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

Szanowni Państwo,

Poniżej znajdują się odpowiedzi na zadane pytania:

1. Dzień dobry, prośba o informacje z jakiej platformy SIEM Państwo korzystają (producent rozwiązania)?

Odpowiedź: SPLUNK.

2. Witam, w związku z chęcią udzielenia odpowiedzi w zapytaniu prowadzonym przez Zamawiającego, zwracamy się z prośbą o podanie nazwy producenta posiadanego przez Zamawiającego rozwiązania klasy SIEM i PAM.

Odpowiedź: SPLUNK oraz FUDO.

3. Zwracam się z prośbą o wyjaśnienie jak należy wyliczyć łączną cenę (SUMY w Lp. od 8 do 12)? By uniknąć wątpliwości przy porównywaniu ofert, prosimy o dopisanie które pozycje Lp. od 1 do 7 składają się na poszczególne SUMY w Lp. 8 do 12.

Odpowiedź: Zamawiający informuje, iż SUMY wskazane w wierszach 8-12 tabeli formularza wyceny należy wyliczać w następujący sposób:

- **SUMA – zakres podstawowy (WARIANT 1) – suma wierszy 1, 3, 5**
- **SUMA – zakres podstawowy (WARIANT 2) - suma wierszy 2, 3, 5**
- **SUMA – prawo opcji - suma wierszy 4, 6, 7**
- **SUMA – zakres podstawowy + prawo opcji (WARIANT 1) - suma wierszy 8 i 10**
- **SUMA – zakres podstawowy + prawo opcji (WARIANT 2) - suma wierszy 9 i 10**

4. Czy w momencie rozpoczęcia wdrożenia Usług SOC/NOC Zamawiający zakłada, że do wdrożonego wcześniej systemu SIEM będą podpięte już źródła danych ? Jeżeli tak to ile ?

Odpowiedź: Do 20 źródeł.

5. Jaką ilość źródeł danych Zamawiający przewiduje do zainstalowania/skonfigurowania w ramach wdrożenia i świadczenia Usług SOC/NOC ?

Odpowiedź: Do 20 źródeł.

6. Czy Zamawiający zakłada, że świadczenie Usługi NOC będzie odbywać się przy użyciu systemu SIEM Zamawiającego ?

Odpowiedź: Tak.

7. Prosimy o podanie producenta systemu SIEM oraz PAM.

Odpowiedź: Splunk, fudo.

8. Czy Zamawiający zakłada użycie systemu ticket'owego jako platformy komunikacyjnej pomiędzy personelem PKP Intercity i Wykonawcy ? Jeżeli tak czy można założyć korzystanie z systemu ITSM Wykonawcy ?

Odpowiedź: Tak.

9. Prosimy o potwierdzenie, że w ramach raportowania Usług Zamawiający oczekuje obligatoryjnie raportów miesięcznych oraz raportów z incydentów Krytycznych i Wysokich, natomiast raporty tygodniowe/dzienne/godzinne będą oczekiwane na żądanie.

Odpowiedź: Tak.

10. Prosimy o potwierdzenie, że Zamawiający oczekuje wdrożenia 10 scenariuszy użycia w fazie wdrożenia Usługi SOC, pozostałe 40 scenariuszy będzie wdrożonych w trakcie świadczenia Usługi.

Odpowiedź: Liczba scenariuszy może być większa, wszystko zależeć będzie od ilości podłączonych źródeł.

11. Dla jakich kategorii danych Zamawiający oczekuje badania trendów: zagrożenia, incydenty, inne - jakie ?

Odpowiedź: Wycieki danych ze Spółki np. loginy, hasła.

12. Na czy ma polegać "Weryfikacja i przygotowanie planów działania" - czy to wymaganie odnosi się do reakcji na incydenty, modyfikacje systemu SIEM/Usługi SOC ? - prosimy o wyjaśnienie oczekiwań.

Odpowiedź: Tak, odnosi się do reakcji na incydenty.

13. Prosimy o potwierdzenie wymagań dotyczących Linii L2 - Zamawiający oczekuje prac wykonywanych przez L2 w określonych godzinach, ale niezależnie od tego wymaga dostępności linii L2 w trybie 24x7.

Odpowiedź: Zgodnie z pkt. 4.2. ppkt (1):

„Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie od godziny 16:00 do 8:00 rano następnego dnia w dni powszednie, w soboty, niedziele i święta dostępność 24h na dobę, zgodnie z określonymi warunkami SLA”

14. Prosimy o określenie wymagania Archiwizacja zdarzeń systemowych i połączeń - czy Zamawiający wymaga archiwizacji danych z systemu SIEM czy chodzi o inny zakres działań ?

Odpowiedź: Zamawiający wymaga archiwizacji danych z systemu SIEM i innych systemów monitorujących.

15. W jakiej formie Zamawiający na etapie postępowania będzie wymagał od Oferenta potwierdzenia, że współpracuje z CSIRT'ami ?

Odpowiedź: W formie deklaracji.

16. Punkt 2.1 Czy Zamawiający posiada wdrożony system SIEM, jeśli tak to czy system kolekcjonuje już logi z systemów Zamawiającego i czy wdrożone są już jakieś scenariusze bezpieczeństwa?

Odpowiedź: Zamawiający nie posiada jeszcze wdrożonego systemu SIEM.

17. Punkt 3.2 Prosimy o podanie listy systemów podlegających integracji. Prosimy o doprecyzowanie zapisu ".....uzgodnienie zasad współpracy...."

    Odpowiedź: Lista systemów zostanie podana na etapie postępowania, Zamawiający rozumie zapis jako uzgodnienie wszelkich kwestii w zakresie wdrożenia usługi, konfiguracji systemu.

    Punkt 4.1 Prosimy o wyjaśnienie dlaczego zakres I linii opisany w tym punkcie jest sprzeczny z opisem priorytetyzacji i zakresu I linii w pkt 7.1.

    Odpowiedź: Zamawiający prosi o doprecyzowanie pytania.

18. Punkt 4.4.1 W pkt. nie ma określonych warunków i terminów na wdrożenie scenariuszy. Prosimy o doprecyzowanie.

    Odpowiedź: Kwestie związane z wdrożeniem scenariuszy zostaną uzgodnione po podpisaniu umowy.

19. Punkt 4.4.1.1.Prosimy o uszczegółowienia zapisu "....Kilku źródeł zdarzeń .." Czy Zmawiający może podać maksymalną ilość źródeł w ramach jednego systemu.

    Czy eskalacja ma być kierowana do zespołu Zamawiającego?, jeśli tak to czy w przypadku scenariuszy Krytycznych, wysoki i średni zespół po stronie Zmawiającego jest dostępny również w trybie 24h?

    Odpowiedź: Zamawiający wymaga aby scenariusz mógł zakładać analizę logów z kilku źródeł danych np. ruter, firewall, oprogramowanie antywirusowe. Zespół Zamawiającego jest dostępny 24 h.

20. Punkt 4.5.1 Prosimy o uszczegółowienia przez Zamawiającego zapisu, czy wymagane jest posiadanie kompetencji w SOC w zakresie administracji systemów?

    Odpowiedź: Pkt. 4.5.1. dotyczy raportu poincydentalnego.

21. Punkt 7.2 Prosimy o uszczegółowienie przez Zamawiającego gdzie kończy się proces reakcji – I Linia a gdzie zaczyna się proces reakcji na incydent realizowany przez Zamawiającego?

    Odpowiedź: Sposób zarządzania poszczególnymi incydentami na linii Wykonawca – Zamawiający zostanie doprecyzowany w poszczególnych scenariuszach reakcji i procedurach operacyjnych (Playbookach).

22. Punkt 7.2 Krytyczny

    Prosimy o wyjaśnienie opisu

    • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min);

Odpowiedź: Wykrywanie anomalii w logach konsoli zarządzającej programów antywirusowych jeżeli wystąpi duża ilość pojedynczych incydentów w podanym okresie czasu (infekcji malware, ransomware, inne) gdzie transfer sieciowy przekroczy np 1KB/ min

23. Prosimy o określenie ile aplikacji ma być objęte zakresem wdrożenia

    • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych;

Odpowiedź: Zamawiający wymaga podłączenia do 10 źródeł, chyba ze będzie podłączona większa liczba systemów.

24. Prosimy o wyjaśnienia kim jest wiarygodny sygnalista.

    Odpowiedź: Firmy zajmujące się cyberbezpieczeństwem świadczące usługi SOC, NOC, SOAR dla podmiotów z infrastruktury krytycznej otrzymują od CESIRTów krajowych lub międzynarodowych alerty bezpieczeństwa o aktualnych lub potencjalnych zagrożeniach, które mogą wystąpić na danym terenie lub w infrastrukturze usługobiorcy - wystąpienie danego zagrożenia stanowi incydent krytyczny.

25. Prosimy o wyjaśnienie jaką rolę ma pełnić SOC w nawiązaniu do zapisów:

    • Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające"

    Odpowiedź: Alerty o wykryciu anomalii - nowego złośliwego oprogramowania luki Zero-day exploit - ataku, który pojawia się przed publikacją poprawki przez producenta. Pracownicy I linii po stwierdzeniu Incydentu krytycznego mają podjąć działania z zachowaniem SLA, w tym zgodnie z ustalonymi procedurami operacyjnymi (Playbookami).

26. Jaki czas przewiduje Zamawiający na obsługę naruszenia w ramach I-szej oraz II linni wsparcia?

Odpowiedź: Czasy SLA zostały wskazane w zapytaniu RFI.

27. Czy Zamawiający przedstawi przykład "Scenariusz użycia systemu bezpieczeństwa" by lepiej poznać wymagania?

    Odpowiedź: Zamawiający wspólnie z Wykonawcą stworzy scenariusze.

28. Czy Zamawiający przedstawi przykład "Scenariusza reakcji" dla I i II-ej linii wsparcia?

    Odpowiedź: J.W.

29. Jaki czas Zamawiający przewiduje na akceptacje otrzymanego scenariusza użycia systemu bezpieczeństwa oraz scenariusza reakcji?

    Odpowiedź: Wszelkie tego typu zagadnienia zostaną omówione po podpisaniu umowy.

30. Czy Zamawiający oczekuje przedstawienia scenariusza użycia systemu bezpieczeństwa oraz scenariusza reakcji łącznie czy też dopuszcza sytuacje w której najpierw następuje akceptacja scenariusza użycia systemu bezpieczeństwa, a następnie przedstawiany jest scenariusz reakcji?

    Odpowiedź: J.W.

31. Czy system SIEM Zamawiającego jest administrowanym wyłącznie własnymi zasobami czy też dodatkowo poprzez wsparcie zewnętrzne?

    Odpowiedź: Zamawiający wymaga od Wykonawcy administrowania systemem SIEM.

32. Z jakim wyprzedzeniem (w dniach) Wykonawca otrzyma informacje o potrzebie utworzenia raportu na żądanie (dobowy, tygodniowy)?

    Odpowiedź: Wszelkie tego typu zagadnienia zostaną omówione po podpisaniu umowy.

33. W jakim czasie powinien być przygotowany raport na żądanie (dobowy, tygodniowy)?

    Odpowiedź: Wszelkie tego typu zagadnienia zostaną omówione po podpisaniu umowy.

34. Dot. 3.4 Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia udostępnione przez Zamawiającego – System SIEM.- Po jakim czasie Wykonawca otrzyma dostęp do narzędzi Zamawiającego?

    Odpowiedź: Wykonawca otrzyma dostęp do systemu niezwłocznie po podpisaniu umowy.

35. Dot. 3.4 Dostęp do narzędzi powinien zostać zrealizowany za pomocą szyfrowanego połączenia oraz systemu klasy PAM nagrywającego sesje osoby łączącej się. Parametry dostępu zostaną ustalone po podpisaniu umowy.- Czy Zamawiający udostępniał swoje zasoby w ten sposób?

    Odpowiedź: Tak.

36. Dot. 4.1.1.(10) Scenariusz użycia systemu bezpieczeństwa - Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od

przekazania informacji od Koordynatora Zamawiającego do Koordynatora Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym. Czy Zamawiający może podać przykład informacji jaka zostanie przekazana do Wykonawcy i będzie dot. przygotowania i wdrożenia scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych?

Odpowiedź: Wszelkie tego typu zagadnienia zostaną omówione po podpisaniu umowy.

37. Dot. 9.4.c) Liczbę wniosków generowanych bezpośrednio przez użytkowników w trybie mail/telefon wraz z rodzajem zgłoszenia, statusem. - Co oznacza liczba wniosków generowanych przez użytkowników w trybie mail/telefon?

    Odpowiedź: Liczba alertów zgłoszonych przez pracowników Zamawiającego.

38. Czy Zamawiający jest w stanie określić całkowitą ilość EPS/FPS z monitorowanych systemów?

    Odpowiedź: do 100 GB logów dziennie.

39. Aby odpowiednio wyskalować platformę SIEM prosimy Zamawiającego o listę monitorowanych źródeł z rozbiciem na rodzaj usługi lub urządzenie, liczbę urządzeń / lodów będących źródłami logów które będą przedmiotem zamówienia.

    Odpowiedź: Kwestie związane z listą usług urządzeń zostaną przekazane po podpisaniu umowy.

40. W odniesieniu do punktu numer 6.1 o treści „W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, w tym z wykorzystaniem technik inżynierii odwrotnej (ang. reverse engineering), w wymiarze zgodnym z ofertą, jednak nie mniejszym niż 10 przypadków i nie większym niż 15 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy" przez pojęcie „analizy złośliwego oprogramowania" [..] w wymiarze nie mniejszym niż 10 przypadków rozumie rozumie ilość zleceń czy ilość dniówek?

    Odpowiedź: Zamawiający rozumie jako ilość zleceń, minimum 10, maksymalnie 15.

41. W odniesieniu do punktu numer „7 Ogólne warunki SLA" Zamawiający definiuje ilość godzin na 10 - jak rozumieć ten zapis w zestawieniu z punktem 6.1 i ilością zleceń od 10 do 15 w skali roku?

    Odpowiedź: Ilość godzin 10 to są wskazane przez Zamawiającego wymogi w zakresie czasu pracy dla III linii wsparcia.

42. W odniesieniu do punktu numer 7 - ogólne warunki SLA - Prosimy o zmianę definicji SLA „Podjęcie" bez definicji priorytetu - Podejmując zdarzenie operator SOC nie jest w stanie określić jeszcze priorytety Incydentu. Na tym etapie mówimy o zdarzeniu i podejmując

zaczynamy od procedury Triage która dopiero określi, czy w ogóle mamy do czynienia z Incydentem i o jakim priorytecie. Zgodnie z definicją podjęcia efektem podjęcia jest dopiero określenie priorytetu, zatem utrudnione jest ustawianie różnych poziomów SLA dla poszczególnych priorytetów incydentu. Proponujemy ujednolicenie wartości „podjęcie" działania.

Odpowiedź: Zamawiający nie wyraża zgody na proponowane zmiany.

43. Czy Zamawiający posiada już wdrożoną platformę typu SIEM - jeżeli tak to jaką?

    Odpowiedź: Zamawiający wdraża platformę SIEM – SPLUNK

44. Czy Zamawiający oczekuje aktywnego monitoringu CTI obejmującego wycieki, analizę Dark/Deep Web etc - jeżeli tak to prosimy o podanie liczby assetow które mają zostać objęte monitoringiem?

    Odpowiedź: Wszelkie tego typu zagadnienia zostaną omówione po podpisaniu umowy.

45. W odniesieniu do punktu 4.8 i innych prosimy o zmianę zapisów - SOC może liczyć od wystąpienia Alarmu/Ofensu w systemie monitoringu SIEM lub równoważnym a nie w systemie źródłowym - Zaznaczamy, że czasami kilka do kilkunastu minut trwa sama analiza logów w systemie SIEM. Prosimy o zmianę treści na „Czas podjęcia Incydentu będzie liczony delta czasu pomiędzy pojawieniem się / odnotowaniem incydentu w systemie SIEM a czasem zweryfikowania poprawności nadania priorytetu.

    Odpowiedź: Zamawiający nie wyraża zgody na proponowane zmiany.