zdarzenia. |  |
| Rozwiązanie musi posiadać wbudowane mechanizmy śledzące wydajność reguł korelacyjnych |  |
| System musi umożliwiać oznaczanie reguł taktykami i technikami frameworku MITTRE ATT&CK |  |
| System nie może wykorzystywać bazy danych ogólnego zastosowania do przechowywania zdarzeń i przepływów |  |
| Baza danych musi umożliwiać wydawanie poleceń w języku zapytań bazy danych. |  |
| Ze względu na zachowanie integralności danych, język bazy danych zdarzeń i przepływów może pozwalać na wykonanie jedynie polecenia SELECT. Baza danych nie może pozwalać na wykonywanie poleceń UPDATE, INSERT i DELETE. |  |
| Dane pochodzące z logów zapisywane są w domyślnie dostępnych polach bazy danych przynajmniej takich jak: nazwa zdarzenia, kategoria zdarzenia, adres IP źródłowy, źródłowy port TCP/IP, adres IP źródłowy przed translacją, adres IP źródłowy po translacji, czas urządzenia, z którego wysłany był log, nazwa protokołu, nazwa użytkownika, nazwa hosta, nazwa grupy, nazwa NetBIOS (o ile zawartość tych pól jest zawarta w logu) |  |
| Dane pochodzące z przepływów sieciowych muszą zostać domyślnie zapisane w dostępnych polach bazy danych przynajmniej takich jak: adres IP źródłowy, port źródłowy, adres IP docelowy, port docelowy, ilość wysłanych/odebranych |  |
| System musi umożliwiać dodanie własnych pól w bazie, które można przywoływać jako kryteria wyszukiwania, określane przy pomocy nowych wzorców |  |
| System musi przechowywać w bazie danych również payloady zdarzeń i przepływów |  |
| System musi umożliwiać wskazanie które pola mają być zapisywane w bazie danych bezpośrednio po otrzymaniu zdarzenia, a które nie. W tym drugim przypadku wartość pola jest każdorazowo wyznaczana z payloadu na podstawie reguł parsera w momencie użycia tego pola (np. przy wyświetleniu lub wykonaniu testu logicznego na polu) |  |
| System musi umożliwić zapisanie wzorca wyszukiwania, a także związanych z nim szablonów prezentacji oraz wyników w celu późniejszego przywołania lub też udostępnienia wyszukiwania innym użytkownikom. |  |
| System musi umożliwiać umieszczenie zapisanego wzorca w ramach utworzonej grupy wzorców, na tablicach (dashboard) oraz w miejscu umożliwiającym szybki dostęp |  |
| System musi być w stanie przyjąć i przetworzyć minimum 195 zdarzeń na sekundę (EPS) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów ilości zdarzeń bez ich utraty |  |
| System musi być w stanie przyjąć i przetworzyć minimum 6000 przepływów sieciowych na minutę (FPM) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów zdarzeń bez ich utraty |  |
| System musi być w stanie monitorować środowisko 14 serwerów |  |
| System musi mieć możliwość budowania profilu stanu i zachowania środowiska IT oraz identyfikowania odchyleń i wykrywania anomalii na podstawie analizy behawioralnej. |  |
| System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości w ostatnim okresie od wartości w okresie historycznym |  |
| System musi mieć możliwość wykrywania anomalii na podstawie przekroczenia wartości progowej |  |
| System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości od zarejestrowanego trendu |  |
| System musi umożliwiać tworzenie szablonów raportów |  |
| Wymagane formaty raportów: co najmniej PDF, HTML, XML, XLS, CSV. |  |
| System musi mieć możliwość generowania raportów zgodnie z ustalonym harmonogramem czasowym |  |
| System musi mieć możliwość wysyłania mailem raportów na wskazane adresy |  |
| System musi mieć możliwość weryfikowania tożsamości użytkowników poprzez wykorzystanie kont lokalnych oraz zewnętrzne systemy uwierzytelnienia – MS Active Directory oraz RADIUS i LDAP. |  |
| System musi zawierać funkcjonalność precyzyjnego nadawania uprawnień użytkownikom i administratorom. |  |
| System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości |  |
| System musi posiadać zaimplementowany dedykowany dashboard prezentujący dokładne statystyki związane z wydajnością systemu, co najmniej utylizacja CPU, utylizacja pamięci RAM, heap usage, disk IO throughtput, disk IOPS, statystyki połączeń sieciowych, ilość wykonywanych zapytań, statystyki dotyczące wywołań API itp. |  |
| System musi zapewniać centralne gromadzenie wszystkich logów i zapewniać ich bezpieczne przechowywanie oraz dostępność przez okres 365 dni |  |
| System musi samodzielnie zarządzać retencją danych |  |
| System musi umożliwiać wyspecyfikowanie różnego czasu retencji danych dla różnych zdarzeń i przepływów - na podstawie zawartości pól bazy danych |  |
| System musi posiadać mechanizm automatycznego archiwizowania danych i konfiguracji systemu do katalogu w lokalnym systemie plików i określenia retencji dla przechowywanych w ten sposób danych. |  |
| System musi umożliwiać włączenie lub wyłączenie indeksacji pola bazy danych z interfejsu graficznego |  |
| Zdarzenia i przepływy muszą być przechowywane w postaci skompresowanej |  |
| System musi zapewniać możliwość obsługi poprzez przeglądarkę |  |
| System musi udostępniać możliwość prezentacji statystyk i wyników działania w postaci tablic (dashboard), których wygląd i rozkład poszczególnych składowych daje się dostosować do potrzeb administratora i użytkownika. Widoczność stworzonych i domyślnie dostępnych tablic można przełączać przy pomocy łatwo dostępnej listy rozwijanych pozycji. |  |
| Informacje prezentowane w poszczególnych tablicach są wynikiem stworzonych przez producenta predefiniowanych korelacji, a także wyników wyszukiwania stworzonych przez użytkownika lub udostępnionych mu przez innych użytkowników i administratorów. |  |
| System nie może wymagać instalacji dedykowanego oprogramowania klienckiego do jego obsługi |  |
| System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtrów tworzonych przy pomocy pól wyboru |  |
| System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru wyspecyfikowanego w języku bazy danych |  |
| System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru specyfikującego słowo występujące w payloadzie |  |
| System musi mieć możliwość tworzenia clustra wysokodostępnego dla każdego z komponentów (za wyjątkiem agenta instalowanych na innym serwerze/stacji oraz analizatora ruchu sieciowego). Awaria pojedynczego komponentu nie może spowodować utraty funkcjonalności i wydajności systemu. |  |
| System musi posiadać architekturę skalowalną horyzontalnie poprzez dodawanie serwerów przechowujących część rozproszonej bazy danych i przetwarzających zdarzenia |  |
| Każda z reguł korelacyjnych musi mieć możliwość korelowania zdarzeń i przepływów z wszystkich serwerów przetwarzających dane, bądź z jednego serwera - zależnie od decyzji projektanta reguły |  |
| System musi umożliwiać prezentację zdarzeń i przepływów w postaci tabelarycznej, z możliwością wyboru okresu lub w czasie rzeczywistym |  |
| System musi posiadać dashboard prezentujący mapę, na której w czasie rzeczywistym są prezentowane incydenty lub dowolnie zdefiniowane zdarzenia. |  |
| System musi umożliwiać automatyczne łączenie wielu incydentów w jeden. |  |
| System musi posiadać aplikację monitorującą charakterystykę zachowań użytkowników (user behavior analysis), która pozwala na ocenę ryzykownych czynności podejmowanych przez wewnętrznych użytkowników na infrastrukturze. |  |
| Aplikacja analizująca zachowania użytkowników musi przypisywać użytkownikom tzw. punkty ryzyka i generować alarm po przekroczeniu wartości progowej sumarycznych punktów ryzyka. Wartość progowa może być ustalana statycznie (bezwzględna wartość liczbowa) lub dynamicznie (na podstawie rozkładu wartości punktów ryzyka dla całej populacji użytkowników) |  |
| Aplikacja musi wyświetlać kształtowanie się poziomu ryzyka dla użytkownika w czasie |  |
| System analizy zachowań użytkowników musi mieć możliwość wykorzystania uczenia maszynowego |  |
| Wbudowane modele uczenia maszynowego mają analizować trendy zachowań w czasie oraz porównywać zachowanie użytkownika z grupą innych użytkowników o podobnych parametrach charakteryzujących danego użytkownika - przykładowo ulokowanie w konkretnym kontenerze Active Directory lub posiadających konkretny atrybut (np. nazwa stanowiska) |  |
| Użytkownik musi mieć możliwość tworzenia własnych modeli uczenia maszynowego analizujących trendy zmian wartości w czasie |  |
| W przypadku braku zdefiniowanych grup użytkowników, system musi sam wykonywać grupowanie użytkowników na podstawie podobnych wzorców zachowań |  |
| System musi mieć możliwość wyspecyfikowania grup użytkowników, dla których punkty ryzyka są modyfikowane o wyspecyfikowany mnożnik |  |
| System musi umożliwić automatyczną geolokalizację źródła zagrożeń. |  |
| System musi mieć możliwość tworzenia szczegółowego logu audytowego zawierającego informacje przynajmniej o logowaniu do systemu i zmianach w jego konfiguracji |  |
| Licencja systemu SIEM oraz system SIEM nie mogą ograniczać liczby równocześnie zalogowanych użytkowników |  |
| System musi posiadać możliwość automatycznego wykrywania nowych elementów infrastruktury poprzez analizę zdarzeń i/lub ruchu sieciowego. SIEM musi wykryć pojawienie się nowego adresu IP, adresu MAC i opcjonalnie zgłosić to operatorowi. |  |
| System musi posiadać możliwość automatycznego grupowania elementów infrastruktury poprzez ich cechy charakterystyczne. Przykładowo, system SIEM powinien być w stanie dokonać klasyfikacji elementów posiadających otwarte porty charakterystyczne dla baz danych jako "serwery bazodanowe" |  |
| System musi umożliwiać tworzenie własnego schematu opisu i oznaczania (tzw. tagowania) assetów |  |
| System musi umożliwiać filtrowanie assetów w oparciu o dowolne pole charakteryzujące dany element infrastruktury |  |
| System musi zapewniać automatyczny mechanizm aplikacji poprawek do systemu. |  |
| System musi umożliwiać utworzenie struktury adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów |  |
| System musi umożliwić konfigurację serwera poczty, przez który wysyłane są wiadomości pocztowe. Musi być możliwość konfiguracji innych serwerów poczty dla różnych serwerów przetwarzających zdarzenia i przepływy. |  |
| System pozwala na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach o bardziej szczegółowe dane. |  |
| System pozwala na integrację z co najmniej tymi systemami zarządzania podatnościami: eEye, BigFix, Juniper NSM, nmap, Qualys, Rapid7, Tenable |  |
| System musi posiadać własną bazę reputacji IP |  |
| System musi posiadać możliwość przeprowadzenia korelacji historycznej, czyli symulacji działania reguły dla zdarzeń historycznych |  |
| System musi posiadać udokumentowany interfejs API |  |
| System musi posiadać narzędzie graficzne umożliwiające testowanie różnych zapytań API i weryfikację otrzymywanych danych |  |
| System musi umożliwiać rozdzielenie plików bazy danych na wiele "domen", z możliwością tworzenia oddzielnych reguł korelacyjnych dla domen |  |
| Licencja nie może bezpośrednio ograniczać wielkości przetwarzanych danych w bajtach. |  |
| System musi umożliwiać obfuskację (ukrywanie) danych wrażliwych zdarzeń i przepływów przed operatorem |  |
| System musi umożliwiać kontrolę integralności bazy danych przez zastosowanie hashowania |  |
| Producent systemu musi udostępniać zestawy dodatkowych reguł, ponad podstawowy zbiór reguł dostępny w produkcie po instalacji |  |
| System musi tworzyć indeks słów znajdujących się w payloadzie, w celu szybszego wyszukiwania zdarzeń. |  |
| System musi umożliwiać detekcję nadużycia protokołu DNS typu: DGA, squatting, tunelowanie |  |
| System musi umożliwiać tworzenie aplikacji osadzanych w interfejsie graficznym systemu |  |
| System musi mieć możliwość blokowania użytkownikom wykonywanie zapytań które mogą trwać zbyt długo lub wyszukiwań, które będą zwracały dużą ilość danych wpływających negatywnie na wydajność systemu. Takie polityki muszą mieć możliwość definiowania na poziomie użytkownika, roli lub tematów. |  |
| System oprócz podstawowego interfejsu przeglądania danych z funkcjonalnością administracyjną musi mieć dodatkowo odseparowany interfejs przeznaczony do pracy dla operatorów SOC. Interfejs musi być pozbawiony funkcjonalności administracyjnych i skoncentrowany na analizie incydentów bezpieczeństwa. |  |
| System musi zawierać funkcjonalność wsparcia przy tuningu reguł. System ma raportować reguły które najczęściej inicjują incydenty bezpieczeństwa oraz reguły które są najmniej efektywne. |  |
| System musi automatycznie informować o nowych dodatkowych funkcjonalnościach dostępnych do ściągnięcia z dedykowanego repozytorium aplikacji. |  |
| System musi zawierać dedykowany dashboard który prezentuje przydatne artykuły, wiadomości, przypadku użycia, podcasty oraz odnośniki do szkoleń. Zawartość musi być dostosowana automatycznie do charakterystyki obsługiwanej infrastruktury |  |
| System musi umożliwiać wykorzystanie tzw. zapytań federacyjnych do różnych niezależnych instancji systemów SIEM w oparciu o format STIX |  |
| System musi umożliwiać prostą integrację z systemem klasy SOAR bez konieczności prowadzenia prac integracyjnych - przykładowo za pomocą gotowej aplikacji |  |
| Licencje na system nie mogą być dostarczane w modelu subskrypcyjnym (ograniczone czasowo) |  |
| Dodanie do system kolejnego komponentu analizującego/przechowującego zdarzenia/przepływy nie może wymagać dokupienia dodatkowej licencji |  |
| Utworzenie clustra HA komponentu poprzez dodanie serwera zapasowego nie może wymagać dokupienia dodatkowej licencji |  |
| System musi znajdować się w "ćwiartce liderów" w najnowszym opracowaniu tzw. magicznego kwadratu systemów SIEM wg. Gartnera. |  |
| Zwiększenie strumienia FPM (przepływów na minutę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji. |  |
| System musi umożliwiać analizę ryzyka poprzez identyfikację (Automatyczne wykrywanie potencjalnych zagrożeń na podstawie danych z różnych źródeł, Możliwość definiowania i dostosowywania kryteriów oceny ryzyka zgodnie z wymaganiami organizacji). |  |
| System musi umożliwiać wizualizację najbardziej krytycznych obszarów ryzyka w widoku siatki na podstawie prawdopodobieństwa wystąpienia ryzyka i jego wpływu na działalność. |  |
| System musi umożliwiać wizualizację potencjalnych wskaźników ryzyka z różnych wektorów, takich jak dane, infrastruktura i tożsamość. |  |
| System w ramach analizy ryzyka musi ciągle monitorować ryzyka i generować alerty w przypadku wykrycia anomalii. |  |
| Zamawiający wymaga, aby w ramach prac Wykonawca zainstalował wymagane maszyny w środowisku Zamawiającego, przygotował integrację z MS AD w zakresie użytkowników i grup oraz integrację w zakresie pobierania logów z serwerów. |  |
| Dokumentacja Powykonawcza musi być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim. |  |

|  |  |
| --- | --- |
| Opisane powyżej wymagania zostaną dostarczone jako wbudowana funkcjonalność produktu lub jako dodatkowe moduły oficjalnie dostarczane przez producenta w repozytorium aplikacji, a nie jako funkcjonalność dodana w ramach dodatkowych prac konfiguracyjnych i integracyjnych |  |

1. Oświadczam, że zapoznałem się z treścią zapytania ofertowego oraz że nie wnoszę zastrzeżeń do jego treści i zdobyłem wszelkie informacje niezbędne do sporządzenia oferty i wykonania zamówienia. Złożona oferta spełnia wszelkie parametry i warunki zapytania ofertowego.
2. Oświadczam, że akceptuję termin związania ofertą wynoszący 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
3. Zobowiązuje się wykonać zamówienie w terminach wskazanych w Zapytaniu ofertowym,
4. W przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy na wykonanie przedmiotu zamówienia w miejscu i terminie wskazanym przez Zamawiającego.
5. Umowa będzie opiewać na kwotę brutto.
6. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
7. Posiadam wiedzę i doświadczenie niezbędne do realizacji przedmiotu zamówienia.
8. Wyrażam zgodę na przetwarzanie przez Zamawiającego danych osobowych na potrzeby realizacji niniejszego postępowania zgodnie z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) do celów związanych z przeprowadzeniem niniejszego postępowania. Moja zgoda obejmuje również przetwarzanie danych w przyszłości pod warunkiem, że nie zostanie zmieniony cel przetwarzania.
9. Jestem świadomy/-a odpowiedzialności karnej za fałszywe zeznania wynikające z art. 233 (podanie nieprawdy lub zatajenie nieprawdy) ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 ze zm.), a zawarte w ofercie informacje są zgodne z prawdą oraz stanem faktycznym.

………….……………………………

Czytelny podpis osoby uprawnionej do reprezentowania podmiotu

Załączniki:

1. Załącznik nr 2 – oświadczenie Wykonawcy – warunki udziału w postępowaniu
2. Załącznik nr 3 – wykaz dostaw

1. Zakres danych i informacji musi także potwierdzać **równoważność** oferowanych urządzeń, w stosunku do wymagań wskazanych przez Zamawiającego [↑](#footnote-ref-2)