***Załącznik nr 3 do SWZ***

**Formularz parametrów wymaganych**

**Zadanie nr 1**

# System służący do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych

|  |
| --- |
| System służący do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych**Producent:****Model/Typ:** |
| LP. | **PARAMETRY WYMAGANE** | **PARAMETRY OFEROWANE** |
| 1. | Przedmiotem zamówienia jest dostarczenie **Systemu służącego do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych** wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych (ang. remediation) – System klasy XDR wraz z mechanizmami aktywnej ochrony obejmującymi stacje końcowe, serwery. System chroniący komputery i serwery przed zaawansowanymi zagrożeniami, między innymi przed niesygnaturowym złośliwym oprogramowaniem i atakami typu 0-day, bez względu na to, czy zagrożenie pochodzi z obszaru plików, urządzeń i systemów końcowych, czy też z obszaru aktywności użytkowników. System zapobiegający atakom, uwzględniający behawiorystkę, umożliwiający wykrycie szkodliwych aktywności, wykorzystujący zaawansowane metody analityczne.Całość rozwiązania musi być dostarczone wraz z usługą wdrożenia, szkoleniem, 2-letnim wsparciem producenta i 2-letnim lokalnym wsparciem Wykonawcy w utrzymaniu i zarządzaniu systemem.* Ilość komputerów objętych ochroną – do 400
* Ilość serwerów objętych ochroną – do 30
* Ilość kont poczty elektronicznej objętych ochroną - 900
 |   |
| 2. | Wszystkie elementy rozwiązania muszą być dostarczone w formie SaaS, gdzie wszystkie komponenty centralne, takie jak centralny serwer zarządzający i bazy danych i dostarczone przez producenta oferowanego rozwiązania jako usługa. Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy). Producent oferowanego rozwiązania jest odpowiedzialny za niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczanych jako usługa typu SaaS. |  |
| 3. | Oferowany system klasy XDR musi posiadać możliwość zbierania danych z różnych warstw środowiska IT, w tym co najmniej:* Stacje robocze i serwer
* Procesy, w tym modyfikacja
* Pliki
* Połączenia sieciowe
* Zapytania DNS
* Rejestry
* Konta i użytkownicy
* Zdarzenia Internetowe (obsługa URL)
* Windows hooks
* Detekcje i zdarzenia bezpieczeństwa

Dane zbierane z poszczególnych warstw muszą być normalizowane i korelowane między sobą w oparciu o machine learning oraz metody dostarczane i aktualizowane przez producenta  |  |
| 4. | W wyniku korelacji system musi tworzyć incydenty o wysokim poziomie pewności (niski poziom false-positive)  |  |
| 5. | Dane muszą być mapowane na matrycę TTP (techniques, takctiques, procedures), z uwzględnieniem matrycy MITRE ATT&CK |  |
| **Zarządzanie** |
| 6. | System musi posiadać mechanizm pozwalający na proste i intuicyjne uruchamianie sensorów lub agentów na poszczególnych elementach środowiska |  |
| 7. | System musi pokazywać status sensora lub agenta na poszczególnych zasobach, w tym pokazywać z jakiej przyczyny sensor nie może zostać uruchomiony |  |
| 8. | Mechanizm tworzenia kont użytkowników w systemie musi pozwalać na zdefiniowanie dostępu do poszczególnych funkcji systemu (np. dostęp tylko do dashboard lub dostęp do listy alertów) |  |
| **Raportowanie** |
| 9. | System musi pozwalać na przedstawianie danych bezpieczeństwa w różnych perspektywach: * + Alerty,
	+ Użytkownicy,
	+ Detekcje,
	+ Zdarzenia w matrycy MITRE ATT&CK
 |  |
| 10. | System musi pozwalać na wysyłanie notyfikacji do wybranego administratora odnośnie: * + Alertów,
	+ Zidentyfikowania wskaźników potencjalnego wystąpienia ataku,
 |  |
| 11. | System musi pozwalać na wyeksportowanie wybranych zdarzeń w formacie CSV lub JSON  |  |
| 12.  | Wszelka aktywności w systemie musi być zapisywana i ewidencjonowana z zapewnieniem odpowiedniej rozliczalności działań analityków w środowisku |  |
| 13. | Threat Intelligence – system musi dostarczać i integrować dane zebrane przez producenta o zagrożeniach i kampaniach przestępczych |  |
| 14. | Dane dostarczane do systemu, muszą być normalizowane w sposób pozwalający na ekstrakt iOC (tam gdzie to możliwe): * Domenę
* SHA-1/SHA-256
* IP
* Adres nadawcy
* URL
 |  |
|  | Środowisko musi być automatycznie przeszukiwane pod kątem wystąpienia artefaktów związanych z danym zagrożeniem/atakiem, a w konsoli musi zostać wyświetlona informacja wskazująca na identyfikację artefaktu. System musi pokazywać:* Poszczególne artefakty, które zostały zidentyfikowane
* Powiązane zasoby (stacja/serwer/użytkownik/konta pocztowe)
* Powiązane linki
 |  |
|  | W przypadku wykrycia zagrożenia system musi co najmniej:* Zalogować wystąpienie niebezpiecznego zdarzenia w centralnej konsoli monitorującej,
* Zablokować zdarzenie
 |  |
| Threat hunting |
|  | System musi pozwalać na przeszukiwanie wszystkich danych zebranych z organizacji pod kątem różnych artefaktów :* Wyszukiwanie ma być realizowane z jednego miejsca dla wszystkich źródeł
* System musi pozwalać na wyszukiwanie po pełnej frazie (np. cała komenda) lub tylko fragmencie
* System musi pozwalać na wyszukiwanie artefaktu nawet jeśli nie jest znany atrybut powiązany z tym artefaktem np. wyszukanie ciągu, który mógłby zaistnieć jako wywołanie URL, fragment komendy, nazwa pliku itd.
* W wyniku wyszukiwania system musi wskazywać linię czasu oraz powiązane ze zdarzeniem obiekty
* Po zidentyfikowaniu obiektu system musi pozwalać na odtworzenie przebiegu zdarzenia w łańcuchu przyczynowo-skutkowym. System ma pokazywać powiązania pomiędzy poszczególnymi zdarzeniami w łańcuchu
* System musi wyświetlać jak najpełniejsze dane odnośnie zdarzenia, w szczególności powinien określać atrybuty z poniższej listy (tam gdzie ma to zastosowanie):
	+ Typ obiektu
	+ Data utworzenia/zmiany
	+ Nazwa procesu
	+ Lokalizacja pliku
	+ Komenda CLI
	+ SHA-1
	+ SHA-256
	+ File MD5
	+ Process ID
	+ Podpis/certyfikat
	+ Ważność podpisu/certyfikatu
	+ Typ pliku
	+ Czy powstał w wyniku zdalnego dostępu
	+ Poziom integralności
	+ Domena
	+ URL
	+ Nazwa punktu końcowego (Endpoint)
	+ Adres IP punktu końcowego (Endpoint)
	+ Adres MAC punktu końcowego (Endpoint)
	+ Rodzaj i wersja systemu operacyjnego
	+ Zalogowany użytkownik
	+ Komunikacja sieciowa
	+ Poziom ryzyka
	+ Schemat ataku
	+ Protokół (np. HTTP)
	+ Metoda (np. GET)
	+ Wskazanie źródła i celu połączenia (client->server)
	+ Response code (np. 200 OK)
	+ MIME type (np. application/octet-stream)
	+ SHA-1/SHA-256
	+ Data i godzina wystąpienia
	+ Przebieg komunikacji w linii czasu
	+ Wskazanie miejsca, w którym zaobserwowano przesyłanie szkodliwego obiektu
	+ Hosty, na których zaobserwowano pliki ze szkodliwą zawartością, w tym zapisie sieciowym
	+ URL/domena
	+ Użytkownik
	+ Port
* Zdarzenia muszą być mapowane, tam gdzie to możliwe, na techniki i taktyki MITRE ATT&CK (wskazanie konkretnego identyfikatora taktyki/techniki)
 |  |
| **Incident response** |
|  | System w wyniku działań korelacyjnych musi tworzyć zagregowane alerty  |  |
|  | Każdy alert musi wskazywać ocenę pod kątem istotności oraz być klasyfikowany wg typu zagrożenia |  |
|  | System musi wskazywać jaki zasięg ma dany alert – ile i jakie serwery/stacje/użytkownicy są powiązani z alertem |  |
|  | System ma pozwalać na zarządzanie statusem alertu:* Nowy (New - status domyślny)
* W trakcie realizacji (in progress)
* Zamknięty (closed)
* False Positive (closed – False Positive)
 |  |
|  | System musi pozwalać na podejmowanie akcji w poszczególnych zdarzeniach:* Izolacja stacji/serwera
* Uruchomienie skryptu
* Nawiązanie zdalnego połączenia ze stacją/serwerem poprzez zdalną powłokę bezpośrednio z konsoli systemu:
	+ Przeglądanie zawartości stacji/serwera (listowanie plików/katalogów)
	+ Wyświetlanie zmiennych środowiskowych
	+ Wyświetlanie konfiguracji sieci
	+ Wyświetlanie aktualnych połączeń sieciowych
	+ Wyświetlanie listy procesów
	+ Przeglądanie kluczy rejestrów i ich wartości
	+ Wyświetlanie listy usług, wraz ze statusem
	+ Wyświetlanie listy użytkowników
	+ Zakończenie procesu
	+ Usunięcie pliku/folderu
	+ Pobranie pliku
 |  |
|  | System musi pozwalać na tworzenie listy obiektów do zablokowania/listy wyjątków |  |
|  | Obiekty muszą być dystrybuowane do poszczególnych systemów podpiętych do systemu centralnego, w szczególności: * System do ochrony stacji końcowych
* System do ochrony serwerów
 |  |
| 1. .
 | Katalog obiektów do zablokowania/wyjątków: * Domena
* Plik (SHA-1/SHA-256)
* Adres IP
* Adres nadawcy
* URL
 |  |
|  | Dla danego obiektu dodawanego do listy obiektów do zablokowania musi być możliwość zdefiniowania dodatkowo:* Poziomu ryzyka
* Akcji (logowanie/blokada lub kwarantanna)
* Ważności blokady
 |  |
| **Specyfikacja technologicznia** |
|  | Sensor XDR dedykowany na serwery/stacje robocze musi integrować się z poniższymi platformami OS: * Windows 10
* Windows 7
* Windows Server 2019 (64-bit)
* Windows Server 2016 (64-bit)
* Windows Server 2012 / 2012 R2 (64-bit)
* Windows Server 2008 R2 (64-bit)
* Red Hat Enterprise Linux 6 (64-bit)
* Red Hat Enterprise Linux 7 (64-bit) Red Hat Enterprise Linux 8 (64-bit)
* CentOS Linux 6 (64-bit)
* CentOS Linux 7 (64-bit)
* CentOS Linux 8 (64-bit)
* Ubuntu 16 (64-bit)
* Ubuntu 18 (64-bit)
* Ubuntu 20 (64-bit)
* macOS Mojave (10.14) i nowsze
 |  |
|  | System musi pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji roboczej/serwera system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą |  |
|  | System musi być oparty o wydajny silnik analityczny pozwalający na pracę z danymi bez zbędnej zwłoki |  |
|  | Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy) |  |
|  | Producent musi dostarczyć zakres danych przetwarzanych w usłudze |  |
|  | System musi posiadać certyfikat potwierdzający zgodność przetwarzania danych z obowiązującymi standardami i dobrymi praktykami np. ISO27001. |  |
| **Wymagania funkcjonalne dla mechanizmów aktywnej ochrony stanowiących element systemu XDR** |
|  | Mechanizmy aktywnej ochrony powinny być realizowane przez tego samego agenta, który realizuje zbieranie danych telemetrycznych na potrzeby analizy XDR lub dodatkowego, niezależnego agenta pochodzącego od tego samego producenta. Wszystkie mechanizmy aktywnej ochrony, informacje o zdarzeniach bezpieczeństwa, wykrytych oraz zablokowanych atakach powinny być przesłane do centralnego systemu XDR, gdzie zostaną poddane korelacji z pozostałymi danymi zebranymi przez sensory XDR (np. danymi telemetrycznymi). |  |
| **Wymagania funkcjonalne dla systemu aktywnej ochrony stacji końcowych** |
|  | Ochrona antymalware* Wszystkie funkcjonalności oprogramowania aktywnej ochrony dla stacji końcowych muszą być zarządzane z tej samej centralnej konsoli, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej.
* Rozwiązanie w obrębie funkcjonalności aktywnej ochrony stacji końcowych musi działać jako jeden agent, odpowiadający zarówno za egzekwowanie polityk bezpieczeństwa jak i komunikację z serwerem zarządzającym.
* Rozwiązanie musi wykorzystywać technologię „Machine Learning” do wykrywania nowych, nieznanych wirusów.
* Rozwiązanie musi zapewniać wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware“, „adware“, „keylogger”, „dialer”, „trojan”.
* Rozwiązanie musi zapewniać ochronę przed atakami typu ransomware.
* Rozwiązanie musi zapewniać automatyczne usuwanie wirusów oraz alarmować w przypadku wykrycia zagrożenia.
* Rozwiązanie musi umożliwiać zablokowanie zmian ustawień konfiguracyjnych klientów rozwiązania na stacjach roboczych w celu uniemożliwienia ich modyfikacji.
* Rozwiązanie musi umożliwiać tworzenie ról administratorów o różnych stopniach uprawnień.
* Rozwiązanie musi mieć możliwość integracji z MS Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów.
 |  |
|  | Kontrola Aplikacji* Funkcjonalność typu application control (kontrola aplikacji) dla stacji końcowych użytkowników. Rozwiązanie powinno realizować co najmniej następujące funkcjonalności:
* Funkcjonalność musi umożliwiać zdefiniowanie zestawu aplikacji które użytkownik końcowy będzie mógł uruchomić – pozostałe aplikacje powinny być blokowane.
* Funkcjonalność musi zapewniać ochronę przed uruchamianiem niepożądanych lub nieznanych aplikacji (plików wykonywalnych, bibliotek DLL, aplikacji Windows, sterowników urządzeń, oraz innych przenośnych plików wykonywalnych (Portable Executable files).
* Funkcjonalność musi zapewniać mechanizm analizy zagrożeń w czasie rzeczywistym bazujący na globalnej bazie reputacji plików.
* Funkcjonalność w celu kontroli aplikacji musi wykorzystywać polityki zawierające zdefiniowane reguły z dwoma metodami kontroli aplikacji:
* Zezwól(Allow) – reguły zezwalające na uruchomienie aplikacji, które nie są wskazane jako zablokowane,
* Blokuj (Block) – reguły blokują uruchomienie wszystkich aplikacji, jedynie aplikacje określone w liscie dozwolonych mogą być uruchomione
* Funkcjonalność Maintenance Mode – musi zepewnić, że w przypadku konieczności wykonania kontrolowanego update’u systemu operacyjnego na stacji roboczej/serwerze kontrola aplikacji przejdzie w tryb Maintenance Mode gdzie autoryzowane aktualizacje plików systemu nie będą trakctowane jako złamanie polityki.
 |  |
|  | HOST IPS/Firewall* Funkcjonalność klasy Host IPS (Host Intrusion Prevention System) dla stacji końcowych użytkowników.
* Funkcjonalność klasy Host IPS powinno chronić systemy użytkowników przed znanymi podatnościami za pomocą dostarczanych przez producenta sygnatur.
* Funkcjonalność Firewall powinno wykrywać skanowania portów, chronić przed atakami sieciowymi wykorzystującymi znane podatności aplikacji oraz systemów operacyjnych.
 |  |
|  | Kontrola urządzeń zawnętrznych* Funkcjonalność musi posiadać możliwość zapewnienia ochrony dostępu do pamięci masowych
* Funkcjonalność musi posiadać możliwość monitorowania:
* Urządzeń pamięci masowej – USB
* Urządzeń pamięci masowej – urzadzenia mobilne
* Funkcji AutoRun na urządzeniach USB
* Funkcjonalność musi umożliwiać utworzenie listy zatwierdzonych urządzeń pamięci masowej USB.
* Funkcjonalność musi zapewniać ochronę co najmniej systemów Windows 7/8.1/10, 11, macOS (10.14) i nowsze.
 |  |
|  | Specyfikacja technologiczna * Sensor aktywnej ochrony stacji końcowych dedykowany na serwery/stacje robocze musi integrować się z poniższymi platformami OS:
	+ Windows 2000
	+ Windows XP
	+ Windows Server 2003
	+ Windows 7,8,8.1,10,11
	+ Windows Server 2008,2012,2016,2019,2022
	+ Windows Server Core
	+ Red Hat Enterprise Linux 5,6,7,8,9
	+ Red Hat OpenShift
	+ Ubuntu 10.04,12.04,14.04,16.04,18.04,20.04,22.04
	+ Ubuntu 12.04
	+ CentOS 5,6,7,
	+ Rocky Linux 8
	+ Debian 6,7,8,9,10,11A
	+ Oracle Linux 5,6,7,8
	+ SUSE Linux Enterprise Server 10,11,12,15
	+ macOS Catalina (10.15 or later)
	+ macOS BigSur (11.0 or later)
	+ macOS Monterey (12.0 or later)
* System musi pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji roboczej/serwera system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą
 |  |
| **Wymagania dotyczące wdrożenia, szkoleń i usług serwisowych** |
|  | W ramach usług wdrożeniowych, szkoleniowych i serwisowych Wykonawca zapewni:* Analizę przedwdrożeniową, której wynikiem prac będzie opracowanie projektu technicznego wdrożenia, na jego podstawie będą prowadzone prace wdrożeniowe,
 |  |
|  | * Instalację i konfigurację systemu XDR zgodnie z projektem technicznym wdrożenia na min. 300 komputerach i do 30 serwerów
 |  |
|  | Przeprowadzenie testów wdrożonego systemu zgodnie z projektem technicznym wdrożenia |  |
|  | Sporządzenie dokumentacji powdrożeniowej |  |
|  | Przeprowadzenie szkoleń dla maksymalnie 4 administratorów ze strony Zamawiającego w zakresie administrowania wdrożonym systemem. Szkolenie będzie się odbywać w lokalizacji Zamawiającego lub Wykonawcy, |  |
|  | 24 miesięcy wsparcia Producenta rozwiązań w trybie 24/7 obsługiwane bezpośrednio przez producenta lub jego autoryzowanego partnera serwisowego na terenie Polski, liczone od dnia podpisania końcowego protokołu odbioru, |  |
|  | 24 miesiące wsparcia Wykonawcy w wymiarze 2 godzin serwisowych miesięcznie w zakresie: przegląd kwartalny wdrożonego środowiska, przekazywanie wiedzy przy rozwiązywaniu problemów, konsultacje, aktualizacje środowiska do nowych wersji, liczone od dnia podpisania końcowego protokołu odbioru. |  |

# **Formularz parametrów wymaganych**

**Zadanie nr 2**

# Rozbudowa istniejącego systemu ochrony UTM o narzędzie do zarządzania logami Stormshield Log Supervisor – SN910 na 3 lata

|  |
| --- |
| **Rozbudowa istniejącego systemu ochrony UTM o narzędzie do zarządzania logami Stormshield Log Supervisor – SN910 na 3 lata** **Producent:****Model/Typ:****Rok produkcji:** |
| **PARAMETRY WYMAGANE** | **PARAMETRY OFEROWANE** |
| Zarządzanie logami: * Gromadzenie zdarzeń przez syslog (TCP oraz UDP)
* Bezpieczne gromadzenie danych przez syslog-TLS
* Syslog Forwarder
* Liczba zdarzeń na sekundę (EPS): > 10 000
* Normalizacja i natywne indeksowanie logów SNS
* Zarządzanie logami przez wiele lat (> 1 roku)
* Liczba urządzeń > 500

• Bezpieczne gromadzenie danych przez syslog-TLS• Syslog Forwarder• Liczba zdarzeń na sekundę (EPS): > 10 000• Normalizacja i natywne indeksowanie logów SNS• Zarządzanie logami przez wiele lat (> 1 roku)• Liczba urządzeń > 500 |  |
| RODZAJE WYSZUKIWAŃ* Wyszukiwanie proste
* Wyszukiwanie zaawansowane w oparciu o wiele
* kryteriów (rodzaj logu, czas, itd.)
* Wyszukiwanie predefiniowane
* Rezultaty wyświetlane jako logi proste, znormalizowane
* i graficzne
* Możliwość wykorzystania zewnętrznych źródeł (CSV,
* IPtoHost, LDAP, GeoIP)
* Nawigacja na podstawie czasu (minut, godzin, dni,
* okresów)
* Historia wyszukiwania
* • Eksport wyników w formacie CSV
 |  |
| PANELE KONTROLNE* Widoki ogólne (zagrożenia, dane, aplikacje internetowe,
* sprzęt i system)
* Możliwość dostosowania istniejących widgetów
* Możliwość tworzenia nowych widgetów
* Ponad 20 rodzajów widoków graficznych (histogramy,
* radary, mapy, itd.)
 |  |
| ZARZĄDZANIE INCYDENTAMI I ALERTAMI* Automatyczne generowanie na podstawie
* ustalonych reguł
* Zarządzanie krytycznością alertów na 4
* poziomach krytyczności
* Możliwość przypisania incydentów do
* administratorów i śledzenie rozwiązania
 |  |
| RAPORTY* Ręczne lub automatyczne (godzinne, dzienne,
* tygodniowe lub miesięczne)
* Możliwość dostosowania układu
* Formaty raportów: PDF, HTML, XLS, DOCX, CSV
* Możliwość wysyłania raportów mailem
 |  |
| KOMPATYBILNOŚĆ* Hiperwizory:
* VMWare ESXi 6.5 oraz 7
* Microsoft HyperV: Windows Server 2016
 |  |

**Formularz parametrów wymaganych**

**Zadanie nr 3**

# Oprogramowanie do tworzenia kopii zapasowych

|  |
| --- |
| **Oprogramowanie do tworzenia kopii zapasowych – 1 szt.****Producent:……………………****Model/Typ:…………………** |
| **LP** | **PARAMETRY WYMAGANE** | **PARAMETRY OFEROWANE** |
|  | 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 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. |  |
|  | Licencja subskrpycyjna na okres 3 lat na 30 maszyn wirtualnych  |  |
|  | Wymagane jest podłączenie magazynów danych z urządzenia logicznego do dostarczonego oprogramowania do backupu,* instalacja modułów oprogramowania do backupu,
* zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do backupu,
* przeprowadzenie testów akceptacyjnych poprawności działania operacji, backupu i odzyskiwania danych. Wykonawca wykorzystując narzędzie RMAN w sposób natywny przygotuje kopię bazy danych ORACLE.
 |  |
|  | Przygotowanie dokumentacji powykonawczej, zawierającej minimum:1. schematy połączeń pomiędzy systemem backupowym, a innymi urządzeniami podłączonymi do dostarczanego systemu,
2. adresację systemów,
3. konfigurację modułów oprogramowania.
 |  |
| **Całkowite koszty posiadania** |
|  | 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 musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. |  |
|  | Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Google Cloud Storage, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |  |
|  | 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 oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) |  |
|  | Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |  |
|  | Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |  |
|  | 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 posiadać mechanizmy chroniące przed utratą hasła szyfrowania |  |
|  | 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. |  |
| **Wymagania RPO** |
|  | 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 oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych |  |
|  | Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru |  |
|  | 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 zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, INFINIDAT, Pure Storage. |  |
|  | Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |  |
|  | Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn |  |
|  | Oprogramowanie musi posiadać wsparcie dla NDMP |  |
|  | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |  |
|  | Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |  |
|  | Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |  |
|  | 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 kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |  |
|  | 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 mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |  |
|  | 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) |  |
| **Wymagania RTO** |
|  | 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
* BSD: UFS, UFS2
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
 |  |
|  | Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. |  |
|  | Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), |  |
|  | Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych |  |
|  | Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych |  |
|  | Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. |  |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |  |
|  | Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego |  |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN . Wykonawca  |  |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA |  |
|  | Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| **Ograniczenie ryzyka** |
|  | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. |  |
|  |  Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |  |
|  | Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |  |
|  | Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere |  |
|  | 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. |  |
|  | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |  |