

## Załącznik nr 1 do SWZ - Opis przedmiotu zamówienia

**CZĘŚĆ 1 (ZADANIE 1) – Dostawa macierzy, serwera i sprzętu sieciowego:****1) Serwer – 1 szt.**

- a) Serwer klasy rack 1U/2U z kontrolerem RAID, dyskami SSD, zdalnym zarządzaniem, redundantnym zasilaniem oraz licencją systemu operacyjnego Windows Server Standard 2025 na wymaganą liczbę rdzeni CPU.
- b) Zakres przedmiotu zamówienia. Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera klasy korporacyjnej (rack), akcesoriów montażowych, oprogramowania systemowego, usług uruchomienia oraz wsparcia serwisowego, obejmująca:
  - Dostawa 1 szt. serwera rack (z szynami) do szafy 19”.
  - Montaż w szafie Rack (jeżeli zamawiający wskaże lokalizację) lub dostawa wraz z zestawem szyn do samodzielnego montażu.
  - Konfiguracja wstępna BIOS/UEFI, kontrolera RAID, wgranie aktualnego firmware (płyta główna, kontroler, dyski, NIC, BMC) oraz weryfikacja poprawności działania.
  - Dostawa i przypisanie licencji Windows Server Standard 2025 (lub równoważny) na liczbę 32 rdzeni (zgodnie z licencjonowaniem per core) – klucze/licencje i nośniki elektroniczne.
  - Gwarancja i wsparcie onsite NBD (Next Business Day) przez minimum 36 miesięcy, z opcją Keep Your Drive (pozostawienie dysków u Zamawiającego w razie awarii) lub równoważną usługą.
  - Przekazanie dokumentacji powykonawczej (konfiguracja, wersje firmware, numery seryjne).
- c) Parametry graniczne i wymagania równoważności
  - Format: serwer rack 1U lub 2U, kompatybilny z szafą 19”.
  - Kieszenie dyskowe: min. 8 zatok 2,5" HotSwap/HotPlug (SAS/SATA/NVMe – dopuszcza się mieszane, przy czym wymagane jest wsparcie SATA).
  - TPM: moduł TPM 2.0 (sprzętowy).
  - Szyny: komplet szyn wysuwanych do montażu w szafie 19”.
  - Zarządzanie: kontroler BMC/IMM klasy Enterprise z dedykowanym portem RJ 45, funkcjami zdalnej konsoli (KVM over IP), zdalnych nośników wirtualnych, monitoringu sprzętowego, powiadomień i zarządzania firmware (równoważny do iDRAC Enterprise).
  - Procesor: serwerowy CPU x86\_64, min. 32 rdzenie / 64 wątki w 1 CPU,  $\geq 3,5$  GHz (bazowe lub all core turbo – warunek spełnienia wydajności należy potwierdzić kartą katalogową, przykład referencyjny: AMD EPYC 9355P (3.55 GHz, 32C/64T) lub równoważny (np. inny model EPYC lub Intel Xeon o porównywalnej liczbie rdzeni i wydajności, potwierdzonej wynikami producenta/specyfikacją).
  - Pamięć operacyjna (RAM): pojemność łączna: min. 128 GB, moduły: min. 4 × 32 GB DDR5, prędkość efektywna  $\geq 5600$ –6400 MT/s (akceptowalne 6400 MT/s lub najbliższy wspierany przez platformę), ECC/Registered: wymagane wsparcie ECC RDIMM lub 3DS RDIMM zgodnie z platformą.
  - Podsystem dyskowy i RAID: kontroler RAID: sprzętowy RAID z pamięcią cache nieulotną  $\geq 8$  GB (np. PERC H965i 8 GB NVC lub równoważny), obsługa co najmniej RAID 0/1/10/5, dyski systemowe/dane: min. 2 × 480 GB SSD SATA 6 Gb/s, min. 4 × 1.92TB SSD SATA 6 Gb/s, Hot-Plug, klasa Read Intensive lub wyższa, 1 DWPD (lub parametry równoważne – dopuszczalne SSD SAS/NVMe, o ile zachowana jest

pojemność i trwałość; minimalna łączna pojemność brutto  $\geq 3,6$  TB), ramki: komplet ramek/koszyków umożliwiające montaż dysków.

- Kontroler HBA w wariantcie "External Passthrough"- SAS 24 Gb/s – interfejs obsługujący połączenia z dyskami i półkami dyskowymi SAS 24G – min 2 zew porty SAS
- Sieć: karta sieciowa: min.  $4 \times 10/25$  GbE (SFP28), z możliwością pracy 10 lub 25 GbE; kompatybilność z transceiverami SFP28 25G (transceivery nie są przedmiotem, chyba że wykonawca wskaże inaczej).
- Zasilanie: zasilacze: redundantne (1+1), o mocy  $\geq 1500$  W (lub odpowiednio dobranej do konfiguracji), sprawność klasy 80 Plus Platinum lub wyższej (jeśli dostępna w danym modelu).
- Oprogramowanie i licencje: system operacyjny: Windows Server Standard 2025, licencjonowanie per core na 32 rdzenie (dla jednego CPU 32 rdzeniowego). Dopuszcza się wersję równoważną systemu serwerowego zapewniającą kompatybilność z planowanym środowiskiem Zamawiającego – w takim przypadku Wykonawca musi dostarczyć opis ekwiwalentności funkcjonalnej (AD DS, DNS, DHCP, SMB, Hyper V lub równoważna wirtualizacja). Dowody legalności: klucze/licencje i dokumenty potwierdzające legalność, bezterminowe uprawnienie do użytkowania.
- Gwarancja i serwis: okres: min. 36 miesięcy od dnia podpisania protokołu odbioru. Poziom: NBD Onsite (naprawa u Zamawiającego w następnym dniu roboczym od zgłoszenia). KYO: Keep Your Drive / Data Retention – w razie awarii dysków nośniki pozostają u Zamawiającego. Kanał zgłoszeń: 24/7 (telefon/portał), numer seryjny urządzenia widoczny w BMC. Aktualizacje: dostęp do aktualizacji firmware/mikrokodu w okresie wsparcia.
- Wymagania jakościowe, bezpieczeństwa i zgodności: sprzęt fabrycznie nowy, nieużywany, z oficjalnej dystrybucji producenta, z pełnym wsparciem serwisowym w Polsce. Zgodność: CE, RoHS lub równoważne wymagane przepisami; pełna zgodność z RODO w zakresie przetwarzania danych przy świadczeniu usług serwisowych (m.in. procedura KYO). Bezpieczeństwo: sprzętowy TPM 2.0, możliwość wymuszenia Secure Boot, szyfrowanie dysków na poziomie OS (BitLocker lub równoważny – konfiguracja po stronie Zamawiającego).

## **2) Napęd taśmowy – ilość 2 sztuki, z taśmami – ilość 24 sztuki, taśmami czyszczącymi – ilość 2 sztuki.**

- a) Dostawa napędów taśmowych klasy korporacyjnej zgodnego z technologią LTO8, wraz z kompletem nośników danych i taśm czyszczących. Zamawiający dopuszcza rozwiązania równoważne do wskazanego produktu HPE StoreEver LTO8 Ultrium 30750, pod warunkiem zachowania minimalnych parametrów granicznych określonych w niniejszym OPZ.
- b) Zakres przedmiotu zamówienia:
  - dostawa 2 szt. napędów taśmowego LTO 8 (interfejs SAS), kompatybilnego z oprogramowaniem backupowym klasy enterprise.
  - dostawa 24 szt. fabrycznie nowych taśm danych LTO 8, kompatybilnych z napędem.
  - dostawa 2 szt. fabrycznie nowych taśm czyszczących (Cleaning Cartridge) zgodnych z LTO 8.
  - dostawa kabli połączeniowych SAS.
  - gwarancja producenta minimum 36 miesięcy.
- c) Parametry techniczne urządzenia:
  - Napęd taśmowy (2szt.) musi należeć do technologii LTO-8 Ultrium i umożliwiać zapisywanie danych na taśmach LTO-8 o pojemności natywnej co najmniej 12 TB, z możliwością osiągnięcia pojemności skompresowanej minimum 30 TB zgodnie ze standardem LTO. Urządzenie powinno zapewniać minimalną natywną prędkość zapisu wynoszącą co najmniej 300 MB/s. Napęd musi być wyposażony

w interfejs SAS 6 Gb/s, umożliwiający współpracę z serwerem backupowym Zamawiającego. Napęd powinien pracować w trybie standalone (obudowa desktop).

- Wymagana jest obsługa szyfrowania sprzętowego AES-256, a także wsparcie dla LTFS (Linear Tape File System).
- Napęd powinien być wyposażony w diody/komunikaty statusowe umożliwiające odczyt informacji o stanie pracy, błędach zapisu/odczytu oraz potrzebie czyszczenia.

d) Parametry techniczne taśm danych LTO-8 (24 szt.)

- Zamawiający wymaga dostarczenia 24 sztuk fabrycznie nowych taśm LTO-8, zgodnych z technologią LTO-8 i w pełni kompatybilnych z oferowanym napędem. Każda taśma musi posiadać pojemność natywną minimum 12 TB i pojemność skompresowaną minimum 30 TB (zgodnie z kompresją referencyjną 2,5:1). Taśmy muszą być oryginalne, nieużywane, w oryginalnych opakowaniach producenta (HPE, Fujifilm, IBM, Sony lub innego producenta certyfikowanego zgodnie z normą LTO Ultrium). Oczekuje się, że taśmy będą oznaczone zgodnie ze standardem LTO Ultrium, z fabrycznymi etykietami lub z możliwością późniejszego etykietowania.

e) Parametry techniczne taśm czyszczących (2 szt.):

- Zamawiający wymaga dostarczenia 2 sztuk taśm czyszczących typu LTO Universal Cleaning Cartridge (UCC). Taśmy muszą być całkowicie kompatybilne z napędem LTO-8. Taśma czyszcząca musi umożliwiać liczbę cykli czyszczenia zgodną ze specyfikacją producenta (zazwyczaj w zakresie 20–50 procesów czyszczących). Nośniki muszą być fabrycznie nowe, zapakowane w oryginalnych opakowaniach.
- Gwarancja i serwis: minimalny okres gwarancji: 36 miesięcy. Typ gwarancji: zgodnie z polityką producenta. Wsparcie producenta: możliwość pobierania firmware i narzędzi diagnostycznych. Wymagane: dokument gwarancyjny w języku polskim lub angielskim.
- Wymagania jakościowe i zgodności: sprzęt fabrycznie nowy, nieużywany, z autoryzowanej dystrybucji na rynek UE/PL. Nośniki również fabrycznie nowe w oryginalnych opakowaniach. Zgodność z wymaganiami CE, RoHS lub równoważnymi. Kompatybilność z posiadanym środowiskiem backupowym (Zamawiający oczekuje deklaracji kompatybilności dla popularnych rozwiązań: Veeam, lub równoważnych).
- Sposób realizacji zamówienia: miejsce dostawy: wskazane przez Zamawiającego. Przekazanie: napędu, taśm danych, taśm czyszczących, dokumentacji, potwierdzenia zgodności.

### 3) Przełącznik sieciowy – ilość 1 sztuka oraz wkładki – ilość 4 sztuki

- a) Dostawa przełącznika sieciowego warstwy L2+/L3 Lite o przepustowości 10 Gb/s oraz kompatybilnych wkładek SFP+ 10Gbit mono-mode (SM). Zamawiający dopuszcza rozwiązania równoważne do wskazanego przełącznika TP-Link TL-SX3008F, pod warunkiem spełnienia minimalnych parametrów technicznych określonych poniżej.
- b) Zakres przedmiotu zamówienia
- dostawa 1 sztuki przełącznika sieciowego 10G z portami SFP+, przystosowanego do pracy całodobowej (24/7).
  - dostawa 4 sztuk wkładek SFP+ 10Gb/s typu single mode (SM), kompatybilnych z oferowanym przełącznikiem.
  - dostarczenie instrukcji obsługi i specyfikacji technicznej.
  - Gwarancja producenta na przełącznik i moduły.
  - dostawa do siedziby Zamawiającego oraz montaż w szafie rack.

## c) Parametry techniczne:

- Przełącznik musi być przełącznikiem warstwy L2+ z obsługą funkcji L3 Lite, w pełni zarządzalnym, przeznaczonym do montażu w szafie Rack 19" lub pracy jako urządzenie wolnostojące (zgodnie z konstrukcją producenta). Oczekuje się, że urządzenie będzie wyposażone w co najmniej 8 portów SFP+ 10GbE, umożliwiających transmisję z prędkością 10 Gb/s na każde gniazdo. Przełącznik musi posiadać nieblokującą architekturę przełączającą, umożliwiającą pełną przepustowość na wszystkich portach SFP+ równocześnie. Oczekuje się wsparcia dla podstawowych i zaawansowanych funkcji warstwy drugiej, takich jak: VLAN 802.1Q, agregacja łączy (LACP 802.1AD), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP), kontrola burzy broadcast/multicast, QoS, listy kontroli dostępu (ACL) oraz IGMP Snooping dla ruchu multicast. Urządzenie musi oferować funkcje warstwy trzeciej w zakresie L3 Lite, co najmniej routing statyczny IPv4 i IPv6. Przełącznik powinien obsługiwać sieci IPv6 zgodnie z obowiązującymi standardami (bezpieczeństwo, zarządzanie, protokoły warstwy drugiej). Przełącznik musi umożliwiać zarządzanie poprzez interfejs webowy, CLI dostępne przez SSH/console oraz SNMP. Wymagane jest wsparcie możliwości aktualizacji oprogramowania (firmware) oraz możliwość monitorowania urządzenia przez SNMP v1/v2/v3. Urządzenie powinno posiadać konstrukcję bezwentylatorową (fanless) lub o bardzo niskim poziomie hałasu – zgodnie z modelem producenta – zapewniającą stabilną pracę w środowisku biurowym lub serwerowni. Wymagane jest wsparcie zabezpieczeń sieciowych takich jak 802.1X, ochrona przed atakami DoS na warstwie przełączania oraz zabezpieczenia portów. Przełącznik musi posiadać metalową obudowę i możliwość pracy w trybie 24/7.
  - Zamawiający wymaga dostarczenia 4 sztuk wkładek SFP+ 10Gb/s single-mode (SM) kompatybilnych z oferowanym przełącznikiem. Wkładki muszą umożliwiać transmisję z przepustowością 10 Gb/s, z zasięgiem co najmniej 10 km na jednomodowym włóknie światłowodowym (SMF, 9/125 μm). Oczekuje się stosowania standardu optycznego 10GBASE-LR lub równoważnego, zapewniającego stabilną transmisję na jednym włóknie optycznym, z typową długością fali nadajnika 1310 nm. Moduły muszą być fabrycznie nowe, zgodne ze standardem MSA, a także w pełni kompatybilne z oferowanym przełącznikiem bez konieczności stosowania dodatkowych licencji lub modyfikacji firmware. Moduły muszą posiadać zabezpieczenia ESD, metalową obudowę i spełniać normy dotyczące bezpieczeństwa pracy urządzeń optycznych klasy laserowej (Class 1 Laser Product).
- d) Gwarancja i serwis: minimalna gwarancja na przełącznik: 36 miesięcy. Minimalna gwarancja na wkładki SFP+: 12 miesięcy. Urządzenia fabrycznie nowe, z oficjalnego kanału dystrybucji UE/PL. Możliwość pobierania firmware i dokumentacji technicznej w okresie gwarancji.

**4) Macierze centralne do backupu i logów, wraz z wyposażeniem – ilość 2 sztuki**

- a) Zakup dwóch serwerów pamięci masowej klasy enterprise wraz z akcesoriami montażowymi, dyskami twardymi, pamięcią RAM oraz kartą sieciową 10GbE. Wskazane nazwy handlowe pełnią funkcję referencyjną – Zamawiający dopuszcza rozwiązania równoważne, spełniające minimalne wymagania techniczne określone w niniejszym dokumencie.
- b) Zakres przedmiotu zamówienia - obejmuje dostawę następujących elementów:
  - 2 sztuki urządzeń NAS klasy enterprise.
  - 2 sztuki zestawów montażowych do szafy rack 19".
  - 12 sztuk dysków HDD klasy enterprise 16 TB.
  - 12 sztuk dysków HDD klasy enterprise 8 TB.
  - 4 moduły pamięci RAM 16 GB DDR4 ECC.

- 1 karta sieciowa 10GbE (podwójny port SFP+).
- W ramach realizacji wymagane jest również dostarczenie dokumentacji, gwarancji producenta oraz niezbędnych akcesoriów.
- c) Serwer NAS klasy enterprise
  - Urządzenie musi być serwerem NAS typu Rack, wyposażonym w ośmiordzeniowy procesor o częstotliwości bazowej 2,1 GHz, osiągający w trybie Turbo Boost minimum 2,7 GHz, którego wynik w teście PassMark na lipiec 2025 wynosi co najmniej 10 020 punktów. CPU musi obsługiwać sprzętowe szyfrowanie AES NI.
  - Serwer musi posiadać minimum 8 GB pamięci RAM DDR4 ECC UDIMM z możliwością rozbudowy do co najmniej 64 GB.
  - Urządzenie powinno być wyposażone w co najmniej 12 kieszeni hot swap na dyski 3,5" z możliwością rozbudowy do 36 dysków poprzez dodatkowe jednostki rozszerzające podłączane przez gniazda Infiniband.
  - Serwer musi posiadać co najmniej następujące porty i złącza: 2 porty USB 3.2.1, 2 gniazda rozszerzenia do półek dyskowych, 4 porty 1GbE RJ 45 z obsługą agregacji i failover, 2 porty 10GbE RJ 45 wbudowane w urządzenie (warunek: muszą być częścią urządzenia, a nie kartą PCIe – gniazda PCIe muszą pozostać wolne), 2 gniazda PCIe 3.0 x8.
  - Urządzenie musi obsługiwać funkcje Wake on LAN/WAN. Wymagana jest obecność co najmniej 4 wentylatorów 80 mm × 80 mm.
  - Urządzenie musi obsługiwać systemy plików: wewnętrzne: Btrfs, ext4, zewnętrzne: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT.
  - Serwer musi umożliwiać tworzenie macierzy RAID: RAID F1, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10.
  - Wymagania dotyczące zarządzania pamięcią masową: maksymalny rozmiar wolumenu 1 PB (wymagane 64 GB RAM, tylko RAID 6), maksymalny rozmiar wolumenu 200 TB (wymagane 32 GB RAM), wolumen standardowy 108 TB,
  - Obsługiwane protokoły: SMB1/2/3, NFSv3/v4/v4.1, NFS Kerberized, iSCSI, Fibre Channel, HTTP/HTTPS, FTP, SNMP, LDAP, CalDAV.
  - Usługi plików: obsługa SMB, AFP, NFS, FTP, WebDAV, Rsync, obsługa min. 1300 jednoczesnych połączeń SMB przy rozszerzonej pamięci RAM, pełna obsługa Windows ACL, Kerberos NFS.
  - Wirtualizacja: kompatybilność z VMware vSphere z VAAI, Windows Server 2022, Citrix, OpenStack.
  - Zabezpieczenia: zaporą, szyfrowanie folderów, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowań, HTTPS z konfigurowalnymi szyframi, Let's Encrypt.
  - Oprogramowanie: system plików z obsługą migawkowania, CRC, lustrzanych metadanych, limitów i szybkiego klonowania folderów, obsługa WORM, niezmiennych migawek, darmowe oprogramowanie do backupu heterogenicznych środowisk IT (komputery, serwery, VM), funkcje chmury prywatnej z aplikacjami klienckimi dla PC/Mac oraz Android/iOS, możliwość konfiguracji HA Cluster z dwoma identycznymi urządzeniami, z replikacją w czasie rzeczywistym i natychmiastowym przełączeniem awaryjnym.
  - Konserwacja: obsługa za pomocą dostarczonych szyn RKS 02, wymiana zasilacza bez wyłączania urządzenia i bez narzędzi.
  - Zasilanie: obowiązkowo redundantny zasilacz.
  - Gwarancja: 5 lat na urządzenia główne, 1 rok na akcesoria montażowe (szyny rack).



- d) Zestawy montażowe do rack – 2 sztuki. Wymagane jest dostarczenie kompletów szyn montażowych kompatybilnych z oferowanymi serwerami NAS. Szyny muszą umożliwiać pełne wysunięcie urządzenia z szafy rackowej w celu serwisowania, bez konieczności jego demontażu. Zestaw musi być wyposażony w pełen komplet śrub, przewodnic i akcesoriów montażowych.
- e) Dyski twarde HDD 16 TB klasy enterprise – 12 sztuk. Dyski muszą mieć pojemność co najmniej 16 TB, interfejs SATA III 6 Gb/s oraz być przeznaczone do pracy 24/7 w środowisku NAS/storage, muszą znajdować się na liście kompatybilności NASa. Oczekuje się klasy pracy enterprise z podwyższoną odpornością na drgania, zwiększoną żywotnością oraz wysoką liczbą średnich godzin bezawaryjnej pracy (MTBF na poziomie klasy enterprise). Dyski powinny wspierać rozszerzone funkcje monitoringu stanu (SMART, telemetria producenta).
- f) Dyski twarde HDD 8 TB klasy enterprise – 12 sztuk. Dyski muszą posiadać pojemność co najmniej 8 TB, być zgodne z interfejsem SATA III 6 Gb/s oraz przeznaczone do intensywnej pracy w rozwiązaniach pamięci masowej. Wymagana jest klasa enterprise, wsparcie dla pracy ciągłej, odporność na wibracje oraz funkcje diagnostyczne SMART i dodatkowe funkcje producenta.
- g) Moduły pamięci RAM 16 GB DDR4 ECC – 4 sztuki (D4EC-2666-16G lub równoważne). Moduły pamięci muszą być zgodne z technologią DDR4, o częstotliwości pracy minimum 2666 MT/s, z obsługą korekcji błędów ECC. Moduły muszą być kompatybilne z oferowanymi serwerami NAS i przeznaczone do pracy w systemach pamięci masowej. Wymagana jest konstrukcja serwerowa oraz pełna zgodność ze specyfikacją platformy.
- h) Karta sieciowa 10GbE – 1 sztuka (E10G30-F2 lub równoważna). Wymagana jest karta sieciowa oferująca co najmniej dwa porty 10GbE SFP+, instalowana w slotcie PCIe kompatybilnym z oferowanymi serwerami NAS. Karta musi zapewniać pełną przepustowość 10GbE na każdy port oraz wspierać funkcje offload, obsługę VLAN, agregację łącz oraz zgodność z modułami SFP+ typu LR/SR zgodnie ze standardem producenta.

##### **5) Macierze do backupu w JST z wyposażeniem – 4 sztuki**

- a) Dostawa czterech serwerów NAS klasy profesjonalnej wraz z szynami montażowymi, dyskami twardymi klasy enterprise oraz kartami sieciowymi 10GbE. Wskazane nazwy producentów i modeli mają charakter referencyjny. Zamawiający dopuszcza rozwiązania równoważne, spełniające minimalne parametry techniczne opisane w niniejszym dokumencie.
- b) Przedmiot zamówienia obejmuje dostawę:
  - 4 szt. serwerów NAS klasy enterprise
  - 4 szt. zestawów szyn rack
  - 24 szt. dysków HDD klasy enterprise 8 TB
  - 4 szt. dwuporowych kart sieciowych 10GbE SFP+
- c) Serwer NAS klasy profesjonalnej – 4 sztuki
  - Urządzenie musi być serwerem NAS w obudowie Rack 2U, przeznaczonym do pracy ciągłej w środowisku firmowym. Serwer musi być wyposażony w czterordzeniowy procesor o częstotliwości 2,2 GHz, osiągający w teście PassMark na lipiec 2025 wynik co najmniej 4 550 punktów. CPU musi wspierać sprzętowe szyfrowanie AES NI. Serwer powinien posiadać co najmniej 4 GB pamięci RAM ECC SODIMM z możliwością rozbudowy do co najmniej 32 GB. Jednostka musi obsługiwać minimum 8 kieszeni dyskowych hot swap, z możliwością rozbudowy do 12 dysków przy użyciu zewnętrznej jednostki rozszerzającej, podłączanej poprzez port eSATA.

- Serwer musi oferować następujące porty: minimum 2 porty USB 3.2.1, 1 port eSATA jako złącze rozszerzenia, minimum 4 porty 1GbE RJ 45 z obsługą agregacji łączy i przełączania awaryjnego. Urządzenie musi obsługiwać funkcję Wake on LAN/WAN oraz musi posiadać co najmniej 1 slot PCIe 3.0 x8 (4 linowy) do instalacji kart rozszerzeń. Chłodzenie urządzenia musi opierać się na minimum 2 wentylatorach 80 × 80 × 25 mm.
  - Wymagane wsparcie systemów plików: pliki wewnętrzne: Btrfs, ext4, pliki zewnętrzne: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT.
  - Obsługiwane macierze RAID: minimum SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10.
  - Wymagania dot. pamięci masowej: maksymalny rozmiar wolumenu: 108 TB, minimum 64 wolumeny, wsparcie klonowania i migawek LUN.
  - Obsługiwane protokoły: SMB1/2/3, NFSv3/v4/v4.1, NFS Kerberized, iSCSI, HTTP/HTTPS, FTP, SNMP, LDAP, CalDAV.
  - Wymagania użytkowników i folderów: minimum 256 folderów współdzielonych, minimum 8 zadań synchronizacji.
  - Usługi plików: obsługa SMB, AFP, NFS, FTP, WebDAV, Rsync, obsługa min. 180 jednoczesnych połączeń SMB, pełna integracja z Windows ACL, uwierzytelnianie Kerberos dla NFS.
  - Wirtualizacja: kompatybilność z VMware vSphere z VAAI, Citrix Ready, Windows Server 2022, OpenStack.
  - Bezpieczeństwo: firewall, szyfrowanie SMB, folderów współdzielonych, SSL/TLS, SFTP, rsync/SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS z możliwością konfiguracji szyfrów.
  - Oprogramowanie: system plików z obsługą migawkowania, CRC, lustrzanych metadanych, limitów i szybkiego klonowania folderów, obsługa WORM i niezmiennych migawek, darmowe środowisko backupu dla heterogenicznych systemów (PC, serwery, VM), wsparcie chmury prywatnej bez opłat cyklicznych, aplikacje mobilne i desktopowe, funkcje pracy grupowej (edytor tekstu, arkusz, prezentacje) z wersjonowaniem i współpracą w czasie rzeczywistym, obsługa klastra High Availability (HA) z dwoma identycznymi urządzeniami.
  - Konserwacja i zasilanie: możliwość serwisu urządzenia z użyciem szyn RKS 02, obowiązkowo redundantny zasilacz.
  - Gwarancja: 3 lata na jednostki główne.
- d) Zestawy montażowe do rack – 4 sztuki. Wymagane jest dostarczenie kompletów szyn montażowych kompatybilnych z oferowanymi serwerami NAS. Szyny muszą umożliwiać pełne wysunięcie urządzenia z szafy rackowej w celu serwisowania, bez konieczności jego demontażu. Zestaw musi być wyposażony w pełen komplet śrub, przewodnic i akcesoriów montażowych.
- e) Dyski twarde HDD 8 TB klasy enterprise. Dyski muszą posiadać pojemność co najmniej 8 TB, być zgodne z interfejsem SATA III 6 Gb/s oraz przeznaczone do intensywnej pracy w rozwiązaniach pamięci masowej, muszą znajdować się na liście kompatybilności NASa. Wymagana jest klasa enterprise, wsparcie dla pracy ciągłej, odporność na wibracje oraz funkcje diagnostyczne SMART i dodatkowe funkcje producenta.
- f) Karty sieciowe 10GbE SFP+ – 4 sztuki. Każda karta musi: posiadać minimum 2 porty SFP+ 10GbE, obsługiwać pełną przepustowość 10 Gbit/s na port, być zgodna z PCIe stosowanym w urządzeniu NAS, obsługiwać VLAN, LACP, offload oraz moduły SFP+ zgodne ze standardami producenta.

## 6) Macierze do logów w JST – 4 sztuki

- a) Dostawa czterech serwerów NAS klasy profesjonalnej, wraz z modułami pamięci ECC, dyskami twardymi klasy enterprise oraz szynami rackowymi. Wskazane modele pełnią rolę referencyjną – Zamawiający

dopuszcza sprzęt równoważny, spełniający wszystkie minimalne parametry funkcjonalne i techniczne opisane poniżej.

b) Przedmiot zamówienia obejmuje dostawę:

- 4 szt. serwerów NAS
- 4 szt. modułów pamięci RAM DDR4 ECC 16 GB
- 4 szt. szyn montażowych
- 16 szt. dysków HDD klasy enterprise HAT5 8 TB
- Wszystkie urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnej dystrybucji na rynek UE/PL.

c) Serwer NAS (4 szt.)

- Urządzenie musi być serwerem NAS w obudowie Rack 1U, przeznaczonym do pracy 24/7 w środowisku profesjonalnym. Serwer musi posiadać czterordzeniowy procesor o taktowaniu 2,2 GHz, osiągający w teście PassMark (czerwiec 2025) minimum 4 550 punktów. Wymagane jest wsparcie sprzętowego szyfrowania AES-NI. Urządzenie musi być wyposażone w minimum 2 GB pamięci ECC SODIMM, z możliwością rozbudowy do minimum 32 GB. Jednostka musi obsługiwać co najmniej 4 kieszenie hot-swap, z możliwością rozszerzenia do 8 kieszeni przy użyciu zewnętrznych jednostek rozszerzających podłączanych przez port eSATA.
- Wymagane porty zewnętrzne: minimum 2 porty USB 3.2.1, minimum 1 port eSATA, minimum 4 porty 1GbE RJ-45 z obsługą Link Aggregation i failover.
- Urządzenie musi obsługiwać: Wake on LAN/WAN, minimum 1 gniazdo PCIe gen.3 x8 (4-linowe) dla kart rozszerzeń. Chłodzenie musi być realizowane przez minimum 2 wentylatory 40 × 40 × 20 mm.
- Wymagane wsparcie systemów plików: wewnętrzne: Btrfs, ext4, zewnętrzne: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT. Obsługiwane typy macierzy RAID: SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, obsługa migawek i klonowania LUN.
- Obsługiwane protokoły: SMB1/2/3, NFSv3/v4/v4.1, NFS Kerberized, iSCSI, HTTP/HTTPS, FTP, SNMP, LDAP, CalDAV.
- Usługi plików: obsługa SMB, AFP, NFS, FTP, WebDAV, Rsync, minimum 130 aktywnych połączeń SMB, pełne wsparcie Windows ACL oraz Kerberos dla NFS.
- Wirtualizacja: obsługa VMware vSphere z VAAI, Windows Server 2022, Citrix, OpenStack.
- Bezpieczeństwo: firewall, szyfrowanie folderów, szyfrowanie SMB, FTP/SSL/TLS, SFTP, rsync/SSH, automatyczne blokowanie logowania, HTTPS z konfigurowalnymi szyframi, obsługa Let's Encrypt.
- Oprogramowanie: system plików z obsługą migawek, CRC, lustrzanych metadanych, limitów i szybkiego klonowania, obsługa WORM i migawek niezmiennych, darmowe centralne narzędzie do backupu heterogenicznych środowisk (PC, serwery, VM), darmowa chmura prywatna z aplikacjami klienckimi i obsługą dokumentów biurowych w czasie rzeczywistym, możliwość pracy w klastrze HA (active-passive) przy użyciu dwóch identycznych urządzeń.
- Konserwacja: możliwość obsługi urządzenia za pomocą szyn RKS-02, możliwość łatwego wysuwania na potrzeby serwisowe
- Zasilanie: wymagany redundantny zasilacz (wariant RP+).
- Gwarancja: 3 lata na serwer.

d) Moduły pamięci RAM 16 GB DDR4 ECC (4 szt.). Moduły muszą: mieć pojemność 16 GB, pracować jako DDR4 ECC SODIMM, być zgodne z oferowanymi serwerami NAS.

e) Zestawy montażowe do rack – 4 sztuki . Wymagane jest dostarczenie kompletów szyn montażowych kompatybilnych z oferowanymi serwerami NAS. Szyny muszą umożliwiać pełne wysunięcie urządzenia z



szafy rackowej w celu serwisowania, bez konieczności jego demontażu. Zestaw musi być wyposażony w pełen komplet śrub, przewodnic i akcesoriów montażowych.

- f) Dyski twarde HDD 8 TB klasy enterprise – 16 sztuk. Dyski muszą posiadać pojemność co najmniej 8 TB, być zgodne z interfejsem SATA III 6 Gb/s oraz przeznaczone do intensywnej pracy w rozwiązaniach pamięci masowej, muszą znajdować się na liście kompatybilności NASa. Wymagana jest klasa enterprise, wsparcie dla pracy ciągłej, odporność na wibracje oraz funkcje diagnostyczne SMART i dodatkowe funkcje producenta.

## 7) Warunki i sposób realizacji:

- a) Miejsce dostawy: siedziba Zamawiającego. Termin realizacji: oczekiwany do 90 dni kalendarzowych od podpisania umowy
- b) Odbiór: protokół odbioru zawierający listę komponentów, numery seryjne, wersje firmware i wynik testu POST/diagnostyk.
- c) Szkolenie: krótkie przekazanie informacji dla administratora: dostęp do BMC, polityka aktualizacji firmware, konfiguracja RAID i powiadomień.

## CZĘŚĆ 2 (ZADANIE 2) – Dostawa oprogramowania do backupu i logów:

### 1) System backupu na urządzenie taśmowe – 1 szt.

- a) Dostarczenie licencji oraz usługi wdrożenia systemu kopii zapasowych, przeznaczonego do wykonywania backupu danych o łącznej wielkości co najmniej 5 TB na napęd taśmowy oraz umożliwiającego ich odtwarzanie zgodnie z zasadami bezpieczeństwa i ciągłości działania Zamawiającego. Wskazane nazwy handlowe mają charakter referencyjny – Zamawiający dopuszcza rozwiązania równoważne, spełniające minimalne wymagania techniczne i funkcjonalne.
- b) Zakres obejmuje:
  - o dostawę licencji Veeam Backup & Replication w modelu subskrypcyjnym lub maintenance na okres 1 roku (1Y) – lub rozwiązania równoważnego.
  - o wdrożenie oprogramowania na dedykowanym serwerze Zamawiającego.
  - o konfigurację co najmniej 5 zadań backupu danych z lokalizacji wskazanych przez Zamawiającego.
  - o konfigurację procesu zapisu backupu na napęd taśmowy wskazany przez Zamawiającego.
  - o przeprowadzenie testów backupu i odtworzenia danych, obejmujących: testy integralności kopii zapasowych, test odtworzenia pliku/folderu, raport z przebiegu testów.
  - o przekazanie dokumentacji powdrożeniowej.
- c) System musi zapewniać: tworzenie kopii pełnych, przyrostowych i różnicowych, możliwość backupu co najmniej 5 TB danych, mechanizmy deduplikacji i kompresji danych, obsługę backupu typu file-level oraz (opcjonalnie) image-level, wsparcie backupu zarówno na zasoby dyskowe, jak i na biblioteki lub napędy taśmowe, możliwość tworzenia wielu polityk retencji. System musi: umożliwiać kierowanie danych na taśmy LTO poprzez bibliotekę lub napęd taśmowy, rotację oraz retencję danych, umożliwiać odczyt kopii z taśmy niezależnie od repozytorium dyskowego.
- d) Wymagania dot. Bezpieczeństwa: szyfrowanie danych backupu, integralność kopii zapasowych, możliwość automatycznego testowania odtwarzania (SureBackup lub równoważny mechanizm), raportowanie błędów i alerty e mail.

- e) System musi współpracować z: serwerem Windows wskazanym przez Zamawiającego, infrastrukturą sieciową Zamawiającego, lokalizacjami źródłowymi wskazanymi do backupu.
- f) Usługa wdrożenia musi obejmować:
  - o instalację oprogramowania: instalacja systemu backupu na dedykowanym serwerze (fizycznym lub wirtualnym) wskazanym przez Zamawiającego. Konfiguracja repozytoriów backupowych, w tym repozytorium taśmowego. Aktualizacja oprogramowania do najnowszej stabilnej wersji.
  - o konfigurację backupów: przygotowanie i konfiguracja co najmniej 5 zadań backupu, obejmujących: wybór źródeł danych, harmonogramy, retencję, polityki backupu. Konfiguracja zapisu backupów na napęd taśmowy. Konfiguracja ewentualnych alertów e-mail.
  - o testy powdrożeniowe: wykonanie testowego backupu wszystkich skonfigurowanych zadań, przeprowadzenie testu odtworzenia danych (restore file/folder), potwierdzenie integralności kopii, przygotowanie raportu z testów.
  - o Dokumentacja: po zakończeniu wdrożenia wykonawca przekazuje: dokumentację konfiguracji systemu, wykaz zadań backupu i ich parametrów, procedurę odtwarzania danych, raport z testów

## 2) Kolektor logów z korelacją zdarzeń i wykrywaniem podatności – 1 szt.

- a) Minimalne wymagania funkcjonalne
  - o System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
  - o System musi pracować w oparciu o architekturę Linux.
  - o System musi mieć możliwość centralnego zbierania i zarządzania logami
  - o System działać w trybie zbliżonym do rzeczywistego
  - o System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
  - o System musi zapewniać retencję danych w okresie minimum 365 dni.
  - o Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
  - o System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
  - o Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
  - o Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
  - o System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
  - o System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.
  - o Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
  - o Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
  - o System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, EDGE, Opera.
  - o Interfejs musi posiadać polską wersję językową.

- System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinien spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
- Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
- Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP,
- Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
- System musi wspierać mechanizm logowania typu Single Sign On.
- System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
- System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
- System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
- System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
- System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
- System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
- System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
- System musi pozwalać na tworzenie parserów z poziomu GUI
- System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
- System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
- System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
- Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
- System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
- System musi zapewniać parsowanie wpływających do niego wiadomości w formatach:
  - Syslog,
  - WEF,
  - Flat file,
  - Event log,
  - WMI,
  - SNMP trap,
  - XML,
  - JSON,
  - JDBC/ODBC
  - CSV,
  - Email,

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

- Wykrycia nowej wartości pola w zadanym okresie czasu,
  - Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
  - System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
  - Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
  - System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
  - System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
  - System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow
  - System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
  - System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
  - System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
  - Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
  - System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
  - Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
  - System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
  - System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
  - System umożliwia konfigurację automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
  - Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
  - System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
  - Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
  - System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
  - System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres min 2 lat.
  - Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
  - System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
  - Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
  - System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
  - System musi umożliwiać integrację z Mitre ATT@CK.
- b) Reguły korelacyjne, alerty i obsługa incydentów



- System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
  - System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
  - System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
  - System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
  - System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
  - System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
  - System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
  - Zamawiający wymaga wdrożenia systemu Security Information and Event Management (SIEM), który będzie zapewniał zaawansowane monitorowanie, analizę oraz korelację zdarzeń w infrastrukturze IT. System musi wspierać wykrywanie incydentów bezpieczeństwa oraz spełniać wymagania określone w aktualnych przepisach i normach dotyczących cyberbezpieczeństwa.
- c) Wdrożenie systemu SIEM musi zostać zrealizowane przez:
- Wykwalifikowanego integratora posiadającego doświadczenie w implementacji i konfiguracji systemów SIEM oraz stosowne certyfikaty potwierdzające kompetencje w zakresie cyberbezpieczeństwa i administracji systemami IT.
  - Producenta oprogramowania SIEM, który zapewni pełne wsparcie w zakresie wdrożenia, integracji oraz dalszej eksploatacji systemu.
- d) Lista źródeł
- System musi zbierać i korelować logi z następujących źródeł:
  - Switch zarządzalny typu enterprise – snmp v3
  - Windows Serwer 2016
  - Windows Serwer 2025
  - Linux Debian/UBUNTU
  - Windows 10/11
  - mail
- e) Usługa wdrożenia systemu zbierania logów, korelacji zdarzeń i wykrywania podatności:
- Projekt i instalacja systemu SIEM - kompleksowe przygotowanie architektury, instalacja komponentów (Agregacja, Prezentacja, Retencja), konfiguracja wysokiej dostępności, retencji danych (≥365 dni), bezpieczeństwa komunikacji (TLS 1.2/1.3) oraz skalowalności środowiska opartego na Linux.
  - Integracja ze źródłami logów i konfiguracja parsowania - podłączenie wymaganych źródeł (Windows, Linux, urządzenia sieciowe SNMPv3, systemy pocztowe), wdrożenie agentów i metod bezagentowych, konfiguracja parserów (w tym niestandardowych), normalizacji, geolokalizacji, reputacji IP oraz importu IoC / integracji MISP i MITRE ATT&CK.
  - Reguły korelacyjne, detekcja zagrożeń i obsługa incydentów - uruchomienie i dostosowanie min. 20 predefiniowanych reguł, budowa nowych korelacji, ML do wykrywania anomalii, FIM, skanowanie podatności, obsługa incydentów, playbooki, automatyczne akcje bezpieczeństwa oraz mechanizmy powiadamiania (email/SMS/czat).



- Dashboardy, raportowanie, testy i szkolenia - przygotowanie wizualizacji i raportów (PDF/JPG/CSV/HTML), testy wydajnościowe i funkcjonalne systemu, dokumentacja powdrożeniowa oraz szkolenie administratorów i analityków bezpieczeństwa.