Załącznik nr 1 C

OPIS PRZEDMIOTU ZAMOWIENIA

<u>Oprogramowanie równoważne do Microsoft Defender for Endpoint for Servers P2</u>

1. Integracja z platformą Microsoft 365:
    - Pełna integracja z platformą Microsoft 365, środowiskiem Azure AD
    - Synchronizacja z platformą Microsoft 365 w celu ułatwienia zarządzania zabezpieczeniami serwerów.
    - Wspólna polityka zabezpieczeń obejmująca serwery, urządzenia i aplikacje w ramach platformy Microsoft 365.
    - Wspólne środowisko zarządzania w ramach jednej platformy
2. Zaawansowane wykrywanie zagrożeń:
    - Wykorzystywanie silników heurystycznych, uczenia maszynowego i sztucznej inteligencji do identyfikacji zaawansowanych zagrożeń na serwerach.
    - Wykrywanie i blokowanie złośliwego oprogramowania, exploitów i innych szkodliwych aktywności na poziomie serwerów.
    - Monitorowanie zachowania serwerów w celu wykrycia podejrzanych aktywności i działań.
3. Zabezpieczenie przed atakami typu ransomware:
    - Wykrywanie i blokowanie prób ataków typu ransomware, które mogą zaszyfrować dane na serwerach.
    - Ochrona przed infekcją ransomware poprzez monitorowanie aktywności plików i aplikacji.
4. Ochrona przed wykorzystaniem podatności:
    - Wykrywanie i blokowanie prób wykorzystania podatności w systemach operacyjnych i aplikacjach serwerowych.
    - Automatyczne aktualizacje i łatki, zapewniające najnowsze zabezpieczenia przed znanymi podatnościami.
5. Analiza zachowania serwerów:
    - Monitorowanie i analiza zachowań serwerów w celu identyfikacji nieautoryzowanych lub podejrzanych działań.
    - Automatyczna analiza zagrożeń, wykrywanie prób naruszenia zabezpieczeń serwerów oraz podejrzanych działań w czasie rzeczywistym.
6. Badanie i reagowanie na incydenty:
    - Rejestracja i analiza zdarzeń związanych z bezpieczeństwem serwerów w celu identyfikacji incydentów.

- Reagowanie na incydenty w czasie rzeczywistym poprzez wdrażanie odpowiednich środków zaradczych.

7. Zarządzanie zabezpieczeniami serwerów:
   - Centralne zarządzanie zabezpieczeniami serwerów w organizacji.
   - Automatyczne aktualizacje definicji wirusów i sygnatur w celu zapewnienia ochrony przed najnowszymi zagrożeniami.
   - Raportowanie i analiza zdarzeń związanych z bezpieczeństwem serwerów.