UNIWERSYTET ROLNICZY
im. Hugona Kołłątaja w Krakowie

Kraków, dnia 04.06.2024 r.

Do

Uczestników postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym pn. **Dostawa i wdrożenie oprogramowania klasy XDR dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie**, nr zamówienia **DZiK-DZP.2921.41.2024**.

Zamawiający – Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, działając na podstawie art. 284 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2023 r., poz. 1605 ze zm.) zwanej dalej ustawą Pzp, przekazuje poniżej treść pytań wraz z wyjaśnieniami.

Pytanie nr 1

W związku brzmieniem punktu WO16, wnosimy, aby Zamawiający zgodził się dostarczyć tego samego typu założenia dla ewaluacji MITRE z 2022 i 2021 roku? Ew. czy zamawiający zgadza się na wykreślenie tego punktu?

Odpowiedź:

Punkt WO16 dopuszcza rozwiązanie podlegające walidacji w roku 2022 i 2021. Celem wprowadzenia zapisu był wybór rozwiązania, które poddaje się regularnej walidacji w MITRE. Punkt WO17 wymaga walidacji w roku 2023. Zamawiający zakłada, że producenci wszystkich rozwiązań walidowanych w latach 2021, 2022 podjęli wysiłek, aby rozwiązać wykryte wtedy uchybienia. Zamawiającemu zależy na wyborze bezpiecznego rozwiązania w oparciu o walidację z 2023r, w związku z tym nie wyraża zgody na wykreślenie punktu WO16 ani zmian w punkcie WO17.

Pytanie nr 2

WO70 – Wnosimy, aby Zamawiający dopuścił możliwość ręcznego odfiltrowania i usunięcia Komputerów

Odpowiedź:

Zamawiający dopuszcza możliwość ręcznego odfiltrowania i usunięcia stacji końcowych nienawiązujących komunikacji z konsolą centralnego zarządzania przez określony czas. Automatyczne lub ręczne usunięcie stacji końcowych z konsoli muś wiązać się ze zwolnieniem przypisanych im licencji.

Pytanie nr 3

WS4 – Wnosimy, aby Zamawiający dopuścił rozwiązanie, które nie zapewnia ochrony UEFI.

Odpowiedź:

Zamawiający wymaga ochrony UEFI i nie dopuszcza rozwiązania niespełniającego tego warunku.

Pytanie nr 4

WS6 - Wnosimy, aby Zamawiający wykreślił zapis „dodanie procesu odpowiedzialnego za szyfrowanie do listy procesów, których nie będzie można ponownie uruchomić na innych stacjach końcowych”

Odpowiedź:

Intencją zamawiającego jest, aby nabyte oprogramowanie, które rozpoznało zagrożenie na późniejszym etapie detekcji, posiadało mechanizm uczenia się i rozpoznawania pojawiającego się ponownie zagrożenia już na pierwszym etapie detekcji. Zamawiający nie zgadza się na wykreślenie tego punktu, ale dopuszcza w ramach tego punktu, rozwiązanie działające inaczej, ale realizujące intencje zamawiającego.

Pytanie nr 5

WS12 i WS13 – Czy zamawiający dopuszcza rozwiązanie, które chroni przed technikami DEP, IAT/EAT oraz ROP?

Odpowiedź:

Zamawiający podtrzymuje zapisy określone w punkcie WS12 i WS13.

Pytanie nr 6

WS16 / WS18 – Wnosimy, aby Zamawiający dopuścił rozwiązanie, które posiada możliwość zdalnego wykonywania skryptów w zamian tych wymagań.

Odpowiedź:

Zamawiający dopuści rozwiązanie, które posiada możliwość zdalnego wykonywania skryptów w zamian za wymagania wskazane w WS16 i wymagania „nawiązywanie interaktywnego połączenia do linii poleceń stacji końcowej” z punktu WS18, tylko wtedy, kiedy rozwiązanie zapewni przechowywanie logów z wykonywanych skryptów oraz zapewni informację zwrotną wskazującą na którym poleceniu przerwano wykonywanie skryptu oraz z jakim błędem, co ułatwi debugowanie skryptu.

Pytanie nr 7

WS22 – Wnosimy, aby Zamawiający dopuścił rozwiązanie, które daje możliwość szyfrowania plików przesyłanych do pamięci przenośnych, w zamian możliwość blokady zapisywania plików na zewnętrznych dyskach USB, urządzenia takie są wówczas dostępne w trybie tylko do odczytu.

Odpowiedź:

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Pytanie nr 8

WS32 – Czy zamawiający dopuszcza rozwiązanie, które zbiera informacje jedynie z Azure Entra ID?

Odpowiedź:

Zamawiający nie dopuszcza rozwiązanie, które zbiera informacje jedynie z Azure Entra ID.

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Pytanie nr 9

WO17 – Czy zamawiający może dostarczyć tego samego typu założenia dla ewaluacji MITRE z 2022 i 2021 roku? Jeśli nie, to czy jest możliwość wykreślenia tego punktu?

Odpowiedź:

Punkt WO16 dopuszcza rozwiązanie podlegające walidacji w roku 2022 i 2021. Celem wprowadzenia zapisu był wybór rozwiązania, które poddaje się regularnej walidacji w MITRE. Punkt WO17 wymaga walidacji w roku 2023. Zamawiający zakłada, że producenci wszystkich rozwiązań walidowanych w latach 2021, 2022 podjęli wysiłek aby rozwiązać wykryte wtedy uchybienia. Zamawiającemu zależy na wyborze bezpiecznego rozwiązania w oparciu o walidację z 2023 r., w związku z tym nie wyraża zgody na wykreślenie punktu WO16, ani zmian w punkcie WO17.

Pytanie nr 10

WO70 – Czy zamawiający dopuściłby możliwość ręcznego odfiltrowywania i usunięcia komputerów?

Odpowiedź:

Zamawiający dopuszcza możliwość ręcznego odfiltrowania i usunięcia stacji końcowych nienawiązujących komunikacji z konsolą centralnego zarządzania przez określony czas. Automatyczne lub ręczne usunięcie stacji końcowych z konsoli musi wiązać się ze zwolnieniem przypisanych im licencji.

Pytanie nr 11

WS4 – Czy istnieje możliwość zaakceptowania rozwiązania, które nie zapewnia ochrony UEFI przez zamawiającego?

Odpowiedź:

Zamawiający wymaga ochrony UEFI i nie dopuszcza rozwiązania nie spełniającego tego warunku.

Pytanie nr 12

WS6 – Czy zamawiający zgodzi się na wykreślenie zapisu dotyczącego dodania procesu odpowiedzialnego za szyfrowanie do listy procesów, których nie będzie można ponownie

uruchomić na innych stacjach końcowych?

Odpowiedź:

Intencją zamawiającego jest, aby nabyte oprogramowanie, które rozpoznało zagrożenie na późniejszym etapie detekcji, posiadało mechanizm uczenia się i rozpoznawania pojawiającego się ponownie zagrożenia już na pierwszym etapie detekcji. Zamawiający nie zgadza się na wykreślenie tego punktu, ale dopuszcza w ramach tego punktu, rozwiązanie działające inaczej, ale realizujące intencje zamawiającego.

Pytanie nr 13

WS12 i WS13 – Czy zamawiający zaakceptuje rozwiązanie, które chroni przed technikami DEP, IAT/EAT oraz ROP?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 14

WS16/WS18 – Czy istnieje możliwość zaakceptowania przez zamawiającego rozwiązania umożliwiającego zdalne wykonywanie skryptów?

Odpowiedź:

Zamawiający dopuści rozwiązanie, które posiada możliwość zdalnego wykonywania skryptów w zamian za wymagania wskazane w WS16 i wymagania „nawiązywanie interaktywnego połączenia do linii poleceń stacji końcowej” z punktu WS18, tylko wtedy, kiedy rozwiązanie zapewni przechowywanie logów z wykonywanych skryptów oraz zapewni informację zwrotną wskazującą na którym poleceniu przerwano wykonywanie skryptu oraz z jakim błędem, co ułatwi debugowanie skryptu.

Pytanie nr 15

WS22 – Czy zamawiający rozważy wykreślenie tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Pytanie nr 16

WS32 – Czy zamawiający zaakceptuje rozwiązanie, które zbiera informacje jedynie z Azure Entra ID?

Odpowiedź:

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Zamawiający nie akceptuje rozwiązania niespełniającego opisy przedmiotu zamówienia.

Pytanie nr 17

WW1 – Czy zamawiający zaakceptuje, aby przynajmniej jedna osoba przydzielona do wdrożenia posiadała minimum roczne doświadczenie?

Odpowiedź:

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Pytanie nr 18

SC2 – Czy zamawiający zaakceptuje, aby szkolenie obejmowało jedynie kluczowe komponenty dostarczonego oprogramowania?

Odpowiedź:

Certyfikowane szkolenia muszą omawiać wszystkie komponenty dostarczonego oprogramowania.

Pytanie nr 19

SC3 – Czy zamawiający zgodzi się na materiały szkoleniowe (tj. slajdy i podręcznik) w języku angielskim?

Odpowiedź:

Zamawiający dopuszcza materiały szkoleniowe (tj. slajdy i podręcznik) w języku angielskim. Osoba prowadząca szkolenie musi biegle posługiwać się i prowadzić szkolenie w języku polskim.

Pytanie nr 20

SC5 – Czy zamawiający zaakceptuje 2-dniowe certyfikowane szkolenie?

Odpowiedź:

Certyfikowane szkolenia muszą omawiać wszystkie komponenty dostarczonego oprogramowania. Zamawiający uważa, że nie ma możliwości nauczenie posługiwania się tak złożonym oprogramowaniem w pełnej jego funkcjonalności w czasie krótszym niż wskazany w OPZ.

Pytanie nr 21

W046 - Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwoli na wyszukiwanie zdarzeń napływających do konsoli w oparciu o wiele artefaktów, w tym przynajmniej: adres IP, Adres MAC, argumenty wiersza poleceń, sumy kontrolne SHA1 i SHA256, wydawca certyfikatu, pochodzenie pliku wykonywalnego, zdarzenie w systemie operacyjnym oraz informacje o pliku (opis, wewnętrzna nazwa, oryginalna nazwa, nazwa firmy tworzącej oprogramowanie, wersja pliku, wersja produktu)?

Odpowiedź:

Zamawiający dopuszcza rozwiązanie wyszukujące zdarzenia na podstawie wskazanych w pytaniu artefaktów, o ile rozwiązanie to pozwoli wskazać dokładną lokalizację uruchomionego pliku na dysku oraz adresy URL.

Pytanie nr 22

W048 - Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwoli na wyzwalanie predefiniowanych reguł na podstawie wykrytych zdarzeń w organizacji zamawiającego?

Odpowiedź:

Zamawiającemu zależy na możliwości przeszukania danych telemetrycznych zebranych ze stacji końcowych pod kątem artefaktów kryminalistycznych. Dotyczy to również zagrożeń, które nie zostało jeszcze wykryte u zamawiającego.

Pytanie nr 23

W055 - Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwoli na dodanie wygenerowanej detekcji do wyłączeń dla poszczególnych stacji lub dla całej sieci?

Odpowiedź:

Tak, Zamawiający dopuszcza tego typu rozwiązanie.

Pytanie nr 24

W060 - Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie chroniło systemy Windows 7 za pomocą starszej wersji produktu, a pozostałe za pomocą najnowszej wersji produktu?

Odpowiedź:

Tak, Zamawiający dopuszcza tego typu rozwiązanie.

Pytanie nr 25

WS16 - Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie dawało zdalny dostęp do funkcji Remote Shell dla użytkowników konsoli z historią do wykonywanych poleceń za pomocą mechanizmów powershella?

Odpowiedź:

Zamawiający dopuści rozwiązania, które pozwolą wykonywać polecenia / zarządzać stacjami końcowymi bezpośrednio z konsoli centralnego zarządzania. Rozwiązanie musi umożliwiać przechowywanie logów z wykonywanych polec eń/skryptów w konsoli centralnego zarządzania lub do przechowywania logów/historii poleceń z wykonywanych poleceń/skryptów wykorzystuje mechanizmy systemu operacyjnego.

Pytanie nr 26

WS32 - Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie dawało możliwość przetwarzania i przechowywania danych telemetrycznych z serwerów, stacji końcowych, a także informacje o zdarzeniach systemowych z kontrolerów domeny za pomocą zainstalowanego agenta i connectora na kontrolerze domeny? Zdarzenia mogą też być zbierane poprzez funkcjonalność generującą log z danego punktu w czasie i odnoszącego się do ostatnich 30 dni.

Odpowiedź:

Zamawiający dopuszcza rozwiązanie, które wymaga instalacji agentów oferowanego oprogramowania na stacjach końcowych w tym kontrolerach domeny (Active Directory), które zbiera dane telemetryczne i zdarzenia systemowe/logi (ang. events).
Jednocześnie oferowane rozwiązanie musi zbierać zdarzenia systemowe/logi (ang. events) z Active Directory i Azure Active Directory lub ochrania aplikacje Microsoft Office 365 i Google Workspace.

Pytanie nr 27

Pytania dotyczące Opisu przedmiotu zamówienia (OPZ) – Załącznik nr 1 do SWZ
Dotyczy PPU §2 ust. 1
Z uwagi na fakt, iż przedmiotem umowy nie jest dostawa i wdrożenie oprogramowania, ale sprzedaż i dostarczenie licencji oraz wdrożenie licencjonowanego oprogramowania, uprzejmie proszę o modyfikację zgodnie z poniższą propozycją zapisu:
"Przedmiotem niniejszej umowy jest sprzedaż i dostarczenie licencji na oprogramowania klasy XDR (Extended Endpoint Detection and Respose) dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie, zwanego dalej oprogramowaniem, a także wdrożenie tego oprogramowania, zgodnie z niniejszą umową, złożoną ofertą na warunkach określonych w Specyfikacji Warunków Zamówienia. W zakresie licencji obowiązują warunki licencyjne producenta stanowiące załącznik do oferty Wykonawcy.”

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia oraz załącznikach do SWZ.

Pytanie nr 28

Dotyczy PPU §2 ust. 3
Uprzejmie proszę o podanie lokalizacji, gdzie ma nastąpić wdrożenie?

Odpowiedź:

Wdrożenie ma nastąpić w siedzibie Zamawiającego na terenie Miasta Kraków. (Zamawiający nie chce podawać dokładanej lokalizacji obawiając się o bezpieczeństwo).
WW3 - Zamawiający dopuszcza wdrożenie i konfigurację oferowanego systemu w formie zdalnej.

Pytanie nr 29

Dotyczy PPU §2 ust. 3
Kiedy nastąpi podpisanie protokołu końcowego? Bowiem zapisy umowy przewidują także 36-miesięczną gwarancje i asystę techniczną, więc wykonanie całości nastąpi de facto po zakończeniu tego okresu.

Odpowiedź:

Podpisanie protokołu odbioru końcowego nastąpi po zakończeniu ETAPU III.

Pytanie nr 30

Dotyczy PPU §2 ust. 5

Wykonawca powinien odpowiadać wyłącznie za okoliczności, na które ma wypływ. W związku z tym proszę o zmodyfikowanie zapisu w punkcie 5 str. 4 zgodnie z poniższą propozycją:

"Wykonawca gwarantuje, iż licencja udzielona na oprogramowanie będące przedmiotem umowy, nie będzie wypowiedziana z przyczyn niezawinionych przez Zamawiającego. W przypadku wypowiedzenia licencji, wbrew zobowiązaniu o którym mowa powyżej, bez winy Zamawiającego, Wykonawca zobowiązuje się do zapłaty na rzecz Zamawiającego 100% kwoty brutto należnej Wykonawcy, o której mowa w § 3 ust. 1 umowy."

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Projektowanych postanowieniach umowy – Załącznik nr 4 do SWZ.

Pytanie nr 31

Dotyczy PPU §2 ust. 6

W związku z tym, iż Wykonawca nie udziela licencji a jedynie je sprzedaje, uprzejmie proszę o zmianę w zapisie w punkcie 6 str. 4:

„Wykonawca oświadcza, iż przysługują mu odpowiednie prawa w zakresie umożliwiającym wykonanie umowy oraz że jest uprawniony do sprzedaży Zamawiającemu licencji do korzystania z oprogramowania na zasadach określonych w umowie."

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Projektowanych postanowieniach umowy – Załącznik nr 4 do SWZ.

Pytanie nr 32

Dotyczy PPU §2 ust. 10

Przedmiotem umowy nie jest sprzedaż oprogramowania, a sprzedaż licencji. Stosunek licencyjny zostanie nawiązany między Zamawiającym a producentem, a Wykonawca nie jest stroną stosunku licencyjnego. Zatem, proszę o wyjaśnienie, na jakiej podstawie Wykonawca ma udzielać gwarancji na to oprogramowanie?

Odpowiedź:

Zamawiający podtrzymuje zapis, że przedmiotem umowy jest dostawa oprogramowania, ale rozumiejąc obawy potencjalnych wykonawców wykreśla punkt dotyczący gwarancji, ograniczając się jedynie do gwarancji producenta dostarczonego oprogramowania.

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że z §2 usuwa ust. 10, 11, 12, 13, 14,15, 16, 17, 18.

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że w §2 dodaje ust. 10, który otrzymuje brzmienie „Wykonawca dostarczy wraz z dokumentacją powykonawczą dokument gwarancyjny wystawiony przez producenta zaoferowanego oprogramowania, jeśli producent wystawia taki dokument".

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść Specyfikacji Warunków Zamówienia w ten sposób, że wykreśla następujące zapisy:

„Wykonawca udzieli Zamawiającemu gwarancji na oprogramowanie, której okres wynosi 36 miesięcy.

Termin gwarancji, będzie liczony od daty podpisania protokołu odbioru Etapu II.

Wykonawca w ramach bezpłatnej udzielonej gwarancji świadczyć usługi, które będą obejmować:

1) zapewnienie świadczenia obsługi zgłoszeń serwisowych we wszystkie dni tygodnia w formie elektronicznej - poprzez internetowy serwis asysty technicznej lub dedykowaną skrzynkę mailową,

2) elektroniczny dostęp do informacji na temat posiadanego oprogramowania,

3) publikowanie i udostepnianie aktualizacji dokumentacji do oprogramowania w postaci elektronicznej przez internetowy serwis, takich jak np.: techniczna dokumentacja, internetowa baza wiedzy lub forum internetowe producenta oprogramowania,

4) wsparcie zespołu certyfikowanych inżynierów,

5) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,

6) doradztwo w zakresie konfiguracji,

7) pomoc w zakładaniu zgłoszeń serwisowych u producenta.

Usługi wskazane świadczone będą w języku polskim w godzinach pracy Zamawiającego tj. pn-pt 8:00-16:00.

Asysta techniczna w szczególności powinna obejmować pomoc w rozwiązywaniu problemów związanych z bieżącym administrowaniem, konfiguracją i utrzymaniem systemu."

Pytanie nr 33

Dotyczy PPU §2 ust. 14

Co to znaczy asysta techniczna i czy jest przedmiotem umowy?

Odpowiedź:

Zamawiający wykreśla punkt dotyczący asysty technicznej.

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że z §2 usuwa ust. 10, 11, 12, 13, 14,15, 16, 17, 18.

Pytanie nr 34

Dotyczy PPU §2 ust. 15

Przedmiotem umowy nie jest sprzedaż oprogramowania, a sprzedaż licencji. Producent może wystawić certyfikat potwierdzający wykupienie licencji wraz ze wsparciem producenta - o ile będzie to stanowić przedmiot umowy.

Odpowiedź:

Zamawiający zmodyfikował treść SWZ oraz Załącznika nr 4 do SWZ w zakresie usług gwarancyjnych.

Pytanie nr 35

Dotyczy PPU §3

Przedmiotem umowy nie jest sprzedaż oprogramowania, ale sprzedaż praw tj. licencji, więc proszę o wskazanie na co ma być udzielona rękojmia?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 36

Dotyczy PPU §3 ust. 2

W przypadku wyboru oferty Wykonawcy jako najkorzystniejszej, uprzejmie proszę o dodanie oświadczenia Wykonawcy o statusie dużego przedsiębiorcy:

"Wykonawca oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych."

Odpowiedź:

Zamawiający wyraża zgodę na dodanie zapisu "Wykonawca oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych."

Pytanie nr 37

Dotyczy PPU §4 ust. 1

Uprzejmie proszę o sprecyzowanie, kiedy nastąpi podpisanie Protokół odbioru końcowego, o którym mowa w §2 ust. 3 ETAP III lit. do niniejszej umowy.

Odpowiedź:

Podpisanie protokołu odbioru końcowego nastąpi po zakończeniu ETAPU III.

Pytanie nr 38

Dotyczy PPU §11

Jakie osoby/podmioty będą uznawane za podwykonawców? Czy osoby fizyczne prowadzące jedenastoosobową działalność gospodarczą i stale współpracujące z Wykonawcą w modelu umów

B2B - co jest standardem na rynku, będą uznane jako zasoby Wykonawcy, a tym samym zamówienie Wykonawca zrealizuje „własnymi siłami", bez udziału podwykonawców?

Odpowiedź:

Za podwykonawcę będzie uznany podmiot, który zawrze umowę z wykonawcą, zgodną z definicją zawartą w PZP.

Pytanie nr 39

Ile stacji roboczych Zamawiającego pracujących pod kontrolą systemu Windows 7 będzie podlegało ochronie na dzień podpisania umowy?

Odpowiedź:

Zamawiający nie poda liczby urządzeń z systemem Windows 7. W opinii Zamawiającego liczba stacji roboczych z system Windows 7 nie jest istotna. Wykonawca ma dostarczyć licencję na co najmniej 2770 stacji roboczych (WO1) i wspierać ochronę stacji końcowych z systemami operacyjnymi określonymi w WO60.

Przez okres 3 lat stacje robocze z systemem Windows 7 będą systematycznie aktualizowane do nowszego systemu operacyjnego lub wymieniane na nowe stacje robocze w związku z czym liczba stacji końcowych z systemem Windows 7 będzie bardzo szybko maleć.

WO2 - Udzielone licencje zezwalać będą na swobodne przenoszenie oprogramowania pomiędzy tego samego typu stacjami końcowymi (pomiędzy stacjami roboczymi, pomiędzy serwerami oraz pomiędzy urządzeniami mobilnymi).

Pytanie nr 40

Czy Zamawiający dopuszcza rozwiązanie przechowujące informacje o alarmach przez okres minimum 90 dni?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 41

Czy Zamawiający dopuszcza rozwiązanie przechowujące informacje o incydentach przez okres minimum 90 dni?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 42

Czy Zamawiający dopuszcza rozwiązanie, które w przypadku przechowywania informacji o alarmach przez okres co najmniej 180 dni będzie pozwalało na zrealizowanie tego wymagania z wykorzystaniem eksportu danych za pośrednictwem API oferowanego rozwiązania?

Odpowiedź:

Tak o ile rozwiązanie takie zapewni możliwość przeszukiwania i filtrowania alarmów i incydentów w konsoli centralnego zarządzania, przy czym dane z ostatnich 90 dni muszą być dostępne w czasie rzeczywistym, z pominięciem API bezpośrednio w konsoli. Pozostałe co najmniej 90 dni z wykorzystaniem eksportu danych za pośrednictwem API oferowanego rozwiązania.
Oferowane rozwiązanie musi posiadać zautomatyzowany mechanizm eksportu danych. Połączenie z API zostanie zrealizowane przez Wykonawcę na swój koszt i ryzyko i nie będzie wiązało się z wniesieniem przez Zamawiającego żadnych dodatkowych opłat przez okres obowiązywania umowy na dostarczone oprogramowanie klasy XDR. Eksport danych nie może wiązać się z koniecznością posiadania przez Zamawiającego jakiejkolwiek dodatkowej infrastruktury i oprogramowania oprócz dodatkowego miejsca na własnym dysku sieciowym.
W przypadku ręcznego importowania pliku do konsoli w celu przeglądnięcia mechanizm musi zapewniać dostęp do danych z 90 dni po zaimportowaniu pojedynczego pliku. Zamawiający nie dopuszcza ręcznego importowania np. 90 plików w celu przeszukiwania alarmów i incydentów.

Pytanie nr 43

Czy Zamawiający dopuszcza rozwiązanie, które w przypadku przechowywania informacji o incydentach przez okres co najmniej 180 dni będzie pozwalało na zrealizowanie tego wymagania z wykorzystaniem eksportu danych za pośrednictwem API oferowanego rozwiązania?

Odpowiedź:

Tak o ile rozwiązanie takie zapewni możliwość przeszukiwania i filtrowania alarmów i incydentów w konsoli centralnego zarządzania, przy czym dane z ostatnich 90 dni muszą być dostępne w czasie rzeczywistym, z pominięciem API bezpośrednio w konsoli. Pozostałe co najmniej 90 dni z wykorzystaniem eksportu danych za pośrednictwem API oferowanego rozwiązania.
Oferowane rozwiązanie musi posiadać zautomatyzowany mechanizm eksportu danych. Połączenie z API zostanie zrealizowane przez Wykonawcę na swój koszt i ryzyko i nie będzie wiązało się z wniesieniem przez Zamawiającego żadnych dodatkowych opłat przez okres obowiązywania umowy na dostarczone oprogramowanie klasy XDR. Eksport danych nie może wiązać się z koniecznością posiadania przez Zamawiającego jakiejkolwiek dodatkowej infrastruktury i oprogramowania oprócz dodatkowego miejsca na własnym dysku sieciowym.
W przypadku ręcznego importowania pliku do konsoli w celu przeglądnięcia mechanizm musi zapewniać dostęp do danych z 90 dni po zaimportowaniu pojedynczego pliku. Zamawiający nie dopuszcza ręcznego importowania np. 90 plików w celu przeszukiwania alarmów i incydentów.

Pytanie nr 44

Czy Zamawiający dopuszcza przeprowadzenie warsztatów, które w zakresie poruszanych zagadnień będą tożsame z zakresem zagadnień poruszanych na certyfikowanych szkoleniach producenta?

Odpowiedź:

Warsztaty i szkolenia certyfikowane nie muszą się pokrywać, ale warsztaty i szkolenia certyfikowane muszą omawiać wszystkie komponenty dostarczonego oprogramowania.
Warsztaty i szkolenia certyfikowane nie są tożsame chociaż musza zawierać te same elementy, Zamawiający dopuszcza, że nacisk kładziony na poszczególne tematy w przypadku warsztatów i szkoleń certyfikowanych jest różny ze względu na różny czas warsztatów i certyfikowanych szkoleń.

Pytanie nr 45

Czy Zamawiający dopuszcza w przypadku warsztatów materiały szkoleniowe w języku angielskim?

Odpowiedź:

Zamawiający dopuszcza materiały szkoleniowe (tj. slajdy i podręcznik) w języku angielskim.
Osoba prowadząca szkolenie musi biegle posługiwać się i prowadzić szkolenie w języku polskim.

Pytanie nr 46

Czy Zamawiający w przypadku Warsztatów w języku polskim, które będą dodatkowo nagrywane i udostępniane w formie nagrania, dopuszcza dostarczenie materiałów szkoleniowych w języku angielskim z racji tego, że rozwiązanie i jego moduły mogą być dostępne w języku angielskim, a odpowiedni komentarz i prezentacja prowadzona przez polskojęzycznego lektora będą się jednoznacznie odnosiły do odpowiednich materiałów szkoleniowych w języku angielskim?

Odpowiedź:

Warsztaty ma prowadzić żywa osoba zgodnie z SW10 która jest merytoryczna, posiada pełną wiedzę techniczną dotyczącą oferowanego produktu i będzie można jej zadawać pytania odnośnie oferowanego produktu i jego funkcjonalności. Zamawiający dopuszcza środowisko informatyczne o którym mowa w SW9 w języku angielskim.
Zamawiający nie dopuszcza warsztatów opartych na nagraniu materiału z lektorem polskim lub prowadzonego/tłumaczonego przez sztuczną inteligencję.

Pytanie nr 47

Jak należy rozumieć zapis "Obsługę zgłoszeń serwisowych we wszystkie dni tygodnia [...]" w kontekście zapisu "Usługi wskazane świadczone będą [...] w godzinach pracy Zamawiającego tj. pn-pt 8:00-16:00"?
Czy Zamawiający dopuszcza sytuację, że Usługi o których mowa będą świadczone wyłącznie w dni pracy Zamawiającego (pn-pt) jednak z pominięciem dni pracy ustawowo wolnych, które mogą w tych dniach tygodnia wypadać? Czy Zamawiający dopuszcza obsługę zgłoszeń serwisowych w dni

wolne od pracy Zamawiającego i w godzinach wykraczających poza godziny pracy Zamawiającego wyłącznie poprzez umożliwienie ich zgłoszenia np. poprzez wysłanie na wskazany adres email, a następnie ich obsługę w dni pracy i w godzinach pracy Zamawiającego (poza dniami ustawowo wolnymi od pracy)?

Odpowiedź:

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że z §2 usuwa ust. 10, 11, 12, 13, 14,15, 16, 17, 18.

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że w §2 dodaje ust. 10, który otrzymuje brzmienie „Wykonawca dostarczy wraz z dokumentacją powykonawczą dokument gwarancyjny wystawiony przez producenta zaoferowanego oprogramowania, jeśli producent wystawia taki dokument".

Pytanie nr 48

Czy Zamawiający będzie wymagał gwarancji na oprogramowanie od Wykonawcy w sytuacji, w której Wykonawca jest tylko dostawcą oprogramowania, a nie jego producentem i nie ma on wpływu na warunki gwarancji udzielanych przez Producenta? Wykonawca może dostarczyć odpowiednie kody aktywacyjne/klucze licencyjne/certyfikaty potwierdzające nabycie licencji do oprogramowania przez Zamawiającego, natomiast warunki użytkowania oprogramowania oraz zakres gwarancyjny może być określony przez Producenta w zapisach Umowy Licencyjnej Użytkownika Końcowego (EULA) zawieranej pomiędzy Zamawiającym i Producentem podczas jej akceptacji przez Zamawiającego - czy Zamawiający wobec tego zmieni odpowiednie zapisy i wymogi SIWZ?

Odpowiedź:

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że z §2 usuwa ust. 10, 11, 12, 13, 14,15, 16, 17, 18.

Zamawiający na podstawie art. 286 ust 1 ustawy Pzp zmienia treść załącznika nr 4 do SWZ w ten sposób, że w §2 dodaje ust. 10, który otrzymuje brzmienie „Wykonawca dostarczy wraz z dokumentacją powykonawczą dokument gwarancyjny wystawiony przez producenta zaoferowanego oprogramowania, jeśli producent wystawia taki dokument".

Pytanie nr 49

Dotyczy WO1

W OPZ brakuje opisu wymagań funkcjonalności dla ochrony urządzeń mobilnych. Zestaw funkcjonalności ochrony dla systemów operacyjnych typu Windows/Linux jest inny niż dla IOS/Android. Producenci oferują ochronę urządzeń mobilnych z wykorzystaniem osobnych konsol

zarządzania, aby zespół odpowiedzialny za zarządzanie urządzeniami mobilnymi nie miał dostępu do całego systemu cyberbezpieczeństwa firmy. W związku z powyższym prosimy o modyfikację zapisów tak, aby wymagane było zapewnienie przez producenta oferowanego systemu możliwości rozbudowy w przyszłości o ochronę urządzeń mobilnych i rezygnację z wymogu dostarczenia 30 licencji do ochrony urządzeń mobilnych w obecnym postępowaniu.

Odpowiedź:

Zamawiający zdaje sobie sprawę, że zestaw funkcjonalności różni się dla systemów operacyjnych typu Windows/MacOS/Linux/iOS/Android.

Zamawiający w OPZ nie ogranicza liczby konsol centralnego zarzadzania dostarczonych przez Wykonawcę oraz dopuszcza rozwiązania oparte o jedną konsolę centralnego zarządzania która posiada możliwość nadania odpowiednich uprawnień dla członków zespołu oraz do jakich grup urządzeń mają uprawnienia do zarządzania.

Zamawiający nie zgadza się na zmianę zapisu, a w szczególności na proponowany zapis ‘’zapewnienie przez producenta oferowanego systemu możliwości rozbudowy w przyszłości o ochronę urządzeń mobilnych i rezygnację z wymogu dostarczenia 30 licencji do ochrony urządzeń mobilnych w obecnym postępowaniu”.

Oferowane oprogramowanie musi być dostarczone z licencją na co najmniej 30 urządzeń mobilnych, przy czym zamawiający dopuszcza możliwość zakupu większej liczby licencji w przyszłości.

Pytanie nr 50

Dotyczy wymagania WO14

Raz zainstalowany system EDR bardzo rzadko jest przeinstalowywany na inny system wirtualizacyjny. Uprzejmie prosimy o modyfikację zapisu w taki sposób by było możliwe zaoferowanie systemu EDR wspierającego instalację na platformie wirtualizacyjnej Vmware LUB Hyper-V.

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę zapisów punktu WO14, w szczególności, że nie ma pewności której platformy wirtualizacji będzie używał w trakcie całego okresu trwania umowy i czy będzie posiadał wsparcie i aktualizacje do obecnie posiadanej.

Pytanie nr 51

Dotyczy WS19

Obecnie dostępne systemy EDR oferują bardzo dużą skuteczność wykrywania i blokowania najbardziej wyrafinowanych i zaawansowanych cyber zagrożeń bez wykorzystywania

mechanizmów Sandbox. Skuteczność tych systemów jest potwierdzona wieloma niezależnymi technicznymi testami, w których te systemy osiągają lepsze wyniki wykrywania i blokowania niż systemy z wbudowanym modułem Sandbox. Prosimy o modyfikację SIWZ tak aby możliwe było zaoferowanie systemu zapewniającego integrację z Sandbox przez API.

Odpowiedź:

Zamawiający dopuści możliwość zaoferowania systemu zapewniającego integrację z Sandbox przez API, o ile integracja zostanie zrealizowane przez Wykonawcę na swój koszt i ryzyko i nie będzie wiązała się z wniesieniem przez Zamawiającego żadnych dodatkowych opłat przez okres obowiązywania umowy na dostarczone oprogramowanie klasy XDR.
Integracja za pomocą API musi być pełna, tzn. obejmować pełną funkcjonalność oferowanego Sandboxa.
Sandbox może być zainstalowany przez Wykonawcę na serwerach zamawiającego lub może być uruchomiony w chmurze znajdującej się na terenie Unii Europejskiej.
Raporty dostarczone z Sandboxa pozwolą Zamawiającemu na wyszukiwanie w konsoli centralnego zarządzania artefaktów które mogą być wspólne dla innych ataków (np. adresy IP wykorzystywane do hostowania złośliwego oprogramowania).
Z uwagi na potencjalną konieczność integracji dostarczonego rozwiązania z zewnętrznym Sandboxem, na potrzeby integracji Sandboxa z rozwiązaniem XDR, zamawiający dopuszcza wyjątek od zapisu WO8 – Sandbox może być rozwiązaniem innego producenta niż dostarczone oprogramowanie XDR.
Wykonawca zobowiązany jest zaoferować urządzenia informatyczne lub oprogramowanie nie wskazane w rekomendacji, o której mowa w art. 33 ustawy o krajowym systemie cyberbezpieczeństwa.

Pytanie nr 52

Dotyczy WS24
Obecnie dostępne systemy EDR w sposób bardzo wyraźny odróżniają się od systemów do zarządzania stacjami roboczymi. Dlatego też producenci tych systemów nie duplikują niepotrzebnych funkcjonalności i koncentrują się na innych zadaniach. Prosimy o zmianę zapisu w SIWZ aby oferowane rozwiązanie umożliwiało jedynie powiadomienie o stanie użycia natywnych mechanizmów szyfrowania OS. Uruchomienie szyfrowania bp Bitlocker jest co do zasady domeną systemów do zarządzania stacją a nie rozwiązań klasy EDX/XDR.

Odpowiedź:

Zamawiający dopuszcza, że dostarczone rozwiązanie posiada funkcjonalność pełnego szyfrowania

dysku co najmniej stacji roboczych i serwerów z systemami Microsoft Windows lub możliwość sprawdzenia stanu natywnych mechanizmów szyfrowania wbudowanego w systemy Microsoft Windows i MacOS.

Pytanie nr 53

Dotyczy WS4

Obecnie dostępne systemy EDR realizują te same cele za pomocą różnych ścieżek, narzędzi lub funkcjonalności. Prosimy o modyfikację SIWZ, aby oferowane rozwiązanie realizowało bezpieczny rozruch systemu za pomocą innych technik kontroli, np. przez ochronę Master Boot Record (MBR).

Odpowiedź:

MBR i UEFI to różne tryby rozruchu, które są ze sobą niezgodne. MBR jest powiązany ze starszym trybem rozruchu i jest potrzebny w trybie Legacy/BIOS. Zamawiający posiada wymagania donośnie trybu MBR w wymaganiu WS6.

Zamawiający wymaga ochrony UEFI i nie dopuszcza rozwiązania niespełniającego tego warunku.

Pytanie nr 54

Zgodnie z zapisem w umowie §2. Pkt 5

Wykonawca gwarantuje, iż licencja udzielona na oprogramowanie będące przedmiotem umowy, nie będzie wypowiedziana z przyczyn niezawinionych przez Zamawiającego. W przypadku wypowiedzenia licencji, wbrew zobowiązaniu, o którym mowa powyżej, bez winy Zamawiającego, niezależnie od przyczyn takiego zdarzenia, włączając w to przyczyny, za które Wykonawca nie ponosi odpowiedzialności, Wykonawca zobowiązuje się do zapłaty na rzecz Zamawiającego 100% kwoty brutto należnej Wykonawcy, o której mowa w § 3 ust. 1 umowy - Wykonawca wnosi o wykreślenie odpowiedzialności za wypowiedzenie licencji Zamawiającemu z przyczyn za które Wykonawca nie ponosi odpowiedzialności.

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Zamawiający nie wyraża zgody na zmianę zapisu.

Pytanie nr 55

Pytanie dot. Specyfikacja Warunków Zamówienia punkt WS7

Czy wykorzystanie mechanizmów bezpośrednio realizowanych w oferowanym oprogramowaniu w postaci wykrywania podejrzanych i złośliwych zachowań oraz artefaktów Zamawiający uzna za wystarczające i usunie podane wymaganie?

Zauważamy, że mechanizm AMSI działający wyłącznie na platformie Windows 10 i wyższych, oparty jest na działaniu sygnaturowym, który stosunkowo prosto może zostać wyłączony lub ominięty np.

poprzez obfuskację kodu. Rozwiązania klasy XDR skupiają się nie na sygnaturch konkretnych komend a na zachowaniu, wykonywanych operacjach i samym działaniu skryptu, w związku z czym dokładniej realizują zadania ochronne.

Nadmieniamy, że proponowane oprogramowanie nie wyklucza wykorzystania działania funkcjonalności AMSI i pozwala wykorzystać ją wraz z dostępnym na platformie Windows oprogramowaniem Windows Defender działając równocześnie.

Odpowiedź:

Zamawiający dopuści rozwiązanie, które posiada mechanizmy wykrywania podejrzanych i złośliwych zachowań oraz artefaktów, a które nie wspiera technologii Antimalware Scan Interface (AMSI) o której mowa w WS7. Warunkiem dopuszczenia takiego rozwiązania jest że oferowane oprogramowanie nie wyklucza wykorzystywania działania funkcjonalności AMSI i pozwala wykorzystywać ją wraz z oprogramowaniem Windows Defender działającym równocześnie z oferowanym oprogramowaniem.

Pytanie nr 56

Zwracamy się z prośbą o usunięcie poniższych zapisów z OPZ dotyczących wymagań szyfrowania dysków systemowych:

1. Wgląd w szczegóły zgłaszającego się hosta, w tym stanu zaszyfrowania dysków systemowych: "Konsola centralnego zarządzania musi umożliwiać wgląd w szczegóły zgłaszającego się hosta, w których zawarte są co najmniej informacje dotyczące: stanu zaszyfrowania dysków systemowych."
2. Wysyłanie zadań do agenta zainstalowanego na stacji końcowej dotyczących zaszyfrowania dysków systemowych: "Konsola centralnego zarządzania umożliwia wysyłanie minimum następujących zadań do agenta zainstalowanego na stacji końcowej: zaszyfrowania dysków systemowych."
3. Wymóg funkcjonalności pełnego szyfrowania dysku lub możliwości wykorzystania natywnego szyfrowania wbudowanego w systemy Microsoft Windows i MacOS: "Dostarczone rozwiązanie posiada funkcjonalność pełnego szyfrowania dysku lub możliwość wykorzystania natywnego szyfrowania wbudowanego w systemy Microsoft Windows i MacOS."

Wg naszej wiedzy oprogramowanie większości dostawców nie spełnia tych wymagań, ponieważ są one nieistotne z punktu widzenia zaawansowanych systemów wykrywania i reagowania na zagrożenia (XDR). Na rynku dostępne są systemy XDR, których producenci korzystają z natywnego szyfrowania dysków (np. BitLocker w Windows), co oznacza, że klient nie uzyskuje dodatkowych korzyści z tytułu spełnienia tych wymagań. Usunięcie w/w wymagań pozwoli na zaoferowanie większej ilości systemów XDR co przełoży się na zwiększenie konkurencyjności.

Odpowiedź:

Zamawiający dopuszcza, że dostarczone rozwiązanie posiada funkcjonalność pełnego szyfrowania dysku co najmniej stacji roboczych i serwerów z systemami Microsoft Windows lub możliwość sprawdzenia stanu natywnych mechanizmów szyfrowania wbudowanego w systemy Microsoft Windows i MacOS.

Zamawiający uzyskuje korzyści wiedząc czy stacja końcowa jest zaszyfrowana lub nie. Zamawiający nie musi kupować dodatkowe oprogramowania, w którym będzie sprawdzał które stacje końcowe są zaszyfrowane.

Pytanie nr 57

Czy Zamawiający dopuści zaoferowania rozwiązania wiodącego producenta, który nie prowadzi jednak certyfikowanych szkoleń?

Wykonawca zapewni w zamian autorskie szkolenie w wymaganym przez Zamawiającego zakresie, które przeprowadzone będzie przez specjalistę, będącego pracownikiem producenta, oferowanego rozwiązania. Uczestnictwo w szkoleniu potwierdzone zostanie wystawieniem certyfikatu.

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Zamawiający wymaga warsztatów prowadzonych przez Wykonawcę, jak i certyfikowanych szkoleń producenta.

Pytanie nr 58

Wnosimy o zmianę Kryterium oceny ofert poprzez modyfikację zapisu:

Jest:

„Kryterium 2 - Możliwość uruchomienia On-Premise lub chmura w Polsce (F)”

Powinno być:

Kryterium 2 - Możliwość uruchomienia On-Premise lub chmura w Polsce lub Unii Europejskiej (F)

Uzasadniając ww. wniosek wskazujemy, że dopuszczenie w ramach kryterium „chmury w Unii Europejskiej” zapewnia ten sam jakościowy poziom przedmiotu zamówienia co chmura w Polsce. Brak jest w związku z tym powodów dla wyróżniania i przyznawania dodatkowych punktów tylko rozwiązaniom umożliwiającym uruchomienie w chmurze w Polsce, podczas gdy dostępne są inne równorzędne jakościowo rozwiązania w Unii Europejskiej, chronione zunifikowanym ustawodawstwem i standardami w tym zakresie. Pozwoli to na uzyskanie punktacji w ramach tego kryterium szerszemu kręgowi rozwiązań na równym poziomie jakościowym, szczególnie mając na uwadze, że wskazane kryterium ograniczone do możliwości uruchomienia w chmurze tylko w Polsce niezasadnie promuje tylko jednego określonego producenta, który oferuje taką możliwość.

Dopuszczenie możliwości uzyskania punktów w ramach tego kryterium także dla uruchomienia w chmurze na obszarze UE jest również zgodne z wytyczną, zgodnie z którą dostawy i usługi pochodzące z Unii Europejskiej powinny być traktowane nie gorzej niż krajowe.

Odpowiedź:

Zamawiający wymaga, żeby oferowane oprogramowanie było hostowane na terenie Unii Europejskiej, jest to obligatoryjny wymóg wynikający z przepisów prawa.

Zamawiający promuje rozwiązania instalowane na serwerach Zamawiającego (On-Promise) lub rozwiązania hostowane w Polsce.

Celem takiego zapisu jest dążenie do spełnienia (zbliżenia się do) wymagań SCCO2 oraz w przypadku zaistnienia incydentów dotyczących cyberbezpieczeństwa zapewnienie jurysdykcji polskich sądów.

Pytanie nr 59

Dotyczy WO44

Producenci wiodących rozwiązań typu EDR/XDR korzystają z własnej bazy reputacyjnej w celu weryfikacji reputacji plików, dlatego prosimy o zmianę brzmienia wymagania:

Jest:

- zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal)

na:

- zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do bazy reputacji, pozwalającej sprawdzić reputację tych plików

Odpowiedź:

Zamawiający dopuszcza własną bazę reputacji oferowanego oprogramowania, jednak baza reputacji oferowanego oprogramowanie nie jest nieomylna. Możliwość dodatkowego sprawdzenia w ogólnodostępnej bazie reputacji pozwala sprawdzić jak inne rozwiązania oceniają badany plik. Zamawiający spotkał się z sytuacją, że rozwiązanie antywirusowe oceniło plik jako bezpieczny, ale inne rozwiązania antywirusowe oceniły plik jako szkodliwy.

Zamawiający dopuści zapis proponowany przez zadającego pytanie tylko wtedy, kiedy oferowane oprogramowanie będzie generował sumę kontrolną podejrzanych plików, tak aby zamawiający mógł samodzielnie na podstawie sumy kontrolnej sprawdzić plik w ogólnodostępnej bazie (np. Virus Total).

Pytanie nr 60

WO56

Dostarczone rozwiązanie posiada wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Istnieje możliwość utworzenia własnych reguł.

Pytanie: Czy Zamawiający dopuszcza możliwość tworzenia własnych reguł wykrywania i wykluczania oraz braku predefiniowanych reguł?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 61

WO58

Dostarczone rozwiązanie posiada możliwość eksportu logów audytowych poprzez Syslog po SSL/TLS w formacie CEF.

Pytanie: Czy Zamawiający dopuszcza format Syslog (JSON) oraz Splunk (http) zamiast formatu CEF?

Odpowiedź:

Zamawiający dopuszcza export logów audytowych w formacie Syslog (JSON) oraz Splunk (http) lub w formacie CEF.

Pytanie nr 62

WS4

Dostarczone rozwiązanie posiada funkcjonalność ochrony UEFI.

Pytanie: Czy Zamawiający dopuszcza brak funkcjonalności ochrony UEFI?

Odpowiedź:

Zamawiający wymaga ochrony UEFI i nie dopuszcza rozwiązania nie spełniającego tego warunku.

Pytanie nr 63

WS5

Dostarczone rozwiązanie posiada mechanizm wykrywania i przeciwdziałania nowym i nieznanym zagrożeniom, bazujący na:

• modelu uczenia maszynowego (ang. Machine Learning - ML)
• analizie behawioralnej, która wykrywa wzorce zachowań atakującego
• algorytmach wykrywania anomalii oraz profilowania komputera i jego użytkownika
• wykrywaniu anomalii w ruchu sieciowym
• technologii chmurowej
• technologii heurystycznej

Pytanie: Czy Zamawiający dopuszcza brak profilowania komputera i użytkownika, z jednoczesnym

rozszerzeniem w/w mechanizmów o analizę w oparciu o schematy MITRE?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Pytanie nr 64

WS6

Dostarczone rozwiązanie posiada następujące funkcjonalności w zakresie ochrony przed ransomware:

• wykrywanie ataków ransomware, w szczególności tych których celem jest uszkodzenie Master Boot Record (MBR) niezależnie od tego, czy zostały uruchomione lokalnie, czy ze zdalnego punktu końcowego

• w przypadku wykrycia ataku przerwanie próby szyfrowania plików na dysku oraz dodanie procesu odpowiedzialnego za szyfrowanie do listy procesów, których nie będzie można ponownie uruchomić na innych stacjach końcowych

Pytanie: Czy Zamawiający dopuszcza brak wykrywania ataków na MBR?

Odpowiedź:

Zamawiający wymaga ochrony MBR i nie dopuszcza rozwiązania nie spełniającego tego warunku.

Pytanie nr 65

WS18

Dostarczone rozwiązanie w ramach odpowiedzi na incydent umożliwia:

• reakcje (remediację) ze wskazaniem kroków, które mogą być podjęte automatycznie

• uruchomienie skryptu na stacji końcowej

Pytanie: Czy Zamawiający dopuszcza możliwość zastąpienia zdalnego wykonywania skryptów na końcówkach, możliwością połączenia zdalnego z poziomu incydentu w celu wykonania określonego skryptu lub operacji?

Odpowiedź:

Zamawiający dopuszcza możliwość zastąpienia zdalnego wykonywania skryptów na stacjach końcowych, możliwością połączenia zdalnego (Remote Shell) z poziomu incydentu bezpośrednio z konsoli centralnego zarządzania. Zestawiona sesja (Remote Shell) udostępni operatorowi linię poleceń systemu operacyjnego w której będzie można wykonać skrypt lub wydawać polecenia tekstowe. Rozwiązanie (Remote Shell) musi umożliwiać przechowywanie logów z wykonywanych poleceń/skryptów oraz zapewni informację zwrotną zawierającą ewentualne błędy w celu ułatwienia debugowania.

Pytanie nr 66

WS26

Telemetria ze stacji końcowych objętych ochroną jest przechowywana centralnie, aby móc korelować zdarzenia między różnymi stacjami.

Pytanie: Czy Zamawiający zamiast przechowywania telemetrii w konsoli zarządzającej dopuszcza przesyłanie wybranych przez administratora danych bezpośrednio do zintegrowanego systemu SIEM?

Odpowiedź:

Zamawiający dopuszcza że rozwiązania przechowujące całą telemetrię poza konsolą centralnego zarządzania.

Oferowane rozwiązanie musi zbierać telemetrię z stacji końcowych i innych źródeł (m.in. Active Directory i Azure Active Directory lub Office365 i Google Workspace) i przetrzymywać telemetrię w wspólnym kolektorze danych. Zebrane dane w kolektorze danych muszą być wykorzystywane w sposób automatyczny do ochrony stacji końcowych (m.in. WS28 itd.).

Zamawiający podtrzymuje zapis - WO8 - Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz prawidłowego funkcjonowania. Zamawiający nie posiada systemu SIEM.

Pytanie nr 67

WS27

Wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywa się na serwerze, a nie na monitorowanej stacji końcowej.

Pytanie: Czy Zamawiający zamiast przechowywania telemetrii w konsoli zarządzającej dopuszcza przesyłanie wybranych przez administratora danych bezpośrednio do zintegrowanego systemu SIEM?

Odpowiedź:

Zamawiający dopuszcza, że rozwiązania przechowujące całą telemetrię poza konsolą centralnego zarządzania.

Oferowane rozwiązanie musi zbierać telemetrię z stacji końcowych i innych źródeł (m.in. Active Directory i Azure Active Directory lub Office365 i Google Workspace. Zebrane dane w kolektorze danych muszą być wykorzystywane w sposób automatyczny do ochrony stacji końcowych (m.in. WS28 itd.).

Zamawiający podtrzymuje zapis - WO8 - Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz

prawidłowego funkcjonowania.

Zamawiający nie posiada systemu SIEM.

Pytanie nr 68

WS31

Telemetria zbierana ze stacji końcowych uwzględnia minimalnie takie elementy jak:

• połączenia sieciowe do/ze stacji, w tym takie szczegóły jak:

- adresy

- porty

- stan połączenia

- ilość danych otrzymanych/wysłanych

- czas utworzenia połączenia

• działania na plikach, operacje:

- utworzenia

- zmiany nazwy

- usunięcia pliku

- zapisywanie

- przesunięcie

- modyfikacja

- wraz z informacją o tym, jaki proces wykonywał dane działanie oraz jaki użytkownik jest zalogowany w systemie podczas tej operacji

• operacje w rejestrze

- skasowanie wartości

- ustawienie wartości

- utworzenie klucza

- kasowanie klucza

- zmiana nazwy klucza

• utworzenie nowego procesu i zakończenie procesu

Pytanie: Czy Zamawiający dopuszcza, aby w ramach telemetrii bezpieczeństwa do systemu SIEM przekazywane były następujące informacje:

- Tworzenie procesu

- Zakończenie procesu

- Połączenie Sieciowe

- Zalogowanie

- Wylogowanie
- Utworzenie pliku
- Usunięcie pliku
- Edytowanie plik
- Wczytanie z pliku
- Przeniesienie pliku
- Tworzenie klucza rejestru
- Usunięcie klucza rejestru
- Usunięcie wartości rejestru
- Modyfikowanie wartości rejestru

Odpowiedź:

Zamawiający podtrzymuje zapisy Specyfikacji Warunków Zamówienia.

Pytanie nr 69

WS32

Dostarczone rozwiązanie musi być dostarczone z funkcją umożliwiającą przetwarzanie i przechowywanie danych telemetrycznych z następujących systemów:

• stacje końcowe

• zdarzenia/logi (ang. events) z Active Directory i Azure Entra ID (Azure Active Directory) lub ochrania aplikacje Microsoft Office 365 i Google Workspace.

Jeśli funkcjonalność wymaga dodatkowych licencji, licencje powinny zostać dostarczone wraz z oferowanym oprogramowaniem.

Pytanie: Czy Zamawiający dopuszcza realizację tego punktu w następujący sposób:

1. Telemetria przesyła na SIEM dane tylko z punktów końcowych.

2. Active Directory, Azure Active Directory, Microsoft Office 365, Google Workspace jako zewnętrzne usługi mogą być monitorowane przez system EDR za pomocą API tych usług, dzięki czemu będzie szerszy wgląd w incydenty bezpieczeństwa, jeśli zdarzenie będzie ich dotyczyć.

a. Office365 – Obejmuje zewnętrzne sensory mail i audit, które rozszerzają wykrywanieo dane dotyczące ruchu i zawartości poczty e-mail, a także działań użytkowników i administratorów pobranych z ujednoliconego dziennika audytu Microsoft 365.

b. Czujnik mail uzyskuje dostęp do zdarzeń, takich jak czas dostępu do elementów poczty, czas odpowiedzi i przekazywania elementów poczty, a także czas i to, czego użytkownik szukał w usługach Exchange Online i SharePoint Online.

c. Czujnik audytu uzyskuje dostęp do działań użytkowników i administratorów wykonywanych w

usługach i rozwiązaniach Microsoft 365. Operacje te są przechwytywane, rejestrowane i przechowywane w ujednoliconym dzienniku inspekcji organizacji.

d. Active Directory - Zbiera i przetwarza informacje o zdarzeniach logowania w lokalnym Active Directory.

e. Azure AD - Zbiera i wstępnie przetwarza dane związane z aktywnością dotyczącą logowania użytkowników, a także zmianami w konfiguracji związanymi z użytkownikami i grupami.

f. Google Workspace - Zbiera i wstępnie przetwarza dane dotyczące aktywności i wykorzystania związane z kontami i usługami Google Workspace.

Odpowiedź:

Usługi Azure Active Directory, Microsoft Office 365, Google Workspace mogą być monitorowane przez API tych usług.

Oferowane rozwiązanie musi zbierać telemetrię z stacji końcowych i innych źródeł (m.in. AD i Azure AD lub Office365 i Google Workspace). Zebrane dane w oferowanym oprogramowaniu muszą być wykorzystywane w sposób automatyczny do ochrony stacji końcowych (m.in. WS28 itd.).

Zamawiający podtrzymuje zapis - WO8 - Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz prawidłowego funkcjonowania.

Zamawiający nie posiada systemu SIEM.

Pytanie nr 70

WS33

System przechowuje szczegółowe dane telemetryczne z wszystkich zabezpieczonych agentem stacji końcowych przez co najmniej 30 dni.

Pytanie: Czy Zamawiający dopuszcza realizację funkcjonalności poprzez przesyłanie danych do SIEM i przechowywanie danych po stronie SIEM?

Odpowiedź:

Zamawiający dopuszcza, że rozwiązania przechowujące całą telemetrię poza konsolą centralnego zarządzania.

Oferowane rozwiązanie musi zbierać telemetrię z stacji końcowych i innych źródeł (m.in. Active Directory i Azure Active Directory lub Office365 i Google Workspace. Zebrane dane w kolektorze danych muszą być wykorzystywane w sposób automatyczny do ochrony stacji końcowych (m.in. WS28 itd.).

Zamawiający podtrzymuje zapis - WO8 - Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz

prawidłowego funkcjonowania.

Zamawiający nie posiada systemu SIEM.

Pytanie nr 71

WS34

System przechowuje informacje o alarmach minimum przez okres 180 dni.

Pytanie: Czy Zamawiający dopuszcza przechowywanie danych o alarmach przez 90 dni?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Zamawiający nie dopuszcza przechowywanie danych o alarmach przez 90 dni.

Pytanie nr 72

WS35

System przechowuje informacje o incydentach minimum przez okres 180 dni.

Pytanie: Czy Zamawiający dopuszcza przechowywanie danych o incydentach przez 90 dni?

Odpowiedź:

Zamawiający podtrzymuje zapisy zawarte w Specyfikacji Warunków Zamówienia.

Zamawiający nie dopuszcza przechowywanie danych o incydentach przez 90 dni.

Pytanie nr 73

Warsztaty i szkolenia

Pytanie: Czy Zamawiający dopuszcza przeprowadzenie szkoleń przez autoryzowanego dystrybutora, który jest jednocześnie pierwszą linią pomocy technicznej dla polskich klientów, wobec faktu, że producent nie prowadzi szkoleń w języku polskim?

Odpowiedź:

Zamawiający wymaga warsztatów prowadzonych przez Wykonawcę, jak i certyfikowanych szkoleń producenta. Językiem warsztatów i certyfikowanych szkoleń musi być język polski.

Kanclerz
Uniwersytetu Rolniczego
im. Hugona Kołłątaja w Krakowie
Dyrektor ds. majątku i inwestycji
mgr Marcin Gałan