# **Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach infrastruktury zabezpieczeń.

# Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Amazon AWS, Citrix XenServer, Google Cloud Platform, Linux KVM, Microsoft Azure, Microsoft Hyper-V Server, Nutanix AHV, OpenSource XenServer, Oracle Private Cloud.

# **Wirtualne zasoby sprzętowe:**

1. System musi obsługiwać co najmniej: 4 interfejsy sieciowe, 4 wirtualne procesory oraz 16 GB pamięci RAM.

# **Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 10 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z systemów bezpieczeństwa NGFW (Next Generation Firewall), które wykorzystuje zamawiający.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

# **Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia.
4. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków

b. Listę najbardziej aktywnych użytkowników/źródeł ruchu

c. Listę najczęściej wykorzystywanych aplikacji

d. Listę najczęściej odwiedzanych stron www

e. Listę krajów, do których nawiązywane są połączenia

f. Listę najczęściej wykorzystywanych polityk Firewall

g. Informacje o realizowanych połączeniach IPSec i SSL VPN

h. Listę najczęściej występujących zdarzeń systemowych

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514.
3. System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów.
4. System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.

# **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.
6. Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW a także z wybranej adresacji IP.
7. Możliwość automatycznego usuwania raportów po określonym czasie.

# **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Możliwość tworzenia własnych reguł korelowania logów.
3. Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia.
4. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

* Malware/AV
* Aplikacje sieciowe
* Email
* IPS
* Web Filter
* Traffic (logi z ruchu sieciowego)
* Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN)

1. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji.

# **Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI.
3. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania.
4. System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów.

# **Gwarancja oraz wsparcie**

System musi być objęty serwisem gwarancyjnym producenta przez 12 miesięcy. W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.