Załącznik Nr 5 do SWZ

FORMULARZ TECHNICZNY

Część II – zakup i dostawa do siedziby Urzędu Miasta Ostrów Mazowiecka licencji oprogramowania do gromadzenia i analizy logów (dzienników zdarzeń) ze stacji roboczych i urządzeń sieciowych

Wymagania ogólne:

- Zakupione licencje mają umożliwiać korzystanie z oprogramowania bez ograniczeń czasowych i funkcjonalnych z możliwością przenoszenia ich na wymieniane urządzenia w ramach posiadanej ilości.
- Zaproponowana cena musi zawierać minimum roczne wsparcie techniczne i wdrożeniowe oraz aktualizacje oprogramowania. Odnowienie opłaty dotyczącej wsparcia technicznego, w przypadku braku jej ciągłości, ma umożliwić aktualizację oprogramowania do najnowszej dostępnej wersji.
- Wykaz urządzeń, z których będą zbierane logi:

L.p.	Nazwa	Ilość
1	Firewall Fortigate	1
2	Router Mikrotik	1
3	Switche	10
4	Microsoft Windows Server	3
5	Microsoft Windows Server Microsoft Windows SQLServer	2
6	Macierz dyskowa	4
7	Stacje robocze z Windows	90

L.p.	OPIS OGÓLNY	Określenie, czy oferowany element przedmiotu zamówienia spełnia, czy nie spełnia minimalnych wymagań	Oferowany parametr/ cecha – należy opisać tyko w przypadku, gdy oferta obejmuje rozwiązania równoważne rozwiązaniom opisywanym w dokumentacji postępowania – szczegółowe określenie parametrów
1	**Najważniejsze funkcjonalności:** 1) Aplikacja obsługuje logi z wielu systemów operacyjnych; 2) Aplikacja obsługuje logi z wielu urządzeń: (Windows, Linux, Unix, AIX, routery, przełączniki, VMWare, dowolne źródło logów w formacie Syslog); 3) Aplikacja zbiera dzienniki zdarzeń w trybie bezagentowym jak też w oparciu o agentów; 4) System umożliwia gromadzenie logów przez minimum 24 miesiące; 5) System pozwala na konfigurowanie własnych widżetów i widoków; 6) Aplikacja umożliwia wyszukiwanie w logach za pomocą operatora logicznego, frazy, zakresów wartości, symboli wieloznacznych i wyszukiwania grupowego; 7) System pozwala użyć trybu aktywnego FTP dla importu pliku dziennika; 8) Aplikacja umożliwia importowanie i analizowanie plików zdarzeń; 9) System wspiera automatyczne wykrywanie hostów; 10) Aplikacja umożliwia filtrowanie zdarzeń przed zapisaniem ich w bazie danych; 11) System pozwala na archiwizowanie zebranych danych do skompresowanego pliku; 1) Aplikacja umożliwia szyfrowanie plików archiwum logów; 2) System wspiera hashowanie i dodawanie znaczników czasu do plików archiwum; 3) System umożliwia na wyświetlanie zdarzeń w czasie rzeczywistym; 4) System posiada automatyczne alerty; 5) Aplikacja wspiera autoryzowany dostęp; 6) Aplikacja umożliwia tworzenie własnych zakładek oraz dashboard`ów; 7) System pozwala na grupowanie hostów w celu wdrożenia zasad parsowania logów; 8) Aplikacja umożliwia zaplanowanie zbierania danych; 9) System pozwala na utworzenie raportów niestandardowych; 10) Aplikacja umożliwia planowane wykonywanie raportów;		

	11) System posiada raporty PUMA; 12) Aplikacja obsługuje wiele formatów raportów; 13) Aplikacja pozwala na eksportowanie raportów w formatach: CSV, PDF; 14) System pozwala na wykonanie analizy trendów; 15) System pozwala na wykonanie analizy bezpieczeństwa; 16) Aplikacja posiada gotowe raporty zgodności (EventLog i Syslog) (predefiniowane i dostosowywalne); 17) System umożliwia wykonanie polecenia/akcji w przypadku alertów; 18) System pozwala na skonfigurowanie powiadomienia w postaci SMS i SNMP Trap dla alertów; 19) Aplikacja umożliwia eksport / import profili alertów, raportów i filtrów; 20) Aplikacja pozwala na zaawansowane wyszukiwanie w surowych logach; 21) System pozwala na zapisywanie wyniku wyszukiwania w logach jako profil raportu; 22) Aplikacja pozwala na udostępnienie raportów innym użytkownikom; 23) Aplikacja umożliwia zaplanowanie cyklicznych importów logów z zasobów lokalnych i zdalnych (FTP / SFTP / Cloud); 24) System pozwala na zbieranie logów podczas przestoju modułu gromadzącego logi; 25) System umożliwia na monitorowanie użytkowników uzyskujących dostęp do aplikacji EventLog Analyzer; 26) Aplikacja pozwala na monitorowanie integralności plików; 27) System posiada wbudowane raporty charakterystyczne dla serwera; 28) System umożliwia monitorowanie wielu lokalizacji; 29) System posiada skalowalną architekturę; 30) Aplikacja pozwala na wyodrębnianie pola logu przy użyciu interaktywnego konstruktora składni wyrażeń regularnych (regex); 31) System stosuje Uniwersalne analizowanie i indeksowanie logów (ULPI) do obsługi dowolnego formatu logów (czytelnego dla człowieka i nieszyfrowanego formatu logów); 32) Aplikacja pozwala na import użytkowników z grup Active Directory; 33) System posiada Agenta do zbierania logów w sieci WAN / Firewall; 34) Aplikacja zezwala na import zapisanych plików Syslog; 35) System umożliwia Rebranding klienta Webowego; 36) Aplikacja potrafi natychmiast dostarczyć wybrane raporty;		

	37) System pozwala na analizę specyficznych logów aplikacji: – Serwer sieci Web MS IIS – Serwery FTP MS IIS – Serwer Windows DHCP – Serwer DHCP Linux – Baza danych MS SQL – Baza danych Oracle – Serwer WWW Apache – Serwer druku 38) Aplikacja wspiera MS SQL Server i MS SQL Cluster jako bazy danych zaplecza; 39) System pozwala na modyfikację gotowych widoków i widoków dedykowanych dla użytkowników; 40) System posiada rozbudowane uwierzytelnianie użytkowników zewnętrznych przez Active Directory i RADIUS Server; 41) System pozwala na analizę logów IBM AS / 400 (seria V5R) ich filtrowanie, raportowanie, alertowanie, archiwizowanie i import; 42) Aplikacja stosuje reguły korelacji zdarzeń w czasie rzeczywistym; 43) Aplikacja pozwala na monitorowanie logów serwera terminali Windows; 44) Aplikacja pozwala na monitorowanie sesji użytkownika; 45) Aplikacja pozwala eksportować i importować reguły korelacji; 46) Aplikacja posiada raporty dotyczące urządzeń Stormshield, takie jak logowanie, zarządzanie regułami zapory, zdarzenia systemowe, ważność i inne; 47) Aplikacja posiada wstępnie zbudowaną regułę korelacji do wykrywania ataku Ransomware Ragnar Locker; 48) Aplikacja posiada pulpit aktywności VPN, pozwalający na wgląd w trendy użytkowania VPN i aktywność użytkowników VPN; 49) Aplikacja posiada raporty aktywności sesji na urządzeniach Palo Alto Networks i WatchGuard; 50) Aplikacja pozwala tworzyć niestandardowe role uprawnień użytkownika; 51) Aplikacja pozwala tworzyć filtry zbierania dzienników z wieloma kryteriami pól i operatorami logicznymi, aby zbierać lub wykluczać dzienniki z wybranych urządzeń; 52) Aplikacja umożliwia uzyskanie kontekstowych danych o zagrożeniach dla określonych		

	adresów IP lub adresów URL z wyników wyszukiwania; 53) Aplikacja zapewnia raporty i profile alertów oparte na strukturze MITRE ATT&CK; 54) Aplikacja pozwala zarządzać incydentami bezpieczeństwa – badać je i śledzić, tworzyć incydenty i przypisywać techników do ich zbadania, kontrolować stan, wagę i postęp w analizie; 55) Aplikacja umożliwia automatyzację tworzenia incydentów za pomocą reguł, aby automatycznie je tworzyć, gdy określone alerty zostaną wyzwolone w zadanym przedziale czasowym; 56) Aplikacja daje możliwość mapowania wyzwolonych alertów, raportów i rejestrowania wyników wyszukiwania jako incydenty i przypisywania technika do ich zbadania; 57) Aplikacja posiada raporty dla Firepower; 58) Aplikacja pozwala przywrócić strefę czasową za pomocą automatycznego wykrywania lub użycia czasu serwera; 59) Aplikacja posiada zakładkę ATA Whois info, która zapewnia informacje na temat źródeł adresów URL i domen; 60) Aplikacja obsługuje zbieranie dzienników historycznych dla systemu AS/400 oraz dostosowane zbieranie dzienników historycznych dla systemu Windows; 61) Aplikacja posiada pulpit nawigacyjny Apache, który zapewnia wgląd w czasie rzeczywistym w działanie serwera WWW Apache; 62) Aplikacja obsługuje dzienniki z urządzeń Dell i Forcepoint; 63) Aplikacja obsługuje dzienniki z Qualys - Vulnerability Management.		
2	**Szczegółowy spis funkcjonalności:** 1) Zarządzanie logami z wspieranych źródeł: a) Źródła logów obsługiwane “Out of the Box”: – Podstawowa infrastruktura systemów Windows: Windows Server 2008 i nowsze, Windows 7 i nowsze, Microsoft Windows DHCP Server; – Platformy baz danych: Serwery Microsoft SQL, Bazy danych Oracle, MySQL, DB2, Firebird; – Rozwiązania Endpoint Security: Microsoft Antimalware, Norton Antivirus, F-secure EPP & EDR; – Zapory ogniowe: MGFWs, IDS, IPS – Fortinet, Juniper, Juniper NetScreen, Palo Alto, pfSense, SonicWall, Sophos;		

	– Środowiska virtualizacji: Microsoft Hyper-V, Vmware; – Urządzeń opartych o systemy Linux i Unix: openSUSE, Debian, macOS, IBM AIX, HP UX; – Urządzeń typu Router i Switch: Cisco, Hewlett-Packard; – Skanerów podatności: Nessus, Nmap, Nexpose, OpenVas, Qualys; – Serwerów webowych: Apache, Microsoft IIS; – Pozostałe źródła logów obsługiwane „Out of the box”: Threat Analytics, CEF Format, SAP ERP audit logs, SNMP Trap, Terminal Server, Printer. b) Aplikacja pozwala na zarządzanie dziennikiem zdarzeń; c) Aplikacja pozwala na zarządzanie Syslogami; d) Aplikacja tworzy uniwersalny zbiór logów; e) Aplikacja pozwala na zbieranie logów bez agenta; f) Aplikacja pozwala na zbieranie logów w oparciu o agenta; g) Aplikacja przeprowadza analizę logów; h) Aplikacja posiada predefiniowane raporty logów zdarzeń; i) Aplikacja pozwala na niestandardową analizę logów; j) Aplikacja pozwala na archiwizację logów bezpośrednio z graficznego interfejsu użytkownika; k) Aplikacja pozwala na przeszukiwanie logów bezpośrednio z graficznego interfejsu użytkownika; l) Aplikacja pozwala na dostosowanie pulpitu nawigacyjnego i widoków dla użytkownika; m) Aplikacja pozwala na zarządzanie logami aplikacji; n) Aplikacja pozwala na monitorowanie sesji użytkownika; o) Aplikacja umożliwia alertowanie w czasie rzeczywistym; p) Aplikacja pozwala nam wybrać metody powiadamiania o alertach; q) Aplikacja pozwala na zmianę nazwy klienta internetowego; r) Aplikacja pozwala na monitorowanie użytkowników uprzywilejowanych; s) Aplikacja pozwala na utworzenie własnych indywidualnych raportów; t) Aplikacja potrafi stworzyć trendy dla wydarzeń historycznych; u) Aplikacja pozwala na importowanie logów zdarzeń. 2) Audyt aplikacji: a) Aplikacja pozwala na monitorowanie logów aplikacji: – Aplikacja pozwala na audyt serwera Microsoft IIS;		

	– Aplikacja posiada predefiniowany analizator logów serwera sieci Web Microsoft IIS; – Aplikacja pozwala predefiniowany analizator logów serwera FTP Microsoft IIS; – Aplikacja pozwala na audyt Microsoft SQL Server; – Aplikacja pozwala na monitorowanie logów Microsoft SQL Server; – Aplikacja pozwala na monitorowanie logów serwera WWW Apache; – Aplikacja pozwala na monitorowanie logów serwera wydruku; – Aplikacja pozwala na monitorowanie logów serwera DHCP (Windows / Linux); – Aplikacja pozwala na audyt bazy danych; – Aplikacja pozwala na monitorowanie logów bazy danych Oracle. b) Aplikacja pozwala na monitorowanie serwera terminali Windows; c) Aplikacja pozwala na zabezpieczanie krytycznych aplikacji biznesowych; d) Aplikacja pozwala na zarządzanie logami krytycznych aplikacji Windows; e) Aplikacja pozwala na wykrywanie ataków na serwer WWW; f) Aplikacja posiada analizator wykrywający ataki SQL injection; g) Aplikacja pozwala na wykrycie i łagodzenie skutków ataków DoS; h) Aplikacja zawiera raporty dla aplikacji Sysmon. 3) Audyt urządzeń sieciowych: a) Aplikacja pozwala na audyt urządzeń sieciowych; b) Aplikacja pozwala na kontrolowanie logów routera; c) Aplikacja potrafi analizować logi Cisco; d) Aplikacja pozwala na monitorowanie aktywności użytkownika w routerze; e) Aplikacja pozwala na monitorowanie ruchu routera; f) Aplikacja pozwala na kontrolę logów zapory; g) Aplikacja pozwala na monitorowanie logów IDS / IPS; h) Aplikacja pozwala na monitorowanie logów switch`y; i) Aplikacja pozwala na monitorowanie logów VPN; j) Aplikacja pozwala na audyt zapory systemu Windows; k) Aplikacja pozwala na audyt logów urządzeń Fortinet / FortiGate. 4) Raporty zgodności IT: a) Aplikacja posiada raport zgodności z: PCI-DSS, SOX, ISO 27001, RODO, HIPAA, FISMA, GLBA, GPG, ISLP, FERPA, NIST, PDPA; b) Aplikacja posiada raporty dotyczące nowej zgodności; c) Aplikacja pozwala na dostosowywanie raportów zgodności;		

	d) Aplikacja pozwala na dodanie własnych raportów zgodności. 5) Funkcjonalności SIEM: a) Aplikacja pozwala agregować i analizować informacje o bezpieczeństwie oraz umożliwia zarządzanie zdarzeniami (SIEM); b) Aplikacja pozwala na monitorowanie Syslog; c) Aplikacja pozwala na monitorowanie logów zdarzeń; d) Aplikacja pozwala na monitorowanie integralności plików Windows; e) Aplikacja pozwala na monitorowanie integralności plików systemu Linux; f) Aplikacja pozwala na korelację zdarzeń z logów w czasie rzeczywistym; g) Aplikacja pozwala budować własne korelacje w oparciu o dowolne zdarzenie odnotowane w monitorowanym środowisku; h) Aplikacja pozwala na zarządzanie logami bezpieczeństwa; i) Aplikacja pozwala na inteligentne wykrywanie zagrożeń na podstawie zebranych logów; j) Aplikacja pomaga w zabezpieczaniu urządzeń na podstawie syslogów; k) Aplikacja działa zgodnie z STIX / TAXII; l) Aplikacja umożliwia zarządzanie incydentami; m) Aplikacja pozwala na zarządzanie przepływem pracy związanej z incydentami; n) Aplikacja pozwala na importowanie plików logów; o) Aplikacja pozwala na audyt użytkowników uprzywilejowanych; p) Aplikacja pozwala na wykrywanie zagrożeń systemu Windows; q) Aplikacja pozwala na ograniczanie zagrożeń zewnętrznych; r) Aplikacja pozwala na zarządzanie dziennikiem aplikacji; s) Aplikacja pozwala na zapisywanie wyniku wyszukiwania jako alerty; t) Aplikacja posiada raporty o zagrożeniach Malwarebytes; u) Inteligentne wykrywanie zagrożeń FireEye; v) Aplikacja pozwala na dodawanie indywidualnych raportów; w) Aplikacja pozwala nam utworzyć dedykowane widoki i nimi zarządzać: – Dodawać do widoków wybrane raporty w postaci widżetów; – Usuwać wybrane widżety; – Zmieniać kolejność wyświetlania widoków; – Zmieniać kolejność wyświetlania widżetów. 6) Audyt międzyplatformowy: a) Aplikacja pozwala na monitorowanie krytycznych metryk serwerów;		

	b) Aplikacja pozwala na audyt logów zdarzeń; c) Aplikacja pozwala na zarządzanie logami serwera VMWare; d) Aplikacja pozwala na kontrolę urządzeń z systemem Windows; e) Aplikacja pozwala na audyt logów urządzeń w oparciu o Syslog; f) Aplikacja pozwala na kontrolę i raportowanie w systemów Linux; g) Aplikacja pozwala na kontrolę i raportowanie w systemów Unix; h) Aplikacja pozwala na kontrolę rejestru systemu Windows; i) Aplikacja pozwala na audyt urządzeń typu Switch oraz Router; j) Aplikacja pozwala na monitorowanie logów infrastruktury w chmurze; k) Aplikacja pozwala na wykrywanie kradzieży danych na podstawie zebranych logów; l) Aplikacja pozwala na monitorowanie instancji AWS; m) Aplikacja pozwala wygenerować raport konfiguracji usługi IIS, umożliwiający przeglądanie zmian, takich jak rejestrowanie zmian, zmiany modułów, zmiany protokołu SSL i inne.		
OFEROWANE OPROGRAMOWANIE: Nazwa oferowanego oprogramowania, nr wersji, kod producenta			