Gmina Stary Dzików
ul. Kościuszki 79
37-632 Stary Dzików

Stary Dzików, 10.01.2025 r.

IGI.271.1.2025

Oferenci

Dot. „Dostawa i wdrożenie serwera i oprogramowania SIEM/SOAR w ramach realizacji projektu Cyberbezpieczna Gmina Stary Dzików"

Pytanie 1:
Dotyczy pkt. 122 OPZ:
Wnioskujemy o modyfikację zapisów.
Proponowany zapis:
Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang. open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/scenariusze reakcji (SOAR), chyba że producent rozwiązania dostarcza je jako jednolity plik instalacyjny, a całość systemu jest w pełni objęta wsparciem technicznym producenta, obejmującym również elementy bazujące na kodzie open source. Zamawiający nie zaakceptuje systemów, które wymagają dodatkowej instalacji, modyfikacji lub konfiguracji komponentów open source przez dostawcę oraz użytkownika końcowego.

Uzasadnienie: Współczesne technologie informatyczne często opierają się na komponentach open-source, które są szeroko uznawane za stabilne, bezpieczne i zgodne z najlepszymi praktykami rynkowymi. Wykluczenie takich rozwiązań ogranicza drastycznie konkurencję oraz dostęp do bardziej innowacyjnych i efektywnych kosztowo systemów. Należy również podkreślić, że istotna większość producentów rozwiązań z branży cyberbezpieczeństwa, w tym liderów rankingów Gartner i Forrester w kwa-drancie SIEM, w różnym stopniu wykorzystuje modyfikowane oprogramowanie otwarte w swoich produktach, wykorzystując m.in. wymienione przez Zamawiającego technologie, AlienVault, OTX, OSSIM, Snort oraz Elasticsearch.

Odpowiedź na pytanie 1:
Po wnikliwej analizie Państwa argumentacji, Zamawiający podtrzymuje swoje stanowisko i nie wyraża zgody na modyfikację wymagań, tym samym oczekujemy ofert zgodnych z pierwotnymi wymaganiami.

Nasza decyzja podyktowana jest następującymi względami:

Zamawiający przywiązuje najwyższą wagę do bezpieczeństwa danych i infrastruktury. Całkowite wykluczenie oprogramowania open source w kluczowych obszarach funkcjonalnych (składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/scenariusze reakcji (SOAR)) ma na celu zminimalizowanie potencjalnych ryzyk związanych z lukami w oprogramowaniu, brakiem pełnej kontroli nad kodem źródłowym oraz ewentualnymi problemami z aktualizacjami i wsparciem. Rozumiemy, że wielu producentów korzysta z komponentów open source, jednak w naszym przypadku priorytetem jest maksymalne ograniczenie ryzyka. Zamawiający oczekuje jednoznacznej odpowiedzialności ze strony dostawcy za całe dostarczone rozwiązanie. W przypadku wykorzystania komponentów open source, odpowiedzialność ta staje się bardziej rozproszona, co jest dla nas nieakceptowalne. Chcemy mieć pewność, że w przypadku jakichkolwiek problemów, mamy jednego, jasno określonego partnera, który w pełni odpowiada za działanie i bezpieczeństwo systemu. Zamawiający patrzy na wdrożenie systemu w perspektywie długoterminowej. Chcemy uniknąć sytuacji, w której w przyszłości mogłyby pojawić się problemy związane z kompatybilnością, licencjami lub brakiem wsparcia dla wykorzystywanych komponentów open source. Wybór rozwiązania opartego wyłącznie na oprogramowaniu komercyjnym zapewnia nam większą stabilność i przewidywalność w dłuższej perspektywie. Specyfika niniejszego projektu i związane z nim wymogi bezpieczeństwa uzasadniają tak restrykcyjne podejście. Zamawiający dokonał analizy ryzyk i uznał, że w tym konkretnym przypadku, korzyści płynące z całkowitego wykluczenia open source przeważają nad potencjalnymi korzyściami z jego wykorzystania.

Wójt Gminy Stary Dzików
Tomasz Jabłoński