Załącznik 2

Opis przedmiotu szacowania

Przedmiotem zapytania jest dostarczenie systemu klasy XDR służącego do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych wraz z mechanizmami aktywnej ochrony obejmującymi stacje końcowe, serwery, urządzenia sieciowe oraz pocztę elektroniczną opartą o rozwiązanie Fortimail firmy Fortigate.

Rozwiązanie musi być dostarczone wraz z usługą pełnego wdrożenia tj. instalacja oprogramowania na serwerze, dostosowaniem możliwości oprogramowania do wymagań Zamawiającego , szkoleniem administratorów w ilości 10 godzin. Całość rozwiązania musi być zintegrowana w jednej konsoli zarządzającej oraz pochodzić od jednego producenta. Oprogramowanie kupowane jest na okres 36 miesięcy z pełnym wsparciem producenta oraz lokalnym wsparciem Wykonawcy w miesięcznej ilości 8 godzin przez cały okres obowiązywania umowy (łącznie 288 godzin wsparcia lokalnego Wykonawcy).

- Ilość komputerów objętych ochroną – 600
- Ilość serwerów objętych ochroną – 150 w tym 25 serwerów fizycznych
- Ilość kont poczty elektronicznej objętych ochroną – 1000
- Ilość ruchu do analizy w sieci - min. 500Mbps

Wymagania funkcjonalne platformy bezpieczeństwa

Wszystkie elementy rozwiązania muszą być dostarczone w formie SaaS, gdzie wszystkie komponenty centralne, takie jak centralny serwer zarządzający i bazy danych i dostarczone przez producenta oferowanego rozwiązania jako usługa. Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy). Producent oferowanego rozwiązania jest odpowiedzialny za niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczanych jako usługa typu SaaS.

Oferowana platforma bezpieczeństwa musi umożliwiać:

- centralne zarządzanie ochroną komputerów, serwerów i urządzeń mobilnychzarządzanie ryzykiem cyber
- wykrywanie i korelowania zagrożeń w oparciu o telemetrię przy pomocy machine learning
- przeszukiwanie wszystkich danych zebranych z organizacji pod kątem różnych artefaktów – Threat Hunting
- dostaraczenie na bieżąco Informacji o prowadzonych kampaniach I zagrożeniach – Threat Intelligance
- Wykrywanie zero-day malware w oparciu o sandbox

Wymagania funkcjonalne systemu XDR

- Oferowany system klasy XDR musi posiadać możliwość zbierania danych z różnych warstw środowiska IT, w tym co najmniej:
    - Stacje końcowe i serwery
        - Procesy, w tym modyfikacja
        - Pliki
        - Połączenia sieciowe
        - Zapytania DNS
        - Rejestry
        - Konta i użytkownicy
        - Zdarzenia Internetowe (obsługa URL)
        - Windows hooks
        - Detekcje i zdarzenia bezpieczeństwa
        - Podatności zidentyfikowane na stacji końcowej
        - Aplikacje zainsalowane na stacji końcowej
        - Usługi publiczne SaaS, do których dostaje się stacja końcowa
    - Systemy analizy ruchu sieciowego,
    - Ochrony urządzeń mobilych,
    - Ochrony poczty eletronicznej,
    - Systemów zarządzania chmurami publicznymi AWS, Azure, GCP
    - Systemów tożsamości użytkoiwnika Microsfot EntraID, Active Directory, Octa
- Dane zbierane z poszczególnych warstw muszą być normalizowane i korelowane między sobą w oparciu o machine learning oraz metody dostarczane i aktualizowane przez producenta
- W wyniku korelacji system musi tworzyć incydenty o wysokim poziomie pewności (niski poziom false-positive)
    - W przypadku wskazanych korelacji system musi zapewnić możliwość tworzenia wyjątków, dla których incydenty nie będą generowane.
- Dane muszą być mapowane na matrycę TTP (techniques, takctiques, procedures), z uwzględnieniem matrycy MITRE ATT&CK
- Dane dotyczące podatności powinny zawierać wyliczony poziom ryzyka dla danego identyfikatora CVE.

Zarządzanie:

- System musi posiadać mechanizm pozwalający na proste i intuicyjne uruchamianie sensorów lub agentów na poszczególnych elementach środowiska
- System musi pokazywać status sensora lub agenta na poszczególnych zasobach, w tym pokazywać z jakiej przyczyny sensor nie może zostać uruchomiony
- Mechanizm tworzenia kont użytkowników w systemie musi pozwalać na zdefiniowanie dostępu do poszczególnych funkcji systemu (np. dostęp tylko do dashboard lub dostęp do listy alertów)

Raportowanie:

- System musi pozwalać na przedstawianie danych bezpieczeństwa w różnych perspektywach:
    - Alerty,

    - Użytkownicy,
    - Detekcje,
    - Zdarzenia w matrycy MITRE ATT&CK
- System musi pozwalać na wysyłanie notyfikacji do wybranego administratora odnośnie:
    - Alertów,
    - Zidentyfikowania wskaźników potencjalnego wystąpienia ataku,
- System musi pozwalać na wyeksportowanie wybranych zdarzeń w formacie CSV lub JSON
- Wszelka aktywności w systemie musi być zapisywana i ewidencjonowana z zapewnieniem odpowiedniej rozliczalności działań analityków w środowisku
- Threat Intelligence – system musi dostarczać i integrować dane zebrane przez producenta o zagrożeniach i kampaniach przestępczych
    - Dane dostarczane do systemu, muszą być normalizowane w sposób pozwalający na ekstrakt iOC (tam gdzie to możliwe):
        - Domenę
        - SHA-1/SHA-256
        - IP
        - Adres nadawcy
        - URL
    - System musi zapewnić możliwość rozszerzenia bazy iOC przez import ekstaktu IOC w formie pliku tekstowego lub integrację z rozwiązaniami firm trzecich poprzez MISP, STIX, CSV, openIOC
    - 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:
        - Poszczególne artefakty, które zostały zidentyfikowane
        - Powiązane zasoby (stacja końcowa/użytkownik)
        - Powiązane linki
    - W przypadku wykrycia zagrożenia system musi co najmniej:
        - Zalogować wystąpienie niebezpiecznego zdarzenia w centralnej konsoli monitorującej,
        - Zablokować zdarzenie
    - System musi zapewnić możliwość przekazania własnych próbek plików do wyizolowanego środowiska testowego „sandbox” i otrzymania raportu z wyniku analizy.

Wymagania funkcjonalne dla mechanizmów aktywnej ochrony stacji końcowych

Wymagania ogólne

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

Wszystkie mechanizmy aktywnej ochrony informacje o zdarzeniach bezpieczeństwa, wykrytych oraz zablokowanych atakach powinny przesyłam do centralnego systemu XDR, gdzie zostaną poddane korelacji z pozostałymi danymi zebranymi przez sensory XDR (np. danymi telemetrycznymi).

Wymagania funkcjonalne dla systemu aktywnej ochrony stacji końcowych

Ochrona antymalware

- Wszystkie funkcjonalności oprogramowania aktywnej ochrony dla stacji końcowych muszą być zarządzane z tej samej centralnej konsoli, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej.
- Rozwiązanie w obrębie funkcjonalności aktywnej ochrony stacji końcowych musi działać jako jeden agent, odpowiadający zarówno za egzekwowanie polityk bezpieczeństwa jak i komunikację z serwerem zarządzającym.
- Rozwiązanie musi zapewniać ochronę co najmniej systemów Windows 7/8.1/10, 11, macOS (10.14) i nowsze.
- Rozwiązanie musi wykorzystywać technologię „Machine Learning" do wykrywania nowych, nieznanych wirusów.
- Rozwiązanie musi zapewniać wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
- Rozwiązanie musi zapewniać ochronę przed atakami typu ransomware.
- Rozwiązanie musi zapewniać automatyczne usuwanie wirusów oraz alarmować w przypadku wykrycia zagrożenia.
- Rozwiązanie musi umożliwiać zablokowanie zmian ustawień konfiguracyjnych klientów rozwiązania na stacjach roboczych w celu uniemożliwienia ich modyfikacji.
- Rozwiązanie musi umożliwiać tworzenie ról administratorów o różnych stopniach uprawnień.
- Rozwiązanie musi mieć możliwość integracji z MS Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów.

Ochrona przed wyciekiem danych

W ramach kompleksowej ochrony stacji końcowych poza systemem ochrony przed atakami i niebezpiecznym kodem wymagane są następujące dodatkowe funkcjonalności, dostarczone przez tego samego lub innego producenta. Poniższe funkcjonalności mogą być realizowane przez tego samego lub dodatkowych agentów instalowanych na chronionej stacji.

- Kontrola podłączanych urządzeń zewnętrznych oraz ochrona przed wyciekiem danych:
    - Funkcjonalność musi zapewniać ochronę przed wyciekiem poufnych danych.
    - Funkcjonalność musi umożliwiać monitorowanie i powiadamianie o incydentach wycieku danych w czasie rzeczywistym.
    - Funkcjonalność musi posiadać możliwość kontroli i ochrony danych wrażliwych przy wykorzystaniu co najmniej takich mechanizmów jak:
        - Wyrażenia regularne: dane o określonej strukturze.
        - Atrybuty plików.
        - Słowa kluczowe: Lista wrażliwych słów i wyrażeń.
    - Funkcjonalność musi posiadać gotowe, dostarczane wraz z rozwiązaniem szablony wyrażeń regularnych pozwalające na kontrolę i ochronę danych typowych dla Polski (przykładowo numer dowodu, numer pesel)

- Funkcjonalność musi posiadać możliwość monitorowania i ochrony następujących kanałów transmisji:
  - Klienci poczty elektronicznej
  - Protokoły HTTP i HTTPS
  - Protokół SMB
  - Poczta elektroniczna dostępna poprzez stronę Web
  - Rejestratory Danych (CD/DVD)
  - Aplikacje wymiany plików peer-to-peer
  - Drukarka
  - Schowek systemu Windows
- Funkcjonalność musi umożliwiać podjęcie następujących czynności w przypadku wykrycia naruszenia polityki ochrony przed wyciekiem poufnych danych:
  - Pomiń – program zapewnia i protokołuje transmisję.
  - Blokuj – program blokuje i protokołuje transmisję.
  - Powiadom – program wyświetla powiadomienie, aby poinformować użytkownika transmisji danych o umożliwieniu lub zablokowaniu transmisji.
  - Zachowanie danych rekordów – niezależnie od operacji podstawowej program zapisze dane oznaczone jako naruszenie polityki do dalszej analizy.
- Funkcjonalność musi umożliwiać szczegółowe raportowanie wszystkich akcji oraz zapewniać możliwość generowania wykresów/diagramów/zestawień (logiczne filtrowanie informacji)
- Funkcjonalność musi posiadać możliwość pracy agenta zainstalowanego na stacji użytkownika w trybie offline, bez kontaktu z serwerem zarządzającym
- Funkcjonalność musi posiadać możliwość zapewnienia ochrony poprzez kontrolę urządzeń zewnętrznych oraz dostępu do pamięci masowych i zasobów sieciowych połączonych z komputerami.
- Funkcjonalność musi posiadać możliwość monitorowania:
  - Urządzeń pamięci masowej:
  - CD/DVD
  - Dyskietek
  - Dysków Sieciowych
  - Urządzeń pamięci masowej USB
  - Urządzeń innych niż pamięci masowe:
  - Portów COM i LPT
  - Modemów
  - Kart PCMCIA
  - Drukarek
  - Klawisza Print Screen
- Funkcjonalność musi posiadać możliwość nadawania uprawnień kontroli dla urządzeń pamięci masowej takich jak:
  - Pełny dostęp, w którym dozwolone są operacje takie jak: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie oraz wykonywanie

        - Odczyt, w którym dozwolone są operacje takie jak: kopiowanie i otwieranie. Niedozwolone są operacje takie jak: przenoszenie, zapisywanie, usuwanie oraz wykonywanie.
    - Funkcjonalność musi umożliwiać utworzenie listy zatwierdzonych urządzeń pamięci masowej USB.
    - Kontrola urządzeń musi umożliwiać blokowanie dostępu do wszystkich urządzeń pamięci masowej USB z wyjątkiem tych, które dodano do listy urządzeń zatwierdzonych. Dla tych urządzeń powinna umożliwiać przyznanie pełnego dostępu lub ograniczyć poziom dostępu.
    - System musi umożliwiać dowolną konfigurację treści powiadomień dla końcowego użytkownika

Kontrola Aplikacji

- Funkcjonalność typu application control (kontrola aplikacji) dla stacji końcowych użytkowników. Rozwiązanie powinno realizować co najmniej następujące funkcjonalności:
    - Funkcjonalność musi umożliwiać zdefiniowanie zestawu aplikacji które użytkownik końcowy będzie mógł uruchomić – pozostałe aplikacje powinny być blokowane.
    - Funkcjonalność musi zapewniać ochronę przed uruchamianiem niepożądanych lub nieznanych aplikacji (plików wykonywalnych, bibliotek DLL, aplikacji Windows, sterowników urządzeń, oraz innych przenośnych plików wykonywalnych (Portable Executable files).
    - Funkcjonalność musi zapewniać mechanizm analizy zagrożeń w czasie rzeczywistym bazujący na globalnej bazie reputacji plików.
    - Funkcjonalność w celu kontroli aplikacji musi wykorzystywać polityki zawierające zdefiniowane reguły z trzema metodami kontroli aplikacji:
        - Zezwól(Allow) – reguły zezwalające na uruchomienie określonych, wyspecyfikowanych aplikacji,
        - Blokuj (Block – reguły blokują określone, wybrane aplikacje lub aplikacje nie określone w regułach typu „Allow”,
        - Izolacja (Lockdown) – blokuje aplikacje dodane po zastosowaniu reguły typu „Lockdown” z możliwością użycia określonych warunków na zezwolenie uruchomienia aplikacji.

HOST IPS

- Funkcjonalność klasy Host IPS (Host Intrusion Prevention System) dla stacji końcowych użytkowników.
    - Funkcjonalność klasy Host IPS powinno chronić systemy użytkowników przed znanymi podatnościami za pomocą dostarczanych przez producenta sygnatur.
    - Funkcjonalność Host IPS powinno wykrywać skanowania portów, chronić przed atakami sieciowymi oraz wykorzystującymi znane podatności aplikacji oraz systemów operacyjnych.

Threat hunting

- System musi pozwalać na przeszukiwanie wszystkich danych zebranych z organizacji pod kątem różnych artefaktów
    - Wyszukiwanie ma być realizowane z jednego miejsca dla wszystkich źródeł
    - System musi pozwalać na wyszukiwanie po pełnej frazie (np. cała komenda) lub tylko fragmencie
    - 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.
    - W wyniku wyszukiwania system musi wskazywać linię czasu oraz powiązane ze zdarzeniem obiekty
    - Po zidentyfikowaniu obiektu system musi pozwalać na odtworzenie przebiegu zdarzenia w łańcuchu przyczynowo-skutkowym. System ma pokazywać powiązania pomiędzy poszczególnymi zdarzeniami w łańcuchu
    - System musi wyświetlać jak najpełniejsze dane odnośnie zdarzenia, w szczególności powinien określać atrybuty z poniższej listy (tam gdzie ma to zastosowanie):
        - Typ obiektu
        - Data utworzenia/zmiany
        - Nazwa procesu
        - Lokalizacja pliku
        - Komenda CLI
        - SHA-1
        - SHA-256
        - File MD5
        - Process ID
        - Podpis/certyfikat
        - Ważność podpisu/certyfikatu
        - Typ pliku
        - Czy powstał w wyniku zdalnego dostępu
        - Poziom integralności
        - Domena
        - URL
        - Nazwa punktu końcowego (Endpoint)
        - Adres IP punktu końcowego (Endpoint)
        - Adres MAC punktu końcowego (Endpoint)
        - Rodzaj i wersja systemu operacyjnego
        - Zalogowany użytkownik
        - Komunikacja sieciowa
            - Poziom ryzyka
            - Schemat ataku
            - Protokół (np. HTTP)
            - Metoda (np. GET)
            - Wskazanie źródła i celu połączenia (client->server)
            - Response code (np. 200 OK)

- MIME type (np. application/octet-stream)
- SHA-1/SHA-256
- Data i godzina wystąpienia
- Przebieg komunikacji w linii czasu
- Wskazanie miejsca, w którym zaobserwowano przesyłanie szkodliwego obiektu
- Hosty, na których zaobserwowano pliki ze szkodliwą zawartością, w tym zapisie sieciowym
- URL/domena
- Użytkownik
- Port

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

Incident response

- System w wyniku działań korelacyjnych musi tworzyć zagregowane alerty
- Każdy alert musi wskazywać ocenę pod kątem istotności oraz być klasyfikowany wg typu zagrożenia
- System musi wskazywać jaki zasięg ma dany alert – ile i jakie stacje końcowe/użytkownicy są powiązani z alertem
- System ma pozwalać na zarządzanie statusem alertu:
  - Nowy (New - status domyślny)
  - W trakcie realizacji (in progress)
  - Zamknięty (closed)
  - False Positive (closed – False Positive)
- System musi pozwalać na podejmowanie akcji w poszczególnych zdarzeniach:
  - Izolacja stacji końcowej
  - Uruchomienie skryptu
  - Nawiązanie zdalnego połączenia ze stację końcową poprzez zdalną powłokę bezpośrednio z konsoli systemu:
    - Przeglądanie zawartości stacji końcowej (listowanie plików/katalogów)
    - Wyświetlanie zmiennych środowiskowych
    - Wyświetlanie konfiguracji sieci
    - Wyświetlanie aktualnych połączeń sieciowych
    - Wyświetlanie listy procesów
    - Przeglądanie kluczy rejestrów i ich wartości
    - Wyświetlanie listy usług, wraz ze statusem
    - Wyświetlanie listy użytkowników
    - Zakończenie procesu
    - Usunięcie pliku/folderu
    - Pobranie pliku
- Wykonane operacje za pomocą zdalnej powłoki muszą być zarejestrowane w postaci logu wraz informacją na jakiej stacji i przez jakiego użytkownika zostały zrealizowane.
- System musi pozwalać na tworzenie listy obiektów do zablokowania/listy wyjątków

- Obiekty muszą być dystrybuowane do poszczególnych systemów podpiętych do systemu centralnego, w szczególności:
    - System do ochrony stacji końcowych
- Katalog obiektów do zablokowania/wyjątków:
    - Domena
    - Plik (SHA-1/SHA-256)
    - Adres IP
    - Adres nadawcy
    - URL
- Dla danego obiektu dodawanego do listy obiektów do zablokowania musi być możliwość zdefiniowania dodatkowo:
    - Poziomu ryzyka
    - Akcji (logowanie/blokada lub kwarantanna)
    - Ważności blokady

Specyfikacja technologiczna

- Sensor XDR dedykowany na stacje końcowe musi integrować się z poniższymi platformami OS:
    - Windows 11
    - Windows 10
    - Windows 8.1
    - Windows 7
    - Windows Server 2019 (64-bit)
    - Windows Server 2016 (64-bit)
    - Windows Server 2012 / 2012 R2 (64-bit)
    - Windows Server 2008 R2 (64-bit)
    - Red Hat Enterprise Linux 6 (64-bit)
    - Red Hat Enterprise Linux 7 (64-bit)
    - Red Hat Enterprise Linux 8 (64-bit)
    - CentOS Linux 6 (64-bit)
    - CentOS Linux 7 (64-bit)
    - CentOS Linux 8 (64-bit)
    - Ubuntu 16 (64-bit)
    - Ubuntu 18 (64-bit)
    - Ubuntu 20 (64-bit)
    - macOS Mojave (10.14) i nowsze
- System musi pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji końcowej system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą
- System musi być oparty o wydajny silnik analityczny pozwalający na pracę z danymi bez zbędnej zwłoki
- Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy)
- Producent musi dostarczyć zakres danych przetwarzanych w usłudze

- System musi posiadać certyfikat potwierdzający zgodność przetwarzania danych z obowiązującymi standardami i dobrymi praktykami np. ISO27001 oraz certyfikat określający wymagania dotyczące klientów oraz dostawców danych w chmurze, np.: ISO27017
- System musi umożliwiać intergracje z systemami firm trzecich za pomocą interfejsu programowania aplikacji API.

Analiza ryzyka

- System musi dla całej organizacji (wszystkich objętych ochroną zasobów) prezentować aktualną wartość ryzyka (co najmniej w skali 80 stopniowej) oszacowaną w oparciu o co najmniej:
    - Zebrane informacje o wykrytych na stacjach zdarzeniach bezpieczeństwa, jak detekcja niebezpiecznego kodu typu malware i inne.
    - Zebrane informacje o zagrożeniach na podstawie alarmów będących wynikiem uruchomienia reguł korelujących systemu XDR
    - Zebrane informacje o wykrytych anomaliach na kontach użytkowników oraz dla zasobów przekazujących dane telemetryczne do modułu analizy ryzyka.
    - Wykryte na stacjach podatności
- System musi dla całej organizacji (wszystkich objętych ochroną zasobów) prezentować historyczną wartość ryzyka i wyświetlać trend zmiany ryzyka w czasie. Zakres linii trendu musi obejmować co najmniej ostatnie 21dni.
- System musi mieć możliwość dokonywania analizy ryzyka dla poszczególnych zasobów, conajmniej:
    - Stacji roboczych, serwerów witualnych oraz fizycznych
    - systemów dostępnych z poziomu publicznego internetu
    - zasobów w chmurze dostarczanych przez największych dostawcych atakich usług jak: AWS, Azure, Google.
    - Kont użytkowników
    - Klastrów Kubernetes uruchominych w ramach usług dostawców chumurowych lub on-premisse.
    - Innych systemów tzw. niezażądzalnych wykrytych w dostarczanych danych telemetrycznych do modułu ryzyka.
- System musi dawać możliwość operatorowi dowolnego konfigurowania krytyczności danego zasobu, zmiany jego poziomu.
- W przypadku decyzji o zaakceptowaniu ryzyka dla danego zasobu system musi umożliwić zarejestrowanie takiego faktu i pomijać w wyliczaniu ryzyka dla całej organizacji.
- System musi udostępniać dane umożiwiające porównanie ryzyka dla całej organizacji do innych organizacji w podobnej branży lub geolokalizacji.
- System musi umożliwiać zbiorcze przedstawienie informacji o czynnikach, które składają się na aktualną ocenę ryzyka dla organizacji.

Wymagania funkcjonalne systemu wykrywania i ochrony przed zaawansowanymi atakami oraz atakami APT – sonda sieciowa

Rozwiązanie musi być dostarczone w formie SaaS, gdzie centralny serwer hostowany jest w chmurze i dostarczony przez producenta oferowanego rozwiązania jako usługa. Producent oferowanego rozwiązania jest odpowiedzialny za niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczanych jako usługa typu SaaS.

Rozwiązanie musi spełniać następujące minimalne wymagania funkcjonalne:

1. Ochrona sieci i rozwiązań teleinformatycznych przed zaawansowanymi atakami typu APT (Advanced Persistent Threat) mającymi na celu uniknięcie wykrycia przez obecne w infrastrukturze zamawiającego systemy zabezpieczające takie jak bramy pocztowe i webowe, systemy IPS/IDS czy oprogramowanie antywirusowe.
2. Rozwiązanie powinno zostać dostarczone jako dedykowane urządzenie fizyczne lub w postaci maszyny (maszyn) wirtualnej w środowisku serwerowym, takim jak: vMWare vSphere, KVM, Microsoft Hyper-V lub AWS.
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).
4. Rozwiązania powinno być dostępne z przepustowością min. 500 Mb/s z możliwością skalowania do 10000 Mb/s
5. Monitorowanie minimum 100 protokołów na pełnym zakresie portów bez potrzeby instalowania dodatkowych elementów systemu.
6. Rozwiązanie powinno móc współpracować z platformą klasy XDR (Extended Detection and Response) producenta oferowanego rozwiązania poprzez dostarczanie zawansowanej telemetrii zdarzeń z monitorowanego ruchu sieciowego takiej jak:
    a. Adresy IP (IPv4, IPv6)
    b. Porty
    c. URL-e
    d. Hasze plików (FileSHA1, FileSHA2)
    e. Domeny
    f. Nazwy plików
    g. Nazwy użytkowników
7. Rozwiązanie musi zapewniać detekcje zagrożeń na podstawie wbudowanych i aktualizowanych reguł przez producenta rozwiązania.
8. Rozwiązanie musi umożliwiać włączenie dostępu SSH, który umożliwi administratorowi zdalne logowanie się w celu zarządzania urządzeniam, wykonywania poleceń oraz kopiowania lub przesyłania plików do urządzenia za pomocą klienta SSH.
9. Rozwiązanie musi udostępniać skrypty demonstracyjne, w celu symulacji ataku i weryfikacji poprawności działania reguł detekcyjnych analizujących ruch z sondy sieciowej.
10. Rozwiązanie musi zapewniać możliwość pobrania plików zidentyfikowanych w telemetrii pochodzącej z sondy sieciowej w postaci skompresowanego i zabezpieczonego hasłem pliku.

Wymagania funkcjonalne dla systemu ochrony usług Office365 oraz Google

Przedmiotem zamówienia jest dostawa systemu ochrony dla pakietu Microsoft 365 przed zagrożeniami i atakami typu APT.

Wymagania funkcjonalne

- Rozwiązanie musi wykorzystywać usługę reputacji sieciowej do analizy i blokowania adresów URL, w szczególności musi wykorzystywać:
    - Statyczna listę reputacji, z możliwością dostrojenia czułości działania (np. najmniej agresywne, średnio agresywne, agresywne)
    - Dynamiczne skanowanie URL - dla nieznanych, nieistniejących jeszcze w bazie statycznej adresów
    - Analizę przy użyciu algorytmów widzenia komputerowego, pozwalająca wykryć i zablokować przypadki phishingu (wyłudzenia poświadczeń do serwisów Microsoft'u)
- Usługa reputacji ma umożliwiać analizę adresów URL pochodzących z treści wiadomości, a także z plików wymienianych jako załączniki oraz przez OneDrive, Sharepoint i czat Teams
- Rozwiązanie musi posiadać mechanizm ochrony przed wyciekiem danych (DLP) dla OneDrive, Teams, Sharepoint oraz Google Drive, umożliwiający co najmniej:
    - Blokowanie na podstawie predefiniowanych wzorców
    - Definiowanie własnych identyfikatorów danych z użyciem wyrażeń regularnych (regex)
    - Tworzenie reguł, z wykorzystaniem własnych oraz wbudowanych list słów kluczowych i identyfikatorów danych
    - Wykorzystania reguł DLP do monitorowania także ruchu poczty elektronicznej
    - Posiadający wbudowane polskie identyfikatory ochrony danych, przynajmniej dla:
        - Pesel
        - Numer Dowodu Osobistego
        - Numer rachunku bankowego
        - Numer telefonu
        - Blokowanie na podstawie listy statycznej słów kluczowych
- Rozwiązanie musi umożliwiać skonfigurowanie akcji jaka zostanie podjęta po wykryciu zagrożeń, w oparciu o ich kategorie:
    - Kwarantanna (musi być zintegrowana ze środowiskiem MS365 Zamawiającego)
    - Kasowanie
    - Przepuszczenie
    - Dla wiadomości email dodatkowo: ostemplowanie treści lub tematu, przeniesienie do folderu wiadomości-śmieci
- Rozwiązanie musi umożliwiać zdefiniowanie powiadomień o wykrytych zagrożeniach odrębnie dla użytkowników i administratorów systemu
- Rozwiązanie musi posiadać wbudowany mechanizm generowania raportów, możliwość szybkiej oceny stanu systemu dzięki specjalnej konsoli (dashboard)
- Rozwiązanie musi umożliwiać szybkie zidentyfikowanie najczęściej atakowanych adresów użytkowników
- Rozwiązanie musi umożliwiać integrację usługi ochrony ze środowiskiem XDR (eXtended Detection and Response)
    - Eskalacja najważniejszych zdarzeń bezpieczeństwa do alertów w dedykowanej konsoli XDR
    - Korelacja detekcji z poczty elektronicznej oraz ze stacji roboczych MS Windows

  - Możliwość blokowania korespondencji według nadawcy i message-id z poziomu konsoli XDR
  - Możliwość przeszukiwania archiwalnych danych telemetrycznych według nadawcy, odbiorcy, tematu oraz message-id
  - Automatyczne wyszukiwanie nowych zagrożeń w zgromadzonych danych telemetrycznych (IOC Sweeping)
  - Możliwość przedstawienia łańcucha ataku w formie graficznej, także po złożeniu zdarzeń z odpowiedniej stacji roboczej oraz systemu pocztowego
- Rozwiązanie musi mieć możliwość działania w trybie, w którym zostanie uruchomione skanowanie i zostaną wykonane skonfigurowane akcje przed dostarczeniem wiadomości odbiorcy poczty elektronicznej.