

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia.

- 1.1. Przedmiotem zamówienia jest **dostawa licencji systemu wykrywania oraz reagowania na zagrożenia na stacjach końcowych.**
- 1.2. Realizacja przedmiotu zamówienia polega na udostępnieniu i wdrożeniu rozwiązania typu EDR (Endpoint Detection and Response) (zwanego dalej Systemem) wraz niezbędnymi licencjami oraz świadczeniu usługi wsparcia dla Systemu.
- 1.3. W szczególności przedmiot zamówienia obejmuje:
 1. Dostarczenie niezbędnych licencji pozwalających na dostęp do serwera zarządzającego Systemem przez okres co najmniej 36 miesięcy.
 2. Wykonanie konfiguracji i parametryzacji Systemu.
 3. Świadczenie usług gwarancyjnych producenta oprogramowania przez okres 36 miesięcy od daty podpisania Protokołu odbioru.
- 1.4. Środowisko Zamawiającego składa się z **950** hostów, w następującej konfiguracji:
 1. Stacje robocze oparte o system operacyjny z rodziny MS Windows w liczbie do 850 sztuk.
 2. Serwery typu Linux i Windows Server w proporcji 80%/20% w liczbie 100 sztuk.

2. Harmonogram realizacji przedmiotu zamówienia:

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 30 Dni roboczych, liczonym od dnia zawarcia Umowy, w podziale na niżej określone etapy:

Etap I – Opracowanie harmonogramu wdrożenia.

W ramach realizacji etapu Wykonawca:

- 2.1. W terminie do 5 dni od daty podpisania umowy, przygotuje i przedstawi Zamawiającemu harmonogram wdrożenia Systemu.
- 2.2. Przygotuje opis niezbędnych prac w celu wdrożenia Systemu wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającego i Wykonawcę w modelu RACI.
- 2.3. Przedstawi listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi minimalnie numer telefonu komórkowego, adres email.
- 2.4. Opracuje scenariusze testowe Systemu:
 1. Scenariusze testowe muszą zawierać propozycje testów funkcjonalnych i bezpieczeństwa. Scenariusze testowe będą przygotowane przez Wykonawcę i wymagają zatwierdzenia przez Zamawiającego.

Etap II - Analiza przedwdrożeniowa.

W ramach realizacji etapu Wykonawca:

- 2.5. Wykona analizę infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem, potrzeb użytkownika i wymagań funkcjonalnych odnośnie konfiguracji Systemu, której wynikiem będzie plan wdrożenia Systemu u Zamawiającego.
- 2.6. Uzgodni z Zamawiającym polityki/reguły bezpieczeństwa Systemu oraz ich wdrożenie.
- 2.7. Uzgodni z Zamawiającym zakres danych przetwarzanych w Systemie, w szczególności danych wykorzystywanych do poszukiwania zagrożeń na chronionych hostach.
- 2.8. Utworzy i udostępni konta dostępowe do serwera zarządzającego Systemu

Etap III – Wdrożenie, konfiguracja i testy Systemu.

W ramach realizacji etapu Wykonawca:

- 2.9. Wdroży w infrastrukturze Zamawiającego System zgodnie z zaakceptowanym harmonogramem, planem wdrożenia Systemu oraz Projektem technicznym Systemu z uwzględnieniem analizy przedwdrożeniowej oraz warunkami opisanymi w pkt 3 OPZ.
- 2.10. Wykona pełną konfigurację i parametryzację Systemu zgodnie z Projektem technicznym będącym wynikiem analizy przedwdrożeniowej .
- 2.11. Przeprowadzi testy akceptacyjne.
- 2.12. Dostarczy Dokumentację powykonawczą dla Zamawiającego.
- 2.13. Przeprowadzi instruktaż dla użytkowników Systemu zgodnie z warunkami opisanymi w pkt. 6.

3. Wdrożenie Systemu.

W ramach realizacji Etapu III, Wykonawca dokona wdrożenia Systemu , rozumianego jako:

- 3.1. Przygotowanie konfiguracji Systemu zgodnie z projektem technicznym Systemu oraz wdrożenie polityk bezpieczeństwa odzwierciedlających obecnie posiadaną konfigurację i wiedzę o aktualnych zagrożeniach.
- 3.2. Przeprowadzenie testów funkcjonalnych zainstalowanego Systemu, zgodnie z opracowanymi w pkt 2.4 OPZ scenariuszami, z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 4.3 Obligatoryjnych funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.
- 3.3. Przygotowanie i dostarczenie Dokumentacji powykonawczej oraz dokumentacji użytkownika (administratora/operatora) systemu. Dokumentacja powinna zawierać architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów akceptacyjnych i funkcjonalnych rozwiązania, opis konfiguracji systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora systemu. Za pełne wdrożenie Systemu uznaje się uruchomienie systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, dostarczenie kompletu dokumentacji, przeprowadzenie instruktażu opisanego w pkt 6, obustronne podpisanie protokołu odbioru.

4. Wymagania minimalne dla Systemu EDR:

4.1. Architektura Systemu.

1. Wszystkie centralne elementy rozwiązania, takie jak centralny serwer zarządzający i bazy danych będą dostarczone w formie SaaS z dostępnością w trybie 24h / 7 przez cały rok na warunkach opisanych w pkt. 5 OPZ .
2. Dane muszą być przetwarzane w EOG (Europejski Obszar Gospodarczy).
3. Retencja danych wykorzystywanych do aktywnego poszukiwania zagrożeń (threat hunting'u) musi wynosić co najmniej 14 dni.
4. System musi być dostępny przez interfejs www i obsługiwany za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersji na dzień składania oferty.
5. Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Windows 10 i nowszych, Microsoft Server 2012 i nowszych, oraz Linux (CentOS/Debian)).
6. System powinien chronić zarządzane punkty końcowe działające w systemach połączonych, systemach rozproszonych i niezależnych środowiskach.

7. Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania, w tym możliwość wdrożenia rozwiązania przez Zasady Grupy w Windows Server (Group Policy) itp.
8. Elementy zarządzające i analityczne Systemu muszą być skalowane w celu obsługi co najmniej 3000 punktów końcowych.
9. Ochrona na stacji końcowej musi być w sytuacjach awaryjnych zapewniona bez dostępu do Internetu.
10. Wymagana jest możliwość wykorzystania mechanizmu serwera proxy do komunikacji z Internetem.

4.2. Zarządzanie Systemem.

1. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika / administratora Systemu.
2. System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.
3. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu, analityk itp.).
4. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.
5. System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb różnych możliwych do skonfigurowania ról. Dashboard powinien umożliwiać schodzenie do szczegółów poszczególnych elementów do poziomu informacji podstawowych.

4.3. Obligatoryjne funkcjonalności Systemu.

- 1 System musi obsługiwać funkcjonalności Next Generation EPP (Endpoint Protection Platform) oraz EDR (Endpoint Detection and Response) w jednym autonomicznym agencie
- 2 System musi umożliwiać automatyczne wykrywanie , rejestrowanie, analizowanie oraz reagowanie w zakresie parametrów i zdarzeń definiowanych przez producenta lub skonfigurowanych i wybranych przez użytkownika w celu oceny działania systemu monitorowanego, wsparcia zarządzania ryzykiem oraz umożliwienia działań związanych z informatyką śledczą i analizą po włamaniową.
- 3 System musi identyfikować zaawansowane zagrożenia, takie jak ataki bezplikowe, 0-day malware czy wykorzystywanie podatności posiadanego software/hardware bez korzystania z silników reputacji lub silników detekcji opartej o sygnatury. Przez silnik reputacyjny Zamawiający rozumie identyfikację zagrożeń z wykorzystaniem następujących elementów reputacji: adresy IP, DNS, URL, skróty/hashe.
- 4 System musi wykorzystywać statyczne oraz dynamiczne uczenie maszynowe do identyfikacji zagrożeń, również tych, które nie są wcześniej znane.
- 5 Agent Systemu musi być w pełni autonomiczny, co oznacza że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani żadnych zasobów zewnętrznych od agenta.

- 6 Wykrywanie i reagowanie na zaawansowane zagrożenia (0-day, bezplikowe, oparte na pamięci RAM, Exploits 0-Day, ransomware, crypto miners, lateral movement, APT) musi być możliwe w czasie rzeczywistym, nie może zależeć od stanu sieciowej stacji (agent musi realizować te same funkcjonalności w trybie online i offline) oraz nie może wymagać innego rodzaju zewnętrznych zasobów.
- 7 System musi automatycznie reagować na pojawiające się zagrożenia, łagodząc zagrożenia w czasie zbliżonym do rzeczywistego, w autonomiczny sposób, z następującymi opcjami odpowiedzi na zagrożenie, definiowane przez politykę bezpieczeństwa:
 - 7.1 Ostrzeżenie: taka notyfikacja musi być stała, nawet jeśli polityka nie jest w trybie ochrony.
 - 7.2 Zabij proces: Aktywna zawartość w dokumentach, plikach wykonywalnych i procesach podrzędnych musi zostać zatrzymana. Agent Systemu musi włączyć funkcję zabicia procesu dla procesów, które działają wbrew normalnemu zachowaniu stacji końcowej lub nie pasują do działań aplikacji, w której ukrywa się proces.
 - 7.3 Kwarantanna: Agent Systemu musi zatrzymać procesy, zaszyfrować plik wykonywalny oraz przenieść go na ograniczoną ścieżkę. W przypadku znanych zagrożeń, agent Systemu przed wykonaniem musi automatycznie je unieszkodliwić.
 - 7.4 Odłącz się od sieci: (kwarantanna sieciowa lub izolacja sieciowa) W przypadku włączenia tej opcji Agent Systemu musi komunikować się wyłącznie z konsolą zarządzającą. Stacja końcowa nie może komunikować się z innymi elementami w sieci. Wszystkie działania na konsoli zarządzania muszą działać niezależnie od stanu izolacji sieci agenta Systemu.
 - 7.5 Funkcja Naprawy (Remediate): Agent Systemu zatrzymuje procesy, poddaje kwarantannie pliki binarne, usuwa połączone biblioteki, usuwa pliki źródłowe i przywraca konfigurację systemu operacyjnego, aplikacji i ustawień użytkownika do stanu sprzed rozpoczęcia ataku.
 - 7.6 Rollback: Agent Systemu przywraca stan stacji końcowej do stanu z momentu utworzenia migawki VSS (Volume Shadow Copy), cofając zmiany wprowadzone przez złośliwy proces i skojarzone z nim zasoby. Agent Systemu musi autonomicznie i w czasie zbliżonym do rzeczywistego przywrócić dane z chronionego hosta w przypadku ataku z wykorzystaniem szkodliwego oprogramowania typu ransomware.
- 8 System musi obsługiwać następujące mechanizmy wykrywania złośliwego oprogramowania :
 - 8.1 Przed wykonaniem (Pre-Execution):
 - 8.1.1 Na podstawie plików za pośrednictwem silnika reputacji. Dla działania funkcjonalności dopuszcza się zależność od chmury lub serwera zarządzającego przy założeniu, że tego typu wykrywanie będzie dotyczyło skanowania całego dysku i odbywało się wyłącznie podczas początkowej instalacji.

8.1.2 Na podstawie plików za pośrednictwem statycznej analizy kodu z wykorzystaniem algorytmów uczenia maszynowego. Analiza kodu musi odbywać się autonomicznie na stacji końcowej, bez zewnętrznych zależności lub zewnętrznego przetwarzania. Funkcjonalność nie może wymagać do działania uwzględnienia znanych IoC (DNS, IP, URL, HASH), a detekcja tego typu musi działać w czasie rzeczywistym podczas dostępu do systemu operacyjnego lub danego pliku.

8.2 W czasie wykonywania (Run-Time):

8.2.1 Agent Systemu musi identyfikować i reagować na ataki z wykorzystaniem wyrafinowanych technik hackerskich (ataki bezplikowe, podatności i malware 0-day, złośliwe skrypt, lateral movement, oprogramowanie ransomware, trojany, APT itp.) Identyfikacja tych zagrożeń nie może wymagać zewnętrznych zależności, interwencji człowieka lub analizy danych poza chronioną stacją końcową. Funkcjonalność musi być realizowana w czasie zbliżonym do rzeczywistego poprzez wykorzystanie algorytmów sztucznej inteligencji.

- 9 System musi zapewniać silny mechanizm „Anti-Tamper”, czyli mechanizmy ochrony przed manipulacją oprogramowaniem przez malware lub użytkownika końcowego. Mechanizm musi być chroniony unikalnym hasłem dla każdego komputera końcowego. Stan Wł./Wył. ochrony przed manipulacją powinien być opcją konfigurowalną w polityce bezpieczeństwa.
- 10 Polityka bezpieczeństwa Systemu musi zapewniać opcję włączenia lub wyłączenia poszczególnych silników detekcyjnych.
- 11 System musi posiadać otwarty interfejs API który umożliwia integracje z innymi rozwiązaniami, monitorowanie środowiska oraz automatyzację niektórych z procesów. Dokumentacja interfejsu API powinna być natywnie dostępna z poziomu konsoli zarządzania.
- 12 System musi obsługiwać architekturę typu Multi-Site lub Multi-Tenancy, w celu całkowitego odseparowania utworzonych w systemie instancji i zapewnić odpowiedni dostęp administracyjny do konkretnej lokacji utworzonej zgodnie z modelem Multi-Site.
- 13 System musi obsługiwać uwierzytelnianie SSO - SAMLv2.
- 14 System musi obsługiwać następujące formaty syslog: CEF, CEF2, RFC-5424, STIX i IOC. System musi obsługiwać certyfikaty SSL i X.509 do szyfrowania i uwierzytelniania transportu syslog.
- 15 System musi zapewniać możliwość wysyłania wiadomości tekstowych do użytkownika stacji końcowej, bezpośrednio z konsoli zarządzania, nawet kiedy agent pracujący na stacji, znajduje się w trybie izolacji sieci / kwarantanny sieciowej.
- 16 System musi umożliwiać zintegrowane z usługą Active Directory w celu automatycznego przypisywania agentów do grup i powiązania ich z zasadami AD. System nie może łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Praca Systemu nie może zależeć od stanu usługi AD.

- 17 Dashboard Systemu musi umożliwiać wyświetlanie chronionych hostów oraz umożliwiać filtrowanie na podstawie ich atrybutów takich jak: OS, typ stacji końcowej, wersja agenta, występujące podatności, atrybuty AD, informacje telemetryczne, adresacja IP, charakterystyki hardware, adresy Mac, interfejsy, nazwa host. Lista powinna być dostępna do przeglądania w celu inwentaryzacji hostów, stosowania akcji dla podzbioru stacji końcowych lub mapowania stacji końcowych do grup. Musi zapewniać opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetry, stan stacji, aplikacje oraz zapewniać następujące opcje działania: Odłącz/ Połącz się od sieci (kwarantanna sieciowa), Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia.
- 18 Polityka ochrony stacji musi umożliwiać odpowiedź na wykryte zagrożenie w oparciu o kwalifikację zdarzenia (zagrożenie [Malicious Threat] czy podejrzane działanie [Suspicious Threat]). Odpowiedź na zagrożenie powinna umożliwiać wybranie opcji ostrzegaj lub opcji aktywnej ochrony w oparciu o klasyfikację zagrożenia. Aktywna odpowiedź na zagrożenie, powinna być wykonywana przez agenta Systemu niezależnie od stanu sieciowego (online, offline).
- 19 System musi zapewniać funkcjonalność lokalnego firewall'a dla chronionej stacji końcowej. Ochrona firewall musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Reguły firewall'a powinny umożliwiać uwzględnienie następujących parametrów: FQDN , IP, CIDR. Funkcjonalność musi być obsługiwana dla systemów operacyjnych Windows oraz Linux.
- 20 System musi posiadać funkcjonalność kontroli urządzeń, które próbują uzyskać dostęp do chronionej stacji. Kontrola urządzeń musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Wymagana jest obsługa kontroli urządzeń dla następujących interfejsów: USB i Bluetooth .
- 21 System musi zarządzać podatnościami aplikacji zainstalowanych na chronionym hoście i dostarczać informacji z CVE związanych z wykrytą podatnością.
- 22 System musi posiadać możliwość automatycznego i autonomicznego wykonywania wstępnego indeksowania i wstępnego korelowania zdarzeń, w momencie ich wystąpienia w chronionym środowisku. Indeksowanie powinno odbywać się w czasie rzeczywistym, a proces ten powinien odbywać się na chronionej stacji, a nie w chmurze. Powiązane ze sobą zdarzenia powinny posiadać unikalny identyfikator, który umożliwi zidentyfikować grupę zdarzeń które są ze sobą powiązane. Zapytanie zawierające tego typu identyfikator powinno zwrócić informację o wszystkich zdarzeniach (IP, DNS, PLIKI, REJESTRY, PROCESY, URL itp.) składających się na daną sytuację, niezależnie od tego czy jest ona związana ze złośliwym oprogramowaniem, czy nie. Dashboard Systemu powinien zawierać eksplorator „drzewa procesów” do graficznej wizualizacji i analizy procesów które składały się na dane zdarzenie.
- 23 System musi umożliwiać budowanie własnych reguły detekcyjnych na podstawie zapytań (EDR / XDR) przekształcanych w automatyczne reguły wykrywające w celu generowania alertów oraz uruchamiania automatycznych odpowiedzi w momencie ich wykrycia.
- 24 System musi zapewniać funkcjonalność Full Remote Shell w celu wykonywania

poleceń na stacji końcowej z uwzględnieniem trybu izolacji sieciowej. System musi zapisywać transkrypcję zestawionej sesji. Transkrypcja musi być chroniona hasłem, a dostęp do powłoki zdalnej powinien wymuszać na Administratorze uwierzytelnianie dwuskładnikowe (2FA) w celu udzielenia dostępu. Funkcjonalność ta powinna być możliwa do włączenia / wyłączenia w polityce bezpieczeństwa Systemu.

4.4 Dodatkowe funkcjonalności Systemu

1. System musi obsługiwać uwierzytelnianie dwuskładnikowe (2FA) w celu uzyskania dostępu administracyjnego.
2. Możliwość odinstalowania rozwiązania powinno zapewniać, że po wykonaniu procesów odinstalowywania nie pozostaną żadne zależności/artefakty, które będą wpływać na poprawne działanie systemu stacji końcowej.
3. Rozwiązanie powinno obsługiwać szybkie rozsyłanie (w ciągu maksymalnie kilku minut) zmian konfiguracji z serwera zarządzania do wszystkich zainstalowanych agentów Systemu.

5. Wsparcie

5.1 System musi być dostarczony wraz z usługą wsparcia technicznego dostarczoną przez producenta rozwiązania.

5.2 Wsparcie techniczne musi uwzględniać rozwiązywanie problemów z dostępem do platformy, błędów działania, wydajności i aktualizacji agenta Systemu. W następującym zakresie czasowym:

Priorytet	Czas podjęcia	Czas na rozwiązanie
Błąd krytyczny	Do 2 godzin dnia roboczego	Do 8 godzin dnia roboczego
Błąd istotny	Do 6 godzin dnia roboczego	Do 5 dni roboczych

Przy czym:

- 1) błąd krytyczny to błąd, który uniemożliwia korzystanie z Systemu.
- 2) błąd istotny to błąd, inny niż błąd krytyczny, w szczególności taki błąd, który ma niewielki bezpośredni wpływ na działanie i bezpieczeństwo Systemu, a wszystkie podstawowe funkcjonalności są zachowane.
- 3) Czas rozwiązania to czas od momentu zgłoszenia błędu do momentu wprowadzenia poprawek przywracających prawidłowe, bezbłędne korzystanie z Systemu.
Czas podjęcia - okres od momentu zgłoszenia błędu do momentu podjęcia pierwszych czynności diagnostycznych przez Wykonawcę.

5.3 Usługa wsparcia musi być dostępna w trybie 24 / 7 z możliwością zgłaszania problemów za pomocą telefonu, wiadomości e-mail lub dedykowanego portalu www.

5.4 Wsparcie musi zapewniać dostęp do bazy wiedzy producenta oraz materiałów szkoleniowych producenta.

5.5 W ramach usługi wsparcia wymaga się od konsultanta wsparcia w zakresie dostosowywania zasad i najlepszych praktyk, przypadków użycia oraz architektury rozwiązania.

5.6 Dostęp do serwerów zarządzających musi być realizowany w trybie 24/7 z roczną dostępnością (RDS) na poziomie ...% (Zamawiający wymaga aby maksymalna wartość

parametru RDS nie była mniejsza niż 99%).

5.7 RDS oblicza się dla okresu rocznego od daty uruchomienia Systemu do końca 12-go pełnego okresu użytkowania, a następnie dla kolejnych 12-tu pełnych okresów użytkowania.

5.6.1 Parametr RDS obliczany jest zgodnie z poniższym wzorem:

$$\text{RDS [\%]} = \frac{\text{czas całkowity} - \sum \text{czas awarii}}{\text{czas całkowity}} \times 100 \text{ [\%]}$$

Do powyższych kalkulacji przyjmuje się:

- 1) czas całkowity (12 pełnych okresów rozliczeniowych), jako ujednoliconą liczbę 365 dni w roku tj. 8 760 godzin w roku (czas całkowity);
- 2) każda rozpoczęta godzina Awarii liczona jest jako pełna godzina Awarii.

5.6.2 Z obliczenia parametru RDS wyłączane są przerwy wynikające z:

- 1) prac utrzymaniowych sieci operatorów międzynarodowych i krajowych. Przerwy w działaniu Systemu nie będą obejmować przerw wynikających z prowadzenia prac konserwacyjnych zleconych Wykonawcy przez Zamawiającego lub leżących po jego stronie,
- 2) działań lub zaniechania działania przez Zamawiającego lub użytkowników usług upoważnionych przez Zamawiającego, powodujących niedostępność Systemu,
- 3) planowanych prac.

6. Instruktaż dla pracowników Zamawiającego

Wykonawca przeprowadzi dla nie więcej niż 8 pracowników Zamawiającego instruktaż, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu administratora oraz użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji Systemu w celu szybkiego wykrywania działań i zachowań złośliwego oprogramowania oraz badania incydentów bezpieczeństwa za pomocą zdefiniowanych reguł filtrujących / korelacyjnych.

- 6.1. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.
- 6.2. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu opisanego w pkt 3.
- 6.3. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą.
- 6.4. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.
- 6.5. Instruktaż będzie trwał minimum 3 Dni Robocze (łącznie minimum 24 godzin zegarowych).
- 6.6. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.
- 6.7. Wykonawca musi posiadać autoryzację producenta Systemu w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego Systemu.

- 6.8. Dla uczestników instruktażu Wykonawca przygotowuje środowisko testowe z zainstalowaną wersją Systemu tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych.
- 6.9. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu;
- 6.10. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019. poz. 1231) będą udostępnione na wolnej licencji zapewniającej licencjobiorcy prawo do dowolnego wykorzystywania utworów do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworów w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych.
- 6.11. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:
 1. Architektura produktu
 2. Poruszanie się po interfejsie użytkownika
 3. Planowanie wdrożenia systemu wraz z architekturą systemu
 4. Instalacja konsoli zarządzania i agentów na stacjach końcowych
 5. Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.
 6. Wykonanie przykładowych scenariuszy:
 - 6.1 Zdefiniowanie reguł pozwalających na wykrywanie określonych plików po dodanej sygnaturze oraz skonfigurowanie reagowania systemu na wykrycia.
 - 6.2 Zdefiniowanie reguł pozwalającej na wykrycie określonego procesu w monitorowanej infrastrukturze oraz skonfigurowanie reagowania systemu na wykrycia.
 - 6.3 Zdefiniowanie reguł pozwalających na wykrywanie masowych zmian na plikach, modyfikacje na plikach w zadanym czasie oraz skonfigurowanie reagowania systemu na wykrycia.
 7. Automatyzacja zadań w tym definiowanie zautomatyzowanych odpowiedzi na incydenty.
 8. Manualne uruchamianie zadań
 9. Analiza i raportowanie wyników
 10. Konfiguracja zadań/reakcji na złośliwe zdarzenia
 11. Zarządzanie użytkownikami i rolami
 12. Zaawansowana skala ryzyka dla wykrytych zagrożeń oraz formy jej odniesienia do innych stosowanych popularnych systemów oceny.