1. Czy Zamawiający rozważy certyfikaty równoważne dla analityków SOC?

Odpowiedź na analogiczne pytanie została udzielona w dokumencie Pytania02.pdf:
„Zamawiający podtrzymuje wymóg przedstawienia certyfikatów CEH i/lub CompTia Security+ posiadanych przez wszystkich analityków bezpieczeństwa, o których mowa w punkcie 3.3. Zapytania Ofertowego, przy czym obowiązek posiadania co najmniej jednego wymaganego certyfikatu dotyczy wszystkich analityków, a każdy z wymaganych certyfikatów powinien wystąpić co najmniej raz. Jednocześnie Zamawiający nie uzna za wystarczające przedstawienie innych certyfikatów."

2. Czy oczekiwanie sformułowane w Zapytaniu pkt.3.4 dot. posiadania przez analityków wskazanych certyfikatów należy rozumieć jako warunek alternatywny? Tj. każdy z analityków powinien posiadać co najmniej jeden z wymienionych certyfikatów.

Zamawiający dopuszcza posiadanie przez każdego z analityków bezpieczeństwa, o których mowa w punkcie 3.3 Zapytania Ofertowego, jednego z certyfikatów CEH i/lub CompTia Security+ lub obu certyfikatów łącznie, przy czym każdy z wymaganych certyfikatów powinien wystąpić co najmniej raz.

3. Czy skanowanie podatności systemów i usług Zamawiającego dotyczy usług dostępnych wyłącznie w LAN?

Przez skanowanie podatności systemów i usług Zamawiającego Zamawiający rozumie działania zmierzające w kierunku znalezienia podatności oraz błędów w konfiguracji urządzeń w celu zaplanowania działań ograniczających możliwość włamania i wycieku danych z systemów Zamawiającego. Biorąc pod uwagę możliwość dokonania włamania do systemów Zamawiającego z zewnątrz, skanowanie podatności powinno być przeprowadzone dla systemów widocznych od strony sieci publicznej.

4. Ile źródeł Zamawiający zaplanował do podłączenia do systemu SIEM na etapie wdrożenia?

Określenie ilości źródeł logów dla systemu SIEM Zamawiający powierza Wykonawcy w ramach okresu wdrożenia. Wykonawca, dysponując wiedzą i doświadczeniem z zakresu świadczenia usługi monitorowania bezpieczeństwa systemów powinien być w stanie określić wymagane źródła logów dla systemu SIEM po zapoznaniu się z architekturą systemu Zamawiającego. Zamawiający nie posiada takiego doświadczenia, które umożliwiałoby określenie ilości źródeł danych dla systemu SIEM na etapie postępowania. W punkcie 3.8 Opisu Przedmiotu Zamówienia minimalna ilość źródeł logów obsługiwana przez Wykonawcę określona jest na 50.

5. Czy Zamawiający dopuszcza współpracę w ramach wymiany informacji z wykorzystaniem systemu klasy ITSM Wykonawcy? System ITSM zapewnia m.in. wysyłanie powiadomień mailowych o nowych zdarzeniach i incydentach.

W par. 2, ust. 1, pkt. 2 Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo mowa jest o redundantnych środkach łączności umożliwiających prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczona jest usługa. Wykorzystanie do tego celu jedynie kanału e-mail zdaniem Zamawiającego jest niewystarczające. W punkcie 3.11 Opisu Przedmiotu Zamówienia określone są dwa sposoby informowania Zamawiającego o wykrytych incydentach: telefon oraz e-mail.

6. Jakie kategorie źródeł posiada w swoim środowisku IT Zamawiający (np. firewall'e, systemy proxy,

systemy ochrony stacji roboczych i serwerów, bramki AV/Aspam dla poczty elektronicznej, systemy IDS/IDP, inne)?

Zamawiający posiada domenę Microsoft Windows, serwery Microsoft Windows, w tym serwery Exchange, system bezpiecznego dostępu do sieci, bramę e-mail, firewall, system antywirusowy, switche, routery. Zamawiający polega na wiedzy i doświadczeniu Wykonawcy w kwestii ustalenia źródeł danych, które powinny być poddane analizie w celu zapewnienia optymalnej ochrony systemów Zamawiającego.

7. Jaki zakres prac obejmuje pisanie złożonych polityk bezpieczeństwa ?

Zamawiający oczekuje pomocy w tworzeniu i ocenie polityk bezpieczeństwa obowiązujących w organizacji Zamawiającego, w których Wykonawca wykorzysta szerszą niż posiada Zamawiający wiedzę na temat zapewnienia bezpieczeństwa monitorowanych systemów.