Opis przedmiotu zamówienia

Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w SP ZOZ Szpitalu Psychiatrycznym w Toszku ze środków pochodzących z Funduszu Przeciwdziałania COVID-19

Spis treści

Część 1

Modernizacja i rozszerzenie systemu antywirusowego

Zamawiający wymaga rozszerzenia funkcjonalności użytkowanego systemu antywirusowego ESET ENDPOINT ANTYVIRUS.

Zamawiający wymaga, aby Wykonawca był autoryzowanym dostawcą oprogramowania.

Dostawa oprogramowania w ramach zamówienia, obejmuje dostarczenie kodów licencyjnych lub nośników z programami ze wszelkimi kodami/instrukcjami, które umożliwią jego legalne i poprawne zainstalowanie oraz funkcjonowanie dla wszystkich zakupionych licencji.

Wykonawca zobowiązany jest zainstalować, skonfigurować i uruchomić dostarczone przez siebie rozwiązania w środowisku teleinformatycznym udostępnionym przez Zamawiającego.

Minimalne wymagania funkcjonalne

System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
System musi pracować w oparciu o architekturę Linux.
System musi mieć możliwość centralnego zbierania i zarządzania logami
System działać w trybie zbliżonym do rzeczywistego
System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
System musi zapewniać efektywną obsługę co najmniej 5000 EPS lub 100 GB danych dziennie
System musi zapewniać retencję danych w okresie minimum 365 dni.
Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.

Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
Interfejs musi posiadać angielską lub polską wersję językową.
System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poz
Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
System musi wspierać mechanizm logowania typu Single Sign On.
System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa
System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
System musi pozwalać na tworzenie parserów z poziomu GUI
System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
System musi zapewniać parsowanie spływających do niego wiadomości w formatach: Syslog, WEF, EventLog, WMI, SNMP, XML, JSON, CSV,email
System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.

System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
System musi posiadać predefiniowany zestaw parserów zdarzeń.
System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
Wykrycia dowolnej treści w logach,
Wykrycia wystąpienia wartości pola na wybranej liście,
Wykrycia niewystępowania wartości pola na wybranej liście,
Wykrycia zmiany jednego z kilku pól,
Wykrycia zdarzeń występujących z zadaną częstotliwością,

Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
Wykrycia zaniku Wiadomości,
Wykrycia nowej wartości pola w zadanym okresie czasu,
Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.

System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 3 lat.
Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.
Support producenta musi być świadczony w formule minimum 8/5.
Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.
Licencja testowa musi być objęta supportem producenta na takich samych zasadach jak licencja produkcyjna.
Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
System musi umożliwiać integrację z Mitre ATT@CK.
System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

Wymagania minimalne dla usługi chmurowej (Sandbox)

Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
Rozwiązanie musi wykorzystywać do działania chmurę producenta.
Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, Podejrzany, Bardzo podejrzany, Szkodliwy
W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

Wymagania dla systemu szyfrującego

System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.
System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej: ilość znaków/duże, małe litery, cyfry, znaki specjalne/okres ważności/mozliwość zmiany hasła/ilość nieudanych logowań
Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

Wymagania minimalne dla serwera EDR

Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.

Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, roz
Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotycz
Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
Konsola administracyjna musi mieć możliwość tagowania obiektów.
Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

Wymagania minimalne dla agenta na stacji roboczej

Agent musi posiadać pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11 oraz Windows Server 2008/2012/2016/2019/2022.
Agent musi posiadać pełne wsparcie dla 32 i 64-bitowej wersji systemu Windows.
Agent musi współpracować z produktem antywirusowym tego samego producenta.

Agent nie może działać bez produktu antywirusowego tego samego producenta.
W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.
Połączenie agenta do serwera zarządzającego musi być szyfrowane.
Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

Wymagania dla licencji

Ważność licencji 4 lata
Liczba nadzorowanych stacji roboczych: 230

Część 2

Urządzenia do uwierzytelnienia dwuskładnikowego

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania urządzenia w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania. Dokumentacja musi być sporządzona w języku polskim.

Charakterystyka (wymagania minimalne)

Zintegrowane z FortiClient i zabezpieczane przez FortiGuard
Zabezpieczenie sprzętowe
Wyświetlacz LCD 6 cyfrowy
Bateria litowa
Ważność OTP max 1 minuta
Odporność IP67
Żywotność baterii: 3 lata
Gwarancja: min 2 lata
Ilość urządzeń: 25

Część 3

Serwer kopii zapasowej

Wykonawca zobowiązany jest zainstalować, skonfigurować i uruchomić dostarczone przez siebie rozwiązania w środowisku teleinformatycznym udostępnionym przez Zamawiającego.

Zamawiający wymaga, aby Wykonawca dostarczył do urządzenia dokumentację Administratora – zawierającą opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego. Dokumentacja musi być sporządzona w języku polskim lub angielskim.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania urządzenia w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania. Dokumentacja musi być sporządzona w języku polskim.

Nazwa komponentu	***Wymagane minimalne parametry techniczne***
Obudowa	Obudowa typu TOWER , z możliwością instalacji min. 8 dysków Hot-Plug w ramach jednej obudowy, akcesoria do montażu w szafie rack
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta powinna obsługiwać minimum 24 sloty pamięci.
Procesor	Jeden procesor in 8 rdzeniowy i 16 wątkowy, osiągające w teście PassMark CPU Mark wynik min. 10100 punktów według wyników ze strony http://www.cpubenchmark.net dla konfiguracji jednoprocesorowej
Pamięć RAM	Minimum 32GB serwerowej pamięci RAM z korekcją błędów, z możliwością rozbudowy do 3 TB.
Sloty PCI Express	Minimum 2 slot PCI-Express x16 generacji 3.0. Minimum 2 slot PCI-Express x4 generacji 3.0.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	Minimum 6 porty USB ,minimum 1 port VGA Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 10Gbps Ethernet w standardzie BaseT

	Minimum dwa interfejsy 10/25GbE SFP28
Kontroler dysków	Zainstalowany 1 sprzętowy kontroler dyskowy z bateryjnym podtrzymaniem pamięci Cache. Kontroler musi obsługiwać dyski 3 Gbps SATA, 6 Gbps SATA/SAS, and 12 Gbps SAS zapewniając ich pełną przepustowość. Możliwe konfiguracje poziomów RAID 0, 1, 5, 6, 10, 50 ,60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min 8 GB.
Wewnętrzna pamięć masowa	Zainstalowane dyski twarde (parametry minimalne) • 2 x 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug 3,5” • 4 x 16TB SAS ISE 12Gb/s 7,2 tys. obr./min 512e 3,5" dysk twardy wymieniany bez wyłączania systemu
Zasilacze	Dwa redundantne zasilacze Hot Plug o mocy minimalnej 495W każdy wraz z kablami zasilającymi o dł.min. 1,8 m każdy.
Okablowanie	Kabel SFP28 do SFP28 25GbE (2 szt.), kabel SAS 12Gps (2 szt.)
Bezpieczeństwo	Wbudowany moduł TPM 2.0
Wentylatory	Minimum 8 redundantnych wentylatorów typu Hot-Plug.
Zarządzanie	Serwer musi posiadać kartę zarządzającą wyposażoną w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalającą na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Karta musi umożliwiać: - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika - podmontowanie zdalnych wirtualnych napędów, - dostęp do myszy, klawiatury z wykorzystaniem wirtualnej konsoli, - wsparcie dla IPv6, - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, Dostarczone oprogramowanie do zdalnego zarządzania serwerem musi umożliwiać: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień droga mailową lub poprzez SNMP.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE.
Oprogramowanie	1 licencja Windows Server 2022 Standard dobrana pod kątem licencyjnym do oferowanego procesora

Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Gwarancja	36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez infolinię telefoniczną producenta lub autoryzowanej firmy serwisującej. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

Część 4

Napęd taśmowy serwera kopii zapasowej wraz z materiałami eksploatacyjnymi

Zamawiający wymaga, aby Wykonawca dostarczył do urządzenia dokumentację Administratora – zawierającą opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego. Dokumentacja musi być sporządzona w języku polskim lub angielskim.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania urządzenia w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania – w wersji elektronicznej. Dokumentacja musi być sporządzona w języku polskim.

Charakterystyka (wymagania minimalne)

minimalna wysokość urządzenia 1U
minimalna ilość slotów na taśmy 8 szt
jeden mailslot
napęd LTO9 SAS
interfejs 2 SAS 12Gb/s
gwarancja standardowa rozszerzona do 60 miesięcy
serwis wykonujący gwarancję powinien posiadać certyfikat EN ISO/IEC 27001:2017 oraz ISO 90012015 w kierunku serwisu urządzeń do zabezpieczania/archiwizacji danych (załączniki)
kontakt do serwisu telefonicznie w języku polskim oraz na e-mail
udostępnienie najnowszych firmware dla urządzenia i napędu poprzez stronę internetową
Kompatybilność ze wszystkimi znanymi oprogramowaniami do backupu , takimi jak np. Veeam, Veritas BackupExec, Veeam, SEP, Comvault , NetVault , Archiware , ARCserve , Acronis, NovaStor
Niezależny interfejs RJ45 do zarządzania
Dokumentacja w języku polskim lub angielskim
Taśma czyszcząca zgodna z zaproponowanym urządzeniem
Taśma LTO-9 zgodna z zaproponowanym urządzeniem - 8 szt.
Etykiety do nośników - 16 szt.

Część 5

Oprogramowanie do wykonywani kopii zapasowej

Zamawiający wymaga, aby Wykonawca był autoryzowanym dostawcą oprogramowania.

Dostawa oprogramowania w ramach zamówienia, obejmuje dostarczenie kodów licencyjnych lub nośników z programami ze wszelkimi kodami/instrukcjami, które umożliwią jego legalne i poprawne zainstalowanie oraz funkcjonowanie dla wszystkich zakupionych licencji.

Wykonawca zobowiązany jest zainstalować, skonfigurować i uruchomić dostarczone przez siebie rozwiązania w środowisku teleinformatycznym udostępnionym przez Zamawiającego.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Charakterystyka (wymagania minimalne)

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs/Windows: NTFS, FAT, FAT32, ReFS
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux:
o Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
Rozwiązanie musi wspierać systemy operacyjne macOS
Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: dyskach i macierzach lokalnych, napędach taśmowych, zasobach sieciowych
Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla: Microsoft Active Directory 2012 i nowszych, Microsoft SQL 2005 i nowszych, Oracle 11g i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Wymagania dla licencji

Ważność: licencji 4 lata
Liczba urządzeń chronionych systemem kopii zapasowych: 30