Załącznik nr 2 – Szczegółowy opis przedmiotu zamówienia

# EDR/XDR

Dostawa i wdrożenie rozwiązania klasy EDR/XDR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Wymaganie** | **Uszczegółowienie** | **Parametr wymagany** | **Parametr oferowany** |
| XDR-1 | Rozwiązanie musi identyfikować złośliwe pliki i zapobiegać ich uruchamianiu, w tym wirusy, trojany, oprogramowanie ransomware, oprogramowanie szpiegujące, kryptominery oraz inne typy złośliwego oprogramowania. | Ochrona przed złośliwym oprogramowaniem oparta na sygnaturach | **TAK** |  |
| Analiza statyczna oparta na uczeniu maszynowym | **TAK** |  |
| Analiza dynamiczna (Sandbox w czasie rzeczywistym) | **TAK** |  |
| Analiza zagrożeń (VT) | **TAK** |  |
| Analiza zagrożeń (źródła inne niż VT) | **TAK** |  |
| Integracja z MS Windows AMSI | **TAK** |  |
| XDR-2 | Rozwiązanie musi identyfikować złośliwe zachowanie już wykonywanych plików \ uruchomionych procesów \ modyfikacji rejestru \ dostępu do pamięci i mieć możliwość zatrzymania takich działań w czasie rzeczywistym lub zgłoszenia alertu w przypadku wykrycia (np. exploity, ataki bezplikowe, makra, skrypty Powershell, aktywności WMI itp.). | Monitorowanie dostępu do pamięci | **TAK** |  |
| Analiza zachowania procesów (heurystyka) | **TAK** |  |
| Wysokie podobieństwo (tzw. hashowanie rozmyte) | **TAK** |  |
| Analiza zagrożeń | **TAK** |  |
| XDR-3 | Rozwiązanie musi obsługiwać tworzenie reguł ostrzegających o komunikacji z określonymi adresami IP. | Czarna lista złośliwych adresów IP i domen | **TAK** |  |
| XDR-4 | Rozwiązanie musi identyfikować i blokować próby ataków eskalacji uprawnień. | Monitorowanie procesów | **TAK** |  |
| XDR-5 | Rozwiązanie musi identyfikować i blokować ataki rozpoznawcze (skanowanie). | Monitorowanie ruchu sieciowego | **TAK** |  |
| Monitorowanie pamięci | **TAK** |  |
| XDR-6 | Rozwiązanie musi identyfikować i blokować próby kradzieży danych uwierzytelniających z pamięci (zrzuty danych uwierzytelniających, ataki brute force) lub ruchu sieciowego (fałszowanie ARP, ataki typu DNS Responder). | Monitorowanie kont użytkowników (próby logowania) | **TAK** |  |
| Analiza zachowania ruchu sieciowego | **TAK** |  |
| XDR-7 | Rozwiązanie musi identyfikować i blokować/alarmować w przypadku wykrycia technik przemieszczania się w sieci (np. SMB relay, pass the hash itp.) | Monitorowanie ruchu sieciowego. | **TAK** |  |
| Oszustwa przy użyciu fałszywych węzłów. | **TAK** |  |
| Oszustwa przy użyciu fałszywych kont użytkowników. | **TAK** |  |
| Oszustwa z użyciem fałszywych połączeń sieciowych. | **TAK** |  |
| XDR-8 | Rozwiązanie musi identyfikować podejrzane działania użytkownika, które mogą świadczyć o wcześniejszym naruszeniu bezpieczeństwa. | Konfigurowanie zasad aktywności użytkowników (naruszenie polityki). | **TAK** |  |
| Profilowanie bazowej aktywności konta użytkownika (wykrywanie anomalii). | **TAK** |  |
| XDR-9 | Rozwiązanie musi wykrywać nietypowe lub niebezpieczne operacje wykonywane na plikach danych. | Oszustwa z użyciem plików wabików/pułapek. | **TAK** |  |
| XDR-10 | Rozwiązanie musi być identyfikować próby wycieku danych przy użyciu dozwolonych kanałów komunikacji (takich jak: tunelowanie DNS, tunelowanie ICMP). | Monitorowanie ruchu sieciowego. | **TAK** |  |
| Monitorowanie dostępu do plików. | **TAK** |  |
| XDR-11 | Rozwiązanie musi identyfikować i blokować korzystanie z popularnych narzędzi atakujących (takich jak: Metasploit, Empire, Cobalt itp.). | Monitorowanie procesów. | **TAK** |  |
| XDR-12 | Rozwiązanie musi posiadać wewnętrzny mechanizm ochrony przed działaniami osób nieuprawnionych. | Alarmowanie i blokowanie przy każdej próbie manipulacji lub wyłączenia. | **TAK** |  |
| XDR-13 | Rozwiązanie musi posiadać funkcjonalność wykrywania i blokowania komunikacji ze złośliwymi domenami. | Filtrowanie domen | **TAK** |  |
| XDR-14 | Rozwiązanie musi stale gromadzić dane o wszystkich podmiotach oraz ich działaniach w środowisku. | Interakcja z plikami - tworzenie, otwieranie, zmiana nazwy, usuwanie, wykonywanie | **TAK** |  |
| Wykonywanie procesów (w tym wyświetlanie drzewa procesów) | **TAK** |  |
| Logowanie użytkownika | **TAK** |  |
| Ruch sieciowy | **TAK** |  |
| Zmiany w rejestrze | **TAK** |  |
| Zainstalowane oprogramowanie | **TAK** |  |
| XDR-15 | Rozwiązanie musi obsługiwać wyświetlanie danych dotyczących podmiotów i ich aktywności. | Wyszukiwanie oparte na wzorcach zachowań we wszystkich obszarach zasięgu (użytkownicy, pliki, maszyny i ruch sieciowy). | **TAK** |  |
| Określanie reguł i/lub tworzenie ostrzeżeń i/lub ustalanie poziomu ryzyka na podstawie reakcji na wykryty wzorzec w czasie rzeczywistym. | **TAK** |  |
| Umożliwienie wielu użytkownikom wykonywania działań równolegle, w oparciu o uprawnienia użytkownika i bez konieczności odłączania innego użytkownika w celu wykonania działania. | **TAK** |  |
| XDR-16 | Rozwiązanie musi obsługiwać dynamiczną analizę (np. Sandbox). | Ręczne przesyłanie plików do odizolowanego środowiska analitycznego. | **TAK** |  |
| XDR-17 | Rozwiązanie musi obsługiwać zapytania międzyorganizacyjne. | Wyszukiwanie występowania aktywności procesów/plików/sieci/użytkowników we wszystkich punktach końcowych w środowisku. | **TAK** |  |
| XDR-18 | Rozwiązanie musi obsługiwać środki do przeprowadzania dochodzeń kryminalistycznych. | Uruchamianie profilu procesu lub pliku. | **TAK** |  |
| Poziom maszyny. | **TAK** |  |
| Aktywność pamięci operacyjnej. | **TAK** |  |
| Uzyskanie zrzutu pamięci. | **TAK** |  |
| XDR-19 | Rozwiązanie musi obsługiwać izolację i ograniczanie złośliwej obecności i aktywności lokalnie na punkcie końcowym. | Możliwość uruchamiania skoordynowanych poleceń (takich jak interfejs CMD). | **TAK** |  |
| Uruchamianie skryptu lub pliku z lokalizacji sieciowej lub mapowanie dysku. | **TAK** |  |
| Wyłączanie punktu końcowego i/lub serwera. | **TAK** |  |
| Izolacja punktu końcowego/serwera od sieci. | **TAK** |  |
| Usunięcie pliku (w tym aktywnych uruchomionych plików). | **TAK** |  |
| Umieszczenie pliku w kwarantannie (w tym aktywnych uruchomionych plików). | **TAK** |  |
| Zakończenie procesu. | **TAK** |  |
| Usunięcie usługi/zaplanowanego zadania. | **TAK** |  |
| Blokowanie konta użytkownika lokalnego lub konta domenowego. | **TAK** |  |
| Zerowanie hasła użytkownika. | **TAK** |  |
| Blokowanie połączeń telekomunikacyjnych na podstawie miejsca docelowego (adresu domeny lub adresu IP). | **TAK** |  |
| Odłączanie kart sieciowych. | **TAK** |  |
| Zmiana adresu IP. | **TAK** |  |
| Możliwość edycji pliku HOST. | **TAK** |  |
| Odnowienie działania stacji końcowej i/lub serwera. | **TAK** |  |
| XDR-20 | Rozwiązanie musi obsługiwać automatyzację reakcji. | Wstępne scenariusze/playbooki reakcji dostarczane w ramach rozwiązania. | **TAK** |  |
| Niestandardowe playbooki reakcji, które są tworzone przez operatora. | **TAK** |  |
| XDR-21 | Rozwiązanie musi obejmować mechanizm automatycznego badania wykrytych zdarzeń bezpieczeństwa i zdolność do ich automatycznego naprawiania, zawsze autonomicznie, tego, co zostało zidentyfikowane. | Dochodzenie: identyfikacja wszelkich trwałych zagrożeń, pierwotnych przyczyn lub naruszonych elementów w całej chronionej infrastrukturze. | **TAK** |  |
| Remediacja: zautomatyzowane usuwanie złośliwych elementów zidentyfikowanych w fazie dochodzenia. | **TAK** |  |
| XDR-22 | Rozwiązanie musi przedstawiać łańcuch zdarzeń oraz powiązanych obiektów, które doprowadziły do incydentu. | Graficzna wizualizacja incydentu, która pokazuje zdarzenia i powiązane dane dotyczące ofiary, sprawcy i relacji między artefaktami danych a drzewem procesów i łańcuchem zdarzeń. | **TAK** |  |
| XDR-23 | Rozwiązanie musi obsługiwać monitorowanie integralności plików (FIM). | Egzekwowanie zasad w stałych środowiskach w celu ostrzegania o wszelkich zmianach plików. | **TAK** |  |
| XDR-24 | Rozwiązanie musi mieć wbudowaną funkcję oceny podatności na zagrożenia. | Wykrywanie brakujących aktualizacji zabezpieczeń w systemach i aplikacjach. | **TAK** |  |
| XDR-25 | Rozwiązanie musi zapewniać środki do zarządzania zasobami. | Mapowanie i korelowanie wszystkich zasobów w środowisku, takich jak punkty końcowe, serwery, zainstalowane aplikacje, konta użytkowników i generowanie okresowych raportów. | **TAK** |  |
| XDR-26 | Rozwiązanie musi zapewniać gromadzenie i przechowywanie krótkoterminowe logów w celu ich analizy. | Zbieranie dzienników uwierzytelniania i aktywności w celu ich analizy krótkoterminowej. | **TAK** |  |
| XDR-27 | Rozwiązanie musi obejmować wyszukiwanie zagrożeń. | Wyszukiwanie złośliwej obecności na podstawie znanych wskaźników (IOC). | **TAK** |  |
| XDR-28 | Rozwiązanie musi wspierać wykrywanie niech a cronionych powierzchni ataku. | Wyszukiwanie podatnych na zagrożenia plików, procesów, połączeń sieciowych i kont użytkowników z niezmienionymi hasłami. | **TAK** |  |
| XDR-29 | Rozwiązanie musi mieć elastyczne opcje wdrażania serwerów, aby pasowało do różnych typów środowisk. | On-prem | **TAK** |  |
| SaaS | **TAK** |  |
| Hybrydowe | **TAK** |  |
| XDR-30 | Rozwiązanie musi obsługiwać szybką i bezproblemową instalację na wszystkich punktach końcowych/serwerach w środowisku. | x | **TAK** |  |
| XDR-31 | Rozwiązanie musi mieć niewielki wpływ na wydajność punktu końcowego/serwera. | ~50 MB pamięci systemowej (RAM) zużywanej przez każdy punkt końcowy/serwer. | **TAK** |  |
| ~2-5% mocy obliczeniowej procesora systemowego na każdej platformie punktu końcowego. | **TAK** |  |
| XDR-32 | Rozwiązanie musi zapewniać szyfrowaną komunikację pomiędzy serwerem zarządzającym a agentami na punktach końcowych/serwerach. | x | **TAK** |  |
| XDR-33 | Rozwiązanie musi obsługiwać wszystkie powszechnie używane systemy operacyjne. | Windows XP\Vista, Server 2003 posiadane przez Zamawiającego | **TAK** |  |
| Windows 7 i nowsze posiadane przez Zamawiającego | **TAK** |  |
| Windows server 2008 R2 i nowsze posiadane przez Zamawiającego | **TAK** |  |
| Główne dystrybucje Linuksa: Fedora, Ubuntu, Debian, Centos, Red Hat, Suse, Oracle, Alma, Amazon posiadane przez Zamawiającego | **TAK** |  |
| MAC OSX 10.15 Catalina i nowsze (Intel i Apple Silicon) posiadane przez Zamawiającego | **TAK** |  |
| XDR-34 | Rozwiązanie musi obsługiwać połączenie z domeną Active Directory posiadaną przez Zamawiającego | Granularne uwierzytelnianie do interfejsu użytkownika. | **TAK** |  |
| Wdrażanie różnych grup jednostek organizacyjnych (OU) w ramach AD posiadanego przez Zamawiającego | **TAK** |  |
| XDR-35 | Rozwiązanie musi umożliwiać definiowanie ról administracyjnych z niestandardowymi uprawnieniami. | Tworzenie ról z niestandardowymi uprawnieniami opartymi na typach dostępnych akcji, które można przypisać do użytkowników i grup lokalnych oraz grupom użytkowników i grup AD posiadanego przez Zamawiającego | **TAK** |  |
| XDR-36 | Rozwiązanie musi współistnieć ze wszelkim oprogramowaniem na punktach końcowych\serwerach. | Płynne działanie chronionego punktu końcowego/serwera bez krytycznych błędów systemowych lub awarii procesów. | **TAK** |  |
| XDR-37 | Rozwiązanie musi zapewniać pełną ochronę punktów końcowych i serwerów, które znajdują się poza siecią organizacji. | Mechanizm ochrony przed zagrożeniami, który nie wymaga połączenia z serwerem zarządzania. | **TAK** |  |
| XDR-38 | Rozwiązanie musi gromadzić dane o punktach końcowych, plikach, procesach, aktywności użytkowników i ruchu sieciowym w sposób w pełni autonomiczny. | Eliminuje potrzebę ręcznej konfiguracji reguł lub zasad oraz konieczność korzystania z dodatkowych urządzeń. | **TAK** |  |
| XDR-39 | Rozwiązanie musi mieć możliwość określenia listy reguł wykluczania alertów dla wybranych obiektów. | x | **TAK** |  |
| XDR-40 | Rozwiązanie musi obsługiwać wdrażanie w wielu lokalizacjach, które raportują do jednej konsoli zarządzania. | x | **TAK** |  |
| XDR-41 | Rozwiązanie musi mieć możliwość eksportowania bieżącej konfiguracji programu w celu późniejszego zaimportowania jej na ten sam lub inny komputer. | x | **TAK** |  |
| XDR-42 | Rozwiązanie musi mieć możliwość włączania/wyłączania określonych typów powiadomień. | x | **TAK** |  |
| XDR-43 | Rozwiązanie musi mieć możliwość oceny ważności alertów bezpieczeństwa. | x | **TAK** |  |
| XDR-44 | Rozwiązanie musi zapewniać centralne gromadzenie i przetwarzanie alertów w czasie rzeczywistym. | x | **TAK** |  |
| XDR-45 | Rozwiązanie musi mieć możliwość blokowania dostępu do ustawień programu dla użytkowników końcowych. | x | **TAK** |  |
| XDR-46 | Rozwiązanie musi zapewniać centralną dystrybucję aktualizacji bez konieczności interwencji użytkownika i ponownego uruchamiania punktu końcowego/serwera. | x | **TAK** |  |
| XDR-47 | Rozwiązanie musi mieć możliwość określenia harmonogramu pobierania aktualizacji, w tym możliwość wyłączenia automatycznej aktualizacji. | x | **TAK** |  |
| XDR-48 | Rozwiązanie musi przypisywać ocenę ryzyka do wszystkich obiektów w chronionym środowisku. | x | **TAK** |  |
| XDR-49 | Rozwiązanie musi obsługiwać rejestrowanie zdarzeń, alertów i aktualizacji. | x | **TAK** |  |
| XDR-50 | Rozwiązanie musi umożliwiać wydłużenie domyślnego okresu przechowywania danych w celu zrównoważenia prywatności i zasad korporacyjnych. | x | **TAK** |  |
| XDR-51 | Rozwiązanie musi obsługiwać integrację z infrastrukturą poczty elektronicznej w celu powiadamiania personelu bezpieczeństwa w przypadku alertów. | x | **TAK** |  |
| XDR-52 | Rozwiązanie musi obsługiwać integrację z popularnymi produktami SIEM (poprzez wyjściowe syslogi, API i json wysyłany do AWS S3 Buckets; zarówno dla alertów, jak i logów). | x | **TAK** |  |
| XDR-53 | Rozwiązanie musi obejmować opcję przyjmowania danych syslog z dowolnego źródła oraz centralizowania ich wszystkich w jednej konsoli (logi te muszą być prezentowane jako dane surowe lub w formie dashboardu z różnymi typami wykresów). | x | **TAK** |  |
| XDR-54 | Rozwiązanie musi obsługiwać standardowe i konfigurowalne raporty. Raporty muszą być eksportowane w różnych formatach, zaplanowane i wysyłane pocztą elektroniczną. | x | **TAK** |  |
| XDR-55 | Rozwiązanie musi oferować aplikację na smartfony, smartwatche i tablety, która może pokazać, ile zasobów jest chronionych, ile otwartych alarmów, nowe alarmy w miarę ich pojawiania się wraz z typem, wpływem, dotkliwością i reakcją, a także możliwość bezpośredniego zaangażowania się z poziomu aplikacji SOC w celu rozpoczęcia dochodzenia. | x | **TAK** |  |
| XDR-56 | Oferowane rozwiązanie EDR/XDR musi posiadać oficjalną dokumentację potwierdzającą udział w testach MITRE Engenuity ATT&CK® Evaluations: Enterprise lub równoważnych testach weryfikujących zdolność wykrywania technik ataków | x | **TAK** |  |
| XDR-57 | Oferowane rozwiązanie musi posiadać potwierdzone wyniki w testach MITRE Engenuity ATT&CK® Evaluations: Enterprise lub równoważnych testach weryfikujących zdolność wykrywania technik ataków, osiągające współczynnik wykrywalności technik ataku na poziomie co najmniej 70% dla edycji z roku 2024 lub 2025. Współczynnik wykrywalności technik ataku rozumiany jest jako procentowy udział wykrytych technik ataku w stosunku do wszystkich technik testowanych w danej rundzie testów | x | **TAK** |  |
| XDR-58 | Wykonawca zapewnia wdrożenie na co najmniej 450 urządzeniach/systemach końcowych wskazanych przez Zamawiającego | x | **TAK** |  |
| XDR-59 | W ramach wdrożenia wykonawca skonfiguruje polityki rozwiązania klasy EDR/XDR zgodnie z wytycznymi Zamawiającego | x | **TAK** |  |
| XDR-60 | Wykonawca przeprowadzi na własny koszt szkolenie dedykowanego personelu Zamawiającego w zakresie obsługi technicznej Oprogramowania, przekazując dokument potwierdzający uczestnictwo personelu w szkoleniu. | x | **TAK** |  |
| XDR-61 | Wykonawca przygotuje dokumentację powykonawczą wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach | x | **TAK** |  |

# SOC/MDR

W ramach świadczenia usług SOC/MDR zamawiający wymaga również realizacji działań prewencyjnych takich jak:

* Kampanie phisingowe
* Działania edukacyjne

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Wymaganie (Opis)** | **Parametr wymagany** | **Parametr oferowany** |
| SOC-1 | Świadczenie usługi pierwszej linii wsparcia SOC - L1, całodobowe 24/7/365, monitorowanie infrastruktury i systemów IT, korelacja zdarzeń, identyfikacja zdarzeń potencjalnie niebezpiecznych, wykrywanie i informowanie o incydentach z czasem reakcji 15 minut.  Wykonawca zapewnia Zamawiającemu:  • przekazywanie informacji o potencjalnych incydentach wypracowanym kanałem komunikacji  • dostęp do konsoli monitorowania SIEM i SOAR / hybrydy 24/7/365 w uzgodnionym zakresie  • możliwość definiowania własnych reguł korelacyjnych SIEM  • monitorowanie potencjalnych naruszeń bezpieczeństwa IT  • przyjmowanie zgłoszeń o podejrzanych aktywnościach od personelu Zamawiającego  • przeprowadzanie wstępnej analizy i eliminacji fałszywych alarmów  • współpraca z II linią wsparcia SOC oraz z administratorami lokalnymi  • przekazywanie uzgodnionych informacji o incydentach do CSIRT któremu zgodnie z dyrektywą NIS 2 będzie podlegał zamawiający i wypełnianie w imieniu Zamawiającego obowiązków wynikających z ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych w zakresie stopni alarmowych CRP i monitorowania systemów informatycznych oraz wsparcie  Zamawiającego w wypełnianiu zaleceń wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz z jej planowaną nowelizacją | **TAK** |  |
| SOC-2 | Świadczenie usługi drugiej linii wsparcia SOC - L2, całodobowe 24/7/365  Wykonawca zapewnia Zamawiającemu:  • przygotowanie z administratorami lokalnymi Zamawiającego scenariuszy reakcji na incydenty wynikające z reguł korelacyjnych  • przygotowanie z administratorami lokalnymi Zamawiającego planów postępowania z incydentami  • analiza zdarzeń i obsługa incydentów, zebranie informacji niezbędnych do poprawnego obsłużenia incydentu, weryfikacja poprawności i kompletności dostarczonych danych źródłowych  • wydanie zaleceń i opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie administratorów IT przy realizacji przygotowanego scenariusza  • opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości  • przygotowanie planu działania w celu ograniczenia strat związanych z incydentem, pozyskanie dodatkowych danych niezbędnych do obsługi incydentu (z I linii wsparcia, z logów systemowych, ze źródeł zewnętrznych – CSIRT, użytkowników i innych)  • proponowanie nowych reguł korelacyjnych i scenariuszy SIEM i playbooków (zautomatyzowanych reakcji na incydenty) SOAR do wdrożenia w systemie SIEM/SOAR i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa  • proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne Zamawiającego, przygotowywanie raportów dla Zamawiającego i jego dostawców  • Wykonawca może w ramach usługi L2 uruchamiać okresowe testy podatności  • Wykonawca może dokonywać niezautomatyzowanej analizy logów Zamawiającego w celu proaktywnego poszukiwania incydentów i zabezpieczenia materiałów po incydencie | **TAK** |  |
| SOC-3 | Świadczenie usługi trzeciej linii wsparcia SOC - L3, która obejmuje pomoc zdalną lub na miejscu w zakresie usunięcia skutków zaistniałego incydentu, rekomendacje w zakresie zachowania materiału dowodowego dla Zamawiającego wraz z pełną analizą powłamaniową, analizę złośliwego oprogramowania; | **TAK** |  |
| SOC-4 | Wykonanie audytów podatności zgodnie z poniższymi wymaganiami  • wykonanie audytu i raportu podatności co 6 miesięcy w zakresie infrastruktury zewnętrznej Zamawiającego oraz co 12 miesięcy w zakresie infrastruktury wewnętrznej i stacji roboczych Zamawiającego - raporty muszą obejmować całą infrastrukturę serwerową, w tym wirtualną, kluczowe urządzenia i stacje robocze wykorzystywane przez użytkowników Zamawiającego (zakres infrastruktury kluczowej i kluczowych stacji roboczych zostanie ustalony w czasie wstępnego audytu)  • wykrywanie podatności w systemach i infrastrukturze Zamawiającego wraz z przekazywaniem na bieżąco rekomendacji z podziałem na podatności wysokiego ryzyka – koniczne do usunięcia (niemożliwe jest ich monitorowanie i zabezpieczenie systemów), średniego ryzyka (włączone do stałego monitorowania, ale generujące ryzyka), podatności niskiego ryzyka – bezpieczne w przypadku monitorowania | **TAK** |  |
| SOC-4 | Raportowanie:  • każdorazowo przy wystąpieniu incydentu, który zwiera informacje o incydencie, wpływ na środowisko Zamawiającego, sposoby mitygacji,  • miesięczny raport w zakresie wykonywanej usługi, który zawiera listę zaobserwowanych zdarzeń w podziale na kategorie zdarzeń typu (DDoS, ransomeware, phishing, brute force, itp.) oraz wykorzystane zabezpieczenia  Miesięczny raport zawierający informacje o stosunku zdarzeń false positive vs true positive z każdej reguły korelacyjnej wraz z rekomendacją ewentualnych zmian | **TAK** |  |
| PH-1 | Do przeprowadzenia kampanii phisingowych muszą być wykorzystane komercyjne platformy lub oprogramowanie komercyjne służące do tworzenia tego typu platform. Zamawiający wymaga wykorzystania komercyjnych rozwiązań ze względów bezpieczeństwa – rozwiązania typu open-source zwiększają ryzyko wycieku listy mailingowych i potencjalnego rzeczywistego ataku. | **TAK** |  |
| PH-2 | Koszty subskrypcji platformy phisingowej pokrywa wykonawca | **TAK** |  |
| PH-3 | Każda z kampanii phisingowych zostanie uzgodniona z zamawiającym w zakresie typów maili i ich formy. | **TAK** |  |
| PH-4 | Raporty bieżące dotyczące kampanii phishingowej muszą zawierać:  Statystyki kampanii w tym:  Ilość wysłanych maili,  Ilość dostarczonych maili,  Ilość skompromitowanych kont pocztowych,  Informacje o użytkownikach, w tym:  Określenie poziomu ryzyka użytkownika dla organizacji,  Status realizacji kampanii przez użytkownika,  Status realizacji szkoleń przez użytkownika, | **TAK** |  |
| PH-5 | Planowanie Kampanii  Realistyczne Symulacje Ataków Phishingowych  Scenariusze dostosowane do Zamawiającego: Symulacje powinny odwzorowywać ataki, na które Zamawiający może być rzeczywiście narażony, np. fałszywe faktury, podrobione pisma urzędowe, próby wyłudzenia informacji o kontrahentach.  Zaawansowana personalizacja kampanii: Możliwość dostosowywania treści phishingowych do różnych działów Zamawiajacego, np. różne kampanie dla działu finansowego, kadr z uwzględnieniem języka specyficznego dla danego obszaru. | **TAK** |  |
| PH-6 | Śledzenie Postępów i Raportowanie  Zaawansowane narzędzia raportowe: Platforma powinna oferować szczegółowe raporty dotyczące wyników kampanii phishingowych i postępów w szkoleniach, z opcją dostosowania do wymagań urzędu.  Wizualizacja danych: Dashboardy i infografiki prezentujące kluczowe metryki, które pomagają w zrozumieniu skuteczności kampanii i szkoleń. | **TAK** |  |
| PH-7 | Bezpieczeństwo i Prywatność  Szyfrowanie danych wrażliwych: Pełne szyfrowanie danych osobowych i innych wrażliwych informacji zarówno podczas transmisji, jak i w spoczynku.  Zgodność z RODO i lokalnymi przepisami o ochronie danych: Zapewnienie, że wszystkie operacje na danych są zgodne z obowiązującymi przepisami o ochronie danych osobowych. | **TAK** |  |
| PH-8 | Zarządzanie Kampaniami  Automatyzacja procesów: Narzędzia do automatyzacji uruchamiania i zarządzania kampaniami phishingowymi, minimalizujące potrzebę interwencji manualnej.  Interaktywny feedback: Możliwość zgłaszania przez użytkowników podejrzanych wiadomości, co może być wykorzystane do poprawy przyszłych kampanii. | **TAK** |  |
| PH-9 | Wsparcie Techniczne i Szkoleniowe  Dostępność wsparcia technicznego: Łatwy dostęp do wsparcia technicznego w razie wystąpienia problemów z platformą.  Materiały pomocnicze dla administratorów: Kompleksowe przewodniki i materiały szkoleniowe, wspierające zarządzanie platformą. | **TAK** |  |
| PH-10 | Raport końcowy z zakończenia kampanii phishingowej powinien zawierać:  Podsumowanie Kampanii  Opis kampanii: Krótkie streszczenie celów kampanii, zastosowanych technik phishingowych, i grupy docelowej.  Okres przeprowadzenia kampanii: Data rozpoczęcia i zakończenia kampanii.  Statystyki Ogólne  Liczba wysłanych wiadomości: Ile e-maili phishingowych zostało wysłanych w ramach kampanii.  Procent otwartych e-maili: Jaki procent odbiorców otworzył e-mail.  Procent kliknięć w linki: Jaki procent osób kliknął w linki zawarte w e-mailach phishingowych.  Liczba wprowadzonych danych: Ile osób podało swoje dane na fałszywej stronie.  Analiza Zachowań Użytkowników  Typowe błędy: Jakie błędy najczęściej popełniali pracownicy, np. ignorowanie oznak ostrzegawczych.  Wzorce odpowiedzi: Czy istnieją konkretne wzorce w odpowiedziach różnych grup pracowników lub działów.  Porównanie z innymi kampaniami: Jak kampania wypada na tle danych statystycznych z innych kampanii pod względem efektywności i zachowań pracowników.  Szczegółowe Wyniki dla Różnych Grup Docelowych  Wyniki według działów: Szczegółowa analiza reakcji różnych działów lub grup zawodowych na kampanię.  Wyniki według lokalizacji: Jeśli urząd ma więcej niż jedną lokalizację, analiza, jak reakcje różniły się między lokalizacjami.  Rekomendacje i Ścieżki Naprawcze  Obszary wymagające poprawy: Wskazanie, które obszary wiedzy lub świadomości wymagają dodatkowych działań edukacyjnych.  Zaproponowanie działań szkoleniowych: Propozycje konkretnych szkoleń lub warsztatów, które mogłyby zwiększyć świadomość i umiejętności pracowników.  Plan poprawek: Krótkoterminowe i długoterminowe działania, które instytucja powinna podjąć, aby poprawić bezpieczeństwo informacyjne.  Feedback od Uczestników | **TAK** |  |
| EDU-1 | Pakiet szkoleniowy w którego skład wchodzą 5 szkoleń oraz moduły treningowe dostępne dla każdego pracownika w formie kursu online do samodzielnego przerobienia | **TAK** |  |
| EDU-2 | Poziom zdawalności testu zostanie ustawiony po konsultacjach z zamawiającym | **TAK** |  |
| EDU-3 | Zakres raportu końcowego z przeprowadzonych szkoleń:  Podsumowanie Szkolenia  Ocena Efektywności Szkolenia  Analiza osiągniętych celów szkoleniowych: Ocena, czy i w jakim stopniu osiągnięto cele szkoleniowe.  Rekomendacje dla przyszłych szkoleń: Sugestie dotyczące zmian w treści, formacie lub dostarczaniu materiału szkoleniowego, na podstawie analizy danych i feedbacku.  Działania Poprawkowe i Kontynuacja Edukacji  Zaplanowane działania poprawkowe: Działania zaplanowane w odpowiedzi na wykryte luki w wiedzy lub umiejętnościach.  Zaplanowane kolejne kroki szkoleniowe: Informacje o przyszłych szkoleniach lub kursach uzupełniających.  Podsumowanie i Wnioski  Ogólne wnioski: Podsumowanie kluczowych wniosków z przeprowadzonego szkolenia.  Zalecenia strategiczne: Zalecenia na poziomie organizacyjnym dotyczące dalszego rozwoju programów szkoleniowych z cyberbezpieczeństwa. | **TAK** |  |
| EDU-4 | Zakres podstawowy szkoleń:  Podstawowe pojęcia odnośnie bezpieczeństwa informacji, cyberbezpieczeństwa  Zagrożenia związane z cyfrową działalnością instytucji  Rodzaje zagrożeń w cyberprzestrzeni  Rodzaje zabezpieczeń, rodzaje działań zabezpieczających  Podstawy bezpiecznego zachowania w cyberprzestrzeni  Rozpoznawanie zagrożeń i im przeciwdziałanie  Bezpieczne hasła – jakie, jak je przechowywać  Bezpieczne poruszanie się w cyfrowym świecie – media społecznościowe, email, strony www, sklepy internetowe  Zasady bezpiecznej pracy w cyfrowym świecie  Nośniki zewnętrzne  Komunikatory i media społecznościowe  Poczta elektroniczna  Zagrożenia jakie można spotkać w Internecie,  Metodyka skutecznego oceniania wiarygodności otrzymanej wiadomości mailowej,  Najczęściej spotykane zagrożenia związane z korzystaniem z serwisów społecznościowych,  Czym jest ransomware i jak się przed nim bronić.  Zakres szkoleń dla kadry kierowniczej dodatkowo obejmuje:  Wdrożenie i utrzymanie systemu zarządzania bezpieczeństwem informacji  Źródła wymagań i zaleceń - norma ISO 27001 lub równoważna  Role i odpowiedzialności.  Klasyfikacja informacji.  Analiza ryzyka bezpieczeństwa informacji.  Zarządzanie ryzykiem bezpieczeństwa informacji.  Zabezpieczenia techniczne i organizacyjne.  Struktura dokumentacji systemu zarządzania.  Szkolenia pracowników.  Utrzymanie systemu zarządzania  Zarządzanie zdarzeniami i incydentami bezpieczeństwa | **TAK** |  |

**Parametry świadczenia usługi**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Wymaganie (Opis)** | **Parametr** | **Parametr wymagany** | **Potwierdzić spełnienie parametru / Podać wartość parametru** |
| SOC-P1 | Ilość korelacji wytwarzanych w SIEM | bez ograniczeń | **TAK** |  |
| SOC-P2 | Tworzenie kolejnych korelacji | bez opłat | **TAK** |  |
| SOC-P3 | Ilość podłączonych źródeł danych do systemu SIEM | bez limitu | **TAK** |  |
| SOC-P4 | Ilość przetwarzanych zdarzeń i incydentów bezpieczeństwa w miesiącu | bez ograniczeń | **TAK** |  |
| SOC-P5 | Liczba scenariuszy działania | bez ograniczeń | **TAK** |  |
| SOC-P6 | Ilość przetwarzanych danych w systemie SIEM | bez ograniczeń | **TAK** |  |
| SOC-P7 | Ilość dostępnych w miesiącu godzin inżyniera wsparcia technicznego | > lub = 8 h | **TAK** |  |
| SOC-P8 | Ilość godzin dla usług III linii SOC rozliczanych w roku | > lub = 160h | **TAK** |  |
| SOC-P9 | Liczba endpointów odjętych usługą | > lub = 450 | **TAK** |  |
| SOC-P10 | Liczba osób objętych szkoleniem | > lub = 600 | **TAK** |  |
| SOC-P11 | Liczba osób objętych kampanią phishingową | > lub = 600 | **TAK** |  |
| SOC-P12 | Liczba źródeł:   * Urządzenia brzegowe – > lub = 6 (w tym dwa działające w klastrze HA) * Serwery i maszyny wirtualne - > lub = 75 * Przełączniki sieciowe – > lub = 35 fizycznych urządzeń, część urządzeń jest podłączona w stack’i * Punkty dostępowe WiFi (Access Point’y) – > lub = 27 | x | **TAK** |  |
| SOC-P13 | Liczba analityków i inżynierów bezpieczeństwa zatrudnionych w SOC tworzących I, II i III linię SOC. Osoby pracująca w poszczególnych liniach powinny dysponować minimum 2 letnim doświadczeniem pracy w cyberbezpieczeństwie. | > lub = 12 | **TAK** |  |

**Parametry świadczenia usług – czasy maksymalne**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Zadanie** | **Wymagany czas reakcji** | **Wymagany czas realizacji** | **Potwierdzić spełnienie parametru / Podać wartość parametru** |
| SOC-PCM1 | SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia lub przekazanie  do SOC L2 | 15 minut | 2 godziny |  |
| SOC-PCM2 | SOC - L2, 24/7/365, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji | 1 godzina | 8 godzin |  |
| SOC-PCM3 | SOC L2 SOAR 24/7/365, zautomatyzowane podjęcie  incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji | 15 minut | 1 godzina |  |
| SOC-PCM4 | SOC L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji | 8 godzin | 40 godzin |  |

**Poziom świadczenia usług (SLA) monitorowania i reakcji na cyberzagrożenia**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Wymaganie (Opis)** | **Parametr wymagany** | **Parametr oferowany** |
| Usługa monitorowania bezpieczeństwa jest świadczona przez SOC z następującymi minimalnymi poziomami SLA dla działań zespołu SOC. | | | |
| SOC-SLA1 | **Pierwsza Linia Wsparcia**   1. czasy dla pierwszych 75 Incydentów każdego dnia, pozostałe zadania realizowane w trybie „Best Effort”:  |  |  |  | | --- | --- | --- | | Priorytet incydentu | Czas od wykrycia do | | | Podjęcia działania | Realizacji | | Krytyczny | 15 min | 2 h | | Wysoki | 60 min | 3 h | | Średni | 90 min | 6 h | | Niski | 2 h | 12 h | | Informacyjny | 4 h | 24 h |  1. dostępność usługi w trybie 24/7/365. | TAK |  |
| SOC-SLA2 | **Druga Linia Wsparcia**   1. czasy dla pierwszych Incydentów każdego dnia, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:  |  |  |  | | --- | --- | --- | | Priorytet incydentu | Czas od wykrycia do | | | Podjęcia działania | Realizacji | | Krytyczny | 30 min | 24 h | | Wysoki | 60 min | 24 h | | Średni | 2 h | 2 dni | | Niski | 4 h | 4 dni | | Informacyjny | 8 h | 7 dni |  1. dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 18:00. Dodatkowo dla incydentów o priorytecie Wysokim - w trybie „on-call” w dni robocze w godzinach 00:00 do 8:00 i 18:00 do 24:00, w pozostałe dni w trybie „on-call” w godzinach 00:00 do 23:59. | TAK |  |
| SOC-SLA3 | **Trzecia Linia Wsparcia/Linia wsparcia**  czasy dla pierwszych Incydentów, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:   |  |  |  | | --- | --- | --- | | Priorytet incydentu | Czas od wykrycia do | | | Podjęcia działania | Realizacji | | Krytyczny | 2 h | 7 dni | | Wysoki | 4 h | 7 dni | | TAK |  |
| **Definicje poziomu incydentu** | | | |
|  | **Poziom KRYTYCZNY**   * + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją rozporządzenia RODO.   + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją tajemnicy przedsiębiorstwa.   + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika:   + Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia  i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min).   + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych.   + Nieautoryzowane dysponowanie uprawnieniami administracyjnymi.   + Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego.   + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności.   + Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych;   + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności;   + Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware);   + Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;   + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego. | TAK |  |
|  | **Poziom WYSOKI**  Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika:   * Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min). * Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych. * Nieautoryzowane dysponowanie uprawnieniami administracyjnymi. * Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego. * Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności. * Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; * Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; * Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); * Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;   Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego. | TAK |  |
|  | **Poziom ŚREDNI**  Zebrane dowody w systemach realizujących monitoring bezpieczeństwa zaświadczą o wystąpieniu co najmniej jednego wskaźnika:   * + Ujawnienie nieznanego przez VirusTotal lub przez inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu.   + Ujawnienie podatności systemów lub infrastruktury mających wartość CVSS powyżej 7.   + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej.   + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego. | TAK |  |
|  | **Poziom NISKI**  Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym.   * + Częściowo personalizowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym.   + Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa.   + Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome działanie. | TAK |  |
|  | Poziom INFORMACYJNY   * Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa. | TAK |  |

# SIEM/SOAR

Wymagania w zakresie wdrożenia, uruchomienia i utrzymania rozwiązania hybrydowego łączącego funkcjonalności klasy SIEM (Security Information and Event Management) i SOAR (Security Orchestration, Automation and Response)

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Wymaganie (Opis)** | **Parametr wymagany** | **Parametr oferowany** |
| SIEM-1 | System musi posiadać możliwość centralnego zbierania i zarządzania logami | **TAK** |  |
| SIEM-2 | System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet, analiza następuje wówczas tylko w oparciu o logi wewnętrzne | **TAK** |  |
| SIEM-3 | System musi zapewniać efektywną obsługę co najmniej 4000 EPS lub 80 GB danych dziennie | **TAK** |  |
| SIEM-4 | System musi zapewniać retencję danych w okresie minimum 730 dni (retencja danych zależna jest od posiadanych przez klienta zasobów na których jest instalowany system zbierania logów). | **TAK** |  |
| SIEM-5 | Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu. | **TAK** |  |
| SIEM-6 | System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska. | **TAK** |  |
| SIEM-7 | System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowań, pełną historię operacji, realizowanych zapytań, zmian uprawnień. | **TAK** |  |
| SIEM-8 | System musi pozwalać na tworzenie parserów z poziomu GUI | **TAK** |  |
| SIEM-9 | System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie. | **TAK** |  |
| SIEM-10 | System musi zapewniać wizualizację danych w postaci oryginalnych logów, list, wykresów i diagramów. | **TAK** |  |
| SIEM-11 | Wizualizacja danych musi być możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach. | **TAK** |  |
| SIEM-12 | System musi umożliwiać eksport danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych. | **TAK** |  |
| SIEM-13 | System musi zapewniać parsowanie spływających do niego wiadomości w formatach:  • Syslog,  • Flat file,  • Event log,  • WMI,  • XML,  • JSON,  • JDBC/ODBC  • CSV | **TAK** |  |
| SIEM-14 | System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem. | **TAK** |  |
| SIEM-15 | System do przyjmowania zdarzeń musi wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe. | **TAK** |  |
| SIEM-16 | System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów. | **TAK** |  |
| SIEM-17 | Interfejs musi umożliwiać parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie jest konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwia zastosowanie innego parsera. | **TAK** |  |
| SIEM-18 | System musi posiadać predefiniowany zestaw parserów zdarzeń. | **TAK** |  |
| SIEM-19 | System musi wspierać geolokalizację zdarzeń na bazie adresów IP. | **TAK** |  |
| SIEM-20 | System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. | **TAK** |  |
| SIEM-21 | Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach. | **TAK** |  |
| SIEM-22 | System musi pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu. | **TAK** |  |
| SIEM-23 | Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System umożliwia budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów. | **TAK** |  |
| SIEM-24 | System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym. | **TAK** |  |
| SIEM-25 | System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących. | **TAK** |  |
| SIEM-26 | System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie:  • Wykrycia dowolnej treści w logach,  • Wykrycia wystąpienia wartości pola na wybranej liście,  • Wykrycia niewystępowania wartości pola na wybranej liście,  • Wykrycia zmiany jednego z kilku pól,  • Wykrycia zdarzeń występujących z zadaną częstotliwością,  • Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,  • Wykrycia zaniku Wiadomości,  • Wykrycia nowej wartości pola w zadanym okresie czasu,  • Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności | **TAK** |  |
| SIEM-27 | System musi pozwalać na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. | **TAK** |  |
| SIEM-28 | System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych | **TAK** |  |
| SIEM-29 | Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (powiadamianie email, opcjonalnie SMS, czat). | **TAK** |  |
| SIEM-30 | System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. | **TAK** |  |
| SIEM-31 | Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać przypisany poziom istotności. Jest możliwość modyfikacji poziomu istotności dla każdej reguły. | **TAK** |  |
| SIEM-32 | Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów. | **TAK** |  |
| SIEM-33 | System ma umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych. | **TAK** |  |
| SISO-1 | Wykonawca zapewnia wdrożenie, uruchomienie i utrzymanie systemu klasy SIEM i SOAR służącego do zbierania i korelacji logów z systemów Zamawiającego przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych | **TAK** |  |
| SISO-2 | W ramach wdrożenia systemu SIEM i podłączenia systemów i urządzeń Zamawiającego Wykonawca zobowiązany jest do przeprowadzenia audytu/ankietowania, które wskaże kluczowe z punktu widzenia cyberbezpieczeństwa systemy, które należy monitorować, audyt przeprowadzony wraz z Zamawiającym musi wskazać również, którym systemom przypisany zostanie wysoki, średni i niski priorytet w zakresie czasu podłączenia do systemu SIEM; zamawiający może wyrazić zgodę na odstąpienie od integracji systemów o niskim priorytecie pod warunkiem, że Wykonawca przedstawi argumenty na brak wpływu rozwiązania na bezpieczeństwo Zamawiającego | **TAK** |  |
| SISO-3 | wykonanie playbooków dla wdrożonego systemu SOAR zapewniającego zabezpieczenie systemów. Wykonawca zobowiązany jest również do wskazania zmian i optymalizacji w konfiguracji wykorzystywanych urządzeń Zamawiającego typu UTM, WAF, XDR, AV i innych w celu wykorzystania pełnego potencjału tych rozwiązań w ramach SOC | **TAK** |  |
| SISO-4 | Zamawiający zakłada, że w ciągu każdego roku trwania umowy do obsługi może zostać dołączonych kolejnych 20 systemów i/lub urządzeń | **TAK** |  |
| SISO-5 | System SIEM i SOAR muszą przechowywać hasła do monitorowanych systemów, bez możliwości dostępu do nich (haseł) pracowników SOC. | **TAK** |  |
| SISO-6 | Wykonawca jest zobowiązany dostarczyć/posiadać wszystkie niezbędne licencje do uruchomienia systemów SIEM i SOAR pozwalające na świadczenie usług na systemach, na czas trwania umowy; w przypadku systemów instalowanych | **TAK** |  |
| SISO-7 | system SIEM i SOAR muszą umożliwić autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność minimum w zakresie login/logoff, zmiana konfiguracji systemu, wykonane akcje; Zamawiający oczekuje minimum dostępu read-only dla systemu | **TAK** |  |
| SISO-8 | system klasy SIEM musi pozwolić na zbieranie logów z systemów Zamawiającego, w szczególności pozwolić na zbieranie informacji z końcówek i systemów klasy XDR oraz z urządzeń UTM; system klasy SOAR musi umieć wykonywać akcje na końcówkach z wykorzystaniem systemów XDR oraz urządzeniach typu UTM | **TAK** |  |
| SISO-9 | system SIEM musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck) | **TAK** |  |
| SISO-10 | system SIEM musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu | **TAK** |  |
| SISO-11 | system SIEM musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez integrację z AD i pobieranie danych odnośnie użytkowników i zasobów i korelowanie ich ze zdarzeniami wykrytymi w infrastrukturze Zamawiającego | **TAK** |  |
| SISO-12 | Wykonawca musi dostosowywać na bieżąco reguły korelacyjne do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alarmy | **TAK** |  |
| SISO-13 | system SOAR musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydenty | **TAK** |  |
| SISO-14 | Wykonawca musi dostosowywać na bieżąco playbooki do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować automatyczną reakcję na incydenty | **TAK** |  |
| SISO-15 | aktywności użytkowników systemu SOAR musi być śledzona i logowana na potrzeby ewentualnej analizy | **TAK** |  |

# Uwagi dotyczące całego Załącznika nr 2:

Zmiana treści lub jej brak, a także zmiana kolejności wierszy lub kolumn oraz ich brak spowoduje odrzucenie oferty. Powyższe warunki graniczne stanowią wymagania odcinające. Niespełnienie nawet jednego z ww. wymagań spowoduje odrzucenie oferty.

W celu potwierdzenia zgodności oferowanych usług z wymaganiami, cechami lub kryteriami określonymi w opisie przedmiotu zamówienia, Zamawiający wymaga złożenia wraz z ofertą:

1. Certyfikat dla aktualnie obowiązującego wydania normy ISO/IEC 27001:2022 bądź jej polski odpowiednik PN-EN ISO/IEC 27001:2023-08 wydany przez jednostkę certyfikującą posiadającą akredytację Polskiego Centrum Akredytacji (PCA) dla jednostek certyfikujących systemy zarządzania w rozumieniu ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. 2019, poz. 544) lub równoważną akredytację międzynarodową instytucji będącej członkiem IAF i obejmujący swym zakresem usługi SOC.
2. Certyfikat dla aktualnie obowiązującego wydania normy ISO/IEC 22301:2020-04 bądź jej polski odpowiednik PN-EN ISO/IEC 27001:22301:2020-04 wydany przez jednostkę certyfikującą posiadającą akredytację Polskiego Centrum Akredytacji (PCA) dla jednostek certyfikujących systemy zarządzania w rozumieniu ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. 2019, poz. 544) lub równoważną akredytację międzynarodową instytucji będącej członkiem IAF i obejmujący swym zakresem usługi SOC.

Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane świadczenia spełniają określone przez zamawiającego wymagania, cechy lub kryteria.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Podpis osoby upoważnionej do reprezentacji Oferenta*