Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa wraz z montażem, skonfigurowaniem i uruchomieniem systemu SIEM oraz XDR dla zakładowej infrastruktury OT.

System SIEM

1. System SIEM musi być licencjonowany na nieograniczoną liczbę assetów oraz na nieograniczony czas eksploatacji.
2. System SIEM powinien móc przyjąć aż do 1000 zdarzeń bezpieczeństwa na sekundę.
3. System SIEM musi umożliwiać rozbudowę do struktury rozproszonej z zapewnieniem pełnej, nieograniczonej skalowalności
4. System SIEM musi pozwalać na aktualizacje, które mogą zostać zakupione w późniejszym czasie.
5. Brak zakupu aktualizacji nie może powodować zablokowania jakiejkolwiek funkcjonalności systemu SIEM.
6. System SIEM musi posiadać grupy funkcyjne umożliwiające:
    - zarządzanie logami źródłowymi
    - tworzenie i zarządzanie korelacjami danych z różnych źródeł
    - graficzne narzędzie do tworzenia plugin do parsowania danych
    - wbudowany moduł IDS
    - rozbudowaną politykę nadawania uprawnień dla użytkowników
    - weryfikację zgodności z ISO 27001
    - tworzenie i zarządzanie zgłoszeniami w formie Ticket
    - Tworzenie raportów na bazie pobranych danych
    - Klasyfikację alarmów
    - Zarządzanie alarmami
    - Wykonanie, na podstawie zdarzenia, akcji w postaci uruchomienia wskazanego scenariusza reakcyjnego

Urządzenie aktywne XDR

Celem uruchomienia monitorowania systemów OT w jednym węźle należy zastosować kolektor przepływowy z funkcją preprocesora i preanalityki danych, który nie będzie miał wpływu na komunikację przemysłową.

1. Licencjonowanie musi pozwalać na pełną pracę urządzenia i systemu nawet w przypadku nie wykupienia aktualizacji;
2. System XDR musi być licencjonowany na nieograniczoną liczbę assetów oraz na nieograniczony czas eksploatacji;
3. System XDR musi umożliwiać rozbudowę do struktury rozproszonej z zapewnieniem pełnej, nieograniczonej skalowalności;
4. Brak zakupu aktualizacji nie może powodować zablokowania jakiejkolwiek funkcjonalności systemu XDR;
5. System XDR musi pozwalać na aktualizacje, które mogą zostać zakupione w późniejszym czasie;
6. System XDR musi posiadać grupy funkcyjne umożliwiające:
    - Pracę z zainstalowanymi agentami bezpieczeństwa,
    - Przyjmowanie danych z kolektora i przekazywania ich do systemu SIEM,
    - Detekcję i korelację zdarzeń z uznanymi dobrymi praktykami i standardami,
    - Analitykę zdarzeń pod kątem bezpieczeństwa;

1. Producent musi zapewnić możliwość zakupu aktualizacji w zakresie:
    - Rozszerzonej gwarancji na sprzęt,
    - Bezpieczeństwa aktualizacji oprogramowania,
    - Bezpieczeństwa aktualizacji modułów i sygnatur bezpieczeństwa;

1. Kolektor musi posiadać minimum następujące grupy funkcyjne:
    - Przełączanie ruchu Ethernet na wszystkich portach komunikacyjnych,
    - Routing L3 (BGP, OSPF, ISIS, Static),
    - Zone Based Firewall,
    - Koncentrator VPN,
    - Trafiic Policy,
    - SPBR,
    - Sondę IDS,
    - Profiler obiektów wraz z detekcją protokołów przemysłowych oraz IT,
    - Ilość portów RJ45 1 Gb/s – 24,
    - Ilość portów SFP 1 Gb/s – 8,
    - Ilość portów SFP+ 10 Gb/s – 4,
    - Wielkość lokalnego storage: min 400 GB,
    - Dwa zasilacze w układzie redundantnym – 230 V
    - Zabudowa w szafie Rack 19”
    - Zarządzanie z poziomu CLI,
    - System musi umożliwiać stosowanie technik SDN dla zarządzania większą ilością urządzeń w środowisku,
    - Możliwość tworzenia skutecznej segmentacji logicznej L2 oraz L3 dla dowolnie wybranych grup portów, odpornej na techniki QinQ potwierdzonym przez producenta urządzenia.

Server do szafy Rack do Systemu SIEM

W zakresie usługi jest wymagane dobranie sprzętu do systemu. Poniżej min. wymagania dla serwera:

PROCESOR	Intel® E-2336
Taktowanie bazowe / turbo	2.90 GHz / 4.80 GHz
Ilość rdzeni / wątków	6 / 12
Pamięć Cache	12 MB
Rodzaj pamięci	DDR4 3200 MHz ECC
Maks. wielkość pamięci	128 GB
Liczba kanałów pamięci	2
TDP	65 W

PAMIĘĆ RAM	32GB DDR4 UDIMM
Szyna	3200 MHz
Typ	DDR4
Rodzaj	UDIMM
Pojemność modułu	32GB

KONTROLER RAID	PERC H355
Typ kontrolera	Sprzętowy
Pamięć cache	Brak
Poziomy RAID	0/1/10
Rodzaje dysków	12Gb/s SAS, 6Gb/s SAS/SATA
Wsparcie PCI	PCIe Gen. 4

DYSKI I NAPĘDY	Obudowa 4x 3.5" HP
Typ dysku	3.5"
Max. ilość dysków	4 (Hot-Plug)

DYSKI I NAPĘDY	2 x 2TB HDD NLSAS 7.2k
Pojemność dysku	2 TB
Wymiary	3.5"
Typ dysku	HDD
Interfejs	SAS 12Gb/s
Prędkość obrotowa	7200 obr/min
Typ obudowy	Hot-Plug

KARTA SIECIOWA	LOM DP (Zintegrowana)
Porty	2x RJ-45
Przepustowość	1Gb/s
Standard	1000Base-T
Typ karty	Zintegrowana

ZDALNE ZARZĄDZANIE	iDRAC9 Basic (1 x RJ-45)
Dedykowany port	Tak

RAMKA ZABEZPIECZAJĄCA	Ramka bez LCD

SZYNY MONTAŻOWE	Szyny ruchome

ZASILANIE	2x 700W (Hot-Plug)
Moc	2x 700 W
Typ	Hot-Plug
Redundancja	Tak

GWARANCJA	3 lata
Okres gwarancji	3 lata
Typ wsparcia	Gwarancja podstawowa
Czas reakcji	Następny dzień roboczy

KARTY ROZSZERZEŃ	Intel® i350 QP (PCIe)
Porty	4x RJ45
Przepustowość	1Gb/s
Standard	10GBase-T
Typ karty	PCIe