SPECYFIKACJA TECHNICZNA ZAMÓWIENIA (STZ)

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

ZADANIE NR 2 - ZAKUP ORAZ WDROŻENIE SKANERA PODATNOŚCI

Minimalne wymagania techniczne skanera podatności:

Wymagania:

1. Prawo do aktualizacji Firmware przez minimum 4 lata
2. System musi mieć możliwość wykrywać podatności przy pomocy dwóch metod:
   skanowania sieciowego - wykrywa porty, sprawdza jakie serwisy działają, można spróbować zalogować się do systemu przy pomocy domyślnych haseł.
   skanowania z uwierzytelnieniem – dostarcza bardziej dokładnych informacji np. wersja systemu, uruchomione usługi, informacja czy hosty nie komunikują się bazą botnetową, zmiany w rejestrach, czy systemy są zgodne z regulacjami np. PCI DSS, zgodność z polityka bezpieczeństwa.
3. System musi mieć możliwość skanowania systemów systemy operacyjne, urządzenia sieciowe, bazy danych, serwery webowe pod kontem zagrożeń i naruszenia zasad zgodności.
4. System musi mieć tak zwaną ocenę ryzyka: ranking oceny podatności w oparciu o np. CVSS
5. System musi pozwalać na zaplanowanie skanowania.
6. System musi mieć predefiniowane polityki i wzorce konfiguracji.
7. System podczas jednego testu musi mieć możliwość przeskanowania jeden klasy C (254 adresy) przy jednym skanowaniu.
8. System musi mieć możliwość przeskanowanie całej sieci Zamawiającego. Jednak nie wymaga jest iż skanowanie odbyło się za jednym zadaniem.
9. System musi mieć dostęp w do stale aktualizowanej bazy zawierającej podatności.
10. System musi mieć możliwość dostępu przez przeglądarkę z dowolnego komputer w sieci Zamawiającego.
11. System musi posiadać możliwość dostosowania raportów wg podatności lub urządzenia.
12. Generowane raporty powinny być w co najmniej w jednym z podanych formatów: PDF, HTML, DOCX, XML,
13. System musi mieć możliwość utworzeniach co najmniej 10 kont dla użytkowników.
14. Wyniki skanowania powinny być wysyłane na maile w formie raportu i dostępne poprzez GUI.
15. System musi mieć możliwość priorytetyzacja: korelacja z danymi z baz exploitów (np.: Metasploit, CoreImpact, Canvas, ExploitHub) i filtrowanie wg prawdopodobieństwa wykorzystania podatności i jej dotkliwości.
16. Raport powinien zawierać informacje o podatności plus zalecenia.
17. System oparty na fizycznych urządzeniach (oferta musi zawierać cenę serwera).
18. Oferta musi zawierać szkolnie oferowanego systemu dla administratorów.