Załącznik nr 6 do Zapytania ofertowego

Zakup <u>Oprogramowania posiadającego prewencyjne mechanizmy zapewniające Zamawiającemu bezpieczeństwo cyfrowe przetwarzanych danych</u> w oparciu o monitorowanie procesów i systemów pozwalających na wykrywanie słabych punktów – 1 zestaw

1. <u>Opis przedmiotu zamówienia</u>

Zakup Oprogramowania posiadającego prewencyjne mechanizmy zapewniające Zamawiającemu bezpieczeństwo cyfrowe przetwarzanych danych w oparciu o monitorowanie procesów i systemów pozwalających na wykrywanie słabych punktów – 1 zestaw.

Celem zakupu i wdrożenia ww. oprogramowania jest: zapewnienie niezawodnego i bezpiecznego przetwarzania danych, zapewnienie bezpiecznej łączności w sieciach operacyjnych (OT) i sieciach informacyjnych (IT) wewnątrz przedsiębiorstwa Zamawiającego.
Efektem wdrożenia ww. oprogramowania winna być bezpieczna sieć, która winna zapewnić w organizacji Zamawiającego: zwiększenie poziomu bezpieczeństwa danych oraz zwiększenie dostępności danych.

Wykonawca zamówienia winien dostarczyć i wdrożyć jeden zestaw oprogramowania/software, zawierającego elementy i/lub rozwiązania z zakresu sztucznej inteligencji, które zaimplementowane do działalności Zamawiającego będą pełnić rolę systemów automatyzujących procesy w zakresie bezpieczeństwa cyfrowego w firmie wykorzystując technologie chmurowe oraz sztucznej inteligencji (AI).

<u>W skład zestawu oprogramowania stanowiącego przedmiot niniejszego zamówienia winny wejść:</u>

A) oprogramowanie w zakresie bezpiecznego dostępu zdalnego z monitorowaniem, diagnozowania zdarzeń oraz incydentów i nagrywaniem sesji zdalnych. Funkcjonalność winna zapewnić możliwość oglądania sesji zdalnie (na odległość) lub na żywo lub wykorzystywać materiał filmowy do analizy. Zapobieganie włamaniom winno być oparte na rozwiązaniach wykorzystujących elementy Sztucznej Inteligencji (AI);

B) oprogramowanie zapewniające ochronę poufnych danych przed ich udostępnieniem osobom nieupoważnionym. Funkcjonalność winna zapewnić możliwość zarządzania z jednego miejsca przepływem danych w organizacji/przedsiębiorstwie. Oprogramowanie winno wykrywać zagrożenia wewnętrzne w przedsiębiorstwie i zapobiegać ryzyku wycieku poufnych danych;

C) oprogramowanie zapewniające dwuskładnikowe uwierzytelnianie dostępu do sieci wewnętrznej Firmy Zamawiającego. Funkcjonalność winna zapewnić integrację z posiadanymi już przez Zamawiającego urządzeniami typu UTM z rodziny FortiNet. Ponadto winna zapewnić możliwość scentralizowanego uwierzytelniania użytkowników z wykorzystaniem mechanizmów typu RADIUS i LDAP.

Oprogramowania będą wykorzystane podczas łączenia się ZSZLS nr 1 i 2 ze światem zewnętrznym przedsiębiorstwa (serwis, konserwacja, AI, działania w chmurze).

2. **Szczegółowy opis przedmiotu zamówienia:**

Ad. A) Oprogramowanie w zakresie bezpiecznego dostępu zdalnego z monitorowaniem, diagnozowania zdarzeń oraz incydentów i nagrywaniem sesji zdalnych.

BEZPIECZNY ZDALNY DOSTĘP – software winien zapewniać bezpieczny dostęp zdalny z monitorowaniem, diagnozowania zdarzeń oraz incydentów i nagrywaniem sesji zdalnych. System winien zapewnić możliwość oglądania sesji zdalnie na żywo lub wykorzystanie materiału filmowego do analizy. Software winie być zorientowany na zapobieganie włamaniom oparty na sztucznej inteligencji.
Planowane do zakupu oprogramowanie winno zawierać elementy i/lub rozwiązania z zakresu sztucznej inteligencji AI, które będą wspierać Specjalistów ds. Bezpieczeństwa firmy Zamawiającego w codziennych obowiązkach, dostarczając niezbędne wytyczne i ułatwiając proces weryfikacji oraz monitorowania.
Rozwiązania z elementami sztucznej inteligencji AI winny odpowiadać za wykrywanie i korelacje zdarzeń potencjalnie niebezpiecznych. Zgodnie z interpretowanymi przez system schematami behawioralnymi (wykorzystującymi algorytmy uczenia maszynowego, gdzie narzędzia analityczne będą ustanawiać linię bazową typowych zachowań użytkowników, a następnie identyfikować odchylenia lub anomalie, które będą wykraczać poza ustalone normy) i semantycznymi, użytkownik winien zostać powiadomiony w momencie, gdy dana sesja zostanie zidentyfikowana jako podejrzana.

Cechy/parametry oprogramowania:

Ogólne - architektura

1. **System klasy PAM (z ang. Privileged Access Management - Zarządzanie Dostępem Uprzywilejowanym)** winien być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM winien zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
2. System winien być dostarczony w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.

Licencjonowanie

1. System klasy PAM winien zostać dostarczony z kompletem licencji **dla 16 użytkowników**, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
   a. Ochrona kont uprzywilejowanych,

b. Ochrona kluczy SSH,
c. Zarządzanie i monitorowanie sesji uprzywilejowanych,
d. Rejestrowanie sesji uprzywilejowanych
e. Raportowanie wykorzystania kont uprzywilejowanych,

2. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych.
3. **Dostarczone licencje winny być udzielone w modelu subskrypcyjnym na minimum 12 miesięcy.**
3. Dostarczone licencje na System PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
4. System powinien być dostarczony wraz z rocznym serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.

Wymagane funkcjonalności

1. System klasy PAM musi zapewniać możliwość zarządzania (w szczególności):
   a. Użytkownikami na systemach operacyjnych: Windows, Unix/Linux * lub równoważnych
   b. Kontami domenowymi: MS Active Directory * lub równoważnymi
   c. Kontami lokalnymi: VMware ESX/ESXi * lub równoważnymi
   d. Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade * lub równoważnymi
   e. Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL * lub równoważnych
   f. Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC * lub równoważnymi
   g. Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS * lub równoważnymi
   h. Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
2. System klasy PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS * lub równoważne.
3. System klasy PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
   a. przeglądarka internetowa,
   b. klient RDP,
   c. klient protokołu SSH/Telnet (np. putty).
4. System klasy PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID * lub równoważne.
5. System klasy PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.
6. System klasy PAM powinien obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
7. System klasy PAM powinien ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.

8. System klasy PAM powinien umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
9. System klasy PAM powinien posiadać log dla wszystkich zdarzeń systemowych.
10. System klasy PAM powinien umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.
11. System klasy PAM powinien umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
12. System klasy PAM powinien umożliwiać raportowanie wszystkich logowań do systemu.
13. System klasy PAM powinien umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.
14. Rozwiązanie powinno posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
15. System klasy PAM powinien umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
16. System klasy PAM powinien mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
    a. umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
    b. generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
    c. generować unikalne hasła dla konta systemów docelowych,
    d. wymuszać automatyczną zmianę hasła po jego podglądzie
17. System klasy PAM powinien umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
18. System klasy PAM powinien umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
19. Audyt poleceń powinien umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
20. System klasy PAM powinien umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.
21. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
22. System klasy PAM powinien rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
23. System klasy PAM powinien umożliwiać odtworzenie zarejestrowanych nagrań sesji.
24. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.
25. System klasy PAM powinien być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
    a. zarządzać kontami uprzywilejowanymi w ramach organizacji,

b. monitorować wykorzystanie kont uprzywilejowanych,
c. nagrywać i archiwizować sesje zdalne,
d. gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,

26. System klasy PAM powinien umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.

Ad. B) <u>Oprogramowanie zapewniające ochronę poufnych danych</u> przed ich udostępnieniem osobom nieupoważnionym.
Funkcjonalność winna zapewnić możliwość zarządzania z jednego miejsca przepływem danych w organizacji/przedsiębiorstwie. Oprogramowanie winno wykrywać zagrożenia wewnętrzne w przedsiębiorstwie i zapobiegać ryzyku wycieku poufnych danych.

<u>SYSTEM OCHRONY DANYCH PRZED ICH UTRATĄ</u> – software zapewniający ochronę poufnym danym przed ich udostępnieniem osobom nieupoważnionym.
System winien: pozwolić zarządzać z jednego miejsca przepływem danych w całej organizacji; wykrywać zagrożenia wewnętrzne i zapobiegać ryzyku wycieku poufnych danych (w tym danych osobowych oraz innych danych wrażliwych). Dzięki natychmiastowej autonomicznej reakcji system winien zapewnić skuteczną ochronę danych. System winien spełniać wymogi prawne oraz wykrywać naruszenia przepisów i im zapobiegać im. Winien wykrywać, kontrolować i zabezpieczać informacje umożliwiając identyfikację osób korzystających z danych: chronionych informacji zdrowotnych, danych finansowych, czy też danych technicznych firmy. System winien zabezpieczać pliki przed niepowołanym dostępem, zarówno wewnątrz jak i na zewnątrz organizacji, a także ostrzegać kadrę zarządzającą przed ryzykiem wycieku kluczowych dla firmy danych.
System poprzez automatyczne procesy i wykorzystanie elementów i/lub rozwiązań z zakresu sztucznej inteligencji AI winien badać korelacje zdarzeń i monitorować incydenty zapobiegając niekontrolowanemu (brak zgody) wypływowi danych osobowych oraz innych wrażliwych.

<u>Cechy/parametry oprogramowania:</u>

- System klasy DLP (z ang. Data Leak Prevention – zapobieganie wyciekom danych) – zabezpieczający informacje/pliki poufne i dane wrażliwe przedsiębiorstwa.
- System winien umożliwiać zabezpieczenie danych we wskazanych miejscach przed akcjami użytkowników.
- System winien przeciwdziałać wyciekowi danych na zewnątrz oraz wykrywać zagrożenia wewnętrzne:
  - wykrywanie i klasyfikacja danych na wskazanych zasobach
  - ochrona i rozpoznawanie danych wrażliwych i krytycznych
  - proaktywna ochrona przed zagrożeniami wewnętrznymi, podejmując szybkie działania w celu ochrony kluczowych danych
  - analizowanie ryzyka w działaniach użytkowników i blokowanie niebezpiecznych zachowań
  - wykrywanie i eliminowanie niechcianego oprogramowania i urządzeń
- wymagana ilość licencji: **16 licencji dla Użytkowników;**
- licencje w 100% winny być zgodne z posiadanym wdrożonym już u Zamawiającego rozwiązaniem Safetica One;
- dostarczone licencje winny być udzielone w modelu subskrypcyjnym na minimum 12 miesięcy.

Ad. C) Oprogramowanie zapewniające <u>dwuskładnikowe uwierzytelnianie dostępu do sieci wewnętrznej firmy</u>.
Funkcjonalność ww. oprogramowania winna zapewnić integrację z posiadanymi już przez Zamawiającego urządzeniami typu UTM z rodziny FortiNet. Ponadto winna zapewnić możliwość scentralizowanego uwierzytelniania użytkowników z wykorzystaniem mechanizmów typu RADIUS i LDAP. Ww. funkcjonalność będzie wykorzystywana podczas łączenia się systemów zintegrowanych zrobotyzowanych linii produkcyjnych SMART nr 1 i 2 ze światem zewnętrznym firmy (serwis, konserwacja, AI, działania w chmurze).

Cechy/parametry oprogramowania:

Przedmiotowe oprogramowanie winno być narzędziem do zarządzania tożsamością użytkowników. Winno pozwolić zwiększyć bezpieczeństwo przedsiębiorstwa poprzez uproszczenie i centralizację zarządzania i przechowywania używanych podczas uwierzytelniania informacji o użytkownikach.
System winien zostać skonfigurowany jako centralna baza danych uwierzytelniających użytkowników oraz umożliwić kontrolowanie dostępu użytkowników za pomocą różnorodnych mechanizmów uwierzytelniających, takich jak uwierzytelnianie dwuskładnikowe, weryfikacja tożsamości i kontrola dostępu do sieci. Zabezpieczy to wnętrze firmy przed niekontrolowaną jej penetracją przez użytkowników firm zewnętrznych, którzy muszą się komunikować w ramach funkcji AI, SMART FACTORY, Linie SMART nr 1 i nr 2.

System winien posiadać funkcję ZTNA - Zero Trust Network Access – w ramach której będzie weryfikować czy komputer, który ma być podłączony do sieci spełni wymagania względem aktualizacji systemu operacyjnego i aktualnego oprogramowania antywirusowego. W przypadku braku wymogów nie zezwoli na dostęp do sieci. W ramach ZTNA dostęp do sieci winien być oparty o ciągłą analizę i ocenę użytkownika, sprzętu oraz kontekstu – według zasady „never trust, always verify" („nigdy nie ufaj, zawsze sprawdza"). System nie powinien pozwolić na jednorazowe przydzielenie dostępu bez późniejszej ponownej weryfikacji. Dzięki temu rozwiązaniu możliwe będzie zablokowanie zdalnego dostępu, jeśli tylko któryś z 25 kluczowych parametrów definiujących korzystającego uległ zmianie (pojawiło się ryzyko niekontrolowanego dostępu). Dostęp do aplikacji, czy zasobów będzie można kontrolować w precyzyjny sposób i bardzo regularnie. Nie będzie mieć znaczenia, skąd łączy się klient końcowy – zarówno pracownik zdalny, jak i użytkownik sieci lokalnej będą uznawani za użytkowników niezaufanych. O tym, czy mogą otrzymać dostępy do poszczególnych zasobów, decydować winna szczegółowa i ciągła ich weryfikacja oraz weryfikacja specyficznych elementów rozpoznawanych i sprawdzanych w sposób ciągły w trakcie sesji połączeniowych.

- wymagana ilość licencji: **16 licencji dla Użytkowników;**
- **licencje zapewniające logowanie do sieci z podwójną autentykacją oraz zapewniający bezpieczne połącznie w trybie szyfrowanym dla 16 Użytkowników** umożliwiające zarządzanie użytkownikami oraz stacjami w trybie klienckim;
- koszt winien obejmować: **licencje i tokeny – 16 kpl.**

Proponowane rozwiązanie musi być w pełni kompatybilne oraz powinno się integrować się z obecnie posiadanym rozwiązaniem przez Zamawiającego, tj. rozwiązania z rodziny FortiNet.

***** Wszędzie tam, gdzie przy opisie przedmiotu zamówienia powołane są normy, aprobaty, specyfikacje techniczne i systemy odniesienia lub procesy technologiczne, bądź wskazane są znaki towarowe, patenty lub źródło pochodzenia, postanowienia te należy odczytywać jako przykładowe, a wykonawca ma każdorazowo prawo zastosowania rozwiązania równoważnego, tj. materiałów, rozwiązań technologicznych, które mają te same cechy funkcjonalne oraz jakościowe co wskazane w zapytaniu ofertowym konkretne z nazwy, pochodzenia lub charakteru procesu produkcji materiały lub rozwiązania technologiczne. Jakość zastosowanych rozwiązań równoważnych nie może być gorsza od jakości określonych w dokumentacji produktu lub rozwiązania technologicznego.