OPIS PRZEDMIOTU ZAMÓWIENIA

ŚWIADCZENIE USŁUG NADZORU BEZPIECZEŃSTWA INFORMATYCZNEGO NA POTRZEBY PRZEDSIĘBIORSTWA ENERGETYKI CIEPLNEJ GLIWICE W MODELU USŁUGOWYM

Przedmiotem Zamówienia jest świadczenie usługi nadzoru bezpieczeństwa informatycznego (ang. MSS – Managed Security Services) w formule zdalnego dyżuru Centrum Nadzoru Bezpieczeństwa, zwanego dalej SOC (ang. Security Operations Center).

Zamawiający oczekuje realizacji SOC jako usługi (ang. SOC as a Service) obejmującej całość instytucji w sposób kompleksowy, zgodnie z wytycznymi aktów prawnych obowiązujących w dniu zawarcia umowy, w szczególności Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 1560), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz Ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych (Dz. U. poz. 1000). Zamawiający informuje jednocześnie, iż w chwili złożenia zamówienia nie posiada kompletnej dokumentacji związanej z analizą ryzyka teleinformatycznego, ani kompletu wytycznych Polityki Bezpieczeństwa, a co za tym idzie oczekuje od Wykonawcy, w początkowej fazie realizacji zadania, usług związanych z doradztwem i konsultacją pod kątem ogólnie przyjętych dobrych praktyk sztuk telekomunikacyjnej z zakresu bezpieczeństwa informacji, w celu zaprojektowania i wdrożenia rozwiązań technicznych pozwalających na skuteczny nadzór i zarządzanie bezpieczeństwem informatycznym, ze szczególnym naciskiem związanym z wymaganiami specyficznymi dla branży energetyki cieplnej.

Celem niniejszego zamówienia jest uruchomienie, wdrożenie, a następnie utrzymanie stałego monitoringu infrastruktury IT Zamawiającego, identyfikacja i raportowanie występujących w jej obszarze zagrożeń, detekcja obsługa incydentów, a także ciągłe, cykliczne dostarczanie rekomendacji dotyczących poprawy stanu bezpieczeństwa. Usługa świadczona przez Wykonawcę powinna pozwolić Zamawiającemu na zachowanie wysokiego poziomu odporności użytkowanych systemów cyfrowych na obecne w przestrzeni technicznej zagrożenia, przy uniknięciu konieczności tworzenia i utrzymywania własnego, wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo IT.

Zamawiający przewiduje podział zadania na dwa kolejne etapy:

1) Etap 1: Wdrożenie i uruchomienie systemu nadzoru cyberbezpieczeństwa.

W ramach tej części zadania pierwszym obowiązkiem Wykonawcy będzie przeprowadzenie inwentaryzacji infrastruktury własnej Zamawiającego, w celu opracowania planu wdrożenia obejmującego użytkowane systemy w sposób optymalny i kompleksowy. Zamawiający zaznacza, iż posiada wyraźny podział funkcyjny, związany z drastycznie odmiennymi wymogami bezpieczeństwa i poziomem ryzyka dotyczącymi systemów użytkowanych w przestrzeni administracyjno-biurowej, oraz systemami użytkowanymi na potrzeby automatyki przemysłowej (infrastruktura OT). Wykonawca zobowiązany będzie do objęcia nadzorem zarówno stacji roboczych pracowników, infrastruktury sieci LAN, urządzeń bezpieczeństwa sieci, stanowiących styk z zasobami publicznej sieci Internet, jak i wewnętrznej infrastruktury serwerowej, użytkowanej na terenie siedziby firmy. Obowiązkiem Zamawiającego będzie umożliwienie wykonania czynności niezbędnych dla prawidłowego wykonania inwentaryzacji, w tym umożliwienie odbycia wizji lokalnych i wglądu w konfigurację urządzeń aktywnych, pod nadzorem personelu technicznego firmy. Zakres przeprowadzonej inwentaryzacji objąć musi,

co najmniej, rodzaj i ilość użytkowanego sprzętu sieciowego, sprzętu serwerowego, maszyn wirtualnych i ich hipernadzorców, stacji roboczych, systemów operacyjnych, wykorzystywanej adresacji IP, rodzaju i ilości wykorzystywanych protokołów komunikacyjnych, oraz podziału funkcyjnego, związanego z separacją stref bezpieczeństwa.

Zamawiający informuje, iż użytkuje systemy eksperckie, uruchomione i obsługiwane przez serwisy firm zewnętrznych. W związku z ich szczególnym charakterem wymagać będzie ścisłej współpracy pomiędzy Wykonawcą i podmiotami trzecimi odpowiedzialnymi za serwis i utrzymanie przedmiotowych systemów. Zobowiązanie podmiotów trzecich do podjęcia cytowanej współpracy będzie, każdorazowo, obowiązkiem Zamawiającego. W przypadku braku możliwości przeprowadzenia pełnego wdrożenia danego systemu eksperckiego, Zamawiający oczekuje nadzoru prowadzonego w schemacie czarnej skrzynki – obserwacji ruchu sieciowego w punktach egressu systemu, stanowiących demarkację jego obszaru działania oraz obserwacji wskaźników kompromisu (ang. IOC – indicators of compromise), których pozyskanie będzie możliwe bez wywarcia wpływu na produkcyjne funkcjonowanie danego elementu.

Zamawiający oczekuje wdrożenia systemu klasy SIEM (ang. Security Information and Event Management), w formie usługi świadczonej przez Wykonawcę, przy czym bezwzględnym oczekiwaniem jest wykorzystanie systemu nadzoru w sposób umożliwiający pełną retencję danych podlegających akwizycji na terenie siedziby Zamawiającego i pod jego bezpośrednią kontrolą. Zamawiający dopuszcza, by wszystkie pozostałe elementy systemu, poza powyżej wymienionymi serwerami pośredniczącymi w przekazywaniu informacji o stanie infrastruktury, funkcjonowały w lokalizacji zdalnej, pod kontrolą Wykonawcy. Opcjonalnie dopuszcza się, dodatkowo, uruchomienie części elementów funkcjonalnych systemu SIEM na terenie siedziby Zamawiającego, jeśli rozwiązanie takowe zapewni wyższą niezawodność wdrożonego rozwiązania. Wymaga się bezwzględnie zachowania zasad poufności informacji, gwarantujących traktowanie wszelkich danych pozyskanych, w trakcie realizacji zadania, jako informacji chronionej, do wyłącznego użytku Zamawiającego, przetwarzanej przez Wykonawcę zgodnie z zasadą minimalizmu w dostępie do informacji, cytowaną w normie ISO 27001.

Etap powyższy obejmować może okres maksymalnie trzech miesięcy, licząc od daty rozpoczęcia prac i uwzględniać powinien przekazanie Zamawiającemu wytycznych konfiguracyjnych dotyczących urządzeń oraz systemów objętych nadzorem, wraz z instrukcją ich zastosowania. Obowiązkiem Wykonawcy będzie udział w ostatecznej konfiguracji elementów infrastruktury, w tym instalacji niezbędnych agentów systemowych, pod ścisłym nadzorem personelu technicznego Zamawiającego. Etap zakończony zostać powinien obustronna weryfikacją poprawności wykonanej konfiguracji oraz pisemnym oświadczeniem Wykonawcy o gotowości do realizacji etapu drugiego.

2) Etap 2: Świadczenie usług nadzoru bezpieczeństwa informatycznego, raportowanie zdarzeń i obsługa incydentów.

Zadaniem Wykonawcy będzie świadczenie usług nadzoru bezpieczeństwa informatycznego SOC w charakterze niebieskiej linii wsparcia, definiowanej jako dyżur odpowiedzialny za analizę zdarzeń obserwowanych w infrastrukturze Zamawiającego, ich wzajemną korelację, wykrywanie i segregacja alertów. Podstawowym celem świadczonej usługi będzie detekcja, klasyfikacja oraz obsługa ewentualnych incydentów bezpieczeństwa, wraz ze sporządzeniem raportów, zawierających rekomendacje działań po stronie Zamawiającego. W przypadku potwierdzenia rzeczywistego zagrożenia incydent, wraz z kontekstem zasięgu i potencjalnego wpływu, podlegał będzie środkom zaradczym, inicjowanym przez Wykonawcę w ścisłym porozumieniu i pod nadzorem personelu technicznego Zamawiającego. Opracowanie procedur postępowania w przypadku detekcji zagrożeń odbywać będzie się na podstawie rekomendacji Wykonawcy, bazujących na doświadczeniu i powszechnie stosowanych dobrych praktykach sztuki telekomunikacyjnej, z uwzględnieniem

fragmentów polityk bezpieczeństwa i analizy ryzyka, ujawnionych Wykonawcy przez Zamawiającego. Wszystkie informacje pozyskane w trakcie realizacji przedmiotu zamówienia będą, obustronnie, traktowane jako informacja poufna i jako takie objęte zostaną osobną umową powierzenia informacji, stanowiącą załącznik do niniejszego zamówienia.

W związku z newralgiczną rolą Zamawiającego, jako instytucji świadczącej usługi kluczowe zarówno z punktu widzenia bezpieczeństwa publicznego jak i utrzymania w ruchu procesów przemysłowych, oczekiwane jest świadczenie usługi pełnej ochrony infrastruktury w rygorze 24/7/365 (24 godziny na dobę, 7 dni w tygodniu przez 365 dni w roku), przy czym analiza i wsparcie związane z dochodzeniem pozdarzeniowym, analiza forensyczna zabezpieczonego materiału, raportowanie oraz działania związane z rekomendacją ewentualnych zmian świadczone być mogą w rygorze 8/5 (analiza i wsparcie w standardowych godzinach urzędowych tygodnia roboczego).

Nie przewiduje się możliwości wykonywania aktywnych działań typu threat hunting, oczekiwane jest świadczenie usługi w pełni neutralnej dla wydajności i sposobu użytkowania obecnie wdrożonych rozwiązań. Ewentualne, niezbędne działania korekcyjne będą przedstawiane przez Wykonawcę w formie propozycji, podlegających weryfikacji Zamawiającego i wprowadzanych w życie wyłącznie pod bezpośrednim nadzorem jego personelu technicznego.

Zamawiający deklaruje pełną współpracę z Wykonawcą pod kątem zarządzania zmianami. SOC zostanie poinformowany o planowanych zmianach dotyczących infrastruktury przed ich wprowadzeniem, w celu uniknięcia fałszywych detekcji, oraz umożliwienia właściwej koordynacji, zapewniającej kompleksową obsługę całości instytucji w sposób bezprzerwowy.

Oczekiwaniem Zamawiającego jest integracja usługi nadzoru z użytkowanymi systemami zarządzania tożsamością i dostępem zdalnym, co pociąga za sobą konieczność przetwarzania danych osobowych. Na okoliczność powyższą zawarta zostanie osobna umowa przetwarzania danych osobowych, stanowiąca załącznik do niniejszego zamówienia.

Zakres danych podlegających korelacji i analizie musi być równoznaczny z logami pozyskiwanymi z kolektorów i agentów systemowych, zaimplementowanych w ramach realizacji etapu 1. Oczekiwana jest analiza postury bezpieczeństwa stacji roboczych, użytkowników końcowych, zdalnego dostępu pracowniczego, oraz zdalnego dostępu kontrahentów zewnętrznych świadczących usługi na potrzeby systemów eksperckich i wsparcia serwisowego, analiza stanu bezpieczeństwa wewnętrznej domeny Active Directory, infrastruktury serwerowej, infrastruktury sieciowej, elementów związanych z usługami telefonii cyfrowej VoIP (ang. Voice over Internet Protocol) oraz systemów wykonywania kopii zapasowych. Kategorycznie kluczowym, z punktu widzenia Zamawiającego, zagadnieniem będzie świadczenie usługi w sposób zapewniający zachowanie ciągłości działania systemów produkcyjnych. Wymagana jest retencja pozyskanych danych w okresie minimum trzech miesięcy dla danych podlegających analizie i korelacji (tzw. dane gorące), oraz pół roku kalendarzowego w przypadku danych archiwalnych, umożliwiających przywołanie w terminie późniejszym, w przypadku wystąpienia szczególnej potrzeby przeprowadzenia analizy wstecznej (tzw. dane zimne).

W ramach etapu 2 przedmiotu niniejszego zamówienia obowiązkiem Wykonawcy będzie sporządzanie cyklicznych raportów z funkcjonowania prowadzonego nadzoru bezpieczeństwa, oraz okazjonalnych raportów związanych z wystąpieniem incydentów, lub zdarzeń mogących prowadzić do materializacji incydentów w przyszłości. Raporty cykliczne generowane być powinny w rygorze miesięcznym, w ciągu 10 dni od zamknięcia danego miesiąca kalendarzowego. Raporty okazjonalne, związane z detekcją incydentów i zdarzeń bezpieczeństwa, dostarczane być powinny w rygorze 14 dni od ich obserwacji.

Obowiązkiem Wykonawcy będzie przygotowanie wkładu merytorycznego do ewentualnych raportów i zgłoszeń incydentów, wymaganych od Zamawiającego w myśl obowiązujących regulacji prawnych, po ówczesnym wezwaniu.

W celu realizacji niniejszego zamówienia Wykonawca spełnić musi następujące, minimalne, wymogi funkcjonalno-użytkowe:

1. Parametry techniczne stosowanego rozwiązania klasy SIEM.

Stosowany system musi zostać ulokowany w infrastrukturze własnej Wykonawcy, za wyjątkiem elementów funkcyjnych wymienionych w ramach wytycznych dotyczących realizacji etapu 1. Niedopuszczalnym kategorycznie jest eksport informacji poza zasoby pozostające pod całkowitą, ciągłą i wyłączną kontrolą Zamawiającego lub Wykonawcy, w szczególności przetwarzanie w chmurze operatora stanowiącego stronę trzecią. Niedopuszczalnym jest eksport informacji poza terytorium Rzeczypospolitej Polskiej. Stosowany system musi być produktem komercyjnym, obecnym na polskim rynku telekomunikacyjnym od co najmniej dwóch lat. Nie może stanowić produktu firmy pozostającej pod bezpośrednią kontrolą obcego mocarstwa. Wykonawca musi posiadać bezpośrednie wsparcie producenta stosowanego rozwiązania, bądź jego certyfikowanego partnera, w całym okresie realizacji umowy. Zastosowane rozwiązanie, oprócz zarządzania informacją bezpieczeństwa, musi umożliwiać analizę obszarów związanych z utrzymaniem ciągłości działania procesów i jako takie wdrożone być powinno w schemacie wysokiej dostępności. Zamawiający dopuści rozwiązanie buforujące pozyskane informacje w przypadku powstania chwilowej przerwy w działaniu systemu, jedynie pod warunkiem iż zostanie ono skutecznie zabezpieczone przed ich utratą. Architektura systemu SIEM musi przewidywać rozdzielenie funkcji związanych z akwizycją danych wejściowych, warstwą analityczną oraz elementami przeznaczonymi do retencji zebranych informacji w sposób umożliwiający umieszczenie wewnątrz infrastruktury Zamawiającego minimalnego zestawu serwerów, przy większości nakładów obliczeniowych realizowanych po stronie Wykonawcy.

System musi pozwalać na:

1.1 pobieranie logów/zdarzeń (w znaczeniu akwizycji informacji, zapisania w bazie systemu, parsowania, normalizacji poprzez nadanie kontekstów znaczeniowych dla poszczególnych fragmentów wiadomości) co najmniej z następujących systemów: Linux/Unix, Windows Server 2012/2016/2019/2022/2025 oraz Windows 7/8.x/10/11, systemy wirtualizacji VMWare ESXi/vCenter;

1.2 pobieranie logów/zdarzeń z urządzeń sieciowych w standardowym formacie syslog, w tym bezproblemowa obsługa zdarzeń dla co najmniej rozwiązań marki: Alcatel-Lucent, Aruba, Fortinet, MikroTik oraz Moxa;

1.3 akwizycję informacji poprzez protokół syslog UDP/TCP oraz/lub przy wykorzystaniu agenta systemowego;

1.4 współpracę z oprogramowaniem klasy EDR marki Bitdefender, posiadanym obecnie przez Zamawiającego;

1.5 współpracę z systemem IDS/IPD będącym integralną częścią rozwiązań bezpieczeństwa sieci marki Fortinet;

1.6 możliwość wzbogacania danych informacjami pochodzącymi z systemów zarządzania tożsamością, w szczególności mechanizmów natywnych dla rozwiązań klasy Microsoft Active Directory;

1.7 współpracę z rozwiązaniami klasy IDS/IPS posiadającymi możliwość analizy postury bezpieczeństwa systemów przemysłowych, funkcjonujących w oparciu o protokoły takie jak CIP i

Modbus, z uwzględnieniem specyfiki rozwiązań stosowanych w bezprzerwowych systemach przemysłowych.

2. Wymogi dotyczące połączenia sieci Zamawiający – Wykonawca.

W celu skutecznego i bezpiecznego przekazywania informacji niezbędnych do realizacji przedmiotu niniejszego zamówienia, Zamawiający wymaga uruchomienia bezpośredniego, dedykowanego połączenia pomiędzy własnym brzegowym urządzeniem bezpieczeństwa sieci i infrastrukturą wewnętrzną Wykonawcy. Połączenie powyższe nie może wykorzystywać zasobów publicznej sieci Internet i musi stanowić dedykowaną linię prywatną, odseparowaną logicznie od ruchu sieciowego służącego innym celom. Dopuszcza się rozwiązania oparte o ciemne włókno światłowodowe, tunel MPLS VPN, lub dedykowaną podsieć VLAN, przy czym żadne z powyższych rozwiązań nie może jednocześnie przetwarzać ruchu sieciowego nie związanego z realizacją przedmiotu niniejszego zamówienia. Zadaniem Wykonawcy będzie uruchomienie przyłącza w kierunku brzegowych urządzeń bezpieczeństwa sieci Zamawiającego, pracujących w trybie HA, w sposób zapewniający jego redundancję. Oczekiwaną przepływność połączenia określa się jako 1 Gbps Ethernet. Całość infrastruktury łączącej strony musi znajdować się pod ich bezpośrednią kontrolą – nie dopuszcza się wykorzystania połączeń dzierżawionych od strony trzeciej, nie objętej umową zachowania poufności, stanowiącą załącznik do niniejszego zamówienia. Przedmiotowe przyłącze nie może stanowić ryzyka ingresu dla ruchu sieciowego pochodzącego spoza infrastruktury własnej Wykonawcy i powinno prowadzić wyłącznie w kierunku stref bezpieczeństwa związanych bezpośrednio z elementami wdrożonego systemu nadzoru bezpieczeństwa informacji.

3. Dostępność i sposób komunikacji z Wykonawcą.

Wykonawca zobowiązany będzie udostępnić Zamawiającemu numer infolinii, objęty dyżurem całodobowym. Wykonawca udostępni Zamawiającemu kanał komunikacji z własnym dyżurem technicznym, na wypadek wykrycia incydentu wymagającego natychmiastowej reakcji. W związku ze szczególnym charakterem instytucji Zamawiającego, prace prowadzone są w systemie całodobowym, 7 dni w tygodniu, przy czym elementy nie wymagające reakcji natychmiastowej, takie jak sporządzanie raportów, analiza wsteczna danych historycznych, oraz wprowadzanie poprawek związanych ze zwiększeniem poziomu bezpieczeństwa infrastruktury, realizowane będą w godzinach urzędowych standardowego tygodnia pracy. Działania związane z koniecznością zaangażowania Zespołów w godzinach nocnych ograniczyć należy do niezbędnego minimum, związanego z utrzymaniem właściwego poziomu bezpieczeństwa systemów. W przypadku zdarzeń nie stwarzających bezpośredniego, natychmiastowego zagrożenia, dopuszczalną formą jest ich obsługa przez systemy zautomatyzowane, generujące informacje w formie elektronicznej, przy weryfikacji eksperta odłożonej w czasie do chwili rozpoczęcia kolejnego dnia roboczego. Za punkt demarkacji odpowiedzialności Wykonawcy uważa się skuteczne powiadomienie personelu technicznego Zamawiającego o zaistniałym incydencie – Wykonawcy nie powierza się możliwości samodzielnego wprowadzania zmian w produkcyjnej infrastrukturze Zamawiającego. Wymaga się jedynie pełnej współpracy z personelem technicznym Zamawiającego, w tym doradztwa związanego z najskuteczniejszym w danej sytuacji sposobem postępowania.

Czasy obsługi związane z realizację zamówienia definiuje się następująco:

- dla incydentów krytycznych (powodujących możliwość przerwy w pracy systemów produkcyjnych, utraty lub modyfikacji danych, wystąpienia kar umownych lub administracyjnych, lub wystąpienia wymiernych strat wizerunkowych): do 1h. minimalny czas reakcji, 24h. maksymalny czas obsługi

incydentu po stronie SOC, 1h. maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego. Przy czym dla zdarzeń kategorii krytycznej ustalić należy bezwzględnie, obustronnie, procedurę eskalacji, w przypadku w którym próby powiadomienia personelu technicznego Zamawiającego przy wykorzystaniu ustalonych kanałów komunikacji okażą się nieskuteczne;

- dla zdarzeń lub incydentów istotnych, niekrytycznych (powodujących możliwość degradacji pracy systemów produkcyjnych, nie posiadającej istotnego wpływu na praktyczny wynik ich funkcjonowania, degradacji bezpieczeństwa systemów potencjalnie otwierającej nowe luki, lub możliwości powstania niewymiernych strat wizerunkowych, takich jak niekorzystne postanowienia audytu lub kontroli wewnętrznej): do 4h. minimalny czas reakcji, 48h. maksymalny czas obsługi incydentu po stronie SOC, 1h. maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego;
- dla zdarzeń o niskim poziomie istotności (nie powodujących degradacji systemów produkcyjnych ani powstania nowych luk bezpieczeństwa): do 48h. minimalny czas reakcji, 120h. maksymalny czas obsługi incydentu po stronie SOC, kontakt z personelem technicznym Zamawiającego w rygorze next-business-day (w trakcie kolejnego, licząc od daty wykrycia zdarzenia, dnia roboczego).

4. Instruktaż stanowiskowy i wsparcie przy rekonfiguracji systemów.

Obowiązkiem Wykonawcy będzie dostarczenie wytycznych związanych z rekonfiguracją systemów Zamawiającego, w celu ich właściwej integracji z usługami SOC. W związku z powyższym przeprowadzi również podstawowe szkolenie i instruktaż stanowiskowy, związany z właściwymi metodami postępowania dla systemów o charakterze powtarzalnym (przykładowo: stacji roboczych pracowników, mogących podlegać wymianie).

W jego wyniku personel techniczny Zamawiającego będzie w stanie prowadzić czynności utrzymaniowe, wynikające z dotychczasowej praktyki, samodzielnie bez ryzyka degradacji bezpieczeństwa.

W przypadku systemów skomplikowanych, o charakterze niepowtarzalnym, obowiązkiem Wykonawcy będzie udzielenie wsparcia technicznego w siedzibie Zamawiającego, na jego bezpośrednie wezwanie. W przypadku systemów eksperckich, obsługiwanych przez podmioty zewnętrzne, niezbędne prace prowadzone będą zdalnie, lub bezpośrednio w siedzibie Zamawiającego. W przypadku konieczności udzielenia wsparcia zdalnego, obowiązkiem Zamawiającego będzie zapewnienie właściwego dostępu do przedmiotowych systemów. Prace związane z koniecznością udzielenia bezpośredniego wsparcia Wykonawcy zaplanowane być muszą z wyprzedzeniem co najmniej 14 dni kalendarzowych, związanym z udostępnieniem przez Zamawiającego opisu technicznego ich planowanego zakresu.

5. Wymagania dotyczące serwisów zewnętrznych i Podwykonawców.

W związku ze skomplikowanym charakterem systemów objętych zamówieniem, w szczególności w obszarze automatyki przemysłowej, Zamawiający dopuści wykorzystanie Podwykonawców zewnętrznych jako wsparcia Wykonawcy, w przypadku konieczności przeprowadzenia rekonfiguracji lub dogłębnej analityki stosowanych rozwiązań, z zastrzeżeniem, iż Podwykonawcy objęci zostać muszą umowami zachowania poufności, podpisanymi trójstronnie przez Zamawiającego i Wykonawcę, oraz kategorycznym obowiązkiem usunięcia wszelkich informacji pozyskanych w związku z udziałem w realizacji zamówienia po zakończeniu świadczonego wsparcia. Podwykonawcą w myśl brzmienia niniejszego punktu może zostać jedynie instytucja z co najmniej ośmioletnim, udokumentowanym, doświadczeniem z zakresu obsługi i wdrożenia systemów telekomunikacyjnych w przemysłowych środowiskach OT, posiadająca certyfikację ISO/IEC 27001

z zakresu zarządzania bezpieczeństwem informacji i stosująca, w sposób udokumentowany i podlegający weryfikacji System Zarządzania Bezpieczeństwem Informacji, lub obejmujący go Zintegrowany System Zarządzania. Podwykonawca musi być instytucją działającą głównie na rynku polskim, skutecznie rozliczalną względem polskiego stanu legislacyjnego.

6. Wymagania dotyczące doświadczenia Wykonawcy:

Newralgiczny charakter działalności prowadzonej przez Zamawiającego, w połączeniu z jej bezpośrednim wpływem na dobro i bezpieczeństwo mieszkańców miasta Gliwice wymaga zachowania najwyższej staranności przy realizacji przedmiotu niniejszego zamówienia. W związku z powyższym Wykonawca musi kategorycznie posiadać aktualną certyfikację normy ISO/IEC 27001 z zakresu zarządzania ryzykiem związanym z bezpieczeństwem informacji, oraz normy ISO/IEC 22301 z zakresu zachowania ciągłości działania procesów. Kategorycznym obowiązkiem Wykonawcy jest utrzymanie certyfikacji powyższych norm w całym okresie realizacji umowy, oraz wdrożenie i stosowanie, w sposób udokumentowany, podlegający weryfikacji, Zintegrowanego Systemu Zarządzania, obejmującego zakresem zapisy obydwu cytowanych norm i całość instytucji Wykonawcy. Wykonawca musi być instytucją obecną na rynku polskim od co najmniej dziesięciu lat i posiadać udokumentowane doświadczenie w realizacji projektów na potrzeby Administracji Publicznej. Wymagane jest dostarczenie referencji wystawionych przez organ Administracji Publicznej Rzeczypospolitej Polskiej, w randze co najmniej Jednostki Samorządu Terytorialnego, potwierdzających rzetelność realizacji projektów z zakresu bezpieczeństwa teleinformatycznego.

7. Wymagania kompetencyjne:

Zadanie w całości realizować powinni pracownicy etatowi Wykonawcy, zatrudnieni na podstawie stałej umowy o pracę i zobowiązani do zachowania poufności informacji przez pracodawcę. Jedynym wyjątkiem od cytowanej zasady mogą być przypadki wykorzystania usług podwykonawców, wymienionych w pkt. 5.

Zamawiający wymaga, by wśród personelu pozostającego do dyspozycji Wykonawcy i związanego z nim bezpośrednią umową znajdowali się co najmniej:

7.1. Jeden ekspert z zakresu konfiguracji, obsługi i bezpieczeństwa sieci komputerowych, korporacyjnych i Operatorskich, posiadający certyfikację na poziomie Professional jednego z powszechnie obecnych na rynku producentów sprzętu sieciowego (CCNP, HCIP, JNCIP lub odpowiednik);
7.2. Dwóch inżynierów z zakresu konfiguracji, obsługi i bezpieczeństwa sieci komputerowych klasy campus, posiadający certyfikację na poziomie Associate jednego z powszechnie obecnych na rynku producentów sprzętu sieciowego (CCNA, HCIA, JNCI lub odpowiednik);
7.3. Jeden audytor wiodący normy ISO/IEC 27001;
7.4. Jeden inżynier bezpieczeństwa posiadający certyfikację z zakresu konfiguracji i obsługi urządzeń bezpieczeństwa sieci wydaną przez producenta sprzętu powszechnie obecnego na rynku polskim;
7.5. Co najmniej trzech techników posiadających pisemne potwierdzenie kompetencji związanych z obsługą wdrożonego i użytkowanego, na potrzeby niniejszego zamówienia rozwiązania klasy SIEM, wydane przez producenta cytowanego rozwiązania lub jego certyfikowanego partnera;
7.6. Jeden technik posiadający pisemne potwierdzenie kompetencji związanych z obsługą rozwiązań telefonii VoIP klasy Operatorskiej, producenta rozwiązań obecnego na rynku polskim od co najmniej ośmiu lat;

7.7. Zasoby po stronie Wykonawcy legitymujące się certyfikacją Attested Cybersecurity Expert – Cyber Resilience Leadership lub równoważne;

W związku z koniecznością zachowania odpowiedniego poziomu merytorycznego w ramach realizacji niniejszego zadania, od Wykonawcy wymaga się, dodatkowo, udokumentowanego doświadczenia z zakresu prowadzenia audytów bezpieczeństwa informacji na potrzeby podmiotów Administracji Publicznej.

WARUNKI MERYTORYCZNE PRZEDMIOTU ZAMÓWIENIA:

1. Przedmiot i zakres zamówienia.

Przedmiotem zamówienia jest świadczenie usługi Security Operations Center. Zakres zamówienia obejmuje następujące główne obszary działania:

1.1. przygotowanie infrastruktury niezbędnej do świadczenia Usługi SOC w środowisku Zamawiającego oraz opracowanie projektu wdrożenia;
1.2. podłączenie infrastruktury Zamawiającego do usługi SOC Wykonawcy;
1.3. przekazanie przez Wykonawcę procedur komunikacji dotyczących postępowania w przypadku wykrycia incydentów lub zdarzeń bezpieczeństwa w infrastrukturze Zamawiającego;
1.4. świadczenie nadzoru nad bezpieczeństwem infrastruktury Zamawiającego w ramach usługi SOC.

2. Opis głównych obszarów działania Wykonawcy w ramach realizacji zamówienia.

2.1. Przygotowanie infrastruktury niezbędnej do świadczenia Usługi SOC w środowisku Zamawiającego;
2.2. Wykonanie analizy infrastruktury Zamawiającego pod kątem dostępnych w infrastrukturze Zamawiającego rozwiązań technologicznych;
2.3. W przypadku wymagania przez Wykonawcę rozwiązań technologicznych niedostępnych w infrastrukturze Zamawiającego Wykonawca powinien dostarczyć odpowiedni system pokrywając koszty licencji;
2.4. Przedstawienie przez Wykonawcę projektu lub koncepcji monitorowania cyberbezpieczeństwa dla systemów Zamawiającego; projekt musi uwzględniać aktualną infrastrukturę Zamawiającego, w tym:
  2.4.1. urządzenia sieciowe,
  2.4.2. urządzenia automatyki przemysłowej,
  2.4.3. infrastruktura komputerowa,
  2.4.4. infrastruktura serwerowa;
2.5. Podłączenie infrastruktury Zamawiającego do usługi SOC Wykonawcy w zakresie zasobów nie mniejszym niż użycie centralnego systemu monitorowania Security Information and Event Management (SIEM) z istniejącym systemem kolekcji logów Zamawiającego;
2.6. Uruchomienie Usługi SOC;
2.7. Zamawiający wymaga, aby Usługą SOC zostały objęte następujące elementy infrastruktury informatycznej Zamawiającego (minimalne ilości wspierane przez dostarczoną Usługę):
- 160 stacji roboczych,
- 40 serwerów,
- 300 urządzeń automatyki przemysłowej i urządzeń sieciowych w wydzielonych podsieciach OT,
- 50 urządzeń sieciowych wchodzących w skład sieci IT;

Podane ilości są wartościami przybliżonymi.
2.8. Przekazanie przez Wykonawcę procedur działania dotyczących postępowania w przypadku wykrycia incydentów i zdarzeń w infrastrukturze Zamawiającego, w tym:
  2.8.1. Określenie procedur działania/eskalacji dla poszczególnych typów zdarzeń.
  2.8.2. Określenie formy kontaktu dla poszczególnych procedur działania.

2.8.3. Wskazanie osób odpowiedzialnych po stronie Zamawiającego za przyjmowanie informacji oraz rekomendacji o zalecanych do wykonania czynnościach niezbędnych dla mitygacji zauważonych nieprawidłowości.

2.9. Świadczenie nadzoru nad bezpieczeństwem infrastruktury Zamawiającego w ramach usługi SOC poprzez prowadzenie następujących działań:

2.9.1. bieżący monitoring zdarzeń oraz weryfikacja zdarzeń pod kątem nieuzasadnionych alertów (False positives),

2.9.2. informowanie Zamawiającego o każdym wykrytym incydencie według harmonogramu raportowania określonego na etapie wdrożenia usługi,

2.9.3. informowanie Zamawiającego o wystąpieniu incydentu lub zdarzenia, z uwzględnieniem ustalonej na etapie wdrożenia usługi klasyfikacji incydentów i zdarzeń oraz zgodnie z ustalonymi z Zamawiającym ścieżkami eskalacji,

2.9.4. przesyłanie na żądanie Zamawiającego (w ustalonym trybie) raportów dla każdego przeanalizowanego zdarzenia i alertu,

2.9.5. integracji Usługi SOC z nowymi elementami istniejących narzędzi, systemów, technologii Zamawiającego w czasie trwania umowy,

2.9.6. podłączenie do usługi nowych narzędzi, systemów, technologii Zamawiającego w czasie trwania umowy będzie realizowane w ramach dodatkowo wycenianych zleceń,

2.9.7. monitoring zagrożeń mogących dotyczyć infrastruktury Zamawiającego w oparciu o ogólnodostępne zasoby np. serwisy informacyjne CSIRT;

2.10. Czasy obsługi związane z realizację zamówienia definiuje się następująco:

- dla incydentów krytycznych: do 1h. minimalny czas reakcji, 24h maksymalny czas obsługi incydentu po stronie SOC, 1h maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego,
- dla zdarzeń lub incydentów istotnych niekrytycznych: do 4h minimalny czas reakcji, 48h maksymalny czas obsługi incydentu po stronie SOC, 1h maksymalny czas wykonania trzech kolejnych prób powiadomienia personelu technicznego Zamawiającego,
- dla zdarzeń o niskim poziomie istotności: do 48h minimalny czas reakcji, 120h maksymalny czas obsługi incydentu po stronie SOC, kontakt z personelem technicznym Zamawiającego w rygorze next-business-day (w trakcie kolejnego, licząc od daty wykrycia zdarzenia, dnia roboczego).

3. Opis wymagań monitorowania zakresu IT.

Zakresem monitorowania obejmowana jest wskazana infrastruktura IT Zamawiającego, w tym serwery, stacje robocze, urządzenia sieciowe, aplikacje oraz usługi, telefonia VoIP. Uwzględnione powinny być także zasoby zarządzane lub obsługiwane przez firmy zewnętrzne.

W przypadku współpracy z podmiotami zewnętrznymi, wymagane jest uzyskanie deklaracji współpracy od obecnego i nowego Wykonawcy oraz określenie zasad wymiany informacji o incydentach.

4. Opis wymagań dla monitorowania zakresu OT.

W związku z koniecznością objęcia zakresem monitorowania infrastruktury OT, należy uwzględnić specyficzne wymagania związane z jej funkcjonowaniem i bezpieczeństwem. Monitoring powinien obejmować systemy sterowania przemysłowego (ICS), systemy SCADA, sensory IoT oraz powiązane z nimi sieci i protokoły komunikacyjne. Wymagane jest dostosowanie polityk zabezpieczeń i detekcji incydentów do realiów OT. W związku ze szczególnym charakterem wymienionych systemów, dopuszcza się możliwość

wykorzystania usług eksperckich Podwykonawców, z zastrzeżeniami wymienionymi w części opisowej zamówienia.

Wykonawca zobowiązuje się dostarczyć oraz skonfigurować do 20 sztuk sond systemów przemysłowych, docelowo umieszczonych w oddzielnych szafach dystrybucyjnych infrastruktury OT, w celu monitorowania ruchu sieciowego oraz systemowego specjalistycznych systemów przemysłowych wraz z dostarczeniem i wdrożeniem systemu przeznaczonego do normalizacji i parsowania danych przemysłowych OT (Radiflow) z niezbędną ilością licencji, w celu prawidłowego parsowania, normalizacji oraz korelacji danych zebranych z sond systemów przemysłowych. Aby możliwy był do zrealizowania powyższy zakres, Zamawiający zapewnia wymagane zasoby sprzętowe dla wdrażanego systemu.

5. Wymagania ilościowe dotyczące realizacji usługi monitorowania w ramach SOC.

Źródła zdarzeń: (zweryfikować ilości systemy operacyjne Windows/Linux itp.)

5.1. Stacje robocze w obszarze IT – System powinien umożliwiać monitorowanie minimum 160 stacji roboczych z obszaru IT;

5.2. Serwery – System powinien umożliwiać monitorowanie minimum 40 serwerów;

5.3. Infrastruktura sieciowa – System powinien umożliwiać monitorowanie minimum 50 aktywnych urządzeń sieciowych w obszarze IT / oraz minimum 300 aktywnych urządzeń sieciowych w obszarze OT;

5.4. Sondy przemysłowe – do 20 sztuk sond zbierających ruch z przemysłowej części infrastruktury OT;

5.5. Kolektor danych OT – system umożliwiający normalizację, korelację oraz parsowanie danych zebranych z sond przemysłowych (Radiflow).

6. Opis połączenia sieci Zamawiający – Wykonawca.

Wymagane jest fizyczne połączenie sieci Zamawiającego z Wykonawcą, w tym doprowadzenie połączenia światłowodowego do lokalizacji Zamawiającego lub wykorzystanie bezpiecznego tunelu MPLS VPN zgodnego z dobrymi praktykami sztuki cyberbezpieczeństwa. Połączenie powinno zapewniać niskie opóźnienia i wysoką niezawodność transmisji danych. Musi zostać kategorycznie odseparowane od zasobów publicznych sieci Internet i stanowić musi dedykowaną linię, przeznaczoną wyłącznie do świadczenia usług związanych z niniejszym zamówieniem. Nie dopuszcza się połączenia realizowanego w formie szyfrowanego tunelu wykorzystującego zasoby publicznej sieci Internet. Nie dopuszcza się przesyłu informacji przy wykorzystaniu infrastruktury podmiotu trzeciego, nie objętego zakresem umowy powierzenia informacji, związanej z realizacją niniejszego zamówienia.

Zestawienie, zabezpieczenie i obsługa połączenia w relacji Zamawiający do SOC poprzez uruchomienie łącza transmisji danych o minimalnej przepustowości 1/1 Gbps.

7. Opis dostępności i sposób komunikacji z Wykonawcą, czasy i terminy.

7.1. Wykonawca zobowiązuje się do zapewnienia telefonu serwisowego oraz możliwości zgłaszania incydentów w formule 24/7/365 poprzez panel zgłoszeń serwisowych;

7.2. Zamawiający określa następujące czasy reakcji na incydent według klasyfikacji incydentu:

- krytyczne - do 1 godziny,
- istotne niekrytyczne - do 4 godzin,
- niskie - do 48 godzin;

7.3. SLA o notyfikacji – do 60 min. od zidentyfikowania incydentu;

7.4. Wykonawca zobowiązuje się przygotować narzędzie SIEM w sposób umożliwiający sporządzanie wymaganych raportów zgodnie z określonym przez Zamawiającego harmonogramem - miesięczne, kwartalne, roczne;
7.5. Wykonawca zobowiązuje się do przestrzegania czasów reakcji na incydenty według zasad klasyfikacji uzgodnionych obustronnie z Zamawiającym, oraz powiadomienie o jego wystąpieniu bezzwłocznie po jego wykryciu;
7.6. Klasyfikacja (poziomy) incydentów uzgadniane będą w ramach wdrożenia i opracowywania procedury monitorowania i reagowania;
7.7. Kanały komunikacji obejmujące notyfikację: e-mail i kontakt telefoniczny;
7.8. Raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa (Dz.U. z 2018 r. poz. 1560) do wskazanego CSIRT do 24h.

8. Potrzeby szkoleniowe.

8.1. Wsparcie w konfiguracji sieci wewnętrznej Zamawiającego, w celu dostosowania do wymogów systemu SIEM;
8.2. Wsparcie w konfiguracji urządzeń końcowych i infrastruktury serwerowej Zamawiającego w celu dostosowania do wymogów systemu SIEM;
8.3. Możliwość przeprowadzenia szkolenia z zakresu cyberhigieny dla wszystkich pracowników Zamawiającego;
8.4. Szkolenie dotyczące właściwych metod postępowania w przypadku zmian powtarzalnych, pozwalające personelowi technicznemu Zamawiającego na samodzielne prowadzenie utrzymania infrastruktury bez ryzyka degradacji skuteczności wdrożonego rozwiązania.

9. Warunki wsparcia trzeciej strony - podwykonawcy dla zakresu IT/OT.

9.1. Wymagania dotyczące doświadczenia i certyfikacji podwykonawcy – ISO/IEC 27001, stosowanie SZBI lub ZSZ;
9.2. Gwarancja zgodności działań z politykami cyberbezpieczeństwa Zamawiającego oraz Wykonawcy, pełna rozliczalność względem polskiego stanu legislacyjnego;
9.3. Objęcie umową zachowania poufności i obowiązkiem zniszczenia pozyskanych informacji po zakończeniu okresu wsparcia.

10. Doświadczenie i kompetencje Wykonawcy.

10.1. Realizacja projektów cyberbezpieczeństwa dla instytucji publicznych;
10.2. Udokumentowane kompetencje w zakresie SOC, SIEM, analizy zagrożeń;
10.3. Doświadczenie w prowadzeniu audytów bezpieczeństwa informacji;
10.4. Udokumentowane kompetencje twarde związane z obsługą infrastruktury sieciowej, telefonii VoIP oraz infrastruktury serwerowej;
10.5. Potwierdzone minimum 3letnie doświadczenie w zakresie monitorowania i zarządzania infrastrukturą teleinformatyczną Jednostek z obszaru Administracji Publicznej;
10.6. Kompetencje w zakresie zarządzania środowiskiem Data Center.

11. Wymagane certyfikacje personelu i instytucji Wykonawcy.

Zadanie w całości realizować powinni pracownicy etatowi Wykonawcy, zatrudnieni na podstawie stałej umowy o pracę i zobowiązani do zachowania poufności informacji przez pracodawcę. Jedynym wyjątkiem od

cytowanej zasady mogą być przypadki wykorzystania usług podwykonawców, wymienionych w pkt. 5. Zamawiający wymaga, by wśród personelu pozostającego do dyspozycji Wykonawcy i związanego z nim bezpośrednią umową znajdowali się co najmniej:

- certyfikaty ISO/IEC 27001, ISO/IEC 22301,
- osobowe certyfikacje dotyczące kompetencji z zakresu obsługi sieci na poziomie Associate oraz Professional,
- osobowe certyfikacje z zakresu konfiguracji i obsługi urządzeń bezpieczeństwa sieci na poziomie Associate oraz Professional,
- osobowe certyfikacje dotyczące kompetencji z zakresu administracji systemami informatycznymi i infrastrukturą Data Center (do dodania nazwy certyfikatów),
- osobowe certyfikacje z zakresu obsługi rozwiązań telefonii VoIP,
- osobowe certyfikacje związane z prowadzeniem audytów bezpieczeństwa informacji,
- certyfikaty potwierdzające znajomość narzędzi SIEM stosowanych do realizacji niniejszego zamówienia,
- certyfikat potwierdzający kompetencje z zakresu zarządzania podmiotami Krajowego Systemu Cyberbezpieczeństwa.

12. Wymogi dotyczące profilu działalności Wykonawcy.

12.1. Udokumentowane doświadczenie we współpracy z jednostkami administracji publicznej;
12.2. Udokumentowana realizacja projektów z zakresu cyberbezpieczeństwa dla sektora publicznego;
12.3. Dogłębna znajomość specyfiki funkcjonowania spółek miejskich i administracji publicznej.

13. Warunki formalne.

13.1. Posiadanie certyfikatu na zgodność działań z normą PN-EN ISO/IEC 27001 System zarządzania bezpieczeństwem informacji przez cały okres obowiązywania umowy;
13.2. Wykonywanie usługi SOC, o której jest mowa w OPZ zgodnie z wymaganiami Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa w zakresie wsparcia Operatorów Usług Kluczowych, rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
13.3. Podejmowanie działań i procesów operacyjnych zgodnie z wymogami norm PN-EN ISO/IEC 27001 lub równoważne, PN-EN ISO 22301 lub równoważne;
13.4. Posiadanie ubezpieczenia OC w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną min. 1.000.000,00 zł przez cały okres obowiązywania umowy.

14. Dodatkowe oczekiwania Zamawiającego.

14.1. Opracowanie procedur reagowania na incydenty, klasyfikacji zdarzeń, oraz eskalacji incydentów krytycznych;

14.2. Pełna zgodność z ogólnie przyjętymi dobrymi praktykami sztuki telekomunikacyjnej z zakresu bezpieczeństwa informacji.

15. Usługa będzie zawierała:

15.1. monitorowanie bezpieczeństwa w ramach SOC w trybie ciągłym: 24/7/365;
15.2. środowisko, na którym realizowana jest usługa SOC oraz SIEM będzie uruchomione na dedykowanym środowisku wysokiej dostępności HA w profesjonalnym Data Center, które jest własnością dostawcy usługi i znajduje się na terenie Polski;
15.3. zestawienie, zabezpieczenie i obsługa połącznia w relacji Zamawiający do SOC poprzez uruchomienie łącza transmisji danych o minimalnej przepustowości 1/1 Gbps;
15.4. realizowanie zadań w ramach 1 linii wsparcia SOC, a w szczególności:
15.4.1. reagowanie na podejrzenia i obsługa zidentyfikowanych incydentów,
15.4.2. analiza incydentów i ich klasyfikowanie,
15.4.3. zarządzanie incydentami;
15.5. składowanie logów i dostęp w ramach zasobów dostawcy usługi, zlokalizowane w Polsce, w trybie wysokiej dostępności HA. Okres przechowania – minimum 6 miesięcy;
15.6. przedstawienie analizy przedwdrożeniowej i harmonogramu realizacji;
15.7. przekazanie dokumentacji powykonawczej;
15.8. uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 90 dni od zawarcia umowy;
15.9. zapewnienie wsparcia grupy projektowej i dedykowanego kierownika projektu;
15.10. niezbędne licencje na uruchomienie systemu bezpieczeństwa.

16. Integracja z istniejącymi systemami.

16.1. Graylog.
16.1.1. Zamawiający wymaga w ramach realizacji usługi SOC integracji z istniejącym w infrastrukturze zamawiającego systemem kolekcji logów/zdarzeń, opartego o rozwiązanie Graylog. Integracja musi uwzględniać możliwość logicznego nacechowania strumieni danych z poszczególnych źródeł infrastruktury teleinformatycznej zamawiającego;
16.2. EDR/XDR.
16.2.1. Zamawiający wymaga w ramach realizacji usługi SOC integracji z istniejącym rozwiązaniem EDR/XDR poprzez kolekcję logów z konsoli zarządzania oprogramowaniem Bitdefender GravityZone;
16.3. Kolektor danych na miejscu.
16.3.1. Dostarczone rozwiązanie powinno umożliwiać kolekcję danych z wykorzystaniem wielu interfejsów sieciowych, zarówno dla infrastruktury IT jak i OT.

17. Analiza przedwdrożeniowa.

W ramach analizy przedwdrożeniowej dostawca usługi przeprowadzi:

17.1. analizę źródeł logów oraz określi sposób ich parsowania w ramach usługi,
17.2. analizę potrzebnych i dostępnych informacji do strojenia wdrażanej usługi (np. adresacje, DMZ, serwery DNS, AD, proxy itd.),

17.3. wstępne określenie sposobu reagowania na poszczególne podejrzenia incydentów;

18. Analiza na etapie wdrożenia.

W ramach podłączenia źródła logów dostawca usługi:

18.1. uruchomi przesyłanie zdarzeń do wdrażanej usługi,
18.2. przygotuje sposób podłączania źródła i przekaże go do Zamawiającego w celu realizacji pozostałych zasobów z tego samego typu,
18.3. dostawca usługi przeprowadzi wstępne strojenie i implementację reguł, a rezultatem tych prac będzie działające parsowanie logów oraz zaimplementowane uzgodnione reguły,
18.4. dostawca usługi dostarczy opis sposobu obsługi każdej z procedur,
18.5. dostawca usługi zbuduje raporty wg. wytycznych Zamawiającego, generowane automatycznie i wysyłane mailowo do wskazanych osób,
18.6. dostawca usługi przeprowadzi strojenie wdrażanej usługi w celu zmniejszenia ilości fałszywych alarmów;

19. Wsparcie 2 linii SOC.

Dostawca usługi zapewni dostęp do usług specjalistycznych 2 linii wsparcia SOC, które realizowane będą dodatkowym zamówieniem, uwzględniając: analizę malware, analizę powłamaniową, informatykę śledczą.

Zadania realizowane w ramach 2 linii wsparcia SOC:

- obsługa incydentów przekazanych z 1 linii w szczególności incydentów krytycznych,
- troubleshooting,
- strojenie systemów,
- tworzenie reguł,
- pisanie scenariuszy,
- kontakt z dostawcą - zgłaszanie znalezionych błędów i zakładania ticket'ów,
- pisanie polityk bezpieczeństwa.

20. Szczegółowe wymogi funkcjonalne dla wdrożonej usługi SOC as a Service:

20.1. Aplikacja typu agent wdrożonego rozwiązania, w wersji przeznaczonej dla systemów rodziny Microsoft Windows, (Windows Agent) musi posiadać możliwości zbierania danych nie mniejsze od istniejących w przypadku obserwacji systemu bez wykorzystania aplikacji typu agent, przy czym wymaga się by komunikacja pomiędzy procesem agenta i centralną częścią systemu odbywała się w sposób bezpieczny, gwarantujący poufność przesyłanych informacji.
20.2. Aplikacja typu agent wdrożonego rozwiązania, w wersji przeznaczonej dla systemów rodziny Linux (Linux Agent), musi posiadać możliwości zbierania danych nie mniejsze od istniejących w przypadku obserwacji systemu bez wykorzystania aplikacji typu agent, wykrywania nieaktualnego oprogramowania oraz podatności (CVE) przy czym wymaga się dodatkowo możliwości akwizycji logów binarnych dziennika systemd, oraz zagwarantowania by komunikacja pomiędzy procesem agenta i centralną częścią systemu odbywała się w sposób bezpieczny, zapewniających poufność przesyłanych informacji.

20.3. Usługa musi zapewniać wsparcie dla systemu nadzoru monitorującego urządzenia sieciowe Zamawiającego, z uwzględnieniem prawidłowego parsowania, normalizacji oraz korelacji danych zawartych w systemie.

20.4. Usługa musi zapewniać wsparcie dla systemu nadzoru typu syslog monitorującego całość infrastruktury Zamawiającego, z uwzględnieniem prawidłowego parsowania, normalizacji oraz korelacji danych zawartych w systemie.

20.5. Aplikacja typu agent wdrożonego rozwiązania, w wersji przeznaczonej dla systemów przemysłowych OT, posiadająca możliwości monitorowania zasobów, wykrywania nieaktualnego oprogramowania oraz podatności (CVE), statystyk oraz zbierania danych nie mniejsze od istniejących w przypadku obserwacji systemu bez wykorzystania aplikacji typu agent,

20.6. Usługa musi pozwolić na integrację z systemami uzupełniającymi, obecnie użytkowanymi przez Zamawiającego, co najmniej w zakresie pozyskania generowanych przez nie zdarzeń, przy czym do systemów tych należą: Graylog, BitDefender GravityZone oraz Zabbix.

20.7. Usługa powinna umożliwiać wykorzystanie danych pochodzących z systemu BitDefender przy użyciu dostępnych mechanizmów eksportu danych w szczególności poprzez Syslog.

20.8. Zamawiający wymaga, by usługa posiadała możliwość akwizycji, parsowania i normalizacji wiadomości syslog pochodzących z przełączników sieciowych marki Alcatel-Lucent, Aruba, Moxa oraz urządzeń bezpieczeństwa sieci marki Fortinet Fortigate.