Załącznik do Zapytania o wycenę

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa oprogramowania oraz licencji – systemu klasy XDR Trend Micro Vision One XDR lub rozwiązania równoważnego służącego do kompleksowego wykrywania, korelowania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznych oraz manualnych działań naprawczych.

Całość rozwiązania musi być dostarczona na okres 24 miesięcy, licząc od dnia 25.12.2024 roku wraz ze wsparciem technicznym producenta obejmującym:

1) Dostęp do pomocy technicznej;
2) Dostęp do poprawek, nowych wersji oprogramowania;
3) Dostęp do dokumentacji technicznej;
4) Dostęp do konta wsparcia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.
5) Zamawiający wymaga umożliwienia zgłaszania problemów on-line lub za pośrednictwem poczty elektronicznej;
6) Zamawiający wymaga zastosowania wskaźnika czasu reakcji oraz priorytetyzacji zgłoszeń zgłaszanych przez Zamawiającego podobnego do poniższego schematu:
   a) Stopień Krytyczny:
      - Główny komponent produktu lub usługi stają się bezużyteczne;
      - Krytyczny wpływ na procesy biznesowe i operacje;
      - Brak dostępnego, gotowego obejścia problemu;
      - Czas odpowiedz: Do 1 godziny.
   b) Stopień Wysoki:
      - Główne oprogramowanie, wydajność lub usługa zostały poważnie upośledzone lub zdegradowane;
      - Znaczący wpływ na procesy biznesowe i operacje
      - Czas odpowiedzi: Do 4 godzin roboczych.
   c) Stopień Średni:
      - Główne oprogramowanie lub funkcja serwisowa jest upośledzona, ale funkcjonuje;
      - Komponent lub funkcja komponentu usługi nie działa zgodnie z dokumentacją;
      - Średni lub niski wpływ na procesy biznesowe i operacje;
      - Istnieje domyślne, dostępne obejście;

- Czas odpowiedzi: Do 1 dnia roboczego.

d) Stopień Niski:

- Kosmetyczne upośledzenie lub prośba o ulepszenie danej funkcjonalności;
- Niewielki lub żaden wpływ na procesy biznes i operacje;
- Nie jest wymagane natychmiastowe rozwiązanie problemu;
- Prośba o informacje ogólne lub inne pytania konfiguracyjne;
- Czas odpowiedzi: Do 2 dni roboczych.

Całość rozwiązania musi być zintegrowana w jednej konsoli zarządzającej.

- Ilość komputerów objętych ochroną Endpoint Detection and Response: 800
- Funkcjonalność jednej wirtualnej sondy sieciowej: z przepustowością minimum do 500 Mbps
- Ilość kont objętych ochroną sondy pocztowej: 900
- Ilość kont objętych ochroną Zero Trust: 15

Opis funkcjonalności dla systemu równoważnego

1. Wymagania Ogólne

1.1. Wszystkie centralne elementy rozwiązania, takie jak centralny serwer zarządzający i bazy danych mogą być dostarczone w formie SaaS lub On-premise;

1.2. W przypadku zaoferowanego rozwiązania w formie SaaS dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy);

1.3. Producent oferowanego rozwiązania jest odpowiedzialny za niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczonego Rozwiązania (w przypadku zaoferowania rozwiązania w formie SaaS);

1.4. Zamawiający dopuszcza, aby komponenty wchodzące w skład oferowanego rozwiązania pochodziły od różnych producentów, pod warunkiem, że oferowany system jako całość będzie spełniał wszystkie przedstawione w zapytaniu wymagania;

1.5. Mechanizmy aktywnej ochrony powinny być realizowane przez tego samego agenta instalowanego na endpointach, który realizuje zbieranie danych telemetrycznych na potrzeby analizy XDR lub dodatkowego, niezależnego agenta pochodzącego od tego samego lub innego producenta;

1.6. Wszystkie mechanizmy aktywnej ochrony, informacje o zdarzeniach bezpieczeństwa, wykrytych oraz zablokowanych atakach powinny być przesyłane do centralnego systemu XDR, gdzie zostaną

poddane korelacji z pozostałymi danymi zebranymi przez sensory XDR (np. danymi telemetrycznymi);

1.7. Zamawiane oprogramowanie musi posiadać mechanizmy aktywnej ochrony obejmującej stacje końcowe;

1.8. Zamawiane oprogramowanie musi - chronić stacje końcowe przed zaawansowanymi zagrożeniami, między innymi przed niesygnaturowym złośliwym oprogramowaniem i atakami typu 0-day (Threat detection), bez względu na to, czy zagrożenie pochodzi z obszaru plików, urządzeń i systemów końcowych, ruchu pocztowego w Microsoft 365 czy też z obszaru aktywności użytkowników;

2. Wymagania funkcjonalne systemu XDR

2.1. Oferowany system klasy XDR musi posiadać możliwość zbierania danych z różnych warstw środowiska IT, w tym co najmniej:

a) Stacje robocze
b) Procesy, w tym modyfikacja
c) Pliki
d) Połączenia sieciowe
e) Zapytania DNS
f) Rejestry
g) Konta i użytkownicy
h) Zdarzenia Internetowe (obsługa URL)
i) Detekcje i zdarzenia bezpieczeństwa

2.2. Rozwiązanie musi udostępniać webową konsolę do zarządzania:

a) Dla wielu administratorów z dostępem opartym na rolach (RBAC), z możliwością zdefiniowania kto ma jaki dostęp do poszczególnych elementów interfejsu (odczyt/zapis ustawień, tylko do odczytu)
b) Z opcją pojedynczego uwierzytelniania SSO, Single Sign-On - za pomocą SAML: wsparcie dla Entra ID, ADFS oraz Okta
c) Z opcją uwierzytelniania dwuskładnikowego (MFA, Multi-Factor Authentication)

2.3. Rozwiązanie musi udostępniać interfejs programistyczny API umożliwiający pobieranie logów;

2.4. Rozwiązanie musi umożliwiać zdefiniowanie powiadomień o wykrytych zagrożeniach odrębnie dla użytkowników i administratorów systemu;

2.5. Rozwiązanie musi posiadać wbudowany mechanizm generowania raportów, możliwość szybkiej oceny stanu systemu dzięki wizualizacji w konsoli (dashboard);

2.6. Dane zbierane z poszczególnych warstw muszą być normalizowane i korelowane między sobą w oparciu o machine learning oraz metody dostarczane i aktualizowane przez producenta;

2.7. W wyniku korelacji system musi tworzyć incydenty o wysokim poziomie pewności (niski poziom false-positive);

2.8. Dane muszą być mapowane na matrycę TTP (techniques, takctiques, procedures), z uwzględnieniem matrycy MITRE ATT&CK;

3. Zarządzanie systemem

3.1. System musi posiadać mechanizm pozwalający na proste i intuicyjne uruchamianie sensorów lub agentów na poszczególnych elementach środowiska;

3.2. System musi pokazywać status sensora lub agenta na poszczególnych zasobach, w tym pokazywać z jakiej przyczyny sensor nie może zostać uruchomiony;

3.3. Mechanizm tworzenia kont w systemie musi pozwalać na zdefiniowanie dostępu do poszczególnych funkcji systemu (np. dostęp tylko do dashboard lub dostęp do listy alertów);

4. Raportowanie

4.1. System musi pozwalać na przedstawianie danych bezpieczeństwa w różnych formach:

a) Alerty

b) Użytkownicy

c) Detekcje

d) Zdarzenia w matrycy MITRE ATT&CK

4.2. System musi pozwalać na wysyłanie notyfikacji do wybranego administratora odnośnie:

a) Alertów

b) Zidentyfikowania wskaźników potencjalnego wystąpienia ataku

4.3. System musi pozwalać na wyeksportowanie wybranych zdarzeń w formacie CSV lub JSON, lub XML;

4.4. Wszelka aktywności w systemie musi być zapisywana i ewidencjonowana z zapewnieniem odpowiedniej rozliczalności działań użytkowników w środowisku;

4.5. Threat Intelligence – system musi dostarczać i integrować dane zebrane przez producenta o zagrożeniach i kampaniach przestępczych ;

4.6. Dane dostarczane do systemu, muszą być normalizowane w sposób pozwalający na ekstrakcję IOC, (ang. Indicator of compromise) tam gdzie to możliwe:

a) Domenę

b) SHA-1/SHA-256

c) IP

d) Adres nadawcy

e) URL

4.7. Środowisko musi być automatycznie przeszukiwane pod kątem wystąpienia artefaktów związanych z danym zagrożeniem/atakiem, a w konsoli musi zostać wyświetlona informacja wskazująca na identyfikację artefaktu. System musi pokazywać:

a) Poszczególne artefakty, które zostały zidentyfikowane

b) Powiązane zasoby (stacja/użytkownik)

c) Powiązane linki

4.8. W przypadku wykrycia zagrożenia system musi co najmniej:

a) Zalogować wystąpienie niebezpiecznego zdarzenia w centralnej konsoli monitorującej,

b) Zablokować zdarzenie

5. Zarządzanie ryzykiem

5.1. Kompromitacja kont - System musi identyfikować konta użytkowników, które wykazują nietypową aktywność lub zostały powiązane ze złośliwą kampanią mailową;

5.2. Podatności - Na podstawie danych pobranych z sensora/agenta na stacji PC system musi zapewniać wykrywanie podatności i zagrożeń oraz udostępniać informacje o tym w konsoli webowej. System powinien również weryfikować, czy podatność została wykorzystana;

5.3. System powinien na bieżąco oceniać zachowanie użytkowników i urządzeń oraz wskazywać na nieprawidłowości mogące identyfikować atak;

5.4. System powinien identyfikować potencjalne błędy konfiguracji, które mogą stanowić zagrożenie dla sieci. Identyfikacja powinna obejmować odsłonięte na zewnątrz porty, niezabezpieczone połączenia z hostami, niebezpieczne konfiguracje oprogramowania stacji PC;

5.5. Określanie poziomów ryzyka – System na podstawie danych ze stacji PC powinien określać łatwo identyfikowalne poziomy ryzyka dla użytkowników lub urządzeń i wyświetlać je w konsoli webowej;

5.6. System musi oceniać i pozwalać na wgląd w stan ryzyka domen publicznych i adresów IP powiązanych z infrastrukturą Zamawiającego;

6. Threat hunting

6.1. System musi pozwalać na przeszukiwanie wszystkich danych zebranych z organizacji pod kątem różnych artefaktów;

6.2. Wyszukiwanie ma być realizowane z jednego miejsca dla wszystkich źródeł;

6.3. System musi pozwalać na wyszukiwanie po pełnej frazie (np. cała komenda) lub tylko po fragmencie;

6.4. System musi pozwalać na wyszukiwanie artefaktu nawet jeśli nie jest znany atrybut powiązany z tym artefaktem np. wyszukanie ciągu, który mógłby zaistnieć jako wywołanie URL, fragment komendy, nazwa pliku itd. ;

6.5. W wyniku wyszukiwania system musi wskazywać linię czasu oraz powiązane ze zdarzeniem obiekty;

6.6. Po zidentyfikowaniu obiektu system musi pozwalać na odtworzenie przebiegu zdarzenia w łańcuchu przyczynowo-skutkowym. System ma pokazywać powiązania pomiędzy poszczególnymi zdarzeniami w łańcuchu;

6.7. System musi wyświetlać jak najpełniejsze dane odnośnie zdarzenia. Opcjonalne przykłady atrybutów w poniższej liście (tam gdzie ma to zastosowanie):

a) Typ obiektu
b) Data utworzenia/zmiany
c) Nazwa procesu
d) Lokalizacja pliku
e) Komenda CLI
f) SHA-1
g) SHA-256
h) File MD5
i) Process ID
j) Podpis/certyfikat
k) Ważność podpisu/certyfikatu
l) Typ pliku
m) Czy powstał w wyniku zdalnego dostępu?
n) Poziom integralności
o) Domena
p) URL
q) Nazwa punktu końcowego (Endpoint)
r) Adres IP punktu końcowego (Endpoint)
s) Adres MAC punktu końcowego (Endpoint)
t) Rodzaj i wersja systemu operacyjnego
u) Zalogowany użytkownik

a. Data i godzina wystąpienia

b. Przebieg komunikacji w linii czasu
c. Wskazanie miejsca, w którym zaobserwowano przesyłanie szkodliwego obiektu
d. Hosty, na których zaobserwowano pliki ze szkodliwą zawartością, w tym zapisie sieciowym
e. URL/domena
f. Użytkownik
g. Port

6.8. Zdarzenia muszą być mapowane, tam gdzie to możliwe, na techniki i taktyki MITRE ATT&CK (wskazanie konkretnego identyfikatora taktyki/techniki);

7. Incident response

7.1. System w wyniku działań korelacyjnych musi tworzyć zagregowane alerty;

7.2. Każdy alert musi wskazywać ocenę (pod kątem istotności alertu dla bezpieczeństwa) oraz być klasyfikowany wg typu zagrożenia;

7.3. System musi wskazywać jaki zasięg ma dany alert – ile i jakie stacje/użytkownicy są powiązane/i z alertem;

7.4. System ma pozwalać na zarządzanie statusem alertu, na przykład:

a) Nowy (New - status domyślny)
b) W trakcie realizacji (in progress)
c) Zamknięty (closed)
d) False Positive (closed – False Positive)

7.5. System musi pozwalać na podejmowanie akcji w poszczególnych zdarzeniach:

a) Izolacja stacji
b) Uruchomienie skryptu
c) Nawiązanie zdalnego połączenia ze stacją poprzez zdalną powłokę bezpośrednio z konsoli systemu:
    a. Przeglądanie zawartości stacji (listowanie plików/katalogów)
    b. Wyświetlanie zmiennych środowiskowych
    c. Wyświetlanie konfiguracji sieci
    d. Wyświetlanie aktualnych połączeń sieciowych
    e. Wyświetlanie listy procesów
    f. Przeglądanie kluczy rejestrów i ich wartości
    g. Wyświetlanie listy usług, wraz ze statusem
    h. Wyświetlanie listy użytkowników

i. Zakończenie procesu
j. Usunięcie pliku/folderu
k. Pobranie pliku

7.6. System musi pozwalać na tworzenie listy obiektów do zablokowania/listy wyjątków;

7.7. Obiekty muszą być dystrybuowane do poszczególnych systemów podpiętych do systemu centralnego;

7.8. Katalog obiektów do zablokowania/wyjątków:

a) Domena
b) Plik (SHA-1/SHA-256)
c) Adres IP
d) Adres nadawcy
e) URL

7.9. Dla danego obiektu dodawanego do listy obiektów do zablokowania musi być możliwość zdefiniowania dodatkowo:

a) Poziomu ryzyka
b) Akcji (logowanie/blokada lub kwarantanna)
c) Ważności blokady

8. Specyfikacja technologiczna

8.1. Sensor dedykowany na stacje robocze musi integrować się z poniższymi OS:

a) Windows 10 (21H2) i nowsze
b) Windows 7 - opcjonalne
c) MacOS Monterey (12) i nowsze

8.2. System musi pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji roboczej system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą;

8.3. System musi być oparty o wydajny silnik analityczny pozwalający na pracę z danymi bez zbędnej zwłoki, uniemożliwiającej podjęcia odpowiedniego działania;

8.4. Producent musi dostarczyć zakres danych przetwarzanych przez oferowane rozwiązanie;

8.5. System musi posiadać certyfikat potwierdzający zgodność przetwarzania danych z obowiązującymi standardami i dobrymi praktykami np. ISO27001 (wymagany przez Zamawiającego);

9. Współpraca z innymi platformami bezpieczeństwa

9.1. Zamawiane oprogramowanie nie może powodować konfliktów z posiadanym przez Zamawiającego systemem AV od McAfee (Trellix);

9.2. System XDR powinien zapewnić współpracę poprzez dzielenie IOC z rozwiązaniami Fortinet FortiGate oraz PaloAlto posiadającymi przez Zamawiającego. W ramach dzielenia się automatycznego powinny być przekazywane dane o blokowanych plikach (hash SHA1), domenach, URL-ach, IP do systemu FortiGate, które będą mogły być wykorzystywane w politykach bezpieczeństwa;

9.3. System XDR musi umożliwiać integrację z systemem typu SIEM – Splunk posiadanym przez Zamawiającego, w formie dedykowanej aplikacji Splunk-owej umożliwiając odczyt alertów w konsoli SIEM; Aplikacja musi być rozwijana przez producenta oferowanego rozwiązania lub przez producenta oprogramowania SIEM oraz być dostępna do pobrania za darmo z portalu Splunkbase;

9.4. Te same rodzaje IOC co wyżej muszą być udostępnione z Systemu XDR w postaci plików tekstowych do wykorzystania przez inne systemy bezpieczeństwa Zamawiającego;

9.5. System XDR oprócz informacji dostarczanych przez producenta o zagrożeniach (Threat Intelligance) musi pozwalać na definiowane własnych danych o zagrożeniach:

a) Ręcznie, poprzez import danych na przykład w formacie STIX/CSV

b) Automatycznie poprzez integrację z zaufanym źródłem danych o zagrożeniach w formacie TAXII – opcjonalne.

c) Przy wprowadzaniu poszczególnych danych, system musi automatycznie wyodrębniać IOC i pozwalać na definicję akcji przy zidentyfikowaniu artefaktu:

a. Logowanie

b. Blokowanie/kwarantanna

10. Dodatkowe funkcjonalności systemu XDR – Analiza sieci

10.1. System musi posiadać funkcjonalność wirtualnej sondy sieciowej o minimalnej przepustowości do 500 Mbps, która będzie w stanie zintegrować się z oferowanym systemem XDR. Integracja musi polegać co najmniej na dostarczaniu przez sondę sieciową do systemu XDR informacji o:

a) Źródłowym adresie IP

b) Docelowym adresie IP

c) Wykorzystywanym protokole sieciowym warstwy 4 modelu ISO/OSI

d) Wykorzystywanych protokołach warstw wyższych

e) Źródłowym i docelowym porcie TCP

f) Czasie wystąpienia danego połączenia sieciowego

g) Szczegółach zapytania http

h) Przesyłanych plikach

10.2. Zebrane przez system XDR informacje z sondy sieciowej muszą mieć możliwość poddania analizie i zaawansowanej korelacji z danymi pochodzącymi z innych źródłem danych (tj. stacje końcowe, ewentualnie serwery) w celu zwiększenia skuteczności wykrywania zagrożeń oraz wzbogacenia generowanych przez system analiz;

10.3. Rozwiązanie powinno wykrywać szkodliwe obiekty oraz zachowania na każdym etapie ataku. Wykrywanie zagrożeń powinno działać w czasie rzeczywistym. System powinien zapewniać możliwość pracy w trybie OFF-LINE (z wykorzystaniem mirror port-u lub interfejsu TAP).

10.4. Monitorowanie minimum 100 protokołów na pełnym zakresie portów bez potrzeby instalowania dodatkowych elementów systemu.

10.5. Rozwiązanie musi zapewniać detekcje zagrożeń na podstawie wbudowanych i aktualizowanych reguł przez producenta rozwiązania.

10.6. Rozwiązanie musi umożliwiać włączenie dostępu SSH, który umożliwi administratorowi zdalne logowanie się w celu zarządzania urządzeniami, wykonywania poleceń oraz kopiowania lub przesyłania plików do urządzenia za pomocą klienta SSH.

10.7. Rozwiązanie musi udostępniać skrypty demonstracyjne, w celu symulacji ataku i weryfikacji poprawności działania reguł detekcyjnych analizujących ruch z sondy sieciowej.

10.8. Rozwiązanie musi zapewniać możliwość pobrania plików zidentyfikowanych w telemetrii pochodzącej z sondy sieciowej w postaci skompresowanego i zabezpieczonego hasłem pliku.

11. Dodatkowe funkcjonalności systemu XDR - ochrona poczty Microsoft 365 i usług chmurowych

11.1. Dedykowana usługa ochrony systemu Microsoft 365 musi być zintegrowana z pakietem Microsoft poprzez API (Application Programming Interface), rozwiązanie nie może wymagać do działania zmiany rekordów MX dla domeny pocztowej;

11.2. Rozwiązanie ma dostarczać ochronę przed zaawansowanymi zagrożeniami ATP (Advanced Threat Protection) dla następujących usług:

a) MS Exchange Online – całość ruchu poczty elektronicznej z zewnątrz oraz wewnątrz organizacji (między pracownikami)

b) MS Sharepoint Online

c) One Drive

d) MS Teams (pliki udostępniane poprzez chat)

11.3. W ramach rozwiązania muszą być realizowane następujące składniki ochrony, dla powyżej wymienionych usług Microsoft 365:

a) Filtrowanie sygnatur plików, wraz z ochroną przed wariantami
b) Filtrowanie plików w oparciu o uczenie maszynowe
c) Analiza plików;

11.4. Rozwiązanie musi wykorzystywać usługę reputacji sieciowej do analizy i blokowania adresów URL, w szczególności musi wykorzystywać:
a) Statyczna listę reputacji, z możliwością dostrojenia czułości działania (np. najmniej agresywne, średnio agresywne, agresywne)
b) Dynamiczne skanowanie URL - dla nieznanych, nieistniejących jeszcze w bazie statycznej adresów
c) Analizę przy użyciu algorytmów widzenia komputerowego, pozwalająca wykryć i zablokować przypadki phishingu (wyłudzenia poświadczeń do serwisów Microsoft'u)

11.5. Usługa reputacji powinna umożliwiać analizę adresów URL pochodzących z treści wiadomości, a także z plików wymienianych jako załączniki oraz przez OneDrive, Sharepoint i MS Teams;

11.6. Ochrona anty-spamowa dla Exchange Online - opcjonalnie:
a) Możliwość zdefiniowania poziomu czułości mechanizmów ochrony (przykładowo: najmniej agresywna, średnio agresywna, agresywna)
b) Wykrywanie i blokowanie wiadomości typu gray-mail, w tym na przykład newsletterów, powiadomień z sieci społecznościowych, forów itp.
c) Ochrona przed atakami BEC – Business Email Compromise – dedykowany silnik analizujący nagłówki oraz treść korespondencji lub podobna funkcjonalność
d) Możliwość zdefiniowania użytkowników typu VIP oraz ważnych domen dla silnika BEC, wykrywanie ataków podszywania się z użyciem bliźniaczych domen oraz nadawców
e) Możliwość dodania wyjątków na podstawie nagłówka wiadomości lub adresów oraz domen nadawców
f) Możliwość ręcznego zablokowania nadawcy lub domeny
g) Blokowanie na podstawie predefiniowanych wzorców
h) Definiowanie własnych identyfikatorów danych z użyciem wyrażeń regularnych (regex)
i) Tworzenie reguł, z wykorzystaniem własnych oraz wbudowanych list słów kluczowych i identyfikatorów danych

11.7. Rozwiązanie musi umożliwiać skonfigurowanie akcji jaka zostanie podjęta po wykryciu zagrożeń, w oparciu o ich kategorie:
a) Kwarantanna (najlepiej zintegrowana ze środowiskiem MS365 Zamawiającego)
b) Kasowanie
c) Przepuszczenie

d) Dla wiadomości email dodatkowo: ostemplowanie treści lub tematu, przeniesienie do folderu wiadomości-śmieci

11.8. Rozwiązanie musi umożliwiać szybkie zidentyfikowanie najczęściej atakowanych adresów użytkowników;

11.9. Rozwiązanie musi umożliwiać integrację usługi ochrony z oferowanym środowiskiem XDR:

a) Eskalacja najważniejszych zdarzeń bezpieczeństwa do alertów w dedykowanej konsoli XDR

b) Korelacja detekcji z poczty elektronicznej oraz ze stacji roboczych MS Windows

c) Możliwość blokowania korespondencji według nadawcy i message-id z poziomu konsoli XDR

d) Możliwość przeszukiwania archiwalnych danych telemetrycznych według nadawcy, odbiorcy, tematu oraz message-id

e) Automatyczne wyszukiwanie nowych zagrożeń w zgromadzonych danych telemetrycznych (IOC Sweeping)

f) Możliwość przedstawienia łańcucha ataku w formie graficznej, także po złożeniu zdarzeń z odpowiedniej stacji roboczej oraz systemu pocztowego – opcjonalne.

12. Dodatkowe funkcjonalności systemu XDR – Zero Trust

12.1. Rozwiązanie powinno umożliwiać kontrolę dostępu do zasobów na podstawie tożsamości użytkownika, a także na podstawie lokalizacji czy sieci z której użytkownik próbuje się połączyć;

12.2. Dostęp do zasobów powinien być udzielany indywidualnie na podstawie uwierzytelnionego użytkownika i jego uprawnień;

12.3. Rozwiązanie powinno uwzględniać zgodność urządzenia, z którego użytkownik próbuje się połączyć, aby zapewnić dodatkową warstwę zabezpieczeń;

12.4. Każde wyznaczone urządzenie i każdy wyznaczony użytkownik muszą być uwierzytelnione i autoryzowane przed uzyskaniem dostępu do zasobów;

12.5. Rozwiązanie powinno zapewniać mechanizmy umożliwiające adaptacyjne, zautomatyzowane decyzje dotyczące dostępu do zasobów. Rozwiązanie powinno dynamicznie dostosowywać udzielanie dostępu na podstawie oceny ryzyka i wykrywania zagrożeń bazując na danych z całego XDR;

12.6. Rozwiązanie powinno umożliwiać tworzenie reguł dostępu. Administrator powinien mieć możliwość definiowania reguł dostępu na poziomie użytkownika, grupy użytkowników (opcjonalne), aplikacji oraz na podstawie oceny ryzyka;

12.7. Rozwiązanie powinno egzekwować zasady kontroli dostępu przykładowo poprzez bezpieczne moduły dostępu zainstalowane na każdej, wskazanej stacji PC;

12.8. Rozwiązanie powinno się bezproblemowo integrować z istniejącymi, popularnymi zaporami ogniowymi lub zapewniać alternatywne mechanizmy, takie jak pliki PAC i bramy lokalne, dla urządzeń niezdolnych do zainstalowania modułu bezpiecznego dostępu;

13. Wymagania dotyczące szkoleń i usług serwisowych

13.1. W ramach usług szkoleniowych i serwisowych Wykonawca zapewni: Przeprowadzenie szkoleń dla 2 administratorów ze strony Zamawiającego w zakresie administrowania wdrożonym systemem. Szkolenie będzie się odbywać w lokalizacji Zamawiającego w Warszawie lub w formie zdalnej; Zamawiający dopuszcza vouchery umożliwiające zapisanie się na szkolenia z oferowanego oprogramowania;

13.2. 24 miesiące wsparcia Producenta rozwiązania w trybie 24/7 obsługiwane bezpośrednio przez producenta;

14. Wymagania dotyczące wsparcia Producenta i czasu reakcji na zgłoszenia

14.1. Zakres wsparcia technicznego producenta

a) Dostęp do pomocy technicznej;

b) Dostęp do poprawek, nowych wersji oprogramowania;

c) Dostęp do dokumentacji technicznej;

d) Dostęp do konta wsparcia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.

14.2. Zamawiający wymaga umożliwienia zgłaszania problemów on-line lub za pośrednictwem poczty elektronicznej;

14.3. Zamawiający wymaga zastosowania wskaźnika czasu reakcji oraz priorytetyzacji zgłoszeń zgłaszanych przez Zamawiającego podobnego do poniższego schematu:

a) Stopień Krytyczny:

a. Główny komponent produktu lub usługi stają się bezużyteczne;
b. Krytyczny wpływ na procesy biznesowe i operacje;
c. Brak dostępnego, gotowego obejścia problemu;
d. Czas odpowiedz: Do 1 godziny.

b) Stopień Wysoki:

a. Główne oprogramowanie, wydajność lub usługa zostały poważnie upośledzone lub zdegradowane;

b. Znaczący wpływ na procesy biznesowe i operacje
c. Czas odpowiedzi: Do 4 godzin roboczych.

c) Stopień Średni:

a. Główne oprogramowanie lub funkcja serwisowa jest upośledzona, ale funkcjonuje;
b. Komponent lub funkcja komponentu usługi nie działa zgodnie z dokumentacją;
c. Średni lub niski wpływ na procesy biznesowe i operacje;
d. Istnieje domyślne, dostępne obejście;
e. Czas odpowiedzi: Do 1 dnia roboczego.

d) Stopień Niski:

a. Kosmetyczne upośledzenie lub prośba o ulepszenie danej funkcjonalności;
b. Niewielki lub żaden wpływ na procesy biznes i operacje;
c. Nie jest wymagane natychmiastowe rozwiązanie problemu;
d. Prośba o informacje ogólne lub inne pytania konfiguracyjne;
e. Czas odpowiedzi: Do 2 dni roboczych.