**Załącznik nr 2a do SWZ -** **Formularz minimalnych parametrów technicznych**

**Część nr 6**

PARAMETRY TECHNICZNE

„Dostawa i wdrożenie systemu typu SIEM”

|  |
| --- |
| **3.5 DOSTAWA I WDROŻENIE SYSTEMU TYPU SIEM WRAZ ZE SZKOLENIEM** |
| **System SIEM – wymagania minimalne** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Minimalne wymagania** | **Parametr wymagany TAK/NIE** | **Parametr oferowany** |
| 1 | Kompatybilność z UTM | Dostarczenie centralnego systemu zbierania logów kompatybilnego z posiadanym systemem UTM Zamawiającego. | Tak |  |
| 2 | Forma dostawy (system zbierania logów) | Platforma działająca w środowisku wirtualnym lub komercyjna platforma bazująca na Linux w środowisku wirtualnym. | Tak |  |
| 3 | Wspierane hypervisory | Możliwość uruchomienia co najmniej na: • VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7 • Microsoft Hyper-V 2008 R2/2012/2012 R2/2016/2019/2022/2025 • Citrix XenServer 6.0+ • Open Source Xen 4.1+ • KVM • AWS • Microsoft Azure • Google Cloud (GCP) | Tak |  |
| 4 | Interfejsy sieciowe | Obsługa co najmniej 4 interfejsów sieciowych. | Tak |  |
| 5 | Pojemność dyskowa | Powierzchnia dyskowa o pojemności minimum 3 TB. | Tak |  |
| 6 | Wydajność przyjmowania logów | Możliwość przyjmowania minimum 5 GB logów na dzień. | Tak |  |
| 7 | Skalowalność źródeł logów | Możliwość kolekcjonowania logów z co najmniej 1000 systemów. | Tak |  |
| 8 | Tryb pracy (on-premise) | Pełna funkcjonalność w środowisku Zamawiającego (instalacja lokalna/on-premise), bez konieczności przekazywania logów i danych eksploatacyjnych do chmury poza infrastrukturę Zamawiającego. | Tak |  |
| 9 | Architektura – sondy monitorujące | Architektura oparta o fizyczne lub wirtualne sondy monitorujące, które: • odbierają kopię ruchu sieciowego, • generują alarmy i/lub metadane o zdarzeniach, • przygotowują przechwycone pliki do dalszej analizy, • przekazują przetworzone dane do urządzenia administracyjnego. | Tak |  |
| 10 | Architektura – urządzenie administrujące | Urządzenie administracyjne zarządzające sondami (reguły detekcji, sygnatury, nadzór stanu), realizujące dogłębną analizę odebranych plików, prezentację wyników detekcji oraz przekazywanie danych do rozwiązań stron trzecich. | Tak |  |
| 11 | Szyfrowanie dysków | Obsługa szyfrowania dysków w standardzie LUKS. | Tak |  |
| 12 | Środowiska wdrożeniowe (wirtualizacja) | Wspierana implementacja na środowisku wirtualnym m.in.: VMWare, Hyper-V, Proxmox, KVM, OVM, OVF. | Tak |  |
| 13 | Model licencjonowania | Licencja na zakup i serwis bazująca na liczbie aktywnie występujących w ruchu sieciowym adresów IP; liczba adresów objętych monitorowaniem: do 400. | Tak |  |
| 14 | Dostęp do modułów | Moduły dostępne w przeglądarce, zabezpieczone połączeniem HTTPS. | Tak |  |
| 15 | Zakres informacji w konsoli | Konsola zawiera informacje m.in.: adresy IP, adresy MAC, porty, protokoły, wyniki skanów plików, payload, sygnatury czasowe. | Tak |  |
| 16 | Ocena ryzyka i tagowanie | Szacowanie poziomu ryzyka dla wykrytego zagrożenia; możliwość tagowania zdarzeń i dodawania notatek. | Tak |  |
| 17 | Filtrowanie zdarzeń | Wbudowane filtrowanie min. po: dacie, agencie, poziomie reguły (priorytet). | Tak |  |
| 18 | Grupowanie zdarzeń (identyczne) | Możliwość grupowania takich samych zdarzeń w ramach jednego wpisu oraz wskazanie liczby wystąpień. | Tak |  |
| 19 | Grupowanie zdarzeń (opis reguły) | Możliwość wyświetlania zdarzeń pogrupowanych wg opisu reguły wraz z liczbą wystąpień. | Tak |  |
| 20 | Prezentacja wyników | Wyświetlanie wyników w postaci tabeli z możliwością sortowania. | Tak |  |
| 21 | Akcje na wpisach | Dla każdego wiersza dostępne opcje: podgląd ostatniego zdarzenia, usunięcie grupy zdarzeń, dodanie do grupy ignorowanych. | Tak |  |
| 22 | Konfiguracja widoku | Możliwość ustawienia liczby wyświetlanych wierszy. | Tak |  |
| 23 | Obsługa zgłoszeń | Możliwość utworzenia zgłoszenia z dowolnego zdarzenia (tytuł i opis), zmiana statusu zgłoszeń, dedykowany panel i widok; zgłoszenia przechowywane w lokalnej bazie danych; możliwość zmiany statusu z poziomu konsoli. | Tak |  |
| 24 | Silniki detekcji | Obsługa silników detekcji (Analiza Shellcode i Powershell) – detekcja technik wykorzystywanych przez cyberprzestępców. | Tak |  |
| 25 | Analiza ruchu sieciowego | Możliwość analizowania całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń. | Tak |  |
| 26 | Logowanie w czasie rzeczywistym | Podgląd logowanych zdarzeń w czasie rzeczywistym. | Tak |  |
| 27 | Logi historyczne | Możliwość przeglądania logów historycznych z funkcją filtrowania. | Tak |  |
| 28 | Raporty podręczne (predefiniowane) | Predefiniowane (lub konfigurowalne) raporty graficzne/tekstowe obejmujące co najmniej: • najczęściej wykrywane ataki • najbardziej aktywnych użytkowników • najczęściej wykorzystywane aplikacje • najczęściej odwiedzane strony www • kraje docelowe połączeń • najczęściej wykorzystywane polityki Firewall • informacje o połączeniach IPSec | Tak |  |
| 29 | Forwarding logów | Możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych; mechanizmy filtrowania dla wysyłanych logów. | Tak |  |
| 30 | Protokoły syslog | Komunikacja z systemem centralnego logowania możliwa co najmniej z użyciem UDP/514 oraz TCP/514. | Tak |  |
| 31 | Eksport logów długoterminowy | Cykliczny eksport logów do zewnętrznego systemu dla długoterminowego składowania: przez SFTP lub na zewnętrzny zasób sieciowy. | Tak |  |
| 32 | Formaty raportów | Generowanie raportów co najmniej w formatach: PDF, CSV. | Tak |  |
| 33 | Raporty predefiniowane | Predefiniowane zestawy raportów z możliwością modyfikacji parametrów prezentowania wyników przez administratora. | Tak |  |
| 34 | Raporty własne | Możliwość definiowania własnych raportów. | Tak |  |
| 35 | Spolszczenie raportów | Możliwość spolszczenia raportów. | Tak |  |
| 36 | Harmonogram raportów i wysyłka | Generowanie raportów cyklicznie lub na żądanie oraz automatyczne przesyłanie wyników na wskazany adres/adresy e-mail. | Tak |  |
| 37 | Korelacja zdarzeń | Korelacja logów z określeniem urządzeń, dla których proces ma być realizowany. | Tak |  |
| 38 | Powiadomienia | Konfiguracja powiadomień: e-mail oraz SNMP dla zdarzeń sieciowych, systemowych i bezpieczeństwa. | Tak |  |
| 39 | Kategorie reguł korelacyjnych | Korelacja zdarzeń co najmniej dla kategorii: • Malware • Aplikacje sieciowe • Email • IPS • Traffic • Systemowe (utracone połączenie VPN, utracone połączenie sieciowe) | Tak |  |
| 40 | Analiza logów archiwalnych | Analiza logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach (wykrywanie potencjalnie narażonych stacji). | Tak |  |
| 41 | Automatyzacja (playbooki) | Zarządzanie zdarzeniami z automatyzacją zadań konfigurowalną za pomocą playbooków (reakcje i sekwencje działań). | Tak |  |
| 42 | Zarządzanie (interfejs) | Zarządzanie lokalne z wykorzystaniem protokołów HTTPS oraz SSH lub dedykowana konsola producenta komunikująca się szyfrowanymi protokołami. | Tak |  |
| 43 | Uwierzytelnianie administratorów | Uwierzytelnianie w oparciu o: lokalną bazę, Radius, LDAP, PKI. | Tak |  |
| 44 | Liczba administratorów | Możliwość zdefiniowania co najmniej 2 administratorów oraz określenia praw dostępu do logów i raportów per źródło logów. | Tak |  |
| 45 | System analizy logów – charakter | Rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa. | Tak |  |
| 46 | System analizy logów – forma dostawy | Dostarczenie jako maszyna wirtualna instalowana w środowisku VMware lub Windows Hyper-V. | Tak |  |
| 47 | Zakres danych analitycznych | Dane powinny zawierać co najmniej informacje o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach. | Tak |  |
| 48 | Obsługa incydentów (reguły) | Obsługa incydentów na podstawie reguł automatycznie wyszukujących zdarzenia z logów. | Tak |  |
| 49 | Synchronizacja czasu | Możliwość synchronizacji z serwerami czasu NTP. | Tak |  |
| 50 | Panele producenta | Predefiniowane panele (dashboardy) w postaci graficznej prezentacji zebranych informacji wykonane przez producenta. | Tak |  |
| 51 | Protokoły zbierania danych | Gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP. | Tak |  |
| 52 | Bezpieczne gromadzenie | Bezpieczne gromadzenie danych przy pomocy protokołu TLS. | Tak |  |
| 53 | Syslog forwarder | Możliwość przesyłania logów do innego serwera logów (funkcja syslog forwarder). | Tak |  |
| 54 | Instalacja lokalna | Rozwiązanie lokalne wymagające instalacji w środowisku klienta. | Tak |  |
| 55 | Wyszukiwanie logów z firewalli | Narzędzie do przeszukiwania logów zebranych z podłączonych firewalli; możliwość wielokrotnego stosowania filtrów/zapytań. | Tak |  |
| 56 | Wyszukiwanie zaawansowane | Wyszukiwanie zaawansowane oparte o wiele kryteriów (rodzaj logu, czas itp.). | Tak |  |
| 57 | Prezentacja wyników wyszukiwania | Wyświetlanie rezultatów wyszukiwania co najmniej jako logi proste i graficzne. | Tak |  |
| 58 | Źródła zewnętrzne | Wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP). | Tak |  |
| 59 | Nawigacja czasowa | Nawigacja na podstawie czasu (minuty, godziny, dni, okresy). | Tak |  |
| 60 | Eksport wyników | Eksport wyników wyszukiwania w formacie CSV. | Tak |  |
| 61 | Raporty statyczne | Możliwość tworzenia statycznych raportów oraz zapisywania raportów do pliku PDF. | Tak |  |
| 62 | Planowanie raportów | Możliwość zaplanowania wykonania raportów. | Tak |  |
| 63 | Reguły alarmujące | Tworzenie reguł alarmujących na podstawie kryteriów przeszukiwania logów; powiadomienie minimum e-mail. | Tak |  |
| 64 | Incydenty z kryteriów | Tworzenie incydentów z kryteriów zapytań i zarządzanie incydentami: przypisywanie osób, komentarze, podgląd logów źródłowych. | Tak |  |
| 65 | Wydajność (EPS) | Liczba zdarzeń na sekundę (EPS): minimum 9 500. | Tak |  |
| 66 | Retencja logów | Możliwość zarządzania logami: minimum 3 lata. | Tak |  |
| 67 | Liczba obsługiwanych urządzeń | Minimum 600 obsługiwanych urządzeń. | Tak |  |
| 68 | Zapis zdarzeń na dobę | Liczba zapisu zdarzeń na dobę: minimum 12 000 MB. | Tak |  |
| 69 | Hypervisory dla systemu logów | System logów musi wspierać hiperwizory: VMware ESXi, Microsoft HyperV oraz Proxmox. | Tak |  |
| 70 | System SIEM – monitorowanie incydentów | Rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego. | Tak |  |
| 71 | System SIEM – tryb pracy | Pełna realizacja funkcjonalności lokalnie (instalacja on-premise). | Tak |  |
| 72 | Serwer/urządzenie administrujące – obudowa | Obudowa rack maksymalnie 2U dla minimum 8 dysków. | Tak |  |
| 73 | Serwer/urządzenie administrujące – procesor | Procesor w architekturze x86; minimum 12 rdzeni. Wynik wydajności procesora powinien przekraczać 173 punkty baseline w teście SPECrate®2017\_int\_base (konfiguracja 2-procesorowa). | Tak |  |
| 74 | Serwer/urządzenie administrujące – pamięć RAM | Minimum 96 GB RAM w maksymalnie 4 modułach. | Tak |  |
| 75 | Serwer/urządzenie administrujące – RAID | Kontroler RAID z minimum 8 GB cache i podtrzymaniem bateryjnym lub minimum 8 GB cache typu flash. | Tak |  |
| 76 | Serwer/urządzenie administrujące – przestrzeń dyskowa | Dostępna powierzchnia dyskowa minimum 38 TB w RAID 5 oraz minimum 1,9 TB SSD w minimum RAID 1. | Tak |  |
| 77 | Serwer/urządzenie administrujące – sieć 10G | Karta sieciowa 2-portowa minimum 10 Gbit SFP+ wraz z modułami umożliwiającymi podłączenie do przełączników LAN Zamawiającego. | Tak |  |
| 78 | Serwer/urządzenie administrujące – sieć 1G | Karta sieciowa 2-portowa minimum 1 Gbit RJ45. | Tak |  |
| 79 | Serwer/urządzenie administrujące – zasilanie | Dwa redundantne zasilacze Hot-Swap. | Tak |  |
| 80 | Serwer/urządzenie administrujące – zdalne zarządzanie | Moduł zdalnego zarządzania poprzez konsolę graficzną wraz z licencją na minimum 3 lata. | Tak |  |
| 81 | Serwer/urządzenie administrujące – gwarancja | Minimum 3 lata gwarancji w miejscu instalacji; rozpoczęcie naprawy NBD. | Tak |  |
| 82 | Serwer dedykowany – redundantne zasilanie | Serwer dedykowany musi posiadać redundantne zasilanie i 3-letnią gwarancję w miejscu instalacji. | Tak |  |
| 83 | Sonda – porty i przepustowość | Sonda posiada co najmniej 4 porty monitorujące i przetwarza ruch do 4 Gb/s. | Tak |  |
| 84 | Wydajność serwera dedykowanego | Obsługa do 3 900 zdarzeń na sekundę, przechowywanie do 9 milionów zdarzeń, detekcja malware oraz analiza silnikiem shellcode/powershell do 3 na sekundę. | Tak |  |
| 85 | Konsola SIEM – grupowanie zdarzeń | Grupowanie takich samych zdarzeń w jednym wpisie wraz z liczbą wystąpień. | Tak |  |
| 86 | Konsola SIEM – zgłoszenia | Możliwość tworzenia i śledzenia zgłoszeń; utworzenie zgłoszenia z dowolnego zdarzenia; dedykowany widok zgłoszeń. | Tak |  |
| 87 | Moduł EDR – zakres dostawy (opcjonalnie) | Wykonawca może dostarczyć moduł EDR wraz z centralną konsolą dla minimum 300 urządzeń (adresów IP) oraz gwarancją i wsparciem technicznym na minimum 36 miesięcy. | Nie |  |
| 88 | Moduł EDR – platformy | EDR dla systemów Windows oraz MacOS; współpraca z używanym przez Zamawiającego systemem antywirusowym. | Nie |  |
| 89 | Moduł EDR – konsola centralna | Centralna konsola administracyjna do monitorowania i wizualizacji danych z urządzeń. | Nie |  |
| 90 | Moduł EDR – serwer administracyjny | Serwer administracyjny umożliwiający wysyłanie zdarzeń do konsoli oraz konfigurowanie wykluczeń. | Nie |  |
| 91 | Moduł EDR – kryteria wykluczeń | Wykluczenia konfigurowane w oparciu o min.: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika. | Nie |  |
| 92 | Moduł EDR – weryfikacja procesów | Weryfikacja uruchomionych plików wykonywalnych na stacji roboczej z podglądem szczegółów min.: SHA-1, rozmiar pliku. | Nie |  |
| 93 | Moduł EDR – klasyfikacja plików | Możliwość oznaczania plików wykonywalnych i DLL jako bezpieczne lub niebezpieczne. | Nie |  |
| 94 | Moduł EDR – audyt i zdalne komendy | Możliwość audytowania działań administratorów oraz połączenia ze stacją roboczą i wykonywania komend zdalnych. | Nie |  |
| 95 | Moduł EDR – bezpieczeństwo dostępu | Dostęp WWW zabezpieczony protokołem SSL; zabezpieczona komunikacja między modułami serwera z użyciem certyfikatów; możliwość utworzenia własnego CA i certyfikatów (agent/serwer zarządzający/serwer proxy). | Nie |  |
| 96 | Moduł EDR – integracje i raporty | Integracja min. z konsolą antywirusa; min. 100 szablonów raportów producenta lub własnych; powiadomienia min. e-mail oraz do dziennika syslog; podział uprawnień administratorów na grupy/polityki; informowanie o niezainstalowanych aktualizacjach. | Nie |  |
| 97 | Monitoring IT – użytkownicy | Tworzenie wielu użytkowników bez dodatkowych opłat; równoległy dostęp; ograniczanie dostępu do wybranych grup hostów. | Tak |  |
| 98 | Monitoring IT – funkcje monitorowania | Monitorowanie m.in.: • serwerów fizycznych, urządzeń sieciowych, stanu połączeń oraz interfejsów sieciowych • maszyn wirtualnych (Windows i Linux) oraz możliwość rozbudowy o kolejne urządzenia • automatyczne wykrywanie usług, powiadamianie o nowych usługach; grupowanie hostów • planowane przerwy serwisowe; ACK (potwierdzanie/obsługa alertów); operacje na grupach hostów • raporty dostępności urządzeń/usług/procesów biznesowych (WWW) • monitorowanie z agentami; serwerów aplikacji (Tomcat, Oracle WebLogic Server, Oracle Application Server) • Active Directory; serwerów plików i udziałów; statusu Apache • baz danych: Oracle, MySQL, Postgress, MSSQL Server, DB2 • protokoły: SNMP, WMI, IPMI; konfiguracja monitoringu przez WWW • DNS; środowisk VMware, Hyper-V, Proxmox; serwera czasu NTP i offsetu czasu • ping (czasy odpowiedzi, straty pakietów); zasobów systemowych (dysk, RAM, CPU) • logów systemowych Windows; macierzy/NAS (status urządzenia i dysków) • dodawanie własnych wtyczek/agentów; zgodność z wtyczkami Nagios • agregacja usług do procesów biznesowych; symulacja awarii i analiza wpływu • monitoring rozproszony (wiele instancji); wykrywanie niestabilnych usług; dostępność WWW • konfiguracja hierarchiczna (dziedziczenie ustawień) | Tak |  |
| 99 | Monitoring IT – prezentacja | Mapa stanu urządzeń; dashboardy; elastyczna konfiguracja dashboardów; wizualizacja całej infrastruktury na jednym dashboardzie; tworzenie dashboardów przez użytkowników. | Tak |  |
| 100 | Monitoring IT – powiadomienia | Globalne wyłączanie powiadomień; powiadomienia e-mail; eskalacja do kolejnych użytkowników; okna czasowe powiadomień; progi alertów na poziomie globalnym/grup/urządzeń/usług. | Tak |  |
| 101 | Monitoring IT – konfiguracja | Konfiguracja przez WWW; automatyczna konfiguracja i działanie z REST-API; centralne zarządzanie agentami; integracja danych z różnych źródeł (JSON, XML, SNMP); monitoring bazy danych systemu HIS. | Tak |  |
| 102 | Monitoring IT – monitoring bazy HIS | Możliwość monitorowania bazy HIS w zakresie co najmniej: Instance state, Version, Jobs, Locks, Processes, aktywne sesje, Recovery area, Log switch activity, tablespaces (info i performance), Long active sessions, Undo retention, checkpoint/backup state, Custom SQLs, RMAN backup status/backups, ASM disk groups, Oracle Data-Guard lag; możliwość dodawania własnych zapytań SQL i monitorowania zwracanych wartości. | Tak |  |
| 103 | Monitoring IT – kolektor logów | Własny kolektor syslog; odbiór z syslog lub SNMP traps; analiza logów tekstowych oraz Windows Event; klasyfikacja wg reguł użytkownika; korelacja/podsumowanie/zliczanie/opisywanie/przepisywanie wiadomości z uwzględnieniem relacji czasowych. | Tak |  |
| 104 | Monitoring IT – cyberbezpieczeństwo (UTM) | Monitorowanie urządzeń klasy UTM m.in.: wykrywanie włamań i szybkość blokowania (progi WARN/CRIT), synchronizacja HA, stany alarmów czujników, liczba sesji, liczba tuneli IPSec VPN, wykrywanie wirusów i szybkość blokowania, poziom wykorzystania CPU (progi konfigurowalne). | Tak |  |
| 105 | Monitoring IT – integracja kolektora syslog | Odbiór i prezentacja danych z UTM i z systemu EDR z wykorzystaniem kolektora logów syslog. | Tak |  |
| 106 | Monitoring IT – zakres monitorowania (ilościowy) | Monitoring krytycznych elementów infrastruktury (maks.): • serwery fizyczne do 8 szt. • VM Windows/Linux/hosty do 25 szt. • serwery AD do 4 szt. • macierze/NAS do 4 szt. • przełączniki rdzeniowe do 2 szt. • przełączniki dostępowe do 15 szt. • UPS do 4 szt. • serwer bazodanowy 1 szt. • serwer backupu 1 szt. Monitoring krytycznych systemów: Oracle (baza systemu szpitalnego), HIS, ERP, PACS. | Tak |  |