Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Specyfikacja Techniczna

Zadanie: „Wdrożenie Systemu bezpieczeństwa cyfrowego”

I. Wstęp

1. W niniejszej Specyfikacji Technicznej przedstawiono wymagania funkcjonalne i techniczne dotyczące dostawy, wdrożenia oraz uruchomienia zintegrowanego systemu cyberbezpieczeństwa zapewniającego ochronę infrastruktury informatycznej i przemysłowej.

2. Celem zakupu jest zapewnienie automatyzacji procesów takich jak: zbieranie, analiza, normalizacja, korelacja oraz przechowywanie zdarzeń (logów) pochodzących z systemów informatycznych Zamawiającego.

3. Realizacja Projektu pozwoli uzyskać następujące korzyści:

   3.1 Centralne przechowywanie i archiwizowanie zdarzeń z systemów informatycznych Zamawiającego.
   3.2 Kategoryzację informacji o zdarzeniach oraz korelację zdarzeń z różnych źródeł.
   3.3 Wsparcie w poszukiwaniu zagrożeń (Threat Hunting).
   3.4 Modelowanie zagrożeń w systemie informatycznym na podstawie wiedzy o technikach i taktykach cyberprzestępców (MITRE ATT&CK).
   3.5 Wzrost efektywności zespołów odpowiedzialnych za utrzymanie systemów informatycznych w zakresie bezpieczeństwa cyfrowego poprzez wykorzystanie technologii chmurowych i sztucznej inteligencji.

II. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja systemu cyberbezpieczeństwa wraz z usługami utrzymania, wsparcia, szkoleniami oraz integracją z istniejącą infrastrukturą informatyczną Zamawiającego.

1. Zakres zamówienia

- Dostawa licencji oraz niezbędnych elementów/urządzeń składowych systemu cyberbezpieczeństwa
- Usługi wdrożeniowe: analiza przedwdrożeniowa, instalacja, konfiguracja, integracja z systemami Zamawiającego, dokumentacja powdrożeniowa
- Szkolenia dla zespołu Zamawiającego
- Utrzymanie i wsparcie techniczne (SLA)

2. Wymagania systemu

1. System powinien dawać możliwość:
    - Analizy zachowania użytkowników i urządzeń (UEBA)
    - Wykrywania anomalii na podstawie AI / uczenia maszynowego
    - Możliwość definiowania tagów i grup wysokiego ryzyka
    - Korelacji zdarzeń z regułami/oknami czasowymi
    - Integracji z systemem SOAR
2. System powinien dawać możliwość zbieranie zdarzeń z wielu źródeł:
    - Obsługa syslog (UDP/TCP/TLS)
    - Obsługa CSV, JSON, XML, Common Log Format
    - Firewalle, Switche, WAF, Proxy, VPN, IDS/IPS, NDR, NAC, DLP, CASB, EDR/XDR/AV
    - Aplikacje i serwery: serwery poczty (SMTP/IMAP/Exchange), serwery www, bazy danych (audit/log), ERP/CRM/SCADA, systemy backupu.
    - Kolekcja logów z systemów:
        - Windows Event Logs (WMI/WinRM/Agent)
        - Linux (rsyslog/syslog-ng/agent).
    - Integracje z usługami katalogowymi AD/LDAP/ENTRA
    - Integracje z platformami chmurowymi (AWS/Azure/GCP), przez API lub natywne konektory
    - Obsługa endpointów (EDR/XDR/AV)
    - Obsługa NetFlow/sFlow/IPFIX na potrzeby analizy ruchu.
    - Obsługa kolektorów/agentów z buforowaniem i odtwarzaniem po utracie łączności.
3. System powinien dawać możliwość analizy zdarzeń i tworzenia dashboardów dla użytkowników systemu
4. System powinien dawać możliwość korelacji zdarzeń z CMDB
5. System powinien dawać możliwość integracji z systemem ticketowym Zamawiającego (np. przez e-mail, REST API, webhook)
6. System powinien dawać możliwość scoringu ryzyka dla użytkowników i urządzeń.
7. System powinien dawać możliwość automatyzacji reakcji na incydenty bezpieczeństwa i tworzenie playbooków.
8. System powinien dawać możliwość integracji z systemami zewnętrznymi za pośrednictwem interfejsów, np.: API, plików tekstowych, baz danych z systemami Zamawiającego.
9. System powinien mieć możliwość implementacji w architekturze wysokiej dostępności HA (sposób implementacji zostanie określony na etapie analizy infrastruktury Zamawiającego)
10. System ma dawać możliwość szyfrowania danych w spoczynku i w tranzycie – komunikacja powinna odbywać się przez bezpieczne protokoły, np.: SSL/TLS (TLS 1.2/1.3)
11. System powinien dawać możliwość utrzymania retencji danych zgodnie z poniższymi założeniami:
    - min. 30 dni dla logów hot
    - min. 6 miesięcy dla logów cold
12. System ma zostać zaimplementowany w chmurze prywatnej wskazanej przez Zamawiającego oraz w lokalizacji w zakładzie wskazanej przez Zamawiającego.

13. System powinien mieć możliwość obsługi dla minimum poniższych parametrów (zgodnie z zapotrzebowaniem wynikającym z analizy przedwdrożeniowej):
    - Rozwiązanie musi posiadać wydajność umożliwiający przetwarzanie zdarzeń na średnim poziomie min. 200 EPS z możliwością skalowania w górę.
    - System musi zapewniać możliwość obsługi dla minimum 100 aktualnych źródeł danych znajdujących się w sieci. Przez źródło danych należy rozumieć zasób IT / zasób sieciowy, który zostanie zdefiniowany w systemie oraz będzie objęty jego logiką działania. Przykładowym źródłem danych może być serwer fizyczny, serwer w postaci maszyny wirtualnej, stacja robocza, urządzenie mobilne, switch , router, urządzenia bezpieczeństwa takie jak firewall, IPS, system ochrony anti-malware, strefa sieci obejmująca stacje robocze i inne.
14. System powinien mieć możliwość skalowania w przyszłości do 10.000 EPS i 3.000 źródeł danych.
15. System ma podsiadać możliwość generowania raportów z zakresu cyberbezpieczeństwa.

3. Szkolenia

1. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
    - Przedstawienie architektury Systemu
    - Omówienie procedur obsługi administracyjnej Systemu
    - Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń Systemu
    - Przekazanie informacji na temat konfiguracji i zarządzania Systemem
    - Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną

2. Zasady realizacji instruktażu stanowiskowego:
    - dla maksimum 5 osób wskazanych przez Zamawiającego
    - łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 2 dni robocze
    - instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
    - instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Systemu,

4. Wsparcie powdrożeniowe

1. Wykonawca zapewni dostęp do aktualizacji na składowe systemu przez okres min. 36 miesięcy.
2. Wykonawca zapewni gwarancje na składowe systemu na okres min 36 miesięcy.
3. Wykonawca zapewni wsparcie gwarancyjne rozwiązania, zgodnie z poniższymi kryteriami, przez okres min. 36 miesięcy od dostarczenia systemu, zgodnie z poniższymi warunkami:

Krytyczny (P1 / Urgent / Awaria)	**Opis:** Całkowita niedostępność systemu lub usługi, brak możliwości pracy. **Czas reakcji:** 30 minut **Czas rozwiązania:** do 2 godzin roboczych

Wysoki (P2 / High)	**Opis:** Poważne ograniczenie funkcjonalności, problem wpływa na dużą grupę użytkowników, ale system działa częściowo (np. problem z logowaniem części użytkowników, spowolnienia). **Czas reakcji:** do 1 godziny **Czas rozwiązania:** do 6 godzin roboczych
Średni (P3 / Medium)	**Opis:** Problem ogranicza pracę pojedynczych użytkowników lub wybranych funkcji, ale nie wpływa krytycznie na działanie całej organizacji (np. błąd w raporcie, brak dostępu do pojedynczej stacji roboczej). **Czas reakcji:** 4 godzin **Czas rozwiązania:** do 2 dni roboczych
Niski (P4 / Low)	**Opis:** Zgłoszenia o charakterze informacyjnym, prośby o zmianę konfiguracji, pytania (np. reset hasła) **Czas reakcji:** do 1 dnia roboczego **Czas rozwiązania:** do 5 dni roboczych

III. Termin wykonania przedmiotu zamówienia

1. Termin realizacji zakresu prac przewidzianych w Zamówieniu do 30.04.2026
2. Świadczenie Wsparcia technicznego przez Wykonawcę od dnia odbioru przez okres min. 36 miesięcy
3. Wykonawca przekaże Zamawiającemu do odbioru wszystkie wyniki prac powstałe podczas realizacji etapów w terminach uzgodnionych w Harmonogramie.

IV. Realizacja przedmiotu zamówienia.

1. Wykonawca zobowiązuje się do przestrzegania wewnętrznych procedur oraz regulaminów obowiązujących osoby przebywające w zakładzie Zamawiającego, o których Wykonawca zostanie poinformowany w dniu podpisania umowy.
2. Wykonawca zobowiązuje się do poinformowania swoich pracowników (współpracowników) o wewnętrznych procedurach oraz regulaminach obowiązujących u Zamawiającego.
3. Zamawiający zastrzega sobie prawo do ograniczenia dostępu do pomieszczeń Zamawiającego dla osób, które nie przestrzegają wewnętrznych procedur oraz regulaminów obowiązujących u Zamawiającego.
4. Wykonawca, a także osoby występujące w jego imieniu podczas realizacji przedmiotu zamówienia, będą zobowiązane do zachowania w tajemnicy wszelkich Informacji poufnych pozyskanych w związku z przystąpieniem do zamówienia i jego wykonywaniem, w szczególności dotyczących skonfigurowanego Systemu i innej infrastruktury teleinformatycznej Zamawiającego oraz informacji prawnie chronionych.

5. Wszelkie dokumenty elektroniczne przekazywane pomiędzy Zamawiającym i Wykonawcą zawierające Informacje poufne muszą być przekazywane w formie zaszyfrowanej.
6. Wykonawca na swój koszt i ryzyko (w tym koszty dostawy) dostarczy Zamawiającemu System, w tym niezbędny sprzęt z gwarancją sprzętową, licencjami oprogramowania, potwierdzeniem prawidłowego wykonania Zamówienia będzie podpisany przez Zamawiającego bez zastrzeżeń Protokół Odbioru.
7. Dostarczone przez Wykonawcę produkty muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia. Wykonawca dostarczy dokładny opis zasad licencjonowania oprogramowania i warunki świadczonego wsparcia dla dostarczanego Systemu.