

Gliwice, 01.09.2022 r.

DO/DZ-TPbn-381-2-47/22

**DO WSZYSTKICH  
ZAINTERESOWANYCH**

**dot. postępowania prowadzonego w trybie podstawowym bez negocjacji ogłoszonym w Biuletynie Zamówień Publicznych w dniu 24.08.2022r. pod nr 2022/BZP 00318686/01, którego przedmiotem zamówienia jest 1. Rozbudowa posiadanego systemu Fortigate o funkcjonalność WAF, 2. Zakup oraz wdrożenie skanera podatności dla Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie – Państwowego Instytutu Badawczego Oddziału w Gliwicach**

**WYJAŚNIENIE TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA**

Na podstawie art. 284 ust. 2 ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t. j. Dz. U. z 2022 r., poz. 1710), Zamawiający przekazuje treść złożonych pytań i udzielonych odpowiedzi:

**Pytanie 1**

**pytania dotyczące części 2 – skaner podatności  
Odnosząc się do dokumentu z załącznika**

2. Czy zamawiający uzna za spełnione, jeżeli narzędzie zapewnia w raporcie wszystkie niezbędne informacje niezbędne do stworzenia raportu PCI DSS, jednak moduł filtrowania raportu nie będzie posiadał gotowego szablonu dla PCI DSS?

**Odpowiedź:**

*Tak, Zamawiający dopuszcza rozwiązanie zaproponowane przez Wykonawcę.*

**Pytanie 2**

**pytania dotyczące części 2 – skaner podatności  
Odnosząc się do dokumentu z załącznika**

12. Czy zamawiający uzna za spełnienie, jeżeli zamiast formatu .docx skaner będzie miał możliwość generowania raportów w formatach dodatkowo niewymienionych w wymaganiach: ARF, CPE, CSV, ITG, LaTeX, NBE, SVG, TXT, VNA?

**Odpowiedź:**

*Tak, Zamawiający dopuszcza rozwiązanie zaproponowane przez Wykonawcę.*

**Pytanie 3**

Zamawiający w §1 pkt 2 (Projekt umowy) zawarł wymóg wdrożenia systemu WAF.

Zwracamy się z prośbą o określenie planowanego zakresu wdrożenia, gdyż informacja ta ma istotny wpływ na możliwość prawidłowego oszacowania kosztów projektu.

W szczególności prosimy o:

1) podanie ilości aplikacji Zamawiającego jakie mają zostać poddane kontroli przez WAF w ramach wdrożenia, (prosimy nie wliczać tych aplikacji, które Zamawiający zrealizuje własnym sumptem po odbyciu szkolenia).

2) potwierdzenie, że następujący zakres wdrożenia obejmujący:

- wdrożenie listy reguł standardowych - weryfikację zgodności protokołu http z RFC
- implementację Ochrony przed atakami sygnaturowymi, z wykluczeniem reguł opisanych jako Reguły rozszerzone
- implementację Ochrony przed atakami SQL Injection Ochrona przed XSS (Cross-Site Scripting)
- implementację Ochrony przed LDAP and Xpath Injection
- implementację Ochrony przed iFrame Injection

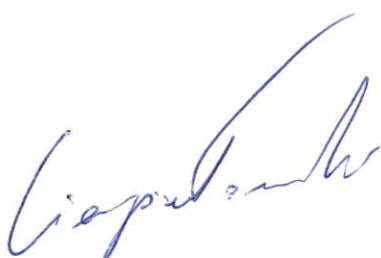
- implementację Ochrony przed znanymi exploitami i trojanami
  - ograniczenie metod http
  - kompresję strony
  - terminowanie ruchu SSL/TLS
- jest zgodny z celami Zamawiającego.

**Odpowiedź:**

Ad. 1) W ramach wdrożenia kontroli poddane zostanie 5 aplikacji Zamawiającego.

Ad. 2) Tak, Zamawiający potwierdza.

Treść udzielonych odpowiedzi stanowi integralną część Specyfikacji Warunków Zamówienia.



Z-CA DYREKTORA  
ds. Finansów i Zarządzania

*mgr Anna Kotula*

KIEKOWIAK  
Działu Zamówień Publicznych  
i Zaopatrzenia

*mgr Urszula Wójcieszek*

załącznik:

- Specyfikacja techniczna zamówienia – zad. 2 (załączona przez Wykonawcę do przesłanych pytań)

*P. Hojda*