|  |
| --- |
| **Wdrożenie i świadczenie usługi Security Operation Center do dnia 31-12-2024** |
| ***Lp.*** | ***Wymagane minimalne parametry techniczne*** | ***Wymóg do spełnienia (warunek graniczny)*** | ***OFEROWANE PARAMETRY TECHNICZNE –*** *podaje Wykonawca**Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę**NIE – wykonawca nie spełnia konkretnego parametru* |
| ***Użytkownicy*** |
| 1. | * Możliwość tworzenia kont dla wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.
* Zapewnienie równoległego dostępu do systemu dla wielu użytkowników.
* Możliwość ograniczania użytkownikom dostępu do wybranych grup hostów.
 | TAK |  |
| ***Monitorowanie*** |
| 1. | * Monitorowania serwerów fizycznych.
* Monitorowani stanu macierzy dyskowych.
* Monitorowania urządzeń sieciowych w tym UTM.
* Monitorowania stanu połączeń.
* Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
* Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
* Monitorowanie stanu rejestratorów NVR.
* Monitorowanie stanu systemów backupu.
* Monitorowanie stanu bibliotek taśmowych.
* Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.
* Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
* Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
* Grupowanie hostów.
* Definiowanie planowanych przerw serwisowych dla hostów i usług.
* Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
* Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
* Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
* Monitorowanie serwerów za pomocą agentów
* Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server .
* Monitorowanie stanu usługi Active Directory.
* Monitorowanie serwerów plików, udziałów sieciowych.
* Monitorowanie statusu serwerów Apache, IIS, ngix
* Monitorowanie baz danych:
* ORACLE,
* MySQL,
* Postgress.
* MSSQL Server
* Monitorowanie urządzeń przez następujące protokoły:
* SNMP,
* WMI,
* IPMI.
* Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
* Monitorowanie poprawności działania DNS.
* Monitorowanie środowiska wirtualizacyjnych Vmware, Hyper-V, Proxmox
* Monitorowanie działania serwera czasu NTP.
* Monitorowanie offsetu czasu na serwerach.
* Monitorowanie ping - czasy odpowiedzi, straty pakietów.
* Monitorowanie zajętości miejsca na poszczególnych partycjach.
* Monitorowanie obciążenia dysków.
* Monitorowanie wykorzystania pamięci RAM.
* Monitorowanie obciążenia CPU.
* Monitorowanie logów systemowych Windows.
* Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
* Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
* Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
* Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)
* Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
* Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
* Wykrywanie niestabilnie działających usług.
* Monitorowanie dostępności stron internetowych.
* Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
 | TAK |  |
| ***Prezentacja*** |
| 1. | * Prezentację stanu urządzeń na mapie.
* Prezentację danych na dashboardach.
* Elastyczną konfigurację dashboardów, wybór elementów.
* Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
* Tworzenie indywidualnych dashboardów przez użytkowników
 | TAK |  |
| ***Powiadomienia*** |
| 1. | * Globalne wyłączanie powiadomień.
* Powiadamianie użytkownika o problemach przez e-mail, sms, telefon
* Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
* Definiowanie przedziałów czasowych, w których wysyłane są powiadomienia do poszczególnych użytkowników.
* Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
 | TAK |  |
| ***Konfiguracja*** |
| 1. | * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW
* Automatyczna konfiguracja i działanie z REST-API
* Centralne zarządzanie agentami
* Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
 | TAK |  |
| ***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
* Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości
 | TAK |  |
| ***Kolektor logów*** |
| 1. | * System posiada własny kolektor logów syslog
* Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps
* Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event
* Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
 | TAK |  |
| ***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” jest uważany za OK, a status „niezsynchronizowany” 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.
* System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog
* System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.
 | TAK |  |
| ***SOC i NOC*** |
| 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
* W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.
* Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA.
* Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
* Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza
* Reakcji.
* Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
* W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:
* Serwery fizyczne 10 sztuk
* Macierze 5 sztuk,
* Przełączniki LAN 50 sztuk
* Serwery Backupu 2 sztuk
* Biblioteki taśmowe LTO 2 sztuk
* Macierze NAS 3 sztuki
* UPS 5 sztuk
* Serwery aplikacji
* IIS 5 sztuk
* Serwer wirtualizacji 10 sztuk
* Serwery wirtualne 50 sztuk
* Serwer AD 4 sztuki
* W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS:
* Monitorowanie komunikacji z platformą P1
* Monitorowanie komunikacji bramek HL7
* Monitorowanie komunikacji EWUŚ
* Monitorowanie KOWAL
* Monitorowanie komunikacji AP-KOLCE
* Monitorowanie RZM
* Monitorowanie bazy danych systemu HIS
 | TAK |  |

Zdarzenia i Incydenty sklasyfikowane na podstawie potencjalnego wpływu na środowisko IT Zamawiającego.

|  |  |  |  |
| --- | --- | --- | --- |
| Poziom | Opis | Zagrożenie | Incydent (przykład) |
| **Krytyczny** | Niezbędne natychmiastowe działaniezłagodzić obecne złośliwe oprogramowaniedziałalność | - Przerwa w działaniu serwera- Brak odbioru danych zlokalizacja klienta | Wyciek danych |
| **3** | Wysokie prawdopodobieństwo incydentu, jeśli nie podejmuje się działań zapobiegawczych | - Znaczące zmiany w SEIM- wskazanie natężenia ruchu danych obniżona wydajność potencjał | Brak potwierdzenia |
| **2** | Niski potencjalny incydent | - Użytkownik nie zaktualizowałhasła w wymaganym odstępie czasu | Znaleziony wirus na stacji roboczej |
| **1** | Aktywności utrzymaniowe lub informacyjne | - | Raport |

W oparciu o powyższą klasyfikację ustalone zostały odpowiednie poziomy SLA

|  |  |  |  |
| --- | --- | --- | --- |
| 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% |

Wymagania dodatkowe:

- W przypadku instalacji przez Zamawiającego nowego rozwiązania obejmującego powyższy zakres, Wykonawca zobowiązany jest podłączyć je do systemu monitorowania SOC w terminie do 14 dni od momentu podpisania umowy.

- 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

Wykonawca zobowiązany jest przeprowadzić szkolenie dla personelu Zamawiającego (6 osób) z podstawowej i zaawansowanej obsługi przedmiotu zamówienia (obsługa zdarzeń SOC/SIEM). Wykonawca po zakończonych szkolenia wyda przeszkolonym pracownikom Zamawiającego certyfikaty potwierdzające udział w przeprowadzonych szkoleniach.