Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1	**Podstawowe funkcje**
1.1	Proponowane rozwiązanie w zakresie monitorowania powinno być w stanie natychmiast wykryć nieprawidłowości w sieci, analizując dane z milionów plików i zdarzeń.
1.2	Powinno wykonywać proaktywną analizę logów i korelację zdarzeń w czasie rzeczywistym w całej infrastrukturze, aby szybko zidentyfikować ataki i wykryć naruszenia zasad.
1.3	Powinno być w stanie skorelować miliony zdarzeń z sieci, systemów, aplikacji, maszyn wirtualnych i infrastruktury pamięci masowej przy użyciu funkcji korelacji w czasie rzeczywistym.
1.4	Powinno przechowywać terabajty danych, logów bez konieczności zakupu dodatkowej pamięci masowej przy użyciu wysokowydajnego modelu danych o wysokiej kompresji, który powinien kompresować dane w stosunku co najmniej 60:1
1.5	Powinno monitorować zarówno urządzenia, jak i systemy. Na przykład, monitorowanie kontrolerów domen Windows pod kątem prób włamania, monitorowanie firewalli pod kątem skanowania portów, monitorowanie oprogramowania antywirusowego pod kątem nieoczyszczonych wirusów, monitorowanie serwerów proxy pod kątem podejrzanego dostępu do adresów URL, monitorowanie bazy danych SQL pod kątem zmian w tabelach itp.
1.6	Proponowane rozwiązanie powinno umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami systemu.
1.7	Powinno pomóc w tworzeniu raportów bezpieczeństwa poprzez monitorowanie naruszeń bezpieczeństwa.
2	**Zgodność**
2.1	Proponowane rozwiązanie do monitorowania powinno zapewniać zgodność z PCI, HIPAA, NCUA, GLBA, NERC-CIP, FISMA, SOX lub niestandardowymi zasadami korporacyjnymi.
3	**Alarmowanie i aktywne reagowanie**
3.1	Proponowane rozwiązanie monitorujące powinno być w stanie wykrywać zagrożenia dzięki aktywnemu reagowaniu na informacje pochodzące z urządzeń i systemów.
3.2	Powinno mieć wiele wbudowanych reguł do natychmiastowego użycia i dostosowania do indywidualnych potrzeb.
3.3	Powinno automatycznie i interaktywnie podejmować działania w celu ochrony infrastruktury poprzez kwarantannę, blokowanie, routing i kontrolowanie usług, procesów, kont i uprawnień.
4	**Graficzny interfejs użytkownika**
4.1	Proponowane rozwiązanie do zarządzania powinno zapewniać wysokiej jakości graficzny interfejs użytkownika dostępny za pośrednictwem standardowych przeglądarek.
4.2	Powinno posiadać konsolę do monitorowania zdarzeń w czasie rzeczywistym.
4.3	Graficzny interfejs użytkownika.
4.4	Powinno posiadać opcje "przeciągnij i upuść" do tworzenia filtrów i reguł.
4.5	Powinno ułatwić wyszukiwanie reguł, najlepiej przy użyciu tagów lub kategorii.
4.6	Powinno mieć możliwość wyświetlania zarówno oryginalnych, jak i znormalizowanych logów w tym samym interfejsie wyszukiwania.
4.7	Powinno mieć widoki „Top 10” dla różnych występujących problemów.

4.8	Konsola do zarządzania powinna być dostępna lokalnie lub zdalnie.
4.9	Konsola do zarządzania powinna zezwalać wielu użytkownikom na logowanie się w tym samym czasie.
4.10	Proponowane rozwiązanie powinno integrować się z Active Directory w celu logowania użytkownika.
4.11	Powinien szybko wskazać nieprawidłowości w sieci.
4.12	Proponowane rozwiązanie powinno być łatwe w użyciu i intuicyjne dzięki funkcjom typu „drill-down”.
5	**Raportowanie**
5.1	Proponowane rozwiązanie w zakresie monitorowania powinno być w stanie szybko wygenerować raporty dotyczące zgodności.
5.2	Powinno mieć wiele wbudowanych raportów (około 300 lub więcej) i gotowych pakietów zgodności z normami, które pomogłyby w celach audytowych.
5.3	Proponowane rozwiązanie powinno umożliwiać dostosowywanie raportów przez dodawanie / usuwanie kolumn, ustawianie filtrów, określanie ram czasowych itp.
5.4	Powinno mieć raporty, które pokazują informacje dotyczące wykorzystania bazy danych.
6	**Wsparcie dla wielu producentów**
6.1	Proponowane rozwiązanie monitorujące nie powinno być specyficzne dla producenta.
6.2	Proponowane rozwiązanie powinno umożliwiać tworzenie nowych alarmów od zera a także definiowanie wartości progowych.
7	**Wdrożenie**
7.1	Powinno umożliwiać szybkie wdrożenie, tak jak w przypadku urządzenia wirtualnego, na popularnych hiperwizorach, takich jak VMware lub Hyper-V.
8	**Dodatkowe komponenty**
8.1	Proponowane rozwiązanie w zakresie monitorowania powinno chronić wrażliwe dane poprzez wykrywanie w czasie rzeczywistym i blokowanie dysków USB.
9	**Integracja**
9.1	Proponowane rozwiązanie monitorujące powinno współdzielić i korelować logi i zdarzenia z rozwiązań do monitorowania sieci, rozwiązań do monitorowania aplikacji i rozwiązań do monitorowania wirtualizacji poprzez integrację współdzielenia danych.
9.2	Powinno być w stanie przyjmować trapy z monitoringu sieci, monitoringu aplikacji i innych rozwiązań do monitoringu.
10	**Skalowanie**
10.1	Proponowane rozwiązanie w zakresie monitorowania powinno zapewniać możliwość długoterminowego przechowywania i wyszukiwania oryginalnych logów.
10.2	Proponowane rozwiązanie powinno obsługiwać opcje wielu wdrożeń - scentralizowane, rozproszone i hybrydowe wdrożenia, z opcją scentralizowanego widoku w jednej konsoli.
11	**Częstotliwość aktualizacji**
11.1	Wydawane aktualizacje produktu, min. dwa razy w roku lub częściej.
12	**Wsparcie produktu**
12.1	Powinien zapewniać wsparcie 24x7x365 przez okres 3 lat.
12.2	Aktywne wsparcie za pośrednictwem forów i społeczności byłoby mile widziane.
13	**Licencjonowanie**
13.1	Liczba nodów objętych licencją 250