PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

NR BST-P6/076/22/2021

Warszawa, dnia 26.08.2021 r.

Z A P Y T A N I E O I N F O R M A C J Ę

Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej dotyczącej dostarczenia, wdrożenia, utrzymania i rozwoju systemu Security Information and Event Management oraz dostarczenia usługi Security Operations Center.

1. **Przedmiotem zapytania jest dostarczenie, wdrożenie, utrzymanie i rozwój systemu Security Information and Event Management oraz dostarczenie usługi Security Operations Center, w tym:**
   1.1. dostarczenie systemu monitorowania i korelacji zdarzeń bezpieczeństwa (Security Information and Event Management, SIEM, dalej System);
   1.2. usługa wdrożenia i integracji Systemu;
   1.3. usługa szkoleniowa w zakresie obsługi dostarczonego Systemu;
   1.4. usługa Security Operations Center;
   1.5. usługa utrzymania i rozwoju Systemu.
2. **Zamawiający prosi o wycenę dla dwóch poniżej opisanych wariantów:**
   2.1. wariant 1 polegający na dostarczeniu oprogramowania SIEM hostowanego w infrastrukturze producenta, wdrożenie oraz integrację systemów Zamawiającego do usługi SIEM, świadczenie usługi Security Operations Center oraz świadczenie usługi utrzymania i rozwoju Systemu SIEM;
   2.2. wariant 2 polegający na dostarczeniu licencji na oprogramowanie SIEM hostowane w infrastrukturze Zamawiającego, integrację systemów Zamawiającego do usługi SIEM, świadczenie usługi Security Operations Center oraz świadczenie usługi utrzymania i rozwoju Systemu SIEM.

3. **Zamawiający wymaga, aby rozliczenie przedmiotu zamówienia realizowane było w miesięcznej opłacie abonamentowej.**

4. **Wymagania ogólne dla oprogramowania SIEM**
   4.1. System monitorowania i korelacji zdarzeń bezpieczeństwa (Security Information and Event Management, SIEM) jest to system teleinformatyczny zapewniający gromadzenie, normalizację i ocenę danych określających pracę innych systemów. System z wykorzystaniem silnika analitycznego zapewnia nadto korelację zagregowanych zdarzeń przez co umożliwia detekcję i reagowanie incydenty bezpieczeństwa w czasie rzeczywistym.
   4.2. Producent Systemu musi być sklasyfikowany w kwadracie liderów raportu z dnia 29 czerwca 2021 roku pn. Gartner Magic Quadrant for Security Information and Event Management.
   4.3. Zapytanie zakłada dostarczenie Systemu oraz Usług w jednym z dwóch wariantów:

a) wariant nr 1: świadczenie Usług w oparciu o System lokowany w infrastrukturze producenta Systemu;
b) wariant nr 2: świadczenie Usług w oparciu o System lokowany w infrastrukturze teleinformatycznej Zamawiającego.

4.4. Infrastruktura teleinformatyczna, na której zostanie uruchomiony System zostanie zapewniona przez Zamawiającego w zakresie:
a) dla wariantu nr 1: do pięciu maszyn wirtualnych lokowanych w trzech częściach sieci Zamawiającego, których celem będzie zapewnienie agregacji danych źródłowych oraz przesłanie danych do Systemu; maszyny zostaną dostarczone w minimalnej konfiguracji: CPU: 4, RAM: 8GB, HDD: 1TB.
b) dla wariantu nr 2: jednej maszynie wirtualnej pełniącej rolę głównego serwera Systemu w minimalnej konfiguracji: CPU: 8, RAM: 32GB, HDD: 10TB oraz do pięciu maszyn wirtualnych lokowanych w trzech częściach sieci Zamawiającego, których celem będzie zapewnienie agregacji danych źródłowych oraz przesłanie danych do Systemu; maszyny wirtualne zostaną dostarczone w minimalnej konfiguracji: CPU: 4, RAM: 8GB, HDD: 1TB.

4.5. Wykonawca dostarczy System oraz wszelkie jego komponenty w najnowszej wspieranej przez producenta wersji.

4.6. Wykonawca zapewni, że System oraz wszelkie jego komponenty nie zostało zakwalifikowane przez producenta Systemu do wycofania wsparcia lub sprzedaży.

5. Wymagania wydajnościowe

5.1. estymacja dla sumarycznego dobowego wolumenu danych: 100 GB.

6. Wymagania funkcjonalne dla Systemu:

6.1. System musi składać się z komponentów zapewniających funkcję: pobierania, normalizacji danych, przechowywania, wyszukiwania i zarządzania bazą zebranych zdarzeń, warstwy analitycznej i interfejsu użytkownika;

6.2. Architektura rozwiązania musi umożliwiać rozdzielenie na osobne serwery funkcji:
a) pobierania danych,
b) przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
c) warstwy analitycznej i interfejsu użytkownika.

6.3. System musi umożliwiać pełną skalowalność infrastrukturalną oraz dodawanie kolejnych komponentów Systemu niezależnie od licencji;

6.4. System musi być zasilany w aktualizowane przez producenta reguły korelacyjne, którymi można zarządzać poprzez ich dodawanie, usuwanie, zawieszenie oraz edycję;

6.5. System musi umożliwiać wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX) lub gotowych wzorców wyboru np.: adres IP źródłowy/docelowy, port, protokół.

6.6. System musi zapewnić kontrolę dostępu na poziomie Role Based Access Control w granulacji określonej na poziomie wartości poszczególnych, identyfikowanych danych;

6.7. System musi posiadać graficzny interfejs użytkownika dostępny przez przeglądarkę internetową, w którym dostępne będą wszystkie funkcjonalności niezbędne do zarządzania;

6.8. System musi umożliwiać przeglądanie (w jednej konsoli systemu) logów pobieranych/dostarczanych do Systemu w celu uniknięcia konieczności logowania się do

każdego monitorowanego systemu osobno, w celu sprawdzenia statusu połączenia (przepuszczone, zablokowane). Filtrowanie w czasie rzeczywistym musi dopuszczać wyszukiwanie informacji za pomocą wyrażeń regularnych (REGEX) lub gotowych wzorców np: adres IP źródłowy/docelowy, port, protokół;

6.9. System musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem tabel, listy zdarzeń, wykresów, map oraz map kolorowanych;

6.10. System musi posiadać możliwość wyświetlania dashbordów w trybach dziennym i nocnym;

6.11. System musi posiadać zestaw predefiniowanych raportów oraz posiadać możliwość tworzenia raportów na podstawie wyników wyszukiwania;

6.12. System musi umożliwiać budowanie dedykowanych widoków oraz dashboard‘ów, które mogą zawierać konfigurowalne elementy prezentacji danych (wykresy, listy, tabele, statystyki, etc.);

6.13. System musi umożliwiać konfigurację silnika normalizacji danych, zwłaszcza poprzez możliwość określenia prezentowanych informacji, dodawania nowych, specyficznych pozycji informacyjnych dla określonego typu danych źródłowych, wzbogacenie prezentowanych informacji o dane analityczne (np. geolokalizacja adresów IP) oraz dodawania nowych kategorii zdarzeń;

6.14. System musi umożliwiać korelację zdarzeń w celu identyfikacji naruszeń bezpieczeństwa;

6.15. System musi umożliwiać normalizację danych źródłowych, w tym prezentować istotne pozycje informacyjne tj. data i czas zdarzenia, adres źródłowy, adres docelowy, port źródłowy, port docelowy, użytkownik;

6.16. System nie może blokować / odrzucać logów / danych w przypadku przekroczenia dziennego limitu danych (w odniesieniu do wykorzystywanych w danym momencie licencji);

6.17. W przypadku problemów wydajnościowych któregokolwiek komponentu zaoferowanego rozwiązania musi istnieć możliwość jego rozbudowy (np. zwielokrotnienia ilości węzłów) bez konieczności zakupu dodatkowych modułów czy licencji;

6.18. Rozbudowa rozwiązania w przypadku zwiększającej się ilości gromadzonych dziennie danych nie może wiązać się z koniecznością wykupienia dodatkowych licencji, poza tylko i wyłącznie tymi związanymi z dziennym limitem gromadzonych logów / danych z systemów źródłowych

6.19. System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę dla co najmniej 10 TB.

6.20. System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line.

6.21. System musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię.

6.22. Proces odpowiedzialny za prasowania logów musi analizowaćˊ poszczególne logi/dane, i wyszukiwaćˊ w nich istotne informacje o logowanym zdarzeniu, między innymi: data i czas zdarzenia, nazwa użytkownika, nazwa systemu logującego, nazwa/adres IP systemu, źródła logów, rodzaj zdarzenia (np. zalogowanie/wylogowanie/ zablokowanie użytkownika, przepuszczenie/zablokowanie ruchu sieciowego, wykrycie szkodliwego kodu itp.);

6.23. System musi umożliwiać zaprojektowanie i wdrożenie przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej z następujących źródeł:
   a) Systemy bezpieczeństwa,
   b) Aplikacyjnych zapór sieciowych WAF: F5 Networks, Imperva, Fortinet,
   c) Urządzeń sieciowych Cisco,
   d) Systemów operacyjnych Microsoft Windows,
   e) Systemów operacyjnych Linux / Unix,
   f) Usług sieciowych tj.: DHCP, DNS,
   g) Bazy danych tj.: Oracle, Microsoft SQL Server, MySQL, Postgres, MariaDB,
   h) Systemów wirtualizacyjnych tj.: Vmware vSphere, Microsoft Hyper-V,
   i) Logów Windows Events (Logi Application, Security, System I inne),
   j) Ruchu sieciowego poprzez Netflow,
   k) Ruchu sieciowego poprzez SPAN port.

6.24. System musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych);

6.25. System powinien pozwalać na analizę niestandardowych logów wygenerowanych przez aplikacje własne, utworzone przez pracowników lub na zamówienie klienta.

6.26. System musi umożliwiać pobieranie logów / danych zapisanych w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów:
   a) Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog);
   b) Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay;
   c) Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog;
   d) Wykonywanie przez zaoferowane rozwiązania zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC.
   e) Windows Management Infrastructure (WMI).

7. Wymagania licencyjne dla oprogramowania SIEM

7.1. Licencja na zaoferowane rozwiązanie nie może posiadać ograniczeń w postaci ilości urządzeń, z których pobierane są logi, również ilości zdarzeń na sekundę (EPS);

7.2. Licencja na zaoferowane rozwiązanie nie może ograniczać liczby elementów gromadzonych oraz analizujących logi;

7.3. Licencja musi dopuszczać dowolne kształtowanie architektury systemu, w szczególności stosowanie dowolnej liczby komponentów Systemu.

8. Dodatkowe wymagania dla Systemu lokowanego w infrastrukturze producenta Systemu

8.1. System musi umożliwić łatwą migrację z infrastruktury producenta Systemu do infrastruktury Zamawiającego po zakończeniu realizacji przedmiotu Zamówienia;

8.2. System musi być lokowany w infrastrukturze zapewniającej szybki dostęp do danych na poziomie poprzez storage obiektowy zgodny z S3.

8.3. Dane musza być przetwarzane na terenie Europejskiego Obszaru Gospodarczego.

9. Wymagania dla usługi Security Operations Center

9.1. Usługa świadczona dla systemów teleinformatycznych Zamawiającego.

9.2. Usługa zakłada:

a) agregację, korelację oraz analizowanie zdarzeń pochodzących z systemów Zamawiającego w rozwiązaniu Security Information and Event Management,

b) monitorowanie zagrożeń i analizę ruchu sieciowego.

c) Podstawowa obsługa incydentów bezpieczeństwa zgodnie z wewnętrznymi politykami oraz procedurami Zamawiającego.

d) Utrzymanie oraz rozbudowanie procedur reakcji na incydent.

e) Zaawansowana obsługa incydentów bezpieczeństwa w zakresie bezpieczeństwa teleinformatycznego, organizacyjnego i prawnego przez wykfalifikowany zespół wsparcia.

f) Wsparcie Zamawiającego we wdrożeniu rekomendacji po wystąpieniu incydentu.

g) Pełnienie roli odpowiedzialnej za kontakt z odpowiednim CSIRTem.

9.3. Usługa realizowana zdalnie w warunkach spełniających wymagania określone 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 cyberbezpieczeństwa.

9.4. Monitorowanie i reakcja na incydent bezpieczeństwa zakłada:

9.5. monitorowanie systemów teleinformatycznych oraz sieci Zamawiającego;

9.6. agregację, korelację oraz analizowanie zdarzeń, które zachodzą w systemach oraz sieci Zamawiającego;

9.7. podstawową obsługę incydentów bezpieczeństwa zgodnie z wewnętrznymi politykami oraz procedurami Zamawiającego;

9.8. zaawansowaną obsługę incydentu w zakresie bezpieczeństwa teleinformatycznego, organizacyjnego i prawnego przez wykfalifikowany zespół wsparcia;

9.9. utrzymanie oraz rozbudowanie procedur reakcji na incydent;

9.10. wsparcie Zamawiającego w wdrożeniu rekomendacji po wystąpieniu incydentu;

9.11. Zarządzanie podatnościami zakłada:

9.12. cykliczną identyfikację oraz analizę podatności dla systemów lokowanych w sieci Klienta;

9.13. monitoring zewnętrzny publicznej klasy adresowej w zakresie zmian eksponowanych usług;

9.14. opracowanie rekomendacji dla zidentyfikowany podatności;

9.15. dostarczenie rekomendacji dla zidentyfikowanych podatności w formie dostępu do systemu teleinformatycznego Wykonawcy;

9.16. monitorowanie oraz wsparcie w przypadku braku możliwości wdrożenia rekomendacji;

9.17. Wsparcie w zakresie architektury bezpieczeństwa zakłada:

9.18. nadzór nad rozwojem utrzymywanego modelu bezpieczeństwa teleinformatycznego;

9.19. opracowanie cyklicznych rekomendacji dot. modelu bezpieczeństwa na podstawie informacji i ryzyk pozyskanych w ramach obsługi incydentu bezpieczeństwa;

9.20. wsparcie w opracowaniu wymagań bezpieczeństwa dla wytwarzanego oraz wdrażanego oprogramowania;

9.21. wsparcie w interpretacji wymagań prawnych odnoszących się do bezpieczeństwa teleinformatycznego w zakresie kompletności utrzymywanego modelu bezpieczeństwa.

10. Wymagania dla usługi utrzymania i rozwoju Systemu SIEM

10.1. utrzymanie, optymalizacja działania oraz zarządzanie systemem SIEM;

10.2. rozwój sprawności detekcji zdarzeń bezpieczeństwa;

10.3. integrację nowych źródeł danych;

10.4. budowanie i aktualizację reguł korelacyjnych;

10.5. utrzymanie dokumentacji technicznej rozwiązania.

11. Informacja cenowa

Formularz odpowiedzi do zapytania:

Lp.	Wariant	Pozycja wariantu	1 rok (opłata m-c)	2 lata (opłata m-c)	3 lata (opłata m-c)
1.	Wariant 1	Usługa SOC as a Service			
2.	Wariant 2	Wdrożenie i utrzymanie SIEM			
3.		Świadczenie usługi Security Operations Center			
4.		Świadczenie usługi utrzymania i rozwoju Systemu SIEM			

12. Terminy składania pytań oraz udzielenie informacji:

- Termin składania informacji upływa w dniu **03.09.2021 do godziny 14:00**
- (ewentualne pytania prosimy kierować do dnia **31.08.2021 r. do godziny 14:00**).
- Odpowiedź proszę przesłać w formie e-mail na adres: it@intercity.pl

„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.