

znak: BAG.261.1.6.2017

Warszawa, 15 maja 2017 r.

Do wszystkich zainteresowanych

dotyczy: postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest „Rozbudowa systemu DLP Fidelis lub dostawa systemu równoważnego wraz z usługą wsparcia technicznego (maintenance)”

Do Centrali Narodowego Funduszu Zdrowia w dniu 28.04.2017 r. oraz w dniu 4.05.2017 r. wpłynęły zapytania o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia. Na podstawie z art. 38 ust. 1 ustawy Prawo Zamówień Publicznych Zamawiający udziela następującej odpowiedzi:

Pytanie nr 1

Dotyczy pkt. 3.2.1.1., 3.2.1.2. załącznika nr 1 do Specyfikacji.

W powyższych punktach Zamawiający wymaga, aby dostarczone rozwiązanie w obszarze ochrony danych przed wyciekami obsługiwało protokół UDP.

W opisie posiadanego obecnie przez Zamawiającego rozwiązania firmy Fidelis (w pkt. 1 i 2) Zamawiający wskazuje, że obecnie posiadane rozwiązanie, dla którego Zamawiający dopuszcza rozwiązanie równoważne, chroni dwa kanały komunikacji, tj. pocztę elektroniczną (na protokole SMTP) oraz dostęp do sieci Internet (na protokole http/HTTPS). Oba te kanały komunikacji korzystają z protokołu TCP. Czy zatem Zamawiający jest gotów zrezygnować z wymagania wsparcia dla protokołu UDP jako nadmiarowego w stosunku do swoich rzeczywistych potrzeb?

Odpowiedź na pytanie 1

Nie, Zamawiający pozostawia zapisy SIWZ bez zmian.

Pytanie nr 2

Dotyczy pkt. 3.2.1.21 załącznika nr 1 do Specyfikacji.

W punkcie tym Zamawiający wymaga obsługi kodowania BASE64. W związku z tym, że wymaganie to jest specyficzne oraz wedle wiedzy Wykonawcy tylko nieliczne systemy DLP dostępne na rynku wspierają ten standard, czy Zamawiający dopuszcza przeniesienie tego wymagania do pkt. 4, tzn. jako wymaganie opcjonalne dodatkowo punktowane?

Odpowiedź na pytanie 2

Nie, Zamawiający pozostawia zapisy SIWZ bez zmian.

Pytanie nr 3

Zamawiający stawia następujący warunek udziału w postępowaniu dotyczący zdolności technicznej i zawodowej:

„(...) Wykonawca wykaże, że wykonał (a w przypadku świadczeń okresowych lub ciągłych uwzględniane są również wykonywane) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres

prowadzenia działalności jest krótszy – w tym okresie, co najmniej 2 dostaw polegających na wdrożeniu systemu DLP Fidelis lub 2 dostaw polegających na wdrożeniu systemu równoważnego, każda o wartości przekraczającej 500.000,00 zł brutto. (...)

Mając na uwadze przedmiot zamówienia, jego zakres oraz specyfikę realizacji, należy wskazać, że podmiot, który należycie zrealizował co najmniej jedno zamówienie w zakresie dostawy i wdrożenia Systemu DLP ma wystarczającą wiedzę i doświadczenie, aby zrealizować przedmiotowe zamówienie. W opinii Wykonawcy warunek w zakresie zrealizowania „co najmniej dwóch dostaw polegających na wdrożeniu systemu DLP Fidelis” jest warunkiem wygórowanym.

Czy wobec powyższego, Zamawiający dopuści i uzna za wystarczające wykazanie w zakresie zdolności technicznej i zawodowej, realizacji przez Wykonawcę co najmniej jednej dostawy polegającej na wdrożeniu systemu DLP Fidelis lub jednej dostawy polegającej na wdrożeniu systemu równoważnego, o wartości przekraczającej 500.000,00 zł brutto?

Odpowiedź na pytanie 3

Nie, Zamawiający pozostawia zapisy SIWZ bez zmian.

Pytanie nr 4

Zamawiający stawia następujący warunek udziału w postępowaniu dotyczący zdolności technicznej i zawodowej, w zakresie osób spełniających wymagania tj. m.in. „jedna z osób posiada certyfikat CISSP”. Zamawiający wymaga konkretnego certyfikatu, nie wskazując na certyfikaty równoważne. Według wiedzy Wykonawcy certyfikat CISSP posiada certyfikaty równoważne, a Zamawiający zobowiązany jest przygotować i przeprowadzić zamówienie w sposób zapewniający zachowanie uczciwej konkurencji i równe traktowanie wykonawców. Wobec powyższego Wykonawca zwraca się z prośbą do Zamawiającego o dopuszczenie, aby osoba - inżynier realizujący zamówienie posiadał certyfikat równoważny do CISSP czyli np. certyfikat CISA (Certified Information Systems Auditor / Certyfikowany Audytor Systemów Informacyjnych).

Odpowiedź na pytanie 4

Zamawiający koryguje brzmienie punktu 5.1c **WARUNKI UDZIAŁU W POSTĘPOWANIU**

➤ Wykonawca na potrzeby realizacji zamówienia musi dysponować 2 osobami spełniającymi poniższe wymagania:

- każda z osób posiada uprawnienia nadane przez producenta zaoferowanego systemu do jego wdrożenia,
- każda z osób, powinna wykazać się udziałem w 2 projektach o podobnym zakresie do zamawianego w ciągu ostatnich trzech lat,
- jedna z osób posiada certyfikat CISSP lub certyfikat CISA (Certified Information Systems Auditor) lub certyfikat CEH (Certified Ethical Hacker).

Z uwagi na powyższe zapisy w załączniku nr 4 do umowy dotyczące certyfikatów zmieniają się w następujący sposób:

Lp.	Imię i nazwisko	Dokument potwierdzający posiadanie uprawnień / certyfikat CISSP lub certyfikat CISA (Certified Information Systems Auditor) lub certyfikat CEH (Certified Ethical Hacker do wdrożenia zaoferowanego systemu
1.		
2.		

Pytanie nr 5

Dotyczy pkt.8 Warsztaty szkoleniowe, załącznika nr 1 do Specyfikacji.

Zamawiający określił wymóg przeprowadzenia szkolenia w formie warsztatów dla 4 pracowników wskazanych przez Zamawiającego, które odbędą się w terminie do 30 dni od wdrożenia, nie określając wymaganej ilości godzin szkolenia.

Wykonawca wnosi o doprecyzowanie ilości wymaganych godzin szkolenia (np. 8 godzin). Wykonawca proponuje następujący zapis określający powyższe: „Wykonawca przeprowadzi szkolenie w formie warsztatów dla 4 pracowników wskazanych przez Zamawiającego w wymiarze 8 godzin dla każdej z dwóch grup szkoleniowych, każda grupa po 2 osoby”.

Odpowiedź na pytanie 5

Zamawiający koryguje brzmienie punktu 8.1. załącznika nr 1 do SIWZ na:

8.1. Wykonawca przeprowadzi szkolenie w formie warsztatów dla 4 pracowników wskazanych przez Zamawiającego, w wymiarze 24 godzin (przez cztery kolejne dni, po 6 godzin dziennie).

Pytanie nr 6

Dotyczy pkt.4 Dodatkowe funkcjonalności ppkt. 4.1, załącznika nr 1 do Specyfikacji.

Zamawiający określił w tym punkcie opcjonalną (dodatkowo punktowaną) funkcjonalność optycznego rozpoznawania tekstu (tzw. OCR). Z uwagi na to, że funkcjonalność ta jest kluczowa dla kompleksowej ochrony danych przed wyciekami (typowy scenariusz wycieku danych to konwersja dokumentu zawierającego dane osobowe do formatu graficznego albo skopiowanie zrzutu ekranowego w formie graficznej do schowka, a następnie wysłanie tak przygotowanego pliku graficznego (albo zawartości schowka) na zewnętrzny adres e-mail) oraz uwzględniając fakt, że opcja OCR może stanowić istotny składnik kosztowy oferowanych rozwiązań DLP Wykonawca zwraca się z prośbą o zwiększenie punktacji za tę funkcjonalność do 5 pkt. kosztem obniżenia wagi punktacji za cenę do 66%. Biorąc pod uwagę powyższe, w ocenie Wykonawcy, oferenci mogą nie być skłonni do oferowania tej – bardzo istotnej w opinii Wykonawcy – funkcjonalności.

Odpowiedź na pytanie 6

Nie, Zamawiający pozostawia zapisy SIWZ bez zmian.

Pytanie nr 7

Dotyczy pkt.5 Wymagania techniczne ppkt. 5.1, załącznika nr 1 do Specyfikacji.

Zamawiający wymaga dostarczenia systemu w formie kompletnego rozwiązania, instalowanego w sieci Zamawiającego. W celu optymalizacji kosztowej oferty (z korzyścią dla Zamawiającego) Wykonawca zwraca się z prośbą o informację, czy i jakie posiadane zasoby infrastruktury Zamawiający jest w stanie udostępnić Wykonawcy na potrzeby wdrożenia:

- czy i w jakim zakresie (max. liczba procesorów, max. wielkość RAM, max. wielkość dysków) zasoby w środowisku wirtualizacji VMware?
- czy i w jakim zakresie licencje na system serwerowy Windows Server (np. licencje Windows Server Datacenter dla środowiska wirtualizacji, o którym mowa wyżej)?
- w jakim zakresie infrastrukturę teletechniczną (ilość szaf – min. 2 szt., max. ilość jednostek U w każdej z szaf, max. moc zasilania w każdej z szaf, max. liczbę gniazd C13 w listwach zasilających w każdej z szaf, max. liczbę portów LAN w każdej z szaf).

Informacje te są niezbędne dla Wykonawcy na etapie przygotowania oferty, aby optymalnie do potrzeb Zamawiającego dobrać i wycenić konfigurację sprzętu i oprogramowania.

Odpowiedź na pytanie 7

Zamawiający oczekuje kompletnego rozwiązania, zatem nie przewiduje własnych zasobów w postaci: sprzętu fizycznego, środowiska wirtualnego, licencji systemów operacyjnych i wirtualizacji. Na potrzeby instalacji Zamawiający dysponuje miejscem w szafie w ilości 20 jednostek U w każdej lokalizacji. Zamawiający dostarczy potrzebną wymaganą ilość portów LAN wg specyfikacji Wykonawcy.

Pytanie nr 8

Dotyczy pkt.6 Usługi migracji i pełnego wdrożenia Systemu pkt. 6.3.1, załącznika nr 1 do Specyfikacji.

Wykonawca zwraca się z prośbą o potwierdzenie, że Zamawiający zapewni (np. w ramach aktywnego abonamentu serwisowego) i przekaze Wykonawcy wszelkie aktualizacje oprogramowania do posiadanych urządzeń IronPort, które okażą się potrzebne do wykonania „niezbędnych zmian w konfiguracji serwerów IronPort”, o których mowa w tym punkcie.

Odpowiedź na pytanie 8

Zamawiający koryguje brzmienie punktu 6.3 oraz 6.3.1. załącznika nr 1 do SIWZ na:

6.3. Po uprzednim uzgodnieniu i uzyskaniu akceptacji Zamawiającego Wykonawca **zobowiązany jest do:**
6.3.1. **wyspecyfikowania** wszelkich niezbędnych zmian w konfiguracji serwerów proxy IronPort, **przy czym prace związane z konfiguracją urządzeń sieciowych, w tym IronPort będą realizowane przez Zamawiającego;**

Pytanie nr 9

Dotyczy pkt. 3.2.1.9. Załącznika nr 1 do specyfikacji.

W punkcie tym Zamawiający wymaga cyt.: „*tworzenia reguł przy pomocy zaimplementowanych formularzy wraz z możliwością stosowania operacji logicznych (OR, AND, NOT itp.) wedle kryteriów:*

- a) urządzenie (IP/Subnet/port);
- b) cel (IP/Subnet/port);

- c) protokół;
- d) zawartość;
- e) użytkownik;
- f) czas; "

Pytanie 9.1

Czy Zamawiający dopuszcza rozwiązanie, w którym nie stosuje się operatorów logicznych w regułach, ale oczekiwana logika działania systemu DLP może zostać osiągnięta w inny sposób, tzn. poprzez odpowiednią konstrukcję reguł (w tym zdefiniowanych w regułach akcji) oraz poprzez ich odpowiednią kolejność (na liście reguł przetwarzania)?

Odpowiedź na pytanie 9.1.

Zamawiający dopuszcza każdy sposób konstruowania reguł, który umożliwia uzyskanie identycznego rezultatu, co rozwiązanie oparte na łączeniu operatorów logicznych.

Pytanie 9.2

Prosimy o wyjaśnienie, co Zamawiający rozumie pod pojęciem „czas” w kryterium w lit. f. Z uwagi na to, że kryterium czasowe w regułach DLP nie jest typowe dla tego typu rozwiązań (ochrona DLP powinna mieć co do zasady charakter ciągły bez ograniczeń czasowych) wnosimy o wykreślenie tego wymagania albo ewentualnie przeniesienie go do pkt. 4 jako wymaganie opcjonalne.

Odpowiedź na pytanie 9.2.

W tym przypadku „czas” należy rozumieć jako możliwość uruchamiania reguł w określonym przedziale czasu.

Pytanie 10a

Zamawiający w punkcie 2.3 pisze: „komponent *Fidelis XPS CommandPost* umożliwiający zarządzanie systemem”.

Czy w rozwiązaniu równoważnym Zamawiający jako system zarządzania rozumie komponent posiadający interfejs graficzny za pomocą, którego zarządza się całym systemem, bez konieczności logowania się lub przełączania do innych komponentów systemu?

Odpowiedź na pytanie 10a

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 10b

Czy komponent zarządzający powinien umożliwiać tworzenie polityk i reguł, propagować poprawki i upgrady do wszystkich komponentów systemu oraz zarządzać licencjami dla wszystkich komponentów systemu?

Odpowiedź na pytanie 10b

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 11

Czy Zamawiający wymaga, aby oferowane rozwiązanie umożliwiało zalogowanie się po SSH do każdego komponentu systemu, na przykład w celach diagnostycznych?

Odpowiedź na pytanie 11

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 12

Zamawiający w punkcie 3.1.3. pisze: „Rejestrowane dane związane z ruchem sieciowym muszą zawierać informacje o parametrach sesji: adresy i porty komunikacyjne, informacje o protokołach komunikacyjnych i aplikacjach, informacje o zawartości komunikacji”. Czy Zamawiający wymaga, aby dostarczone rozwiązania miało możliwość pełnej konfiguracji trybu pracy w tym zakresie, tj. czy zapisywany jest cały ruch sieciowy, czy wyłącznie metadane całego ruchu sieciowego, czy wyłącznie metadane powiązane z wykrytym incydem bezpieczeństwa czy cały ruch powiązany z wykrytym incydem bezpieczeństwa?

Odpowiedź na pytanie 12

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 13

Zamawiający w punkcie 3.2.1.1. pisze: „System musi mieć możliwość analizowania ruchu w czasie rzeczywistym na wszystkich portach TCP i UDP oraz niezależnie od portu wykrywać i analizować zawartość komunikacji sieciowej”. Czy Zamawiający przewiduje oprócz analizy w czasie rzeczywistym również analizę retrospektywną - zarówno na żądanie, jak i w sposób zautomatyzowany? Analiza retrospektywna (na danych historycznych) jest jedyną metodą adresowania coraz bardziej popularnych ataków rozciągniętych w czasie (np. ostatnie ataki na sektor bankowy poprzez stronę www KNF). Możliwość analizy danych historycznych ruchu sieciowego pozwala na identyfikację poszczególnych etapów ataku (sekwencji zdarzeń kończących się np. kradzieżą danych) i natychmiastowe ich blokowanie już we wczesnej fazie - zanim dojdzie do przejścia maszyny ofiary. Jest to bardzo istotna funkcja z punktu widzenia szeroko pojętych analiz bezpieczeństwa, np. rozwiązanie umożliwiające retrospektywną analizę pozwala potwierdzić, czy do domniemanego zdarzenia które zostało potwierdzone dzisiaj jako incydent bezpieczeństwa doszło/dochodziło również w przeszłości oraz których stacji końcowych dotyczyło. Przykładem może być weryfikacja, czy zatrzymany dzisiaj wyciek danych np. w formie wysłanego komunikatorem dokumentu typu .XLSX miał już miejsce wcześniej, np. weryfikując czy plik o tej samej sumie kontrolnej, tej samej nazwie etc.. był wcześniej widziany w sieci oraz kto i jakim kanałem go wysyłał. Ta sama funkcjonalność jest bardzo przydatna w ochronie przed atakami typu APT, kiedy można sprawdzić czy plik o konkretnej sumie kontrolnej w wykrytej dzisiaj kampanii pojawił się już wcześniej w sieci, a jeśli tak to na które komputery / zasoby sieciowe trafił. Czy z uwagi na planowane wykorzystanie rozwiązania w zakresie ochrony przed wyciekami danych oraz do ochrony przed atakami typu APT, Zamawiający wymaga aby dostarczone rozwiązanie umożliwilo zarówno analizę w czasie rzeczywistym jak i analizę retrospektywną? Jeśli tak to jakiego okresu retencji (kwartał? pół roku?) danych historycznych oczekuje Zamawiający.

Odpowiedź na pytanie 13

Zamawiający oczekuje funkcjonalności analizowania ruchu w czasie rzeczywistym.

Pytanie 14

Zamawiający w punkcie 3.2.1.10. pisze: „System musi mieć możliwość dowolnego łączenia wielu warunków w jednej polityce”. Czy Zamawiający rozumie przez to, aby dostarczone rozwiązanie umożliwilo tworzenie pojedynczych, prostych wyrażeń, które następnie łączone są w reguły i polityki bezpieczeństwa? Czy rozwiązanie ma umożliwiać wykorzystanie tych samych wyrażeń i reguł w wielu politykach jednocześnie? Funkcjonalność taka znacznie ułatwia administrację rozwiązaniem, ponieważ raz utworzone wyrażenie / reguła może być dowolnie i wielokrotnie wykorzystywana w politykach, w różnych konfiguracjach i kontekstach dzięki możliwości łączenia wyrażeń / reguł operatorami logicznymi (OR, AND, NOT, XOR itp.), w o których Zamawiający pisze w punkcie 3.2.1.9.

Odpowiedź na pytanie 14

Rozwiązanie ma umożliwiać wykorzystanie tych samych wyrażeń i reguł w wielu politykach jednocześnie. Zamawiający dopuszcza każdy sposób konstruowania reguł, który umożliwia uzyskanie identycznego rezultatu, co rozwiązanie oparte na łączeniu operatorów logicznych.

Pytanie 15

Czy oferowane rozwiązanie powinno mieć możliwość przypisywania adekwatnych polityk bezpieczeństwa do wybranego komponentu systemu, tak aby Zamawiający nie był zmuszony do wykorzystywania wszystkich polityk (nawet tych nieadekwatnych do chronionego obszaru) na każdym posiadanym komponentcie? Przykład: polityki chroniące dane w kanale pocztowym nie mają zastosowania przy ochronie ruchu do baz danych itp...

Odpowiedź na pytanie 15

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 16

Czy Zamawiający wymaga, aby oferowane rozwiązanie umożliwiało odkładanie całej komunikacji sieciowej pomiędzy adresami IP, które naruszyły politykę bezpieczeństwa systemu? Odłożony w ten sposób materiał w formie pliku PCAP stanowi materiał dowodowy w sprawie, ponieważ jest to zapisany czysty, niezmodyfikowany ruch sieciowy.

Odpowiedź na pytanie 16

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 17

Zamawiający w punkcie 3.2.1.27 pisze: „System musi mieć możliwość elastycznego zarządzania uprawnieniami Użytkownika m.in. poprzez:

- a) stosowanie oddzielnych ról do administracji systemem, w tym tworzenia i edycji polityk;
- b) stosowanie oddzielnych ról do zarządzania incydentami”

Czy Zamawiający wymaga, aby oferowane rozwiązanie pozwalało na bardziej granularne zarządzanie uprawnieniami użytkowników poprzez definiowanie uprawnień „full, view lub none” dla kluczowych obszarów zarządzania systemem takich jak: alerty, szczegóły alertów, kwarantanna, raporty, polityki, użytkownicy, administratorzy komponentów, administrator komponentu zarządzania, audytor, metadane, endpoint.

Odpowiedź na pytanie 17

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 18

Zamawiający w punkcie 3.2.1.22 pisze: „System musi mieć możliwość wykrywania i blokowania prób wycieku informacji chronionej w przesyłanych dokumentach Microsoft Office (Word, Excel, PowerPoint)”. Tak niewielki zakres chronionych typów plików stanowi istotne ograniczenie możliwości ochrony danych wrażliwych, które mogą być przesyłane w wielu innych powszechnie stosowanych formatach jak np pdf, txt, csv, html. Czy Zamawiający wymaga, aby oferowane rozwiązanie oferowało kompleksową ochronę danych poprzez możliwość wykrywania i blokowania prób wycieku informacji chronionej w przesyłanych dokumentach innego typu - co najmniej: pdf,txt,csv,html?

Odpowiedź na pytanie 18

Zamawiający koryguje brzmienie punktu 3.2.1.22 załącznika nr 1 do SIWZ na:

3.2.1.22 System musi mieć możliwość wykrywania i blokowania prób wycieku informacji chronionej w przesyłanych dokumentach Microsoft Office oraz dokumentach typu pdf, txt, csv, html.

Pytanie 19

Czy Zamawiający wymaga, aby oferowane rozwiązanie adresowało problem tzw. „powolnych wycieków”, gdzie eksfiltracja danych rozciągnięta jest w czasie? Wycieki tego typu z uwagi na swoją charakterystykę nie są wykrywane wprost, jednak wykrycie ich jest możliwe dzięki zastosowaniu mechanizmów wykrywających powtarzające się zjawiska sieciowe na przestrzeni długiego czasu. Na przykład sama polityka blokująca próby wysłania więcej niż 10 numerów PESEL jednocześnie jest niewystarczająca, ponieważ można wysłać co 5 minut zbiory zawierające nie więcej niż 10 numerów PESEL. Takie powtarzające się zjawisko może być jednak przechwycone poprzez inny mechanizm bezpieczeństwa, adresujący właśnie powtarzalne zjawiska sieciowe. Czy Zamawiający wymaga, aby oferowane rozwiązanie wyposażone było w mechanizmy wykrywania i korelacji zdarzeń sieciowych rozciągniętych w czasie?

Odpowiedź na pytanie 19

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 20

Zamawiający w punkcie 3.3.1.9. pisze: „System musi mieć możliwość automatycznego odpytywania zewnętrznych usług na temat reputacji analizowanych plików”. Czy Zamawiający ma na myśli usługę

zewnętrzna/obca – czy komponent systemu, który wysyła próbki plików do analizy w chmurze, przy jednoczesnej możliwości decydowania jakie typy plików mają być wysyłane (np. Wszystkie pliki, Nie wysyłaj żanych plików, Zaznaczone typy plików: exe, html, java-class, ms-excel, ms-office, ms-powerpoint, ms-rtf, ms-word, pdf, zip itp.). Czy Zamawiający także ma na myśli możliwość ręcznego wysyłania plików do analizy i przedstawianie ich analizy w taki sam sposób jak plików wysyłanych automatycznie?

Odpowiedź na pytanie 20

Wymaganie dotyczy automatycznego odpytywania zewnętrznych usług na temat reputacji analizowanych plików w ramach usługi zewnętrznej/obcej.

Pytanie 21

Czy Zamawiający wymaga, aby system miał możliwość zasilania go własnymi bazami informacji? Informacje takie, dostarczone w formie pliku płaskiego np. od organizacji typu CERT lub własnej komórki bezpieczeństwa, mogą być wykorzystywane w regułach i politykach bezpieczeństwa systemu.

Odpowiedź na pytanie 21

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 22

Zamawiający w punkcie 3.3.1.10. pisze: „System musi mieć możliwość wykonania automatycznej detonacji pozostałych podejrzanych plików. Wynik detonacji musi zostać przedstawiony w konsoli systemu i zawierać wszystkie zachowania, które detonowany plik wykonał z zaznaczeniem, które są niepożądane a które nie. Wszystkie zdarzenia dotyczące bezpieczeństwa z systemu ochrony przed APT muszą być eksportowane via Syslog”. Czy Zamawiający wymaga, aby oferowane rozwiązanie po za wynikami detonacji pliku przedstawiało również informacje dotyczące powiązanych z nim innych incydentów wykrytych przez to rozwiązanie wraz z pokazaniem ich części wspólnej / zależności pomiędzy wykrytymi incydentami a wynikiem detonacji pliku?

Odpowiedź na pytanie 22

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 23

Zamawiający w punkcie 5.2. pisze: „System musi zostać zintegrowany z rozwiązaniem klasy SIEM – ArcSight. Integracja polega na wysyłaniu logów i zdarzeń w trybie on-line z Systemu do ArcSight'a.”.

Pytanie 23a

Czy według Zamawiającego, oferowane rozwiązanie musi posiadać dedykowany, gotowy sposób exportu danych do ArcSight SIEM , który umożliwi prostą i szybką integrację z oferowanym systemem ?

Odpowiedź na pytanie 23a

Jeżeli system znajduje się na liście źródeł obsługiwanych przez ArcSighta, to nie musi posiadać dodatkowego sposobu exportu danych do ArcSight SIEM.

Pytanie 23b

Czy system musi mieć wbudowany sposób exportu zdarzeń wygenerowanych przez konkretne reguły, polityki, lub alerty z wybranych komponentów?

Odpowiedź na pytanie 23b

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 23c

Czy system musi posiadać możliwość definicji exportu alertu/grupy alertów z podziałem na kryteria alertu odpowiadające kolumnom w ArcSight SIEM?

Odpowiedź na pytanie 23c

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 24

Czy oferowane rozwiązanie powinno posiadać funkcjonalność wewnętrznego audytu, umożliwiającą logowanie wszystkich działań podjętych przez użytkowników na wszystkich komponentach takich jak: logowanie, zmiana konfiguracji, modyfikacja polityk, reguł, zarządzania alertami itp.?

Odpowiedź na pytanie 24

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

Pytanie 25

Zamawiający w punkcie 3.2.1.4. pisze: „System musi mieć możliwość tworzenia własnych wzorców danych podlegających ochronie”. oraz w punkcie 3.2.1.5. pisze: „System musi mieć możliwość rejestrowania informacji (dokumentu) podlegającego ochronie, w tym tworzenia sygnatur dokumentów chronionych”.

Czy według Zamawiającego oferowane rozwiązanie powinno w zakresie klasyfikacji informacji wrażliwych udostępniać wszystkie popularne metody klasyfikacji tych informacji tj. słowa kluczowe, słowniki słów kluczowych, wyrażenia regularne, tworzenie sygnatur z całych dokumentów, tworzenie sygnatur z wybranych części dokumentów oraz klasyfikacja znaków graficznych takich jak np. logo?

Odpowiedź na pytanie 25

System może posiadać wskazaną w pytaniu funkcjonalność, natomiast nie wchodzi to w zakres zasadniczych wymagań.

W związku z udzieloną odpowiedzią na zapytania oraz wprowadzonymi modyfikacjami Zamawiający informuje o przesunięciu terminu składania ofert na 5 czerwca 2017 r, i w związku z powyższym zmienia zapisy SIWZ odpowiednio:

- zapis Specyfikacji w rozdziale XI otrzymuje następujące brzmienie:

Termin wniesienia wadium upływa w dniu 5 czerwca 2017 r.

- zapis Specyfikacji w rozdziale XIII **OPIS SPOSOBU PRZYGOTOWANIA OFERT** pkt 11 otrzymuje następujące brzmienie:

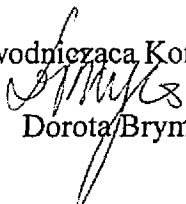
Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem wykonawcy oraz napisem „POSTĘPOWANIE NR BAG.261.1.6.2017 OFERTA – „Rozbudowa systemu DLP Fidelis lub dostawa systemu równoważnego wraz z usługą wsparcia technicznego (maintenance)” **NIE OTWIERAĆ PRZED 5 czerwca 2017 r. GODZ. 10:30.**”

- zapis Specyfikacji w rozdziale XIV **MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT** pkt 1, otrzymuje następujące brzmienie:

Oferty należy składać w zamkniętych kopertach w Narodowym Funduszu Zdrowia Centrala w Warszawie, przy ul. Grójeckiej 186, 02-390 Warszawa, pok. 0.02 **w terminie do dnia 5 czerwca 2017 r. do godz. 10:00.**

- zapis Specyfikacji w rozdziale XIV **MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT** pkt. 6 otrzymuje następujące brzmienie:

Otwarcie ofert odbędzie się **w dniu 5 czerwca 2017 r. o godz. 10:30** w Narodowym Funduszu Zdrowia Centrala w Warszawie przy ul. Grójeckiej 186, pok. 0.02.

Przewodnicząca Komisji Przetargowej

Dorota Brymas