****

 **Załącznik nr 1 do oferty**

**DOSTAWA SPRZĘTU**

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymaganie minimalne** | **Parametry i Spełnienie wymagań****Spełnia /nie spełnia****Wypełnia wykonawca** |
| **Obudowa** | Obudowa o wysokości 2U do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Obudowa w ramach cache musi posiadać zainstalowane minimum 4 dyski 1.92TB SSD SAS każdy. |  |
| **Architektura** | Oferowany deduplikator musi być zbudowany w oparciu o architekturę active-active tj. posiada minimum dwa kontrolery do obsługi danych, pracujące nadmariowo w trybie active-active |  |
| **Kontrolery** | Deduplikator musi być wyposażona w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.  |  |
| **Wydajność kopii zapasowych** | Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Wydajność podawana bez uwzględnienia deduplikacji na źródle. |  |
| **Wydajność odtworzenia kopii zapasowych** | Oferowany model deduplikatora w oferowanej konfiguracji musi osiągać zagregowaną wydajność odtworzenia backupu co najmniej 0.8 TB/h. Wymagane oświadczenia producenta lub wydruk z oryginalnego estymatora producenta. |  |
| **Wymagana przestrzeń** | Przestrzeń użytkowa HDD po zbudowaniu RAID 6 (z min. dyskiem hot-spare lub przestrzenią hot-spare) musi wynosić min 16 TB. Ze względów wydajnościowych oraz niezawodnościowych pojemność RAW pojedynczego dysku nie może być większa niż 4 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń hot-*spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.  |  |
| **Zabezpieczenie RAID** | Dane przechowywane w obrębie urządzenia na dyskach HDD muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 3 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-Mpoprzez mechanizm nadpisywania danych. |  |
| **Pamięć cache** | Co najmniej 256GB pamięci cache zbudowanej z pamięci RAM (nie dopuszcza się zbudowania 256GB pamięci cache w ramach dysków SSD) na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.  |  |
| **Dostępne interfejsy** | Urządzenie musi posiadać minimum:8 portów Ethernet 10Gb/s SFP+ z możliwością obsługi każdym portem Ethernet protokołów iSCSI, CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne.4 portów Ethernet 10Gb/s SFP+ wszystkie porty wyposażone we wkładki optyczne oraz 8 portów Ethernet Gb/s RJ45.Minimum 12 przewodów każdy o długości minimum 3 metry dla powyższych portów Ethernet 10Gb/s SFP+. |  |
| **Obsługiwane protokoły** | Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.  |  |
| **Szyfrowanie** | Deduplikator musi zapewniać szyfrowanie zasobów w ramach zastosowania algorytmu AES. |  |
| **Zarządzanie** | Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:- cały deduplikator- kontrolery- CPU- porty front-end- porty logiczne- dyski- file systemyPod kątem parametrów takich jak:- operacje wejścia/wyjścia IOPS- przepustowość (KB/s lub MB/s)- czas odpowiedzi (latency)- średnie użycie (w % dla CPU)Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagany dostęp do prognozy zużycia przestrzeni.Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| **Redukcja danych** | Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej oczekiwanej pojemności. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych min. 60:1. |  |
| **Kontrola zasobów plikowych** | Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.Dostarczenie powyższych funkcjonalności jest wymagane wraz z dostawą przedmiotu zamówienia. |  |
| **Ochrona zasobów plikowych** | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia.Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia.Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia. |  |
| **Replikacja danych** | Urządzenie musi umożliwiać replikację danych do drugiego takiego samego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00).Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.Dostarczenie powyższych funkcjonalności nie jest wymagane wraz z dostawą przedmiotu zamówienia. |  |
| **Wspierana oprogramowania do kopii zapasowych** | Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam. |  |
| **Obsługa serwisowa** | Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż w 2024 roku i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.Usługi gwarancyjne muszą być świadczone przez producenta lub autoryzowanego przedstawiciela producenta posiadającego co najmniej certyfikat ISO 9001 na świadczenie usług serwisowych.Urządzenie musi zostać objęte minimum 36 miesięcznym okresem gwarancji w trybie 9x5 NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki.Deduplikator musi posiadać możliwość upgradeu firmware-u kontrolerów bez przerywania dostępu do danych.Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.Urządzenie musi umożliwiać zdalne zarządzanie. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:• możliwość pobierania najnowszego firmware.• dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń.• dostęp do centrum pomocy technicznej producenta.• otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware.• otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z deduplikatorem oraz oprogramowania wewnętrznego deduplikatora.W przypadku awarii dysków uszkodzone nośniki pozostają u Zamawiającego. |  |

Zasilacz awaryjny UPS – 4 sztuki

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymaganie minimalne** | **Parametry i Spełnienie wymagań****Spełnia /nie spełnia****Wypełnia wykonawca** |
| **Obudowa** | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.Maksymalna wysokość: 4UMaksymalna głębokość: 800mm |  |
| **Moc znamionowa** | Min. 2700W |  |
| **Zakres napięcia wejściowego** | Min. 110-290V |  |
| **Napięcie nominalne wyjściowe** | 200/208/220/230/240V AC |  |
| **Gniazda wyjściowe** | 6x IEC320 C13-10A (podzielone na dwa segmenty z możliwością przydzielenia odrębnych ustawień) |  |
| **Czas podtrzymania** | Dla obciążenia 100% - min. 3 minuty |  |
| **Interfejs użytkownika** | Wyświetlacz LCD |  |
| **Gwarancja** | Min. 24 miesiące na sprzęt i akumulatory |  |

Serwer

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymaganie minimalne** | **Parametry i Spełnienie wymagań****Spełnia /nie spełnia****Wypełnia wykonawca** |
| **Obudowa** | Rack |  |
| **Wysokość** | Max 2U |  |
| **Procesor**  | DWA procesory MIN 16 RDZENI taktowanie rdzenia MIN 2.4 GHz,  |  |
| **Pamięć** | 32 gniazda DIMM z dwoma procesorami (16 gniazd DIMM na procesor). Każdy procesor ma 8 kanałów pamięci, z 2 modułami DIMM na kanał. ZAINSTALOWANE 128GB W modułach RDIMM 3200 MHz  |  |
| **Maksymalna pamięć** | Do 8 TB z 32 modułami 3DS RDIMM 256 GB |  |
| **Ochrona pamięci** | ECC, SDDC, Patrol/Demand Scrubbing, DRAM Address Command Parity with Replay, DRAM Uncorrected ECC Error Retry, Post Package Repair |  |
| **Kieszenie na dyski** | Wymagane min 8 szt. 2,5-calowych wnęk na dyski typu hot-swap, z możliwością wymiany podczas pracy |  |
| **pamięć wewnętrzna** | 2 x dysk min 480GB , 6x dysk 1,92 TB ssd  |  |
| **Kontroler pamięci masowej** | Wbudowany NVMe (bez RAID) Wbudowane złącze SATA (bez RAID) Adapter SAS/SATA RAID: z 2 GB pamięci podręcznej z obsługą pamięci flash obsługa RAID 0, 1, 10, 5, 50, 6, 60 |  |
| **Interfejsy sieciowe** | Wymagane : 2 porty 10/25 GbE  |  |
| **Gniazda rozszerzeń PCI** | 2 gniazda PCIe 4.0 x16 |  |
| **Porty** | Przód: 1x port USB 3.1 G1 (5 Gb/s), 1x port USB 2.0 zewnętrzny port diagnostyczny wraz panelem LCD lub rozwiązanie równoważne Tył: 3 porty USB 3.1 G1 (5 Gb/s), 1 port wideo VGA, 1 port zarządzania systemami RJ-45 1 GbE do zdalnego zarządzaniaWewnętrzne: 1x złącze USB 3.1 G1 do systemu operacyjnego lub klucza licencyjnego |  |
| **Chłodzenie** | 6 nadmiarowych wentylatorów 60 mm N+1 z możliwością wymiany podczas pracy, w zależności od konfiguracji. Jeden wentylator zintegrowany w każdym zasilaczu. |  |
| **Zasilacz** | Dwa zasilacze sieciowe z możliwością wymiany podczas pracy, certyfikat 80 PLUS Platinum. min 750 W obsługujące 220 V AC. obsługujące również zasilanie wejściowe 110 V.  |  |
| **Wideo** | Grafika G200 z 16 MB pamięci z akceleratorem sprzętowym 2D, zintegrowana z kontrolerem XClarity. Maksymalna rozdzielczość to 1920x1200 32 bpp przy 60 Hz. |  |
| **Części wymieniane podczas pracy serwera** | Napędy, zasilacze, wentylatory. |  |
| **Zarządzanie systemami** | Dedykowany port wraz z kontrolerem do monitorowania parametrów serwera z funkcją zdalnego sterowania obsługę montowania zdalnych plików multimedialnych (plików obrazów ISO i IMG)  |  |
| **Funkcjonalność związana z bezpieczeństwem** | Przełącznik naruszenia obudowy, hasło włączenia zasilania, hasło administratora, Trusted Platform Module (TPM), obsługa TPM 2.0.  |  |
| **Obsługiwane systemy operacyjne** | Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi.  |  |
| **Gwarancja** | 3letnia na miejscu z 9x5 następnego dnia roboczego (NBD)., realizowana przez autoryzowany serwis producenta lub partnera serwisowego  |  |
| **Serwis i wsparcie** | Możliwość rozszerzenia usługi gwarancji producenta w trakcie trwania gwarancji o 2-godzinny czas reakcji wraz z 4-godzinnym czasem naprawy w dowolnym momencie w ciągu 5 lat trwania serwisu. W przypadku niesprawności dysków w ramach naprawy gwarancyjnej pozostają one u Zamawiająćego. |  |
| **Wymiary**  | Dostosowane do szafy 42U o głębokości 80 cm Serwer dostarczony wraz z szynami montażowymi do wysuwania serwera  |  |

Przełącznik sieciowy – 3 sztuki

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymaganie minimalne** | **Parametry i Spełnienie wymagań****Spełnia /nie spełnia****Wypełnia wykonawca** |
| **Obudowa** | Rack |  |
| **Architektura sieci** | Gigabit Ethernet |  |
| **Dostęp**  | Przeglądarka WWW (GUI)Wiersz poleceń (CLI)SNMP v1/v2c/v3RMONSNTPTelnetAplikacja |  |
| **Całkowita liczba portów** | 28 |  |
| **Złącza** | RJ-45 10/100/1000 Mbps - 24 szt.SFP - 4 szt.Console port - 1 szt.microUSB Console Port - 1 szt. |  |
| **Liczba portów PoE/PoE+** | 24 |  |
| **Rozmiar tablicy MAC** | 8k |  |
| **Ramka Jumbo** | 9,000 B |  |
| **Liczba grup VLAN** | 4096 |  |

**DOSTAWA OPROGRAMOWANIA**

Oprogramowanie do monitoringu serwerów oraz usług

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Spełnienie wymagań****Spełnia /nie spełnia****(wypełnia Wykonawca)** |
| **Ogólne** | Głównym zadaniem do realizacji przez system monitoringu jest zarządzanie wydajnością i dostępnością w zakresie komponentów tj.:- serwery- urządzenia sieciowe- bazy danych- aplikacjeSystem musi wspomagać administrowaniu w proaktywnym zarządzaniu kondycją infrastruktury IT identyfikując potencjalne problemy i awarie, zanim wpłyną one negatywnie na działanie Urzędu. |  |
| System musi umożliwiać monitorowanie urządzeń zarówno w sposób agentowy jak i bezagentowy (sieciowy) |  |
| System musi umożliwiać monitorowanie agentowe co najmniej systemów:- Microsoft Windows- Linux (dowolna dystrybucja)- MacOS |  |
| System musi posiadać możliwość monitorowanie bezagentowego dostępności i wydajności dowolnej witryny WWW |  |
| System musi umożliwiać bezagentowy monitoring z wykorzystaniem protokołów SNMP |  |
| System musi być dostarczony na licencji umożliwiającej na monitorowanie dowolnej liczby komponentów IT i pracę dowolnej liczby operatorów |  |
| System musi posiadać narzędzia do zbierania danych o wydajności i dostępności usług |  |
| System musi umożliwiać konfigurację interwałów i częstotliwości monitoringu poszczególnych komponentów lub grup komponentów |  |
| System musi posiadać narzędzia umożliwiające wizualizację danych w postaci wykresów |  |
| System musi umożliwiać budowanie map infrastruktury sieci oraz osadzania komponentów na mapach |  |
| System musi posiadać mechanizm alertów z możliwością ich wysyłki co najmniej przez email, sms, MS Teams |  |
| System musi posiadać API umożliwiającego integrację z innymi narzędziami |  |
| System musi posiadać funkcję wykrywania anomalii oraz monitorowania trendów |  |
| System musi posiadać możliwość definiowania i zamawiania okresowych raportów dotyczących kondycji środowiska |  |
| System musi posiadać mechanizm budowania dedykowanych kokpitów do monitoringu |  |
| Komunikacja pomiędzy wszystkimi komponentami systemu musi odbywać się z wykorzystaniem bezpiecznych i szyfrowanych połączeń |  |
| System musi posiadać rozbudowany moduł zarządzania użytkownikami, grupami użytkowników oraz uprawnieniami |  |
| System musi umożliwiać uwierzytelnianie użytkowników przy pomocy:- kont wbudowanych- usługi katalogowej LDAP/AD- usługi pojedynczego logowania SSO |  |
| System musi posiadać narzędzia do automatycznego wykrywania topologii sieci oraz wykrywania i podłączania komponentów |  |

Oprogramowanie do zarządzania incydentami

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Spełnienie wymagań****Spełnia/nie spełnia****(wypełnia Wykonawca)** |
| **Ogólne** | System do zarządzania incydentami ma na celu kompleksową obsługę zgłoszeń incydentów w zakresie:- przyjęcie zgłoszenia- przypisanie odpowiedniej obsługi zgodnie z kontaktem (SLA)- obsługa wielokrokowa zgłoszenia wraz z informowaniem zgłaszającego oraz zapewnieniem automatycznej eskalacji- zamknięcie zgłoszenia- raportowanie ilościowe i jakościowe w zakresie obsługi zgłoszeń |  |
| System musi obsługiwać zgłoszenia z następujących źródeł:- dedykowany portal klienta- wiadomość email- zgoszenie telefoniczne (rejestracja przez operatora infolinii)- zgłoszenie automatyczne z systemu monitorowania lub SIEM |  |
| System powinien zawierać dwukierunkowe API w technologii REST |  |
| System powinien posiadać wbudowany dziennik zdarzeń umożliwiający na podgląd komunikatów systemowych, błędów w obsłudze skrzynek email, błędów API, informacji o wydajności |  |
| System powinien umożliwiać podgląd i zarządzanie sesjami użytkowników |  |
| System musi posiadać dokumentację dla administratora oraz użytkowników |  |
| System musi posiadać możliwość rozbudowy z wykorzystaniem mechanizmu wtyczek, w taki sposób aby możliwe było dodawanie nowych funkcjonalności bez konieczności modyfikacji rdzenia systemu |  |
| **Administracja** | System musi umożliwiać tworzenie dowolnej liczby kolejek do obsługi zgłoszeń, grupowanie kolejek oraz tworzenia podkolejek |  |
| System musi umożliwiać zarządzanie użytkownikami odpowiedzialnymi za realizację zgłoszeń tj. dodawanie, edycja, przypisywanie do grup, przypisywanie do kolejek z odpowiednimi uprawnieniami |  |
| System musi pozwalać na zarządzanie usługami, w tym w szczególności raportowaniem w ich kontekście |  |
| System musi posiadać mechanizm definiowania szablonów podpisów oraz ich przypisywanie do wybranych kolejek |  |
| System musi posiadać mechanizm definiowania szablonów automatycznych odpowiedzi oraz ich przypisywania do wybranych kolejek |  |
| System musi posiadać mechanizm definiowania umów SLA z obsługą kalendarzy oraz możliwością zdefiniowania odpowiednich poziomów i czasów eskalacji dla zgłoszeń oraz możliwością przypisywania umów do odpowiednich kolejek |  |
| System musi posiadać mechanizm definiowania priorytetów dla zgłoszeń |  |
| System musi posiadać mechanizm definiowania schematów wiadomości oraz ich użycia w dowolnym momencie obsługi zgłoszenia przez operatora |  |
| System musi umożliwiać konfigurację dowolnej liczby skrzynek email (IMAP/POP3), z których pobieraną będą wiadomości na podstawie których zakładane będą zgłoszenia. |  |
| System musi umożliwiać połączenie wybranej skrzynki email z kolejką zgłoszeń |  |
| System musi umożliwiać automatyczne dekretowanie zgłoszeń drogą mailową do kolejek na podstawie adresata lub fragmentu adresu email |  |
| **Zgłaszanie i obsługa incydentów** | Zgłoszenie incydentów musi być możliwe z wykorzystaniem dedykowanego portalu klienta z wykorzystaniem przeglądarki internetowej, bez konieczności instalacji dodatkowego oprogramowania na komputerze zgłaszającego. |  |
| System musi umożliwiać konfigurację dwuskładnikowego uwierzytelnianie dla użytkowników |  |
| System musi posiadać rozbudowaną wyszukiwarkę |  |
| System mus posiadać wersję kontrastową interfejsu użytkownika w celu dostosowanie do wymogów WCAG |  |
| System musi umożliwiać dodawania notatek do zgłoszeń z możliwością decydowania o ich widoczności dla poszczególnych grup użytkowników |  |
| System musi umożliwiać łączenie i dzielenie zgłoszeń oraz dodawanie linków (relacji) pomiędzy zgłoszeniami |  |
| System musi dostarczać mechanizm operacji masowych tj. grupowa zmiana statusu, przenoszenie pomiędzy kolejkami |  |
| Użytkownik systemu musi posiadać dostęp do wszystkich swoich zgłoszeń wraz z podglądem historii obsługi każdego zgłoszenia |  |

System SIEM

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Spełnienie wymagań****Spełnia/nie spełnia****(wypełnia Wykonawca)** |
| **Serwer** | System musi być rozwiązaniem klasy SIEM z rozszerzeniem XDR umożliwiającym monitorowanie bezpieczeństwa, wykrywania zagrożeń, monitorowania integralności oraz odpowiedzi na incydenty. |  |
| System musi umożliwiać monitorowanie infrastruktury IT w czasie rzeczywistym. Infrastruktura IT Zamawiającego składa się z:* 2 serwery
* 1 urządzeń UTM
* 3 przełączników sieciowych
* 33 komputery
 |  |
| Komponenty serwerowe systemu muszą być możliwe do zainstalowania na systemie operacyjnym z rodziny Linux. |  |
| System musi być możliwy do zainstalowania w środowisku wirtualizacyjnym opartym o Proxmox VE. |  |
| Instalacja i konfiguracja systemu musi być możliwa do automatyzacji z wykorzystaniem Ansible. |  |
| Wykonawca w ramach postępowania dostarczy wszelkie niezbędne licencje umożliwiające uruchomienie Systemu takie jak np. systemy operacyjne, serwery baz danych, itp. |  |
| System musi być dostarczony w konfiguracji wysokodostępnej (klaster High Availability) dla każdego z komponentów z wyłączeniem agentów. |  |
| System musi umożliwiać monitorowanie agentowe oraz bezagentowe (sieciowe). |  |
| Silnik system musi udostępniać API w technologii REST pozwalające na rejestrację zdarzeń, zarządzanie konfiguracją agentów oraz odczyt stanu każdego z monitorowanych komponentów. |  |
| Logowanie operatorów do systemu musi odbywać się z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością (SSO) co najmniej w zakresie protokołu SAML2. |  |
| System musi posiadać kontrolę dostępu opartą na rolach (RBAC). |  |
| System musi posiadać funkcję wysyłania powiadomień do użytkowników lub grup w odpowiedzi na występujące zagrożenia. System musi wysyłać powiadomienia co najmniej za pomocą email oraz SMS. |  |
| System musi być dostarczony wraz z wbudowanymi regułami detekcji. Musi istnieć możliwość dodawania własnych reguł. |  |
| System musi umożliwiać zaawansowane metody detekcji poprzez integrację z frameworkiem MITRE ATT&CK. |  |
| System musi wykrywać i aktywnie blokować ataki typu brute-force na hasła systemów operacyjnych. |  |
| System musi umożliwiać integrację z oprogramowaniem NIDS tj. Suricata. |  |
| System musi wykrywać i zapobiegać atakom typu SQL Injection. |  |
| System musi wykrywać i blokować ataki typu DDoS. |  |
| System musi umożliwiać wykrywania i usuwanie malware poprzez integrację z zewnętrznymi bazami i narzędziami tj. VirusTotal. |  |
| System musi wykrywać znane podatności na każdym monitorowanym obiekcie z wykorzystaniem baz CVE. |  |
| System musi wykrywać ukryte procesy oraz wykonywanie podejrzanych operacji przez zainstalowane w systemie operacyjnym monitorowanego obiektu aplikacje. |  |
| **Agent** | System musi udostępniać dedykowane pliki instalacyjne agentów dla systemów co najmniej Windows, Linux oraz MacOS. |  |
| Agent musi komunikować się z serwerem systemu za pomocą szyfrowanego i autoryzowanego połączenia. |  |
| Agent musi posiadać funkcjonalność zdalnej konfiguracji oraz zdalnej aktualizacji po podłączeniu się do serwera. |  |
| Agent musi posiadać budowę modułową z możliwością wyłączenia poszczególnych modułów w zależności od wymaganej konfiguracji oraz możliwości wydajnościowych monitorowanego obiektu. |  |
| Agent musi posiadać co najmniej następujące moduły:* Moduł zbierania logów (kolektor logów)
* Moduł wykonywania poleceń
* Moduł monitorowania integralności plików
* Moduł inwentaryzacji zasobów
* Moduł oceny konfiguracji bezpieczeństwa (SCA)
* Moduł wykrywania podatności
* Moduł zgodności ze standardami bezpieczeństwa
* Moduł reaktywnej odpowiedzi
* Moduł wykrywania malware
 |  |
| Agent musi posiadać kolektor logów wspierający filtry XPath do przetwarzania Dziennika zdarzeń systemu Windows. |  |
| Kolektor logów musi wspierać odczyt wielolinijkowych logów (co najmniej format Linux Audit). |  |
| Monitor integralności plików musi umożliwiać rejestrowania zdarzeń tj. utworzenie pliku, modyfikacja lub usunięcie wraz ze wskazaniem użytkownika oraz czasu zdarzenia. Dodatkowo moduł musi umożliwiać monitorowanie zmian atrybutów, uprawnień, właściciela oraz monitoring zawartości pliku. |  |
| Moduł inwentaryzacji zasobów musi zbierać i udostępniać informacje o obiekcie w zakresie co najmniej:* Rodzaj i wersja systemu operacyjnego,
* Lista i rodzaj interfejsów sieciowych,
* Lista aktywnych procesów systemu operacyjnego,
* Lista zainstalowanych aplikacji,
* Lista otwartych portów sieciowych.
 |  |
| Moduł oceny konfiguracji bezpieczeństwa musi umożliwiać, za pomocą predefiniowanych reguł, skanowanie obiektu w celu wykrycia zagrożeń lub błędnych konfiguracji w zakresie co najmniej:* Siła haseł,
* Usunięcie niepotrzebnego lub niebezpiecznego oprogramowania,
* Wyłączenie zbędnych usług

Moduł musi posiadać predefiniowane reguły SCA dla każdego z wymaganych systemów operacyjnych oraz udostępniać możliwość tworzenia własnych polityk SCA. |  |
| Moduł wykrywania podatności musi umożliwiać wykrywania luk w aplikacjach zainstalowanych na obiekcie za pomocą dostawców tj. National Vulnerability Database, Red Hat, Canonical, ALAS, MSU. |  |
| Moduł zgodności ze standardami bezpieczeństwa musi umożliwiać badania obiektu pod katem zgodności ze standardami tj. PCI DSS, HIPAA, NIST 800-53 oraz GDPR. |  |
| Moduł reaktywnej odpowiedzi musi umożliwiać automatyczne (bez udziału operatora SIEM) uruchomienie akcji tj.:* Zablokowanie połączenia sieciowego,
* Zatrzymanie aktywnego procesu,
* Usunięcie pliku,
* Przeskanowanie pliku pod kątem obecności wirusów.
 |  |
| Moduł wykrywania malware musi posiadać możliwość wykrywania anomalii i na tej podstawie obecności złośliwego oprogramowania. Moduł musi umożliwiać wykrywania ukrytych procesów, ukrytych plików oraz podejrzanych otwartych portów TCP/UDP. |  |

Platforma szkoleniowa

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Spełnienie wymagań****Spełnia/nie spełnia****(wypełnia Wykonawca)** |
| **Ogólne** | System musi umożliwiać kompleksowe przeprowadzanie szkoleń przez Internet. |  |
| System musi zapewniać instruktaże krok po kroku. |  |
| System musi umożliwiać dodanie filmów szkoleniowych. |  |
| System udostępniania poradniki i materiały dla uczestnika. |  |
| System umożliwia dodanie dwóch rodzajów uczestników szkoleń – urzędnik i mieszkaniec. |  |
| System musi umożliwiać przeszukiwanie bazy szkoleń. |  |
| System musi zapewniać możliwość wystawiania certyfikatów z odbytych szkoleń. |  |
| System generuje raporty pozwalające na kontrolę stopnia wykorzystania narzędzia. |  |
| System zbudowana jest w sposób modułowy i opiera się o architekturę klient-serwer:a) serwer (WWW/Aplikacji LMS/Bazy Danych),b) klient (dowolny system operacyjny, dowolna przeglądarka internetowa); |  |
| System musi zapewniać prowadzenie szkoleń za pośrednictwem Internetu z wykorzystaniem:a) komputerów,b) smartfonów,c) tabletów; |  |
| System umożliwia dostęp on-line do szkoleń z dowolnego systemu operacyjnego i dowolnej przeglądarki internetowej. |  |
| System musi umożliwiać prowadzenie szkoleń z wykorzystaniem kursów multimedialnych, książek elektronicznych, elementów audio/wideo, telewizji internetowej. |  |
| System jest wyposażony w platformę do zarządzania szkoleniami (LMS). |  |
| System posiada narzędzie dla autorów szkoleń do tworzenia kursów e-learning (LCMS). |  |
| System pozwala na modyfikację istniejących szkoleń (edycja m.in. w zakresie opisu kursów i zawartości). |  |
| System posiada mechanizm autoryzacji dostępu z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością. |  |
| System posiada mechanizm określenia dostępności szkoleń (w tym: czas dostępności, sposób zapisu, klucz dostępu, widoczność elementów, itp.). |  |
| System pozwala na dezaktywację szkoleń. |  |
| System udostępnia uprawnionym użytkownikom narzędzia do sprawdzania wiedzy i umiejętności opanowanych przez kursantów/uczniów z możliwością tworzenia bazy pytań kontrolnych różnego rodzaju spośród których tworzony jest test, w tym: jednokrotnego/wielokrotnego wyboru, prawda/fałsz, wartość liczbowa, odpowiedź tekstowa, itp. |  |
| System udostępnia narzędzia monitorowania i oceniania aktywności uczestników kursów z możliwością przypisywania oceny do zadań wykonanych przez kursantów. |  |
| System posiada mechanizm dziennika zawierającego wyniki przeprowadzanych testów/sprawdzianów. |  |
| **Zarządzanie szkoleniami** | System posiada interfejs oraz mechanizm pomocy kontekstowej w języku polskim. |  |
| System musi zapewniać nieograniczoną liczbę użytkowników |  |
| System musi zapewniać moduł raportowania. |  |
| System musi zapewniać współpracę z bazami danych. |  |
| System musi zapewniać zarządzanie programami i planowaniem szkoleń. |  |
| System musi zapewniać zarządzanie profilami/kontami użytkowników. |  |
| System musi zapewniać przypisywanie użytkownikom globalnie (w obrębie całego systemu) określonych ról (np. edytor, autor, administrator, itd.) lub lokalnie (w ramach pojedynczego kursu) wskazywanie uczestników kursu. |  |
| System musi zapewniać harmonogram kursu. |  |
| System musi zapewniać mechanizm administracji szkoleniami i kursantami. |  |
| System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami. |  |
| System musi zapewniać interfejs w języku polskim. |  |
| **Tworzenie kursów** | System musi zapewniać mechanizm pomocy kontekstowej w języku polskim. |  |
| System musi zapewniać dokumentację w języku polskim. |  |
| System musi zapewniać tworzenie scenariuszy lekcji. |  |
| System musi zapewniać możliwość umieszczania na stronach różnego rodzaju interakcji. |  |
| System musi zapewniać możliwość tworzenia kursów on-line. |  |
| System musi zapewniać tworzenie testów. |  |
| System musi zapewniać zarządzanie zawartością szkoleń. |  |
| System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami. |  |
| System musi zapewniać możliwość eksportu do LMS. |  |
| System musi zapewniać możliwość edycji wyglądu kursów. |  |
| System musi zapewniać interfejs w języku polskim. |  |
| System musi zapewniać mechanizm pomocy kontekstowej w języku polskim. |  |
| System musi zapewniać dokumentację w języku polskim. |  |
| **Egzaminy** | System musi umożliwić tworzenie egzaminów z kursu |  |
| System musi umożliwić dodanie więcej niż jednego egzaminu do kursu. |  |
| Tworzenie pytań do egzaminów powinno być możliwe do wykonania z dwóch miejsc:- z panelu administracyjnego - z poziomu danego egzaminu. Przy czym wszystkie pytania utworzone z poziomu egzaminu również trafiają na listę wszystkich pytań. |  |
| Tworzenie pytania powinno polegać na określeniu:- treści pytania- dodatkowego opisu- typu pytania- prawidłowej odpowiedzi- treści widomości dla poprawnej odpowiedzi- treści widomości dla niepoprawnej odpowiedzi- ilość punktów za prawidłową odpowiedź- wskazówki do odpowiedzi |  |
| System musi umożliwić korzystanie przynajmniej z poniższych typów pytań:- Jednokrotny wybór - jedna prawidłowa odpowiedź- Wielokrotny wybór - wiele prawidłowych odpowiedzi- Pytanie otwarte - należy wpisać odpowiedź- Sortowanie - ułożenie obiektów w prawidłowej kolejności- Sortowanie w macierzy - dopasowywanie elementów do siebie w tabeli dwuwymiarowej- Wypełnij puste miejsce - wypełnienie pustego miejsca znakiem, liczbą lub tekstem- Ocena - wskazanie wartości- Esej / Otwarta odpowiedź - dłuższa wypowiedź pisemna |  |
| W przypadku pytania:- Wielokrotny wybór- Pytanie otwarte- Sortowanie- Sortowanie w macierzy- Wypełnij puste miejscew systemie musi istnieć możliwość określenia przyznanych punktów za każdą odpowiedź. |  |
| W przypadku pytania typu "Esej/Otwarta odpowiedź" musi istnieć możliwość wpisania odpowiedzi bezpośrednio w systemie oraz załączenia pliku. |  |
| System musi umożliwić przypisanie każdego pytania do jednego testu. |  |
| System musi umożliwić zapis każdego pytania jako szkic lub opublikować. |  |
| System musi umożliwić usunięcie każdego pytania lub przeniesienie do kosza oraz opublikowanie w dowolnym momencie. |  |
| System musi umożliwić eksport egzaminów do pliku xml |  |
| System musi umożliwić tworzenie nowego egzaminu poprzez:- manualne wprowadzenie- sklonowanie egzaminu który już istnieje w systemie- import z pliku xml |  |
| W przypadku tworzenie egzaminu manualnie należy wpisać tytuł strony, dodać treść (opcjonalnie) oraz wskazać pytania do egzaminu. |  |
| Wskazanie pytań do egzaminu musi odbywać się poprzez wskazanie pytań z repozytorium lub poprzez utworzenie ich z poziomu budowania testu. |  |
| System musi umożliwić przypisanie egzaminu do kursu |  |
| System musi umożliwić przypisanie egzaminu do konkretnej lekcji kursu |  |
| System musi umożliwić określenie od kiedy egzamin jest dostępny dla użytkowników:- natychmiast - test jest dostępny od momentu zapisania się na kurs- na podstawie daty zapisu - test dostępny X dni po zapisaniu się na kurs- konkretna data - test dostępny w konkretnym dniu, od określonej godziny |  |
|  | System musi umożliwić określenie czy wzięcie udziału w egzaminie wymaga ukończenia wcześniej innego egzaminu. Jeśli tak, należy wskazać jakie konkretnie egzaminy musi zdać użytkownik aby móc przystąpić do tego. |  |
|  | System musi umożliwić określenie procentowej ilosć punktów niezbędną do zdania egzaminu. |  |
|  | System musi umożliwić wskazanie szablonu dla wydawanego certyfikatu po zdanym egzaminie. |  |
|  | W systemie musi istnieć możliwość uruchomienia zapisywania egzaminu na serwerze |  |
|  | W systemie musi istnieć możliwość ograniczenia ilości podejść do egzaminu |  |
|  | Musi istnieć możliwość wymuszenia uzupełnienia wszystkich pytań w celu zakończenia egzaminu |  |
|  | Musi istnieć możliwość określenia limitu czasu na przesłanie egzaminu |  |
|  | Musi istnieć możliwość dodania materiałów dotyczących egzaminu (np. Materiałów edukacyjnych). |  |
|  | Musi istnieć możliwość uruchomienia egzaminu automatycznie lub po wybraniu startu przez egzaminowanego. |  |
|  | Musi istnieć możliwość przeglądu tabeli wszystkich pytań z możliwością podglądu podsumowania oraz pominięciem pytania |  |
|  | Musi istnieć możliwość ustawienia losowej kolejności pytań dla każdego uzytkownika |  |
|  | Musi istnieć możliwość określenia kilku wiadomości na zakończenie egzaminu (w zależności od osiągniętej ilości punktów). |  |
|  | Musi istnieć możliwość wyświetlenia użytkownikowi ilości zdobytych punktów oraz czasu poświęconego na egzamin. |  |
|  | System musi wysyłać powiadomienia do użytkownika o odbytym egzaminie |  |
|  | System musi wysyłać powiadomienia administratorowi o użytkownikach którzy odbyli egzamin |  |
|  | Musi istnieć możliwość ograniczenia czasu trwania egzaminu. W przypadku przekroczenia czasu przez użytkownika egzaminu zostaje zakończony administracyjnie. |  |
|  | System musi umożliwiać tworzenie certyfikatów ukończenia egzaminu |  |
|  | Tworzenie certyfikatu musi się odbywać za pomocą edytora blokowego. |  |
|  | System musi umożliwić użycie jednego certyfikatu do wielu egzaminów oraz tworeznie certyfikatów dla każdego egzaminu osobno. |  |
|  | System musi umożliwić przeglądanie statystyk egzaminu. |  |
|  | Statystyka z egzaminu musi zawierać przynajmniej informacje:- użytkownik egzaminowany- liczba punktów- ilość poprawnych odpowiedzi- ilosć niepoprawnych odpowiedzi- ilość użytych wskazówek- czas poświęcony na egzamin- wynik egzaminu |  |
|  | System musi umożliwić eksport pełnych statystyk z systemu do pliku CSV |  |

System centralnego zarządzania tożsamością

|  |  |  |
| --- | --- | --- |
| **Cecha** | **Wymagania minimalne** | **Spełnienie wymagań****Spełnia/nie spełnia****(wypełnia Wykonawca)** |
| **Funkcjonalne** | System musi dostarczać mechanizmy Single-Sign On (SSO) oraz Single-Sign Out (SLO) dla aplikacji klienckich działających w oparciu o protokół http |  |
| System musi posiadać centralną konsolę zarządzającą (administracyjną), posiadająca funkcje:* 1. Zarządzanie użytkownikami,
	2. Zarządzanie grupami użytkowników,
	3. Zarządzanie atrybutami użytkowników wraz z możliwością mapowania atrybutów z AD/LDAP,
	4. Zarządzanie konfiguracją systemu,
	5. Zarządzanie systemami podłączonymi,
	6. Zarządzanie źródłami autoryzacji,
	7. Zarządzanie strefami (realm),
	8. Zarządzanie sesjami użytkowników,
	9. Zarządzanie panelami logowania użytkowników
		1. Możliwość włączenia rejestracji nowych użytkowników,
		2. Możliwość włączenia resetu hasła,
		3. Możliwość włączenia opcji zapamiętania użytkownika w panelu,
	10. Zarządzanie pełną konfiguracją systemu tj. klucze, skórki, cache, polityki bezpieczeństwa
	11. Zarządzanie przepływami,
	12. Możliwość wylogowania użytkownika z wybranych lub wszystkich systemów (sesji).
 |  |
| System musi umożliwiać wykonanie przez administratora akcji w dowolnym systemie w imieniu użytkownika (impersonate) |  |
| System musi umożliwiać zarządzanie logowaniem operacji (konfiguracja, przegląd, eksport) |  |
| System musi posiadać możliwość eksportu i importu konfiguracji, użytkowników, grup, klientów |  |
| System musi posiadać możliwość tworzenia federacji z usługami katalogowymi LDAP, AD |  |
| System musi umożliwiać współpracę z serwerem Kerberos – tworzenie relacji zaufania |  |
| **Techniczne** | System musi posiadać wsparcie dla protokołów OpenID Connect, OAuth 2.0, SAML |  |
|  | System musi posiadać wsparcie dla certyfikatów X.509 |  |
|  | System musi posiadać wsparcie dla W3C Web Authentication |  |
|  | System musi posiadać wsparcie dla mechanizmów MFA w zakresie co najmniej OTP |  |
|  | Konsola administracyjna i portal klienta muszą wspierać wielojęzyczność |  |
|  | System musi umożliwiać tworzenie polityk haseł zbudowanych o wymagalność małe/duże litery, cyfry, znaki specjalne, wyrażenia regularne wraz z możliwością podpięcia z zewnętrznego pliku listy haseł zabronionych |  |
|  | System musi posiadać rozbudowane API pozwalające na integrację z innymi systemami. API musi udostępniać co najmniej metody:1. Wyszukiwania, tworzenia, edycji i usuwania użytkowników,
2. Wyszukiwania, tworzenia, edycji i usuwania grup,
3. Wyszukiwania, tworzenia, edycji i usuwania ról systemów podłączonych,
4. Wyszukiwania, tworzenia, edycji i usuwania ról dostawców tożsamości,
5. Zarządzanie mapowaniem użytkowników do ról.
 |  |