

System Zarządzania Zdarzeniami i Informacjami Bezpieczeństwa (SIEM)

Przedmiotem zamówienia jest dostawa licencji, wdrożenie, serwis i utrzymanie rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (ang. SIEM - Security Information and Event Management), zwanego dalej SIEM, wykorzystującego produkt Splunk Enterprise.

- 1 Licencja na oprogramowanie Splunk Enterprise obejmująca swoim zakresem wyłącznie „Core” środowiska powinna umożliwiać obsługę wolumenu rejestrowanych zdarzeń w wielkości co najmniej 30 GB na dzień przez okres 12 miesięcy od momentu jej instalacji.
- 2 Usługa wdrożenia systemu powinna obejmować w swoim zakresie:
 - 2.1 Instalację systemu w środowisku wirtualnym Vmware vCenter przygotowanym przez zamawiającego;
 - 2.2 Konfigurację systemu w zakresie dwóch źródeł danych tj. Checkpoint oraz Microsoft Active Directory;
 - 2.3 Analizę przedwdrożeniową środowiska;
 - 2.4 Przygotowanie projektu wdrożenia;
 - 2.5 Właściwe prace wdrożeniowe;
 - 2.6 Przygotowanie dokumentacji powdrożeniowej;
 - 2.7 Przeszkolenie administratorów i operatorów systemu z wdrożonego systemu.
 - 2.8 Gwarancję prawidłowo działającego produktu oraz usunięcie ewentualnych usterek wynikających z nieprawidłowej instalacji.