Opis przedmiotu zamówienia

Centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń funkcjonujących w ZKZL sp. z o.o.

Wymagania Ogólne

W ramach Zamówienia wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie Linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Szczegółowe oczekiwane parametry dostarczonego rozwiązania:

Lp.	Nazwa parametru	Minimalna wartość parametru
1.	**Interfejsy, Dysk**	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.
2.	**Parametry wydajnościowe**	System musi być w stanie przyjmować minimum 5 GB logów na dzień. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
3.	**Logowanie**	• Podgląd logowanych zdarzeń w czasie rzeczywistym. • Możliwość przeglądania logów historycznych z funkcją filtrowania. • System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: o Listę najczęściej wykrywanych ataków. o Listę najbardziej aktywnych użytkowników. o Listę najczęściej wykorzystywanych aplikacji. o Listę najczęściej odwiedzanych stron www. o Listę krajów , do których nawiązywane są połączenia. o Listę najczęściej wykorzystywanych polityk Firewall. o Informacje o realizowanych połączeniach IPSec. • Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

		• Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. • 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
4.	**Raportowanie**	• Generowanie raportów co najmniej w formatach: PDF, CSV. • Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. • Funkcję definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
5.	**Korelacja logów**	• Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. • Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. • Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: ○ Malware. ○ Aplikacje sieciowe. ○ Email. ○ IPS. ○ Traffic. ○ Systemowe: utracone połączenie VPN, utracone połączenie sieciowe. • Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
6.	**Zarządzanie**	• System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. • System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

7.	**Serwisy i licencje**	Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
8.	**Ogólne wymagania**	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System do przechowywania logów zebranych w ramach centralnego systemu logowania.

Oprogramowanie typu SDS współpracujące z macierzami użytkowanymi przez Zamawiającego – szczegółowy opis funkcji dostarczanego oprogramowania.

Lp.	Nazwa parametru	Minimalna wartość parametru
9.	**Licencje**	Wymagane dostarczenie licencji dożywotnich nie ograniczonych czasowo z wsparciem i dostępem do nowych wersji zgodnych z punktem 8 specyfikacji.
10.	**Pojemność**	System musi zostać dostarczony z licencją na: 20 TB oraz posiadać możliwość rozbudowy do 400TB per node (serwer fizyczny na którym jest zainstalowany). System SDS musi wspierać dyski w technologii: • SAS 10k • SATA/NL-SAS • SSD System musi pozwalać na rozbudowę do klastra 8 nodów (serwerów). Pojedynczy node musi pozwalać na obsługę do 8 wirtualnych procesorów oraz 64GB RAM. System (pojedynczy node) musi pozwalać na obsługę do 60 dysków. W przypadku klastrowania nodów, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego.
11.	**Obsługa wirtualizatora (Hypervisor)**	Wsparcie dla następujących rozwiązań do wirtualizacji: • VMware vSphere 7.0 oraz 8.0 • KVM na RedHat Enterprise Linux 8.6, 8.7, 8.8, 9.0, 9.1, oraz 9.2 • KVM na Rocky Linux 8 oraz 9
12.	**Obsługiwane Interfejsy**	Oferowany system SDS (dla pojedynczego noda) musi wspierać minimum: • 2 porty 1GbE, • 1 port 10GbE
13.	**Kopie Migawkowe**	System musi być wyposażony w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%

14.	**Obsługiwane protokoły**	System musi obsługiwać jednocześnie protokoły iSCSi, CIFS, NFS oraz S3 - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z systemem
15.	**Inne wymagania**	System musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. System musi posiadać funkcjonalność priorytetyzacji zadań. System musi posiadać funkcjonalność kompresji danych. System musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. System powinien mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotnie większej ilości licencji na TB przestrzeni wyspecyfikowanej. Rozwiązanie musi posiadać funkcjonalność replikacji danych z innym nodem w trybie co najmniej asynchronicznym. Przed procesem replikacji system musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych. Oferowane rozwiązanie musi posiadać licencje na stworzenie klastra geograficznego, który pozwala na synchroniczną replikację danych pomiędzy nodami oraz automatyczne przełączanie w przypadku awarii nodu. System musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne Systemu SDS. Z systemem zamawiający wymaga dostarczenia oprogramowania które pozwala na: • monitoring wykorzystania przestrzeni na systemie • monitoring grup RAIDowych • monitoring wykonywanych backupów/replikacji danych między systemami • monitoring wydajności systemu • analizę i diagnozę spadku wydajności Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność systemu. Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:

		a) Narzędzie do tworzenia procedury aktualizacji oprogramowania: • procedura musi opierać się na aktualnych danych pochodzących z systemu oraz najlepszych praktykach producenta. • procedura musi uwzględniać systemy zależne np,inne systemy SDS lub inne macierze replikujące • procedura musi umożliwiać generowanie planu cofnięcia aktualizacji. b) Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom systemu. c) Wyświetlanie konfiguracji systemu oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji. Portal lub oprogramowanie może pochodzić od innego producenta niż producent system.
8.	**Gwarancja i serwis**	1 rok serwisu oraz 1 rok subskrypcji dla oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.