Załącznik nr 6d

Opis Przedmiotu Zamówienia

Przedmiot zamówienia: Dostawa i wdrożenie systemu monitorowania sieci przemysłowej

Przedmiotem zamówienia jest:

1. wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),

2. dostawa licencji oraz trzech sond sprzętowych,

3. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.

2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.

3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.

4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.

5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.

6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.

7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.

8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.

9. System IDS musi zapewniać:

a. pasywne monitorowanie sieci przemysłowej Zamawiającego,

b. automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.

c. szczegółową inwentaryzację urządzeń,

d. automatyczne odzwierciedlenie połączeń komunikacyjnych,

e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,

f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,

g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,

h. obsługę LLDP, CDP, CIP, SSDP.

10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.

11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.

12. System IDS musi mieć możliwość dodawania nowego typu protokołu.

13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.

14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.

15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).

16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.

17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.

18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.

19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)

20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.

21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.

22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.

23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.

24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.

25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.

26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.

27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.

28. System IDS musi wykrywać zagrożenia min.:

a. malware/”zero-day”,

b. atak DOS/DDOS,

c. atak typu ATP,

d. spyware, skanowanie sieci,

e. zagrożenia Man-in-the-Middle,

f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,

g. wykrywanie połączeń do innej sieci LAN/internet,

h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.

29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.

30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.

31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.

32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.

33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.

34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.

35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.

36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.

37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.

38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.

39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.

40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.

41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.

42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.

43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.

44. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.

45. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.

46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.

47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.

48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.

49. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.

50. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.

51. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

Dostawa, wdrożenie.

1. Wykonawca dostarczy:

a. sondy sprzętowe w liczbie … szt. do monitorowania sieci przemysłowej,

b. licencję wieczystą na system IDS nielimitowanej monitorowanych urządzeń,

c. usługi wsparcia serwisowego producenta systemu IDS na okres 36 miesięcy.

serwis producenta systemu IDS ma obejmować:

- Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
- Dostęp do nowych wersji systemu IDS.
- Dostęp do aktualizacji i poprawek systemu IDS.
- Dostęp do aktualizacji oprogramowania sond sprzętowych.
- Wymianę uszkodzonych sond sprzętowych w razie awarii.
- Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
- Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
- Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.

3. Sprzęt serwerowy wraz z niezbędnym oprogramowaniem tj. jak system operacyjny, wirtualizator, itp. - zapewni Zamawiający.

4. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.

5. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.

6. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.

7. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.

8. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.

9. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.

10. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.