



Gmina

NAKŁO NAD NOTECIĄ

Nakło nad Notecią, dnia 8 kwietnia 2025r.

GMINA NAKŁO NAD NOTECIĄ

89-100 Nakło n. Notecią
ul. Ks. Piotra Skargi 7, tel. 52 386 79 01
gm. Nakło n. Notecią, pow. nakielski
woj. kujawsko-pomorskie
REGON: 092350895, NIP 558-176-86-32

Zainteresowani Wykonawcy

Odpowiedzi na pytania

w postępowaniu prowadzonym na potrzeby szacowania wartości zamówienia w ramach realizacji projektu „Podniesienie poziomu cyberbezpieczeństwa Gminy Nakło nad Notecią” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Uprzejmie informuję, że w postępowaniu prowadzonym na potrzeby szacowania wartości zamówienia w ramach realizacji projektu „Podniesienie poziomu cyberbezpieczeństwa Gminy Nakło nad Notecią” wpłynęły pytania Wykonawcy. Poniżej przedstawiam treść pytań wraz z odpowiedziami:

Pytanie nr 1:

Dotyczy Zewnętrzna usługa Security Office

Zamawiający w pkt. 1.2) ppkt 2) wskazuje wymagania na posiadanie zespołu świadczącego usługę SOC. Wskazano posiadanie 9 osobowego zespołu. Co biorąc pod uwagę obowiązujące w Polsce prawo oznacza, że przyjęto założenie, że na jednej zmianie będzie pracowała tylko 1 osoba. Wynika to z wymagania 40 godzinnego tygodnia pracy oraz 11 godzinnych odstępów pomiędzy zmianami.

Z wieloletniej praktyki świadczenia usługi SOC uważamy, że taki zespół powinien liczyć co najmniej 12 osób.

W ppk.2 wskazano skład zespołu realizującego usługę SOC. W dalszych podpunktach określających zakres prac SOC wskazano, że Zamawiający oczekuje jedynie wykonywanie prac obejmujących swoim zakresem działanie linii 1 SOC (L1). Przy takim podejściu wymagania postawione przez Zamawiającego co do składu osobowego zespołu Wykonawcy są niewspółmiernie zawyżone. W szczególności wskazanie osób o kompetencjach ofensywnych nie ma swojego odzwierciedlenia w pracy analityków L1. W szczególności dotyczy to:

- inżynier bezpieczeństwa – posiadanie co najmniej dwóch osób z ważnym certyfikatem OSCP (ang. Offensive Security Certified Professional) jest to certyfikat osoby, która odpowiada za wykonywanie działań ofensywnych z reguły pentestów. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającego w dalszych punktach.
- architekt bezpieczeństwa – posiadanie co najmniej jednej osoby z ważnym certyfikatem CISSP (ang. Certified Information Systems Security Professional) jest to certyfikat osoby, która odpowiada za projektowanie infrastruktury bezpieczeństwa. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającego w dalszych punktach.
- pentester – posiadanie co najmniej jednej osoby z ważnym certyfikatem CEH (ang. Certified Ethical Hacker) lub OSCP (ang. Offensive Security Certified Professional) jest to certyfikat osoby, która odpowiada za wykonywanie działań ofensywnych z reguły pentestów. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują



Gmina

NAKŁO NAD NOTECIĄ

również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.

- jedną osobę, która posiada ważny certyfikat GIAC Certified Incident Handler (ang. GIAC Certified Incident Handler – GCIH) jest to certyfikat osoby, która odpowiada za wykonywanie działań związanych mitygacją zagrożeń. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.

- jedną osobę, która posiada ważny certyfikat Audytora Wiodącego Systemu Zarządzania Ciągłością Działania wg normy PN-EN ISO 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach. Audytowanie pod kątem ciągłości działania nie mieści się w żadnej definicji pracy SOC.

- kierownik zespołu – posiadanie co najmniej jednej osoby, która posiada:
 - o doświadczenie w prowadzeniu audytów co najmniej 5 lat.
 - o aktualny certyfikat w zakresie ciągłości działania, zgodnie z wymogami normy ISO 22301
 - o aktualny certyfikat w zakresie zarządzania bezpieczeństwem informacji zgodnie z wymogami normy ISO/IEC 27001

- o ważny certyfikat ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;

- o Certyfikat Prince2 Foundation – w zakresie zarządzania projektami;

Wymaganie postawione dla osoby pełniącej rolę Kierownika zespołu SOC nie są zgodne z charakterem pracy SOC, zwłaszcza w zakresie L1. Wymaganie doświadczenia w zakresie audytów nie ma związku z kierowaniem zespołu SOC, wymaganie certyfikatu w zakresie ciągłości działania ISO 23301 czy też ISO27001 nie ma również związku z zarządzaniem pracą zespołu SOC w zakresie L1. Podobnie sprawa ma się również w zakresie certyfikatu ITIL – rolę kierownika zespołu SOC w zakresie L1 nie jest projektowanie usług informatycznych po stronie klienta. A więc wymaganie takie certyfikatu jest głęboko nadmiarowe. Wymaganie certyfikatu w zakresie zarządzania projektami również nie ma żadnego uzasadnienia, zważywszy, że nie ma mowy w zapytaniu o realizacji prac projektowych.

Podsumowując Spółka wskazuje, że takie wymaganie nie są zasadne przy przedstawionym przez Zamawiającego zakresie pracy SOC, który dotyczy jedynie działań L1. Żaden zakres prac zespołu SOC nie wymaga, aby wymienieni specjaliści byli zaangażowani w prace.

W związku z powyższym Spółka zwraca się z wnioskiem o odstąpienie od tego wymagania oraz o wykreślenie komentowanego wymogu. Natomiast zwracamy się z sugestią powiększenia wymogu co do wielkości zespołu, aby zapewnić profesjonalne świadczenie usługi. Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt. 2):

„Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że skieruje do realizacji zamówienia co najmniej 12 specjalistów z odpowiednimi kwalifikacjami w zakresie monitorowania cyberbezpieczeństwa posiadającymi co najmniej 2 letnie doświadczenie na stanowisku analityka bezpieczeństwa.” certyfikatu ISO22301. Uzasadnieniem dodatkowym dla rezygnacji z tego zapisu jest również fakt, że Zamawiający w ppkt.2. stawiając wymagania wobec jednego z członków zespołu SOC oczekiwał ważnego certyfikatu Audytora ISO27001 w zakresie ciągłości działania, potwierdzając tym samym, że do potwierdzenia spełnia wymagań w zakresie ciągłości działania wystarczy certyfikat ISO 27001 w najnowszej wersji.

Prosimy o wykreślenie ppkt. 5).



Gmina

NAKŁO NAD NOTECIĄ

W przedstawionym w pkt. 1.2 zakresie pracy SOC, nie zostały uwzględnione działania linii 2 i linii 3. Zwracamy się z pytaniem, czy Zamawiający powyższe działania będzie realizował w swoim zakresie. Jeżeli nie, to naszym zdaniem zakres prac SOC powinien być rozszerzony o działania L2 i L3. Bazując na naszych wieloletnich doświadczeniach typowy zakres prac L2 i L3 obejmuje:

II Linia SOC – Zaawansowana Analiza i Reakcja

Zadania II linii SOC koncentrują się na zaawansowanej analizie, długoterminowej remediacji i zarządzaniu incydentami.

Zaawansowana Analiza Zagrożeń:

Przeprowadzanie szczegółowych analiz danych zbieranych przez SIEM i XDR, aby zrozumieć naturę i źródło zagrożeń.

Korzystanie z zaawansowanych narzędzi analitycznych do badania złośliwego oprogramowania, analizy penetracji i zrozumienia taktyk, technik oraz procedur (TTP) stosowanych przez przeciwników.

Manualna Remediacja i Długoterminowe Rozwiązania:

Opracowywanie i wdrażanie zaawansowanych strategii remediacji, które wykraczają poza automatyczne działania, w tym zmiany w konfiguracji, łatanie luki, usunięcie złośliwego oprogramowania. Współpraca z zespołami IT klienta do wprowadzenia zmian w infrastrukturze - w celu zapobiegania przyszłym atakom.

Zarządzanie Incydentami:

Koordynowanie działań w odpowiedzi na incydenty, w tym zarządzanie kryzysowe i komunikacja z klientem.

Dokumentowanie incydentów, ich przyczyn i podjętych działań w celu poprawy procedur i zabezpieczeń.

▪ Szkolenia i Rozwój:

Prowadzenie wewnętrznych szkoleń dla I linii SOC oraz innych działów związanych z bezpieczeństwem w celu podnoszenia ich kwalifikacji i świadomości.

Opracowywanie nowych scenariuszy reakcji na incydenty na podstawie obserwowanych ataków i zmieniającego się krajobrazu zagrożeń.

III Linia SOC Działania postincydentalne

Zadania III linii SOC koncentrują się na najbardziej zaawansowanych i skomplikowanych zadaniach, odgrywa ona kluczową rolę w przygotowaniu zaleceń dla klienta i wyjaśnienia pochodzenia incydentu.

▪ **Zaawansowana Analiza Zagrożeń**

Głęboka analiza danych: Trzecia linia SOC powinna specjalizować się w zaawansowanej analizie danych zebranych przez systemy monitorowania. Obejmuje to korzystanie z zaawansowanych narzędzi do analizy behawioralnej i heurystycznej, które pomagają identyfikować subtelne i złożone zagrożenia. Forensic cyfrowy: W przypadku incydentów trzecia linia odpowiedzialna jest za przeprowadzenie dogłębnej analizy incydentu (forensic, aby zrozumieć źródło, metodę ataku oraz zakres wpływu zagrożenia na systemy.

▪ **Reagowanie na Incydenty**

Rozwój i implementacja środków zaradczych: Opracowywanie skomplikowanych strategii reagowania na incydenty, które mogą obejmować izolację zainfekowanych systemów, eliminację zagrożeń oraz przywracanie operacji.

Automatyzacja reakcji: Tworzenie i wdrażanie automatycznych skryptów lub procedur, które umożliwiają szybkie reagowanie

▪ na podobne incydenty w przyszłości.

Rozwój i Implementacja Polityk Bezpieczeństwa

Opracowywanie polityk i procedur: Trzecia linia SOC bierze aktywny udział w tworzeniu i aktualizacji polityk bezpieczeństwa, które odpowiadają wymogom NIS2 i najlepszym praktykom branżowym.

Zgodność i audyty: Przeprowadzanie regularnych przeglądów bezpieczeństwa, aby zapewnić zgodność z



Gmina

NAKŁO NAD NOTECIĄ

obowiązującym prawem (np. dyrektywą NIS2) i innymi standardami. Współpraca z klientem w zakresie kontaktu z zewnętrznymi audytorami i inspektorami.

- **Szkolenia i Rozwój Umiejętności**

Szkolenia dla innych linii wsparcia: Przeprowadzanie zaawansowanych szkoleń dla personelu pierwszej i drugiej linii SOC, podnosząc ich umiejętności w zakresie wykrywania i reagowania na incydenty.

- **Zarządzanie Kryzysowe**

Planowanie i testowanie ciągłości działania: Opracowywanie kompleksowych planów ciągłości działania i regularne przeprowadzanie testów tych planów, aby zapewnić gotowość firmy na różne scenariusze cyberataków.

Koordinacja działań kryzysowych: Współpraca z klientem w celu koordynacji działań podczas poważnych incydentów bezpieczeństwa.

W przedstawionych w pkt. 1.2 wymaganiach na zespół realizujący usługę SOC wymieniono oczekiwania wobec osób zatrudnionych w takim zespole. Pomijając fakt, że tak specyficzne wymagania mogą ograniczać konkurencyjność poprzez fakt, że dużo większe niż wskazywane zespoły mogą po prostu nie dysponować konkretnymi certyfikatami. Ze względu na przedmiot zamówienia, regułą jest, że zamawiający oczekują posiadania przez wykonawców doświadczenia i posługiwania się referencjami od podmiotów z konkretną liczbą użytkowników lub komputerów, objętych świadczeniem usług monitorowania cyberbezpieczeństwa. W związku z powyższym Spółka proponuje zamianę wymagania postawionego wykonawcom w zakresie doświadczenia na wymaganie przedstawienia referencji ze świadczonych usług. Sugerujemy Zamawiającemu określenie liczby takich referencji według swoich potrzeb.

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 2):

„Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że skieruje do realizacji zamówienia co najmniej 12 specjalistów z odpowiednimi kwalifikacjami w zakresie monitorowania cyberbezpieczeństwa posiadającymi co najmniej 2 letnie doświadczenie na stanowisku analityka bezpieczeństwa oraz jeżeli Wykonawca wykaże, że w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie wykonał lub wykonuje co najmniej XXX usługi, w zakresie świadczenia usługi monitorowania cyberbezpieczeństwa dla podmiotów posiadających co najmniej 150 komputerów lub użytkowników, a przynajmniej XXX z ww. usług jest/była świadczona przez co najmniej 12 miesięcy do dnia upływu terminu składania ofert.”

Odpowiedź:

W SWZ do zadania pt. Zewnętrzna usługa Security Office Zamawiający ujął minimum, jakie musi spełnić Wykonawca.

Pytanie nr 2:

Zamawiający w pkt. 1.5) wskazuje wymagania na wdrożenie narzędzia SIEM jednocześnie w ppkt.2 Zamawiający wskazuje, że oczekuje od systemu SIEM możliwości reagowania. Zwracamy się z pytaniem, czy Zamawiający oczekuje, że elementem wdrożenia będzie również moduł SOAR? Moduł SOAR umożliwia integrację z urządzeniami sieciowymi i systemami bezpieczeństwa, co umożliwia półautomatyczne reagowanie na zdarzenia i zarządzanie incydentami. Posiadanie takiego modułu przyspiesza czas reakcji na zdarzenie co ma istotne przełożenie na działań SOC i bezpieczeństwo Zamawiającego jak również ma istotne znaczenie w przypadku wystąpienia masowych zdarzeń. Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 1): *„Przedmiotem zamówienia jest dostawa Systemu składającego się z rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management) wraz modułem SOAR(Security Orchestration,*



Gmina

NAKŁO NAD NOTECIĄ

Automation and Response) zwanego dalej Systemem SIEM."

SIEM – Security

Information and Event Management) wraz modulem SOAR (Security Orchestration, Automation and Response) zwanego dalej Systemem SIEM."

W ppkt. 7 Zamawiający wymaga, aby: „SIEM musi posiadać możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak:

- Elasticsearch,
- Kibana,
- Splunk,
- Docker,

aby umożliwić elastyczne dostosowanie platformy do indywidualnych potrzeb Zamawiającego “.

Zwracamy się z pytaniem z czego wynika potrzeba integracji:

1. narzędziem SIEM jakim jest SPLUNK,
2. narzędziem SIEM jakim jest Elasticsearch,
3. narzędziem do wizualizacji danych Kibana,
4. środowiskiem Docker.

Naszym zdaniem integracja narzędzia SIEM z innymi takimi samymi narzędziami jest nadmiarowa. Nasuwa się pytanie, czy Zamawiający dysponuje tymi wszystkimi narzędziami? Naszym zdaniem konieczna jest integracja narzędzia SIEM z urządzeniami brzegowymi, urządzeniami sieciowymi, innymi systemami bezpieczeństwa (np. DLP, XDR) w zakresie pobierania logów i możliwości reakcji na zdarzenia. Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 7):

„SIEM musi posiadać możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak urządzenia sieciowe, firewalle, systemy bezpieczeństwa (np. EDR/XDR), systemy operacyjne, bazy danych itp. W celu pobrania logów i dla wybranych urządzeń i systemów reakcji na zdarzenia”.

Odpowiedź:

Zamawiający podczas składania projektu wnioskował o system SIEM, moduł SOAR nie jest systemem SIEM, tak więc Zamawiający nie przewiduje modułu SOAR.

Zamawiający przychyliła się do propozycji zmiany wpisu w ppkt. 7.

Pytanie nr 3:

Zamawiający wymaga, aby: „Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania”.

W powyższym wymaganiu, brakuje informacji o zapewnieniu wsparcia technicznego producenta i wykupionym serwisem odnośnie aktualizacji i rozwoju systemu (nowe funkcjonalności).

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 12):

„wdrożone system klasy SIEM musi być produktem komercyjnym, oferowanym na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta. Wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia systemu SIEM pozwalające na świadczenie usług na systemach, na czas trwania umowy wraz aktualizacją systemu o pojawiające się nowe wersje. W ramach zapewnionego wsparcia Wykonawca musi dostosowywać na bieżąco reguły korelacyjne do



Gmina

NAKŁO NAD NOTECIĄ

zmieniającego się środowiska Zamawiającego tak, aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alarmy."

Odpowiedź:

Zamawiający dopuszcza zmianę w zapisie zgodnie z propozycją, dokonując zmiany w propozycji polegającej na wykreśleniu wzmianki o produktach komercyjnych co mogłoby mieć znaczący wpływ na możliwość zaproponowania różnych rozwiązań.

Pytanie nr 4:

Zamawiający wymaga, aby: „Cotygodniowe raportowanie błędów w konfiguracji opartych o benchmarki CIS oraz podatności zidentyfikowane przez system SIEM”

Prosimy o wyjaśnienie celu tworzenia takiego raportu w SIEM, skoro za badanie podatności odpowiadają inne narzędzia?

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na usunięcie tego wymagania.

Odpowiedź:

Zamawiający przychylił się do propozycji usunięcia wpisu.

Pytanie nr 5:

W związku z faktem, iż zapytanie obejmuje zarówno dostawę i wdrożenie narzędzi w zakresie ochrony endpointów, rejestracji incydentów oraz uruchomienia usługi SOC i wdrożenia SIEM Spółka zwraca się z wnioskiem o wydzielenie pkt. 2 i pkt 5 jako odrębnego zapytania obejmującego wdrożenia narzędzia SIEM i świadczenie usługi SOC, naszym zdaniem są to działania komplementarne.

Odpowiedź:

Zamawiający nie wyraża zgody na wyodrębnienie niniejszych zadań jako odrębnych zapytań. Dotyczy:

1. Zewnętrzna usługa Security Office
2. Wdrożenie SIEM

Pytanie nr 6:

Wymagania sprzętowe, które zostały przedstawione, odnoszą się do konkretnego modelu urządzenia. Po konsultacji z producentem otrzymaliśmy informację, że wskazany sprzęt posiada status EOL (End of Life), co oznacza, że osiągnął koniec swojego cyklu życia. W praktyce producent zaprzestął jego wspierania tego modelu w tym jego produkcji i sprzedaży.

W związku z powyższym, czy zmienia Państwo opis specyfikacji urządzenia tak aby dopuszczał również rozwiązania innych producentów, takich jak Hewlett Packard Enterprise.



Gmina

NAKŁO NAD NOTECIĄ

Odpowiedź:

Zamawiający dokonał aktualizacji OPZ - Wdrożenie pełnego systemu kopii zapasowej w modelu 3-2-1 według wskazanych uwag.

Pytanie nr 7:

Opis specyfikacji wskazuje na jedno konkretne rozwiązanie. W rezultacie zwracamy się z prośbą o zmianę opisu specyfikacji urządzenia, tak aby umożliwiał także rozwiązania innych producentów, takich jak Hewlett Packard Enterprise.

Odpowiedź:

Zamawiający dokonał aktualizacji OPZ - Wdrożenie pełnego systemu kopii zapasowej w modelu 3-2-1 według wskazanych uwag.

Pytanie nr 8:

Dotyczy Zewnętrzna usługa Security Office

Prosimy o wyjaśnienie/korektę zapisów w pkt. 1.2) W ppk.2 wskazano skład zespołu realizującego usługę SOC. W dalszych podpunktach określających zakres prac SOC wskazano, że Zamawiający oczekuje jedynie wykonywanie prac obejmujących swoim zakresem działanie linii 1 SOC (L1).

Jednocześnie Zamawiający postawił wymagania na Certyfikaty posiadane przez pracowników SOC. Opierając się na zakresie prac, które ma realizować zespół SOC postawione wymagania utrudniają uczciwą konkurencję.

Ze względu na przedmiot zamówienia, regułą jest, że zamawiający oczekują posiadania przez wykonawców doświadczenia i posługiwania się referencjami od podmiotów z konkretną liczbą użytkowników lub komputerów, objętych świadczeniem usług monitorowania cyberbezpieczeństwa. Zamawiający w swoich wymaganiach postawił konieczność posiadania przez pracowników SOC certyfikatów, które:

- Są niewspółmierne dla pracowników L1,
- Są związane z rolami, które nie występują w zakresie prac oczekiwanych przez Zamawiającego:
 - a. inżynier bezpieczeństwa – posiadanie co najmniej dwóch osób z ważnym certyfikatem OSCP (ang. Offensive Security Certified Professional) - jest to certyfikat osoby, która odpowiada za wykonywanie działań ofensywnych z reguły pentestów. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.
 - b. architekt bezpieczeństwa – posiadanie co najmniej jednej osoby z ważnym certyfikatem CISSP (ang. Certified Information Systems Security Professional) jest to certyfikat osoby, która odpowiada za projektowanie infrastruktury bezpieczeństwa. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.
 - c. pentester – posiadanie co najmniej jednej osoby z ważnym certyfikatem CEH (ang. Certified Ethical Hacker) lub OSCP (ang. Offensive Security Certified Professional) jest to certyfikat osoby, która odpowiada za



Gmina

NAKŁO NAD NOTECIĄ

wykonywanie działań ofensywnych z reguły pentestów. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.

d. jedną osobę, która posiada ważny certyfikat GIAC Certified Incident Handle (ang. GIAC Certified Incident Handler – GCIH) - jest to certyfikat osoby, która odpowiada za wykonywanie działań związanych mitygacją zagrożeń. Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach.

e. jedną osobę, która posiada ważny certyfikat Audytora Wiodącego Systemu Zarządzania Ciągłością Działania wg normy PN-EN ISO 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób - Działania takiej roli nie występują w zakresie prac L1 SOC, w najbardziej popularnych standardach opisujących pracę SOC – np. Security Framework NIST. Takie działania nie występują również w zakresie zdefiniowanym przez Zamawiającą w dalszych punktach. Audytowanie pod kątem ciągłości działania nie mieści się w żadnej definicji pracy SOC.

Wskazanie wymogu posiadania w zespole pracowników o tak konkretnych kompetencjach, nie związanych z pracą L1 SOC oraz wymogu posiadania tych konkretnych certyfikatów nosi w sobie znamiona naruszenia zasad nieuczciwej konkurencyjności i faworyzowania konkretnego dostawcy posiadającego pracowników posiadających te konkretne certyfikaty.

Podobnie rzecz ma się z wymogiem na osobę kierownika zespołu. Tak szczegółowe wymagania co do posiadania przez kierownika certyfikatów, nie związanych z pełnioną rolą sugerują znamiona naruszenia zasad nieuczciwej konkurencyjności i faworyzowania konkretnego dostawcy posiadającego pracowników posiadających te konkretne certyfikaty.

- kierownik zespołu – posiadanie co najmniej jednej osoby, która posiada:

- o doświadczenie w prowadzeniu audytów co najmniej 5 lat.

- o aktualny certyfikat w zakresie ciągłości działania, zgodnie z wymogami normy ISO 22301

- o aktualny certyfikat w zakresie zarządzania bezpieczeństwem informacji zgodnie z wymogami normy ISO/IEC 27001

- o ważny certyfikat ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;

- o Certyfikat Prince2 Foundation – w zakresie zarządzania projektami;

Wymaganie postawione dla osoby pełniącej rolę Kierownika zespołu SOC nie są zgodne z charakterem pracy SOC, zwłaszcza w zakresie L1. Wymaganie doświadczenia w zakresie audytów nie ma związku z kierowaniem zespołu SOC, wymaganie certyfikatu w zakresie ciągłości działania ISO 23301 czy też ISO 27001 nie ma również związku z zarządzaniem pracą zespołu SOC w zakresie L1. Podobnie sprawa ma się również w zakresie certyfikatu ITIL – rolą kierownika zespołu SOC w zakresie L1 nie jest projektowanie usług informatycznych po stronie klienta. A więc wymaganie takiego certyfikatu jest głęboko nadmiarowe. Wymaganie certyfikatu w zakresie zarządzania projektami również nie ma żadnego uzasadnienia, zważywszy, że nie ma mowy w zapytaniu o realizację prac projektowych. Podsumowując Spółka wskazuje, że takie wymagania nie są zasadne przy przedstawionym przez Zamawiającego zakresie pracy SOC, który dotyczy jedynie działań L1. Żaden zakres prac zespołu SOC nie wymaga, aby wymienieni specjaliści byli zaangażowani w prace. Postawione wymagania drastycznie ograniczają konkurencyjność. W związku z powyższym Spółka zwraca się z wnioskiem o odstąpienie od tego wymagania oraz o wykreślenie komentowanego wymogu. Natomiast zwracamy się z sugestią powiększenia wymogu co do wielkości zespołu, aby zapewnić profesjonalne świadczenie usługi.



Gmina

NAKŁO NAD NOTECIĄ

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt. 2):

„Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że skieruje do realizacji zamówienia co najmniej 9 specjalistów z odpowiednimi kwalifikacjami w zakresie monitorowania cyberbezpieczeństwa posiadającymi co najmniej 2 letnie doświadczenie na stanowisku analityka bezpieczeństwa. “

1. W zakresie prac wykonywanych przez SOC wskazano skład zespołu realizującego usługę SOC. W dalszych podpunktach określających zakres prac SOC wskazano, że Zamawiający oczekuje jedynie wykonywanie prac obejmujących swoim zakresem działanie linii 1 SOC (L1).

Pytanie do zamawiającego: Prosimy o potwierdzenie, że wymaganiem Zamawiającego jest jedynie pozyskanie Pierwszej linii SOC, a pozostałe kompetencje tj. linię II i III Zamawiający dostarczy w swoim zakresie?

Zamawiający w pkt. 1.2) ppkt 5) wskazuje wymagania na posiadanie ważnego certyfikatu ISO 22301 potwierdzającego posiadanie i możliwość realizacji procesów pozwalających utrzymać wszystkie działania SOC w deklarowanej ciągłości działania.

Przyjmując, że narzędzia wykorzystywane w zakresie monitorowania będą zainstalowane w infrastrukturze Zamawiającego oraz zważywszy na fakt, iż jednym z elementów nowej wersji normy ISO27001 jest również ciągłość działania Spółka wnosi o rezygnację z postanowienia i wymogu posiada certyfikatu ISO22301.

Uzasadnieniem dodatkowym dla rezygnacji z tego zapisu jest również fakt, że Zamawiający w ppkt.2. stawiając wymagania wobec jednego z członków zespołu SOC oczekiwał ważnego certyfikatu Audytora ISO27001 w zakresie ciągłości działania, potwierdzając tym samym, że do potwierdzenia spełnia wymagań w zakresie ciągłości działania wystarczy certyfikat ISO 27001 w najnowszej wersji.

Prosimy o wykreślenie ppkt. 5).

Odpowiedź:

Zamawiający częściowo odpowiedział już na zadane pytanie w punkcie oznaczonym jako Pytanie nr 1: „W SWZ do zadania pt. Zewnętrzna usługa Security Office Zamawiający ujął minimum, jakie musi spełnić Wykonawca, jeśli Wykonawca zaproponuje większość ilość zasobów będzie to na plus.”.

Uzupełniając odpowiedź o zadane dodatkowe pytania informujemy, że:

- a. nie wskazaliśmy jakie oczekiwania mamy odnośnie dostarczenia rozwiązania SOC wskazując na konkretne linie wsparcia, jest to do zaproponowania i zaprojektowania przez Wykonawcę,
- b. Zamawiające przychyła się do wniosku o usunięcie ppkt. 5 dotyczącego certyfikatu ISO27001.

Pytanie nr 9:

Dotyczy – wdrożenia SIEM

Zamawiający w pkt. 1.5) wskazuje wymagania na wdrożenie narzędzia SIEM jednocześnie w ppkt.2 Zamawiający wskazuje, że oczekuje od systemu SIEM możliwości reagowania.

Zwracamy się z pytaniem, czy Zamawiający oczekuje, że elementem wdrożenia będzie również moduł SOAR?

Moduł SOAR umożliwia integrację z urządzeniami sieciowymi i systemami bezpieczeństwa, co umożliwia półautomatyczne reagowanie na zdarzenia i zarządzanie incydentami. Posiadanie takiego moduły przyspiesza czas reakcji na zdarzenie co ma istotne przełożenie na działań SOC i bezpieczeństwo Zamawiającego jak również ma istotne znaczenie w przypadku wystąpienia masowych zdarzeń.

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 1):



Gmina

NAKŁO NAD NOTECIĄ

„Przedmiotem zamówienia jest dostawa Systemu składającego się z rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management) wraz modulem SOAR(Security Orchestration, Automation and Response) zwanego dalej Systemem SIEM.”

W ppkt. 7 Zamawiający wymaga, aby: „SIEM musi posiadać możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak:

- Elasticsearch,
- Kibana,
- Splunk,
- Docker,

aby umożliwić elastyczne dostosowanie platformy do indywidualnych potrzeb Zamawiającego“.

Zwracamy się z pytaniem z czego wynika potrzeba integracji:

1. narzędziem SIEM jakim jest SPLUNK,
2. narzędziem SIEM jakim jest Elasticsearch,
3. narzędziem do wizualizacji danych Kibana,
4. środowiskiem Docker.

Naszym zdaniem integracja narzędzia SIEM z innymi takimi samymi narzędziami jest nadmiarowa.

Prosimy o odpowiedź czy Zamawiający dysponuje wskazanymi narzędziami?

Jeśli nie, to jaki jest powód takiej integracji ?

Naszym zdaniem konieczna jest integracja narzędzia SIEM z urządzeniami brzegowymi, urządzeniami sieciowymi, innymi systemami bezpieczeństwa (np. DLP, XDR) w zakresie pobierania logów i możliwości reakcji na zdarzenia.

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 7):

„SIEM musi posiadać możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak urządzenia sieciowe, firewalle, systemy bezpieczeństwa (np. EDR/XDR), systemy operacyjne, bazy danych itp. W celu pobrania logów i dla wybranych urządzeń i systemów reakcji na zdarzenia”.

W ppkt 10) Zamawiający wymaga aby: „System SIEM musi mieć możliwość pracy w architekturze pozwalającej na instalację i konfigurację w wielu lokalizacjach,

Pytanie do zamawiającego: W ilu lokalizacjach ma być zainstalowany system SIEM ?

W ppkt. 12) Zamawiający wymaga aby: „Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania”.

W powyższym wymaganiu, brakuje informacji o zapewnieniu wsparcia technicznego producenta i wykupionym serwisem odnośnie aktualizacji i rozwoju systemu (nowe funkcjonalności).

Czy Zamawiający, w związku z powyższym, wyrazi zgodę na następującą zmianę treści ppkt 12):

„wdrożone system klasy SIEM musi być produktem komercyjnym, oferowanym na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta. Wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia systemu SIEM pozwalające na świadczenie usług na systemach, na czas trwania umowy wraz aktualizacją systemu o pojawiające się nowe wersje. W ramach zapewnionego wsparcia Wykonawca musi dostosowywać na bieżąco reguły korelacyjne do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alarmy.”

W ppkt. 13) Zamawiający wymaga aby: „Cotygodniowe raportowanie błędów w konfiguracji opartych o benchmarki CIS oraz podatności zidentyfikowane przez system SIEM”

Prosimy o wyjaśnienie celu tworzenia takiego raportu w SIEM, skoro za badanie podatności odpowiadają inne narzędzia? Czy Zamawiający, w związku z powyższym, wyrazi zgodę na usunięcie tego wymagania.



Gmina

NAKŁO NAD NOTECIĄ

Odpowiedź:

Podobnie jak w zapytaniu nr 8, Zamawiający udzielił już częściowo odpowiedzi:

- a. Zamawiający podczas składania projektu wnioskował o system SIEM, moduł SOAR nie jest system SIEM, tak więc Zamawiający nie przewiduje modułu SOAR,
- b. Zamawiający przychylił się do propozycji zmiany wpisu w ppkt. 7,
- c. Dotyczy ppkt 10. Zamawiający wymaga instalację systemu SIEM w jednej lokalizacji, w siedzibie głównej Zamawiającego. Zamawiający posiada kilka lokalizacji, wskazuje również o konieczność integracji w tych lokalizacjach z siedzibą główną,
- d. Dotyczy ppkt 12. Zamawiający dopuszcza zmianę w zapisie zgodnie z propozycją, dokonując zmiany w propozycji polegającej na wykreśleniu wzmianki o produktach komercyjnych co mogłoby mieć znaczący wpływ na możliwość zaproponowania różnych rozwiązań.
- e. Dotyczy ppkt. 13. Zamawiający przychylił się do propozycji usunięcia wpisu.

Pytanie nr 10:

Dotyczy – Bezpieczeństwo na urządzeniach końcowych wraz z ochroną poczty

Zamawiający wymaga aby ochronie podlegały Urządzenia mobilne z systemami Android.

Pytanie do zamawiającego: Proszę o podanie informacji, ile urządzeń mobilnych będzie podlegało ochronie przez agenta oprogramowania. Zamawiający wymaga aby ochronie podlegały serwery MS Exchange i jednocześnie M365.

Pytanie do zamawiającego: Prosimy o informacje, czy taki wymóg wynika z faktu iż Zamawiający posiada serwery pocztowe onprem i chmurowe (usługa M365 z pocztą).

Odpowiedź:

Zamawiający przewiduje instalacje ochrony na 150 końcówkach z systemem Android. Wymóg ochrony dla MS Exchange i M365 wynika z posiadanego przez Zamawiającego rozwiązania.

W związku z odpowiedziami na pytania oraz koniecznością modyfikacji opisu przedmiotu zamówienia, Zamawiający zmienia formularz szacowania - stanowiący załącznik do niniejszego pisma oraz przekazuje OPZ po zmianach.

Z up. BURMISTRZA
Krzysztof Koptyszka
Sekretarz Miasta i Gminy

