Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, REGON 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

załącznik nr 2H do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Zakup sprzętu komputerowego: SIEM
Element	101	Opis przedmiotu zamówienia
Wersja	1	2022-10-06

2. OPIS SERWERA

Funkcjonalność systemu SIEM:

1. Najważniejsze funkcjonalności:
    - 1.1.1.1. Aplikacja musi obsługiwać logi z wielu systemów operacyjnych
    - 1.1.1.2. Aplikacja musi obsługiwać logi z wielu urządzeń:
        - 1.1.1.2.1. (Windows, Linux, Unix, routery, przełączniki, VMWare, dowolne źródło logów w formacie Syslog)
    - 1.1.1.3. System musi pozwalać na konfigurowanie własnych widżetów i widoków
    - 1.1.1.4. Aplikacja musi umożliwiać wyszukiwanie w logach za pomocą operatora logicznego, frazy, zakresów wartości, symboli wieloznacznych i wyszukiwania grupowego
    - 1.1.1.5. Aplikacja musi korzystać z ElasticSearch`a w celu zwiększenia szybkości wyszukiwania i pobierania danych
    - 1.1.1.6. System musi pozwalać użyć trybu aktywnego FTP dla importu pliku dziennika
    - 1.1.1.7. Aplikacja musi umożliwiać importowanie i analizowanie plików zdarzeń
    - 1.1.1.8. System musi wspierać automatyczne wykrywanie hostów
    - 1.1.1.9. Aplikacja musi umożliwiać filtrowanie zdarzeń przed zapisaniem ich w bazie danych
    - 1.1.1.10. System musi pozwalać na archiwizowanie zebranych danych do skompresowanego pliku
    - 1.1.1.11. Aplikacja musi umożliwiać szyfrowanie plików archiwum logów
    - 1.1.1.12. System musi wspierać hashowanie i dodawanie znaczników czasu do plików archiwum
    - 1.1.1.13. System musi umożliwiać na wyświetlanie zdarzeń w czasie rzeczywistym
    - 1.1.1.14. System musi posiadać automatyczne alerty
    - 1.1.1.15. Aplikacja musi wspierać autoryzowany dostęp
    - 1.1.1.16. Aplikacja musi umożliwiać tworzenie własnych zakładek oraz dashboard`ów
    - 1.1.1.17. System musi pozwalać na grupowanie hostów w celu wdrożenia zasad parsowania logów
    - 1.1.1.18. Aplikacja musi umożliwiać zaplanowanie zbierania danych
    - 1.1.1.19. System musi pozwalać na utworzenie raportów niestandardowych
    - 1.1.1.20. Aplikacja musi umożliwiać planowane wykonywanie raportów
    - 1.1.1.21. System musi posiadać raporty PUMA
    - 1.1.1.22. Aplikacja musi obsługiwać wiele formatów raportów
    - 1.1.1.23. Aplikacja musi pozwalać na eksportowanie raportów w formatach:
        - 1.1.1.23.1. CSV
        - 1.1.1.23.2. PDF
    - 1.1.1.24. System musi pozwalać na wykonanie analizy trendów
    - 1.1.1.25. System musi pozwalać na wykonanie analizy bezpieczeństwa
    - 1.1.1.26. Aplikacja musi posiadać gotowe raporty zgodności (Syslog) (predefiniowane i dostosowywalne)
    - 1.1.1.27. System musi umożliwiać wykonanie polecenia/akcji w przypadku alertów
    - 1.1.1.28. System musi pozwalać na skonfigurowanie powiadomienia w postaci SMS i SNMP Trap dla alertów
    - 1.1.1.29. Aplikacja musi umożliwiać eksport / import profili alertów, raportów i filtrów
    - 1.1.1.30. Aplikacja musi pozwalać na zaawansowane wyszukiwanie w surowych logach
    - 1.1.1.31. System musi pozwalać na zapisywanie wyniku wyszukiwania w logach jako profil raportu
    - 1.1.1.32. Aplikacja musi pozwalać na udostępnienie raportów innym użytkownikom
    - 1.1.1.33. Aplikacja musi umożliwiać zaplanowanie cyklicznych importów logów z zasobów lokalnych i zdalnych (FTP / SFTP / Cloud)
    - 1.1.1.34. System musi pozwalać na zbieranie logów podczas przestoju modułu gromadzącego logi
    - 1.1.1.35. Aplikacja musi pozwalać na monitorowanie integralności plików
    - 1.1.1.36. System musi posiadać wbudowane raporty charakterystyczne dla serwera
    - 1.1.1.37. System musi umożliwiać monitorowanie wielu lokalizacji
    - 1.1.1.38. System musi posiadać skalowalną architekturę

1.1.1.39. Aplikacja musi pozwalać na wyodrębnianie pola logu przy użyciu interaktywnego konstruktora składni wyrażeń regularnych (regex)
1.1.1.40. System musi stosować Uniwersalne analizowanie i indeksowanie logów (ULPI) do obsługi dowolnego formatu logów (czytelnego dla człowieka i nieszyfrowanego formatu logów)
1.1.1.41. Aplikacja musi pozwalać na import użytkowników z grup Active Directory
1.1.1.42. System musi posiadać Agenta do zbierania logów w sieci WAN / Firewall
1.1.1.43. Aplikacja musi zezwalać na import zapisanych plików Syslog
1.1.1.44. System musi umożliwiać Rebranding klienta Webowego
1.1.1.45. Aplikacja musi potrafić natychmiast dostarczyć wybrane raporty
1.1.1.46. System musi pozwalać na analizę specyficznych logów aplikacji:
1.1.1.46.1. Serwer sieci Web MS IIS
1.1.1.46.2. Serwery FTP MS IIS
1.1.1.46.3. Serwer Windows DHCP
1.1.1.46.4. Serwer DHCP Linux
1.1.1.46.5. Baza danych MS SQL
1.1.1.46.6. Baza danych Oracle
1.1.1.46.7. Serwer WWW Apache
1.1.1.46.8. Serwer druku
1.1.1.47. Aplikacja musi wspierać MS SQL Server i MS SQL Cluster jako bazy danych zaplecza
1.1.1.48. System musi pozwalać na modyfikację gotowych widoków i widoków dedykowanych dla użytkowników
1.1.1.49. System musi posiadać rozbudowane uwierzytelnianie użytkowników zewnętrznych przez Active Directory i RADIUS Server
1.1.1.50. Aplikacja musi stosować reguły korelacji zdarzeń w czasie rzeczywistym
1.1.1.51. Aplikacja musi pozwalać na monitorowanie logów serwera terminali Windows
1.1.1.52. Aplikacja musi pozwalać na monitorowanie sesji użytkownika
1.1.1.53. Aplikacja musi pozwalać eksportować i importować reguły korelacji.
1.1.1.54. Aplikacja musi posiadać wstępnie zbudowaną regułę korelacji do wykrywania ataku Ransomware Ragnar Locker.
1.1.1.55. Aplikacja musi posiadać pulpit aktywności VPN, pozwalający na wgląd w trendy użytkowania VPN i aktywność użytkowników VPN.
1.1.1.56. Aplikacja musi pozwalać tworzyć niestandardowe role uprawnień użytkownika.
1.1.1.57. Aplikacja musi pozwalać tworzyć filtry zbierania dzienników z wieloma kryteriami pól i operatorami logicznymi, aby zbierać lub wykluczać dzienniki z wybranych urządzeń.
1.1.1.58. Aplikacja musi umożliwiać uzyskanie kontekstowych danych o zagrożeniach dla określonych adresów IP lub adresów URL z wyników wyszukiwania.
1.1.1.59. Aplikacja musi zapewniać raporty i profile alertów oparte na strukturze MITER ATT&CK.
1.1.1.60. Aplikacja musi pozwala zarządzać incydentami bezpieczeństwa – badać je i śledzić, tworzyć incydenty i przypisywać techników do ich zbadania, kontrolować stan, wagę i postęp w analizie.
1.1.1.61. Aplikacja musi umożliwiać automatyzację tworzenia incydentów za pomocą reguł, aby automatycznie je tworzyć, gdy określone alerty zostaną wyzwolone w zadanym przedziale czasowym.
1.1.1.62. Aplikacja musi dawać możliwość mapowania wyzwolonych alertów, raportów i rejestrowania wyników wyszukiwania jako incydenty i przypisywania technika do ich zbadania.
1.1.1.63. Aplikacja musi pozwalać przywrócić strefę czasową za pomocą automatycznego wykrywania lub użycia czasu serwera.
1.1.1.64. Aplikacja musi posiadać zakładkę ATA Whois info, która zapewnia informacje na temat źródeł adresów URL i domen.
1.1.1.65. Aplikacja musi obsługiwać zbieranie dzienników historycznych dla systemu AS/400 oraz dostosowane zbieranie dzienników historycznych dla systemu Windows.
1.1.1.66. Aplikacja musi posiadać pulpit nawigacyjny Apache, który zapewnia wgląd w czasie rzeczywistym w działanie serwera WWW Apache.
1.1.1.67. Aplikacja musi obsługiwać dzienniki z Qualys - Vulnerability Management.
1.1.1.68. Aplikacja musi obsługiwać raporty zgodności dla certyfikacji Cybersecurity Maturity Model Certification (CMMC).

2. Szczegółowy spis funkcjonalności:
2.1. Zarządzanie Logami z wspieranych źródeł:
2.1.1. Źródła logów, które muszą być obsługiwane “Out of the Box”:
2.1.1.1. Podstawowa infrastruktura systemów Windows:
2.1.1.1.1. Windows Server 2003 i nowsze
2.1.1.1.2. Windows Vista i nowsze
2.1.1.1.3. Microsoft Windows DHCP Server
2.1.1.2. Platformy baz danych:
2.1.1.2.1. Serwery Microsoft SQL
2.1.1.2.2. Bazy danych Oracle
2.1.1.2.3. MySQL

2.1.1.2.4. DB2
2.1.1.3. Rozwiązania Endpoint Security:
2.1.1.3.1. ESET Antivirus
2.1.1.3.2. Microsoft Antimalware
2.1.1.3.3. Norton Antivirus
2.1.1.3.4. Sophos Antivirus
2.1.1.3.5. FireEye
2.1.1.3.6. Malwarebytes
2.1.1.3.7. McAfee
2.1.1.3.8. Symantec Endpoint Protection
2.1.1.3.9. Symantec DLP
2.1.1.3.10. Trend Micro-deep security
2.1.1.4. Zapory ogniowe: MGFWs, IDS, IPS
2.1.1.4.1. F5 BIG-IP
2.1.1.4.2. Barracuda
2.1.1.4.3. Check Point
2.1.1.4.4. Cisco
2.1.1.4.5. Cisco Meraki
2.1.1.4.6. Cyberoam
2.1.1.4.7. Fortinet
2.1.1.4.8. H3C
2.1.1.4.9. Huawei
2.1.1.4.10. Juniper
2.1.1.4.11. Juniper NetScreen
2.1.1.4.12. Palo Alto
2.1.1.4.13. pfSense
2.1.1.4.14. SonicWall
2.1.1.4.15. Sophos
2.1.1.4.16. Watchguard
2.1.1.4.17. HP
2.1.1.4.18. F5
2.1.1.4.19. FirePower
2.1.1.5. Środowiska virtualizacji:
2.1.1.5.1. Microsoft Hyper-V
2.1.1.5.2. Vmware
2.1.1.6. Urządzeń opartych o systemy Linux i Unix:
2.1.1.6.1. Linux
2.1.1.6.2. macOS
2.1.1.6.3. IBM AIX
2.1.1.6.4. HP UX
2.1.1.6.5. Solaris
2.1.1.6.6. IBM AS/400
2.1.1.6.7. Linux file monitoring
2.1.1.7. Urządzeń typu Router i Switch:
2.1.1.7.1. Cisco
2.1.1.7.2. Hewlett-Packard
2.1.1.7.3. Arista
2.1.1.8. Skanerów podatności:
2.1.1.8.1. Nessus
2.1.1.8.2. Nmap
2.1.1.8.3. Nexpose
2.1.1.8.4. OpenVas
2.1.1.8.5. Qualys
2.1.1.9. Serwerów webowych:
2.1.1.9.1. Apache
2.1.1.9.2. Microsoft IIS
2.1.1.10. Pozostałe źródła logów, które muszę być obsługiwane „Out of the box”:
2.1.1.10.1. Threat Analytics
2.1.1.10.2. CEF Format
2.1.1.10.3. SNMP Trap
2.1.1.10.4. Terminal Server
2.1.1.10.5. Printer
2.1.2. Aplikacja musi pozwalać na zarządzanie dziennikiem zdarzeń
2.1.3. Aplikacja musi pozwalać na zarządzanie Syslogami
2.1.4. Aplikacja musi tworzyć uniwersalny zbiór logów
2.1.5. Aplikacja musi pozwalać na zbieranie logów bez agenta

2.1.6. Aplikacja musi pozwalać na zbieranie logów w oparciu o agenta
2.1.7. Aplikacja musi przeprowadzać analizę logów
2.1.8. Aplikacja musi posiadać predefiniowane raporty logów zdarzeń
2.1.9. Aplikacja musi pozwalać na niestandardową analizę logów
2.1.10. Aplikacja musi pozwalać na archiwizację logów bezpośrednio z graficznego interfejsu użytkownika
2.1.11. Aplikacja musi pozwalać na przeszukiwanie logów bezpośrednio z graficznego interfejsu użytkownika
2.1.12. Aplikacja musi pozwala na dostosowanie pulpitu nawigacyjnego i widoków dla użytkownika
2.1.13. Aplikacja musi pozwalać na zarządzanie logami aplikacji
2.1.14. Aplikacja musi pozwalać na monitorowanie sesji użytkownika
2.1.15. Aplikacja musi umożliwiać alertowanie w czasie rzeczywistym
2.1.16. Aplikacja musi pozwalać wybrać metody powiadamiania o alertach
2.1.17. Aplikacja musi pozwalać na zmianę nazwy klienta internetowego
2.1.18. Aplikacja musi pozwalać na monitorowanie użytkowników uprzywilejowanych
2.1.19. Aplikacja musi pozwalać na utworzenie własnych indywidualnych raportów
2.1.20. Aplikacja musi potrafić stworzyć trendy dla wydarzeń historycznych
2.1.21. Aplikacja musi pozwalać na importowanie logów zdarzeń

2.2. Audyt aplikacji:
2.2.1. Aplikacja musi pozwalać na monitorowanie logów aplikacji
2.2.1.1. Aplikacja musi pozwalać na audyt serwera Microsoft IIS
2.2.1.2. Aplikacja musi posiadać predefiniowany analizator logów serwera sieci Web Microsoft IIS
2.2.1.3. Aplikacja musi pozwalać predefiniowany analizator logów serwera FTP Microsoft IIS
2.2.1.4. Aplikacja musi pozwalać na audyt Microsoft SQL Server
2.2.1.5. Aplikacja musi pozwalać na monitorowanie logów Microsoft SQL Server
2.2.1.6. Aplikacja musi pozwalać na monitorowanie logów serwera WWW Apache
2.2.1.7. Aplikacja musi pozwalać na monitorowanie logów serwera wydruku
2.2.1.8. Aplikacja musi pozwalać na monitorowanie logów serwera DHCP (Windows / Linux)
2.2.1.9. Aplikacja musi pozwalać na audyt bazy danych
2.2.1.10. Aplikacja musi pozwalać na monitorowanie logów bazy danych Oracle
2.2.2. Aplikacja musi pozwalać na monitorowanie serwera terminali Windows
2.2.3. Aplikacja musi pozwalać na zabezpieczanie krytycznych aplikacji biznesowych
2.2.4. Aplikacja musi pozwalać na zarządzanie logami krytycznych aplikacji Windows
2.2.5. Aplikacja musi pozwalać na wykrywanie ataków na serwer WWW
2.2.6. Aplikacja musi posiadać analizator wykrywający ataki SQL injection
2.2.7. Aplikacja musi pozwalać na wykrycie i łagodzenie skutków ataków DoS
2.2.8. Aplikacja musi zawierać raporty dla aplikacji Sysmon.

2.3. Audyt urządzeń sieciowych:
2.3.1. Aplikacja musi pozwalać na audyt urządzeń sieciowych
2.3.2. Aplikacja musi pozwalać na kontrolowanie logów routera
2.3.3. Aplikacja musi potrafić analizować logi Cisco
2.3.4. Aplikacja musi pozwalać analizować logi Cisco Meraki
2.3.5. Aplikacja musi pozwalać na monitorowanie aktywności użytkownika w routerze
2.3.6. Aplikacja musi pozwalać na monitorowanie ruchu routera
2.3.7. Aplikacja musi pozwalać na kontrolę logów zapory
2.3.8. Aplikacja musi pozwalać na monitorowanie logów IDS / IPS
2.3.9. Aplikacja musi pozwalać na monitorowanie logów Switch`y
2.3.10. Aplikacja musi pozwalać na monitorowanie logów VPN
2.3.11. Aplikacja musi pozwalać na audyt Zapory systemu Windows
2.3.12. Aplikacja musi pozwalać na audyt zapory SonicWall
2.3.13. Aplikacja musi pozwalać na audyt zapory ogniowej H3C
2.3.14. Aplikacja musi pozwalać na audyt zapory ogniowej Palo Alto
2.3.15. Aplikacja musi pozwalać na audyt logów urządzeń Juniper
2.3.16. Aplikacja musi pozwalać na audyt logów urządzeń Fortinet / FortiGate
2.3.17. Aplikacja musi pozwalać na kontrolę logów urządzeń Check Point
2.3.18. Aplikacja musi pozwalać na monitorowanie logów Sophos
2.3.19. Aplikacja musi pozwalać na monitorowanie logów urządzeń Huawei
2.3.20. Aplikacja musi potrafić analizować logi urządzeń HP

2.4. Raporty zgodności IT:
2.4.1. Aplikacja musi posiadać raport zgodności PCI DSS
2.4.2. Aplikacja musi posiadać zgodności SOX
2.4.3. Aplikacja musi posiadać raport zgodności z SOX
2.4.4. Aplikacja musi posiadać raport zgodności z ISO 27001
2.4.5. Aplikacja musi posiadać raport zgodności z RODO
2.4.6. Aplikacja musi posiadać raport zgodności z HIPAA
2.4.7. Aplikacja musi posiadać raport zgodności PCI
2.4.8. Aplikacja musi posiadać raport zgodności FISMA
2.4.9. Aplikacja musi posiadać raport zgodności z GLBA

2.4.10. Aplikacja musi posiadać raport zgodności GPG
2.4.11. Aplikacja musi posiadać raport zgodności ISLP
2.4.12. Aplikacja musi posiadać raport zgodności FERPA
2.4.13. Aplikacja musi posiadać raport zgodności NIST
2.4.14. Aplikacja musi posiadać raport zgodności PDPA
2.4.15. Aplikacja musi posiadać raport dotyczące nowej zgodności
2.4.16. Aplikacja musi pozwalać na dostosowywanie raportów zgodności
2.4.17. Aplikacja musi pozwalać na dodanie własnych raportów zgodności

2.5. Funkcjonalności SIEM:
2.5.1. Aplikacja musi pozwalać agregować i analizować informacje o bezpieczeństwie oraz umożliwia zarządzanie zdarzeniami (SIEM)
2.5.2. Aplikacja musi pozwalać na monitorowanie Syslog
2.5.3. Aplikacja musi pozwalać na monitorowanie logów zdarzeń
2.5.4. Aplikacja musi pozwalać na monitorowanie integralności plików Windows
2.5.5. Aplikacja musi pozwalać na monitorowanie integralności plików systemu Linux
2.5.6. Aplikacja musi pozwalać na korelację zdarzeń z logów w czasie rzeczywistym
2.5.7. Aplikacja musi pozwalać budować własne korelacje w oparciu o dowolne zdarzenie odnotowane w monitorowanym środowisku
2.5.8. Aplikacja musi pozwalać na zarządzanie logami bezpieczeństwa
2.5.9. Aplikacja musi pozwalać na inteligentne wykrywanie zagrożeń na podstawie zebranych logów
2.5.10. Aplikacja musi pomagać w zabezpieczaniu urządzeń na podstawie syslogów
2.5.11. Aplikacja musi działać zgodnie z STIX / TAXII
2.5.12. Aplikacja musi umożliwiać zarządzanie incydentami
2.5.13. Aplikacja musi pozwalać na zarządzanie przepływem pracy związanej z incydentami
2.5.14. Aplikacja musi pozwalać na importowanie plików logów
2.5.15. Aplikacja musi pozwalać na audyt użytkowników uprzywilejowanych
2.5.16. Aplikacja musi pozwalać na wykrywanie zagrożeń systemu Windows
2.5.17. Aplikacja musi pozwalać na ograniczanie zagrożeń zewnętrznych
2.5.18. Aplikacja musi pozwalać na zarządzanie dziennikiem aplikacji
2.5.19. Aplikacja musi pozwalać na zapisywanie wyniku wyszukiwania jako alerty
2.5.20. Aplikacja musi pozwalać raporty o zagrożeniach Malwarebytes
2.5.21. Inteligentne wykrywanie zagrożeń FireEye
2.5.22. Aplikacja musi pozwalać na dodawanie indywidualnych raportów
2.5.23. Aplikacja musi pozwalać utworzyć dedykowane widoki i nimi zarządzać:
2.5.23.1. Dodawać do widoków wybrane raporty w postaci widżetów
2.5.23.2. Usuwać wybrane widżety
2.5.23.3. Zmieniać kolejność wyświetlania widoków
2.5.23.4. Zmieniać kolejność wyświetlania widżetów

2.6. Audyt międzyplatformowy:
2.6.1. Aplikacja musi pozwalać na monitorowanie krytycznych metryk serwerów
2.6.2. Aplikacja musi pozwalać na audyt logów zdarzeń
2.6.3. Aplikacja musi pozwalać na zarządzanie logami serwera VMWare
2.6.4. Aplikacja musi pozwalać na kontrolę urządzeń z systemem Windows
2.6.5. Aplikacja musi pozwalać na audyt logów urządzeń w oparciu o Syslog
2.6.6. Aplikacja musi pozwalać na kontrolę i raportowanie w systemów Linux
2.6.7. Aplikacja musi pozwalać na kontrolę i raportowanie w systemów Unix
2.6.8. Aplikacja musi pozwalać na kontrolę rejestru systemu Windows
2.6.9. Aplikacja musi pozwalać na audyt urządzeń typu Switch oraz Router
2.6.10. Aplikacja musi pozwalać na monitorowanie logów infrastruktury w chmurze
2.6.11. Aplikacja musi pozwalać na wykrywanie kradzieży danych na podstawie zebranych logów
2.6.12. Aplikacja musi pozwalać na monitorowanie instancji AWS
2.6.13. Aplikacja musi pozwalać wygenerować raport konfiguracji usługi IIS, umożliwiający przeglądanie zmian, takich jak rejestrowanie zmian, zmiany modułów, zmiany protokołu SSL i inne.
2.6.14. Aplikacja musi posiadać wbudowany PostgreSQL w wersji 10.18.
2.6.15. Aplikacja musi posiadać Security Hardening w celu zwiększenia bezpieczeństwa podczas korzystania.
2.6.16. Aplikacja musi pozwalać na konfigurowanie Log Collection Filters dla aplikacji wewnętrznych.
2.6.17. Aplikacja musi posiadać wbudowany Spring Framework w wersji 5.3.18.
2.6.18. Aplikacja musi posiadać wstępnie zdefiniowane zasady korelacji dla Mitre ATT&CK TTP(s).