Załącznik nr 9 - CYBERBEZPIECZEŃSTWO

1. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu antywirusowym i przy włączonej zaporze Windows wykorzystywanej przez Zamawiającego, a także przy włączonych mechanizmach bezpieczeństwa wbudowanych w system operacyjny serwera. Niedopuszczalne jest wyłączanie jakiejkolwiek z powyższych funkcji.

2. Oprogramowanie musi dopuszczać tylko niezbędny ruch do prawidłowego funkcjonowania oprogramowania (hardening)

3. Oprogramowanie musi realizować wszystkie swoje funkcje przy włączonym oprogramowaniu realizującym wykrywanie i reagowanie na incydenty cyberbezpieczeństwa w punktach końcowych (EDR)

4. Wykonawca dostarczy pełną dokumentację w zakresie adresów i portów sieciowych, z którymi komunikowało się będzie Oprogramowanie albo będą niezbędne do jego poprawnej pracy.

5. Wykonawca dostarczy pełną specyfikację komunikacji z systemami zewnętrznymi, tj. minimum adresy z którymi ma nastąpić połącznie, nazwy protokołu / numer portu, zakres przesyłanych danych.

6. W przypadku stwierdzenia podatności, zagrożenia bezpieczeństwa cybernetycznego czy incydentu dotyczącego oprogramowania, do którego Wykonawca posiada prawa autorskie, Wykonawca niezwłocznie usunie stwierdzone zdarzenie na własny koszt, zabezpieczając na czas usuwania usterki analogiczne oprogramowanie pozbawione tej podatności. Jeżeli Wykonawca wykorzystuje oprogramowanie firm trzecich jako komponent czy narzędzie systemów własnych, to odpowiedzialność z tytułu podatności na zagrożenia cybernetyczne dotyczy również i tego oprogramowania.

7. Oprogramowanie nie może wykorzystywać oprogramowania firm trzecich wobec produktów których stwierdzono występowanie podatności lub wydany został komunikat bezpieczeństwa cybernetycznego o zagrożeniu. W takim przypadku Wykonawca niezwłocznie dokona usunięcia stwierdzonej podatności oprogramowania, ewentualnie zastosuje rozwiązanie zastępcze nieposiadające podatności.

8. Wykonawca wyraża zgodę na instalację na serwerze oprogramowania (typu Agent) posiadanego przez zamawiającego systemu do monitorowania podatności o nazwie Endpoint Central firmy ManageEngine

9. Oprogramowanie monitoruje zdarzenia i zapisuje je w dzienniku zdarzeń (logu).