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**

W odniesieniu do wymagania nr 26 prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie, w którym poszczególne moduły posiadają odrębne interfejsy użytkownika, pod warunkiem zapewnienia pełnej integracji funkcjonalnej pomiędzy nimi oraz wspólnego procesu uwierzytelniania.

**Odpowiedź:**

Zamawiający wyjaśnia, że intencją zapisów OPZ jest dążenie do maksymalnej spójności środowiska i wygody operatorów, stąd wskazanie, że moduły powołane w wymaganiu nr 26 powinny posiadać jeden interfejs użytkownika. Mając na uwadze cel zapytania (RFI), Zamawiający dopuszcza rozwiązanie, w którym poszczególne moduły posiadają odrębne interfejsy użytkownika, pod warunkiem zapewnienia pełnej i płynnej integracji funkcjonalnej pomiędzy nimi (w tym m.in. przekazywania kontekstu oraz danych między modułami) oraz bezwzględnego zapewnienia wspólnego, jednolitego procesu uwierzytelniania użytkowników (Single Sign-On).

**Pytanie nr 2**

W odniesieniu do wymagania nr 27 prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie, w którym raporty Compliance dostępne są dla wybranych modułów systemu, natomiast dla pozostałych modułów funkcjonalność ta może zostać zapewniona poprzez dodatkowy komponent producenta.

**Odpowiedź:**

Zamawiający dopuszcza rozwiązanie, w którym funkcjonalność raportów Compliance dla części modułów zostanie zapewniona poprzez dodatkowy komponent producenta, pod warunkiem, że komponent ten zostanie dostarczony, zainstalowany i wdrożony w ramach oferowanej ceny, a dostęp do tych raportów będzie realizowany z poziomu panelu użytkownika zgodnie z wymaganiem nr 27 OPZ.

**Pytanie nr 3**

W odniesieniu do pkt 3 OPZ prosimy o doprecyzowanie, czy w przypadku oferowania rozwiązania instalowanego na infrastrukturze Zamawiającego, Zamawiający dopuści dostawę wyłącznie licencji i niezbędnego oprogramowania, bez obowiązku dostawy serwerów lub urządzeń sprzętowych

**Odpowiedź:**

Zamawiający informuje, że nie udostępnia własnej infrastruktury sprzętowej ani wirtualnej na potrzeby instalacji i utrzymania oferowanego systemu. W związku z tym Wykonawca jest zobowiązany do skalkulowania i dostarczenia w ramach zamówienia kompletnego rozwiązania, w tym niezbędnych serwerów i urządzeń sprzętowych zapewniających prawidłowe, stabilne i wydajne działanie wszystkich modułów Systemu zgodnie z wymaganiami OPZ.

**Pytanie nr 4**

W odniesieniu do wymagania nr 20 prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie, w którym informacje niezbędne do przygotowania raportu poincydentalnego (oś czasu incydentu, wykonane działania oraz ich rezultaty) są gromadzone przez system, natomiast sam raport jest przygotowywany przez administratora, a nie generowany automatycznie.

**Odpowiedź:**

Zamawiający nie dopuszcza rozwiązania, w którym raport poincydentalny jest w całości przygotowywany manualnie przez administratora. Zgodnie z wymaganiem nr 20 OPZ, System musi posiadać wbudowany mechanizm generowania dokumentacji poincydentalnej na podstawie osi czasu incydentu, wykonanych akcji i ich wyników. Zamawiający dopuszcza sytuację, w której wygenerowany automatycznie raport może być edytowany lub uzupełniany przez administratora przed jego ostatecznym zapisem.

**Pytanie nr 5**

W odniesieniu do wymagania 3.2 dotyczącego wykrywania aktywności charakterystycznej dla oprogramowania ransomware prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie realizujące wybrane scenariusze detekcji wskazane w OPZ, bez konieczności zapewnienia wszystkich wymienionych mechanizmów.

**Odpowiedź:**

Zamawiający nie dopuszcza ograniczenia scenariuszy detekcji. Wymaganie 3.2 lit. a) w sekcji MODUŁ 1 (SIEM) wyraźnie wskazuje minimalny oczekiwany zakres detekcji aktywności ransomware (masowe zmiany rozszerzeń plików, kasowanie kopii cieniowych VSS, szyfrowanie w krótkim czasie). Oferowane rozwiązanie musi realizować wszystkie wskazane mechanizmy detekcji w celu skutecznego wykrywania zagrożeń.

**Pytanie nr 6**

W odniesieniu do wymagania 3.2 dotyczącego wykrywania prób ataków na aplikacje webowe prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie zapewniające wykrywanie części wskazanych scenariuszy, przy jednoczesnym zachowaniu możliwości rozbudowy reguł korelacyjnych przez administratora.

**Odpowiedź:**

Zamawiający nie dopuszcza rozwiązania, które w bazie predefiniowanej nie realizuje pełnego zakresu wskazanego w wymaganiu 3.2 lit. b) MODUŁU 1 (SQL Injection, XSS, skanowanie ścieżek, wykrywanie skanerów podatności). Predefiniowana baza reguł korelacyjnych producenta musi zapewniać wykrywanie wszystkich wymienionych typów ataków w dniu dostawy. Możliwość rozbudowy reguł przez administratora stanowi wymaganie dodatkowe, a nie zastępcze.

**Pytanie nr 7**

W odniesieniu do wymagania dotyczącego wykrywania anomalii sieciowych i wolumetrycznych prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie niewykrywające natywnie wszystkich wskazanych scenariuszy, pod warunkiem możliwości integracji z zewnętrznymi źródłami danych lub innymi komponentami środowiska bezpieczeństwa.

**Odpowiedź:**

Zamawiający dopuszcza realizację tego wymagania poprzez integrację z zewnętrznymi źródłami danych lub innymi komponentami środowiska bezpieczeństwa Zamawiającego (np. logi z firewalli, IPS/IDS), o ile integracja ta zostanie w całości wykonana przez Wykonawcę w ramach prac wdrożeniowych, a System w oparciu o te dane będzie skutecznie i w czasie rzeczywistym realizował korelację oraz wykrywanie anomalii sieciowych i wolumetrycznych opisanych w wymaganiu 3.2 lit. c).

**Pytanie nr 8**

W odniesieniu do wymagania dotyczącego automatycznego budowania linii bazowych zachowania użytkowników i hostów prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie, w którym reguły wykrywania anomalii oraz progi alarmowe definiowane są przez administratora systemu.

**Odpowiedź:**

Zamawiający nie dopuszcza rozwiązania bazującego wyłącznie na ręcznym definiowaniu progów. Zgodnie z wymaganiem nr 3.3 w sekcji MODUŁ 1 (SIEM) oraz wymaganiem nr 1.4 w sekcji MODUŁ 2 (Audyt AD), system musi budować dynamiczne linie bazowe (baseline) normalnego zachowania bez konieczności ręcznego definiowania progów dla każdego zasobu z osobna. Definiowanie progów przez administratora może stanowić jedynie funkcjonalność uzupełniającą.

## Pytanie nr 9

W odniesieniu do wymagania dotyczącego obsługi wskaźników kompromitacji (IoC) prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie zapewniające integrację z platformami Threat Intelligence, niewspierające jednak ręcznego importu list IoC w formatach CSV oraz OpenIOC.

## Odpowiedź:

Zamawiający nie dopuszcza rozwiązania niespełniającego wymogu ręcznego importu. Zgodnie z wymaganiem nr 3.4 w sekcji MODUŁ 1 (SIEM) oraz wymaganiem nr 2.6 w sekcji MODUŁ 3 (SOAR), system musi zarówno wspierać pobieranie wskaźników kompromitacji (IoC) przez standardy STIX 2.x/TAXII 2.x, jak i umożliwiać ręczny import list IoC w formatach CSV i OpenIOC. Spełnienie obu tych kryteriów jest kluczowe dla zachowania pełnej operacyjności systemu.

**Pytanie nr 5**

**Odpowiedź:**

**Pytanie nr 6**

**Odpowiedź:**