Dostawa urządzenia typu sBDS (Server Breach Detection System) służącego do wykrywania zagrożeń sieciowych i reagowania (NDR - Network Detection and Response) dla Izerskiego Centrum Pulmonologii i Chemioterapii „Izer-Med" Spółka z o.o.

Wymagane parametry techniczne i cechy użytkowe urządzenia

NTA (Network Trafic Analayzer)

Lp.	Parametr	Charakterystyka
1.	Dane techniczne:	• Wysokość 1U do montażu w szafie rack • Posiadać co najmniej dwa porty USB • Urządzenie musi posiadać minimum interfejsów: 4x GE • Urządzenie musi posiadać możliwość rozbudowy interfejsów o conajmniej 4 interfejsy SFP • Musi obsługiwać co najmniej 1T przestrzeni dyskowej • Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń • Proponowane rozwiązanie musi obsługiwać minimum 750 tys. jednoczesnych sesji • Proponowane rozwiązanie musi obsługiwać 20 700 nowych sesji w ruchu HTTP
2.	Usługi sieciowe:	• Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta • Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń • Musi posiadać możliwosc rozwiązywania wiadomości przez protokół MPLS oraz VXLAN i wykrywania zagrożeń w tych wiadomościach
3.	Kontrola aplikacji:	• Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp. • Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android • Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje
4.	Wykrywanie zagrożeń:	• Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń • Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow • Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA • Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. • Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku • Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS • Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS

		• Rozwiązanie musi mieć opcję przechwytywania pakietów • System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
5.	Skanowanie antywirusowe:	• Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur • Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP • Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach • Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
6.	Wykrywanie botnetów C&C:	• Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C • Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C • Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen • Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS • Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA • Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS
7.	Sandbox w chmurze:	• Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń • Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy • Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP • Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty • Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików • Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie
8.	Wykrywanie spamu:	• Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym • Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości • Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 • Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen
9.	Dodatkowe funkcje ochrony:	• Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. • Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP • Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu

		• Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
10.	Inteligentne funkcje bezpieczeństwa:	• Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki • Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym • Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp. • Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania • Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut • Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów • Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS • Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji • Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym • Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń • Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia • Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta • Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd. • Rozwiązanie musi obsługiwać przechwytywanie pakietów online • Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania • Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych • Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę • Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń
11.	Widoczność ryzyka/zagrożeń:	• Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego • Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch

		• Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu • Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. • Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni • Rozwiązanie musi wspierać wskazanie ścieżki ataku
12.	Analiza i odpowiedzi na incydenty:	• Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury • Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach • Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie • Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania • Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail
13.	Administracja:	• Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) • Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli • Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło • Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów • Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych • Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny • Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
14.	Logowanie i raportowanie:	• Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP • Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp. • Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS • Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń • Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje • Wstępnie zdefiniowane zadania raportowania • Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni • Rozwiązanie musi wspierać restAPI

15.	Gwarancja/dostawa:	Dostawa musi zawierać również: • 60-miesięczną gwarancję producenta na dostarczone elementy systemu • Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 60 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C) • Wsparcie techniczne dystrybutora rozwiązań w języku polskim

Producent urządzenia: …… *(wpisać)*

Nazwa i typ: …… *(wpisać)*

Kalkulacja ceny

Lp.	**Nazwa art.**	**j.m.**	**Ilość**	**Cena jedn. netto**	**Wartość netto** [kol. 4 x kol. 5]	**VAT ….%**	**Wartość brutto** [kol. 6 + kol. 7]
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***
1.	Urządzenie typu sBDS	szt.	**1**				
Razem netto, VAT, brutto *Kwoty należy przenieść do Formularza oferty pkt 4.3.*							

Miejscowość, data ……