Załącznik nr 1 do Umowy nr ……z dnia……

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**ROZDZIAŁ I. OGÓLNE WARUNKI REALIZACJI ZAMÓWIENIA**

* 1. Aktualnie Zamawiający posiada nw. środowisko - platformę do analizy złośliwych plików:
  2. Serwer fizyczny AX: Trellix AX 5550 (poprzednio FireEye AX);
  3. Platforma SaaS CM: Trellix CM2500Virtual (poprzednio FireEye CM);
  4. Serwer fizyczny EX: Trellix 3500;
  5. Serwer fizyczny EX: Trellix 3500;
  6. Serwer fizyczny FX: Trellix 6500.
  7. **PRZEDMIOT ZAMÓWIENIA**

**Przedmiotem zamówienia jest zapewnienie ciągłości funkcjonowania platformy do analizy złośliwych plików**

**Wykonawca może zrealizować przedmiot zamówienia, wybierając jedno z dwóch rozwiązań:**

1. Zaoferowanie rozwiązania wykorzystującego aktualnie posiadaną przez Zamawiającego infrastrukturę (w ramach oferty podstawowej):
2. przedłużenie działania posiadanej przez Zamawiającego platformy do analizy złośliwych plików - rozwiązania Trellix AX (poprzednio FireEye AX) oraz rozwiązania do zarządzania komponentami systemu Trellix CM (poprzednio FireEye CM) poprzez dostawę, instalację, konfigurację serwera fizycznego Trellix AX 5600, CM 4600 oraz dostarczenie niezbędnych licencji, zgodnie ze specyfikacją techniczną opisaną w Rozdziale III w pkt. 1 i 2 wraz z dostosowaniem istniejącej konfiguracji z obecnie użytkowanego środowiska na środowisko powstałe w wyniku prac związanych z przedłużeniem działania platformy składającej się z:
   1. Serwera fizycznego AX: Trellix AX 5550 (poprzednio FireEye AX)
   2. Platformy SaaS CM: Trellix CM2500Virtual (poprzednio FireEye CM)
   3. Serwera fizycznego EX: Trellix 3500
   4. Serwera fizycznego EX: Trellix 3500
   5. Serwera fizycznego FX: Trellix 6500
3. świadczenie usług serwisu i wsparcia technicznego dla środowiska powstałego w wyniku przedłużenia działania platformy. Wymagania dotyczące serwisu i wsparcia technicznego zostały opisane w Rozdziale I pkt. 5,
4. wykonanie projektu wdrożeniowego i dokumentacji powykonawczej opisanych szczegółowo w Rozdziale II w pkt. 3,
5. świadczenie usług asysty technicznej eksperta w liczbie do 100 roboczogodzin. Wymagania dotyczące usług asysty technicznej eksperta zostały uszczegółowione w Rozdziale II w pkt. 2.
6. Zaoferowanie rozwiązania wariantowego do rozwiązania określonego w lit. A, zgodnie z poniższymi warunkami (w ramach oferty wariantowej zamiast oferty podstawowej):
7. dostawy, instalacji, konfiguracji i uruchomienia systemu składającego się z:
   1. modułu AntyMalware dla poczty e-mail,
   2. modułu Sandbox,
   3. modułu ochrony udziałów sieciowych,
   4. moduł zarządzania systemem,

oraz dostarczenie niezbędnych licencji, zgodnie ze specyfikacją techniczną opisaną w Rozdziale IV.

1. świadczenie usług serwisu i wsparcia technicznego dla środowiska oraz uruchomienia systemu zarządzania i zbierania logów, z wyłączeniem świadczeń gwarancyjnych. Wymagania dotyczące serwisu i wsparcia technicznego zostały opisane w Rozdziale I w pkt. 5.
2. wykonania projektu wdrożeniowego i dokumentacji powykonawczej opisanych szczegółowo w Rozdziale II w pkt. 3.
3. świadczenia usług asysty technicznej eksperta w liczbie do 500 roboczogodzin. Wymagania dotyczące usług asysty technicznej eksperta zostały uszczegółowione w Rozdziale II w pkt. 2.
4. przeprowadzenia warsztatów szkoleniowych. Wymagania dotyczące warsztatów szkoleniowych zostały opisane w Rozdziale IV w pkt. 5.
   1. **TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA:**
5. w zakresie wymienionym w pkt. 2 lit. A pkt 1 lub lit. B pkt 1 – w terminie do …… dni roboczych od dnia zawarcia umowy (zgodnie z ofertą Wykonawcy), nie później niż 15 dni roboczych od dnia zawarcia umowy.
6. w zakresie wymienionym w pkt. 2 lit. B ppkt 3:

- dla projektu wdrożeniowego w terminie do 10 dni od dnia zawarcia Umowy,

- dla dokumentacji powykonawczej w terminie do 20 dni od dnia uruchomienia środowiska.

1. w zakresie wymienionym w pkt. 2 lit. A ppkt 4 lub w pkt 2 lit. B ppkt 4 w okresie do 04.09.2025 od dnia zawarcia Umowy, lub do wyczerpania puli roboczogodzin, w zależności, które zdarzenie nastąpi wcześniej
2. w zakresie wymienionym w pkt. 2 lit. B ppkt 5 – w okresie 3 miesięcy od dnia zawarcia Umowy;
3. w zakresie wymienionym w pkt 2 lit. A i lit. B ppkt 2 – w okresie do 04.09.2025 od dnia zawarcia Umowy.
   1. **MIEJSCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA**
4. Miejscem realizacji przedmiotu zamówienia jest Ministerstwo Sprawiedliwości w Warszawie przy ul. Czerniakowskiej 100.
5. Zamawiający zastrzega sobie prawo do zmiany lokalizacji urządzeń w trakcie trwania Umowy, wynikającej ze zmian organizacyjnych Zamawiającego, w tym m.in. w związku ze zmianą siedziby Zamawiającego lub zmianą miejsca realizacji przedmiotu zamówienia w obrębie województwa mazowieckiego, po pisemnym zawiadomieniu Wykonawcy, na co najmniej 5 dni przed terminem zmiany.
6. Zamawiający zastrzega sobie prawo do zmiany miejsca umieszczenia urządzeń będących przedmiotem zamówienia, przy czym nowa lokalizacja nie będzie wykraczała poza obręb województwa mazowieckiego.
7. Zamawiający wymaga realizacji zgłoszeń w miejscu lokalizacji sprzętu.
8. Zamawiający nie dopuszcza realizacji serwisu i wsparcia środowiska oraz napraw sprzętowych poza miejscem lokalizacji środowiska.
9. Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.
   1. **SERWIS I WSPARCIE TECHNICZNE**
10. Wykonawca nie później niż w terminie 10 dni od dnia zawarcia Umowy, ma obowiązek przekazać Zamawiającemu w formie pisemnej dokument „Instrukcja zgłaszania, obsługi i eskalacji zgłoszeń serwisu", zawierający:
11. instrukcje zgłaszania awarii;
12. szczegółowy opis procedury eskalacji zawierającej co najmniej dodatkowy numer telefonu i adres e-mail (pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub braku reakcji na zgłoszenie);
13. dane Wykonawcy - adresy, numery telefonów, adresy poczty elektronicznej;
14. instrukcje dotyczące przeglądania statusu umowy oraz urządzeń nią objętych;
15. instrukcje dotyczące pobierania poprawek i nowych wersji oprogramowania ze strony internetowej dla urządzeń i oprogramowania bez ponoszenia dodatkowych kosztów;
16. wzór Raportu z naprawy urządzenia.

Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe procedury. Przekazane przez Wykonawcę instrukcje i procedury podlegają akceptacji Zamawiającego. Zamawiający może zgłosić uwagi i poprawki do instrukcji i procedur przekazanych przez Wykonawcę, a Wykonawca jest zobowiązany do ich niezwłocznego uwzględnienia i przedstawienia do ponownej akceptacji przez Zamawiającego.

1. W przypadku jakichkolwiek zmian danych, o których mowa jest powyżej, w tym danych, o których mowa w ppkt. 1 lit. c, Wykonawca niezwłocznie poinformuje o tym Zamawiającego pisemnie. Instrukcje, o których mowa powyżej, nie mogą być sprzeczne lub niezgodne z postanowieniami Umowy.
2. Zgłoszenie awarii będzie dokonywane poprzez:
3. zgłoszenie telefoniczne,
4. serwis www. udostępniony przez Wykonawcę,
5. pocztę elektroniczną.

W przypadku dokonania zgłoszenia telefonicznego, Zamawiający potwierdzi je z wykorzystaniem serwisu www. udostępnionego przez Wykonawcę lub za pomocą poczty elektronicznej.

1. Wykonawca będzie przyjmował zgłoszenia awarii lub konsultacji technicznych w ramach serwisu i wsparcia technicznego całodobowo - 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.
2. Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia awarii w terminie do 60 minut od jego zgłoszenia na adres poczty elektronicznej [..................](mailto:popd@ms.gov.pl) lub telefonicznie - na numer podany podczas rejestracji zgłoszenia. W przypadku braku potwierdzenia zgłoszenia awarii, po upływie 60 minut od zgłoszenia, Zamawiający wdroży procedurę eskalacji zgłoszenia.
3. Konsultacje techniczne w ramach wsparcia technicznego mogą być przeprowadzone pomiędzy Wykonawcą a Zamawiającym osobiście, telefonicznie lub za pomocą poczty elektronicznej.
4. Wykonawca jest zobowiązany do zapewnienia Zamawiającemu możliwości bieżącego śledzenia statusu zgłoszenia serwisowego za pośrednictwem co najmniej strony www – Wykonawca przekaże Zamawiającemu za pomocą poczty e-mail wszystkie niezbędne informacje, w tym login i hasło, niezbędne do śledzenia statusu zgłoszenia, nie później niż w ciągu 3 dni od dnia zawarcia Umowy.
5. Wykonawca będzie realizował zgłoszenia awarii w następujący sposób:
6. awaria krytyczna, tj. niedostępność systemu dla wszystkich użytkowników: **czas reakcji do 4 godziny od chwili zgłoszenia awarii** przez Zamawiającego, **czas naprawy awarii** (przywrócenia funkcjonalności systemu) **do** **12 godzin** od chwili zgłoszenia awarii przez Zamawiającego, bez względu na to, czy zgłoszenie zostało potwierdzone czy nie;
7. awaria niekrytyczna (niepowodująca niedostępności systemu): **czas reakcji do 4 godziny** od chwili zgłoszenia awarii przez Zamawiającego, **czas naprawy awarii** (przywrócenia funkcjonalności systemu) **do 72 godzin** od chwili zgłoszenia awarii niekrytycznej przez Zamawiającego, bez względu na to, czy zgłoszenie zostało potwierdzone czy nie.
8. W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z ppkt. 8:
9. Zamawiający ma prawo bez oddzielnego wyroku sądu wypożyczyć, zainstalować i uruchomić urządzenie zastępcze, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do żądania kary umownej i odszkodowania.
10. Zamawiający ma prawo zlecić innemu podmiotowi naprawę urządzenia, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do żądania kary umownej i odszkodowania.
11. W ramach usunięcia awarii Zamawiający dopuszcza możliwość wymiany przez Wykonawcę po uzgodnieniu z Zamawiającym poszczególnych elementów lub podzespołów urządzenia lub całego urządzenia na fabrycznie nowe, wolne od wad, takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie. Postanowienie ppkt. 11 stosuje się odpowiednio.
12. W przypadku, gdy w wyniku usuwania awarii Wykonawca zapewnił urządzenie zastępcze, a naprawa urządzenia Zamawiającego trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/część urządzenia będzie podlegać naprawie trzykrotnie w okresie obowiązywania umowy i nastąpi kolejna (czwarta) awaria, Zamawiający ma prawo żądać wymiany urządzenia na nowe, takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie, co urządzenie podlegające wymianie. Wykonawca zobowiązany jest wymienić urządzenie w ciągu 30 dni od zgłoszenia takiego żądania przez Zamawiającego. Dostarczone w ramach wymiany urządzenie musi być wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą, wolne od wad, fabrycznie nowe - bez śladów używania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczypospolitej Polskiej i dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. W przypadku wymiany urządzenia na nowe Wykonawca sporządzi protokół z wymiany urządzenia dostarczonego w ramach wymiany - Protokół Wymiany Sprzętu lub Licencji. Z chwilą podpisania protokołu na Zamawiającego przechodzi prawo własności nowego urządzenia.
13. Wykonawca każdorazowo dostarczy Zamawiającemu Raport z naprawy urządzenia, zawierający datę i godzinę zgłoszenia, przystąpienia do realizacji zgłoszenia, datę i godzinę usunięcia awarii, informację co było przedmiotem naprawy. Raporty z naprawy urządzenia będą przygotowywane przez Wykonawcę w języku polskim i przekazywane Zamawiającemu w formie pisemnej (papierowej) do siedziby Biura Cyberbezpieczeństwa. Zamawiający w terminie 3 dni roboczych od otrzymania Raportu z naprawy urządzenia dokonuje jego akceptacji lub zgłasza do niego uwagi, przesyłając je na adres poczty elektronicznej Wykonawcy. Wykonawca zobowiązany jest w terminie 2 dni roboczych od dnia otrzymania uwag do ich uwzględniania i przedstawienia poprawionej wersji Raportu z naprawy urządzenia, a w razie nieuwzględnienia uwag – do pisemnego uzasadnienia swojego stanowiska. W takim przypadku stosuje się postanowienie zdania poprzedniego.
14. W przypadku awarii dysku twardego, powodującej konieczność jego wymiany, uszkodzony dysk pozostanie u Zamawiającego. Koszty dysków twardych wymienianych z powodu ich awarii ponosi Wykonawca.
15. W celu zapewnienia kompatybilności i poprawności eksploatacji infrastruktury informatycznej posiadanej przez Zamawiającego, Zamawiający wymaga, aby w ramach wsparcia Wykonawca zapewnił:
16. dostęp do portali internetowych zawierających narzędzia wsparcia elektronicznego urządzeń i oprogramowania stanowiącego przedmiot umowy oraz zapewni możliwość korzystania z nich przez cały okres obowiązywania Umowy, w tym informacji o statusie Umowy oraz o urządzeniach nią objętych
17. przeszukiwanie portalu internetowego z bazą wiedzy dotyczącej urządzeń i oprogramowania stanowiącego przedmiot umowy,
18. pobieranie z serwera WWW lub FTP poprawek i aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego urządzeń (firmware) stanowiących przedmiot umowy, umożliwiających jego instalację, udostępnionych w okresie trwania umowy; pobieranie tych aktualizacji musi być zgodne z zasadami licencjonowania producenta oprogramowania,
19. W okresie trwania Umowy Zamawiający ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów (np. modułów optycznych itp.) oraz rozbudowy urządzeń oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego posiadanych urządzeń (firmware) zgodnie z zasadami wiedzy technicznej przez Zamawiającego lub podmiot zewnętrzny, któremu zleci te prace Zamawiający.
20. Oferowane produkty w ramach zamówienia będą pochodziły z oficjalnego kanału dystrybucyjnego na terenie Unii Europejskiej.
21. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień poprzedzający dzień składania ofert.
22. Zamawiający w ramach wsparcia technicznego musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną do Wykonawcy, bez ograniczeń, co do liczby zgłoszeń.
23. Rozszerzenie licencji o kolejne funkcjonalności nie może powodować utraty praw gwarancyjnych do oprogramowania oraz nie może wymagać zgody Wykonawcy lub producenta licencji.
24. Zamawiający wymaga, aby Wykonawca w ramach serwisu na wniosek Zamawiającego aktualizował firmware urządzeń.
25. Wykonawca zapewni serwis dla wszystkich dostarczonych urządzeń oraz licencji. Wykonawca zobowiązany jest do udzielenia gwarancji jakości oraz rękojmi dla dostarczonych urządzeń i licencji.
26. Okres serwisu oraz gwarancji i rękojmi nie będzie krótszy niż do dnia zakończenia umowy.

**ROZDZIAŁ II. WYMAGANIA WSPÓLNE ZARÓWNO DLA OFERTY PODSTAWOWEJ JAK I WARIANTOWEJ (WSKAZANYCH W ROZDZIALE I PKT 2 LIT. A I B)**

1. **W zakresie Umowy Wykonawca zobowiązany jest do:**
   1. Migracji całej konfiguracji z dotychczasowych urządzeń Zamawiającego
   2. Migracji lub wdrożenia od nowa wszystkich polityk skonfigurowanych na obecnych urządzeniach Zamawiającego
   3. W przypadku zaoferowania rozwiązania wariantowego (oferty wariantowej) migracja, którą musi przeprowadzić Wykonawca z obecnych urządzeń zamawiającego   
      do nowo zaoferowanych urządzeń musi odbyć się w maksymalnie dwóch przerwach serwisowych po 1 godzinie każda z nich.
2. **Asysta techniczna eksperta - wymagania**
3. Wykonawca będzie świadczyć usługi asysty technicznej eksperta dla całości rozwiązania wdrożonego przez Wykonawcę do końca trwania umowy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji oraz Uruchomienia Środowiska lub do wyczerpania puli roboczogodzin usług asysty technicznej eksperta, w zależności, które zdarzenie nastąpi wcześniej;
4. W roboczogodzinę usługi asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie, tzn. nie ma znaczenia, ile osób będzie świadczyło usługę asysty technicznej eksperta w danej roboczogodzinie/roboczogodzinach u Zamawiającego. Rozliczenie roboczogodzin usług asysty technicznej eksperta odbywać się będzie miesięcznie za faktycznie wykorzystane roboczogodziny na podstawie Protokołów Odbioru Usług Asysty Technicznej Eksperta. Do roboczogodzin usługi asysty technicznej eksperta nie wlicza się godzin usług wykonywanych w ramach gwarancji lub rękojmi oraz serwisu.
5. Zakres czynności wykonywanych w ramach usług asysty technicznej eksperta nie może być tożsamy z zakresem objętym serwisem i wsparciem technicznym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu i wsparcia technicznego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.
6. Zlecenia w ramach usługi asysty technicznej eksperta będą dotyczyły w szczególności rozwoju i modyfikacji sprzętu, zaawansowanej konfiguracji sprzętu, wsparcia w zakresie utrzymania sprzętu, będą zgłaszane przez Zamawiającego.
7. Zamawiający będzie przekazywać Wykonawcy zlecenia w ramach usługi asysty technicznej eksperta, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
8. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż 1 dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia wraz z rozbiciem na poszczególne czynności.
9. Zamawiający może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
10. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
11. Rozliczenie usługi asysty technicznej eksperta odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Wykonawcę i Zamawiającego, Protokołów Odbioru Usług Asysty Technicznej Eksperta, raz na miesiąc, w którym była świadczona usługa.
12. Zamawiający dopuszcza realizację wsparcia eksperckiego zdalnie, z zastrzeżeniem lit. k)
13. Na wniosek Zamawiającego Wykonawca zobowiązany jest do zapewnienia obecności eksperta we wskazanym miejscu na terenie Warszawy lub w miejscu lokalizacji środowiska.
14. **Projekt wdrożeniowy i dokumentacja powykonawcza – wymagania**

Wykonawca opracuje projekt wdrożeniowy oraz dokumentację powykonawczą dla oferowanego systemu i rozbudowy urządzeń zawierające co najmniej:

1) Dla projektu wdrożeniowego:

1. diagramy połączeniowe dla wszystkich komponentów sieci Zamawiającego powiązanych   
   z przedmiotem zamówienia,
2. konfigurację przewidzianą dla wszystkich urządzeń oraz propozycje zmian dla istniejących urządzeń połączonych z przedmiotem zamówienia,
3. harmonogram wdrożenia,
4. koncepcję testów następujących po wszystkich etapach wdrożenia,
5. plan awaryjny „backout” dla każdego kroku wdrożenia,
6. koncepcję testów redundancji wykonywanych po zakończeniu wdrożenia.

2) Dla dokumentacji powykonawczej:

1. diagramy połączeń,
2. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu,
3. pełne konfiguracje urządzeń,
4. wyniki testów redundancji.

**Rozdział III. WYMAGANIA DLA OFERTY PODSTAWOWEJ OKREŚLONEJ W ROZDZIALE I, PKT 2. LIT. A (NIE DOTYCZY OFERTY WARIANTOWEJ OKREŚLONEJ W Rozdziale I pkt. 2 lit. B)**

**1. Przedłużenie działania modułu Trellix AX:**

Urządzenie wymienione w Rozdziale II w pkt. 1, obecne w sieci Zamawiającego, w związku z wygaśnięciem licencji oraz zmiany platformy sprzętowej powinno zostać zastąpione przez serwer fizyczny Trellix AX 5600 wraz z wymaganymi subskrypcjami i licencjami. Licencje oraz subskrybcje muszą zawierać wsparcie, aktualizacje sygnatur oraz licencje uprawniające Zamawiającego do pozostawienia dysków w razie ich awarii.

Urządzenia wymienione w Rozdziale I pkt 2A w ppkt. 2 lit. c, d i e, obecne w infrastrukturze Zamawiającego, powinny zostać zintegrowane z nowymi modułami.

**2. Przedłużenie działania modułu Trellix CM:**

Rozwiązanie wymienione w Rozdziale II w pkt. 2, obecnie wykorzystywane przez Zamawiającego, w związku z wygaśnięciem licencji oraz zmiany z SaaS na OnPremise powinno zostać zastąpione przez serwer fizyczny Trellix CM 4600 wraz z wymaganymi subskrypcjami i licencjami. Licencje oraz subskrypcje muszą zawierać wsparcie, aktualizacje sygnatur oraz licencje uprawniające Zamawiającego do pozostawienia dysków w razie ich awarii.

Urządzenia wymienione w Rozdziale I pkt 2A w ppkt. 2 lit c, d i e , obecne w infrastrukturze Zamawiającego, powinny zostać zintegrowane z nowymi modułami.

**ROZDZIAŁ IV. WYMAGANIA DLA OFERTY WARIANTOWEJ OKREŚLONEJ W ROZDZIALE I, PKT 2. LIT. B (NIE DOTYCZY OFERTY PODSTAWOWEJ OKREŚONEJ W ROZDZIALE I PKT. 2 LIT. A)**

**W przypadku zaoferowania rozwiązania wariantowego należy dostarczyć sprzęt oraz licencje o następujących parametrach:**

1. **Moduł AntyMalware dla poczty e-mail:**
   * + 1. Analiza dynamiczna w maszynach wirtualnych i wykrywanie w załącznikach ataków nie może opierać się na analizie w rozwiązaniach typu chmurowego (poza infrastrukturą Zamawiającego), lecz na urządzeniu zainstalowanych w infrastrukturze Zamawiającego. Analiza ataku musi odbywać się za pomocą dynamicznej analizy zachowania kodu umożliwiających równoczesną analizę zagrożenia w różnych wersjach systemu operacyjnego i aplikacjach.
       2. Architektura Modułu AntyMalware musi składać się z:
          1. Centralnego serwera zarządzania Modułu AntyMalware, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa dodatkowej ochrony poczty elektronicznej i raportowania oraz
          2. Analizatorów dynamicznych służących do wykonywania głębokiej analizy w piaskownicy (sandbox) w środowisku maszyn wirtualnych oraz wykrywania zawansowanych zagrożeń poczty elektronicznej oraz pracujących w trybie MTA (ang. Mail Transfer Agent).
       3. Każdy analizator dynamiczny musi być przekazany w postaci urządzenia fizycznego Producenta. Urządzenie MUSI działać w oparciu o dedykowane platformy sprzętowe (appliance) przekazane przez Wykonawcę oferowanego rozwiązania Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
       4. Analizatory dynamiczne Modułu AntyMalware muszą działać w postaci klastra nadmiarowego. Klaster odporny na awarie musi być przekazany jednej lokalizacji (fizyczna lokalizacja; dwa urządzenia w lokalizacji dla całego Modułu ). sumarycznie minimum 2 analizatory.
       5. Integracja z posiadanym serwerem centralnego zarządzania musi umożliwiać przynajmniej zarządzanie alertami pochodzącymi z analizatorów dynamicznych, możliwość zwalniania z kwarantanny zatrzymanych wiadomości, zarządzanie politykami bezpieczeństwa na wszystkich klastrach analizatorów jednocześnie i możliwość wykonywania bezpośredniej aktualizacji oprogramowania analizatorów.
       6. Moduł AntyMalware musi integrować się z system SIEM i zasilać go wszelkimi wykrytymi zdarzeniami bezpieczeństwa
       7. Moduł AntyMalware musi być przekazany w postaci fizycznych urządzeń wraz z Oprogramowaniem i wszystkimi niezbędnymi licencjami (z uwzględnieniem licencji niezbędnych dla maszyn wirtualnych w SandBox, w tym posiadanych przez Zamawiającego programów MS Windows, MacOS, MS Office).
       8. Każdy z analizatorów dynamicznych musi mieć wydajność analizy minimum 8 tys. przychodzących wiadomości email na godzinę, w tym minimalnie 600 unikalnych załączników do email na godzinę.
       9. Równoległa analiza dynamiczna musi być wykonywana na maszynach wirtualnych w różnych wersjach systemu operacyjnego (co najmniej Microsoft Windows 7 posiadanego przez Zamawiającego (w wersjach zarówno 32 jak i 64 bit), co najmniej Microsoft Windows 10 64-bit, Mac OS, CentOS posiadanych przez Zamawiającego.
       10. Każdy z analizatorów dynamicznych musi być wyposażony w co najmniej 2 interfejsy monitorujące ruch poczty email oraz dedykowany port zarządzający do podłączenia do osobnego segmentu sieci.
       11. Analizator dynamiczny musi umożliwiać wdrożenie w następujących trybach:
           1. in-line - urządzenie działa jako MTA będąc pośrednikiem w ruchu email do serwerów poczty,
           2. monitorowania - przez podłączenie do portu SPAN przełącznika sieciowego lub do urządzenia typu TAP,
           3. BCC – do urządzenia dociera kopia oryginalnych maili poprzez protokół SMTP (generowanych przez bramkę pocztową lub serwer pocztowy).
       12. Analizator dynamiczny musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa redundantne dyski pracujące w RAID.
       13. Analizator dynamiczny musi zapewnić wykrywanie zaawansowanych ataków przenoszonych w załącznikach poczty elektronicznej oraz kontrolę adresów URL umieszczanych w treści wiadomości oraz analizę samej wiadomości, przy czym:
           1. po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie złośliwego email w kwarantannie,
           2. po wykryciu nieznanego wcześniej adresu URL prowadzącego do pliku musi być możliwe automatyczne nawiązanie połączenia przez urządzenie do Internetu, pobranie pliku i przeanalizowanie go, a następnie w razie wykrycia zagrożenia, wygenerowanie alertu i zatrzymanie wiadomości email w kwarantannie,
           3. po wykryciu nieznanego wcześniej adresu URL nie prowadzącego do obiektu musi być możliwe automatyczne przekazanie go do centralnego systemu zarządzania celem korelacji z alertami generowanymi przez inne analizatory dynamiczne.
       14. W przypadku nieznanych wcześniej adresów URL Moduł musi umożliwiać administratorowi zdefiniowanie czasu wstrzymania dostarczenia wiadomości, tak aby możliwe było ukończenie zaawansowanej, przedłużonej analizy URL po stronie dostawcy rozwiązania.
       15. Cała analiza załączników w celu wykrycia ataków w poczcie email musi odbywać się w infrastrukturze Zamawiającego.
       16. Moduł AntyMalware na potrzeby analizy dynamicznej musi wykorzystywać dedykowane środowisko wirtualne (hypervisor), a nie standardowe dostępne na rynku rozwiązania jak VMware, MS Hyper-V czy też Virtual Box, w celu utrudnienia wykrycia rodzaju środowiska wirtualnego przez podlegające analizie dynamicznej próbki złośliwego oprogramowania.
       17. Moduł AntyMalware musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty email niezależnie od użytego rozszerzenia pliku.
       18. Moduł AntyMalware musi analizować i blokować niebezpieczne treści dla załączników takich jak:
           1. plików wykonywalnych (EXE,MSI),
           2. dokumentów (PDF, RTF),
           3. plików Java (JAR, JS, JSE),
           4. plików z pakietu MS Office,
           5. plików multimedialnych (FLASH),
           6. plików skompresowanych (RAR, ZIP, 7ZIP, GZIP, SFX),
           7. skrótów MS Windows (LNK),
           8. plików www (HTML, HTM),
           9. plików z bibliotekami (DLL),
           10. plików zawierających skrypty (Powershell, VBS, BAT, CMD, VBE, VB, COM).
       19. Moduł AntyMalware musi zostać wdrożony w trybie "in-line" w trybie aktywnego blokowania zainfekowanych wiadomości e-mail i umieszczać je w lokalnej kwarantannie
       20. Moduł AntyMalware musi dodawać oznaczenia (X header) do nagłówków wiadomości e-mail zależnie od akcji podjętej przez Moduł analizy (m.in. e-mail przeskanowany bez wykrytego zagrożenia, e-mail zawiera kod złośliwy) do wykorzystania przez inne systemy ochrony Zamawiającego i analizy wstecznej.
       21. Moduł AntyMalware musi automatycznie tworzyć reguły umożliwiające blokowanie zagrożeń na podstawie:
           1. wyników analizy malware wykonanej na danym urządzeniu,
           2. danych przekazanych z centralnego systemu zarządzania, pochodzących z wyników analizy wykonanych na innych urządzeniach Modułu AntyMalware w środowisku Zamawiającego,
           3. danych dostępnych z centralnego repozytorium Producenta oferowanego rozwiązania wariantowego (centrum reputacyjne Producenta).
       22. Moduł AntyMalware musi umożliwiać stosowanie własnych reguł opisujących parametry z nagłówków wiadomości e-mail (header) i na tej podstawie wykrywać groźne wiadomości pocztowe.
       23. Moduł AntyMalware musi posiadać dodatkowe, uzupełniające mechanizmy chroniące pocztę e-mail Zamawiającego przed atakami:
           1. phishing / spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających),
           2. impersonation (CEO fraud) - kompromitacja kadry zarządzającej w celu kradzieży informacji,
           3. infekcją kodu JavaScript, VBScript,
           4. spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.
           5. z opóźnionym startem – w których obiekty niebezpieczne (załączniki/URL) zostają aktywowane już po dostarczeniu wiadomości – w tym wypadku Moduł musi generować alerty o niebezpiecznych wiadomościach e-mail, które zostały dostarczone do odbiorców (atak retroaktywny);
       24. Moduł AntyMalware musi umożliwiać deszyfrację załączników przesyłanych przez pocztę e-mail Zamawiającego przy użyciu listy najczęściej używanych haseł lub inteligentnego wyszukiwania haseł w treści e-maila, w tym z opcją OCR hasła przesłanego w obrazku. Lista haseł MUSI mieć możliwość dodania haseł specyficznych dla języka polskiego z polskimi znakami.
       25. Moduł AntyMalware musi posiadać możliwość konfiguracji środowisk wirtualnych analizy dynamicznej co najmniej w zakresie: nazwy domeny, nazwy użytkownika, folderów użytkowników, ostatnio otwartych plików, historii przeglądania stron www w przeglądarce internetowej, kont FTP, Outlook i Skype w celu utrudnienia wykrycia przez analizowany malware.
       26. Moduł AntyMalware musi umożliwiać analizę wiadomości e-mail w trybie "LIVE", to jest z możliwością połączenia malware detonowanego w środowisku wirtualnym z zewnętrznym łączem internetowym. Łącze to musi stanowić separowany link do Internetu („brudny Internet”) konfigurowany na dedykowanym porcie fizycznym Urządzenia.
       27. W wyniku analizy Moduł musi zapewniać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy wiadomości e-mail. Wśród danych muszą się znaleźć co najmniej:
           1. adres nadawcy i adres odbiorcy,
           2. analiza nagłówka wiadomości (header)
           3. body wiadomości,
           4. wyniki analizy załączników i adresów URL,
           5. informacje kontekstowe na temat wykrywanego zagrożenia malware, adware, spyware,
           6. funkcja skrótu (HASH), przynajmniej MD5 i SHA256
       28. Moduł AntyMalware musi zapewniać dostęp do sekwencyjnego (krok po kroku) zapisu zmian wykonywanych przez analizowany niebezpieczny załącznik z wiadomości pocztowej: w rejestrze, procesach, systemie plików, sposobie startu systemu, próby nawiązania połączenia sieciowego (wraz z zapisem tych prób w postaci plików PCAP dostępnych w GUI urządzenia).
       29. Moduł AntyMalware musi posiadać graficzne przedstawienie zmian wykonywanych przez obiekt z wiadomości pocztowej (przekazany bezpośrednio lub poprzez adres URL) po analizie w środowisku wirtualnym w postaci grafu powiązań wykonywanych czynności.
       30. Moduł AntyMalware musi być zoptymalizowany pod kątem minimalizacji liczby przypadków false-positive (błędne wykrycie zagrożenia w poprawnej wiadomości e-mail).
       31. Moduł AntyMalware musi posiadać dodatkowy mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
           1. skrypty przesyłane w wiadomości e-mail,
           2. pliki wykonywalne przesyłane w załączniku lub URL,
           3. dokumenty MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym,
           4. nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO,
           5. wiadomości e-mail ze skróconymi linkami (tiny URL),
           6. dokumenty MS OFFICE z flash,
           7. pliki JAR,
           8. hasła z formularzy przesyłanych w formie HTTP request,
           9. zaszyfrowane pliki PDF,
           10. pliki typu wygaszacz ekranu,
           11. nieznanych plików konfiguracyjnych. SettingContent-ms.
           12. zaszyfrowane dokumenty MS Office
           13. Dokumenty MS Office z obiektami Embedded Object
           14. Dokumenty PDF, HWP lub MS Office z aktywnością sieciową
           15. pliki MS Office z makrem tworzącym plik wykonywalny
           16. uszkodzone pliki wykonywalne PE
           17. obiekty próbujące wykryć rozwiązania AV/Firewall za pomocą WMI
           18. pliki z niezgodnym rozszerzeniem (innym niż w magic byte)
           19. dokumenty Office z zagnieżdżonymi obiektami SWF
       32. Moduł AntyMalware musi mieć możliwość przepisania adresów URL w przesyłanej wiadomości tak aby pomimo kliknięcia użytkownik nie był przekierowany do potencjalnie złośliwej treści. W wypadku kiedy adres URL będzie złośliwy, przedstawiony ekran informujący o blokadzie musi umożliwiać dostosowanie prezentowanych użytkownikowi komunikatów do wymagań Zamawiającego (grafika i tekst z informacją o blokadzie w języku polskim).
       33. Moduł AntyMalware musi umożliwiać konfigurację reguł blokujących i dopuszczających bazując na wyrażeniach regularnych, w celu modyfikacji ochrony w zakresie: adresu e-mail nadawcy, domeny nadawcy, adresu IP nadawcy i adresu e-mail odbiorcy (zarówno „whitelista” jak i „blacklista”).
       34. Moduł AntyMalware musi mieć zaimplementowany mechanizm wyszukiwania analizowanych wiadomości pocztowych i filtry wyszukujące co najmniej na: adres e-mail odbiorcy, adres e-mail nadawcy, temat wiadomości, URL, załącznik.
       35. Moduł AntyMalware musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości e-mail i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
       36. Moduł AntyMalware musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie Yara.
       37. Moduł AntyMalware musi umożliwiać generowanie raportów zawierających co najmniej:
           1. statystyki wykrytych alertów, typy i opis wykrytych zagrożeń, akcje podjęte w związku z wykrytym zagrożeniem,
           2. statystyki przeanalizowanych wiadomości e-mail,
           3. statystyki analizowanej poczty, z podziałem na poszczególne godziny, w celu oceny obciążenia systemu
       38. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
       39. Moduł AntyMalware musi generować automatycznie (za pomocą wbudowanej funkcji) raport z analizy dynamicznej, zarówno dla graficznej reprezentacji wyniku analizy jaki i wykonanych po sobie czynności krok po kroku.
       40. Moduł AntyMalware musi umożliwiać przesyłanie do zewnętrznego odbiorcy (typu SIEM/Log Collector) metadanych o wszystkich procesowanych wiadomościach e-mail (szkodliwe i nieszkodliwe); eksport musi być możliwy za pomocą minimum rsyslog oraz formatu json (http listener).
       41. Metadane muszą uwzględniać takie informacje, jak: rozmiar wiadomości, werdykt analizy, domenę nadawcy, nagłówki wiadomości (header), pola to/cc/bcc, temat, messageid; jeśli wiadomość zawiera załącznik, to dodatkowo metadane muszą opisywać takie parametry jak: rozmiar załącznika, sumy kontrole MD5 oraz SHA256, nazwę załącznika oraz werdykt analizy.
       42. Moduł AntyMalware musi zapewniać system powiadamiania o przeciążeniach wynikających ze zbyt dużej liczby wiadomości e-mail do analizy. Gdy liczba wiadomości e-mail w kolejce oczekiwania na analizę osiągnie 30% progu przeciążenia, Moduł musi generować powiadomienie o statusie ostrzegawczym. Gdy liczba wiadomości e-mail w kolejce osiągnie 70% progu przeciążenia, Moduł musi generować powiadomienie o statusie krytycznym.
       43. Alarmy generowane przez system na bazie analizy dynamicznej w maszynach wirtualnych muszą obejmować mapowanie MITRE, wskazujące na technikę/techniki MITRE zidentyfikowane w ramach analizy danej próbki.
2. **Moduł Sandbox:**
   * + 1. Zamawiający wymaga, aby sandbox (serwer) jako element Systemu posiadał wydajność umożliwiającą wykonanie co najmniej 9000 analiz dziennie.
       2. Zamawiający wymaga, aby analiza próbek była realizowana w izolowanym środowisku funkcjonującym na dedykowanym, fizycznym urządzeniu typu appliance (APP).
       3. Zamawiający wymaga, aby analiza próbek była realizowana w całości w infrastrukturze Zamawiającego, gdzie cały proces analizy musi się odbywać w tym środowisku wirtualnym. Nie jest dopuszczalne wysyłanie analizowanych plików/obiektów poza to środowisko (dopuszczalne jest jedynie wysyłanie cech charakterystycznych np. sum kontrolnych plików).
       4. Zamawiający wymaga, aby sandbox służący do analizy próbek malware był wyposażony w maszyny wirtualne wykonujące równolegle analizę dynamiczną próbek malware (w tym także adresów URL) w różnych wersjach systemu operacyjnego i aplikacji jednocześnie (co najmniej: posiadane przez Zamawiającego systemy Windows XP, Windows 7 SP1, Windows 10, MacOS) oraz różnych aplikacji i ich różnych wersji zainstalowanych w tych systemach (co najmniej posiadane przez Zamawiającego FireFox, Chrome, Adobe Reader, Java, MS Office). Wszystkie niezbędne licencje na systemy operacyjne i aplikacje muszą być dostarczone wraz z oferowanym Systemem.
       5. Zamawiający wymaga, aby na potrzeby analizy próbek malware (tj. uruchamiania plików w izolowanym środowisku) element Sandbox zapewniał co najmniej:
3. by środowisko, w jakim jest wykonywana analiza dynamiczna, posiadało mechanizmy utrudniające jego wykrycie przez analizowany malware,
4. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku posiadały mechanizmy symulacji pracy realnego użytkownika,
5. możliwość nawiązania połączenia sieciowego badanej próbki umożliwiającego pobranie dodatkowej zawartości z Internetu; kontaktu z serwerami C&C, itp. (celem śledzenia działania badanej próbki w sieci),
6. możliwość parametryzacji środowisk wirtualnych w zakresie: nazwy domeny, folderów użytkowników, ostatnio otwartych plików, języka systemu operacyjnego, wpisania hasła w celu automatycznego odszyfrowania przekazywanej do analizy próbki malware,
7. możliwość ręcznego wysyłania próbek (plików/obiektów) jak również adresu URL do analizy dynamicznej z poziomu konsoli zarządzającej Systemu i poprzez REST API oraz możliwość prezentacji wyników tej analizy.
   * + 1. Zamawiający wymaga, aby element Systemu służący do analizy próbek malware umożliwiał generowanie raportów zawierających co najmniej wyniki analiz i statystyki przeanalizowanych próbek. Raporty powinny mieć możliwość eksportu na przykład do formatu CSV lub XML wraz z możliwością ustalenia okresu dla generowanego raportu (przykładowo: ostatnie 24 godziny, ostatnie 7 dni, ostatnie 30 dni).
       2. Sandbox musi umożliwiać integrację z konsolą do zarządzania Systemem w zakresie przesyłania wskaźników kompromitacji IoC, raportowania zdarzeń, konfiguracji ustawień systemu, aktualizacji oraz weryfikacji aktualnego stanu urządzenia.
8. **Moduł ochrony udziałów sieciowych:**
   * + 1. W ramach dostawy modułu AntyMalware musi być także przekazany analizator zasobów plikowych, pozwalający na masową detonacje i weryfikacje plików, obiektów przechowywanych na serwerach plikowych i macierzach. Analizator plikowy ma za zadanie wykonywać analizę dynamiczną w środowisku maszyn wirtualnych plików pochodzących m.in. z komunikacji e-mail (załączniki) które nie zostały wykryte na etapie przesyłania wiadomości, a mogą przenosić złośliwy kod, malware itp.
       2. Analizator plikowy musi mieć możliwość analizy repozytoriów plikowych w celu znalezienia złośliwego oprogramowania (typu malware, exploit, itp).
       3. Wykrywanie ataków musi odbywać się przez dedykowane fizyczne urządzenie przeznaczone do instalacji w szafie w posiadanej przez Zamawiającego RACK.
       4. Analizator plikowy musi być wyposażone w co najmniej 4 interfejsy miedziane 1Gb/s.
       5. Analizator plikowy musi posiadać minimum dwa redundantne zasilacze i co najmniej dwa dyski redundantne pracujące w RAID.
       6. Analizator plikowy musi mieć wydajność umożliwiającą skanowanie co najmniej 60 000 analiz unikalnych obiektów dziennie wykazanych w specyfikacji Producenta.
       7. Analizator plikowy musi wykonywać analizę dynamiczną (sandbox) w równoległym środowisku (uruchamianym jednocześnie) maszyn wirtualnych.
       8. Analizator plikowy musi działać w oparciu o dedykowane platformy sprzętowe (urządzenia fizyczne) przekazane przez Wykonawcę oferowanego rozwiązania Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
       9. Analizator plikowy musi wykonywać skanowanie udziałów plikowych: ciągłe, zaplanowane i na żądanie oraz poddawać kwarantannie złośliwe oprogramowanie odnalezione na zasobach plikowych
       10. Analizator plikowy musi umożliwiać tworzenie niezależnych skanowań (zadań skanowania) dla podłączonych repozytoriów plikowych (zasobów plikowych).
       11. Analizator plikowy musi mieć możliwość skanowania i filtrowania tylko wskazanych typów plików do skanowania.
       12. Analizator plikowy musi umożliwiać zatrzymanie i wznawianie skanowania.
       13. Analizator plikowy musi mieć możliwość przenoszenia niezłośliwych plików do wskazanego zasobu, a złośliwych plików do oddzielnego zasobu kwarantanny.
       14. Analizator plikowy musi być w stanie przywrócić plik do jego pierwotnej lokalizacji po zwolnieniu go z kwarantanny.
       15. Analizator plikowy musi być w stanie dostarczać raporty analityczne z informacjami o zachowaniu pliku - zaangażowanych procesach, dostępie do plików / zapisie na dysku, zmianach w rejestrze.
       16. Analizator plikowy musi oferować możliwość filtrowania zadania skanowania na podstawie typu pliku oraz daty modyfikacji.
       17. Analizator plikowy musi posiadać oprócz silnika analizy dynamicznej, silnik analizy statycznej.
       18. Analizator plikowy musi mieć możliwość analizy plików do 1024 MB. Maksymalny rozmiar plików, które będą skanowane, musi być konfigurowalny.
       19. Analizator plikowy musi mieć możliwość analizowania plików .eml (wiadomości e-mail zapisane do pliku)
       20. Analizator plikowy musi obsługiwać natywną integrację z posiadanego przez Zamawiającego programu Microsoft SharePoint w trybie online, aby zapewnić bezpieczne udostępnianie plików.
       21. Analizator plikowy musi wspierać skanowanie i ochronę dla następujących typów repozytoriów plikowych: CIFS, NFS, WebDAV, Secure WebDAV.
       22. Analizator plikowy musi mieć możliwość analizy malware w formatach co najmniej: JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, htm, ico, jar, , jpg, mov, mp4, pdf, png, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
       23. Funkcjonalność analizy obiektów musi realizować statyczną analizę (analizę cech) i dynamiczną analizę (analizę zachowania po uruchomieniu środowisku wirtualnym) podejrzanych obiektów zebranych z analizowanego ruchu.
       24. Analizator plikowy musi na potrzeby analizy dynamicznej wykorzystywać środowisko wirtualne (hypervisor), przy czym:
           1. środowisko, w jakim jest wykonywana analiza dynamiczna, musi posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware,
           2. maszyny wirtualne, w których wykonywana jest analiza zachowania ataku muszą posiadać mechanizmy symulacji realnego użytkownika (w tym co najmniej: ruchy myszą, historię odwiedzanych stron web, pliki cookies).
       25. Analizator plikowy musi posiadać możliwość konfiguracji środowisk wirtualnych co najmniej w zakresie: nazwy domeny, nazwy użytkownika, folderów użytkowników, ostatnio otwartych plików, historii przeglądania stron www w przeglądarce internetowej oraz kont FTP, Outlook i Skype w celu utrudnienia wykrycia przez analizowany malware.
       26. Analiza zachowania i cech ataku musi się odbywać z poziomu hypervisora – nie może być wymagane instalowanie dodatkowych procesów/agentów monitorujących wewnątrz maszyn wirtualnych.
       27. Maszyny wirtualne z różnymi systemami operacyjnymi i aplikacjami muszą być przekazane wraz z urządzeniami i okresowo aktualizowane przez Producenta i nie mogą wymagać dodatkowych licencji wymaganych do konfiguracji po stronie Zamawiającego.
       28. Sposób działania maszyn wirtualnych musi umożliwiać wykonanie analizy zachowania obiektów PDF, Java, MS Office z użyciem kilku wersji tych aplikacji bez uruchamiania dodatkowych maszyn wirtualnych.
       29. Analiza ataku musi umożliwiać wykrywanie zagrożeń typu kernel rootkit, code injection, DLL injection.
       30. W wyniku analizy analizator plikowy musi zapewniać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy. Wśród tych danych muszą się znaleźć co najmniej: adresy URL jeśli są związane z analizowanym malware, funkcje skrótu (hash) MD5 oraz wykryty plik malware.
       31. Analizator plikowy musi być zoptymalizowany pod kątem minimalizacji liczby przypadków false-positive (błędne wykrycie zagrożenia w poprawnym ruchu).
       32. Analizator plikowy musi umożliwiać wykrywanie wszystkich faz zaawansowanych ataków: exploit, dropper/malware, callback oraz lateral movement.
       33. Analizator plikowy wykonując analizę zagrożeń musi umożliwiać generyczne (bez wcześniejszej znajomości złośliwego kodu) wykrywanie ataków typu exploit, w tym nowych exploit, nie znanych wcześniej.
       34. Wykrywanie exploit musi się odbywać po analizie co najmniej takich formatów plików jak Java Script, zakodowany (obfuscated) Java Script, obiekty Flash, PDF, pliki graficzne, pliki multimedialne mp3/mp4, pliki MS Office, Java.
       35. Informacja o wykryciu fazy exploita musi być wskazana w zapisie sekwencyjnym z analizy dynamicznej ataku.
       36. Analizator plikowy musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
       37. Analizator plikowy musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie YARA.
       38. Analizator plikowy musi posiadać dodatkowy mechanizm wykrywania zdarzeń typu "prawdopodobny malware" (takich jak zaszyfrowane dokumenty w posiadanym przez Zamawiającego programie MS Office, zdegradowane pliki wykonywalne Windows PE, formularze web przekazujące hasła, pliki niewykonywalne umożliwiające komunikację do niestandardowego portu). Zdarzenia te muszą być konfigurowalne jako alert lub automatyczna kwarantanna.
       39. Analizator plikowy musi generować wynik analizy dynamicznej co najmniej do pliku PDF.
       40. Analizator plikowy musi umożliwiać tworzenie raportów ze szczegółami wykrytych alertów do formatów co najmniej JSON, CSV.
       41. Analizator plikowy musi umożliwiać tworzenie raportów z przeprowadzonych skanowań do formatu PDF zawierających co najmniej statystyki wykrytych zagrożeń.
       42. Analizator plikowy musi umożliwiać przegląd nowych funkcjonalności po aktualizacji oprogramowania.
       43. Analizator plikowy musi umożliwiać przegląd statystyki danych zebranych na poszczególnych interfejsach urządzenia.
       44. Analizator plikowy musi umożliwiać tworzenie raportów uruchamianych cyklicznie (godzinowo/dzienne/tygodniowo/miesięcznie) zawierających co najmniej wykryte zagrożenia. Raporty te muszą być dostarczane przez email.
       45. Analizator plikowy musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły RSYSLOG, SMTP, SNMP, HTTP.
       46. Analizator plikowy musi integrować się bezpośrednio z posiadanym przez zamawiającego modułem centralnego zarządzania FireEye CM co najmniej w oparciu o wymianę artefaktów ataku wykrytych w skanowanych repozytoriach plików oraz musi umożliwiać przegląd generowanych alertów,
       47. Analizator plikowy musi umożliwiać korelację alertów z MITRE Technics.
       48. Analizator plikowy musi umożliwiać natywną integrację umożliwiającą skanowanie plików z posiadanego przez Zamawiającego programu Office 365 SharePoint Online storage.
       49. Analizator plikowy musi umożliwiać natywną integrację umożliwiającą skanowanie plików z posiadanego przez Zamawiającego programu Microsoft OneDrive.
       50. Analizator plikowy musi wspierać możliwość podłączenia repozytoriów CIFS po SMBv3.
9. **Moduł zarządzania systemem:**
10. System musi pozwalać na zarządzanie innymi komponentami zaproponowanego rozwiązania oraz wszystkimi ich parametrami (np.: konfiguracja trybów pracy, konfigurację zasad alarmowania, zasad eksportu danych do innych systemów bezpieczeństwa, zasad wykonywania kopii bezpieczeństwa, propagowanie poprawek i aktualizacje oprogramowania, zarzadzanie licencjami).
11. Korzystanie z centralnego systemu zarządzania musi odbywać się przy pomocy interfejsu graficznego dostępnego zdalnie, przy wykorzystaniu przeglądarki internetowej oraz poprzez wiersz poleceń przy wykorzystaniu klienta SSH.
12. Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu, jak również komunikacja sieciowa pomiędzy poszczególnymi jego elementami, musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.
13. Zarządzanie Systemem powinno być dostępne jako platforma on-prem.
14. System zarządzania powinien zapewniać co najmniej:
15. automatyczną korelację wyników analiz między modułami, zwłaszcza pochodzących z analizy próbek malware,
16. przegląd wyników analiz z wszystkich elementów Systemu,
17. dostęp do statystyk z działania Systemu,
18. możliwość tworzenia kont użytkowników Systemu o różnych poziomach uprawnień,
19. logowanie i przegląd działań w Systemie.
20. System musi udostępniać możliwość integracji z systemem klasy SIEM poprzez API (preferowany otwarty standard RESTful Interface lub co najmniej syslog).
21. **Warsztaty szkoleniowe – wymagania minimalne:**
22. Wykonawca przeprowadzi warsztaty szkoleniowe w Warszawie lub w formie zdalnej dla 4 osób w wymiarze co najmniej 5 dni w zakresie administracji modułami:
23. moduł AntyMalware dla poczty e-mail,
24. moduł Sandbox,
25. moduł ochrony udziałów sieciowych,
26. moduł zarządzania systemem,
27. Każdy uczestnik warsztatu szkoleniowego otrzyma certyfikat jego ukończenia.
28. Warsztaty szkoleniowe muszą być prowadzone w języku polskim.
29. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatów szkoleniowych. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2-letnie doświadczenie w przedmiocie warsztatu szkoleniowego z zakresu oferowanego rozwiązania.
30. Wykonawca musi dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazą z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia warsztatu szkoleniowego dla osób dorosłych tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowania i pomoce dydaktyczne niezbędne do wykonania zamówienia.
31. Wykonawca w terminie do 30 dni od dnia podpisania bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji oraz Uruchomienia Środowiska – Załącznik nr 6 do Umowy, w zakresie dostawy i uruchomienia systemu będącego przedmiotem niniejszego zamówienia, przedstawi Zamawiającemu do akceptacji Program Warsztatów Szkoleniowych. Program powinien zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów szkoleniowych.
32. Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy warsztatów szkoleniowych – z rozpisaniem na dni i godziny i dostarczy je do 30 dni, od dnia podpisania bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji oraz Uruchomienia Środowiska – Załącznik nr 6 do Umowy, w zakresie dostawy systemu będącego przedmiotem niniejszego zamówienia. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu szkoleniowego.
33. Zajęcia powinny odbywać się w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin zegarowych dziennie. Harmonogram i program powinny zostać przekazane uczestnikom warsztatu podczas pierwszego spotkania.
34. Wykonawca przygotuje i zapewni materiały warsztatowe dla każdego uczestnika do danego rodzaju warsztatu, pozwalające na samodzielną edukację z zakresu tematyki warsztatów szkoleniowych (opracowania, wydruku materiałów warsztatowych).
35. Komplet materiałów warsztatowych dla każdego uczestnika warsztatu szkoleniowego obejmuje:

a) papierową wersję materiałów warsztatowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych;

b) materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji warsztatu szkoleniowego.

1. Komplet materiałów powinien zostać rozdany uczestnikom warsztatu szkoleniowego w pierwszym dniu zajęć.
2. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
3. Wykonawca zapewni: na potrzeby wyżywienia uczestników warsztatów szkoleniowych odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca warsztatu; obiady powinny być zróżnicowane, dany zestaw obiadowy nie powinien powtarzać się częściej niż raz na 3 dni warsztatowe; Wykonawca zapewni 2 przerwy kawowe podczas jednego dnia warsztatowego.
4. Koszty posiłków, dowozu, osprzętu, urządzeń i obsługi ponosi Wykonawca.
5. Potwierdzeniem prawidłowej realizacji warsztatów szkoleniowych będzie podpisany bez zastrzeżeń przez Zamawiającego Protokołu Odbioru Warsztatu Szkoleniowego – Załącznik nr 11 do Umowy, wraz z dołączonymi załącznikami, tj. oryginalną listą obecności, harmonogramem i programem warsztatu szkoleniowego oraz ankiety oceny warsztatu szkoleniowego przeprowadzonej wśród uczestników warsztatu szkoleniowego.