Oznaczenie sprawy: 23/ZP/2022 Załącznik Nr 2 do SWZ

**Opis Przedmiotu Zamówienia**

* **Urządzenie firewall – 1 szt.**

|  |  |
| --- | --- |
|  | **UTM - funkcjonalność** |
| **1** | System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| **2** | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 2,1 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS) i obsługiwać nie mniej niż 400 000 jednoczesnych połączeń i minimum 72 000 nowy sesji na sekundę |
| **3** | System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Ethernet 1G. |
| **4** | Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| **5** | Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). |
| **6** | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać minimum 4094 znaczników VLAN. |
| **7** | System zabezpieczeń firewall musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. |
| **8** | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| **9** | Polityka zabezpieczeń 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 zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| **10** | System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| **11** | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. |
| **12** | Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż  4 Gbit/s . |
| **13** | Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). |
| **14** | Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. |
| **15** | Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. |
| **16** | System zabezpieczeń firewall musi wykrywać co najmniej 3600 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| **17** | System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| **18** | System zabezpieczeń firewall musi zapewniać możliwość segmentacji aplikacji na standardowych dla nich portach usług w obrębie pojedynczej reguły polityki firewall, tj. musi istnieć możliwość takiej konfiguracji pojedynczej reguły firewall, która zezwoli na działanie kilku aplikacji, wyłącznie jeśli nawiązanie połączenia następuje na port właściwy dla danej aplikacji, np. jeśli pojedyncza reguła zezwala na ruch SMTP i DNS, to SMTP nie może być dozwolone na porcie 53 (właściwym dla DNS), a DNS na porcie 25 (właściwym dla SMTP). |
| **19** | System zabezpieczeń firewall powinien automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punktu widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook” potrzebne jest dodatkowo użycie aplikacji „SSL”, a administrator nie uwzględni tej aplikacji w polityce, to system powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki. |
| **20** | System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| **21** | System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |
| **22** | System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |
| **23** | System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików. |
| **24** | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| **25** | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| **26** | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. |
|  | System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. |
| **27** | System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |
| **28** | System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |
| **29** | System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. |
| **30** | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |
| **31** | Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| **32** | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. |
| **33** | System zabezpieczeń firewall musi umożliwiać kategoryzacje strony WWW za pomocą mechanizmu przypisującego do konkretnej strony kilka kategorii (np. portal finansowy i portal informacyjny). Kategoryzacja powinna zapewniać co najmniej cztery kategorie per strona. Dodatkowo, powinna istnieć możliwość budowania własnych kategorii bazujących na kombinacji kategorii standardowych (np. własna kategoria wiadomości finansowe zawierające wszystkie strony skategoryzowane jako portale finansowe i informacyjne) jak również budowanie kategorii na bazie ryzyka bezpieczeństwa danej strony (niskie, średnie, wysokie) i określenia czy dana strona jest stroną nowopowstałą. |
| **34** | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| **35** | System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| **36** | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| **37** | System zabezpieczeń musi umożliwiać deszyfrację ruchu SSL, przesłanie go w postaci rozszyfrowanej przez rozwiązania zewnętrzne firm trzecich (np. system DLP, system IPS, system Sand-box) i ponowne zaszyfrowanie protokołem SSL przed dalszą transmisją. |
| **38** | System zabezpieczeń musi umożliwiać wysyłanie kopii zdeszyfrowanego ruchu SSL na wskazany interfejs urządzenia. |
| **39** | System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| **40** | System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| **41** | System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| **42** | System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| **43** | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| **44** | System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| **45** | System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| **46** | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| **47** | System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| **48** | System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |
| **49** | System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| **50** | System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| **51** | System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany. |
| **52** | System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| **53** | System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, Ms-Offfice, jar, flash, apk, rar, MacOSX, Linux, JScript, PowerShell, Shell Scripts, VBScript) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 150 Mbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. |
| **54** | Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". |
| **55** | Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”. |
| **56** | System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. |
| **57** | System zabezpieczeń 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. |
| **58** | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| **59** | System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| **60** | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). |
| **61** | System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach. |
| **62** | System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0. |
| **63** | System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
|  | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. |
| **64** | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |
| **65** | System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |
| **66** | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| **67** | System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. |
| **68** | System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. |
| **69** | System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. |
| **70** | System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| **71** | Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| **72** | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. |
| **73** | System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). |
| **74** | System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 128 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |
| **75** | System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. |
| **76** | System zabezpieczeń firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa, polityki PBR (policy based routing) oraz polityki QoS wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur. |
| **77** | System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. |
| **78** | System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. |
| **79** | System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia. |
| **80** | System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. |
| **81** | System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. |
| **82** | System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. |
| **83** | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| **84** | Całość objęta minimum 12-miesięcznym wsparciem producenta. Wszystkie licencje dostarczone w ramach postępowania mają być objęte minimum 12- miesięcznym wsparciem liczonym od momentu dostawy – kryterium oceny ofert |
|  |  |
| **85** | Zamawiający wymaga aby wykonawca był partnerem producenta dostarczonego rozwiązania na poziomie minimum Innovator lub równoważnym i posiadał w swoich zasobach personalnych inżyniera minimum z certyfikatem PCNSA lub równoważnym. |
| **86** | Zamawiający przekaże niezbędne informacje umożliwiające wykonawcy przeniesienie/odtworzenie/migracje kompletnej konfiguracji z obecnego rozwiązania firewall do nowego. Miedzy innymi: polityki firewall, polityki NAT, routing, VPN, konfiguracja interfejsów sieciowych i wszystkie inne, które są wymagane do działania w środowisku zamawiającego. Ewentualnie udostępni wykonawcy dostęp do obecnego rozwiązania Firewall w celu pobrania/odtworzenia  bieżącej konfiguracji na nowym urządzeniu. |
| **87** | Instalacja, konfiguracja, szkolenie z zakresu funkcjonalności oraz obsługi. |
| **88** | Wraz z dostawą sprzętu należy dostarczyć wszystkie elementy potrzebne do podłączenia się do istniejącej infrastruktury. |
| **89** | Gwarancja min. 36 miesięcy |

* **System zarządzania zasobami – 1 szt.**

|  |
| --- |
| **Zarządzanie zasobami** |
| **Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne** |
|  |
| Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania |
| Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP |
| Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji |
| Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy |
| Odwzorowanie struktury organizacji w oparciu o Active Directory |
| Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) |
| Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci |
| Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów) |
| Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.) |
| Utworzenie własnych typów elementów wyposażenia |
| Łączenie elementów wyposażenia w zestawy |
| Przypisywanie zasobu do wielu zestawów |
| Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia |
| Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach |
| Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików |
| Przypisywanie sprzętu do konkretnych osób |
| Przypisywanie sprzętu do wybranej firmy |
| Automatyczne wyznaczanie 'Głównego użytkownika' komputera |
| Wiązanie wielu rekordów wyposażenia z użytkownikiem |
| Przypisywanie sprzętu do dowolnej lokalizacji |
| Definiowanie własnych, dowolnych atrybutów sprzętu |
| Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu' |
| Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia |
| Określanie loga firmy oraz użycia go na wydrukach |
| Grupowa zmiana domeny/grupy roboczej zasobu |
|  |
| **Informacje o sprzęcie** |
|  |
| Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu |
| Wykrywanie komputerów typu All-In-One |
| Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF) |
| Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu |
| Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM |
| Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany |
| Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd. ) |
| Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc. ) |
| Odczyt informacji o module TPM |
| Odczyt D3Dscore z WinSAT |
| Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.) |
| Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu |
| Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika) |
| Automatyczne tworzenie zestawów: Komputer + Monitor |
| Automatyczne utworzenie zestawów: Komputer + drukarka lokalna |
| Automatyczne utworzenie zestawów: host + maszyny wirtualne |
| Automatyczne wykrywanie czy komputer jest maszyną wirtualną |
| Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform |
| Określanie informacji o wykorzystywanej wirtualizacji |
| Podgląd zestawów, do których należy zasób |
| Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami |
| Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu |
| Definiowanie szczegółowych informacji finansowych |
| Obsługa walut w danych finansowych |
| Definiowanie bazy dostawców sprzętu i oprogramowania |
| Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) |
| Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta |
| Agent odczytuje identyfikator SID komputera |
| Określanie adresu interfejsu webowego urządzenia sieciowego |
| Określanie typu gwarancji dla zasobu |
| Określenie wpływu biznesowego wybranego zasobu |
| Tworzenie własnych typów gwarancji |
| Określanie ikony dla typów zasobów |
|  |
| **Raporty zasobów** |
|  |
| Raport dodanych załączników |
| Automatyczne tworzenie historii zmian sprzętu |
| Raport zbiorczy historii zmian w sprzęcie |
| Ewidencja zdarzeń serwisowych |
| Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów |
| Informacja na temat pojemności dysków twardych oraz wolnego miejsca |
| Wydruk\dodanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu |
| Wydruk\dodanie jako załącznik protokołu przekazania dla całego zestawu |
| Kreator szablonów wydruków WYSIWYG |
| Definiowanie dedykowanych profili protokołów |
| Zapisywanie protokołów podczas generowania jako załącznik do zasobu |
| Wydruk\dodanie jako załącznik Karty informacyjnej dla elementu wyposażenia |
| Wydruk lub zapisanie do pliku raportów ze szczegółami sprzętu |
| Porównywarka wyników skanowania sprzętu |
| Dzienniki zdarzeń systemu Windows |
| Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu |
|  |
| **Funkcje dodatkowe** |
|  |
| Zdalne wykonywanie skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych |
| Wykonywanie zadań dla wszystkich komputerów (uwzględnia komputery, które zostaną dodane w przyszłości) |
| Edytor skryptów (batch) z funkcją kolorowania składni |
| Wykorzystywanie predefiniowanych skryptów (batch) |
| Import informacji o wyposażeniu z pliku CSV |
| Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL) |
| Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu) |
| Generowanie kodów paskowych, QR dla każdego elementu wyposażenia |
| Obsługa kodów QR |
| Archiwum zasobów |
| Przeniesienie utylizowanego wyposażenia do archiwum |
| Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego |
| Zarządzanie sprzętem przez aplikacje mobilną (Android, Windows Phone) |
| Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu |
| Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych |
| Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej |
| Grupowa zmiana atrybutów |
| Personalizacja statusów zasobów |
|  |
| **Zarządzanie oprogramowaniem** |
| **Licencje** |
|  |
| Inwentaryzacja licencji |
| Automatyczne tworzenie licencji na podstawie kluczy produktów |
| Import licencji z pliku tekstowego |
| Automatyczne generowanie historii zmian w licencji |
| Określanie statusu licencji |
| Utworzenie własnych atrybutów licencji |
| Tworzenie notatek oraz załączników w dowolnym formacie do licencji |
| Tworzenie licencji z poziomu rozliczenia audytu legalności |
| Tworzenie licencji z poziomu raportu kluczy licencji |
| Tworzenie zestawów licencji |
| Relacja licencji z użytkownikiem, firmą, działem, lokalizacją |
| Zmiana typu licencji dla wybranej grupy |
| Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe) |
| Przypisywanie licencji do komputera |
| Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.) |
| Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska |
| Definiowanie licencji przeznaczonych do przyszłego zakupu |
| Definiowanie kluczy seryjnych i przypisywanie do licencji |
| Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją |
| Określenie wpływu biznesowego wybranej licencji |
|  |
| **Skanowanie oprogramowania** |
|  |
| Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera |
| Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów |
| Śledzenie zmian w stanie zainstalowanego oprogramowania |
| Zdalny skan komputerów (bieżący lub okresowy) |
| Zmiana priorytetu skanowania oprogramowania |
| Skan komputerów niepodłączonych do sieci |
| Wysyłanie wyników skanowania offline na serwer FTP (Audyt) |
| Przekazywanie konfiguracji wzorcowej dla skanera offline |
| Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania |
| Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy |
| Określanie masek plików dla publikacji elektronicznych (e-book) |
| Skan plików skompresowanych |
| Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz |
| Wbudowane profile skanowania (np. profil wzorcowy) |
| Definicja własnych ustawień skanowania |
| Porównywanie wyników skanowania oprogramowania |
| Wykrywanie plików multimedialnych |
| Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika) |
| Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI |
| Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie |
| Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych |
| Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta |
| Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (**\*** , **%**) |
|  |
| **Audyt legalności** |
|  |
| Rozliczanie pakietów aplikacji |
| Rozliczanie systemów operacyjnych |
| Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji |
| Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji. |
| Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty) |
| Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę |
| Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie) |
| Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji |
|  |
| **Funkcje** |
| Mechanizm informujący o nowej bazie wzorców oprogramowania |
| Definiowanie własnych wzorców oprogramowania |
| Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych |
| Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania |
| Wykrywanie kluczy/identyfikatorów programów |
| W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza |
| Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office |
| Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania |
| Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji |
| Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd. |
| Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd. |
| "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki) |
| Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (\*.msi) |
| Zdalne dezinstalacja oprogramowania |
| Utworzenie harmonogramu dezinstalacji oprogramowania |
| Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania |
| Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej |
| Raport zainstalowanych aktualizacji systemu Windows |
|  |
| **Kontrola wykorzystania sprzętu i oprogramowania** |
| **Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne** |
|  |
| Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach |
| Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów) |
| Określanie firmy do której należy użytkownik |
| Określanie przełożonego dla użytkownika |
| Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy). |
| Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.) |
| Zarządzanie stanowiskami użytkowników |
| Przeniesienie rekordu użytkownika do archiwum |
| Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika |
| Odczytywanie informacji o użytkownikach z Active Directory |
| Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) |
| Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień |
| Podgląd zdjęcia przypisanego do użytkownika |
| Przypisywanie do użytkownika załączników (pliki) |
| Przypisywanie notatek do użytkownika |
| Ewidencja zdarzeń przypisanych do użytkowników |
| Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory |
|  |
|  |
| **Raporty** |
|  |
| Analiza aktywności użytkowników |
| Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP ) |
| Analiza przerw w pracy |
| Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków) |
| Analiza aktywności mikrofonu oraz kamery |
| Analiza wykorzystania poszczególnych aplikacji w czasie |
| Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie |
| Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika |
| Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny). |
| Statystyki najczęściej wykorzystywanych aplikacji |
| Statystyki wykorzystania komputerów przez poszczególnych użytkowników |
| Statystyki aktywności użytkownika i grup użytkowników |
| Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin |
| Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników |
| Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.) |
| Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi) |
| Monitoring wydruków na drukarkach sieciowych |
| Monitoring użytkowników stacji terminalowych |
| Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.) |
| Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca |
| Raport zbiorczy historii zmian w rekordach użytkowników |
|  |
| **Funkcje** |
|  |
| Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników. |
| Autoryzacja nośników zewnętrznych |
| Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych |
| Baza informacji o napędach zewnętrznych |
| Blokada dostępu do napędów zewnętrznych ([m.in](http://m.in/). HDD, FDD, Pen Drive, etc.) |
| Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM |
| Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy |
| Informacje o ostatnio zalogowanych osobach na stacjach klienckich |
| Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje |
| Komentowanie przerw pracy |
| Kategoryzacja przerwy w pracy na podstawie komentarza |
|  |
| **Kontrola wykorzystania Internetu** |
| **Funkcje** |
|  |
| Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType) |
| Blokada stron internetowych dla protokołu http \ https (IE, Chrome, Firefox, Opera, Edge, Chromium, Vivaldi) |
| Kategoryzacja stron internetowych |
| Blokada dostępu do witryn zgodnie z harmonogramem |
| Blokada trybu incognito w przeglądarce Google Chrome |
|  |
| **Raporty** |
| Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach |
| Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki ) |
| Monitoring stron internetowych dla protokołu http \ https (IE, Edge, Chrome, Firefox, Opera, Vivaldi) |
| Analiza liczby wejść na poszczególne strony lub domeny |
| Analiza odwiedzanych domen i stron |
| Raport informujący o plikach pobranych przez przeglądarki WWW |
| Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe |
|  |
| **Helpdesk** |
| **Obsługa** |
|  |
| Rejestracja i obsługa zgłoszeń |
| Obsługa zgłoszeń w modelu Kanban |
| Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny) |
| Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii |
| Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów |
| Opis zgłoszenia w formacie HTML |
| Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent |
| Tworzenie notatek dla zgłoszeń |
| Zapisywanie wersji roboczej komentarza |
| Archiwizacja zgłoszeń |
| Monitoring czasu pracy nad incydentem (time tracking) |
| Raport ewidencji czasu pracy nad zgłoszeniem |
| Informacja o czasie reakcji do podjęcia zgłoszenia |
| Dodanie prywatnego komentarza |
| Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia |
| Dodanie załączników do incydentów, również do komentarza |
| Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie |
| Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów) |
| Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń |
| Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń |
| Wydruk historii zgłoszenia |
| Widok kalendarza (Planowanie rozwiązania incydentów) |
| Korelacja incydentu z elementem zasobów |
| Raport zbiorczy historii zmian |
| Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej |
| Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania |
| Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA |
| Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu |
| Określenie wpływu biznesowego wybranego zgłoszenia |
| Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email |
| Duplikacja i replikacja zgłoszeń |
|  |
| **Konfiguracja** |
|  |
| Architektura drzewa dla kategorii zgłoszeń |
| Tworzenie szablonów odpowiedzi |
| Cykliczne raportowanie Listy incydentów |
| Utworzenie własnych dodatkowych atrybutów dla zgłoszeń |
| Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu |
| Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline) |
| Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP) |
| Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox) |
| Obsługa wielu kont pocztowych (Import + notyfikację email) |
| Tworzenie własnych trybów oraz priorytetów incydentów |
| Personalizacja widoku raportu listy incydentów |
| Profile zgłaszających w helpdesk |
| Personalizacja kolorów statusów zgłoszeń |
| Automatyczne przypisywanie zgłoszeń do użytkowników |
|  |
| **Moduł połączeń zdalnych** |
|  |
| Operacje na plikach i katalogach |
| Zarządzanie procesami i rejestrem |
| Monitoring pracy wykonywanej na komputerze |
| Zdalny podgląd pulpitów wielu stacji (Funkcja Company Online) |
| Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji |
| Wysyłanie wiadomości do użytkowników |
| Uruchamianie na stacjach programów z wiersza poleceń Command Line |
| Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan |
| Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego |
| Przejęcie kontroli nad stacją roboczą |
| Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego |
| Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie |
| Przejęcie kontroli nad komputerem bez zalogowanego użytkownika |
| Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu |
| Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen |
| Obsługa wielu monitorów dla podglądu pulpitu |
| Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu |
| Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie |
| Połączenie pulpitem zdalnym w konfiguracji NAT-NAT |
| Zarządzanie usługami systemu Windows |
| Raport Sesje zdalnego pulpitu |
| Wybór adresu IP, na którym ma być zestawione połączenie DirectPC |
| Wybór portu, na którym klient nasłuchuje połączenia zdalnego |
|  |
| **Baza wiedzy** |
|  |
| Wbudowana baza wiedzy |
| Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk |
| Edytor HTML |
| Osadzanie załączników w treści artykułów |
| Osadzanie multimediów w treści artykułów |
| Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych |
| Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk |
| Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów |
| Informacja o liczbie odsłon artykułu bazy wiedzy |
| Bezpośrednie linkowanie artykułów bazy wiedzy |
|  |
| **SLA** |
|  |
| Definiowanie planów umów SLA |
| Definiowanie czasu obowiązywania umów SLA |
| Definiowanie czasu pracy działów wsparcia technicznego |
| Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych |
| Definiowanie czasów reakcji oraz realizacji zgłoszenia |
| Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji |
| Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie |
| Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA |
|  |
| **Centralne repozytorium załączników** |
| **Funkcje** |
|  |
| Załączniki przechowywane w centralnym repozytorium |
| Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu) |
| Dodawanie i modyfikacja załączników z poziomu innych zasobów |
| Załączniki typu: link, udział oraz plik |
| Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura |
| Historia zmian załącznika |
|  |
| **Zarządzanie użytkownikami** |
| **Funkcje** |
|  |
| Raportowanie aktywności pracy |
| Przeglądanie ostatnio zgłoszonych incydentów |
| Powiązanie użytkownika z licencją |
| Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów |
| Cykliczne, automatyczne generowanie raportów |
| Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze |
| Zgłoszenia dotyczące wniosków nieobecności użytkowników |
| Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności |
| Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika |
| Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory |
| Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO |
| Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych |
| Planowanie dni wolnych w widoku kalendarza |
| Planowanie zastępstw podczas nieobecności |
|  |
| **Raportowanie cykliczne** |
| **Użytkownicy** |
|  |
| Raport historia sesji |
| Raport Nośniki danych |
| Raport Operacje na plikach |
| Raport wydruków |
| Raport użycia aplikacji |
| Raport odwiedzonych stron WWW |
| Raport Wysyłane pliki |
| Raport czasu pracy przy komputerze |
| Raport Bizlook |
|  |
| **Zasoby** |
|  |
| Raport historii zasobów |
| Raport informujący o nowych zasobach |
| Raport informujący o nadchodzących terminach w zasobach |
| Raport Zasoby zarchiwizowane |
|  |
| **Podstawowe** |
|  |
| Raport Informacje o autoryzowanych agentach |
|  |
| **Oprogramowanie** |
|  |
| Raport zainstalowanego oprogramowania |
| Raport Szczegóły plików |
|  |
| **Helpdesk** |
|  |
| Raport incydentów (Helpdesk) |
| Raport czasu pracy nad zgłoszeniem |
| Raport Czasy SLA |
|  |
| **Automatyzacja** |
| **Lista dostępnych reguł** |
|  |
| **Ogólne** |
|  |
| Zakończenie asysty serwisowej AS lub AS Plus |
| Wygaśnięcie certyfikatu SSL |
| Kończące się licencje na agenta |
| Zapełniona baza danych |
|  |
| **Zasoby** |
|  |
| Brak połączenia od agenta |
| Brak wolnej przestrzeni na dysku |
| Ostrzeżenie od Windows Security Center |
| Zakończenie skanowania sprzętu |
| Dodanie zasobu |
| Zmiana zasobu |
| Usunięcie zasobu |
| Zakończenie okresu gwarancyjnego |
| Zakończenie umowy serwisowej |
|  |
| **Oprogramowanie** |
|  |
| Zmiana oprogramowania |
| Zakończenie skanowania oprogramowania |
| Zamknięcie audytu |
|  |
| **Licencje** |
|  |
| Dodanie licencji |
| Zmiana licencji |
| Usunięcie licencji |
| Wygaśnięcie licencji |
| Planowana wymiana licencji |
|  |
| **Użytkownicy** |
|  |
| Dodanie użytkownika |
| Zmiana użytkownika |
| Usunięcie użytkownika |
|  |
| **Helpdesk** |
|  |
| Dodanie zgłoszenia |
| Usunięcie zgłoszenia |
| Zmiana zgłoszenia |
|  |
| **Lista dostępnych Akcji** |
|  |
| Wykonywanie skryptu na podstawie zdefiniowanej reguły |
| Wysłanie powiadomienia w konsoli Master |
| Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły |
| Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły |
|  |
|  |
| **RODO** |
| **Funkcje** |
|  |
| Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie |
| Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie |
| Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia |
| Wstępne wypełnienie wniosków o zmianę dostępu |
| Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji |
| Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych |
| Archiwizacja zbiorów |
| Definiowanie czynności przetwarzania |
| Przypisywanie zbioru danych do czynności przetwarzania |
| Przydzielanie dostępów do czynności przetwarzania |
| Zapisywanie historii zmian wniosków o dostęp do zbiorów |
|  |
| **Raporty** |
|  |
| Raport zbiorczy Czynności przetwarzania |
| Raport zbiorczy Zbiory danych |
| Raport zbiorczy zinwentaryzowanych dostępów |
| Raport zbiorczy zinwentaryzowanych powierzeń |
| Raport zbiorczy zinwentaryzowanych dokumentów |
| Raport zbiorczy historii naruszeń bezpieczeństwa |
| Raport zbiorczy wniosków o dostęp |
|  |
| **Sygnalista** |
| **Funkcje** |
|  |
| Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej |
| Usuwanie metadanych z załączników zgłoszeń |
| Usuwanie danych osobowych ze zgłoszeń |
| Podział interfejsu na publiczny oraz dla wewnętrzny |
| Dashboard podsumowujący wykorzystanie portalu sygnalisty |
| Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła |
| Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka |
| Definiowanie stron publicznych (dostępnych dla sygnalistów) |
| Obsługa wielu języków stron publicznych |
|  |
| **Raporty** |
|  |
| Raport zgłoszeń |
| Historia zmian |
| Statystyka zgłoszeń |
| Pozostały czas na przyjęcie zgłoszenia |
| Pozostały czas do zakończenia |
| Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane |
|  |
| **Portal Web** |
| **Funkcje** |
|  |
| Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów |
| Rozbudowane filtry dla raportów tabelarycznych |
| Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami |
| Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji |
| Raporty dla każdego modułu w formie tabelarycznej |
| Obsługa helpdesk oraz bazy wiedzy |
| Obsługa modułu RODO |
| Obsługa modułu automatyzacja |
| Automatyczne logowanie przy pomocy aplikacji |
| Logowanie za pomocą poświadczeń domenowych (SSO) |
| Wydruk raportów tabelarycznych |
| Kontrola statystyk użytkowników |
| Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania) |
| Przełączanie wersji językowej bez ponownego logowania do systemu |
| Nawigacja Breadcrumb |
|  |
| **Funkcjonalności ogólne** |
|  |
|  |
| Określanie praw dostępu do grup zasobów lub użytkowników |
| Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca") |
| Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem |
| Wersja angielska (en-US) interfejsu użytkownika |
| Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL |
| Swobodna migracja danych pomiędzy MS SQL i PostgreSQL |
| Zdalna instalacja i dezinstalacja agentów na stacjach roboczych |
| Odczytywanie struktury organizacji z Active Directory |
| Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta |
| Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta |
| Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory |
| Definiowanie nieograniczonej liczby użytkowników systemu |
| Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy |
| Indywidualny login i hasło dla poszczególnych użytkowników |
| Automatyczne logowanie do systemu |
| Zarządzanie uprawnieniami użytkowników - możliwość ograniczenia dostępu do poszczególnych funkcji programu |
| Określanie ról użytkowników - zarządzanie grupami |
| Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem |
| Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP) |
| Zgodny z pracą w sieciach WLAN |
| Podgląd aktualnych zadań serwera |
| Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników |
| Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami |
| Wyszukiwanie danych w tabelach raportów |
| Dowolne definiowania grup sprzętu i użytkowników |
| Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne |
| Definiowanie i zapamiętywanie własnych widoków |
| Eksport danych bezpośrednio do MS Excel |
| Budowa zestawień metodą drag'n'drop |
| Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów |
| Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server. |
| Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP |
| Mechanizm kompresji pakietów danych przesyłanych przez Agenta |
| Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery) |
| Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy) |
| Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server |
| Mechanizm zdalnego pobierania bieżących aktualizacji do programu |
| Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej |
| Dostęp do bazy wiedzy systemu |
| Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów) |
| Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym |
| Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania |
| Personalizacja pakietu instalacyjnego agenta |
| Określanie polityki haseł dla systemu |
| Zmiana języka systemu podczas logowania |
| Określenie numeru BDO przy definiowaniu rekordu firmy |
| Opcja resetu hasła podczas logowania |
| Globalne wyszukiwanie obiektów w systemie |
| Utworzenie atrybutów jako lista/słownik |
| Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników |
| Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring |
| Wyszukiwarka ustawień w opcjach systemowych |
| Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych) |
| Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie |
| Skanowanie lasu domen |
| Automatyczne zamknięcie programu po zakończeniu sesji |
| Logowanie do portalu Web za pomocą mechanizmu Single Sign On |
| Logowanie operacji kont serwisowych |
|  |
| **Dodatkowe informacje** |
|  |
|  |
| Wersja darmowa z ograniczeniem do 3 agentów oraz 3 użytkowników |
| Kreator instalacyjny ułatwiający wdrożenie systemu |
| Aplikacja Master\Server\ Agent w wersji x86\x64 |
| Rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach ) |
| Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019 32/64 bit) |
| Praca w oparciu o PostgreSQL 9.6 lub nowszy |
| Obsługa systemów operacyjnych - **Agent**: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11 |
| Obsługa systemów operacyjnych - **Master** : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11 |
| Obsługa systemów operacyjnych - **Serwer**: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, Windows 11 |
| Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem Symantec SHA256 TimeStamping Signer - G2 |
| Sterowniki systemowe są podpisane certyfikatem GlobalSign Extended Validation CodeSigning CA - SHA256 - G3 i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™. |
|  |

* **Oprogramowanie SIEM**

|  |  |
| --- | --- |
| Lp. | **Wymaganie** |
|  | Wszystkie opisane poniżej wymagania muszą być dostarczone jako wbudowana funkcjonalność produktu lub jako dodatkowe moduły oficjalnie dostarczane przez producenta w repozytorium aplikacji, a nie jako funcjonalność dodana w ramach dodatkowych prac konfiguracyjnych i integracyjnych |
|  | System musi zbierać dane z przynajmniej następujących źródeł: Windows, Linux, Oracle, ESET, urządzenia sieciowe: Stormshield, Mikrotik, Palo Alto, FortiGate, D-Link, Ruckus, Ubiquiti. W przypadku braku modułu integracyjnego dostępnego "z pudełka", dopuszczalne jest stworzenie modułu integracyjnego podczas prac wdrożeniowych. |
|  | System musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod. Minimalny wymagany zakres to: Syslog, CEF, LEEF, SNMP, Kafka, JDBC, flat file, OPSEC/LEA, |
|  | System musi umożliwiać analizowanie logów wielolinijkowych |
|  | System musi udostępniać mechanizmy pozwalające na integracje urządzeń źródłowych nie znajdujących się w powyższej liście, z wykorzystaniem graficznego kreatora reguł parsowania. |
|  | Graficzny kreator reguł parsowania musi obsługiwać co najmniej formaty: JSON, CEF, LEEF, lista, lista par "klucz-wartość", XML. |
|  | Graficzny kreator reguł parsowania musi umożliwiać tworzenie reguł z wykorzystaniem wyrażeń regularnych. |
|  | Graficzny kreator reguł parsowanie musi mieć możliwość podpowiadania użytkownikowi wzorca wyrażenia regularnego dla wskazanego łańcucha w payloadzie. |
|  | Mechanizmy integracji źródeł, zarówno tych wskazanych przy wdrożeniu, jak i integrowanych w przyszłości przez Zamawiającego, nie mogą być w żaden sposób ograniczane licencyjnie przez producenta ani wymagać dodatkowych opłat ze strony Zamawiającego. |
|  | System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu i pozwalać na równoległe używanie różnych sposobów normalizacji logów. |
|  | System musi posiadać możliwość automatycznego rozpoznawania źródeł logów, które są przekierowane do SIEM (zakładając, że posiada parser dla technologii tego źródła danych). Musi automatycznie rozpoznać typ logu i dobrać odpowiedni parser, tak aby nie była wymagana żadna aktywność ze strony administratora systemu |
|  | System musi umożliwiać pobieranie i analizę przepływów co najmniej w formatach: Netflow w wersji 1, 5, 7 i 9, IPFIX, sFLow w wersji 2, 4 i 5, J-Flow i Packeteer |
|  | System musi posiadać możliwość zainstalowania natywnego komponentu generującego dane o przepływach na podstawie analizy ruchu sieciowego |
|  | System musi mieć możliwość przeprowadzenia bezagentowej akwizycji danych. W uzasadnionych przypadkach dopuszczamy stosowanie agentów. W przypadku stosowania agentów, system nie może ograniczać licencyjnie ilości wykorzystywanych agentów. |
|  | Zbierane informacje muszą być poddane w systemie korelacji, na podstawie których administratorzy systemu będą informowani o stanie bezpieczeństwa infrastruktury Zamawiającego oraz ostrzegani o ewentualnych incydentach bezpieczeństwa |
|  | System musi zawierać bazę co najmniej 100 predefiniowanych reguł korelacyjnych, których wykorzystanie przez Zamawiającego nie wymaga ponoszenia dodatkowych nakładów z tym związanych. |
|  | System musi umożliwiać budowanie reguł korelacyjnych bazujących na zdarzeniach, przepływach, jednocześnie zdarzeniach i przepływach, a także na innych korelacjach |
|  | System umożliwia wykorzystanie reguł korelacyjnych jako bloków do wykorzystania w nadrzędnych regułach korelacyjnych. |
|  | System, oprócz prezentowania informacji o alertach w tablicach, musi posiadać możliwość powiadamiania o zdarzeniach co najmniej przez: powiadomienie ekranowe, e-mail, syslog, SNMP, wywołanie skryptu |
|  | System musi umożliwiać zastosowanie w regułach korelacyjnych testów logicznych na wartościach pól bazy danych zdarzeń i przepływów |
|  | System musi umożliwiać zastosowanie w regułach języka zapytań bazy danych zdarzeń i przepływów |
|  | System musi umożliwiać zastosowanie w regułach testów zawartości payloadu zdarzenia |
|  | Rozwiązanie musi posiadać wbudowane mechanizmy śledzące wydajność reguł korelacyjnych |
|  | System musi umożliwiać oznaczanie reguł taktykami i technikami frameworku MITTRE ATT&CK |
|  | System nie może wykorzystywać bazy danych ogólnego zastosowania do przechowywania zdarzeń i przepływów |
|  | Baza danych musi umożliwiać wydawanie poleceń w języku zapytań bazy danych. |
|  | Ze względu na zachowanie integralności danych, język bazy danych zdarzeń i przepływów może pozwalać na wykonanie jedynie polecenia SELECT. Baza danych nie może pozwalać na wykonywanie poleceń UPDATE, INSERT i DELETE. |
|  | Dane pochodzące z logów zapisywane są w domyślnie dostępnych polach bazy danych przynajmniej takich jak: nazwa zdarzenia, kategoria zdarzenia, adres IP źródłowy, źródłowy port TCP/IP, adres IP źródłowy przed translacją, adres IP źródłowy po translacji, czas urządzenia, z którego wysłany był log, nazwa protokołu, nazwa użytkownika, nazwa hosta, nazwa grupy, nazwa NetBIOS (o ile zawartość tych pól jest zawarta w logu) |
|  | Dane pochodzące z przepływów sieciowych muszą zostać domyślnie zapisane w dostępnych polach bazy danych przynajmniej takich jak: adres IP źródłowy, port źródłowy, adres IP docelowy, port docelowy, ilość wysłanych/odebranych |
|  | System musi umożliwiać dodanie własnych pól w bazie, które można przywoływać jako kryteria wyszukiwania, określane przy pomocy nowych wzorców |
|  | System musi przechowywać w bazie danych również payloady zdarzeń i przepływów |
|  | System musi umożliwiać wskazanie które pola mają być zapisywane w bazie danych bezpośrednio po otrzymaniu zdarzenia, a które nie. W tym drugim przypadku wartość pola jest każdorazowo wyznaczana z payloadu na podstawie reguł parsera w momencie użycia tego pola (np. przy wyświetleniu lub wykonaniu testu logicznego na polu) |
|  | System musi umożliwić zapisanie wzorca wyszukiwania, a także związanych z nim szablonów prezentacji oraz wyników w celu późniejszego przywołania lub też udostępnienia wyszukiwania innym użytkownikom. |
|  | System musi umożliwiać umieszczenie zapisanego wzorca w ramach utworzonej grupy wzorców, na tablicach (dashboard) oraz w miejscu umożliwiającym szybki dostęp |
|  | System musi być w stanie przyjąć i przetworzyć minimum 600 zdarzeń na sekundę (EPS) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów ilości zdarzeń bez ich utraty |
|  | System musi być w stanie przyjąć i przetworzyć minimum 6000 przepływów sieciowych na minutę (FPM) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów zdarzeń bez ich utraty |
|  | System musi mieć możliwość budowania profilu stanu i zachowania środowiska IT oraz identyfikowania odchyleń i wykrywania anomalii na podstawie analizy behawioralnej. |
|  | System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości w ostatnim okresie od wartości w okresie historycznym |
|  | System musi mieć możliwość wykrywania anomalii na podstawie przekroczenia wartości progowej |
|  | System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości od zarejestrowanego trendu |
|  | System musi umożliwiać tworzenie szablonów raportów |
|  | Wymagane formaty raportów: co najmniej PDF, HTML, XML, XLS, CSV. |
|  | System musi mieć możliwość generowania raportów zgodnie z ustalonym harmonogramem czasowym |
|  | System musi mieć możliwość wysyłania mailem raportów na wskazane adresy |
|  | System musi mieć możliwość weryfikowania tożsamości użytkowników poprzez wykorzystanie kont lokalnych oraz zewnętrzne systemy uwierzytelnienia – MS Active Directory oraz RADIUS i LDAP. |
|  | System musi zawierać funkcjonalność precyzyjnego nadawania uprawnień użytkownikom i administratorom. |
|  | System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości |
|  | System musi posiadać zaimplementowany dedykowany dashboard prezentujący dokładne statystyki związane z wydajnością systemu, co najmniej utylizacja CPU, utylizacja pamięci RAM, heap usage, disk IO throughtput, disk IOPS, statystyki połączeń sieciowych, ilość wykonywanych zapytań, statystyki dotyczące wywołań API itp. |
|  | System musi zapewniać centralne gromadzenie wszystkich logów i zapewniać ich bezpieczne przechowywanie oraz dostępność przez okres 90 dni |
|  | System musi samodzielnie zarządzać retencją danych |
|  | System musi umożliwiać wyspecyfikowanie różnego czasu retencji danych dla różnych zdarzeń i przepływów - na podstawie zawartości pól bazy danych |
|  | System musi posiadać mechanizm automatycznego archiwizowania danych i konfiguracji systemu do katalogu w lokalnym systemie plików i określenia retencji dla przechowywanych w ten sposób danych. |
|  | System musi umożliwiać włączenie lub wyłączenie indeksacji pola bazy danych z interfejsu graficznego |
|  | Zdarzenia i przepływy muszą być przechowywane w postaci skompresowanej |
|  | System musi zapewniać możliwość obsługi poprzez przeglądarkę |
|  | System musi udostępniać możliwość prezentacji statystyk i wyników działania w postaci tablic (dashboard), których wygląd i rozkład poszczególnych składowych daje się dostosować do potrzeb administratora i użytkownika. Widoczność stworzonych i domyślnie dostępnych tablic można przełączać przy pomocy łatwo dostępnej listy rozwijanych pozycji. |
|  | Informacje prezentowane w poszczególnych tablicach są wynikiem stworzonych przez producenta predefiniowanych korelacji, a także wyników wyszukiwania stworzonych przez użytkownika lub udostępnionych mu przez innych użytkowników i administratorów. |
|  | System nie może wymagać instalacji dedykowanego oprogramowania klienckiego do jego obsługi |
|  | System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtrów tworzonych przy pomocy pól wyboru |
|  | System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru wyspecyfikowanego w języku bazy danych |
|  | System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru specyfikującego słowo występujące w payloadzie |
|  | System musi mieć możliwość tworzenia clustra wysokodostępnego dla każdego z komponentów (za wyjątkiem agenta instalowanych na innym serwerze/stacji oraz analizatora ruchu sieciowego). Awaria pojedynczego komponentu nie może spowodować utraty funkcjonalności i wydajności systemu. |
|  | System musi posiadać architekturę skalowalną horyzontalnie poprzez dodawanie serwerów przechowujących część rozproszonej bazy danych i przetwarzających zdarzenia |
|  | Każda z reguł korelacyjnych musi mieć możliwość korelowania zdarzeń i przepływów z wszystkich serwerów przetwarzających dane, bądź z jednego serwera - zależnie od decyzji projektanta reguły |
|  | System musi umożliwiać prezentację zdarzeń i przepływów w postaci tabelarycznej, z możliwością wyboru okresu lub w czasie rzeczywistym |
|  | System musi posiadać dashboard prezentujący mapę, na której w czasie rzeczywistym są prezentowane incydenty lub dowolnie zdefiniowane zdarzenia. |
|  | System musi umożliwiać automatyczne łączenie wielu incydentów w jeden. |
|  | System musi posiadać aplikację monitorującą charakterystykę zachowań użytkowników (user behavior analysis), która pozwala na ocenę ryzykownych czynności podejmowanych przez wewnętrznych użytkowników na infrastrukturze. |
|  | Aplikacja analizująca zachowania użytkowników musi przypisywać użytkownikom tzw. punkty ryzyka i generować alarm po przekroczeniu wartości progowej sumarycznych punktów ryzyka. Wartość progowa może być ustalana statycznie (bezwzględna wartość liczbowa) lub dynamicznie (na podstawie rozkładu wartości punktów ryzyka dla całej populacji użytkowników) |
|  | Aplikacja musi wyświetlać kształtowanie się poziomu ryzyka dla użytkownika w czasie |
|  | System analizy zachowań użytkowników musi mieć możliwość wykorzystania uczenia maszynowego |
|  | Wbudowane modele uczenia maszynowego mają analizować trendy zachowań w czasie oraz porównywać zachowanie użytkownika z grupą innych użytkowników o podobnych parametrach charakteryzujących danego użytkownika - przykładowo ulokowanie w konkretnym kontenerze Active Directory lub posiadających konkretny atrybut (np. nazwa stanowiska) |
|  | Użytkownik musi mieć możliwość tworzenia własnych modeli uczenia maszynowego analizujących trendy zmian wartości w czasie |
|  | W przypadku braku zdefiniowanych grup użytkowników, system sam wykonuje grupowanie użytkowników na podstawie podobnych wzorców zachowań |
|  | System ma możliwość wyspecyfikowania grup użytkowników, dla których punkty ryzyka są modyfikowane o wyspecyfikowany mnożnik |
|  | System musi umożliwić automatyczną geolokalizację źródła zagrożeń. |
|  | System musi mieć możliwość tworzenia szczegółowego logu audytowego zawierającego informacje przynajmniej o logowaniu do systemu i zmianach w jego konfiguracji |
|  | Licencja systemu SIEM oraz system SIEM nie mogą ograniczać liczby równocześnie zalogowanych użytkowników |
|  | System musi posiadać możliwość automatycznego wykrywania nowych elementów infrastruktury poprzez analizę zdarzeń i/lub ruchu sieciowego. SIEM musi wykryć pojawienie się nowego adresu IP, adresu MAC i opcjonalnie zgłosić to operatorowi. |
|  | System musi posiadać możliwość automatycznego grupowania elementów infrastruktury poprzez ich cechy charakterystyczne. Przykładowo, system SIEM powinien być w stanie dokonać klasyfikacji elementów posiadających otwarte porty charakterystyczne dla baz danych jako "serwery bazodanowe" |
|  | System musi umożliwiać tworzenie własnego schematu opisu i oznaczania (tzw. tagowania) assetów |
|  | System musi umożliwiać filtrowanie assetów w oparciu o dowolne pole charakteryzujące dany element infastruktury |
|  | System musi zapewniać automatyczny mechanizm aplikacji poprawek do systemu. |
|  | System musi umożliwiać utworzenie struktury adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów |
|  | System musi umożliwić konfigurację serwera poczty, przez który wysyłane są wiadomości pocztowe. Musi być możliwość konfiguracji innych serwerów poczty dla różnych serwerów przetwarzających zdarzenia i przepływy. |
|  | System pozwala na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach o bardziej szczegółowe dane. |
|  | System pozwala na integrację z co najmniej tymi systemami zarządzania podatnościami: eEye, BigFix, Juniper NSM, nmap, Qualys, Rapid7, Tenable |
|  | System musi posiadać własną bazę reputacji IP |
|  | System musi posiadać możliwość przeprowadzenia korelacji historycznej, czyli symulacji działania reguły dla zdarzeń historycznych |
|  | System musi posiadać udokumentowany interfejs API |
|  | System musi posiadać narzędzie graficzne umożliwiające testowanie różnych zapytań API i weryfikację otrzymywanych danych |
|  | System musi umożliwiać rozdzielenie plików bazy danych na wiele "domen", z możliwością tworzenia oddzielnych reguł korelacyjnych dla domen |
|  | Licencja nie może bezpośrednio ograniczać wielkości przetwarzanych danych w bajtach. |
|  | System musi umożliwiać obfuskację (ukrywanie) danych wrażliwych zdarzeń i przepływów przed operatorem |
|  | System musi umożliwiać kontrolę integralności bazy danych przez zastosowanie hashowania |
|  | Producent systemu musi udostępniać zestawy dodatkowych reguł, ponad podstawowy zbiór reguł dostępny w produkcie po instalacji |
|  | System musi tworzyć indeks słów znajdujących się w payloadzie, w celu szybszego wyszukiwania zdarzeń. |
|  | System musi umożliwiać detekcję nadużycia protokołu DNS typu: DGA, squatting, tunelowanie |
|  | System musi umożliwiać tworzenie aplikacji osadzanych w interfejsie graficznym systemu |
|  | System musi mieć możliwość uniemożliwienia użytkownikom wykonywanie zapytań które mogą trwać zbyt długo lub wyszukiwań które będą zwracały dużą ilość danych co może mieć negatywny wpływ na wydajność systemu. Takie polityki muszą mieć możliwość definiowania na poziomie użytkownika, roli lub tenantów. |
|  | System oprócz podstawowego interfejsu przeglądania danych z funkcjonalnością administracyjną musi mieć dodatkowo odseparowany interfejs przeznaczony do pracy dla operatorów SOC. Interfejs ten musi być pozbawiony funkcjonalności administracyjnych i powinien w pełni być skoncentrowany na analizie incydentów bezpieczeństwa. |
|  | System musi zawierać funkcjonalność wsparcia przy tuningu reguł. System powinien raportować reguły które najczęściej inicjują incydenty bezpieczeństwa oraz reguły które są najmniej efektywne. |
|  | System musi automatycznie informować o nowych dodatkowych funkcjonalnościach dostępnych do ściągnięcia z dedykowanego repozytorium aplikacji. |
|  | System musi zawierać dedykowany dashboard który prezentuje przydatne artykuły, wiadomości, przypadku użycia, podcasty oraz odnośniki do szkoleń. Zawartość musi być dostosowana automatycznie do charakterystyki obsługiwanej infrastruktury |
|  | System musi umożliwiać wykorzystanie tzw. zapytań federacyjnych do różnych niezależnych instancji systemów SIEM w oparciu o format STIX |
|  | System musi umożliwiać prostą integrację z systemem klasy SOAR bez konieczności prowadzenia prac integracyjnych - przykładowo za pomocą gotowej aplikacji |
|  | Licencje na system nie mogą być dostarczane w modelu subskrypcyjnym (ograniczone czasowo) |
|  | Dodanie od system kolejnego komponentu analizującego/przechowującego zdarzenia/przepływy nie może wymagać dokupienia dodatkowej licencji |
|  | Utworzenie clustra HA komponentu poprzez dodanie serwera zapasowego nie może wymagać dokupienia dodatkowej licencji |
|  | System musi znajdować się w "ćwiartce liderów" w najnowszym opracowaniu tzw. magicznego kwadrata systemów SIEM wg. Gartnera. |
|  | Zwiększenie strumienia EPS (zdarzeń na sekundę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji |
|  | Zwiększenie strumienia FPM (przepływów na minutę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji |
|  | Okres gwarancji – min. 36 miesięcy |

* **Usługa serwisowania oraz monitorowania systemu SIEM z funkcją powiadamiania Administratora lokalnego o wystąpieniu zdarzenia niepożądanego - 36 miesięcy**
* **Oprogramowanie antywirusowe – 67 szt.**

Rozbudowa aktualnego oprogramowania antywirusowego **ESET PROTECT ESSENTIAL ON-PREM licencja GOV z okresem ważności do 2026.02.20.**

Zamawiający posiada aktualnie 133 szt. licencji ESET PROTECT ESSENTIAL ON-PREM – przedmiotem jest rozbudowa o dodatkowe licencje.

* **Certyfikat SSL typu Wildcard**
* **Karta sieciowa do serwer backup – 1 szt.**

Karta 2 portowa 10GB SFP+ do serwera Lenovo System x3650 M5 – 2017 r.

2x przewód DAC SFP, SFP+ 10Gb dł 3m - do połączenia karty sieciowej ze switchem.

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.