**Wymagania techniczne dla usługi MDR (managed detection & response)**

1. Przedmiotem zamówienia jest realizacja usługi MDR tj. manager detection and response.
2. Usługa musi być realizowana na systemie klasy EDR ESET Inspect. Zamawiający dysponuje odpowiednimi licencjami i nie będą one dostarczane w ramach tego zamówienia. Zamawiający do celów realizacji usługi nie dopuszcza opcji zmiany systemu EDR.
3. Usługa musi być świadczona w trybie 24/7/365.
4. Usługa będzie realizowana w dwóch etapach:
   1. ETAP 1 – Wykonawca zrobi pełny przegląd systemu ESET Inspect oraz ESET Protect. Przegląd zakończy się przekazaniem raportów i wsparciem Zamawiającego celem dokonania niezbędnych zmian wynikających z przekazanych raportów, na które Zamawiający wyrazi zgodę. W ramach ETAPu 1 Wykonawca zrealizuje wszelkie niezbędne prace celem uruchomienia usługi MDR. Prace zostaną wykonane w terminie do 30 dni od momentu podpisania Umowy.
   2. ETAP 2 – Wykonawca będzie realizował przez 12 kolejnych miesięcy po zakończeniu ETAPu 1 monitorowanie i reagowanie na incydenty w ramach usługi MDR (managed detection & response) w następującym zakresie:
      1. Zostanie wyznaczona przez Zamawiającego lista komputerów oraz serwerów, na których Zamawiający wymaga wykonania reakcji przez zespół Wykonawcy. Dla pozostałych (nie wymienionych) urządzeń Zamawiający wymaga, aby Wykonawca powiadomił go o konieczności wykonania reakcji oraz jak przeprowadzić dane działania.
      2. Warunki realizacji usługi to: podjęcie działania do 60 minut od momentu pojawienia się zdarzenia oraz podjęcie reakcji do 180 minut od momentu przyjęcia zdarzenia.
      3. W ramach wykonania customizacji systemu EDR ESET Inspect Wykonawca wymaga wsparcia inżyniera systemowego w zakresie 2 godzin miesięcznie, dostępne w każdym miesiącu trwania usługi.
      4. Wykonawca będzie przesyłał na wyznaczony do kontaktu przez Zamawiającego adres e-mail raporty: tygodniowo oraz miesięcznie.
      5. Wraz z raportem miesięcznym Wykonawca zorganizuje spotkanie zdalne w każdym kolejnym miesiącu celem omówienia raportu miesięcznego i przekazania niezbędnych rekomendacji
   3. Zamawiający wymaga, aby w ramach usługi MDR Wykonawca dostarczył również wsparcie w zakresie poprawy cyberbezpieczeństwa organizacji poprzez udostępnienie puli 12 godzin w ramach całości trwania usługi na następujące czynności: profesjonalne doradztwo w zakresie Cyberbezpieczeństwa, auditor as a service w zakresie norm ISO 27001 oraz 22301 a także realizacji postanowień UoKSC oraz aktualizacji o NIS2, testów penetracyjnych, skanów podatności, kampanii phishing
   4. Zamawiający również wymaga, aby w ramach usługi MDR Wykonawca jednorazowo w ramach usługi zrealizował analizę bezpieczeństwa infrastruktury oraz procesów Zamawiającego i wsparł go w poprawie. Analiza będzie realizowana poprzez przygotowany wcześniej i zaakceptowany przez Zamawiającego zestaw ankietowy obejmujący obszary:
      1. Infrastruktura sieciowa: internet, sieć LAN, sieć WAN, serwery i wirtualizatory, komunikacja sieciowa, zarządzanie
      2. Systemy bezpieczeństwa IT: posiadane przez Zamawiającego Systemy
      3. Bezpieczeństwo informacji
5. W ramach usługi MDR Zamawiający wymaga obsługi miesięcznej do 24 incydentów.
6. Usługa będzie realizowana poprzez zbieranie logów z EDR ESET Inspect do Systemów Wykonawcy. Logi powinni być składowane przez okres 1 miesiąca.
7. W celu realizacji usługi postanowień punktu nr 6 Wykonawca udostępni Zamawiającemu możliwość wysyłania logów do Systemu o wymaganiach:
   1. System skonfigurowany i zarządzany w pełni przez Wykonawcę na jego serwerach. Zamawiający nie udostępnia swoich zasobów sprzętowych i nie mogą być one wymagane do działania systemu SIEM.
   2. Możliwość implementacji agenta monitorującego zasoby pod kątem optymalizacji, agent służy do komunikacji z Systemem i gromadzenia logów w formie buforu, na wypadek zerwania połączenia pomiędzy Zamawiającym a Wykonawcą.
   3. Zaproponowane rozwiązanie musi umożliwić dodawanie kolejnych stacji roboczych i serwerów do systemu EDR ESET Inspect. Koszty Systemu muszą być stałe, wliczone w cenę usługi MDR i nie mogą zależeć od ilości danych.
   4. System musi umożliwiać integrację z rozwiązaniami firm trzecich i nie może być zależne od typu licencji
   5. Rozwiązanie musi mieć możliwość reindeksowania (kopiowania danych z jednego indeksu do drugiego) bez konieczności zatrzymania procesu przesyłania logów.
   6. Rozwiązanie musi zapewnić możliwość budowania własnych pluginów w oparciu o JavaScript służący do weryfikacji lokalizacji adresu IP ale także nowych zupełnie indywidualnych (z poza już dostępnych do wyboru) form wizualizacji zdarzeń w dashboard.
8. Obsługa zdarzeń/incydentów będzie realizowana przez zespół Wykonawcy w oparciu o najlepsze praktyki i wiedzę.
9. Wykonawca będzie realizował usługę w oparciu o logi zebrane z systemu ESET Inspect. Usługa nie może być zależna od ilości pracowników, sprzętu czy wielkości infrastruktury Zamawiającego. W trakcie trwania usługi Zamawiający dopuszcza możliwość rozbudowy swojej infrastruktury i personelu co nie może mieć wpływu na koszt świadczonej przez Wykonawcę usługi.
10. Wykonawca zapewni składowanie logów w dwóch fizycznie oddzielonych lokalizacjach. W każdej lokalizacji Wykonawca musi dysponować redundantnym zasilaniem i bazować w oparciu o dwóch niezależnych dostawców usług internetowych. W docelowej lokalizacji (głównej) Wykonawca zapewni również wsparcie zasilaniem awaryjnym. Zamawiający nie dopuszcza, aby logi były składowane, przetrzymywane, korelowane lub analizowane w oparciu o systemy chmurowe. Wszystkie przesłane logi muszą być zbierane i zabezpieczone w infrastrukturze będącej własnością Wykonawcy.
11. Zamawiający wymaga, aby usługa MDR była realizowana w 100% przez personel Wykonawcy i nie dopuszcza, aby część lub całość zadań była powierzana firmom i osobom trzecim nie będących pracownikami Wykonawcy.

**Wymagania formalne dla usługi MDR (managed detection & response)**

1. Wykonawca oświadcza, że dysponuje następującym zespołem do realizacji usługi MDR:
   1. analitycy linii 1 – min 5 osób,
   2. analitycy linii 2 – min 2 osoby,
   3. analitycy linii 3 – min 2 osoby,
   4. SOC manager – min 1 osoba,
   5. inżynierowie systemowi – min 4 osoby,
   6. compliance – min 2 osoby,
   7. konsultanci – min 2 osoby,
2. Wykonawca musi spełniać wymagania posiadania minimum 4 różne certyfikaty z listy aktualnych certyfikatów. Zamawiający dopuszcza użycie certyfikatów równoważnych dla niżej wskazanych przy 100% pokryciu założeń programowych (teoria i praktyka):
   1. CEH (certified ethical hacker)
   2. CISSP (cetified information systems security professional)
   3. CISA (certified information systems auditor)
   4. CISM (CIS information security manager)
   5. OSCP (offensive security certified professional)
   6. eWPT (web application penetration tester)
   7. eWPTX (web application penetration tester eXtreme)
   8. MITRE ATT&CK Defender™ (MAD) ATT&CK® SOC Assessments Certification Training
3. Wykonawca chcący ubiegać się o świadczenie usługi MDR musi posiadać ważny i aktualny certyfikat obejmujący swoim zakresem świadczoną przez niego usługę:
   1. ISO 27001
   2. ISO 22301
4. Wykonawca musi dbać o jakość swoich usług potwierdzone aktualnym certyfikatem ISO 9001 wraz z wdrożonym Wewnętrznym Systemem Kontroli.
5. Z uwagi na to, iż Zamawiający wykorzystuje jako rozwiązanie klasy EDR system ESET Inspect Wykonawca musi dysponować odpowiednimi certyfikatami do realizacji usługi, minimum 3 ze wskazanych. Zamawiający dopuszcza użycie certyfikatów równoważnych dla niżej wskazanych przy 100% pokryciu założeń programowych (teoria i praktyka):
   1. Certified ESET Managed Client Security Specialist
   2. Certified ESET Managed Client Security Professional
   3. Certified ESET Inspect Optimalization Specialist
   4. Certified ESET Malware Support Specialist
   5. ESET Enterprise Inspector Certified Deployment Specialist
   6. ESET Enterprise Inspector Certified Optimization Specialist
6. Dodatkowe wymagane certyfikaty minimum 4 ze wskazanych. Zamawiający dopuszcza użycie certyfikatów równoważnych dla niżej wskazanych przy 100% pokryciu założeń programowych (teoria i praktyka):
   1. EC Council – Applied Threat Hunting
   2. EC Council – Dark Web Cyber Deception Demystified
   3. EC Council - Detection Engineering Demystified
   4. EC Council - Planning and Implementing a Security Incident Response
   5. EC Council - Practical Cyber Threat Intelligence
   6. EC Council - Project Management for Cybersecurity Professionals
   7. EC Council - Security Information and Event: Management
7. Wykonawca musi wykazać – potwierdzone odpowiednią referencją – że świadczy lub świadczył - usługę MDR u minimum 2 klientów, z czego jeden z nich musi być klientem publicznym (urząd, ministerstwo).