Załącznik nr 3 – opis przedmiotu zamówienia do zapytania nr DZ/DI-072-11/26

Wymogi główne – Usługi Centrum Operacji Bezpieczeństwa (Security Operations Center)

Poniższe wymagania stanowią **wymogi główne** realizacji przedsięwzięcia w ramach Inwestycji D.1.1.2 i podlegają obligatoryjnemu spełnieniu przez Wykonawcę.

Usługi Centrum Operacji Bezpieczeństwa (Security Operations Center – SOC) muszą być realizowane przez profesjonalne podmioty świadczące usługi z zakresu cyberbezpieczeństwa, spełniające wymagania organizacyjne oraz techniczne określone w **Ustawie z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa** oraz aktach wykonawczych do tej ustawy.

1. Usługa Pierwszej Linii Wsparcia (SOC L1)

W ramach Pierwszej Linii Wsparcia Wykonawca zobowiązany jest zapewnić co najmniej:

- całodobowe (24/7) monitorowanie zdarzeń naruszenia cyberbezpieczeństwa, zgodnie z uzgodnionymi parametrami SLA,
- wstępną analizę oraz ocenę zdarzeń bezpieczeństwa,
- realizację zatwierdzonych Scenariuszy Reakcji (playbooków),
- korelację zdarzeń i incydentów cyberbezpieczeństwa,
- dokumentowanie wszystkich wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji,
- eskalowanie zdarzeń i incydentów zgodnie z ustalonymi procedurami,
- zamykanie zdarzeń błędnie zaklasyfikowanych jako zagrożenia (false positive),
- priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa,
- przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa,
- modyfikację oraz dostrajanie (tuning) polityk bezpieczeństwa systemów, aplikacji i rozwiązań Zamawiającego w celu zwiększenia skuteczności wykrywania zagrożeń.

1.1 Zakres monitorowanych zasobów

Monitorowaniem muszą zostać objęte w szczególności kluczowe zasoby Zamawiającego, w tym:

- stacje robocze oraz serwery,
- urządzenia sieciowe, w tym urządzenia brzegowe,

- systemy i aplikacje serwerowe, w tym systemy informacji medycznej (jeżeli są wykorzystywane),
- kontrolery domenowe,

1.2 Zakres monitorowanych zdarzeń

Zakres monitorowanych zdarzeń musi uwzględniać co najmniej:

- powiadomienia o zagrożeniach generowane ze stacji roboczych i serwerów, w szczególności przez narzędzia ochrony,
- zdarzenia dotyczące dezaktywacji lub nieprawidłowego działania narzędzi bezpieczeństwa,
- powiadomienia z modułów ochrony urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych,
- zdarzenia związane z nieudanymi i wielokrotnymi próbami logowania,
- kluczowe zdarzenia dotyczące kont uprzywilejowanych (utworzenie konta, zmiana hasła, usunięcie konta, zmiana przynależności do grup),
- zdarzenia sieciowe i systemowe mogące świadczyć o rekonesansie infrastruktury (np. enumeracja, skanowanie portów i adresacji),
- zdarzenia związane z modyfikacją harmonogramów zadań w systemach operacyjnych,
- zdarzenia dotyczące modyfikacji mechanizmów audytu zdarzeń i dzienników systemowych,
- zdarzenia dotyczące integralności plików, w szczególności zasobów sieciowych,
- zdarzenia związane z logowaniem zdalnym.

2. Usługa Drugiej Linii Wsparcia (SOC L2)

W ramach Drugiej Linii Wsparcia Wykonawca zobowiązany jest zapewnić co najmniej:

- analizę incydentów cyberbezpieczeństwa eskalowanych przez Pierwszą Linię Wsparcia,
- przygotowanie raportów poincydentalnych wraz z zaleceniami naprawczymi i prewencyjnymi,
- realizację Scenariuszy Reakcji zgodnie z wymaganiami Zamawiającego,
- przygotowywanie miesięcznych raportów z realizacji usług SOC,
- dostępność usługi Drugiej Linii Wsparcia w wymiarze 8 godzin dziennie, 5 dni w tygodniu (8/5).

3. Scenariusze Reakcji (Playbooki)

Wykonawca zobowiązany jest do przygotowania, wdrożenia, uzgodnienia oraz bieżącej aktualizacji Scenariuszy Reakcji dla zidentyfikowanych zagrożeń i typów incydentów cyberbezpieczeństwa.

4. Dodatkowe wymogi Zamawiającego

W ramach realizacji przedsięwzięcia Wykonawca zobowiązany jest do spełnienia następujących dodatkowych wymagań:

1. Wraz z usługą SOC musi zostać dostarczony system klasy **Security Information and Event Management (SIEM)** pełniący rolę centralnego kolektora logów.
2. System SIEM musi obsługiwać monitorowanie i przetwarzanie zdarzeń bezpieczeństwa dla **co najmniej 6 000 unikalnych adresów IP**.
3. System musi obsługiwać co najmniej 3500 komputerów i serwerów oraz 2500 innych urządzeń podpiętych do sieci LAN (np. drukarki, punkty dostępowe sieci bezprzewodowej, przełączniki sieciowe itp.),
4. System SIEM musi zostać **zainstalowany i uruchomiony w infrastrukturze Zamawiającego** (on-premise lub w środowisku prywatnym Zamawiającego).
5. System SIEM musi zostać zintegrowany ze źródłami logów Zamawiającego, w szczególności:
   - Active Directory,
   - serwerami Windows i Linux,
   - systemami DNS/DHCP/NTP,
   - systemem NAC,
   - systemami antywirusowymi / EDR,
   - systemem WAF,
   - systemem UTM,
   - systemem PAM,
   - systemem VPN,
   - systemem DLP,
   - systemem pocztowym,
   - systemem do monitorowania środowiska,
   - systemem do monitorowania elementów pasywnych sieci lan,
   - przełącznikami sieciowymi,
   - innymi niewymienionymi systemami, umożliwiającymi wysyłanie logów za pomocą protokołu *syslog*.
6. Wszystkie zdarzenia bezpieczeństwa gromadzone w systemie SIEM muszą być przekazywane do SOC Wykonawcy **za pośrednictwem odpowiednio zabezpieczonego kanału komunikacyjnego**, w szczególności z wykorzystaniem tunelu szyfrowanego typu **IPsec** lub równoważnego rozwiązania spełniającego aktualne standardy bezpieczeństwa.
7. Dane przesyłane do SOC nie mogą naruszać integralności, poufności ani dostępności informacji przetwarzanych w infrastrukturze Zamawiającego.

Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028

8. SIEM musi zostać zainstalowany na dedykowanym fizycznym urządzeniu/serwerze dostarczonym w ramach zamówienia.
9. Usługa SOC ma być świadczona przez co najmniej 36 miesięcy.
10. Wsparcie oraz gwarancja dla systemu SIEM muszą wynosić co najmniej 36 miesięcy.
11. System SIEM musi obsługiwać co najmniej 150 GB danych dziennie, z możliwością dalszej rozbudowy.
12. SOC ma dostarczać raz w miesiącu raport zawierający podsumowanie działań z minionego miesiąca.
13. SOC musi dostarczać ostrzeżenia dotyczące trwających kampanii phishingowych oraz ataków na inne szpitale lub podmioty publiczne, bez podawania źródeł informacji ani nazw jednostek.
14. SOC musi przedstawiać rekomendacje w zakresie cyberbezpieczeństwa.
15. SOC musi spotykać się ze specjalistą ds. cyberbezpieczeństwa Zamawiającego raz na kwartał, w celu omówienia raportów, rekomendacji oraz innych istotnych zagadnień związanych z bezpieczeństwem.
16. W przypadku wystąpienia cyberataku mającego wpływ na infrastrukturę Zamawiającego lub naruszenia zabezpieczeń w sposób bezpośredni lub pośredni, musi zostać zorganizowane minimum dwa spotkania podczas których zostaną omówione następujące kwestie:
    a. Co dokładnie się wydarzyło?
    b. Jaki był wpływ zdarzenia na Zamawiającego?
    c. W jaki sposób doszło do incydentu?
    d. Jak zaradzić zdarzeniu lub zminimalizować ryzyko jego ponownego wystąpienia?
17. Zespół SOC musi mieć możliwość podejmowania działań po godzinach pracy działu IT, w tym blokowania zagrożeń (np. poprzez dodawanie adresów IP lub adresów MAC urządzeń do czarnych list). Każde takie działanie musi zostać niezwłocznie zgłoszone specjaliście ds. cyberbezpieczeństwa i Kierownika Działu IT Zamawiającego.
18. W przypadku wystąpienia incydentu związanego z cyberbezpieczeństwem SOC zobowiązany jest do niezwłocznego podjęcia działań informacyjnych, obejmujących:

a) powiadomienie specjalisty ds. cyberbezpieczeństwa Zamawiającego;
b) powiadomienie administratora systemu teleinformatycznego, którego dotyczy incydent;
c) powiadomienie administratora sieci teleinformatycznej Zamawiającego;
d) w przypadku niedostępności osoby, o której mowa w lit. a, zgłoszenie incydentu do właściwych podmiotów, zgodnie z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w szczególności do CSIRT GOV, CSIRT NASK oraz CSIRT CEZ;
e) jeżeli incydent dotyczy również naruszenia ochrony danych osobowych – powiadomienie Inspektora Ochrony Danych.

Państwowy Instytut Badawczy
Oddział w Gliwicach

ul. Wybrzeże Armii Krajowej 15
44-102 Gliwice

dyrektor@gliwice.nio.gov.pl
www.gliwice.nio.gov.pl

Fax: +48 32 231 35 12

NIP: 5250008057
REGON: 000288366-00028