**Załącznik nr 1A**

**D/23/2025**

**OPIS PRZEDMIOTU ZAMÓWIENIA / UMOWY**

Przedmiot zamówienia: **Zakup i dostawa systemu klasy NDR (Network Detection and Response)**

1. System NDR musi składać się z sprzętu fizycznego (min. 2 serwerów) oraz oprogramowania (wraz z niezbędnymi licencjami) zainstalowanego na wcześniej wspomnianym sprzęcie (serwerach). Całość elementów składających się na system NDR powinna zostać dostarczona i uruchomiona w infrastrukturze lokalnej Zamawiającego (on-premise).
2. System musi być dostarczony wraz z licencjami na okres 1 roku z możliwością dokonania zakupu kolejnych licencji po wygaśnięciu okresu obowiązywania licencji dostarczonych w ramach niniejszego postępowania.
3. Przez cały okres na jaki zostanie dostarczona licencja, wykonawca musi zapewnić wsparcie techniczne producenta systemu NDR lub partnera obejmujące dostęp do aktualizacji systemu.
4. Dostarczony sprzęt musi być objęty gwarancją producenta lub dostawcy przez okres wskazany w ofercie lecz nie mniejszy niż 24 miesiące i nie większy niż 60 miesięcy.
5. System NDR powinien składać się co najmniej z następujących elementów:
6. serwer centralny (fizyczna maszyna z zainstalowanym oprogramowaniem),
7. sonda sieciowa (fizyczna maszyna z zainstalowanym oprogramowaniem).
8. Serwer centralny (urządzenie fizyczne) musi posiadać następujące funkcjonalności/opcje:
9. zarządzanie systemem zainstalowanym na tej maszynie oraz podłączonymi do niego sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu,
10. wykonywanie analizy zebranych danych i plików w oparciu o:
11. analizę shellcodes;
12. inżynierię wsteczną;
13. ROP (Return Oriented Programming);
14. JOP (Jump Oriented Programming);
15. heurystykę w czasie rzeczywistym;
16. być wyposażony w statyczne silniki malware,
17. prezentację wyników analiz (detekcji) w postaci wykresów i scoringu,
18. przechowywanie metadanych na potrzeby dalszej analizy (tzw. threat hunting),
19. przekazywanie danych do systemu klasy SIEM,
20. połączenie między serwerem centralnym, a sondami powinno odbywać się za pomocą sieci IP z uwagi na rozproszoną infrastrukturę Zamawiającego,
21. możliwość podłączenia co najmniej 3 sond fizycznych zlokalizowanych w infrastrukturze zamawiającego (przedmiot zamówienia wymaga dostarczenia wyłącznie 1 sondy, pozostałe 2 sondy – jako możliwość dokonania dodatkowego zakupu w przyszłości).
22. Wydajność serwera centralnego musi pozwalać na:
23. obsługę co na mniej 2000 zdarzeń na sekundę,
24. przechowywać co najmniej 1 milion zdarzeń w pamięci trwałej,
25. analizowanie przy pomocy silników detekcji malware co najmniej 10 plików na sekundę,
26. analizowanie przy pomocy silnika detekcji shellcode/powershell co najmniej 1 pliku na sekundę,
27. Sonda fizyczna zbierająca ruch sieciowy musi posiadać następujące funkcjonalności/opcje:
28. architekturę modułową, umożliwiającą rozbudowywanie urządzenia za pomocą kart rozszerzeń, np. dodatkowe porty sieciowe,
29. co najmniej 4 porty monitorujące z możliwością rozszerzenia o kolejne 4 porty,
30. wyboru standardu interfejsu (elektryczny lub optyczny),
31. przetworzenia danych dla maksymalnego odbieranego ruchu sieciowego na poziomie co najmniej 4Gbps,
32. konfiguracji macierzy RAID1 lub RAID5 (do wyboru),
33. dedykowanych interfejsów monitorujących w standardzie SFP lub SFP+, co najmniej 2 szt.,
34. odbierania kopii ruchu sieciowego na dedykowanych portach monitorujących,
35. wstępnej weryfikacji przechwyconego ruchu, pod kątem podatności, realizowaną za pomocą mechanizmów traffic payloads opartych o analizę formalną i statystyczną, przekazywanie wstępnie przetworzonego strumienia do urządzenia nadrzędnego (w postaci metadanych),
36. generowania alarmów oraz metadanych o zdarzeniach,
37. odczytywania plików w standardzie co najmniej .pcap,
38. raportowania informacji o stanie sondy do urządzenia nadrzędnego.
39. Zarówno serwer centralny, jak i sonda musi zostać dostarczona z oprogramowaniem producenta będącym w pełni kompatybilnym z dostarczonym sprzętem fizycznym, jak i zapewniać wszystkie opisane funkcje dotyczące komunikacji pomiędzy serwerem centralnym, a sondą(ami).
40. Wszystkie urządzenia muszą obsługiwać szyfrowanie dysków za pomocą zewnętrznego klucza USB, którego usunięcie uniemożliwi dostęp do systemu i danych.
41. Połączenie pomiędzy urządzeniem administrującym (serwer centralny), a sondą musi być realizowane w sposób szyfrowany np. poprzez połączenie na bazie protokołu IPSec.
42. Producent musi pozwalać na zaimplementowanie sondy w formie fizycznej oraz jako maszyny wirtualnej, przy czym dostawa licencji lub innych elementów, niezbędnych do uruchomienia sondy wirtualnej nie jest przedmiotem zamówienia (dodatkowa dostępna opcja).
43. System musi umożliwiać konfigurację architektury typu single-tenant i multi-tenant.
44. Sonda musi odbierać dane w formie pełnej kopii ruchu sieciowego (full package capture), np. dostarczanych poprzez wykorzystanie technologii port mirroringu (span port) na przełącznikach sieciowych lub urządzeniach typu traffic access point (TAP).
45. Sonda musi wspierać protokoły IPv4, IPv6 i 802.1Q.
46. Sonda musi posiadać niezbędne zasoby pamięci na okoliczność krótkotrwałego przerwania połączenia z urządzeniem administrującym, w celu agregacji danych lokalnie.
47. Zarówno sonda fizyczna, jak i urządzenie administrujące (serwer centralny) musi:
48. posiadać redundantne zasilanie,
49. obsługiwać technologię hot-swap i hot-plug (zasilanie, karty rozszerzeń, moduły SFP);
50. **System NDR musi posiadać co najmniej następujące funkcjonalności/opcje:**
51. Wykrywania i obsługi co najmniej 1000 unikatowych adresów IP występujących w infrastrukturze lokalnej Zamawiającego.
52. Indywidualnego definiowania zasad detekcji.
53. Definiowania zakresów sieci na podstawie adresacji IP lub VLAN.
54. Wstępnej analizy, która musi się odbywać zgodnie z mechanizmem parsowania (analizy składniowej danych).
55. Obsługi rozpoznawania oraz analizowania co najmniej następujących protokołów; DCE-RPC, DHCP, DNP3, DNS\_udp, DNS\_tcp, ENIP, FTP, HTTP, HTTP/2, IKEv2, Kerberos (KRB5), MQTT, NFS, RDP, RFB, SIP, SMB, SMTP, SNMP, SSH, TFTP, TLS.
56. Dostępu do konsoli serwera centralnego za pomocą protokołu HTTPS z wykorzystaniem dowolnej przeglądarki. Konsola powinna posiadać co najmniej 2 moduły tj. konsola NDR oraz konsola administracyjna urządzenia.
57. Konsoli NDR, która musi posiadać następujące funkcjonalności/opcje:
58. informowania o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, silnik detekcji odpowiedzialny za wykrycie, sygnatury czasowe,
59. podglądu zdarzeń w formie przeglądów odnosząc się do najważniejszych wydarzeń, assetów, użytkowników (bez konieczności instalacji agenta),
60. szacowania poziomu ryzyka dla każdego wykrytego zagrożenia, w oparciu o dedykowany algorytm,
61. mapowania zagrożeń w odniesieniu do co najmniej jednego z tzw. framework’ów (np. MITRE) opisującego znane i wykorzystywane taktyki w kontekście cyberataków,
62. tagowania zdarzeń i załączania opisu, notatek.
63. Konsoli administracyjnej, która musi posiadać następujące funkcjonalności/opcje:
64. kontroli stanu urządzeń i wykorzystania zasobów,
65. zbierania danych diagnostycznych,
66. konfiguracji eksportu danych,
67. konfiguracji ustawień komponentu uczenia maszynowego,
68. konfiguracji ustawień komponentu antymalware,
69. konfiguracji ustawień komponentu analizy ruchu sieciowego, w tym jego modyfikacji oraz dodawania źródeł definicji reguł,
70. zarządzania kontami użytkowników,
71. parowania urządzenia administrującego z sondami.
72. Katalogowania zebranych detekcji i dokonywania ich korelacji na bazie filtrów.
73. Przesłania podejrzanych plików w celu przeskanowania ich pod kątem szkodliwego oprogramowania co najmniej powershell i shellcode.
74. Definiowania reguł zarówno w sondach, jak i centralnie w urządzeniu administrującym.
75. Wykrywania zagrożeń w oparciu o co najmniej następujące silniki detekcji:
76. antymalware – skanowanie plików w ruchu sieciowym w celu identyfikacji szkodliwego oprogramowania, realizowany poprzez co najmniej 1 silnik detekcji przy użyciu analiz statycznych i heurystycznych (z możliwością rozszerzenia do 16 silników). Silniki skanowania w poszukiwaniu zagrożeń typu malware powinny obsługiwać również mechanizm skanowania plików sklasyfikowanych jako podejrzane, z użyciem nowych sygnatur po aktualizacji silnika detekcji.
77. Analiza shellcode i powershell – detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wykrywania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
78. Analiza ruchu w oparciu o definicje zagrożeń – analiza całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń, musi umożliwiać dodawanie i modyfikowanie własnych sygnatur ataków.
79. Domain generation algorithm (DGA) – wykrywanie losowego generowania domen, które mogą być używane jako odnośniki do połączeniami z serwerami C&C (Command and Control).
80. Przeprowadzenia aktualizacji w następujący sposób:
81. aktualizacja komponentów oprogramowania narzędziowego wykonywana musi być manualnie i realizuje ją administrator systemu,
82. aktualizacja sygnatur musi pozwalać na wybór 1 z dostępnych metody, a wszystkie muszą być obsługiwane przez dostarczony system:

* online – w sposób automatyczny z repozytorium producenta,
* manualnie – poprzez pobranie paczki aktualizacyjnej i przesłanie jej do oprogramowania narzędziowego przy użycia nośnika przenośnego;
* lokalnie – przy użyciu lokalnego repozytorium.

1. Zarządzania kopiami danych oraz retencją przechowywanych informacji, w co najmniej następujący sposób:
2. backup – pozwala na tworzenie i przywracanie kopii zapasowych konfiguracji systemu,
3. retencja danych – dane przechowywane są na urządzeniu administrującym, przez ograniczony czas, który może być uzależniony od zajętości pamięci lub ręcznie ustawionego czasu retencji danych,
4. zdarzenia systemowe – system musi umożliwiać tworzenie i archiwizowanie logów systemowych oraz logów na potrzeby wsparcia technicznego,
5. usuwanie danych – system musi mieć możliwość usuwania danych z możliwością wyboru, których typów danych ta akcja dotyczy.
6. Zarządzania dostępem użytkowników systemu w następujący sposób:
7. możliwość tworzenie wielu kont użytkowników,
8. każde konto użytkownika musi posiadać co najmniej następujące atrybuty:

* Nazwy konta,
* Hasła,
* Adresu e-mail,
* Imienia,
* Nazwiska,

1. różnicowanie uprawnień dostępowych do danych oraz modyfikacji ustawień, system musi mieć możliwość zdefiniowania przynajmniej trzech poziomów uprawnień: administratora, użytkownika uprzywilejowanego oraz operatora,
2. zarządzanie dostępem musi umożliwiać wykorzystanie protokołu LDAP,
3. system musi przechowywać historię autentykacji użytkowników.
4. Udostępniania danych do rozwiązań stron trzecich np. SIEM, syslog:
5. system musi umożliwiać definiowanie automatycznej synchronizacji zebranych danych i detekcji do innych rozwiązań poprzez API,
6. system musi umożliwiać rejestrowanie i przesyłanie informacji o zdarzeniach systemowych w standardzie syslog do zewnętrznego serwera.

W związku z realizacją niniejszego postępowania o udzielenie zamówienia publicznego nie występuje konieczność uwzględnienia wymogów dostępności dla osób ze szczególnymi potrzebami zgodnie z zasadami wynikającymi z postanowień ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (t.j. Dz. U. z 2024 r., poz. 1411 ze zm.).