Załącznik nr 1 do Zapytania ofertowego nr IT/AW/143/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiot zamówienia**
   Przedmiotem zamówienia jest zapewnienie ciągłej usługi monitorowania bezpieczeństwa infrastruktury teleinformatycznej i systemów Zamawiającego przy wykorzystaniu systemu analizy i wykrywania zdarzeń typu SIEM Wykonawcy.
2. **Termin realizacji oraz miejsce świadczenia Usługi**
   2.1. Świadczenie usługi zostanie rozpoczęte nie później niż w ciągu 90 dni od zawarcia umowy i będzie trwało przez okres 36 miesięcy od daty zakończenia okresu wdrożenia, o którym mowa w ust 2 pkt. 2.2 poniżej.
   2.2. Czas 90 dni od zawarcia umowy do rozpoczęcia świadczenia usługi traktuje się jako okres wdrożenia, w którym Wykonawca będzie zobowiązany do podjęcia działań zmierzających do zapewnienia współpracy posiadanego przez Wykonawcę systemu SIEM z systemem Zamawiającego, w tym określenia źródeł informacji dla systemu SIEM oraz scenariuszy bezpieczeństwa.
   2.3. Zakończenie okresu wdrożenia potwierdzone będzie przygotowanym przez Wykonawcę protokołem, który powinien zawierać wyszczególnienie monitorowanych elementów systemu Zamawiającego oraz wykaz przygotowanych scenariuszy bezpieczeństwa. Podpisany przez Wykonawcę i Zamawiającego protokół będzie podstawą do wystawienia przez Wykonawcę faktury VAT za wykonanie usługi wdrożenia.
   2.4. Wykonawca oświadcza, że wszystkie obiekty, w których będzie świadczona Usługa (w szczególności miejsce pracy analityków oraz Data Center, w którym zainstalowany jest system SIEM) spełniają wymagania ujęte w Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, przy czym obiekty, które będą miejscem świadczenia usługi, stanowią własność Wykonawcy lub są miejscem zarejestrowania działalności gospodarczej Wykonawcy.
   2.5. Wykonawca umożliwi wizytację jednostki SOC Wykonawcy na wniosek Zamawiającego.
3. **Wymagania dla Usługi**
   3.1. Wykonawca musi posiadać ważny (przechodzący audyty nadzoru) certyfikat ISO/SEC 27001 dla świadczenia usług z zakresu cyberbezpieczeństwa, obejmujący swoim zakresem usługi SOC, wystawiony na Wykonawcę w całym czasie świadczenia Usługi przez podmiot certyfikujący akredytowany przez Polskie Centrum Akredytacji w zakresie normy, której dotyczy certyfikat.
   3.2. Wykonawca musi posiadać kapitał zakładowy przynajmniej na poziomie wartości Usługi.
   3.3. Wykonawca musi posiadać ubezpieczenie OC działalności gospodarczej na kwotę minimum 2 miliony zł.
   3.4. W ramach usługi Wykonawca zapewni monitorowanie bezpieczeństwa infrastruktury teleinformatycznej, systemów i działań użytkowników Zamawiającego w trybie 24/7/365.

3.5. Wykonawca uruchomi system SIEM na swoich zasobach. System SIEM wykorzystywany w ramach świadczenia Usługi musi mieć wsparcie producenta przez cały okres świadczenia Usługi.

3.6. System SIEM Wykonawcy powinien umożliwiać uruchomienie usługi UBA (User Behavior Analytics) dla 500 użytkowników.

3.7. Wykonawca zapewni obsługę minimum 500 EPS (events per second).

3.8. Wykonawca zapewni obsługę co najmniej 50 źródeł logów, w tym logów serwerów i urządzeń sieciowych.

3.9. Wykonawca zapewni komunikację z systemami Zamawiającego za pomocą łącza w technologii MPLS (2 porty 50/50 Mbps).

3.10. Wykonawca zapewni klasyfikację wykrytych incydentów oraz obsługę do 10 incydentów krytycznych w ciągu każdych 24 godzin świadczenia Usługi w czasie określonym w poniższym SLA, pozostałe w trybie best effort.

Poziom incydentu i czas reakcji (SLA):

Poziom incydentu		
Krytyczny	**Średni**	**Niski**
Czas reakcji		
60 minut	**240 minut**	**240 minut**

3.11. Wykonawca gwarantuje informowanie Zamawiającego o wykrytych incydentach krytycznych w ciągu 1 godziny oraz o wykrytych innych incydentach w ciągu 4 godzin od momentu ich wykrycia oraz o podjętych działaniach za pośrednictwem ustalonych w umowie kanałów komunikacji (telefon, e-mail).

3.12. Wykonawca gwarantuje składowanie logów otrzymanych od Zamawiającego oraz dostęp do nich w ramach zasobów Wykonawcy przez czas nie krótszy niż 6 miesięcy w sposób umożliwiający ich wykorzystanie w celu dokonania analizy powłamaniowej lub przekazanie organom prowadzącym postępowanie związane z wystąpieniem incydentu.

3.13. Wykonawca zapewnia raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa do właściwego CSIRT w ciągu 24 godzin od momentu ich wykrycia.

3.14. Wykonawca zapewnia przekazywanie Zamawiającemu miesięcznych raportów dotyczących wykrytych incydentów i związanych z nimi podjętych działań.

4. Linie wsparcia

4.1. Wykonawca gwarantuje w ramach opłaty za świadczenie Usługi dostęp do Pierwszej i Drugiej Linii Wsparcia, oraz w ramach dodatkowych odrębnych zamówień dostęp do Trzeciej Linii Wsparcia, obejmujących:

4.1.1. Pierwsza Linia Wsparcia (L1)

4.1.1.1. Monitoring systemów i usług Zamawiającego w trybie 24/7/365 w celu wykrywania zdarzeń naruszenia cyberbezpieczeństwa (incydentów).

4.1.1.2. Analiza wykrywanych incydentów i klasyfikacja incydentów. Klasyfikacja (poziomy) incydentów uzgodnione będą w ramach wdrożenia i opracowania scenariuszy monitorowania i reagowania.

4.1.1.3. Reakcja na wykryte incydenty zgodnie z przygotowanymi scenariuszami i warunkami określonymi w SLA (zarządzanie incydentami).
4.1.1.4. Odbieranie zgłoszeń telefonicznych i mailowych od Zamawiającego.
4.1.1.5. Skanowanie podatności systemów i usług Zamawiającego.
4.1.1.6. Przekazywanie obsługi incydentów do Drugiej Linii Wsparcia zgodnie z przygotowanymi scenariuszami.
4.1.1.7. Przekazywanie informacji o incydentach do wyznaczonych pracowników Zamawiającego z użyciem uzgodnionych kanałów informacji: telefon, e-mail.
4.1.1.8. Przekazywanie Zamawiającemu uzgodnionych miesięcznych raportów dotyczących wykrytych incydentów.
4.1.1.9. Raportowanie incydentów poważnych w rozumieniu Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560) do właściwego CSIRT w ciągu 24 godz. Od momentu wykrycia incydentu oraz udzielanie odpowiedzi na ewentualne zapytania CSIRT.

4.1.2. Druga Linia Wsparcia (L2)
4.1.2.1. Obsługa incydentów przekazanych przez L1, w szczególności incydentów krytycznych.
4.1.2.2. Troubleshooting.
4.1.2.3. Strojenie systemów.
4.1.2.4. Tworzenie scenariuszy dla L1.
4.1.2.5. Zaawansowane skanowanie podatności systemów i usług Zamawiającego.
4.1.2.6. Kontakt z dostawcą w zakresie zgłaszania znalezionych błędów i zakładania ticketów.

4.1.3. Trzecia Linia Wsparcia (L3):
4.1.3.1. Analiza złożonych incydentów, w tym wszelkie analizy forensic, analizy powłamaniowe, analizy malware, itp.
4.1.3.2. Zaawansowane testy penetracyjne.
4.1.3.3. Pisanie złożonych polityk bezpieczeństwa.
4.1.3.4. Zabezpieczenie i przechowanie nośników danych oraz innych dowodów w związku z analizą incydentów, o której mowa w punkcie 4.1.3.1 powyżej, do momentu zakończenia działań obsługi incydentu przez L3 oraz inne organy uprawnione do przeprowadzania działań w zakresie incydentu i jego skutków (Policja, Prokuratura, itp.) lub do chwili ich przekazania jako dowód w sprawie uprawnionym organom prowadzącym takie działania.

4.2. Zamawiający dopuszcza inny podział zadań pomiędzy Pierwszą (L1) i Drugą (L2) linią wsparcia z zachowaniem pełnego ich zakresu i czasów reakcji (SLA).

5. Wdrożenie

W ramach wdrożenia, obejmującego okres 90 dni od daty podpisania umowy Wykonawca:

5.1. Przeprowadzi analizę źródeł logów oraz określi sposób ich parsowania w SIEM;
5.2. Przeprowadzi analizę potrzebnych i dostępnych informacji do strojenia reguł i systemu SIEM (adresacje, strefy DMZ, serwery AD, serwery DNS, itp.).
5.3. Przedstawi propozycję i uzgodni z Zamawiającym minimum 10 scenariuszy reagowania na wykryte incydenty.

5.4. Dostarczy opis sposobu obsługi każdego ze scenariuszy.
5.5. Uruchomi przesyłanie zdarzeń (logów) do SIEM. Przygotuje sposób podłączenia źródła zdarzeń i przekaże go do Zamawiającego w celu podłączenia pozostałych zasobów tego samego typu.
5.6. Przeprowadzi wstępne strojenie i implementację reguł a rezultatem tych prac będzie działające parsowanie logów oraz zaimplementowane uzgodnione reguły.
5.7. Zbuduje raporty wg, wytycznych Zamawiającego, generowanie automatycznie i wysyłane mailowo do wskazanych osób.
5.8. Przeprowadzi strojenie systemu SIEM w celu zmniejszenia ilości fałszywych alarmów.
5.9. Przekaże Zamawiającemu informacje o sposobie dostępu do składowanych logów.
5.10. Przygotuje protokół zakończenia okresu wdrożenia, zawierający wykaz źródeł logów z systemu Zamawiającego oraz wykaz przygotowanych scenariuszy reagowania na wykryte incydenty. Podpisany przez obie Strony (Wykonawcę i Zamawiającego) protokół będzie podstawą do wystawienia faktury za wdrożenie usługi.

Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o.
ul. B. Prusa 75-79, 50-316 Wrocław
+48 71 308 50 70, fax: +48 71 325 08 02
biuro@mpk.wroc.pl, www.mpk.wroc.pl

NIP: 896-10-04-279, REGON: 930879788, KRS: 0000027173
Sąd Rejonowy dla Wrocławia-Fabrycznej
VI Wydział Gospodarczy Krajowego Rejestru Sądowego
Kapitał zakładowy: 318 184 875 PLN