Poz. 1 Zakup i wdrożenie oprogramowania typu EDR (Endpoint Detection and Response), narzędzia służącego do wykrywania i reagowania na podejrzane aktywności na urządzeniach końcowych w infrastrukturze Uczelni

Wymagania dotyczące oferowanego oprogramowania:

- Zaoferowane oprogramowanie musi posiadać funkcjonalność antywirusa sygnaturowego
- Zaoferowane oprogramowanie musi być w wersji agentowej, tj. agent oprogramowania instalowany jest na komputerze użytkownika
- Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania w czasie rzeczywistym operacji wykonywanych na komputerze z zainstalowanym agentem przedmiotowego oprogramowania, np.. uruchomienie oprogramowania przeglądarki internetowej przez użytkownika
- Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania urządzeń pamięci masowej USB podłączanych do stacji końcowych i zezwalania lub blokowania użycia tych urządzeń. Wymagana jest też funkcjonalność wgrywania listy dopuszczonych urządzeń w organizacji, tak aby system automatycznie zezwalał na ich używanie
- W zakresie agenta, Zamawiający wymaga, aby funkcjonalności monitorowania zdarzeń na komputerze, ochrony USB oraz antywirusa sygnaturowego były zaimplementowane w jednym agencie
- Zamawiający wymaga, aby konsola zarządcza oprogramowania była umiejscowiona w chmurze publicznej na obszarze Unii Europejskiej. Aktualizacja konsoli należy do zadań producenta oprogramowania
- Zamawiający wymaga, aby z poziomu konsoli istniała możliwość wyświetlania triage alertowego dla nieprawidłowych zachowań (ataku, zagrożenia) wraz z liczbą pokazującą ważność (ang. severity)
- Zamawiający wymaga możliwości tworzenia polityk antywirusa nowej generacji sprawdzających pliki, aplikacje oraz ich działanie na stacji z zainstalowanym agentem pod względem minimum: potencjalnych ataków ransomware, komunikacji poprzez sieć komputerową, wykonywania skryptu typu „fileless", modyfikacji pamięci innego procesu, wywoływania nieznanego procesu
- Wymaga się, aby w przypadku zastosowania polityki bezpieczeństwa skonfigurowanej przez administratora, istniała możliwość zastopowania pojedynczego procesu danego oprogramowania (np. jedna instancja edytora tekstu stwarzająca zagrożenie) lub wszystkich procesów danego oprogramowania na raz (np. wyłączenie wszystkich instancji edytora tekstu pomimo faktu, że tylko jedna z nich powoduje niebezpieczeństwo)
- Zaoferowane oprogramowanie musi posiadać ekran pokazujący zbiorowo wykryte malware z możliwością dodania do listy zatwierdzonych (ang. approved), niedopuszczonych (ang banned) oraz możliwością usunięcia danego pliku ze środowiska

- Zaoferowanie oprogramowanie musi mieć możliwość zatwierdzania aplikacji (ang approved) i wyłączania ich z użytkowania (ang. banned list) w oparciu o hash, nazwę, położenie w drzewie katalogów na dysku oraz certyfikat
- Zaoferowane oprogramowanie musi mieć możliwość kwarantanny stacji na takiej zasadzie, żeby tylko administrator, z poziomu konsoli oprogramowania, mógł mieć dostęp do stacji, którą poddał kwarantannie
- Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia administratorów z przypisywaniem im granularnych uprawnień do poszczególnych funkcjonalności w konsoli oraz tworzenia grup administratorów
- Zaoferowane oprogramowanie musi wyświetlać zdarzenia, które zadziały się na chronionych stacjach do 30 dni wstecz, a w przypadku wykrytej anomalii/ataku/podatności do 180 dni wstecz
- Zamawiający wymaga, aby wszystkie opisane funkcjonalności były dostępne poprzez jednego agenta instalowanego na stacji końcowej
- Zaoferowane oprogramowanie musi w pełni współpracować z technologia VMware Instant Clones
- Zaoferowane oprogramowanie musi posiadać możliwość wystosowywania zapytań do stacji chronionych za pomocą języka zapytań SQL zaszytego w oprogramowaniu. Minimalne wymaganie dla zapytań to: stan RDP, stan Firewall, zapytanie o konkretne wpisy w rejestrze, użycia dysku, użycia RAM, wyszukiwanie plików na dyskach, błędy logowania, odnajdowanie pustych haseł, zainstalowane oprogramowanie
- Zaoferowane oprogramowanie musi posiadać dodatkową, uruchamianą dla danej stacji, bezpieczną konsolę, za pomocą której, po podłączeniu się do stacji, administrator może wykonywać między innymi: terminowanie procesu na stacji, listowanie procesów stacji, wgrywanie plików na stację, ściąganie plików ze stacji, uruchamianie poleceń, kasowanie plików na stacji
- Zamawiający wymaga, aby wszystkie opisane funkcjonalności były dostępne poprzez jednego agenta instalowanego na stacji końcowej
- Zamawiający wymaga, aby po włączeniu ochrony, bez dodatkowych działań wykonywanych przez administratora w konsoli, zarówno VMware vCenter jak i konsoli w chmurze publicznej wyświetlane były podatności dotyczące bezpieczeństwa (w oparciu o CVE) dla danego serwera wirtualnego, na którym ochrona została włączona. Wymagany jest podział podatności na minimum 3 kategorie ze względu na ważność/poziom zagrożenia. Zamawiający wymaga, aby maszyny wirtualne z włączoną ochroną były automatycznie skanowane pod względem podatności minimum raz na dobę. Dodatkowo, musi istnieć ręczne wywoływanie skanu podatności dla konkretnej maszyny wirtualnej
- Zamawiający wymaga, aby dostarczona licencja dawała możliwość instalacji oprogramowania na co najmniej 100 stacjach roboczych

Poz. 2 Zakup i wdrożenie oprogramowania zabezpieczającego sieć na poziomie poszczególnych maszyny wirtualnych

Wymagania dotyczące oferowanego oprogramowania:

- Zaoferowane oprogramowanie musi posiadać funkcjonalność bezpieczeństwa sieciowego zarządzanego oraz instalowanego w ramach jednego interfejsu graficznego (pojedynczej konsoli). Oprogramowanie musi mieć możliwość integracji poprzez plugin/dodatek z konsolą GUI VMware vSphere min. 7
- Zaoferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego (vNIC) w hipervisorze wirtualizacyjnym VMware ESX dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym segmencie sieci - VLAN) bez wynoszenia ruchu do fizycznych przełączników lub firewalli na zewnątrz hypervisora.
- Zaoferowane oprogramowanie musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego bezpośrednio w jądrze wirtualizatora VMware ESX umożliwiającego tworzenie polityk bezpieczeństwa w warstwach ISO OSI 2, 3 i 4 oraz warstwie 7 z identyfikacją aplikacji. Nie dopuszcza się stosowania filtracji ruchu sieciowego typu "reflexive".
- Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci VLAN i na tym samym fizycznym serwerze (hoście)
- Zaoferowane oprogramowanie do tworzenia reguł polityk bezpieczeństwa, musi umożliwiać wykorzystanie, oprócz parametrów takich jak adres IP, porty i protokoły, dodatkowych obiektów, m. in.: nazwa maszyny wirtualnej, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny.
- Zaoferowane oprogramowanie musi zapewniać możliwość wdrożenia polityk bezpieczeństwa bez żadnych zmian w sieci fizycznej.
- Zaoferowane oprogramowanie musi mieć możliwość wizualizacji przepływów sieciowych pomiędzy maszynami wirtualnymi w środowisku w którym zainstalowane jest oprogramowanie
- Zaoferowane oprogramowanie musi mieć możliwość przeanalizowania ruchu powiązanego z wybraną grupą maszyn wirtualnych w zadanym okresie czasu i na tej podstawie zarekomendowania reguł bezpieczeństwa polityki dla wybranej grupy maszyn wirtualnych
- Zaoferowane oprogramowanie musi dawać możliwość przeprowadzenia symulacji jak będzie wyglądała komunikacja w ramach danej aplikacji po zastosowaniu rekomendowanych reguł bezpieczeństwa.
- Zaoferowane oprogramowanie musi umożliwiać implementację zarekomendowanych reguł bezpieczeństwa po uprzednim zatwierdzeniu ich przez administratora systemu.
- Zaoferowane oprogramowanie musi obejmować usługę pobierania informacji o podejrzanych adresach IP w sieci Internet aby wdrożyć je jako element polityki bezpieczeństwa

- Zaoferowane oprogramowanie musi posiadać funkcjonalność REST API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
- Zaoferowanie oprogramowanie musi być sprzedawane wraz ze wsparciem technicznym na okres trwania subskrypcji/gwarancji, liczebność licencji: 8 procesorów po 24 rdzenie = 192 rdzeni
- Zaoferowane oprogramowanie musi mieć wbudowany silnik IDS/IPS (Intrusion Detection System/Intrusion Prevention System)
- IPS/IDS w zaoferowanym oprogramowaniu musi działać na podstawie silników: sygnaturowego, dekodera protokołu oraz wykrywania anomalii w ruchu sieciowym w sposób behawioralny. IPS/IDS w zaoferowanym oprogramowaniu musi działać w sposób granularny, tj. np. dawać możliwość przypisywania tylko polityki bazodanowej do tylko serwerów bazodanowych, czyli możliwości wykorzystania tylko kontekstu działania maszyny wirtualnej
- Silnik IDS/IPS musi działać w sposób rozproszony, tj instalowany bezpośrednio w jądrze wirtualizatora VMware zapewniając ochronę dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym segmencie sieci - VLAN) bez wynoszenia ruchu do na zewnątrz hypervisora.

Poz. 3 Aktualizacja wirtualizatora Vmware

Wymagania dla oprogramowania do wirtualizacji:

- Zaoferowane oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego
- W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego
- Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera
- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM
- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
- Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13, Asianux 4/7, Rocky Linux 8/9
- W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
- Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)
- Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi

- Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
- Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
- Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów
- Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
- Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
- Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
- Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi

- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
- Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
- Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
- Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).
- Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
- Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
- Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019
- Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
- Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016.

Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.

- Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność musi być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
- Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
- Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
- Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
- Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
- Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych
- Zaoferowane oprogramowanie podczas pracy w klastrze zarządzanym przez VMware vCenter musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej

- Zaoferowane oprogramowanie musi posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji AI i frameworków przeznaczonych dla kompleksowego rozwiązania AI;
- Zaoferowane oprogramowanie musi umożliwiać włączenie najnowszej generacji procesorów graficznych NVIDIA do swojego środowiska wirtualnego i skorzystanie z takich funkcji jak Multi-Instance GPU (MIG), pozwalające na współdzielenie cykli GPU przez wielu użytkowników.
- Zaoferowane oprogramowanie do wirtualizacji, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (Hypervisora), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne istniejące w tym klastrze. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją. Przełącznik rozproszony musi współpracować z protokołem NetFlow
- Zaoferowane oprogramowanie umożliwia uruchamianie poufnych kontenerów w serwerach opartych na procesorach EPYC ™ firmy AMD.
- Zaoferowane oprogramowanie do wirtualizacji, w ramach zaimplementowanego w nim rozproszonego przełącznika sieciowego, musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych
- Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
- Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej
- Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne

- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformami wirtualnej
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie ośmiu procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
- Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
- Zaoferowane oprogramowanie musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone
- Zaoferowane oprogramowanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych
- Zaoferowane oprogramowanie musi wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)
- Zaoferowane oprogramowanie musi wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2 i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA
- Zaoferowane oprogramowanie musi posiadać możliwość testowania wybranych serwerów (w szczególności tych, na których uruchomione są aplikacje przetwarzające dane wrażliwe i które mają dostęp do kluczy szyfrujących maszyny wirtualne) w celu weryfikacji, czy oprogramowanie jest autentyczne i nie zostało zmodyfikowane. Funkcjonalność ta musi działać w oparciu o chip TPM 2.0 zainstalowany w serwerze i odbywać się poza centralną konsolą zarządzającą (która sama jest maszyną wirtualną) wyłącznie w oparciu o sprzętowe źródło zaufania (hardware root of trust). Tylko serwery, które przejdą weryfikację mogą mieć dostęp do kluczy szyfrujących

- W przypadku pracy w oparciu o zarządzanie z centralnej konsoli zarządzającej, centralna konsola zarządzająca musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu jej aktualizacji na pozostałe podłączone do niej komponenty klastra oraz uruchomione na nim funkcjonalności. Musi również wspierać proces aktualizacji całego klastra poprzez automatyczne raportowanie kolejności aktualizacji podłączonych do niej komponentów i rekomendowanej ich wersji.
- Zaoferowane oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej wirtualizacją przez API i umożliwiać wykorzystanie jej jako szablonu przy kreowaniu kolejnych instancji centralnej konsoli zarządzającej oraz do weryfikacji poprawności konfiguracji zainstalowanych już instancji.
- Zaoferowane oprogramowanie musi wspierać funkcje DPU (ang. Digital Processing Unit) na zasadzie przekazywania obciążeń sieci wirtualnej z hipervisora do oddzielnej jednostki DPU zainstalowanej w serwerze fizycznym
- Zaoferowane oprogramowanie musi wspierać funkcjonalność bezpośredniego tworzenia kontenerów oraz klastrów Kubernetes na hiperwizorze (warstwie wirtualizatora) za pomocą dostarczonej konsoli zarządzającej Kubernetes (Kubectl)

Wymagania dla oprogramowania do zarządzania wirtualizacją:

- Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna musi działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtaul appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
- Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
- Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
- Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5
- Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na rozwiązaniu VMware vSphere
- Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu

wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz HTTP

- Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage)
- Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
- Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
- Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
- Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
- Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. high availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
- Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
- Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory
- Zaoferowane oprogramowanie musi wspierać zarządzanie nielimitowaną liczbą hostów wirtualizacyjnych
- Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska

Poz. 4 Aktualizacja oprogramowania firewalla sieciowego

Wymagania dotyczące oferowanego oprogramowania:

- System bezpieczeństwa musi zawierać bazę wiedzy eksperckiej, która pozwoli ocenić poprawność zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych i lokalnych w stosunku do potencjalnych wektorów ataków.
- Interfejs systemu bezpieczeństwa musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie zaimplementowanego składnika infrastruktury teleinformatycznej oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej.

- Dla zdarzeń zawierających adres IP interfejs musi umożliwiać wyświetlanie informacji o zasobach powiązanych z adresem.
- Zaimplementowany system odpowiedzialny za bezpieczeństwo teleinformatyczne musi zawierać szczegółową dokumentację pozwalają administrować systemem.
- System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników.
- System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń; wykryte zdarzenia będą priorytetyzowane w odniesieniu do ważności zasobów dla organizacji, które dotyczą np. wspomagania procesów.
- System musi umożliwiać korelację zdarzeń z anomaliami wykrywanymi w przepływach sieciowych oraz podatnościami pozyskanymi ze skanerów aplikacyjnych i bazy CVE.
- System musi umożliwiać określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym, bądź regułom wykonania.
- System musi umożliwiać wykorzystanie baz reputacyjnych w regułach bezpieczeństwa teleinformatycznego.
- System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi.
- System musi posiadać zestaw predefiniowanych scenariuszy obsługi.
- System musi pozwalać na tworzenie własnych scenariuszy obsługi.
- System musi pozwalać na przekazywanie aktywnych linków pomiędzy innymi zintegrowanymi systemami.
- System musi umożliwiać identyfikowanie kontekstu odbiegającego od normalnego zachowania użytkownika, korzystając z danych zewnętrznych Threat Intelligence, Active Directory.
- System musi umożliwiać archiwizację danych na zewnętrzne repozytoria.
- System musi umożliwiać współpracę z bazami danych MS SQL, My SQL, Oracle.
- System musi umożliwiać kontrolę dostępu do oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
- System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie.
- System musi być dostępny z poziomu dedykowanego klienta aplikacji oraz za pomocą dowolnej przeglądarki internetowej.
- Zaoferowany system musi gwarantować redundantność tj. zapewnić ciągłość pracy w przypadku awarii jednej instancji.

Szczegółowy zakres i wytyczne procesu wdrożenia systemu:

obszar analizy, zakładający przegląd organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji - obszar analizy ma na celu

identyfikację potencjalnych zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja – zakres musi zawierać kolejno:

- pracę z konsultantem,
- wytyczne dla Zamawiającego celem przygotowania środowiska do instalacji systemu,
- instalację systemu,
- zestawienie połączenia zdalnego,
- aktywację licencji,
- wstępną konfigurację,
- import ustawień z organizacji Zamawiającego w tym adresacji znaczących stref bezpieczeństwa wymaganych przez mechanizmy wykrywania (sieci serwerów, DMZ, LAN),
- przekierowanie logów z obecnych systemów Zamawiającego do nowego systemu,
- uruchomienie reguł wykrywania i reguł wykonywania zdarzeń,
- pasywną analizę transmisji sieciowej (ruch z/do serwerów, baz danych, poczty, kontrolerów),
- analizę podatności,
- zidentyfikowanie zagrożeń,
- rekomendacja zabezpieczeń,
- transfer wiedzy;

obszar detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowanych modułów - obszar detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń - zakres prac powinien uwzględniać kolejno:

- podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację,
- podłączenie zapór sieciowych,
- podłączanie mechanizmów dedykowanych do wykrywania incydentów bezpieczeństwa,
- podłączanie centralnego systemu reagowania na incydenty,
- w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji,
- adaptację reguł profilowych pozwalających na dostosowanie zdarzeń do wskazanych zasobów,
- obserwacja i doprecyzowanie postępu w tym wykluczenie/dodanie nowych reguł zdarzeń użytkowników/hostów,
- dostrojenie systemu w tym reguł priorytetyzacji zdarzeń i incydentów mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;

obszar reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia - obszar reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa - zakres prac powinien uwzględniać kolejno:

- pracę z konsultantem (wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian),
- konfigurację zespołów obsługi celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi,
- konfigurację mechanizmów powiadamiania.
- System bezpieczeństwa musi posiadać uruchomioną usługę piaskownicy, która daje możliwość wstrzymania dostarczenia treści do czasu uzyskania weryfikacji.

Systemy odpowiedzialne za bezpieczeństwo teleinformatyczne muszą realizować:

- Dynamiczne filtrowanie pakietów poprzez aktywny monitoring połączeń sieciowych, a następnie blokowanie niechcianych pakietów lub przepuszczanie dozwolonych. Ta funkcjonalność musi działać w protokole UDP, filtracja musi odbywać się poprzez regułę wykrywania pakietów komunikacyjnych przez określony czas i badania zarówno pakietów przychodzących, jak i wychodzących.
- System śledzi pakiety wychodzące, które żądają określonego rodzaju pakietów przychodzących i zezwala na przechodzenie pakietów przychodzących, o ile stanowią one dokładną odpowiedź.
- System monitoruje wszystkie sesje i weryfikuje wszystkie pakiety. Na przykład system przechwytuje informacje o stanie i kontekście pakietu i porównuje je z dominującymi danymi sesji. Jeśli identyczny wpis już istnieje, pakiet może przejść przez system. Jeśli dopasowanie nie zostanie znalezione, pakiet musi przejść pewne kontrole zasad. W tym czasie, jeśli pakiet spełnia wymagania polityki, system zakłada, że jest to połączenie zastępcze i przechowuje dane sesji w odpowiednich tabelach. Następnie pozwala pakietowi przejść. Jeśli pakiet nie spełnia warunków polityki, jest odrzucany;
- Funkcję serwera DNS oraz filtrowanie zapytań DNS lokalnie oraz w ruchu przechodzącym przez system;
- Inspekcję SSL/TLS dla http/2, smtp, ftp, pop3;
- Dwuskładnikowe uwierzytelnianie sprzętowe polegające na generowaniu unikalnych kodów cyfrowych na dedykowanym urządzeniu odrębnym od centrali systemu oraz urządzenia typu telefon, autoryzujących połączenia VPN;
- Mechanizm DLP, ochrona przed wyciekiem informacji;
- Oznaczanie metodą określania priorytetów dla ruchu różnego typu pakietów w sieci w zależności od kodu zapisanego w polu pakietu IP, który umożliwia przypisywanie różnemu typowi ruchu w sieci różnych poziomów jakości usług;
- Kontrolę pasma QoS oraz kształtowanie ruchu poprzez zarządzanie przepustowością i opóźnianie wybranych datagramów celem dostosowania do pożądanego profilu ruchu;
- Ochronę poczty, z wykorzystaniem smtp oraz pop3, przed niechcianymi informacjami; - Weryfikowanie zawartości stron internetowych; -
- Ochronę przed malware;
- Zarządzanie pasmem dla wybranych rodzajów stron internetowych;
- Ochronę przed atakami w czasie rzeczywistym, poprzez analizę polegającą na defragmentacji, łączeniu pakietów w strumienie danych, analizie nagłówków pakietów oraz analizie protokołów

aplikacyjnych lub polegającą na wyszukiwaniu w pakietach ciągów danych charakterystycznych dla znanych ataków sieciowych;

- Uruchamianie szyfrowanych wirtualnych sieci prywatnych, w których ochrona posiada kilka faz negocjowanych, przy czym jako pierwsze negocjowane są: algorytmy szyfrowania (DES, 3DES, AES 128 i 256 bit w trybie GCM), funkcje haszowania (MD5, SHA), rodzaj autentykacji (PSK, RSA), grupa 19, 20 Diffiego-Hellmana, czas ważności, następnie negocjowane są materiały do tworzenia kluczy i algorytmy do szyfrowania danych przesyłanych przez tunel; obsługa tych sieci prywatnych musi być zgodna ze standardami RFC2409 oraz RFC4306;
- Monitorowanie tuneli vpn i stałe utrzymywanie ich aktywności;
- Określenie pasma dla wybranego użytkownika bez względu na adres IP;
- Uruchamianie połączeń miejsce-miejsce oraz klient-miejsce; definiowane protokoły statycznego i dynamicznego przekierowywania adresów pomiędzy sieciami dla tuneli;
- monitorowanie tunelu szyfrowanego, a w przypadku niedostępności automatyczne uruchomienie zapasowego połączenia;
- Definiowanie statycznego przekierowywania adresów pomiędzy sieciami połączeń szerokopasmowych;
- Analizę tras równoważnych dla przekierowywania adresów pomiędzy sieciami na zasadzie Equal cost multi-path;
- Protokół używany do wykrywania błędów między dwoma urządzeniami sieciowymi połączonymi łączem, poprzez zapewnienie niskich narzutów na wykrywanie usterek nawet na nośnikach fizycznych, które nie obsługują wykrywania awarii jakiegokolwiek rodzaju, takich jak Ethernet, obwody wirtualne, tunele i MPLS Label Switched Paths, sesje w tym protokole muszą działać w trybie asynchronicznym (oba punkty końcowe okresowo wysyłają do siebie pakiety, jeśli pewna liczba tych pakietów nie zostanie odebrana, sesja kończy się) oraz w trybie na żądanie (pakiety nie są wymieniane po ustanowieniu sesji; zakłada się, że punkty końcowe mają inny sposób weryfikacji łączności między sobą);
- Filtrowanie tras w protokołach dynamicznego przekierowywania adresów pomiędzy sieciami;
- Monitoring adresu IP z danego interfejsu systemu, jeśli adresu nie ma, to system automatycznie usuwa go z tablicy przekierowywania adresów pomiędzy sieciami;
- Type of Service w nagłówkach IP;
- Reguły bazowego przekierowywania adresów pomiędzy sieciami polegające na wyborze trasy w zależności od adresu źródłowego;
- Trasowanie dynamiczne z wykorzystaniem PIM, BGP, OSPF w wersji 3, RIP w wersji 2, RIPng;
- Określanie maksymalnej i gwarantowanej ilości pasma oraz wskazanie priorytetu ruchu;
- Określanie pasma dla konkretnej aplikacji;
- Określenie ochrony malware dla wybranego zakresu ruchu oraz dla urządzeń mobilnych typu telefon;
- Blokowanie i oznaczanie zasobów, które są zaszyfrowane, uszkodzone lub wykraczają poza zdefiniowaną ochronę przed szkodliwym oprogramowaniem;
- sprawdzanie archiwów zagnieżdżonych z określeniem zakresu zagnieżdżeń, które będą dekompresowane celem sprawdzenia, dotyczy zasobów zip, rar;

- Mechanizm ochrony przed szkodliwym oprogramowanie musi działać na protokołach: http/s, ftp, pop3, imap, smtp, cifs, dwukierunkowy ftp również na portach niestandardowych;
- Usuwanie wrażliwej treści plików docx, xlsx, pdf;
- Dla połączeń szyfrowanych kapsułkowanie pakietów na protokół o niewielkim narzucie danych sterujących, nie więcej niż 8 bajtów, a następnie translację NAT;
- Metodę podtrzymywania nieaktywnych sesji IKE zgodną z RFC3706;
- Technikę dzięki której można zdefiniować które aplikacje i urządzenia mają kierować połączenie przez sieć VPN, a które z jej pominięciem;
- Technikę dla szyfrowanych wirtualnych sieci prywatnych gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki z wykorzystaniem html5 oraz z wykorzystaniem dedykowanego oprogramowania, kiedy to można zdefiniować które aplikacje i urządzenia mają kierować połączenie przez sieć VPN, a które z jej pominięciem;
- Translację adresów jeden do wielu oraz jeden do jeden oraz translację PAT;
- Dla protokołu SIP musi istnieć dedykowana brama proxy aplikacji, która wykonuje translację adresów i portów, alokację zasobów, kontrolę odpowiedzi aplikacji oraz synchronizację danych i sterowanie ruchem, kontrolować inicjowanie sesji aplikacji i chronić serwery aplikacji, uniemożliwiając lub przerywając połączenia, gdy jest to konieczne, w celu zapewnienia bezpieczeństwa;
- Korzystanie z zewnętrznych zasobów adresacji IP oraz kategorii stron internetowych przy tworzeniu polityki bezpieczeństwa;
- Dla funkcji ochrony sieci szerokopasmowej musi być dostępny harmonogram włączania i wyłączania reguł ochrony;
- Pełną zgodność z Amazon, Microsoft, Cisco, Google, OpenStack, Kubernetes, VMWare w zakresie budowania polityki kontroli dostępu;
- Logowanie do aplikacji chmurowej lub komercyjnego systemu logowania, w ramach logowania przekazywane są dane o dozwolonym i blokowanym ruchu, aktywności użytkowników, kondycji systemu; logowanie musi obejmować wszystkie moduły sieciowe i bezpieczeństwa i umożliwiać wyłączenie dla danej reguły;
- Dostęp do panelu administratora systemu musi być ograniczony wskazaniem określonego adresu IP oraz musi być podział ról administracyjnych, tak, aby dany administrator mógł zarządzać jedynie wybraną częścią systemu bez dostępu do obszarów zastrzeżonych;
- Dostęp poprzez API z pełną dokumentacją wykorzystania;
- Protokoły zarządzania zgodne z snmp 3;
- W celu bezpiecznego uwierzytelniania użytkowników system musi prowadzić weryfikacje tożsamości poprzez: statyczne hasła i definicje użytkowników zapisane lokalnie oraz w bazie LDAP, zewnętrzne bazy danych z wykorzystaniem RADIUS, RSA, SSO w integracji z Microsoft AD, RADIUS, API, SYSLOG, dla ruchu http musi być dostępny protokół SAML;
- Ochronę stron internetowych wykorzystując definiowane kategorie (po włączeniu dostęp będzie zabroniony) dynamic dns, proxy, phishing, malware; dodatkową możliwość dopisywania kategorii oraz konieczność wykonania akcji potwierdzającej przed otwarciem określonej strony; mechanizm blokowania niechcianych treści w wyszukiwarkach google, yahoo; wysyłanie

definiowanych komunikatów zwrotnych do użytkownika dla akcji podejmowanych przez filtr stron internetowych;

- Określanie dozwolonych protokołów na konkretnym porcie oraz zablokowanie pozostałych protokołów, chcących korzystać z tego portu;
- Kontrolę czynności wykonywanych w aplikacjach Facebook, Google, Microsoft;
- Blokowanie aplikacji na niestandardowych portach;
- Dostęp do bazy sygnatur z kategoriami aplikacji proxy, p2p, których uruchamianie jest szczególnie istotne dla bezpieczeństwa;
- Monitorowanie poprzez port SPAN;
- Funkcję zapory sieciowej w trybie transparentnym oraz z techniką przesyłania ruchu sieciowego, która wiąże się ze zmianą źródłowych/docelowych adresów protokołu internetowego, numerów portów UDP, pakietów protokołu internetowego podczas ich przepływu, sum kontrolnych (zarówno w pakiecie protokołu internetowego, jak i w segmencie UDP);
- Pełną aktywną, pasywną, klastrową dwuinstancyjność fizyczną oraz logiczną, z synchronizacją sesji pomiędzy instancjami, (zarządzaną łącznie przez ośmiu administratorów) w obszarach: przekierowania ruchu sieciowego/internetowego, szyfrowanych połączeń wirtualnych sieci prywatnych, kontroli i prewencji przeciwko włamaniom, kontroli aplikacji;
- Pełne wsparcie dla protokołów internetowych wersji 4 i 6 w obszarach: zapory sieciowej, ochrony warstwy aplikacji, protokołów dynamicznego przekierowywania ruchu sieciowego pomiędzy różnymi sieciami;
- Monitoring i wykrywanie uszkodzenia elementów programowych systemów zabezpieczeń oraz łączy sieciowych oraz stanu realizowanych połączeń wirtualnych sieci prywatnych;
- Przy włączonym zapisie logowania oraz włączonych usługach: zapory, kontroli i prewencji przed włamaniem, kontroli aplikacji, ochrony przed szkodliwym oprogramowaniem - przepustowość dla typowego jednoczesnego ruchu sieciowego: 3% youtube oraz twitter, 20% http, 5% ftp, 1% bazy danych Oracle, AOL oraz ssh, 6% Facebook, 11% osobno https, poczta Google oraz Yahoo, 8% Amazon - ma być nie mniej niż pięć gigabitów na sekundę dla kontroli i ochrony przed włamaniem, ponad trzy gigabity na sekundę dla zapory sieciowej, nie mniej niż trzy gigabity na sekundę dla ochrony przed zagrożeniami teleinformatycznymi;
- Przepustowość ponad dwadzieścia sześć gigabitów na sekundę przy ochronie pakietów 1504 oraz 512 bajtowych;
- Protokół sterowania transmisją z wydajnością nie mniej niż trzy miliony jednoczesnych sesji na sekundę przy zdolności nawiązywania ponad dwieście siedemdziesiąt pięć tysięcy nowych sesji na sekundę;
- Szyfrowane połączenia wirtualnych sieci prywatnych muszą odbywać się z wydajnością nie mniej niż trzynaście gigabitów na sekundę dla pakietów 512 bajtowych;
- Wydajność szyfrowanych protokołem SSL połączeń wirtualnych sieci prywatnych nie mniej niż dwa gigabity na sekundę, przy utrzymaniu ponad pięciuset jednoczesnych połączeń w trybie szyfrowania, gdzie oryginalny pakiet protokołu internetowego jest enkapsulowany i dodawany jest do niego nowy nagłówek tego protokołu;

- Funkcję kontroli aplikacji z wydajnością trzynaście gigabitów na sekundę, przy zapewnieniu przesyłania ponad szesnastu milionów pakietów na sekundę;
- Szyfrowanie połączeń sieci prywatnych z wykorzystaniem algorytmu SHA256 z wydajnością trzynaście gigabitów na sekundę przy pakietach 512 bajtowych;
- Ochronę przed zagrożeniami na zasadzie: analizy anomalii w protokołach sieciowych chroniąc przed atakamia DoS oraz DDoS; analizy zachowania aplikacji przeglądarkowych chroniąc przed atakami CSS, SQL, roboty, trojany, exploity; kontrolowania długości nagłówka, ilości parametrów adresów internetowych, ciasteczek; blokowania komunikacji C&C; włączania ochrony prewencyjnej tylko dla wybranych zakresów komunikacji sieciowej;
- Pełną zgodność z jednym ze standardów: ANSA, CGF, SERV, FCC, BSMI, VCC, ICSA w zakresie obsługi działania: technik ochrony na styku Internetu, szyfrowania protokołu internetowego, ochrony antywirusowej, zgodności z protokołem internetowym wersji 6, szyfrowania wirtualnych sieci prywatnych.

Zasady wsparcia gwarancyjnego w powyższym zakresie, udzielonego na przedmiot zamówienia:

- wykonawca zapewni fabryczne wsparcie wszystkich producentów, których składniki zostaną użyte do realizacji przedmiotu zamówienia;
- wsparcie, o którym mowa powyżej, ma zapewnić bez ponoszenia dodatkowych kosztów aktualizację wszystkich komponentów składających się na realizację przedmiotu zamówienia;
- wsparcie musi być zagwarantowane pisemnie na etapie składania ofert;
- jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi on mieć swoje regionalne przedstawicielstwo w Polsce i zadeklarować, że utrzyma je przez okres gwarancji;
- alternatywnie, jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi wyznaczyć pełnomocnika, który będzie ponosił odpowiedzialność przez okres gwarancji, w przypadku niedostępności wykonawcy;
- jeśli producentem systemu bezpieczeństwa nie jest wykonawca, to wsparcie o którym mowa powyżej, musi być zapewnione Zamawiającemu bezpośrednio od producenta, tzn. bez pośrednictwa wykonawcy, już na etapie dostarczenia przedmiotu zamówienia;
- w przypadku problemu lub wątpliwości w działaniu dowolnego składnika wdrożonego systemu, producent systemu zobowiązuje się do pisemnej odpowiedzi serwisowej w czasie 2 godzin, zaś w przypadku usterki – w czasie 15 minut, w tym celu producent systemu lub wykonawca (w porozumieniu z producentem) uruchomi dla Zamawiającego dedykowany portal przeglądowy i monitorujący działanie systemu, przy czym to uruchomienie nastąpi przed odebraniem przedmiotu zamówienia;

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

- Rozwiązanie musi zostać dostarczone w postaci platformy działającej w środowisku wirtualnym lub w postaci platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5,

6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

- System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.
- System musi być w stanie przyjmować minimum 5 GB logów na dzień.
- Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

- Podgląd logowanych zdarzeń w czasie rzeczywistym;
- Możliwość przeglądania logów historycznych z funkcją filtrowania;
- System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
  - Listę najczęściej wykrywanych ataków;
  - Listę najbardziej aktywnych użytkowników;
  - Listę najczęściej wykorzystywanych aplikacji;
  - Listę najczęściej odwiedzanych stron www;
  - Listę krajów , do których nawiązywane są połączenia;
  - Listę najczęściej wykorzystywanych polityk Firewall;
  - Informacje o realizowanych połączeniach IPSec.
- Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
- Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
- System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania.
- Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

W zakresie raportowania system musi zapewniać:

- Generowanie raportów co najmniej w formatach: PDF, CSV;
- Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników;
- Funkcję definiowania własnych raportów;
- Możliwość spolszczenia raportów;
- Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

W zakresie korelacji zdarzeń system musi zapewniać:

- Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany;
- Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa;
- Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne.

System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

- Malware,
- Aplikacje sieciowe,
- Email, IPS, Traffic,
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
- System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
- System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

Poz. 5 Aktualizacja oprogramowania firewalla poczty

Wymagania dotyczące oferowanego oprogramowania:

System musi zapewniać/mieć:

- zapewniać ochronę zarówno poczty przychodzącej jak i wychodzącej,
- zapobiegać próbom spoofingu, phisingu i spyware,
- zabezpieczać przed atakami typu DoS
- zabezpieczać pocztę wychodzącą, w skład której wchodzi ochrona antywirusowa, kontrola ilości wysłanych wiadomości przez użytkownika,
- zapewniać ochronę przed atakami typu DHA
- W ramach ważnego serwisu administrator ma możliwość zainstalowania skanera antywirusowego dla MS Exchange 2003/2007/2010.
- Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam.
- Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości wychodzących, wg której wiadomości mogą być blokowane lub przesyłane do kwarantanny.
- Analiza odcisku palca wiadomości (fingerprint), pozwalająca na zweryfikowanie wiadomości przychodzącej z bazą odcisków wiadomości zawierających spam, stworzonej przez producenta.
- Analiza obrazów dołączonych do wiadomości przy pomocy skanera OCR (Optical Character Recognition).
- Weryfikacja adresów URL zawartych w wiadomości z bazą danych znanych adresów URL zawierających spam. Możliwość blokowania, oznaczania, przenoszenia do kwarantanny takich wiadomości spamowych.
- możliwość korzystania z filtrów Bayesa.
- Możliwość określania maksymalnej ilości połączeń z danego adresu IP w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy zarówno poczty wychodzącej jak i przychodzącej.
- Możliwość określania maksymalnej ilości wysłanych wiadomości od danego nadawcy w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy poczty wychodzącej.
- Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.
- Możliwość ustawienia kwarantanny dla każdego użytkownika.
- Możliwość nadania uprawnień użytkownikom do zmiany własnych ustawień: włączenie/wyłączenie kwarantanny, włączenie/wyłączenie skanowanie antyspamowego, zmiany języka i częstotliwości wysyłanych powiadomień kwarantanny, dodawania adresów do osobistej białej/czarnej listy, zmiany ustawień osobistych filtru Bayes'

- Możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach przychodzących przeniesionych do kwarantanny: codziennie, raz w tygodniu lub nigdy.
- Możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach wychodzących od tego użytkownika przeniesionych do kwarantanny: codziennie, co tydzień, natychmiast lub nigdy.
- Możliwość ustawienia ilości miejsca na dysku przeznaczonej na kwarantannę dla poczty wychodzącej.
- Możliwość zdefiniowania w przypadku poczty wychodzącej jak długo wiadomości będą przechowywane w kwarantannie.
- Uwierzytelnianie nadawcy wiadomości na podstawie SPF (Sender Policy Framework).
- Uwierzytelnianie nadawcy wiadomości na podstawie mechanizmu DKIM (Domain Keys).
- Zapobieganie niepożądanym wiadomościom bounce z wykorzystaniem metody oznaczania nagłówków wiadomości wysyłanych przez oprogramowanie.
- Możliwość korzystania z dowolnych zewnętrznych baz RBL.
- Oprogramowanie ma zapewniać dostęp do baz reputacyjnych producenta, które zawierają listę znanych spamerów.
- Możliwość zdefiniowania wykluczeń ze skanowania antyspamowego dla wiadomości wychodzących/przychodzących ze określonego adresu IP lub zakresu adresów IP.
- Możliwość zdefiniowania akcji dla wiadomości przychodzących w przypadku gdy wiadomości zostały wysłane z określonego adresu IP lub określonej podsieci. Dostępne akcje w tym przypadku to: blokowanie, poddanie kwarantannie lub oznaczenie wiadomości jako spam.
- Możliwość zdefiniowania białej listy domen, subdomen.
- Możliwość zdefiniowania czarnej listy domen, subdomen. Wiadomości przychodzące z tych domen/subdomen mogą być blokowane, oznaczone jako spam lub przenoszone do kwarantanny.
- Możliwość określenia dla jakich domen chronionych przez oprogramowanie poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
- Możliwość określenia domen chronionych przez oprogramowanie, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
- Możliwość określenia dla jakich adresów email poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
- Możliwość określenia adresów email, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
- Możliwość blokowania wiadomości pochodzących z konkretnego kraju, w tym: Argentyna, Brazylia, Chile, Chiny, Kolumbia, Niemcy, Włochy, Rosja, Turcja.
- Możliwość tworzenia reguł pozwalających na blokowanie, przesyłanie do kwarantanny lub oznaczenia wiadomości jako spam wiadomości pochodzących z danego hosta.
- Produkt powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości posiadające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam.

- system ma umożliwiać korzystanie użytkownikom z dodatkowego pluginu do aplikacji Microsoft Outlook i Lotus Notes.
- Możliwość konfiguracji ilości dni przechowywania wiadomości w kwarantannie użytkownika.
- Możliwość uruchomienia SMTP over TLS zarówno dla połączeń wychodzących jak i przychodzących.
- Możliwość wymuszenia zgodności protokołu SMTP z RFC 821.
- Możliwość blokowania wiadomości które nie używają FQDN (fully-qualified domain name) w polu 'From' adresu.
- Kontrola zawartości załączników po:
- typie pliku, co najmniej następujące typy: MS Access, MS Excel, MS Word, Adobe PDF, MS PowerPoint, Windows exe, Windows Script. Skaner sprawdza również archiwa pod kątem obecności zdefiniowanych typów pliku,
- nazwie pliku lub rozszerzenia pliku, definiowane przez administratora,
- typie MIME pliku, definiowane przez administratora zgodnie ze standardem RFC.
- Dostępne akcje w przypadku kontroli załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
- poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
- Dostępne akcje w przypadku spakowanych, zabezpieczonych hasłem załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
- poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
- Możliwość tworzenia reguł, przy pomocy wyrażeń regularnych filtrujących wiadomości po temacie, nagłówku i treści wiadomości. Możliwość tworzenia takich reguł zarówno dla wiadomości przychodzącej jak i wychodzącej. Dostępne akcje mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
- poczta przychodząca: blokowanie, przeniesienie do kwarantanny, oznaczenie wiadomości, dodanie do białej listy,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie wiadomości, dodanie do białej listy, przekierowanie na inny serwer.
- Minimum 4 predefiniowane, stworzone przez producenta reguły poczty wychodzącej, filtrujące wiadomości po temacie, nagłówku i treści wiadomości.
- system ma zapewniać skanowanie antywirusowe poczty przychodzącej przy pomocy minimum 3 różnych silników antywirusowych działających jednocześnie.
- Weryfikacja odcisku wiadomości lub wirusa z bazą danych producenta, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie na urządzenia
- system ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur wirusów.

- system ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur antyspamowych.
- system ma być konfigurowany za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową.
- Interfejs administratora ma być dostępny co najmniej w języku polskim.
- Możliwość określenia czy administratorzy mają dostęp do interfejsu dostępnego przez przeglądarkę tylko poprzez protokół https.
- system ma mieć możliwość integracji z usługami katalogowymi LDAP oraz Active Directory przynajmniej do weryfikacji docelowych odbiorców przychodzących przesyłek pocztowych.
- system ma mieć możliwość skonfigurowania wirtualnych adresów IP do fizycznej karty sieciowej.
- system ma mieć możliwość konfigurowania tras statycznych.
- System ma mieć możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak: ping, telnet, dig, tcpdump, traceroute.
- system ma mieć możliwość uruchomienia bezpiecznego, szyfrowanego połączenia z działem wsparcia technicznego producenta na życzenie administratora.
- system ma mieć możliwość tworzenia kopii zapasowej konfiguracji urządzenia, ustawień wszystkich lub wybranych użytkowników.
- Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb.
- Możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb.
- Możliwość tworzenia kopii zapasowej baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników.
- Możliwość skonfigurowania adresu email, na który będą przesyłane kopie każdej wiadomości przychodzącej lub wychodzącej.
- System ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).

Gwarancja/usługi serwisowe:

- Oferowane oprogramowanie musi zawierać co najmniej roczną gwarancję producenta.
- W czasie trwania gwarancji zamawiający ma prawo do wykonywania aktualizacji oprogramowania.
- W czasie trwania gwarancji zamawiający ma prawo do bezpłatnego dostępu do wszystkich aktualizacji, baz oraz sygnatur niezbędnych do prawidłowej pracy oprogramowania.
- W czasie trwania gwarancji zamawiający ma dostęp do wsparcia technicznego producenta świadczonego w systemie 24 godziny/dobę 7 dni w tygodniu.
- Zaoferowana usługa wsparcia serwisowego dla oferowanego oprogramowania musi być świadczona przez wyłącznie jeden podmiot lub organizację reprezentującą jeden podmiot na każdym etapie procesowania zgłoszenia. W łańcuchu obsługi zgłoszenia serwisowego, Zamawiający wyklucza możliwość przekazywania zgłoszeń serwisowych pomiędzy różnymi podmiotami. Zamawiający wyklucza również możliwość wykupienia usługi serwisowej przez Wykonawcę u partnera typu OEM (ang. Original Equipment Manufacturer) producenta przedmiotowego oprogramowania.
- Zaoferowana usługa wsparcia musi zapewniać poufność komunikacji na poszczególnych etapach procesowania zgłoszenia. Nie dopuszcza się procesowania zgłoszeń serwisowych w systemach informatycznych nie zarządzanych przez producenta zaoferowanego oprogramowania.
- Opis zaoferowanej usługi wsparcia serwisowego musi być dostępny na oficjalnej stronie internetowej producenta przedmiotowego oprogramowania.

Prace wdrożeniowe:

Prace wdrożeniowe nie mogą powodować zakłóceń w ciągłej pracy aktualnie działających systemów w infrastrukturze zamawiającego. Należy dostarczyć wszystkie (nawet jeśli nie opisano powyżej) usługi, licencje i składniki oprogramowania, aby zapewnić uzyskanie opisanych funkcjonalności.

Szkolenie:

Wykonawca przeprowadzi 2 dniowe szkolenie (16 godz. dydaktycznych) dla 3 administratorów.