SAMODZIELNY PUBLICZNY ZESPÓŁ ZAKŁADÓW OPIEKI ZDROWOTNEJ W PRZASNYSZU

ISO 9001 BUREAU VERITAS Certification N°PL10000591/P

06-300 Przasnysz, ul. Sadowa 9, centrala tel. 29 753 43 00, sekretariat 29 753 43 18, fax 29 753 43 80

NIP 761-13-33-881 REGON 000302480 BDO: 000110316

www.szpitalprzasnysz.pl sekretariat@szpitalprzasnysz.pl

SPZZOZ.ZP/7/2024 Przasnysz, 25.01.2024 r.

Do wszystkich,
którzy pobrali zapytanie

Dotyczy: zapytania ofertowego na świadczenie usług w zakresie cyberbezpieczeństwa w rozumieniu art. 14 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa dla SPZZOZ w Przasnyszu

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Przasnyszu prostuje odpowiedź na pytanie nr 1 z dnia 23.01.2024 r.

Pyt. 1
Zapytanie ofertowe, Rozdział III, Umowa, §2
Prosimy o potwierdzenie, że przedmiotem zamówienia jest zobowiązanie Wykonawcy do świadczenia na rzecz Zamawiającego usługi SOC (Security Operations Center).
Jednocześnie prosimy o potwierdzenie, że Zamawiający uzna za spełnione świadczenie usługi SOC jeśli Wykonawca w ramach realizacji przedmiotu zamówienia zapewni poniższe warunki i zakres świadczenia usługi:
System monitoringu infrastruktury IT i usługa SOC:

I. **MINIMALNE WYMAGANIA TECHNICZNE**
   1. **Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.**
   2. **Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.**
   3. **Ograniczania użytkownikom dostępu do wybranych grup hostów.**

II. **Monitorowanie**
   1. **Monitorowania serwerów fizycznych.**
   2. **Monitorowania urządzeń sieciowych.**
   3. **Monitorowania stanu połączeń.**
   4. **Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów**
   5. **Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.**
   6. **Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.**
   7. **Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.**
   8. **Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.**
   9. **Grupowanie hostów.**
   10. **Definiowanie planowanych przerw serwisowych dla hostów i usług.**
   11. **Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).**

12. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
13. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
14. Monitorowanie serwerów za pomocą agentów
15. Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server .
16. Monitorowanie Active Directory.
17. Monitorowanie serwerów plików, udziałów sieciowych.
18. Monitorowanie statusu serwerów Apache.
19. Monitorowanie baz danych:
    - ORACLE,
    - MySQL,
    - Postgress.
    - MSSQL Server
    - DB2
20. Monitorowanie urządzeń przez następujące protokoły:
    - SNMP,
    - WMI,
    - IPMI.
21. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
22. Monitorowanie poprawności działania DNS.
23. Monitorowanie środowiska VMware.
24. Monitorowanie środowiska Hyper-V.
25. Monitorowanie działania serwera czasu NTP.
26. Monitorowanie offsetu czasu na serwerach.
27. Monitorowanie ping - czasy odpowiedzi, straty pakietów.
28. Monitorowanie zajętości miejsca na poszczególnych partycjach.
29. Monitorowanie obciążenia dysków.
30. Monitorowanie wykorzystania pamięci RAM.
31. Monitorowanie obciążenia CPU.
32. Monitorowanie logów systemowych Windows.
33. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
34. Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
35. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
36. Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)

37. Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
38. Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
39. Wykrywanie niestabilnie działających usług.
40. Monitorowanie dostępności stron internetowych.
41. Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządze

III. Prezentacja
1. Prezentację stanu urządzeń na mapie.
2. Prezentację danych na dashboardach.
3. Elastyczną konfigurację dashboardów, wybór elementów.
4. Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
5. Tworzenie indywidualnych dashboardów przez użytkowników

IV. Powiadomienia
1. Globalne wyłączanie powiadomień.
2. Powiadamianie użytkownika o problemach przez e-mail.
3. Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
4. Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.
5. Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług

V. Konfiguracja
1. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW
2. Automatyczna konfiguracja i działanie z REST-API
3. Centralne zarządzanie agentami
4. Integracja danych z różnych źródeł danych (JSON, XML, SNMP)

VI. Monitoring bazy danych systemu HIS
1. Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:

- Instance state
- Version
- Jobs
- Locks
- Processes
- Number of active sessions
- Recovery area
- Log switch activity
- General tablespace information
- Tablespaces performance
- Long active sessions
- Undo retention
- Checkpoint and online backup state

- Custom SQLs
- RMAN backup status
- RMAN backups
- ASM disk groups
- Apply and transport lag of Oracle Data-Guard

2. Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości

VII. Kolektor logów

1. System posiada własny kolektor logów syslog
2. Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps
3. Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event
4. Klasyfikuje wiadomości bazując na zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.

VIII. Cyberbezpieczeństwo

1. System monitoruje urządzenia klasy UTM minimum w zakresie:

- wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika
- monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany" ustawienie stanu na OK, a status „niezsynchronizowany" na CRIT.
- monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz" (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda" (1).
- monitoruje aktualną liczbę sesji na urządzeniu
- monitoruje liczbę dostępnych tuneli IPSec VPN
- monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.
- monitoruje poziom wykorzystania procesora
- Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.

2. System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog
3. System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.

IX. Warunki świadczenia usługi

1. Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty

2. W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.
3. Aktualizacje dostarczonego Systemu SOC do nowych wersji oprogramowania przez okres 12 miesięcy.
4. Szkolenia administratorów on-line z nowych funkcjonalności,
5. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu,
6. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7
7. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24/7/365, zgodnie z określonymi poniżej warunkami SLA
8. Zgłoszenia i Incydenty są klasyfikowane na podstawie potencjalnego wpływu na Klienta. Wykorzystywane są 4 poziomy klasyfikacji, jak przedstawiono w poniższej tabeli:

Poziom	Opis	Zagrożenie	Przykład
Krytyczny	Niezbędne natychmiastowe działanie złagodzić obecne złośliwe oprogramowanie Działalność	- Przerwa w działaniu serwera/systemu - Brak odbioru danych z lokalizacja klienta	Wyciek danych
3	Wysokie prawdopodobieństwo incydentu, jeśli nie podejmuje się działań zapobiegawczych	- Znaczące zmiany w SIEM - wskazanie natężenia ruchu danych obniżona wydajność potencjał	Brak potwierdzenia
2	Niski potencjalny incydent	- Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu	Znaleziony wirus na stacji roboczej
1	Aktywności utrzymaniowe lub informacyjne	-	Raport

9. W oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.

Poziom	Opis	Zagrożenie	SLA
Critical	1 godzina	1 godzina	96%

3	24 godziny	2 godziny	96%
2	72 godziny	8 godzin	96%
1	5 dni	24 godzin	96%

10. **W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:**
    - **Serwery 5..... szt.,**
    - **Macierze ..... szt.,**
    - **Przełączniki LAN ..... szt.,**
    - **Serwer Backupu ..... szt.,**
    - **Bibliotekę taśmowa LTO .....sztuka**
    - **serwer AD ..... szt.**
    - **UPS .....**

    W przypadku instalacji przez Zamawiającego nowego rozwiązania będącego jednym z powyższych elementów musi ono zostać objęte systemem monitorowania w ramach usługi SOC.

11. **W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS:**
    - **Monitorowanie komunikacji z platformą P1**
    - **Monitorowanie komunikacji EWUŚ**
    - **Monitorowanie bazy danych systemu HIS**
12. **Producent Systemu SOC musi posiadać certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017**

Odp. Zamawiający wymaga realizacji przedmiotu zamówienia zgodnie z zapytaniem ofertowym jednakże dopuszcza jak w zapytaniu.

Z poważaniem:

Z-ca DYREKTORA
ds. Administracyjno-Technicznych
mgr Urszula Makowska

STARSZY INFORMATYK
mgr Michał Brodziński

Sporządziła:
Magdalena Krzykowska
st. insp. ds. zamówień publicznych
i eksploatacji sprzętu
tel. 29 75 34 405