

Opis przedmiotu zamówienia (OPZ) na dostarczenie rozwiązań, usług, sprzętu, oprogramowania i wdrożenia w celu podniesienia poziomu Cyberbezpieczeństwa w Gminie Nakło nad Notecią

Przedmiotem zamówienia jest dostarczenie kompleksowych rozwiązań, usług, dostarczenie niezbędnego sprzętu, oprogramowania oraz ich wdrożenie w celu podniesienia poziomu Cyberbezpieczeństwa w Gminie Nakło nad Notecią. W tym celu Zamawiający podzielił OPZ na pod-części, które są przedmiotem jednego kompleksowego zamówienia.

Lp.	Nazwa	Liczba sztuk
1	Bezpieczeństwo na urządzeniach końcowych wraz z ochroną poczty	150
2	Zewnętrzna usługa Security Office	1
3	Rejestracja incydentów	1
4	Zarządzanie podatnościami	1
5	Wdrożenie SIEM	1
6	Wdrożenie rozwiązania EDR	150
7	Usługa wdrożenia i szkolenia	1

1.1 Wymagania: Bezpieczeństwo na urządzeniach końcowych wraz z ochroną poczty

Lp.	Parametr wymagany
1	Wymagana jest analiza obecnych rozwiązań Zamawiającego, dostosowanie zaproponowanych rozwiązań konfiguracji po wcześniejszym obopólnym uzgodnieniu i zaakceptowaniu przez strony.
2	Zamawiający posiada i używa rozwiązania opartego na licencji ESET Protect Enterprise On-Prem.
3	Wymagana jest zaproponowanie takiego rozwiązania, aby zapewnić adekwatny poziom ochrony dla produktów Microsoft Office 365.
4	Zaproponowane rozwiązanie musi posiadać wbudowaną opcję konfiguracji uwierzytelniania wieloskładnikowego.
5	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
6	Administracja zdalna w chmurze: - Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. - Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW - Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. - Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. - Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. - Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. - Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. - Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak. - Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. - Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. - Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. - Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
7	Ochrona stacji roboczych: - Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). - Rozwiązanie musi wspierać architekturę ARM64. - Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. - Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. - Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

- Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
- Rozwiązanie musi integrować się z Intel Threat Detection Technology.
- Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
- Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
- Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
- Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
 - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

	○ tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, ○ tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, ○ tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. • Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. • Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. • Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. • Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. • Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. • Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. • W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
8	Ochrona serwera: • Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. • Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. • Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. • Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. • Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. • Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. • Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. • Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
9	Dodatkowe wymagania dla ochrony serwerów Windows: • Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. • Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). • Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. • Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. • Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. • Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. • Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. • Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co

	najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
10	Dodatkowe wymagania dla ochrony serwerów Linux: - Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. - Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. - Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. - Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.
11	Szyfrowanie: - System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. - System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). - Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. - Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
12	Ochrona urządzeń mobilnych opartych o system Android: - Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. - Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. - Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). - Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. - Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: - usunięcie zawartości urządzenia, - przywrócenie urządzenia do ustawień fabrycznych, - zablokowania urządzenia, - uruchomienie sygnału dźwiękowego, - lokalizację GPS. - Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. - Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: - nazwę aplikacji, - nazwę pakietu, - kategorię sklepu Google Play, - uprawnienia aplikacji, - pochođenje aplikacji z nieznanego źródła.
13	Ochrona serwera pocztowego MS Exchange: - Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych. - Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019. - Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub. - Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. - Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI. - Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika,

	rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum. • Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty. • System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty. • Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystała aplikacja. • Rozwiązanie ma posiadać mechanizm greylisting (szara lista). • Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
14	Sandbox w chmurze: • Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. • Rozwiązanie musi wykorzystywać do działania chmurę producenta. • Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. • Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. • Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. • Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. • Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów. • Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. • Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. • Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo. • Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: ○ Czysty, ○ Podejrzany, ○ Bardzo podejrzany, ○ Szkodliwy. • W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. • W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. • Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
15	Ochrona usługi Microsoft 365: • Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams. • Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365. • Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną. • Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci. • Rozwiązanie musi być dostępny w języku polskim. • Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: ○ użytkowników, otrzymujących najwięcej spamu, ○ użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,

	○ użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, ○ kont użytkowników, które mogą być podejrzane. • Konsola rozwiązań musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive. • Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: ○ jaka ilość wiadomości została przeskanowana, ○ wynik skanowania poszczególnych wiadomości, ○ czynność podjęta przez rozwiązanie. • Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: ○ zagrożeniach, które zostały wykryte, ○ na jakim koncie zostały wykryte, ○ jakie zagrożenie zostało wykryte, ○ podjętą czynność. • Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive. • Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem. • Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników. • Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: ○ wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, ○ wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online, ○ dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing. • Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day. • Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta. • Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. • Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. • Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.
--	---

1.2 Wymagania: zewnętrzna usługa Security Office

Lp	Parametr wymagany
1	Spełnienie wymagań określonych Rozporządzeniem Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.
2	Posiadanie zespołu, który musi obejmować minimum 9 osób, w szczególności wykonujących role: - kierownik zespołu – posiadanie co najmniej jednej osoby, która posiada: - doświadczenie w prowadzeniu audytów co najmniej 5 lat. - aktualny certyfikat w zakresie ciągłości działania, zgodnie z wymogami normy ISO 22301 - aktualny certyfikat w zakresie zarządzania bezpieczeństwem informacji zgodnie z wymogami normy ISO/IEC 27001 - ważny certyfikat ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi; - Certyfikat Prince2 Foundation – w zakresie zarządzania projektami; - analityk bezpieczeństwa – posiadanie co najmniej dwóch osób z ważnym certyfikatem CIHE (ang. Certified Incident Handling Engineer), pozwalających zagwarantować 1 stanowisko analityka w trybie pracy SOC 24/7, - inżynier bezpieczeństwa – posiadanie co najmniej dwóch osób z ważnym certyfikatem OSCP (ang. Offensive Security Certified Professional), - architekt bezpieczeństwa – posiadanie co najmniej jednej osoby z ważnym certyfikatem CISSP (ang. Certified Information Systems Security Professional), pozwalających na stałe wsparcie w podnoszeniu poziomu bezpieczeństwa infrastruktury Zamawiającego, - pentester – posiadanie co najmniej jednej osoby z ważnym certyfikatem CEH (ang. Certified Ethical Hacker) lub OSCP (ang. Offensive Security Certified Professional). - jedną osobę, która posiada ważny certyfikat GIAC Certified Incident Handle (ang. GIAC Certified Incident Handler – GCIH) - jedną osobę, która posiada ważny certyfikat Audytora Wiodącego Systemu Zarządzania Ciągłością Działania wg normy PN-EN ISO 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
3	Posiadanie ważnego certyfikatu ISO 27001 potwierdzającego bezpieczne przetwarzanie danych Klienta w całym ich zakresie.
4	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
5	Posiadanie ważnego certyfikatu ISO 22301 potwierdzającego posiadanie i możliwość realizacji procesów pozwalających utrzymać wszystkie działania SOC w deklarowanej ciągłości działania.
6	Wymagania funkcjonalne usługi SOC: - usługa SOC musi zapewniać unikalną identyfikację każdego monitorowanego urządzenia/hosta, - usługa SOC musi zapewniać korzystanie z mechanizmów uwierzytelniania dla administratorów i użytkowników, - usługa SOC musi zapewniać wysoki poziom bezpieczeństwa komunikacji poprzez szyfrowanie przy użyciu protokołu TLS / SSL, - usługa SOC musi zapewniać wysoki poziom bezpieczeństwa, w tym poufności gromadzonych danych i zapewniać ochronę przed nieautoryzowanymi zmianami, - usługa SOC musi zapewniać graficzną prezentację wykresów z możliwością agregacji (grupowania) danych, - usługa SOC musi zapewniać raportowanie zdarzeń, w tym incydentów, poziomu wykorzystania infrastruktury oraz zasobów wykorzystywanych w infrastrukturze Zamawiającego, - usługa SOC musi zapewniać generowanie raportów w oparciu o zaplanowany harmonogram na dany okres w zakresie stanu hostów i usług oraz udostępnianie go za pośrednictwem poczty elektronicznej,

	- usługa SOC musi zapewnić możliwości generowania raportów w standardowych formatach, minimum: PDF, CSV, XLS, - usługa SOC musi zapewnić monitorowanie logów systemowych oraz aktywności usług, - usługa SOC musi zapewnić monitorowanie w szczególności następujących systemów operacyjnych: Windows Server 2022, Windows Server 2019, Windows Server 2016, Oracle, Linux, CentOS, Red Hat, Debian.
7	Usługa SOC musi być świadczona przy pomocy następujących komponentów: - Integracja z systemem SIEM - Łącze danych IPSEC VPN zestawione pomiędzy CPD klienta i CDP dostawcy - Systemy objęte monitoringiem – systemy IT klient, infrastruktura - Zasoby osobowe wykonawcy Usługi SOC – 1 Linia Wsparcia SOC: - Monitoring 24/7 - W trakcie pracy Urzędu zgłaszanie według wcześniej ustalonego SLA, które uprzednio musi zostać przedstawione i zaakceptowane przez obie strony - Poza godzinami pracy urzędu interwencja w postaci odcięcia ruchu sieciowego oraz informacja do Administratorów
8	Monitorowanie i reagowanie na zdarzenia bezpieczeństwa w systemach IT klienta musi być realizowane w następujący sposób: - Personel SOC L1 monitoruje w trybie 24x7x365 za pomocą systemu (SECOPS) alarmy sygnalizujące potencjalne naruszenia zasad bezpieczeństwa w środowisku IT klienta. Alarmy będą generowane przez reguły detekcyjne systemu SIEM. - Obsługa alarmów realizowana jest przez linie SOC L1 - obejmuje analizę alarmów Critical i High, eliminację fałszywych alarmów, rejestrację naruszeń w systemie biletowym, informowanie personelu klienta o naruszeniach, pozyskiwanie od personelu klienta dodatkowych danych z monitorowanych systemów niezbędnych do analizy naruszeń, przygotowanie rekomendacji dotyczących sposobów postępowania z naruszeniem, zamykanie obsługi incydentów, tworzenie raportów dotyczących incydentów oraz raportów zbiorczych (tygodniowych i miesięcznych). - Komunikacja z personelu dostawcy z personelem klienta powinna być realizowana za pomocą systemu ticketowego ITSM (SECOPS), powiadomień mailowych lub bezpośredniego kontaktu telefonicznego ze wskazanymi przez klienta osobami.
9	Zadania realizowane przez SOC L1 muszą obejmować: - Monitorowanie potencjalnych naruszeń bezpieczeństwa monitorowanych systemów, przyjmowanie zgłoszeń o podejrzanych aktywnościach dotyczących monitorowanych systemów od personelu klienta, - Rejestracja naruszeń w systemie ticketowym, powiadamianie o naruszeniach personelu klienta, - Przeprowadzanie wstępnej analizy alarmów, eliminacja fałszywych alarmów, pozyskiwanie danych niezbędnych do obsługi incyduentu - Obsługa incydentów bezpieczeństwa kategorii Critical i High w ramach zdefiniowanych scenariuszy reakcji. - Przygotowanie raportów okresowych (tygodniowych) dotyczących podatności raportowanych przez system SIEM
10	- Przegląd, weryfikacja i obsługa incydentów kategorii Critical i High w trybie 24x7x365, przez specjalistów 1 Linii SOC, zgodnie z zaimplementowanymi regułami korelacyjnymi i scenariuszami reakcji. - W przypadku wystąpienia incydentów sklasyfikowanych jako Critical i High personel klienta zostanie poinformowany mailem i telefonicznie przez specjalistów SOC o wystąpieniu incyduentu bezzwłocznie po jego identyfikacji. - Informacje o wszystkich incydentach zarejestrowanych w ramach okresu rozliczeniowego (1 miesiąc) muszą zostać umieszczone w Raporcie miesięcznym.
11	Wdrożenie Usługi SOC musi obejmować następujące etapy: - Inicjacja projektu - Uzgodnienie harmonogramu - Wdrożenie systemu SIEM - Uzgodnienie warunków technicznych niezbędnych do uruchomienia usługi SOC (łącza, zasoby sprzętowe i software'owe) - Przygotowanie niezbędnych zasobów technicznych po stronie klienta oraz dostawcy - Konfiguracja systemu SIEM, zestawienie łącza danych pomiędzy Dostawcą i klientem - Podłączenie źródeł danych do systemu SIEM

	• Uzgodnienie, konstrukcja i wdrożenie reguł detekcyjnych • Uzgodnienie procesu i procedur obsługi incydentów, konfiguracja kont w systemie ticket'owym dla uprawnionego personelu klienta • Implementacja raportów tygodniowych i miesięcznych • Testy systemów • Aktywacja usługi SOC
--	---

1.3 Wymagania: rejestracja incydentów

Lp	Parametr wymagany
1	W planach jest ich wdrożenie i konfiguracja systemu typu Service Desk jako systemu, który zapewni bieżącą obsługę i archiwizację zgłoszeń. Do tego celu ma zostać przystosowany obecny system Axence Nvision, który jest w posiadaniu Gminy, a docelowo a również być udostępniony Wykonawcy, w ramach pełnienia usługi SOC.
2	Wymagana jest analiza obecnych rozwiązań Axence Nvision u Zamawiającego, dostosowanie zaproponowanych rozwiązań konfiguracji po wcześniejszym obopólnym uzgodnieniu i zaakceptowaniu przez strony oraz ich wdrożenie.
3	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
4	Rejestracja incydentów jest integralnie połączona z usługą zewnętrzną Security Office i musi spełniać następujące wymagania: • usługa SOC musi zapewniać raportowanie zdarzeń, w tym incydentów, poziomu wykorzystania infrastruktury oraz zasobów wykorzystywanych w infrastrukturze Zamawiającego, • usługa SOC musi zapewniać generowanie raportów w oparciu o zaplanowany harmonogram na dany okres w zakresie stanu hostów i usług oraz udostępnianie go za pośrednictwem poczty elektronicznej, • usługa SOC musi zapewnić możliwości generowania raportów w standardowych formatach, minimum: PDF, CSV, XLS, • usługa SOC musi zapewnić monitorowanie logów systemowych oraz aktywności usług, • usługa SOC musi zapewnić monitorowanie w szczególności następujących systemów operacyjnych: Windows Server 2022, Windows Server 2019, Windows Server 2016, Oracle, Linux, CentOS, Red Hat, Debian
5	Rejestracja incydentów w ramach usługi SOC musi zostać dostarczona według wymagań opisanych w punkcie 1.2 opisującego wymagania dostarczenia zewnętrznej usługi Security Office
6	Zamawiający wymaga integracji zaproponowanego rozwiązania z rozwiązaniem SIEM, EDR oraz usługą SOC.

1.4 Wymagania: zarządzanie podatnościami

Lp	Parametr wymagany
1	Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2	Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3	Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych.
4	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
5	Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, przynajmniej raz dziennie.
6	Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum: • nazwę aplikacji lub systemu operacyjnego • punktacje CVSS • opis wykrytej podatności • wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
7	Moduł wykrywania podatności musi wykrywać podatności dla popularnych aplikacji.
8	Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla popularnych aplikacji.
9	Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10	Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
11	Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
12	Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
13	Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
14	Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
15	Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności

1.5 Wymagania: wdrożenie SIEM

Lp	Parametr wymagany
1	Przedmiotem zamówienia jest dostawa Systemu składającego się z rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management) zwanego dalej Systemem SIEM.
2	System musi umożliwiać monitorowanie, detekcję i reagowanie na różnego rodzaju zagrożenia bezpieczeństwa w środowiskach informatycznych.
3	W celu identyfikacji potencjalnych zagrożeń wymagane jest analizowanie logów z wielu różnych źródeł, takich jak: • serwery, • aplikacje, • urządzenia sieciowe.
4	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
5	System SIEM musi posiadać wbudowane reguły detekcji oraz zaawansowanych technik analizy zachowań w celu wykrywania niepożądanych aktywności oraz prób włamań do systemów.
6	Konieczna jest możliwość konfiguracji reguł reagowania, które mogą wyzwać działania w odpowiedzi na wykryte zagrożenia, takie jak wysyłanie powiadomień, blokowanie adresów IP
7	SIEM musi posiadać możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak: • Elasticsearch, • Kibana, • Splunk, • Docker, aby umożliwić elastyczne dostosowanie platformy do indywidualnych potrzeb Zamawiającego.
8	Wszystkie komponenty wchodzące w skład Systemu SIEM muszą być w wersji produkcyjnej.
9	System SIEM musi zapewniać skalowalność pozwalającą na pracę w dużych organizacjach.
10	System SIEM musi mieć możliwość pracy w architekturze pozwalającej na instalację i konfigurację w wielu lokalizacjach.
11	System SIEM musi mieć możliwość uruchomienia w architekturze zapewniającej wysoką dostępność
12	Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania.
13	Zakres instalacji i konfiguracji systemu SIEM w celu dostosowania systemu do świadczenia usługi SOC przez Wykonawcę. • W ramach realizacji zadania Zamawiający wymaga zaimplementowane reguły detekcyjne systemu SIEM oraz zaimplementowaną funkcję izolacji zainfekowanego hosta Windows/Linux • Integracja systemów SIEM z systemem Incident Workflow obejmująca przekazywania alertów do systemu SECOPS dostawcy oraz zestawienie kanału IPSEC VPN pomiędzy infrastrukturą klienta i dostawcą usługi • Implementacja reguł detekcyjnych w systemach SIEM generujących alerty sygnalizujące potencjalne incydenty bezpieczeństwa • Implementacja scenariuszy reakcji dla alertów kategorii Critical oraz High, definiujących reakcję SOC L1 na wygenerowane alerty • Uzgodnienie z personelem klienta procesu obsługi incydentów, implementacja scenariuszy reakcji w systemie Incident Workflow Dostawcy

	• Monitorowanie przez 1 Linie Wsparcia SOC w trybie 24x7x365 alarmów wygenerowanych przez system SIEM na podstawie reguł detekcyjnych oraz ich weryfikacja przez specjalistów SOC • Obsługę incydentów. Obsługa incydentów musi być realizowana zgodnie z uzgodnionymi warunkami SLA przez 1 Linie Wsparcia SOC w trybie 24x7 poprzez wykonanie zadań wchodzących w skład scenariuszy reakcji dla zidentyfikowanych w ramach weryfikacji alarmów incydentów kategorii Critical i High • Comiesięczne raportowanie zawierające szczegółowe zestawienie incydentów obsługiwanych w okresie poprzedniego miesiąca wraz z zaleceniami dotyczącymi potencjalnych zmian w środowisku IT klienta, regułach detekcyjnych i scenariuszach reakcji. • Cotygodniowe raportowanie błędów w konfiguracji opartych o benchmarki CIS oraz podatności zidentyfikowane przez system SIEM • Utrzymanie infrastruktury niezbędnej do świadczenia Usługi SOC – systemów SIEM, ITSM, łącza IPSEC VPN.
14	Wdrożenie Usługi SIEM obejmie następujące etapy: • Inicjacja projektu • Uzgodnienie harmonogramu • Wdrożenie systemu SIEM • Uzgodnienie warunków technicznych niezbędnych do uruchomienia usługi SOC (łącza, zasoby sprzętowe i software'owe) • Przygotowanie niezbędnych zasobów technicznych po stronie klienta oraz dostawcy • Konfiguracja systemu SIEM • Podłączenie źródeł danych do systemu SIEM • Uzgodnienie, konstrukcja i wdrożenie reguł detekcyjnych • Uzgodnienie procesu i procedur obsługi incydentów, konfiguracja kont w systemie ticket'owym dla uprawnionego personelu klienta • Implementacja raportów tygodniowych i miesięcznych • Testy systemów • Aktywacja usługi SIEM

1.6 Wymagania: wdrożenie usługi EDR

Lp	Parametr wymagany
1	Zamawiający posiada oprogramowanie EDR serwerowe w wersji ESET Protect Enterprise On-Prem. Jednym z wymagań jest migracja do chmury.
2	Zamawiający wymaga konfigurację usług i wdrożenie rozwiązania zgodnie z „Dobrymi praktykami”.
3	Wymagana jest analiza obecnych rozwiązań Zamawiającego, dostosowanie zaproponowanych rozwiązań konfiguracji po wcześniejszym obopólnym uzgodnieniu i zaakceptowaniu przez strony.
4	Zaproponowane rozwiązanie powinno być zgodne z wymaganiami systemowymi posiadanego rozwiązania: - Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. - Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej posiadanego rozwiązania Zamawiającego. - Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. - Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. - Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. - Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. - Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. - Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwalenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. - Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. - Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. - Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. - Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. - W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. - W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: - modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. - Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

	• Konsola administracyjna musi mieć możliwość tagowania obiektów. • Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
--	---

1.7 Wymagania: Usługa wdrożenia oraz szkolenia

Kolejność wdrożenia poszczególnego zadania:

Etap	Nazwa zadania	Liczba dni wykonania zadania od podpisania umowy
1	Bezpieczeństwo na urządzeniach końcowych wraz z ochroną poczty	14
2	Zarządzanie podatnościami	14
3	Wdrożenie rozwiązania EDR	14
4	Zewnętrzna usługa Security Office	30
6	Wdrożenie SIEM	30
7	Rejestracja incydentów	30
8	Instruktaż powdrożeniowy dla Administratorów systemu: min. 8h w terminach wcześniej ustalonych i potwierdzonych przez Zamawiającego dla każdej z części.	Po zakończeniu pełnego wdrożenia