

Załącznik nr 1 do umowy

Szczegółowy opis przedmiotu zamówienia

Informacje ogólne

Jeżeli w opisie przedmiotu zamówienia Zamawiający wskazuje znaki towarowe, patenty lub pochodzenie, źródła lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę – Zamawiający zgodnie z art. 99 ust. 5 ustawy PZP, dopuszcza oferowanie rozwiązań równoważnych.

Zgodnie z art. 101 ust. 4 ustawy PZP, w sytuacji gdy w opisie przedmiotu zamówienia zawarto odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy PZP, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy „lub równoważne”.

Zakup i wdrożenie systemu kompleksowej ochrony sieci teleinformatycznej Urzędu.

W celu podniesienia bezpieczeństwa organizacji, Urząd Miasta Knurów planuje zakup i wdrożenie systemu sieciowego odpowiadającego za kompleksową ochronę i nadzorowanie ruchu w sieci teleinformatycznej Urzędu, łączący funkcje zapory sieciowej, systemu analizy ruchu wykrywania intruzów, prób ataków i podejrzanych aktywności sieciowych takich jak IDS (ang. Intrusion Detection System) lub IPS (ang. Intrusion Prevention System) wraz z minimum dwuletnim wsparciem technicznym. Planowane jest również utrzymanie wsparcia technicznego w kolejnych latach.

1. System bezpieczeństwa chmur publicznych lub prywatnych - wymagania podstawowe

1.1. System bezpieczeństwa musi pozwalać na uruchomienie w postaci Appliance VM w co najmniej poniższych chmurach publicznych oraz prywatnych:

- a) AWS
- b) Azure Virtual WAN
- c) Aviatrix
- d) Equinix
- e) Google Cloud
- f) VMware Cloud
- g) VMware ESXi
- h) VMware NSX-T 4.1
- i) IBM Cloud
- j) KVM/OpenStack/Nutanix AHV
- k) Oracle Private Cloud

1.2. System bezpieczeństwa musi działać w architekturze rozproszonej tzn. takiej w której komponenty odpowiadające za zarządzanie systemem oraz wymuszanie polityki bezpieczeństwa działają na dedykowanych platformach.

1.3. W ramach komponentu zarządzania systemem Zamawiający wymaga minimum następujących funkcjonalności:

- a) centralne zarządzanie polityką bezpieczeństwa (w zakresie polityki dostępowej oraz ochrony przed zagrożeniami) na wszystkich zarządzanych urządzeniach typu Appliance VM,
- b) funkcja serwera logów pozwalająca na centralne przechowywanie oraz indeksowanie logów pochodzących z zarządzanych urządzeń UTM lub Appliance VM,

- c) funkcja korelacji oraz wykrywania incydentów bezpieczeństwa – wykrywanie oraz raportowanie incydentów bezpieczeństwa na bazie logów pochodzących z zarządzanych urządzeń,
 - d) moduł raportowania,
- 1.4. Zamawiający wymaga, aby komponenty odpowiedzialne za zarządzanie systemem działały w architekturze pozwalającej na rozdzielenie funkcji zarządzania polityką bezpieczeństwa oraz funkcji serwera logów/korelacji zdarzeń/raportowania pomiędzy minimum dwie osobne platformy sprzętowe lub wirtualne. Każda platforma – niezależnie fizyczna czy wirtualna - powinna zapewniać minimalnie 1TB powierzchni dyskowej.
 - 1.5. Zamawiający wymaga, aby komponenty odpowiedzialne za wymuszanie polityki bezpieczeństwa dostarczone zostały w formie dedykowanych maszyn wirtualnych wspierających rozwiązania wirtualizacji opisane w punkcie 1.1.
 - 1.6. Komunikacja pomiędzy wszystkimi komponentami systemu bezpieczeństwa musi być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych.
 - 1.7. Zamawiający zobowiązuje Wykonawcę do potwierdzenia, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowiło naruszenia majątkowych praw autorskich osób trzecich, w szczególności Wykonawca nie może zaoferować sprzętu i oprogramowania, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
 - 1.8. Zamawiający wymaga, aby dostarczony system zabezpieczeń był produktem o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej 36 miesięcy z rzędu.
 - 1.9. Zamawiający wymaga, aby wszystkie określone w niniejszym dokumencie funkcje systemu były realizowane w aktualnie dostępnych komercyjnie urządzeniach oraz wersjach oprogramowania.
 - 1.10. Zamawiający wymaga, aby elementy systemu zostały dostarczone ze stabilną wersją oprogramowania. Oznacza to, iż rozwiązanie (urządzenia + oprogramowanie) musi być dostępne na rynku nie krócej niż 3 miesiące od daty ogłoszenia postępowania przetargowego.
 - 1.11. System bezpieczeństwa musi zostać dostarczony z zestawem licencji pozwalających na realizację następujących funkcjonalności przez okres min. 2 lat:
 - a) funkcja firewall,
 - b) wykrywanie i przeciwdziałanie próbom włamań (IPS),
 - c) tworzenie reguł polityki bezpieczeństwa z wykorzystaniem definicji konkretnych aplikacji (kontrola aplikacji),
 - d) tworzenie reguł polityki bezpieczeństwa z wykorzystaniem kategorii URL,
 - e) wykrywanie stron typu “web phishing”,
 - f) ochrona antywirusowa,
 - g) wykrywanie i blokowanie komunikacji z sieciami botnet,
 - h) wykrywanie i blokowanie komunikacji DNS wykorzystywanej do transportu/infiltracji danych,
 - i) tworzenie reguł polityki w oparciu o tożsamość użytkownika (możliwość korelacji tożsamości użytkowników z wykorzystywanym adresem IP), obiektów chmur publicznych i prywatnych (nazwy maszyn, tagi etc.),
 - j) inspekcja zawartości danych transportowanych w komunikacji sieciowej,
 - k) wykonywanie inspekcji ruchu szyfrowanego,
 - l) możliwość realizacji połączeń IPSec VPN,
 - m) wykrywanie urządzeń typu IOT,
 - n) możliwość sterowania ruchem do Internetu oraz ruchem S2S VPN wykorzystując nadmiarowe połączenia fizyczne ISP WAN oraz ISP MPLS poprzez technologię SDWAN.

Funkcjonalność opisana w pt. 1.11 jest zachowana po okresie obowiązywania licencji (pt. 1.11) na ostatnich pobranych bazach i aktualizacjach.

2. Moduł zarządzania

2.1. Wymagania funkcjonalne

- 2.1.1. Moduł zarządzania musi mieć możliwość zarządzania minimum pięcioma punktami wymuszania polityki bezpieczeństwa.
- 2.1.2. Moduł zarządzania musi mieć możliwość uruchomienia osobnego serwera raportującego dla minimum pięciu systemów jakimi zarządza system centralnego zarządzania.
- 2.1.3. Moduł zarządzania musi umożliwiać jednoczesną pracę wielu administratorów - w tym także jednoczesną pracę w ramach pojedynczej polityki bezpieczeństwa.
- 2.1.4. Moduł zarządzania musi zapewniać możliwość tworzenia wielu różnych polityk bezpieczeństwa oraz umożliwiać ich przypisanie do poszczególnych urządzeń zarządzanych z poziomu serwera.
- 2.1.5. Moduł zarządzania musi umożliwiać tworzenie modułowej polityki bezpieczeństwa. System musi umożliwiać współdzielenie modułów (zestawów reguł polityki bezpieczeństwa) pomiędzy różnymi politykami bezpieczeństwa.
- 2.1.6. Moduł zarządzania musi posiadać mechanizmy automatycznej weryfikacji spójności i niesprzeczności implementowanej polityki bezpieczeństwa przed zainstalowaniem jej na urządzeniach typu Appliance VM lub UTM.
- 2.1.7. Moduł zarządzania musi posiadać mechanizmy pozwalające na weryfikację poprawności działania nowej wersji polityki bezpieczeństwa po jej uruchomieniu na urządzeniu UTM lub Appliance VM oraz możliwość automatycznego powrotu do poprzedniej wersji w przypadku stwierdzenia nieprawidłowości na bazie zestawu testów utworzonych przez administratora- np. brak dostępu do wybranych usług powstały w wyniku błędu administratora.
- 2.1.8. Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa, a także opcję cofnięcia konfiguracji do wybranej wersji.
- 2.1.9. Moduł zarządzania musi zapewniać możliwość uwierzytelniania administratorów za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych.
- 2.1.10. Moduł zarządzania musi zapewniać możliwość definiowania szczegółowych zestawów uprawnień dla poszczególnych administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkownikami itp.).
- 2.1.11. Moduł zarządzania musi posiadać mechanizmy zapewniające rozliczalność zmian konfiguracyjnych wykonanych przez poszczególnych administratorów w formie generowania i przechowywania logów audytowych. Logi muszą zawierać minimum informacje o tożsamości administratora oraz czasie i zakresie wykonywanych zmian.
- 2.1.12. Moduł zarządzania musi posiadać mechanizmy centralnego zarządzania licencjami dla wszystkich komponentów wchodzących w skład systemu bezpieczeństwa (serwery logów, serwer korelacji zdarzeń i raportowania, zapory sieciowe).
- 2.1.13. Moduł zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych urządzeń takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa.
- 2.1.14. Moduł zarządzania musi dostarczać mechanizmy pozwalające na graficzne prezentowanie statystyk ruchu sieciowego, przetwarzanego przez zarządzane zapory sieciowe. Dostępne statystyki obejmują minimum informacje o najczęściej wykorzystywanych usługach sieciowych, najczęstszych źródłach transmisji, najczęstszych adresach docelowych, aktywnych i nieaktywnych tunelach IPsec VPN (site-to-site oraz remote access).
- 2.1.15. Moduł zarządzania musi posiadać dedykowane API umożliwiające automatyzację czynności administracyjnych. Mechanizm API powinien umożliwiać minimum wykonanie następujących czynności:

- a) tworzenie, edycja oraz usuwanie obiektów sieciowych i usług,
 - b) tworzenie, modyfikowanie oraz usuwanie reguł polityki bezpieczeństwa oraz reguł NAT,
 - c) instalacja polityki bezpieczeństwa,
 - d) zarządzania kontami administratorów systemu,
- 2.1.16. Moduł zarządzania musi realizować funkcję serwera logów, w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych zapór sieciowych. W ramach funkcji serwera logów muszą istnieć wbudowane mechanizmy ochrony przestrzeni dyskowej przed przepełnieniem. Mechanizm powinien umożliwiać wykonywanie różnych akcji systemu w zależności od poziomu zajętości dysku. Możliwe akcje to minimum wysyłanie alertów do administratorów oraz automatyczne usuwanie najstarszych plików logów.
- 2.1.17. Moduł zarządzania musi posiadać mechanizmy pozwalające na implementację rozwiązania wysokiej dostępności, w ramach której możliwe jest dodanie zapasowego serwera zarządzania oraz uruchomienie automatycznej synchronizacji konfiguracji polityk bezpieczeństwa. Dostarczenie zapasowego serwera zarządzania nie jest wymagane w ramach postępowania.
- 2.1.18. Moduł zarządzania musi mieć możliwość wykrywania incydentów bezpieczeństwa na bazie logów pochodzących z minimum pięciu zarządzanych urządzeń.
- 2.1.19. Moduł zarządzania musi pozwalać na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych bez konieczności definiowania wartości dla poszczególnych atrybutów (tzw. freetext/full-text search).
- 2.1.20. Moduł zarządzania musi pozwalać na grupowanie wyników wyszukiwania logów/incydentów bezpieczeństwa według określonych atrybutów (minimum typ incydentu, zasoby, nazwa użytkownika).
- 2.1.21. Moduł zarządzania musi umożliwiać wykonywanie analizy incydentów bezpieczeństwa od poziomu ogólnego do szczegółowych logów odpowiedzialnych za wygenerowanie zdarzenia (tzw. drill-down).
- 2.1.22. Moduł zarządzania musi umożliwiać administratorom tworzenie własnych raportów oraz widoków (formatka prezentująca określony podzbiór danych w formie zdefiniowanej przez administratora), a także modyfikowanie raportów i widoków dostarczonych razem z systemem.
- 2.1.23. Moduł zarządzania musi umożliwiać graficzną prezentację danych (logi/incydenty bezpieczeństwa) za pomocą interaktywnych pasków, wykresów kołowych i czasowych.
- 2.1.24. Moduł zarządzania musi umożliwiać filtrowanie logów/incydentów bazując na parametrach takich jak: aplikacja, źródłowy i docelowy adres IP, usługa, typ zdarzenia, istotność ataku, kraj pochodzenia itd.
- 2.1.25. Moduł zarządzania musi posiadać możliwość budowania własnych raportów przez administratorów w trybie na żądanie oraz zgodnie z zadanym harmonogramem.
- 2.1.26. Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF oraz Microsoft Excel. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców.
- 2.1.27. Moduł zarządzania musi posiadać możliwość tworzenia niestandardowych reguł korelacji zdarzeń bezpieczeństwa.
- 2.1.28. Moduł zarządzania musi posiadać możliwość konfigurowania automatycznych reakcji na wykryte incydenty bezpieczeństwa - minimum w postaci wysłania wiadomości e-mail, wygenerowanie SNMP trap lub uruchomienie skryptu.

3. Zapory sieciowe

- 3.1. Ogólne (redundancja/tryby pracy)
- 3.1.1. Urządzenia pełniące rolę zapór sieciowych muszą posiadać możliwość pracy w klastrze w trybie Active-Standby lub Active-Active. Mechanizm klastrowania musi zapewniać funkcję synchronizacji informacji o stanie połączeń sieciowych pomiędzy urządzeniami wchodzącymi w skład klastra.

- 3.1.2. Mechanizm klastrowania działający w trybie Active-Active musi wspierać komunikację asynchroniczną przechodzącą przez urządzenia wchodzące w skład klastra. Decyzja o ruchu wychodzącym i powrotnym wykonywana jest w oparciu o routing dynamiczny.
- 3.1.3. Interfejsy zapory sieciowej muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (monitoring).
- 3.1.4. Tryb pracy interfejsu zapory sieciowej musi być ustalany w konfiguracji interfejsu sieciowego, a zaporą musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
- 3.1.5. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 1024 znaczników VLAN w trybie Gateway oraz 4096 znaczników w trybie wirtualnych systemów.
- 3.1.6. Zapora sieciowa musi pozwalać na podział platformy na mniejsze logiczne konteksty,
- 3.1.7. Zapora sieciowa musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF (v2 oraz v3).
- 3.1.8. Zapora sieciowa musi posiadać możliwość pracy w trybie serwera DHCP oraz DHCP relay.
- 3.1.9. Zapora sieciowa musi być zgodna z poniższymi standardami (RFC) dotyczącymi IPv6:
 - a) RFC 1981 Path Maximum Transmission Unit Discovery for IPv6,
 - b) RFC 2460 IPv6 Basic specification,
 - c) RFC 2464 Transmission of IPv6 Packets over Ethernet Networks,
 - d) RFC 4007 IPv6 Scoped Address Architecture,
 - e) RFC 4193 Unique Local IPv6 Unicast Addresses,
 - f) RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – wsparcie dla tuneli 6w4,
 - g) RFC 4443 ICMPv6,
 - h) RFC 4862 IPv6 Stateless Address Auto-configuration,

3.2. Firewall

- 3.2.1. Moduł Firewall musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanie aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu.
- 3.2.2. Polityka zabezpieczeń modułu firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzania pasmem.
- 3.2.3. Moduł firewall musi posiadać możliwość raportowania ilości „trafień” wybranej reguły polityki bezpieczeństwa do serwera zarządzania. Musi istnieć możliwość prezentowania liczby trafień dla reguł w wybranych okresach czasu, minimum w okresie 1 dnia, 7 dni oraz miesiąca.
- 3.2.4. Moduł firewall musi pozwalać na konfigurację reguł polityki bezpieczeństwa z uwzględnieniem okresu czasu w jakim dana reguła będzie aktywna (egzekwowana). Definicja okresu czasu w ramach którego dana reguła jest aktywna powinna uwzględniać następujące parametry: data i/lub godzina startu, data i/lub godzina zakończenia oraz rekurencyjność.
- 3.2.5. Moduł firewall musi posiadać możliwość konfiguracji reguł polityki bezpieczeństwa w oparciu o tożsamość użytkownika (identity firewall).
- 3.2.6. Moduł firewall musi domyślnie działać zgodnie z zasadą blokowania całego ruchu sieciowego, poza tym który jest zdefiniowany w regułach polityki bezpieczeństwa i wskazany jako dozwolony.
- 3.2.7. Rozwiązanie musi pozwalać na kontrolę przynajmniej 150 predefiniowanych usług/protokołów.
- 3.2.8. Moduł firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

3.3. Moduł przeciwdziałania próbom włamań (IPS)

- 3.3.1. Moduł IPS musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
- 3.3.2. Moduł IPS musi posiadać jednocześnie możliwość pracy zarówno w trybie pasywnym (Detect) jak i aktywnym (z możliwością blokowania ruchu).
- 3.3.3. Moduł IPS musi dokonywać inspekcji całych sesji/połączeń. Nie dopuszcza się rozwiązań określających bezpieczeństwo sesji poprzez szcztątkową analizę ruchu podczas ustanawiania sesji.
- 3.3.4. Moduł IPS musi zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
 - a) sygnatury ataków opartych na exploitach,
 - b) reguły oparte na zagrożeniach,
 - c) mechanizm wykrywania anomalii w protokołach,
- 3.3.5. Moduł IPS musi mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szeroki zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
- 3.3.6. Moduł IPS musi posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia oraz mieć możliwość zapisywania pakietów generujących zagrożenie.
- 3.3.7. Moduł IPS musi posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji.
- 3.3.8. Moduł IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera aktualizacji w sposób uniemożliwiający ich modyfikację podczas przesyłania pomiędzy serwerem aktualizacji oraz serwerem zarządzania/zaporą sieciową.
- 3.3.9. Moduł IPS musi zapewniać mechanizm zarządzania wersjami bazy sygnatur oraz umożliwiać powrót do wybranej wersji.
- 3.3.10. Moduł IPS musi posiadać mechanizm automatycznej aktywacji sygnatur minimum w oparciu o następujący zestaw parametrów: poziom zagrożenia, wpływ na wydajność urządzenia, dokładność identyfikacji zagrożenia.
- 3.3.11. Moduł IPS musi zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie i być zarządzany tylko poprzez system centralnego zarządzania za pomocą szyfrowanego połączenia.
- 3.3.12. Moduł IPS musi zapewniać możliwość obsługi reguł Snort.
- 3.3.13. Moduł IPS musi zapewniać możliwość detekcji i blokowania ataków i zagrożeń opartych na protokole IPv6.
- 3.3.14. Moduł IPS musi pozwalać na objęcie ochroną protokołów SCADA bez potrzeby zakupu dodatkowych licencji.
- 3.3.15. Moduł IPS musi pozwalać posiadać możliwość aktywowania ochrony dla wybranych zasobów definiowanych minimum w postaci adresów hostów, adresów sieci oraz zakresów adresów IP. Nie jest dopuszczalne, aby moduł IPS uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
- 3.3.16. Moduł IPS nie może posiadać możliwości ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu. Ręcznie tworzone reguły IPS mają być dostarczane poprzez system centralnego zarządzania.
- 3.3.17. Moduł IPS musi posiadać programowy mechanizm pozwalający na wyłączenia ochrony IPS w przypadku wysokiego obciążenia procesora lub pamięci operacyjnej zapory sieciowej. Wartości aktywujące mechanizm muszą być konfigurowalne przez administratora systemu.
- 3.3.18. Moduł IPS musi posiadać mechanizmy wykrywania i blokowania operacji tunelowania ruchu w ramach innych protokołów, np. DNS tunneling.

3.4. Moduł kontroli aplikacji

- 3.4.1. Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 10000 pozycji. Baza modułu powinna być dostępna do weryfikacji online.
- 3.4.2. Moduł kontroli aplikacji powinien pozwalać na granularną kontrolę przynajmniej 255000 aplikacji.
- 3.4.3. Moduł kontroli aplikacji musi posiadać mechanizm ograniczenia użycia pasma dla poszczególnych aplikacji niezależnie dla każdego kierunku przepływu danych (download oraz upload)
- 3.4.4. Moduł kontroli aplikacji musi posiadać możliwość współpracy z modułem analizy treści w zakresie wykrywania i blokowania przesyłania określonych typów danych (np. nr kart kredytowych) oraz określonych typów plików (np. csv, pdf i inne) w ramach zidentyfikowanej aplikacji. W przypadku, kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa.
- 3.4.5. Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej aplikacji.
- 3.4.6. Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowanie użytkowników do stron umieszczonych na zewnętrznych serwerach.
- 3.4.7. System musi umożliwiać administratorom tworzenie sygnatur nowych aplikacji za pomocą dedykowanego oprogramowania dostępnego w ramach licencji na moduł kontroli aplikacji.
- 3.4.8. Moduł kontroli aplikacji musi automatycznie identyfikować/wykrywać aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.

3.5. Moduł identyfikacji

- 3.5.1. Moduł identyfikacji musi umożliwiać uzyskiwanie informacji o tożsamości użytkowników z następujących źródeł:
 - a) integracja z usługą katalogową Microsoft Active Directory,
 - b) integracja z usługą AWS – pobranie nazw obiektów oraz tagów,
 - c) integracja z usługą Azure – pobranie nazw obiektów oraz tagów,
 - d) integracja z usługą Google Cloud – pobranie nazw obiektów oraz tagów,
 - e) integracja z usługami VMware Vcenter, NSX-T 4.1 i niższych – pobranie nazw obiektów oraz tagów,
 - f) integracja z usługą Cisco ISE,
 - g) identyfikacja w portalu www (captive portal),
 - h) identyfikacja z wykorzystaniem dedykowanego agenta instalowanego na stacji użytkownika,
 - i) integracja z serwerem RADIUS,
 - j) integracja z serwerem Syslog,
 - k) połączenia remote access VPN,
 - l) identyfikacja obiektów w chmurach publicznych oraz prywatnych (punkt 1.1) poprzez ich nazwy lub tagowanie.
- 3.5.2. Moduł identyfikacji użytkowników we współpracy z usługą Microsoft Active Directory musi umożliwiać pozyskiwanie informacji o grupach, do których należy zidentyfikowany użytkownik.
- 3.5.3. Moduł identyfikacji użytkowników musi umożliwiać skuteczną identyfikację użytkowników pracujących z wykorzystaniem serwerów terminali (np. Citrix) współdzielących pojedynczy adres IP.
- 3.5.4. Moduł identyfikacji użytkowników musi umożliwiać identyfikację użytkowników znajdujących się za urządzeniem typu http proxy poprzez wykorzystanie informacji zawartej w nagłówku X-

- Forwarded-For. Moduł po pozyskaniu informacji z nagłówka XFF musi go usunąć przed przekazaniem komunikacji do serwera docelowego.
- 3.5.5. Moduł identyfikacji użytkowników przy współpracy z usługą katalogową Microsoft Active Directory powinien wykorzystywać minimalne wymagane uprawnienia po stronie usługi Active Directory. Niedopuszczalna jest integracja z domeną MS Active Directory w ramach, której wymagane jest zastosowanie uprawnień administratora domeny.
- 3.5.6. Moduł identyfikacji użytkowników musi posiadać możliwość współdzielenia informacji o zidentyfikowanych użytkownikach pomiędzy zaporami sieciowymi pochodzącymi od tego samego producenta i zarządzanymi z tego samego lub odrębnego serwera zarządzania.
- 3.5.7. System bezpieczeństwa musi umożliwiać wykorzystanie informacji uzyskanych przez moduł identyfikacji użytkowników w ramach definicji reguł polityki bezpieczeństwa w celu zapewniania użytkownikom lub grupom użytkowników spójnych reguł dostępu do zasobów niezależnie od ich lokalizacji.
- 3.6. Inspekcja ruchu szyfrowanego (HTTPS, SSH).
- 3.6.1. System bezpieczeństwa musi zapewniać mechanizmy inspekcji komunikacji szyfrowanej HTTPS oraz inspekcji komunikacji realizowanej w oparciu o protokół SSH.
- 3.6.2. System bezpieczeństwa w ramach inspekcji ruchu HTTPS musi wspierać protokoły TLS 1.2 oraz TLS 1.3.
- 3.6.3. System bezpieczeństwa musi pozwalać na inspekcję ruchu HTTPS zarówno dla ruchu wychodzącego z sieci organizacji (np. komunikacja użytkowników z usługami w sieci Internet) jaki i ruchu przychodzącego kierowanego do usług udostępnianych przez organizację. Inspekcja powinna obejmować analizę ruchu pod kątem zgodności z regułami polityki dostępowej (np. kontrola aplikacji oraz kategorii URL) oraz weryfikować ruch pod kątem ewentualnych zagrożeń (np. moduł IPS, moduł antywirusowy, sandboxing).
- 3.6.4. System musi umożliwiać administratorom zdefiniowanie reguł określających jaka część ruchu HTTPS ma zostać poddana inspekcji, a jaka ma zostać z niej wykluczona. W ramach definiowania reguł administrator musi posiadać możliwość określenia jakie mechanizmy inspekcyjne (moduły) mają zostać wykorzystane podczas analizy ruchu (np. ochrona antywirusowa).
- 3.6.5. System musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa.
- 3.6.6. W ramach mechanizmu inspekcji wychodzącego ruchu HTTPS system musi umożliwiać weryfikację stanu certyfikatu cyfrowego serwera docelowego. System musi umożliwiać blokowanie ruchu do określonego serwera docelowego w przypadku kiedy jego certyfikat został unieważniony, wygaś lub nie został podpisany przez zaufany urząd certyfikacji.
- 3.6.7. System bezpieczeństwa musi umożliwiać tworzenie listy niezaufanych certyfikatów cyfrowych i w efekcie pozwalać na blokowanie ruchu kierowanego do serwerów, które takie certyfikaty wykorzystują.
- 3.6.8. System bezpieczeństwa musi umożliwiać wysyłanie kopii odszyfrowanego ruchu HTTPS na wskazany interfejs urządzenia.
- 3.6.9. System bezpieczeństwa musi zapewniać mechanizmy pozwalające na inspekcję szyfrowanej komunikacji SSH. Niedopuszczalne jest, aby system do deszyfracji SSH używał jednego globalnego klucza deszyfrującego.
- 3.6.10. W ramach inspekcji ruchu SSH system musi zapewniać możliwość analizy ruchu przy pomocy modułu wykrywania włamań (IPS) oraz umożliwiać analizę przesyłanych plików minimum przy pomocy modułu antywirusowego.

- 3.7. Moduł do realizacji bezpiecznych połączeń zdalnych (IPSec VPN/Mobile Access).
- 3.7.1. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w trybie punkt-punkt (site-to-site) oraz zapewniać możliwość dostępu do zasobów dla użytkowników zdalnych (remote access).
 - 3.7.2. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w oparciu o protokół IKEv1 oraz IKEv2.
 - 3.7.3. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w następujących topologiach: full mesh, star, hub-and-spoke.
 - 3.7.4. Moduł IPSec VPN musi umożliwiać kreowanie tuneli w oparciu o klucz współdzielony (preshared key) oraz certyfikaty cyfrowe. W przypadku certyfikatów cyfrowych musi istnieć możliwość wykorzystania certyfikatów wystawianych przez wewnętrzny urząd certyfikacji wbudowany w produkt lub przez zewnętrzne urzędy certyfikacji.
 - 3.7.5. Moduł IPSec VPN musi umożliwiać uruchomienie mechanizmu split-tunneling dla połączeń od użytkowników zdalnych.
 - 3.7.6. Moduł IPSec VPN musi wspierać nawiązywanie połączeń L2TP.
 - 3.7.7. Niedopuszczalne jest, aby moduł IPSec VPN ograniczał licencyjnie liczbę tuneli punkt-punkt jakie mogą zostać nawiązane z poziomu zapory sieciowej.
 - 3.7.8. Dostęp VPN dla użytkowników zdalnych musi być możliwy za pomocą portalu SSL VPN lub za pomocą dedykowanego oprogramowania agenta instalowanego w systemie operacyjnym zdalnego urządzenia.
 - 3.7.9. Dostarczony system bezpieczeństwa musi umożliwiać jednoczesne nawiązanie minimum 50 tuneli IPSec/SSL VPN.
 - 3.7.10. W ramach dostępu VPN realizowanego przez portal SSL musi istnieć możliwość weryfikacji ustawień stacji użytkownika (compliance) przed udzieleniem jej dostępu do zasobów. Niespełnienie warunków musi skutkować uniemożliwieniem dostępu do zasobów pomimo poprawnych poświadczeń posiadanych przez użytkownika. Weryfikacja stacji użytkownika musi być możliwa na dwóch etapach: na etapie logowania do portalu SSL VPN lub w momencie próby uzyskania dostępu do określonej aplikacji udostępnianej w ramach portalu.
 - 3.7.11. Producent musi zapewnić dedykowane oprogramowanie agenta minimum na następujące systemy operacyjne: Microsoft Windows, iOS oraz Android.
- 3.8. Moduł filtrowania kategorii URL
- 3.8.1. Moduł filtrowania kategorii URL musi posiadać możliwość tworzenia reguł polityki zawierających jednocześnie wiele kategorii URL.
 - 3.8.2. Moduł filtrowania kategorii URL musi dostarczać wbudowane kategorie URL opisujące niebezpieczne witryny kategoryzowane w oparciu o poziom zagrożenia (np. CriticalRisk lub High Risk), a także w oparciu o rodzaj zagrożenia (np. witryny wyludzające dane lub witryny będące centrami C&C).
 - 3.8.3. Moduł filtrowania kategorii URL musi umożliwiać tworzenie własnych obiektów opisujących witryny URL oraz ich kategoryzowanie.
 - 3.8.4. Moduł filtrowania kategorii URL musi umożliwiać tworzenie obiektów należących do więcej niż jednej kategorii URL.
 - 3.8.5. Moduł filtrowania kategorii URL musi umożliwiać lokalne nadpisywanie domyślnej kategorii URL dla wybranych witryn.
 - 3.8.6. Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej witryny.
 - 3.8.7. Moduł filtrowania kategorii URL musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowania użytkowników do stron umieszczonych na zewnętrznych serwerach.

- 3.9. Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet
- 3.9.1. System zapobiegania komunikacji z sieciami botnet musi umożliwiać wykrycie oraz zablokowanie podejrzanego zachowania w chronionych segmentach sieci.
 - 3.9.2. System zapobiegania komunikacji z sieciami botnet w celu identyfikacji podejrzanych zachowań musi wykorzystywać mechanizmy zabezpieczeń oparte o reputację adresów IP, URL oraz DNS w połączeniu z wykrywaniem wzorców ruchu specyficznych dla połączeń kierowanych do serwerów C&C.
 - 3.9.3. System zapobiegania komunikacji z sieciami botnet musi posiadać możliwość identyfikacji urządzeń wewnętrznych będących źródłem podejrzanych zapytań DNS w przypadku kiedy wykorzystują one wewnętrzny serwer DNS pośredniczący w generowaniu zapytań. Mechanizm musi umożliwiać modyfikację/falszowanie odpowiedzi DNS i przekierowywanie urządzeń do wcześniej ustalonego adresu IP (DNS malware trap)
 - 3.9.4. Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, FTP, SMB/CIFS (w tym SMBv3), SFTP/SCP, IMAP, POP3
 - 3.9.5. Moduł ochrony antywirusowej musi w zależności od konfiguracji posiadać możliwość inspekcji lub blokowania pobierania poszczególnych typów plików - minimum bat, cab, dll, doc, pdf, jpg, jpeg, exe, com, pif, scr, gif, png, tif, asf, mp3, mdb, bmp, ps, rtf, rar, tgz, tar.gz, bz2, tar.bz2, tbz2, tb2, jar, , arc, reg, arj, zoo, ace, wmf, emf, xml, doc, ppt, xls, swf, mov, mpeg, js, wav, tar, ico, zip, hml, htm, hta.
 - 3.9.6. Moduł ochrony antywirusowej musi umożliwiać skanowanie adresów URL oraz załączników znajdujących się w wiadomościach poczty elektronicznej.
 - 3.9.7. Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych. Administrator musi mieć możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji (przełącz lub zablokuj) która zostanie podjęta w momencie przekroczenia zdefiniowanego limitu.
 - 3.9.8. Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji.
 - 3.9.9. Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet muszą posiadać możliwość interakcji z użytkownikami w zakresie informowania o zablokowaniu dostępu do niebezpiecznych zasobów.
 - 3.9.10. System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) w formacie CSV lub STIX XML (STIX 1.0).
- 3.10. Wymagania wydajnościowe
- 3.10.1. Urządzenie Wirtualne, pełniące rolę zapory sieciowej musi umożliwiać pracę z wykorzystaniem minimum 6 vCPU oraz posiadać przepływność w ruchu full-duplex nie mniej niż 7,9 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 3.1 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day).
 - 3.10.2. Podane w punkcie 3.10.1 parametry przepływności dotyczą wydajności zapory sieciowej w warunkach typu Enterprise. Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab”, „ideal” itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne.

4. Moduł raportowania oraz korelacji wydarzeń.

4.1. Wymagania ogólne.

- 4.1.1. Musi zapewniać zintegrowane zarządzanie zagrożeniami w czasie rzeczywistym, w tym: rejestrowanie, monitorowanie, logowanie zdarzeń, zarządzanie zagrożeniami oraz kontrolę zgodności z regulacjami.
- 4.1.2. Musi istnieć możliwość identyfikacji i analizy zagrożeń w czasie rzeczywistym wykorzystując logi bieżące jak i logi historyczne.
- 4.1.3. Musi istnieć możliwość wyszukiwania określonych wartości w całej bazie danych zdarzeń (bez potrzeby definiowania wyszukiwanych atrybutów).
- 4.1.4. Musi istnieć możliwość grupowania wyników wyszukiwania według poszczególnych atrybutów (typ incydentu, zasoby, nazwa użytkownika).
- 4.1.5. Musi istnieć możliwość zarządzania wieloma domenami; musi istnieć możliwość utworzenia co najmniej 5 domen administracyjnych na podstawie położenia geograficznego, jednostki biznesowej lub funkcji bezpieczeństwa (licencja musi być częścią oferty).
- 4.1.6. Musi istnieć możliwość zwiększenia liczby domen administracyjnych w przyszłości do co najmniej 200.
- 4.1.7. Musi obsługiwać interfejs API dla zapewnienia automatyzacji pracy z systemem.
- 4.1.8. Producent musi zapewniać regularne aktualizacje dla nowych wersji formatu logów.
- 4.1.9. Musi istnieć możliwość analizy typu Forensics; kliknięcie na linię czasu, wykres graficzny lub mapę powinno skutkować tzw. drill-down do poziomu pakietów.
- 4.1.10. Logi muszą być przesyłane poprzez uwierzytelniony i szyfrowany tunel.
- 4.1.11. Musi zostać dostarczony z co najmniej 2 letnim wsparciem technicznym producenta.

4.2. Widoki i Raporty.

- 4.2.1. Wszystkie widoki i raporty muszą być konfigurowalne.
- 4.2.2. Musi istnieć możliwość definiowania filtrów, dodawania / usuwania / dostosowywania komponentów i stron.
- 4.2.3. Musi istnieć możliwość tworzenia własnych widżetów, widoków i raportów lub korzystania z dowolnego predefiniowanego raportu.
- 4.2.4. Musi istnieć możliwość personalizowania raportów pod kątem ról takich jak: specjalista ds. bezpieczeństwa, inżynier sieciowy, kadra kierownicza itp.
- 4.2.5. Musi istnieć możliwość dodawania niestandardowych lub predefiniowanych widoków do raportów.
- 4.2.6. Musi zawierać raporty i kontrole zgodności z regulacjami dla co najmniej 300 praktyk i wymogów bezpieczeństwa.
- 4.2.7. Musi zawierać ujednolicony widok dla wszystkich aspektów monitorowania.
- 4.2.8. Musi istnieć możliwość tworzenia niestandardowych widoków odzwierciedlających i wyświetlających tylko informacje istotne dla organizacji.
- 4.2.9. Musi graficznie wyświetlać kategorie zdarzeń w postaci różnorodnych wizualizacji, np. interaktywnych pasków, wykresów kołowych i czasowych.
- 4.2.10. Musi istnieć możliwość tworzenia filtrów bazując na parametrach zdarzenia takich jak: aplikacja, źródłowy i docelowy adres IP, usługa, typ zdarzenia, istotność ataku, kraj pochodzenia itd.
- 4.2.11. Musi obsługiwać automatycznie generowanie raportów według harmonogramu (codziennie, co tydzień i co miesiąc); musi także umożliwiać administratorowi określenie daty i godziny, w której system raportowania zacznie generować zaplanowany raport.
- 4.2.12. Musi obsługiwać następujące formaty raportów: PDF i XLS/X.

- 4.2.13. Musi posiadać możliwość korelacji logów pochodzących ze wszystkich urządzeń w celu zidentyfikowania podejrzonej aktywności, śledzenia trendów oraz anomalii; wszystko to musi być dostępne z wykorzystaniem jednego interfejsu użytkownika.
- 4.2.14. Wszystkie logi bezpieczeństwa i zdarzenia muszą być skorelowane.
- 4.2.15. Wszystkie logi oraz powiązane zdarzenia muszą być indeksowane.
- 4.2.16. Musi istnieć możliwość tworzenia niestandardowych reguł korelacji zdarzeń bezpieczeństwa.
- 4.2.17. Musi zapewniać obsługę przechowywania zdarzeń, przetwarzania i korelację logów z urządzeń firm trzecich, z wykorzystaniem co najmniej Syslog i protokołu SNMP.
- 4.2.18. Musi istnieć możliwość definicji poziomu istotności poszczególnych zdarzeń na podstawie reguł korelacji.
- 4.2.19. Musi obsługiwać automatyczną reakcję na określone zdarzenie bezpieczeństwa - minimalne działanie: wyślij wiadomość e-mail, SNMP trap, uruchom skrypt.
- 4.2.20. Musi istnieć możliwość graficznego tworzenia parsera logów w przypadku ich niestandardowego formatu.
- 4.2.21. Musi istnieć możliwość „skoku” bezpośrednio od zdarzenia do reguły w polisie bezpieczeństwa, która dane zdarzenie wygenerowała; wszystko musi być wykonane z użyciem jednego interfejsu użytkownika.
- 4.2.22. Musi istnieć możliwość natychmiastowego powiadomienia administratora w wyniku wystąpienia określonych zdarzeń i logów.
- 4.2.23. Musi umożliwiać definiowanie i zapisywanie niestandardowych filtrów użytkownika dla każdego zdarzenia.
- 4.2.24. Musi istnieć możliwość definicji globalnych wyjątków związanych ze zdarzeniami; musi istnieć możliwość dostosowywania alarmów, aby wykluczyć zdarzenia według źródła, celu i usługi.
- 4.2.25. Musi istnieć możliwość grupowania zdarzeń w celu ich analizy.
- 4.2.26. Musi zapewniać predefiniowane raporty: godzinowy, dzienny, tygodniowy i miesięczny; raport musi zawierać co najmniej najczęstsze: źródło, cel, usługi, zdarzenia, cele i odpowiadające im zdarzenia, usługi i odpowiadające im zdarzenia.

5. Moduł analizy konfiguracji

5.1. Wymagania ogólne

- 5.1.1. Moduł musi umożliwiać ciągłe monitorowanie w czasie rzeczywistym urządzeń typu firewall, uruchomionych modułów, zainstalowanych polityk oraz konfiguracji pod kątem zgodności z regulacjami oraz dobrymi praktykami.
- 5.1.2. Moduł musi umożliwiać generowanie graficznych widoków oraz raportów przedstawiających zgodność z regulacjami oraz dobrymi praktykami.
- 5.1.3. Widoki oraz raporty muszą przedstawiać między innymi poziom zgodności z regulacjami oraz dobrymi praktykami.
- 5.1.4. Moduł musi umożliwiać generowanie alertów w przypadku wykrycia niezgodności.
- 5.1.5. Moduł musi umożliwiać konfigurację i monitorowanie własnych regulacji.
- 5.1.6. Moduł musi umożliwiać tworzenie wyjątków dla zestawu dobrych praktyk poprzez wyłączanie monitoringu pojedynczych rekomendacji.
- 5.1.7. Moduł musi posiadać wsparcie dla przynajmniej następujących regulacji:
 - a) Australian Privacy Principles (APP)
 - b) AUISM
 - c) CIPA
 - d) CIS Benchmarks
 - e) CJIS
 - f) CMMC

- g) CobiT 4.1 (IT SOX)
- h) Cobit 5.0
- i) Customer Security Programme (CSP) (SWIFT)
- j) Cyber Essentials
- k) Deng Bao
- l) DISA Firewall STIG
- m) DSD
- n) FIPS 200
- o) GDPR
- p) GLBA
- q) GPG13
- r) HIPAA Security
- s) ICDM
- t) IDSML
- u) IEC 62443-2-1
- v) ISA TR99
- w) ISO 27001
- x) ISO 27001:2013
- y) ISO 27002
- z) IT Grundschutz - Security Gateway
- aa) Katakri 3.0
- ab) K-ISMS
- ac) LGPD (Brazil)
- ad) MAAGTIC-SI
- ae) MAS TRM
- af) Mauritius Data Privacy
- ag) N-CIPA
- ah) NERC CIP
- ai) NERC CIP (v.5)
- aj) New York State Cybersecurity Regulation (NYDFS)
- ak) NIST 800-41
- al) NIST 800-53 Revision 5
- am) NIST 800-171
- an) NIST SP800-82
- ao) NORMEN
- ap) NZISM
- aq) PCI DSS
- ar) PCI DSS 2.0
- as) PCI DSS 3.0
- at) PCI-DSS 3.2.1
- au) PCI-DSS 4.0
- av) PPG234
- aw) Protection of Personal Information Act, 2013 (POPI)
- ax) SAMA
- ay) SANS Top 20 Critical Controls
- az) SOX
- ba) Statement of Controls (ISAE 3402)
- bb) Statement of Controls (ISAE 3402)

6. Zakres wdrożenia systemu.

- 6.1. Wszystkie czynności wdrożeniowe powinny być wykonywane u Zamawiającego i w obecności Zamawiającego.

- 6.2. Wykonawca powinien zaimplementować współpracę dostarczonego systemu z usługą katalogową Microsoft Active Directory.
- 6.3. Wykonawca powinien w pełni skonfigurować dostarczony system do pracy z protokołem SNMP.
- 6.3.1. Zamawiający do gromadzenia danych SNMP używa systemu „Elastic Stack 8.x, (Elasticsearch-Logstash-Kibana) (ELK) (wer.: min. 8.7.0) (<https://www.elastic.co/>) na systemie operacyjnym Linux oraz do wizualizacji i analizy danych oprogramowania „Grafana” (wer.: min. 11.0.0) (<https://grafana.com/>).
- 6.3.2. Do pobierania danych SNMP (opis urządzenia, czas pracy, liczba CPU, status pracy, wykorzystanie rdzeni procesora, wykorzystanie storage (w tym z podziałem na dyski lub volumeny), zużycie pamięci (w tym wirtualnej), transfer danych przez interfejsy sieciowe (w tym z podziałem na VLAN'y), użycie interfejsów sieciowych (w tym z podziałem na VLAN'y). Zamawiający wykorzystuje skrypty Python'a. Jeżeli posiadane przez Zamawiającego skrypty Python'a nie będą w 100% współdziałać z danymi otrzymywanymi z dostarczonym systemem, Wykonawca odpowiednio zmodyfikuje powyższe skrypty tak, aby pobierane dane były zgodne z rodzajem danych pobieranych w już posiadanych przez Zamawiającego skryptach.
- 6.3.3. Pobierane dane SNMP przez skrypt Python'a przesyłane są do Elasticsearch'a.
- 6.3.4. Wizualizacja danych realizowana jest w programie „Grafana”.
- 6.3.5. Dane SNMP pobrane z dostarczonego systemu powinny być w pełni wizualizowane w programie „Grafana”. W przypadku rozbieżności Zamawiający odpowiednio zmodyfikuje skrypty Python'a.
- 6.4. Zamawiający do gromadzenia logów i ich analiz używa systemu „Elastic Stack 8.7.x, (Elasticsearch-Logstash-Kibana) (ELK) (wer.: min. 8.7.0) (<https://www.elastic.co/>) na systemie operacyjnym Linux oraz do dodatkowej wizualizacji i analizy danych oprogramowanie „Grafana” (wer.: min. 11.0.0) (<https://grafana.com/>).
- 6.4.1. Wykonawca w obecności Zamawiającego powinien w pełni skonfigurować dostarczony system do wysyłania logów na wskazane przez Zamawiającego serwery i określone porty w standardzie Syslog oraz NetFlow.
- 6.4.2. Wykonawca w obecności Zamawiającego powinien skonfigurować proces przetwarzania danych (logów) po stronie serwera (Logstash) do pobierania danych z dostarczonego systemu w standardzie Syslog oraz NetFlow (v5, v9, v10).
- 6.4.3. W celu dostosowania logów do formy bardziej czytelnej (rozdzielanie rodzaju logów: informacyjne, ostrzeżenia, błędy itp.) Zamawiający powinien w pełni skonfigurować Logstash, używając jego języka konfiguracji (w tym GROK) do przetworzenia surowych logów w bardziej czytelne. O czytelności logów decyduje Zamawiający.
- 6.4.4. Wykonawca powinien tak skonfigurować Logstash, aby przetworzone logi w Logstash przesyłane były do Elasticsearch'a.
- 6.4.5. Testy otrzymywanych logów powinny być poprawnie obrazowane w programie Kibana.
- 6.4.6. Wykonawca w obecności Zamawiającego w programie Grafana powinien utworzyć źródło danych dla baz logów gromadzonych dla dostarczonego systemu.
- 6.4.7. Wykonawca w obecności Zamawiającego z logów zgromadzonych przez Elasticsearch'a, dla logów z dostarczonego systemu, powinien w oprogramowaniu Kibana stworzyć dwie przykładowe wizualizacje w postaci wykresów oraz jedną w postaci tabelarycznej.
- 6.4.8. Wykonawca w obecności Zamawiającego w programie Grafana powinien utworzyć/zaktualizować dashboard dla logów gromadzonych z dostarczonego systemu.
- 6.4.9. Wykonawca w obecności Zamawiającego przeprowadzi testy związane z gromadzeniem i wizualizacją logów, które powinny zakończyć się pozytywnie.
- 6.5. Zamawiający w swojej infrastrukturze informatycznej wykorzystuje odpowiednie oprogramowanie do realizacji zadań związanych z backupem maszyn wirtualnych w systemie

VMware. Dostarczony system powinien w pełni współpracować z systemem VMware.

6.6. Migracja istniejącej funkcjonalności zapory sieciowej Zamawiającego do nowego systemu.

6.6.1. Wykonawca powinien z istniejącego u Zamawiającego systemu zapory sieciowej przenieść następujące funkcjonalności:

- 6.6.1.1. trasy statyczne,
- 6.6.1.2. użytkownicy lokalni z nadanymi uprawnieniami,
- 6.6.1.3. autentykacja użytkowników w Captive Portal za pomocą grup w Active Directory,
- 6.6.1.4. VLAN,
- 6.6.1.5. zgrupowane interfejsy do zarządzania,
- 6.6.1.6. wirtualne IP,
- 6.6.1.7. ruch DHCP pomiędzy VLAN'ami,
- 6.6.1.8. zgrupowane hosty/sieci/porty/URL i implementacja ich w firewallu,
- 6.6.1.9. forwardowanie portów,
- 6.6.1.10. NAT 1:1,
- 6.6.1.11. schedules - włączanie/wyłączanie reguł w określonym czasie,
- 6.6.1.12. ustawione wyjątki w regułach zapory,
- 6.6.1.13. serwer NTP,
- 6.6.1.14. OpenVPN do IPSec,
- 6.6.1.15. śledzenie parametrów zapory sieciowej i bezpieczeństwa za pomocą NETDATA.

7. Szkolenia:

7.1. Przeprowadzenie (certyfikowanych przez producenta dostarczonego systemu) szkoleń dla 4 administratorów.

7.1.1. Liczba wszystkich szkoleń 8.

7.2. Rodzaje certyfikowanych szkoleń online:

7.2.1. podstawowe szkolenie dla administratorów. Skonfigurowanie od podstaw typowych środowisk centralnego zarządzania, budowanie polityk bezpieczeństwa, monitorowanie systemów, sposoby licencjonowania, konfiguracja NAT, VPN Site to Site, konserwacja systemów itp., w tym:

- 7.2.1.1. opis podstawowych komponentów architektury systemu (wszystkie warstwy) jak i współdziałanie ich w środowisku pracy,
- 7.2.1.2. sposób zabezpieczania komunikacji i kierowanie ruchu w dostarczonym systemie,
- 7.2.1.3. funkcje systemu operacyjnego dostarczonego systemu,
- 7.2.1.4. podstawowe przepływy pracy w celu instalowania komponentów systemu dla rozwiązań jednodomenowych,
- 7.2.1.5. tworzenie obiektów odpowiadające topologii organizacji, do wykorzystania w zasadach i regułach,
- 7.2.1.6. funkcje i możliwości, usprawniające konfigurację i zarządzanie zasadami bezpieczeństwa,
- 7.2.1.7. wpływ zasad bezpieczeństwa na inspekcję ruchu,
- 7.2.1.8. wpływ translacji adresów sieciowych na ruch,
- 7.2.1.9. sposoby skonfigurowania (ręczny/automatyczny) translacji adresów sieciowych (NAT),
- 7.2.1.10. konfigurowanie funkcji kontroli aplikacji i filtrowania adresów URL oraz autonomicznego zapobiegania zagrożeniom w celu spełnienia wymagań bezpieczeństwa organizacji,
- 7.2.1.11. sposoby udostępniania kluczy i certyfikatów do uwierzytelniania VPN,
- 7.2.1.12. analizowanie i interpretowanie ruchu tunelu VPN,
- 7.2.1.13. konfigurowanie parametrów rejestrowania pracy systemu zabezpieczeń,
- 7.2.1.14. używanie wstępnie zdefiniowanych i niestandardowych zapytań do filtrowania wyników rejestrowania,

- 7.2.1.15. monitorowanie stanu pracy systemu za pomocą portalu monitorującego jak i wiersza poleceń,
 - 7.2.1.16. różne metody tworzenia kopii zapasowych informacji systemowych systemu bezpieczeństwa i najlepsze praktyki i zalecenia dla każdej metody.
- 7.2.2. zaawansowane szkolenie dla administratorów. Skonfigurowanie od podstaw zaawansowanych środowisk pracy, budowanie zaawansowanych polityk bezpieczeństwa, kontroli aplikacji, zaawansowane połączenia VPN i konfiguracji klastra w tym:
- 7.2.2.1. typy technologii obsługiwanych przez system bezpieczeństwa w celu automatyzacji pracy,
 - 7.2.2.2. cele wdrożeń rozwiązań High Availability (HA),
 - 7.2.2.3. przepływy pracy stosowane w celu wdrożenia serwerów podstawowych i pomocniczych,
 - 7.2.2.4. podstawowe koncepcje klastrowania, w tym protokoły, synchronizację,
 - 7.2.2.5. wykluczanie usług z synchronizacji lub opóźnianie synchronizacji,
 - 7.2.2.6. zarządzanie dostępem użytkowników wewnętrznych i zewnętrznych,
 - 7.2.2.7. komponenty i konfiguracje w celu identyfikowania użytkowników i tożsamości komputerów,
 - 7.2.2.8. różne rozwiązania wielowarstwowej ochrony przed infekcjami,
 - 7.2.2.9. modułu IPS,
 - 7.2.2.10. zapobieganie atakom na sieć i urządzenia,
 - 7.2.2.11. cele sieci VPN opartych na domenach,
 - 7.2.2.12. zewnętrzne zarządzanie uwierzytelnieniami certyfikatów,
 - 7.2.2.13. rozwiązanie do łączenia się z aplikacjami korporacyjnymi przez Internet za pomocą urządzenia mobilnego lub komputera. Zapewnienie dostępu zdalnego klasy korporacyjnej zarówno za pomocą warstwy 3 VPN, jak i SSL VPN,
 - 7.2.2.14. określanie i ustalanie czy konfiguracja jest zgodna z najlepszymi praktykami,
 - 7.2.2.15. rozwiązania dostrajania wydajności w konfiguracji przepływów pracy,
 - 7.2.2.16. procedury i metody migracji bram bezpieczeństwa,
 - 7.2.2.17. procedury i metody aktualizacji bram bezpieczeństwa.
- 7.2.3. Zapobieganie zagrożeniom
- 7.2.4. Przeszkolenie teoretyczne oraz praktyczne w zakresie:
- 7.2.4.1. zapobieganie zagrożeniom, weryfikacja środowiska bezpieczeństwa,
 - 7.2.4.2. ochrona IPS (włączanie i konfigurowanie niestandardowej ochrony przed zagrożeniami, konfigurowanie ustawień inspekcji, aktualizowanie zabezpieczeń IPS, konfigurowanie zabezpieczeń ogólnych i szczegółowych, konfigurowanie i testowanie zabezpieczeń podstawowych),
ochrona antywirusowa i antybotowa – konfiguracja,
 - 7.2.4.3. profile i polityki zapobiegania zagrożeniom (tworzenie niestandardowych profili zapobiegania zagrożeniom),
 - 7.2.4.4. warstwy polityki zapobiegania zagrożeniom (konfigurowanie ustawień interfejsu bramy, konfigurowanie warstw zasad zapobiegania zagrożeniom, konfigurowanie reguł zapobiegania zagrożeniom z niestandardowymi profilami),
 - 7.2.4.5. zapobieganie zagrożeniom, analiza dziennika i ruchu sieciowego (przegląd dzienników i zdarzeń zapobiegania zagrożeniom, testowanie zabezpieczeń, konfiguracja ustawień w w/w zakresie),
 - 7.2.4.6. wyjątki w zapobieganiu zagrożeniom (wyjątki ustawień IPS i inspekcji),
 - 7.2.4.7. generowanie widoków i raportów dotyczących korelacji zapobiegania zagrożeniom (tworzenie i konfiguracja raportów),
 - 7.2.4.8. aktualizacja systemu przeciwdziałania zagrożeniom i badanie jego skuteczności,
 - 7.2.4.9. zaawansowane funkcje zapobiegania zagrożeniom i rozwiązywanie problemów z działaniem systemów.

8. Wsparcie techniczne

- 8.1. Oferowany system bezpieczeństwa musi być objęty wsparciem producenta przez cały okres obowiązywania umowy w następującym zakresie:
 - 8.1.1. ciągły dostęp do aktualizacji elementów bezpieczeństwa takich jak IPS, Kontrola aplikacji, URL Filtering, Antivirus, AntiBot, SandBox,
 - 8.1.2. automatycznie instalowane krytyczne poprawki, pakiety serwisowe i uaktualnienia,
 - 8.1.3. proaktywne zapobieganie zagrożeniom, zanim staną się problemami,
 - 8.1.4. dostęp do narzędzi diagnostycznych i zasobów online między innymi jak baza wiedzy itp.
 - 8.1.5. producent oferowanego rozwiązania musi posiadać całodobowe globalne centra pomocy technicznej i realizować wsparcie techniczne:
 - 8.1.5.1. co najmniej w dni robocze przez minimum 9 godzin dziennie,
 - 8.1.5.2. czas odpowiedzi na zgłoszony problem nie może przekraczać 4 godzin,
 - 8.1.5.3. producent musi zapewniać nielimitowane wsparcie ekspertów,
 - 8.1.5.4. przesyłanie, przeglądanie i aktualizowanie żądań serwisowych musi odbywać się online za pomocą dedykowanego portalu serwisowego.

9. Dokumentacja

- 9.1.1. Dokumentacja powykonawcza powinna zawierać min.:
 - 9.1.1.1. Licencje dostarczonego systemu.
 - 9.1.1.2. Szczegółową specyfikację dostarczonego systemu.
 - 9.1.1.3. Opis konfiguracji do produkcji.
 - 9.1.1.4. Zestawy domyślnych wizytowników i ich hasła.
 - 9.1.1.5. Karty katalogowe oraz instrukcje dla dostarczonego systemu (wersja elektroniczna).
 - 9.1.1.6. Karty gwarancyjne (jeżeli istnieją).
 - 9.1.1.7. Schematy połączeń z istniejącą infrastrukturą IT Zamawiającego.