Odpowiedzi na zadane pytania dotyczące RFI: **Zakup systemu do monitorowania logów oraz zarządzania i monitorowania bezpieczeństwa infrastruktury teleinformatycznej wraz z pracami wdrożeniowymi oraz z wsparciem technicznym**

Pytanie nr 1

Czy Zamawiający dopuści zaoferowanie rozwiązania SIEM licencjonowanego w modelu opartym o dzienny wolumen przetwarzanych danych (GB/dzień), zamiast modelu opartego o liczbę źródeł logów, urządzeń lub EPS, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych i wydajnościowych określonych w OPZ?
Jeżeli tak, prosimy o podanie przewidywanego średniego oraz maksymalnego dziennego wolumenu danych (GB/dzień), który należy przyjąć do kalkulacji licencji

Odpowiedź:

Zamawiający nie dopuszcza zaoferowania rozwiązania SIEM licencjonowanego w modelu opartym o dzienny wolumen przetwarzanych danych (GB/dzień). Zamawiający nie korzystał dotychczas z takiego modelu licencjonowania i na obecnym etapie nie jest w stanie precyzyjnie oszacować średniego oraz maksymalnego dziennego wolumenu danych w celu dokonania porównywalnej kalkulacji. Wymagania określone w OPZ nie ulegają zmianie.

Pytanie nr 2

W związku z brakiem określenia wymagań licencyjnych dla modułu SOAR, prosimy o wskazanie:

1. Przewidywanej liczby użytkowników modułu SOAR (analitycy SOC, operatorzy, administratorzy oraz pozostali użytkownicy wymagający dostępu do systemu).
2. Wymaganej maksymalnej liczby użytkowników jednocześnie zalogowanych do modułu SOAR.
3. Potwierdzenie, że Zamawiający dopuści zaoferowanie liczby licencji użytkowników odpowiadającej wskazanym powyżej wymaganiom, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych określonych w OPZ.

Powyższe informacje są niezbędne do prawidłowego doboru i wyceny licencji dla oferowanego rozwiązania SOAR.

Odpowiedź:

Przewidywana liczba użytkowników modułu SOAR (analitycy SOC, operatorzy, administratorzy oraz pozostali użytkownicy) wynosi: 6 osób. Wymagana maksymalna liczba jednocześnie zalogowanych użytkowników modułu SOAR wynosi: 3 osoby. Zamawiający potwierdza, że dopuści zaoferowanie liczby licencji użytkowników odpowiadającej wskazanym powyżej wymaganiom, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych określonych w OPZ.

Pytanie nr 3

Czy Zamawiający wymaga natywnego zarządzania kluczami SSH (SSH Key Management), czy dopuszcza realizację funkcjonalności wykrywania, inwentaryzacji, audytu i reakcji na klucze SSH poprzez integracje, skrypty oraz playbooki automatyzacyjne?

Odpowiedź:

Zamawiający dopuszcza realizację funkcjonalności wykrywania, inwentaryzacji, audytu i reakcji na klucze SSH poprzez integracje, skrypty oraz dedykowane playbooki automatyzacyjne, bez konieczności posiadania modułu dedykowanego stricte natywnemu zarządzaniu kluczami SSH (SSH Key Management), o ile zapewni to pełną realizację celów biznesowych i bezpieczeństwa Zamawiającego oraz pod warunkiem spełnienia wszystkich wymagań funkcjonalnych określonych w OPZ.

Pytanie nr 4

Prosimy o doprecyzowanie wymagania 1.11 „Moduł analizy logów powinien posiadać raporty typu PUMA" poprzez wskazanie definicji raportów PUMA lub oczekiwanego zakresu funkcjonalnego.

Odpowiedź:

Zamawiający wyjaśnia, że pod pojęciem raportów typu PUMA (ang. Privileged User Monitoring and Audit) należy rozumieć monitorowanie i audyt użytkowników uprzywilejowanych w tym administratorów w zakresie tego co wykonują w systemach. Funkcjonalność ta powiązana jest z śledzeniem czynności danego użytkownika i pozwala na przykład w śledzeniu takich operacji jak: User Logons, User Logoffs, Failed Logons, Successful User Account Validation, Failed User Account Validation, Audit Logs Cleared, Audit Policy Changes, Objects Accessed, User Account Changes and User Group Change. Zamawiający oczekuje tworzenia przez system raportów analitycznych oraz statystycznych, które pozwolą na elastyczne profilowanie, wykrywanie anomalii oraz analizę zachowań użytkowników i systemów. Raporty mają być tworzone w postaci pliku CSV lub PDF, a także system musi umożliwiać ich wysyłanie automatycznie za pomocą serwera poczty - email.

Pytanie nr 5

Czy Zamawiający dopuści realizację raportów wymaganych przez UKSC/NIS2 poprzez konfigurowalne szablony raportów przygotowane w trakcie wdrożenia, zamiast dostarczania gotowych predefiniowanych raportów producenta?

Odpowiedź:

Zamawiający dopuszcza realizację raportów wymaganych przez UKSC/NIS2 poprzez konfigurowalne szablony raportów przygotowane i wdrożone w trakcie prac implementacyjnych, jako równoważne do gotowych, predefiniowanych raportów dostarczanych bezpośrednio przez producenta systemu.

Pytanie nr 6

Prosimy o potwierdzenie, czy wymagany okres 36 miesięcy dotyczy wyłącznie wsparcia technicznego, czy również licencji na oferowane moduły Systemu (SIEM, Audyt AD, SOAR, CLM, UEBA, ATA).
Jednocześnie prosimy o potwierdzenie, że Zamawiający dopuści rozwiązania oferowane w modelu subskrypcyjnym, pod warunkiem zapewnienia pełnej funkcjonalności Systemu przez wymagany okres obowiązywania wsparcia technicznego.

Odpowiedź:

Zamawiający potwierdza, że wymagany okres 36 miesięcy dotyczy wyłącznie świadczenia wsparcia technicznego dla oferowanego rozwiązania. Wszystkie oferowane moduły Systemu (SIEM, Audyt AD, SOAR, CLM, UEBA, ATA) muszą zostać dostarczone na podstawie licencji wieczystych. W związku z powyższym, Zamawiający nie dopuszcza rozwiązań oferowanych w modelu subskrypcyjnym (terminowym).