

Specyfikacja techniczna przedmiotu zamówienia

Nazwa zadania: **Kompleksowe szkolenie z obsługi Menagera logów , dobrych praktyk i obsługi dla informatyków Starostwa Powiatowego w Chodzieży. W07 i W34**

Kwalifikacje szkolących muszą być **równoważne lub lepsze** niż podane w specyfikacji.

Lp	Parametry techniczne.
1. Kompleksowe szkolenie z obsługi Menagera logów , dobrych praktyk i obsługi dla informatyków Starostwa Powiatowego w Chodzieży. W07 i W34	Typ Szkolenia: Zdalne Liczba szkolonych pracowników: 3 Zakres szkolenia: • Wdrożenie systemu z zadania: „Zakup Menagera logów, czyli oprogramowanie umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z niegraniczonej liczby źródeł. W08” • Przedstawiane dobrych praktyk Menagera logów • Możliwość przeprowadzenia szkolenia z obsługi na systemie wdrożonym • Możliwość zadawania pytań podczas szkolenia • Możliwość rozwiązywania scenariuszy/problemów zaproponowanych przez szkolących Poruszone zagadnienia: 1. Wprowadzenie do zarządzania zdarzeniami bezpieczeństwa – czym jest, po co się stosuje, kto jest odbiorcą. 2. Przykłady zastosowania systemów zarządzania logami i bezpieczeństwem. 3. Architektura systemów do zarządzania logami oraz przepływ logów w systemie. 4. Pierwsze kroki konfiguracyjne – szybki start. 5. Procesy aktualizacji i przywracania wcześniejszych wersji systemu. 6. Zaawansowane opcje konfiguracji subsystemu sieciowego. 7. Zarządzanie użytkownikami i uprawnieniami. 8. Klasyfikacja danych – szablony klasyfikacji, listy prefiksów IP (część praktyczna). 9. Tagowanie logów – metody oznaczania logów dla późniejszej analizy i wizualizacji. 10. Reguły parsowania – omówienie działania i tworzenie prostych reguł parsowania przez użytkownika (z demonstracją). 11. Rejestrowanie danych z systemów, które nie mogą bezpośrednio przesyłać logów (np. aplikacje bazodanowe, środowiska wirtualizacyjne, rozwiązania chmurowe). 12. Logowanie zdarzeń z systemów Windows oraz aplikacji działających na Windows, filtrowanie logów. 13. Działanie i konfiguracja komponentów pośredniczących w przesyłaniu logów. 14. Tworzenie pulpitów (dashboardów), pozyskiwanie danych, generowanie raportów (część praktyczna). 15. Alerty – zasada działania, konfiguracja, testowanie oraz dobre praktyki tworzenia reguł alarmowych. 16. Szablony powiadomień o alertach. 17. Podsumowanie materiału szkoleniowego



	Kwalifikacje szkółących: Certyfikowany ekspert producenta, rozwiązania dostarczonego w ramach zadania: „Zakup Menagera logów, czyli oprogramowanie umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z niegraniczonej liczby źródeł. W08” Ważny certyfikat producenta - oprogramowania dostarczonego w ramach zadania: „Zakup Menagera logów, czyli oprogramowanie umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z niegraniczonej liczby źródeł. W08” Wymóg przedłożenia ważnego certyfikatu eksperta. Język szkolenia: polski
--	---

Sporządził: Mateusz Wieczorek