Zał. Nr 7 do SIWZ

Szczegółowy opis przedmiotu zamówienia

W ramach zamówienia Wykonawca dostarczy, zainstaluje i wdroży moduły systemu zarządzania i monitorowania urządzeń w postaci MS System Center 2012 lub systemu równoważnegowraz z niezbędnym sprzętem serwerowym i zasilaniem UPS. Dostarczone rozwiązanie spełniać powinno minimalne wymagania:

A) Wymagania systemu w zakresie zarządzania infrastrukturą i oprogramowaniem.

System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji.

1. Inwentaryzacja i zarządzanie zasobami:

   a) Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętui oprogramowania,

   b) Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu,

   c) Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp...),

   d) System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta,

   e) Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera.

2. Użytkowane oprogramowanie – pomiar wykorzystania

   a) System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania,

   b) Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.

3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

4. Definiowanie i sprawdzanie standardu serwera:

   a) System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,

   b) Reguły powinny sprawdzać następujące elementy systemy komputerowego:

   - stan usługi (Windows Service),
   - obecność poprawek (Hotfix),
   - WMI,
   - rejestr systemowy,
   - system plików,
   - Active Directory,
   - SQL (query),
   - Metabase;

5. Raportowanie, prezentacja danych:

a) System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services,

b) System powinien posiadać predefiniowane raporty w następujących kategoriach:

- Sprzęt (inwentaryzacja),
- Oprogramowanie (inwentaryzacja),
- Oprogramowanie (wykorzystanie),
- Oprogramowanie (aktualizacje, w tym system operacyjny),

c) System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport,

d) System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu,

6. Analiza działania systemu, logi, komponenty:

a) Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy,

b) Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

B) Wymagania systemu w zakresie zarządzania komponentami.

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura:

a) Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być dostępne dla klientów systemu w celu automatycznej konfiguracji,

b) Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług,

c) System uprawnień musi być oparty o role (role basedsecurity), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych,

d) Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny,

e) Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509,z możliwością odrzucania połączeń od klientów niezaakceptowanych,

f) Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany,

2. Audyt zdarzeń bezpieczeństwa

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemówi gwarantować:

a) Przekazywanie zdarzeń z podległych klientów w czasie prawie rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących),

b) Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XMLz możliwością dodawania i modyfikacji,

c) Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie burst – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co

najmniej 10 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 20 serwerów,

3. Konfiguracja i monitorowanie

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a) Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

- rejestru,
- WMI,
- OLEDB,
- LDAP,
- skrypty (uruchamiane w celu wykrycia atrybutów obiektu),w definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi,

b) Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp.,

c) Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp. elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dlasystemów w których posiadaniu jest Zamawiający:

- Windows Server 2003/2008/2008R2/2012,
- Active Directory 2003/2008,/2012,
- Exchange 2010,
- SQL 2012,
- Windows Client OS (XP/Vista/7),
- Information Worker (Office, IExplorer, Outlook, itp...),
- IIS 6.0/7.0/7.5,

d) System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego,

e) System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:

- interfejsy sieciowe,
- porty,
- sieci wirtualne (VLAN),
- grupy Hot Standby Router Protocol (HSRP),

f) System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:

- SNMP (trap, probe),
- WMI Performance Counters,
- Log Files (text, text CSV),
- Windows Events (logisystemowe),
- Windows Services,
- Windows Performance Counters (perflib),
- WMI Events,
- Scripts (wyniki skryptów, np.: WSH, JSH),

g) Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów;

4. Tworzenie reguł

a) w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:

- Eventbased (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event),
- Performance based (SNMP performance, WMI performance, Windows performance),
- Probe based (scripts: event, performance),

b) System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia,

c) Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:

- na ilość takich samych próbek o takiej samej wartości,
- na procentową zmianę od ostatniej wartości próbki,

d) Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, uczenia się monitorowanego parametru w zakresie przebiegu bazowego baseline w zadanym okresie czasu,

e) System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji,

f) System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:

- ASP .Net Application,
- ASP .Net Web Service,
- OLE DB,
- TCP Port,
- Web Application,
- Windows Service 10,
- Process Monitoring,

Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji,

g) System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji,

h) Z każdym elementem monitorującym (monitor, reguła, alarm, itp.) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu),

i) System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych,

j) System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostepność), i licznika wydajności (z agregacją dla wartości – min, max, avg),

5. Przechowywanie i dostęp do informacji:

a) Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych,

b) System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w

obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane,

c) System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy),

d) System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności,

e) System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych,

f) System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:
- XML,
- CSV,
- TIFF,
- PDF,
- XLS,
- Web archive;

6. Konsola systemu zarządzania:

a) Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli,

b) System powinien udostępniać dwa rodzaje konsoli:
- w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna),
- w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa),

c) Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:
- Alerts,
- Events,
- State,
- Performance 11,
- Diagram,
- Task Status,
- Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu),

d) Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie,

e) Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp...), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach kolumnowych,

f) Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu,

g) Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza -- opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
- opcji definiowania ról użytkowników,
- opcji definiowania widoków,
- opcji definiowania i generowania raportów,
- opcji definiowania powiadomień,
- opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących,
- opcji instalacji/deinstalacji klienta,



h) Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego),

7. Wymagania dodatkowe:
   a) System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:
      - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
      - Wykonywanie operacji w systemie z poziomu linii poleceń,
      - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
      - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.

C) Wymagania systemuw zakresietworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych (macierz dyskowa) musi spełniać następujące wymagania:

1. System musi składać się z:
   a) serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych,
   b) agentów kopii zapasowych instalowanych na komputerach zdalnych,
   c) konsoli zarządzającej,
   d) relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
   e) wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną,
   f) system kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service).
2. System kopii zapasowych musi umożliwiać:
   a) zapis danych na puli magazynowej złożonej z dysków twardych,
   b) zapis danych na bibliotekach taśmowych.
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
   a) danych plikowych,
   b) danych aplikacyjnych,
   c) stanu systemu (Systemstate),
   d) obrazu systemu operacyjnego (tzw. Bare Metal Restore).
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych.



10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości.

11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy.

12. System kopii zapasowych musi rozpoznawać aplikacje:

a) ze względu na tworzone logi transakcyjne:
- Microsoft Exchange Server,
- Microsoft SQL Server,

b) ze względu na zapewnienie nieprzerwalności pracy
- Microsoft Hyper-V server,

13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach.

14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.

15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów.

16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.

17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki Poprzednie wersje.

18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.

19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.

20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku.

22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 5 lat.

23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.

24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.

25. System kopii zapasowych musi umożliwiać odtworzenie danych do:

a) lokalizacji oryginalnej

b) lokalizacji alternatywnej

c) w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych

D) Wymagania systemu w zakresie automatyzacji zarządzania środowisk IT.

System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.



2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.

3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.

4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.

5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow.

6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, do zarządzania oprogramowaniem i sprzętem.

E) Wymagania systemu w zakresie zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna).

2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.

3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.

4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.

5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:

- Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
- Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
- Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
- Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
- Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
- Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
- Tworzenie baz wiedzy na temat rozwiązywania problemów,
- Automatyzację działań w przypadku znanych i opisanych problemów,
- Wykrywanie odchyleń od założonych standardów ustalonych dla systemu;

F) Wymagania systemy w zakresie ochrony antymalware.

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.

2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem

3. Centralne zarządzanie politykami ochrony.

4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.

5. Mechanizmy wspomagające masową instalację.

6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię minifiltrów, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki

temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.

7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.

8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.

9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto gościa, itd.).

10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.

11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

12. Możliwość natywnego współdziałania z systemami typu rights-management

13. Możliwość filtrowania i blokowania zabronionych przez polityki treści czy słów kluczowych.

G) Wymagania i informacje ogólne.

1. Dostarczone i wdrożone oprogramowanie musi być w pełni kompatybilne ze sprzętem dostarczonym przez firmę projektującą i budującą sieć E-Leader, na którą składają się m. in. przełączniki CISCO z serii 3750X-24SE, 2960, serwery firmy HP.

2.Zamawiający zastrzega udział w zamówieniu pracowników firmy Atena (projektującej i budującej sieć E-Leader) jako ekspertów działających na rzecz Zamawiającego w celu zapewnienia kompatybilności dostarczonych przez Wykonawcę usług, sprzętu i budowanych punktów styku z nowopowstałą infrastrukturą E-Leader.

3.Zamawiający zastrzega udział w zamówieniu pracowników Instytutu Inteligentnych Systemów Informatycznych Wydziału Inżynierii Mechanicznej i Informatyki Politechniki Częstochowskiej, którzy są autorami dokumentacji Projektowej, jako ekspertów działających na rzecz Zamawiającego, stanowiących bazę wiedzy technicznej.

4.Dostarczone oprogramowanie będzie licencjonowane, a zamawiający nabędzie prawo do licencji w ramach tego zadania.

5.Sposób licencjonowania powinien uwzględniać oferty dla jednostek rządowych i zapewniać pokrycie ilościowe dla urządzeń serwerowych oraz klienckich wg załącznika nr 6.

6.Poszczególne licencje nie mogą być przypisane do konkretnego urządzenia (tzw. OEM).

7. W cenie zamówienia należy przewidzieć 5 lat aktualizacji.

8. Wszystkie dostarczone licencje muszą być nieograniczone czasowo, dedykowane dla jednostek samorządowych.

9. Jeżeli system zarządzania będzie wymagał jakichkolwiek dodatkowych licencji dla oprogramowania lub usług np. bazodanowych, licencji użytkowników serwerów WWW, to obowiązkiem Wykonawcy jest ich dostarczenie w niniejszym zamówieniu.

10. Zamawiający dopuszcza wizję lokalną w okresie od ogłoszenia zamówienia do terminu złożenia ofert w serwerowni Zamawiającego a także u wybranych Ostatecznych Beneficjentów objętych instalacją oprogramowania dostarczonego w ramach przedmiotowego Zamówienia.

11. Wsparcie techniczne:

Wymaga się, aby Wykonawca wraz z dostawą sprzętu i oprogramowania zapewnił bezpłatne wsparcie techniczne w wymiarze nie większym niż 600 osobo-godzin w okresie 6 miesięcy od bezusterkowego Protokołu Odbioru. Specjaliści wydelegowani do udzielenia wsparcia technicznego po otrzymaniu zgłoszenia od Zamawiającego muszą być dostępni w siedzibie Zamawiającego nie później niż 5 godzin od momentu zgłoszenia. Wsparcie techniczne musi być dostępne codziennie, 24 godziny na dobę, 7 dni w tygodniu.Wsparcie techniczne będzie udzielane przez minimum 2 osobowy zespół konsultantów specjalistów.

Wsparcie dotyczyć będzie zarówno konfiguracji urządzeń jak i usług objętych niniejszym zamówieniem.

H) Wdrożenie dostarczonego oprogramowania

Wdrożenie obejmuje następujące elementy

1) Instalacja i konfiguracja serwera, którego parametry zostały określone **pkt. J)** dedykowanego dla dostarczonego przez Wykonawcęoprogramowania. Zadanie to obejmuje:

a) dostawę i montaż serwera w szafie RACK i podłączenie go do istniejącej infrastruktury- przełączników, zasilania, itd. Wszystkie niezbędne do tego celu elementy (kable, porty do przełączników, itd..) powinien dostarczyć Wykonawca,

b) Instalacja i konfiguracja Systemu Windows Server 2012 Data Center SA na tym serwerze oraz usługi Hyper V. Oprogramowanie to ma obowiązek dostarczyć Wykonawca w ramach niniejszego zamówienia,
c) Instalacja i konfiguracja maszyn wirtualnych dla dodatkowych kontrolerów domen (Active Directory) dla domen już istniejących (Elider.net, MSC.local, BDK.local, UJD.local, CZN.local), na maszynach tych powinny znaleźć się także serwery DNS i DHCP pracujące w klastrze z już istniejącymi,
d) Instalacja i konfiguracja usługi PKI,
e) Instalacja i konfiguracja maszyn wirtualnych dla potrzeb dostarczonego rozwiązania System Center bądź rozwiązania równoważnego.

2) Należy dostarczyć, zamontować i uruchomić dodatkowe zasilanie rezerwowe (UPS) w obudowie RACK 19 cali o mocy pozornej nie mniejszej niż 3000 VA, mocy rzeczywistej, co najmniej 2700W. Oprogramowanie i sterowniki do urządzenia muszą być w pełni kompatybilnej wspierane przez Ms Hyper V oraz maszyny wirtualne z Windows 2012 Server. Komunikacja między ups a serwerem musi odbywać z wykorzystaniem sieciEthernet.UPS musi mieć możliwość monitorowania swojego otoczenia w zakresietemperatury i wilgotności, stosowne moduły do tego celu są objęte niniejszym zamówieniem. Zarządzanie i monitorowanie odbywać się musiprzynajmniej z wykorzystaniem protokołu http. Urządzenie musi wspierać możliwośćzdefiniowania, co najmniej 3 grup poziomów uprawnień;
3) Instalacja i konfiguracja oprogramowania klienckiego na 514 mobilnych stacjach roboczych znajdujących się na terenie mieszkańców 4 gmin;
4) Instalacja i konfiguracja oprogramowania klienckiego na 70 komputerach (57 plus istniejące w LPK) w Lokalnych Punktach Konsultacyjnych;
5) Instalacja i konfiguracja poszczególnych modułów oprogramowania serwerowego opisanego w niniejszym Zamówieniu;
6) Wykonawca dostarczy 10 sztuk modułów stackujących(flexstack moduł) do przełącznikówz serii CISCO 2960s, w których posiadaniu jest Zamawiający;
7) Wykonawca dostarczy także 10 wkładek optycznych do przełączników CISCO o przepustowości 10 Gb/s symboluSP-SM31020D-GP lub równoważnych o następujących minimalnych parametrach:

Dystans	***Moc nadajnika***		***Czułość***	***Przeciążenie***	***Pobór***
	Min	***Max***	***odbiornika***	***odbiornika***	***Mocy***
60km	(2)dBm	5dBm	(-20) dBm	(-8)dBm	nie większy niż 1.8W

I) Szkolenie

Ponadto Wykonawca dokona przeszkolenia pracowników Zamawiającego, m.in. w zakresie zarządzania i konfiguracji dostarczonego rozwiązania przez Wykonawcę.Szkolenie odbędzie się w dniu uzgodnionym pomiędzy Zamawiającym, a Wykonawcą nie później jednak niż w terminie do dnia **29.12.2014 r.** Przeszkolenie pracowników Zamawiającego będzie jednym z warunków niezbędnych do wystawienia końcowego protokołu odbioru przedmiotu zamówienia;Ilość uczestników, które wezmą udział w szkoleniu to ok. 10 osób, miejsce przeprowadzenia szkolenia – siedziba Zamawiającego, czas trwania szkolenia: łącznie do 16 godz.

J) Wymagania w zakresie serwera:

1. Obudowa o wysokości max. 2U dedykowana do zamontowania w szafie rack 19 cali z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
2. Dwa procesory serwerowe ośmiordzeniowe, 64bit, wspierające wirtualizację, minimalnaczęstotliwość taktowania rdzenia 2,6GHz, cache 16 MB
3. Pamięć RAM 64 GB Dual Rank x8 PC3-10600 (DDR3-1333) Registered
4. Możliwość konfiguracji pamięci z ochrona memory mirror
5. Możliwość instalacji w serwerze min 256 GB pamięci RAM
6. Minimum 3sloty PCI-Express, Serwer musi posiadać możliwość rozbudowy do 6 slotów PCIExpress. Jeśli nie ma możliwości rozbudowy, serwer musi posiadać 6 slotów PCI-Express wstandardzie.
7. 8 dysków 2,5 cala 300GB 6G SAS 10K , możliwość rozbudowy do min 8 dysków w serwerze
8. Kontroler macierzowy SAS wyposażony w pamięć cache co najmniej 512 MB oraz baterię podtrzymującą zawartość pamięci w razie awarii zasilania, zapewniający obsługę 8 napędów dyskowych SAS lub SATA oraz obsługujący poziomy RAID 0/1/1+0/5
9. 2porty Ethernet 10/100/1000/10000, Mb/s z funkcją Wake-On-LAN, RJ45,
10. Serwer musi posiadać gniazdo do instalacji modułu TPM
11. Zintegrowana karta graficzna
12. 1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
13. 4porty USB (w tym jeden port wewnętrzny)
14. 1 port VGA (15-pin video)
15. 1 port szeregowy
16. Porty do podłączenia klawiatury i myszy
17. Napęd DVD
18. Redundantne zasilacze Hot-Plug minimum dwa w oferowanym serwerze
19. Redundantne wiatraki typu Hot-Plug
20. Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS).
Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
21. Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycz.
Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI
22. Panel serwisowy, prezentujący poprawność pracy poszczególnych elementów serwera.
23. Serwer musi posiadać wsparcie dla systemów: MS Windows Server 2012 i platformy Hyper V.

24. Ze względu na już istniejącą infrastrukturę i wykorzystywane oprogramowanie systemowe wymagany jest System operacyjny Windows 2012DataCenter SA lub nowszy umożliwiający skonfigurowanie co najmniej pięciu serwerów wirtualnych.
25. Serwer powinien być wyposażony w streamer o minimalnych wymaganiach:
- Interfejs SCSI
- Pojemność 1.6 TB, bufor 128 MB
- Funkcja szyfrująca AES 256 bit
- Szybkość przesyłania danych ponad 450 GB/s
- Musi zawierać zestaw sterowników dla Windows 2012 Server oraz współpracować z Systemem Zarządzania urządzeniami w sieci E-Leader, które zostanie dostarczone w ramach niniejszego zamówienia. Interfejs komunikacyjny z serwerem musi być kompatybilny z maszynami wirtualnymi osadzonymi na Hyper V.
W przypadku zastosowania streamer zewnętrznego musi być on przystosowany do montażu w szafie RACK.
Wykonawca ma obowiązek dostarczyć zestaw 10 kaset do zapisu danych, wykonać montaż i podłączenie urządzenia. Dostawa niezbędnych kabli leży po stronie Wykonawcy

Zamawiający informuje, że komputery klienckie, na których ma zostać przeprowadzona instalacja są obecnie dodane do usługi Active Directory. 514 mobilnych stacji roboczych znajduje się u użytkowników, którzy zamieszkują obszar 4 gmin. Podłączeni są oni do sieci Eleader przy pomocy łączy WiFi o przepustowości 2 Mb/s. Wykonawca musi dopuścić sytuację, w której niektóre komputery w wyniku korzystania z nich przez użytkowników zostały wyrzucone z katalogu AD. Ze względu na dynamiczną sytuację Zamawiający nie jest w stanie określić dokładnie tej liczby. W takim przypadku (stacja odłączona od AD) Wykonawca ma obowiązek dodać dany komputer do katalogu tej usługi.

K) Wykaz sprzętu i komponentów zamawiającego do zarządzania:
Serwery HP z serii DL380 + Microsoft Windows Server 2012 Datacenter 64bit – 4 sztuki
- Notebooki (HP ProBook serii 6400) - 514 sztuk
- Komputery dedykowane (HP Compaq z serii 6000) - 57 sztuk.