SPECYFIKACJA PRZEDMIOTU ZAMÓWIENIA
ZAŁĄCZNIK NR 1 DO ZAPYTANIA OFERTOWEGO

KPOD.01.11-IP.06-0146_23/A2.1.1./2024/2 z dnia 20.03.2024 r.

W ramach projektu pt. ***„Zwiększenie zg. z koncepcją Przemysłu 4.0 zdoln.produkc. PEKABEX BET S.A. poprzez uruchomienie zautomatyzowanej, zrobotyzowanej i zintegrowanej z cyfrowymi procesami zarządz. produkcją linii wytwarzania ścian prefabryk. w zakładzie w Bielsku-Białej”,*** realizowanego w ramach programu Krajowego Planu Odbudowy i Zwiększenia Odporności (KPO), Komponent A, Cel szczegółowy A2., Reforma A2.1., Inwestycja A2.1.1. tj. *Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach*. Planowane jest nabycie następujących elementów:

1. **Opis przedmiotu zamówienia:**

Przedmiotem zamówienia jest dostarczenie systemu bezpieczeństwa SoC składającego się z kolektora danych wraz z oprogramowaniem do inwentaryzacji sieci i świadczeniem usługi Security Operations Center, monitorowania i reakcji na incydenty wraz 4h wsparcia architekta miesięcznie.

2. **Wymagania dla usługi monitorowania Security Operations Center:**

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych zgodnie z opisanymi poniżej wymaganiami:

1. Identyfikacja oraz utrzymanie bazy zasobów teleinformatycznych, wykorzystywanych portów i usług, protokołów komunikacyjnych oraz innych niezbędnych informacji wykorzystywanych do analizy incydentu bezpieczeństwa.
2. Proaktywna identyfikacja oraz zarządzanie cyklem życia podatności zasobów teleinformatycznych lokowanych wewnątrz sieci aż do momentu zabezpieczenia środowiska.
3. Identyfikacja i klasyfikacja podatności, oraz opracowanie i priorytetyzację rekomendacji mitygującej.
4. Usługa adresuje wymagania Rozporządzenia o ochronie danych osobowych (RODO), Ustawy o krajowym systemie cyberbezpieczeństwa (NIS), normy ISO/IEC 27001 oraz ISO/IEC 20000.
5. Analiza w czasie rzeczywistym z wykorzystaniem mechanizmów sztucznej inteligencji oraz przetwarzania w chmurze dostawcy, zdarzeń generowanych przez źródła danych takie jak aplikacje, serwery aplikacyjne, systemy operacyjne, sprzęt sieciowy czy usługi bezpieczeństwa.
6. Detekcja naruszeń bezpieczeństwa oraz reakcja na wystąpienie incydentów bezpieczeństwa teleinformatycznego poprzez powstrzymanie działań atakujących oraz eliminację zagrożenia. Realizacja procesu polega na monitorowaniu kolejki incydentów w systemie klasy SIEM, wykonywaniu triage oraz klasyfikacji incydentu bezpieczeństwa, analizie oraz opracowaniu rekomendacji w przypadku potwierdzenia incydentu bezpieczeństwa (w tym w ramach etapu powstrzymania, eliminacji oraz odzyskania sprawności) a następnie wyciąganie wniosków w ramach procesu raportowania. Proces jest realizowany zgodnie z NIST Incident Response Framework oraz wymaganiami Krajowego Systemu Cyberbezpieczeństwa.
7. Sandboxing i analiza zabezpieczonego oprogramowania malware w labolatorium Wykonawcy w celu określenia wpływu działania oprogramowania złośliwego na środowisko Zamawiającego, pozyskania danych umożliwiających podjęcie kontr działań zabezpieczających

infrastrukturę teleinformatyczną oraz opracowania ekspertyzy z analizy malware.

8. Dostarczenie informacji statystycznych w ujęciu dobowym dot. ilości i typu obsłużonych incydentów oraz transfer informacji operacyjnych w ujęciu kwartalny na poziom zarządczy dot. ryzyk oraz propozycji działań mających na celu usprawnienie modelu bezpieczeństwa.
9. Przyjęcie informacji o incydencie bezpieczeństwa teleinformatycznego poprzez całodobową infolinię oraz system ticketowy.
10. W ciągu jednej godziny od detekcji incydenty bezpieczeństwa zapewnienie sztabu kryzysowego, którego celem jest zarządzenie incydentem, wypracowanie reakcji w przypadku poważnego incydentu bezpieczeństwa oraz dostęp do zespołu zajmującego się reakcją na incydent
11. Wykonawca dostarczy raport dla zarządu z informacjami operacyjnymi o tendencjach zgrożeń i ryzyk wraz z rekomendacjami propozycji działań majcych na celu usprawnienie modelu bezpieczeństwa.
12. Okres świadczenia usugi: 24 miesiące

Wykonawca zapewni następujące parametry SLA usługi:

- Świadczenie usługi w trybie 24/7/365
- Wsparcie architekta usługi: 4h w miesiącu
- Reakcja i odpowiedź na incydent krytyczny/poważny: 1h
- Reakcja na incydent krytyczny wraz z dojazdem do siedziby Zamawiającego: 1h
- Reakcja i odpowiedź na incydent średni: 8h
- Reakcja i odpowiedź na incydent niski: 16h
- Dostarczenie raportu operacyjnego: raz w miesiącu
- Spotkanie dotyczące raportu operacyjnego: raz w miesiącu
- Powołanie i dostęp do sztabu kryzysowego: w momencie eskalacji
- Dostępność do contact center: SLA 99,9
- Utrzymanie systemów, automatyzacja procesów bezpieczeństwa w celu usprawnienia odpowiedzi na wystąpienie incydentów: Reakcja 8h, rozwiązanie problemu lub work-arround: 24h

3. Wymagania dla kolektora danych wraz z oprogramowaniem:

W ramach realizacji zamówienia, Wykonawca dostarczy kolektor danych wraz z oprogramowaniem do inwentaryzacji sieci o następujących parametrach minimalnych.

- Procesor: 8 rdzeniowy
- Pamięć RAM: 4 x 16GB
- Dyski z przeznaczeniem na system operacyjny: 2 x 300GB SAS 10K
- Dyski dodatkowe: 2 x 1,2TB 10K
- Karty sieciowe: 2 x 1Gb

Kolektor danych wraz z oprogramowaniem musi posiadać funkcjonalność filtrowania danych przed wysłaniem danych do SIEM z włączeniem Regex oraz spełniać następujące wymagania dotyczące obsługiwanych danych wejściowych:

- Przyjmuje zdarzenia z Azure Event Hubs
- Przyjmuje zdarzenia Elastic Beats
- Pobiera zdarzenia z interfejsu API Amazon Web Services CloudWatch
- Streamuje zdarzenia z adresu URI _changes CouchDB

- Czyta zdarzenia z Logstash DLQ
- Przyjmuje zdarzenia z Elastic Agent
- Akceptuje zdarzenia z Elastic Serverless Forwarder
- Odczytuje wyniki zapytań z klastra Elasticsearch
- Przechwytuje wynik polecenia shell jako zdarzenie
- Streamuje zdarzenia z plików
- Odczytuje pakiety Ganglia przez UDP
- Odczytuje wiadomości w formacie GELF z Graylog2 jako zdarzenia
- Generuje losowe zdarzenia dziennika w celach testowych
- Odczytuje zdarzenia z webhooka GitHub
- Wyciąga zdarzenia z plików z Google Cloud Storage
- Odbiera zdarzenia z usługi Google Cloud PubSub
- Odczytuje metryki z narzędzia graphite
- Generuje zdarzenia heartbeat w celach testowych
- Przyjmuje zdarzenia za pośrednictwem HTTP lub HTTPS
- Dekoduje wynik interfejsu API HTTP jako zdarzenia
- Odczytuje wiadomości e-mail z serwera IMAP
- Odczytuje zdarzenia z serwera IRC
- Generuje syntetyczne zdarzenia log
- Odczytuje zdarzenia ze standardowego wejścia
- Tworzy zdarzenia na podstawie danych JDBC
- Odczytuje zdarzenia z Jms Broker
- Pobiera metryki z zdalnych aplikacji Java za pomocą JMX
- Odczytuje zdarzenia z Kafka topic
- Przyjmuje zdarzenia poprzez strumień AWS Kinesis
- Odczytuje z wyjścia Logstash innej instancji Logstash
- Odczytuje zdarzenia za pomocą gniazda TCP z Log4j SocketAppender
- Przyjmuje zdarzenia przy użyciu protokołu Lumberjack
- Przechwytuje output command line jako zdarzenie
- Streamuje zdarzenia z long-running command pipe
- Przyjmuje Facts z serwera Puppet
- Pobiera zdarzenia z wymiany RabbitMQ
- Odczytuje zdarzenia z instancji Redis
- Przyjmuje zdarzenia RELP przez gniazdo TCP
- Przechwytuje wynik narzędzi wiersza polecenia jako zdarzenie
- Streamuje zdarzenia z plików w bucket S3
- Odczytuje dzienniki z bucket AWS S3 za pomocą SQS
- Tworzy zdarzenia na podstawie zapytania SOQL Salesforce
- Odpytuje urządzenia sieciowe przy użyciu protokołu SNMP
- Tworzy zdarzenia w oparciu o komunikaty pułapek SNMP
- Tworzy zdarzenia na podstawie wierszy w bazie danych SQLite
- Pobiera zdarzenia z kolejki usługi Simple Queue Service Amazon Web Services
- Odczytuje zdarzenia ze standardowego wejścia
- Tworzy zdarzenia otrzymane z protokołu STOMP
- Odczytuje wiadomości syslog jako zdarzenia
- Odczytuje zdarzenia z gniazda TCP
- Odczytuje zdarzenia z interfejsu API Twitter Streaming
- Odczytuje zdarzenia przez UDP
- Odczytuje zdarzenia przez gniazdo UNIX
- Odczytuje z pamięci współdzielonej dziennika varnishcache
- Odczytuje zdarzenia z websocketu

- Tworzy zdarzenia na podstawie wyników zapytania WMI
- Przyjmuje zdarzenia za pośrednictwem protokołu XMPP/Jabber

4. Wymagania jakie musi spełnić Wykonawca

1) posiada niezbędną wiedzę i doświadczenie,

Opis sposobu dokonywania oceny spełniania tego warunku:
Niniejszy warunek zostanie uznany za spełniony, jeżeli Wykonawca:

- posiada wdrożony i certyfikowany przez akredytowana jednostkę certyfikującą System Zarządzania Bezpieczeństwem Informacji ISO 27001 w zakresie cyberbezpieczeństwa

- posiada ważne świadectwo bezpieczeństwa przemysłowego III stopnia o klauzuli "POUFNE", potwierdzające pełną zdolność Wykonawcy do ochrony informacji niejawnych,

- przedstawi co najmniej 3 dokumenty (lub w przypadku braku możliwości jego przedstawienia oświadczenie Wykonawcy) potwierdzający prawidłowe wykonanie lub wykonywanie usługi odpowiadających swoim zakresem przedmiotowi zamówienia (tj. Świadczenie usług Security Operations Center w podmiocie zatrudniającym min 1000 osób zrealizowanych w ciągu ostatnich 3 lat przed upływem terminu składania ofert)

- przedstawi co najmniej 1 dokument lub w przypadku braku możliwości jego przedstawienia oświadczenie Wykonawcy) potwierdzający prawidłowe wykonanie lub wykonywanie usługi odpowiadającej swoim zakresem przedmiotowi zamówienia (tj. Świadczenie usług Security Operations Center w podmiocie działającym w branży budowlanej.

- przedstawi co najmniej 3 dokumenty lub w przypadku braku możliwości ich przedstawienia oświadczenia Wykonawcy) potwierdzający prawidłowe wykonanie lub wykonywanie usługi Forensic dla organizacji zatrudniającej powyżej 500 osób.

Wyżej wymienione warunki mogą być spełnione łącznie w ramach jednego lub kilku projektów

2) Dysponowanie osobami zdolnymi do wykonania zamówienia

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy wykażą, że dysponują lub będą dysponować min 5 osobowym zespołem, który będzie uczestniczyć w wykonaniu zamówienia, spełniającymi następujące wymagania:

Kierownik projektu
- 1 osoba posiadająca następujące kwalifikacje i doświadczenie zawodowe:

- wykształcenie wyższe
- Certyfikat potwierdzający wiedzę z zakresu zarządzania projektami – Prince2 Practitioner lub równoważny
- Certyfikat CISM, CISA lub CISSP
- posiada co najmniej 3-letnie doświadczenie kierowania projektami w zakresie usług objętych przedmiotem zamówienia

Eksperci

Minimum 5 osób posiadających następujące kwalifikacje i doświadczenie zawodowe:

- wykształcenie wyższe (przy czym co najmniej dwóch członków zespołu ekspertów posiada wykształcenie wyższe techniczne)
- posiada co najmniej 2-letnie doświadczenie w zakresie świadczenia usług odpowiadających przedmiotowi zamówienia.
- Jako zespół posiadają następujące certyfikaty:
  - Co najmniej jeden z członków zespołu posiada certyfikat CISM lub równoważny,
  - Co najmniej jeden z członków zespołu podsiada certyfikat CISA lub równoważny,
  - Co najmniej jeden z członków zespołu posiada certyfikat CEH lub równoważny,
  - Co najmniej jeden z członków zespołu posiada certyfikat CISSP lub równoważny,
  - Co najmniej pięciu członków zespołu posiada certyfikat CompTIa Security + lub równoważny,
  - Co najmniej jeden z członków zespołu posiada certyfikat Fortinet Certified Professional Network Security
  - Co najmniej jeden z członków zespołu posiada certyfikat Blue Team Level 1
  - Co najmniej dwóch członków zespołu posiada certyfikat audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji lub równoważny,

*Jako certyfikat równoważny zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.

3) **znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie Przedmiotu Zamówienia.**

<u>Opis sposobu dokonywania oceny spełniania tego warunku:</u>

Niniejszy warunek zostanie uznany za spełniony, jeżeli wykonawca wykaże, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie świadczonych usług na kwotę 1 mln zł.

Pekabex Bet S.A.
Ul. Szarych Szeregów 27
60-462 Poznań

…….
Data i miejsce

……
Podpis upoważnionego przedstawiciela Oferenta/Wykonawcy