ROZDZIAŁ III SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Świadczenie kompleksowych usług z zakresu cyberbezpieczeństwa (SOC)

1. Definicje

1.1. **Zdarzenia:** Dane i informacje, których źródłem są systemy bezpieczeństwa, prezentowane w formie charakterystycznej dla tych systemów. Na przykład: uruchomienie procesu, modyfikacja rejestru, nawiązanie połączenia sieciowego, zapytanie DNS.

1.2. **Alert / wskaźnik incydentu:** Zdarzenia, których źródłem są systemy bezpieczeństwa lub zgłoszenie użytkowników, których cechy (priorytet, opis, źródło, zasób) świadczą o możliwości wystąpieniu incydentu. Na przykład: alert systemu EDR/NDR o wysokim priorytecie, którego opis oraz artefakty wskazują na wystąpieniu incydentu bezpieczeństwa.

1.3. **Incydent (cyber)bezpieczeństwa:** Zdarzenia i alerty w systemach bezpieczeństwa, które świadczą o wystąpieniu okoliczności stanowiących zagrożenie dla systemów organizacji, danych przetwarzanych w tych systemach oraz stanowiących naruszenie polityk bezpieczeństwa. Na przykład: infekcja złośliwym oprogramowaniem umożliwiającym wykradanie poufnych danych, infekcja złośliwym oprogramowaniem typu ransomware, przełamanie bezpieczeństwa aplikacji i systemów z wykorzystaniem podatności, nieuprawniony dostęp do zasobów informatycznych, niezgodne z politykami bezpieczeństwa wykorzystanie zasobów informatycznych.

1.4. **Artefakt:** Dane określające techniczne i behawioralne cechy zdarzeń, alertów i incydentów. Na przykład: suma kontrolna pliku (MD5, SHA1, SHA256), nazwa pliku, ścieżka pliku, typ pliku, gałąź i wartość rejestru, adres IP (źródłowy i docelowy), protokół sieciowy, aplikacja sieciowa, port sieciowy, domena, URL, dostęp do zasobu c$.

1.5. **Proces obsługi incydentu:** Wszystkie działania realizowane od wystąpienia wskaźnika incydentu do zakończenia reakcji na incydent. Działania te zwykle obejmują: monitoring systemów, obsługę zgłoszeń, analizę i selekcję zdarzeń i alertów oraz reakcję na incydenty.

1.6. **Analiza i selekcja zdarzeń i alertów:** proces realizowany w ramach procesu obsługi incydentów, którego celem jest ustalenie czy poddawany analizie alert bądź zdarzenie może stanowić o wystąpieniu incydentu bezpieczeństwa.

1.7. **Analiza incydentu:** proces realizowany w ramach procesu obsługi incydentów, którego celem jest określenie: szczegółów technicznych, zakresu, wpływu, priorytetu oraz sposobów reakcji na incydent.

1.8. **Reakcja na incydent:** Proces realizowany w ramach procesu obsługi incydentów, na który składają się: analiza incydentu, powstrzymanie incydentu, zażegnanie zagrożenia, przywrócenie systemów, wyciąganie wniosków, raportowanie.

1.9. **Czas reakcji:** Czas, który upłynął od momentu wystąpienia zdarzenia w systemie bezpieczeństwa, lub odebrania zgłoszenia od użytkownika do momentu podjęcia działań związanych z analizą i selekcją zdarzeń. Na przykład: analizę zdarzenia podjęto po upływie 15 min. od momentu wystąpienia zdarzenia w konsoli systemu EDR. Oczekiwane czasy reakcji

ustalane w zależności od ustalonych priorytetów incydentów mogą stanowić jeden z parametrów usług świadczonych przez zespół Wykonawcy.

1.10. **Pivoting:** Proces wzbogacania listy artefaktów zdarzenia / incydentu o kolejne artefakty na podstawie informacji pozyskanych z dodatkowych źródeł informacji (TI , OSINT, systemów i użytkowników). Na przykład: Adres IP (artefakt nr 1) związany jest z domeną / adresem URL (dodatkowy artefakt), które były wykorzystywane w kampanii związanej ze złośliwym oprogramowaniem. Suma MD5 (dodatkowy artefakt), nazwa pliku (dodatkowy artefakt), ścieżka (dodatkowy artefakt), klucz rejestru (dodatkowy artefakt) to cechy charakterystyczne tego oprogramowania. W trakcie analizy zdarzeń i incydentów analitycy dokonują krzyżowej weryfikacji występowania artefaktów w dostępnych źródłach danych. Rozszerzona lista artefaktów pomaga w potwierdzeniu bądź zaprzeczeniu wystąpienia incydentu bezpieczeństwa w procesie analizy i selekcji zdarzeń. W trakcie analizy incydentów artefakty pomagają w ustaleniu skali, wpływu oraz szczegółów technicznych incydentu.

1.11. **Aktywne poszukiwanie zagrożeń / Threat Hunting**: Proces aktywnego poszukiwania zagrożeń poprzez analizę zdarzeń w ustalonych systemach bezpieczeństwa. W ramach tego procesu analitycy, wykorzystując mechanizmy grupowania, filtrowania i wizualizacji, w połączeniu z wiedzą o zagrożeniach i informacjami z TI, identyfikują aktywności wskazujące na możliwość wystąpienia incydentu.

1.12. **Osoba kontaktowa:** Osoba wskazana do komunikacji w zakresie procesu obsługi incydentów. Rolę osób kontaktowych mogą pełnić: pojedynczy punkt kontaktu (PoC - Point of Contact) w organizacji zamawiającego lub lista kontaktów w relacji do priorytetów incydentów, zasobów, lokalizacji i procesów.

1.13. **Ścieżka eskalacji:** Uzgodnione i sformalizowane zasady komunikacji w zakresie procesu obsługi incydentów, które definiują w szczególności: dostępne kanały komunikacji (np.: email, telefon, SMS, komunikator), kolejność powiadamiania osób kontaktowych, kolejność i sposoby eskalacji w przypadku braku możliwości nawiązania kontaktu lub w przypadku braku reakcji, osoby kontaktowe i dostępne kanały komunikacji w zależności od: zasobu, którego dotyczy incydent, lokalizacji, priorytetu, typu incydentu, czynności w ramach procesu obsługi incydentu.

1.14. **Ustalone systemy bezpieczeństwa:** Systemy bezpieczeństwa dostarczone w ramach usług oraz źródła danych (w tym systemy bezpieczeństwa) udostępnione przez zamawiającego, które SOC wykorzystuje zgodnie z przyznaną autoryzacją i poziomem dostępu w ramach procesu obsługi incydentów.

1.15. **Autoryzacja:** Uzgodniony i sformalizowany zakres działań aktywnych i proaktywnych, które SOC może podjąć w systemach zamawiającego w ramach procesu obsługi incydentów. Autoryzacja może uwzględniać konieczność uzyskania zgody na podjęcie działań od wskazanych osób kontaktowych, zgodnie z przyjętymi ścieżkami eskalacji. Autoryzacja ustala formalne i organizacyjne granice działań podejmowanych przez dostawcę w ramach świadczonych usług.

1.16. **Poziom dostępu:** Uzgodniony i sformalizowany poziom uprawnień , którymi dysponuje SOC w Ustalonych Systemach Bezpieczeństwa, niezbędnych do realizowania zadań obsługi incydentów zgodnie z przyznaną autoryzacją. Poziom dostępu stanowi praktyczną granicę

działań, które może wykonać dostawca w ramach swoich działań związanych ze świadczoną usługą.

1.17. **System obsługi incydentów:** System, w którym pracownicy dostawcy prowadzą rejestr prac wykonywanych w ramach procesu obsługi incydentów. Podstawowym obiektem systemu są zgłoszenia. Zgłoszenia powstają automatycznie lub są zakładane manualnie niezwłocznie po zaobserwowaniu wskaźnika incydentu, powiadomienia od użytkownika lub w wyniku prac aktywnego poszukiwania zagrożeń. Każde zgłoszenie zawiera podstawowe informacje o zdarzeniu: źródło, opis, status, priorytet, typ zdarzenia, czas powstania. W miarę postępu prac informacje te są uzupełniane o dane uzyskane w rezultacie analizy. Każda zmiana w zgłoszeniu jest rejestrowana i opatrzona znacznikiem czasowym oraz nazwą użytkownika.

1.18. **Raport z incydentu:** Podsumowanie informacji dotyczących przebiegu prac w ramach procesu obsługi incydentów. Dodatkowo każdy raport zawiera następujące informacje:

- Analiza – szczegółowy opis prac analitycznych wraz z ich rezultatami.
- Werdykt - ocena wynikająca z analizy (incydent, fałszywy alarm, zdarzenie informacyjne).
- Rekomendacje – zalecenia dalszych działań.
- Podjęte działania – działania wykonane w ramach reakcji na incydent.
- Uwagi.
  Raport stanowi wydruk z systemu obsługi incydentów Wykonawcy i dostarczany jest w formie dokumentu PDF. Zawartość raportu może być dostosowana do potrzeb klienta. Zakres zmian może obejmować dodatkowe pola raportu które będą wypełniane przez analityków podczas obsługi incydentów.

1.19. Mapowanie sieci – realizowany przez zamawiającego proces utrzymywania świadomości sytuacyjnej w zakresie architektury logicznej sieci, lokalizacji, funkcji oraz konfiguracji zabezpieczeń, informacji (adres IP, nazwa, typ, rola, priorytet) na temat zasobów zamawiającego.

Opis wymagań w zakresie realizacji usługi SOC.

W ramach świadczonych usług zamawiający zapewni:

1.20. Przyjmowanie i rejestracja zgłoszeń związanych z incydentami lub podejrzeniami incydentów cyberbezpieczeństwa. Zgłoszenia mogą być dokonywane przez osoby wskazane przez zamawiającego za pośrednictwem ustalonych kanałów komunikacji (e-mail, telefon, komunikator internetowy, interfejs systemu obsługi zgłoszeń). Przyjmowanie zgłoszeń musi być realizowane przez personel dysponujący wiedzą i doświadczeniem w zakresie analizy incydentów cyberbezpieczeństwa.

1.21. Prowadzenie rejestru obejmującego szczegółowe informacje o zgłoszeniach z uwzględnieniem: czasu przyjęcia zgłoszenia, osób odpowiedzialnych za obsługę zgłoszenia, przebiegu i wyników przeprowadzonych analiz, historii podjętych czynności i komunikacji. Informowanie o statusie zgłoszeń zgodnie z przyjętymi ścieżkami eskalacji. Każde zgłoszenie musi być oznaczone unikalnym identyfikatorem, który zostanie przekazany osobie zgłaszającej oraz będzie wykorzystywany w dalszej komunikacji. Rejestr zgłoszeń, wraz ze wszystkimi szczegółami

dotyczącymi zgłoszeń będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do informacji o każdym zgłoszeniu niezwłocznie, na każde żądanie.

1.22. Stały monitoring alertów i zdarzeń, *o priorytecie wskazanym przez zamawiającego (ograniczenie dziennej liczby alertów) / o ustalonym priorytecie (jeśli nie ma ograniczania alertów)*, występujących w ustalonych systemach bezpieczeństwa.

1.23. Prowadzenie rejestru obejmującego szczegółowe informacje o alertach ze szczególnym uwzględnieniem: czasu wystąpienia alertu, osób zaangażowanych w proces obsługi, przebiegu i wyników analizy, historii podjętych czynności i komunikacji. Informowanie o wynikach analizy zgodnie z ustalonymi ścieżkami eskalacji. Każde wystąpienie alertu musi być oznaczone unikalnym identyfikatorem wykorzystywany w dalszej komunikacji. Rejestr zdarzeń, wraz ze wszystkimi szczegółami dotyczącymi alertów będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do informacji o każdym zdarzeniu niezwłocznie, na każde żądanie.

1.24. Analizę zdarzeń i alertów występujących w systemach bezpieczeństwa oraz informacji uzyskanych w wyniku zgłoszeń. Analiza musi uwzględniać co najmniej: wyodrębnianie artefaktów za pośrednictwem ustalonych systemów bezpieczeństwa, uzupełnianie danych i kontekstu zdarzeń z wykorzystaniem źródeł Threat Intelligence, OSINT, informacji w ramach procesu mapowania sieci, informacji uzyskanych od administratorów i użytkowników zgodnie ze ścieżkami eskalacji, pivoting. W przypadku zdarzeń związanych ze złośliwym lub podejrzanym oprogramowaniem działania muszą uwzględniać dynamiczną analizę w środowiskach sandbox oraz, jeśli to konieczne, w środowisku laboratoryjnym w celu ustalenia szczegółów technicznych (IOC), charakteru i potencjalnych skutków uruchomienia tego oprogramowania. W przypadku zdarzeń związanych z podejrzanymi lub złośliwymi domenami adresami IP i URL działania muszą uwzględniać weryfikację tych adresów w źródłach Threat Intelligence oraz, jeśli to konieczne, bezpośrednią weryfikację ich zawartości. Analiza zgromadzonych danych i sekcja zdarzeń pod kątem możliwości wystąpienia incydentów bezpieczeństwa.

1.25. Ustalenie szczegółów technicznych incydentów bezpieczeństwa, ich wpływu na systemy zamawiającego oraz klasyfikacja incydentów zgodnie z *ustalonymi metodami klasyfikacji*. Określenie metod powstrzymania incydentów bezpieczeństwa, działań naprawczych oraz działań, które powinny być podjęte w celu uniknięcia podobnych incydentów w przyszłości.

1.26. Informowanie *zamawiającego* zgodnie z ustalonymi ścieżkami eskalacji o wystąpieniu incydentu lub podejrzeniu wystąpienia incydentu z uwzględnieniem ustalonej klasyfikacji incydentów.

1.27. Informowanie *zamawiającego* na żądanie o postępach prac związanych z analizą incydentów.

1.28. Niezwłoczne informowanie *zamawiającego* zgodnie z ustalonymi ścieżkami eskalacji o ustaleniach dotyczących incydentów ważnych oraz krytycznych jeśli ustalenia te wskazują na istotny wpływ na systemy lub aktywność organizacji.

1.29. Współpraca z osobami wskazanymi przez zamawiającego w ramach obsługi incydentów w zakresie organizacyjnym i technicznym. W szczególności informowanie zamawiającego o rekomendacjach dotyczących działań związanych z powstrzymaniem incydentu, oraz zalecanych środkach naprawczych.

1.30. Podejmowanie działań związanych z reakcją na incydenty zgodnie z ustaloną autoryzacją oraz poziomem dostępu za pośrednictwem ustalonych systemów bezpieczeństwa.

1.31. Dla każdego przeanalizowanego zgłoszenia i alertu, na każde żądanie, niezwłoczne dostarczenie raportu uwzględniającego co najmniej:

- Dokładny czas wystąpienia alertu / przyjęcia zgłoszenia.
- Dokładny czas rozpoczęcia i zakończenia analizy.
- Opis analizy z uwzględnieniem prowadzonych działań.
- Zgromadzone i przeanalizowane artefakty.
- Rezultat analizy i klasyfikację.
- Rekomendację.
- Osoby zaangażowane w analizę.

Zawarte w raporcie rekomendacje, rezultaty analizy i klasyfikacje muszą wynikać z analizy.

1.32. Dla każdego incydentu wykonawca, niezwłocznie i zgodnie z przyjętymi ścieżkami eskalacji dostarczy raport uwzględniający co najmniej:

- Dokładny czas wystąpienia alertu / przyjęcia zgłoszenia.
- Dokładny czas rozpoczęcia i zakończenia analizy.
- Dokładny czas zakwalifikowania alertu jako incydent.
- Opis analizy z uwzględnieniem prowadzonych działań.
- Zgromadzone i przeanalizowane artefakty.
- Rezultat analizy i klasyfikację.
- Listę działań podjętych w ramach reakcji na incydent.
- Rekomendacje. W tym rekomendacje zmian technicznych i organizacyjnych w celu uniknięcia wystąpienia podobnych incydentów w przyszłości.
- Osoby zaangażowane w analizę.

Zawarte w raporcie rekomendacje, rezultaty analizy i klasyfikacje muszą wynikać z analizy.

1.33. *Raz w miesiącu / raz na kwartał* w pierwszym tygodniu kolejnego *miesiąca / kwartału* wykonawca prześle zamawiającemu raport zawierający co najmniej:

- Informacje zbiorcze na temat ilości przeanalizowanych alertów.
- Informacje na temat ilości i priorytetów wykrytych incydentów.
- Zestawienie typów występujących alertów i incydentów.
- Zestawienie priorytetów alertów i incydentów.
- Średni czas reakcji.
- Średni czas obsługi.
- Zestawienie najważniejszych rekomendacji.
- Informacje na temat stanu (wydajności, obciążenia, problemów) ustalonych systemów bezpieczeństwa.

1.34. Przegląd i omówienie procedur, ścieżek eskalacji, konfiguracji systemów, parametrów usługi w ramach kwartalnych spotkań warsztatowych. Spotkania będą odbywały się w siedzibie zamawiającego lub, za zgodą zamawiającego, on-line.

1.35. Koordynacja działań związanych z reakcją na incydent w przypadku konieczności podjęcia działań wymagających zaangażowania osób i zasobów technicznych po stronie *zamawiającego* , po stronie *dostawcy* oraz podmiotów zewnętrznych. Zapewnienie stałego kontaktu do osoby odpowiedzialnej za koordynację działań w całym procesie reakcji na incydent.

1.36. *Realizowanie działań związanych z reakcją na incydenty w siedzibie *zamawiającego* oraz w lokalizacjach wskazanych przez *zamawiającego* gdzie znajdują się systemy *zamawiającego* dotknięte incydentem, zgodnie z *ustalonymi* czasami reakcji, w *zatwierdzonym* zakresie oraz zgodnie z *ustaloną* autoryzacją.*

*1.37. Zabezpieczanie materiałów takich jak: logi, pliki, zrzuty pamięci operacyjnej, obrazy dysku, związanych z incydentem na żądanie *zamawiającego*, w ramach reakcji na incydenty.*

*1.38. Na żądanie *zamawiającego* prowadzenie analiz materiałów związanych z incydentami w celu ustalenia ich przebiegu.*

1.39. Zarządzanie konfiguracją *ustalonych* systemów bezpieczeństwa *zamawiającego* zgodnie z *ustalonym* procesem wprowadzania zmian oraz w ramach *ustalonej* autoryzacji i poziomów dostępów: Przeprowadzanie aktualizacji oprogramowania, wprowadzanie zmian w regułach i mechanizmach wykrywania zagrożeń w celu podniesienia efektywności wykrywania, rozwiązywanie problemów.

1.40. Rekomendowanie zmian w konfiguracji i architekturze systemów bezpieczeństwa *zamawiającego* w celu podnoszenia efektywności ochrony oraz zminimalizowania ilości fałszywych alarmów. Informowanie *zamawiającego* o rekomendacjach niezwłocznie po wystąpieniu okoliczności wskazujących na konieczność zmian. Przekazywanie *zamawiającemu* w ustalonej formie raportów opisujących przedstawione rekomendacje oraz status ich implementacji zgodnie z *ustalonym* harmonogramem.

1.41. Mapowanie sieci w oparciu o informacje przekazane przez zamawiającego oraz uzyskane w ramach procesów analizy zdarzeń i reakcji na incydenty. Utrzymywanie aktualnej bazy wiedzy o zasobach i architekturze sieci zamawiającego na poziomie umożliwiającym określenie roli, typu oraz priorytetu zasobów. Wykorzystanie pozyskanych informacji w procesach analizy zdarzeń i reakcji na incydenty w celu ograniczenia zaangażowania zamawiającego w te procesy.

1.42. Skanowanie podatności zasobów zamawiającego z wykorzystaniem automatycznych narzędzi. Skanowanie zasobów dostępnych z sieci Internet musi być realizowane co najmniej dwa razy w miesiącu. Skanowanie zasobów sieci LAN będzie realizowane raz w miesiącu w zakresie i oknie czasowym wskazanym przez zamawiającego. Informacje na temat wykrytych podatności zostaną przekazane zamawiającemu zgodnie z ustalonymi ścieżkami eskalacji. Podatności krytyczne będą traktowane jak incydenty. Ich obsługa będzie przebiegać zgodnie z procesami stosowanymi w analizie, raportowaniu i reakcji na incydenty. Informacje o podatnościach będą uwzględniane jako dodatkowy kontekst w procesach obsługi incydentów.

1.43. Na żądanie zamawiającego implementacja zamian w konfiguracji *ustalonych* systemów bezpieczeństwa *zamawiającego* oraz w systemach wykorzystywanych przez *dostawcę* w ramach świadczonych usług w celu podniesienia ich efektywności oraz ograniczenia ilości fałszywych alarmów.

1.44. Usługi monitoringu zdarzeń muszą być realizowane co najmniej na podstawie dwóch źródeł danych: informacji o ruchu sieciowym na poziomie szczegółowości dostarczonego systemu NDR, urządzeń bezpieczeństwa (FortiAnalyzer). W ramach analizy procesu obsługi incydentów dla wszystkich zdarzeń zakwalifikowanych jako potencjalny incydent*dostawca* dokona krzyżowego sprawdzenia danych w powyższych źródłach informacji.

1.45. Dostawca* będzie prowadził ciągły monitoring i analizę zdarzeń z punktów końcowych (stacji użytkowników i serwerów) *zamawiającego*. Szczegółowa analiza i korelacja informacji obejmie: m.in. logowania/wylogowania użytkowników, uruchomienia/zakończenia procesów, nawiązywanych połączeń sieciowych, zapytań DNS, zmian w systemach plików, modyfikacji rejestrów, zmian w konfiguracji komputerów, podłączenia pamięci zewnętrznych, w celu wykrycia ataków i naruszeń bezpieczeństwa. Analiza wyżej wymienionych danych będzie prowadzona w zestawieniu ze wskaźnikami IOC, źródłami threat intelligence oraz w kontekście informacji o ruchu sieciowym i logów i będzie obejmowała zdarzenia bieżące oraz historyczne*co najmniej z 30 dni*.

1.46. *Dostawca* będzie prowadził ciągły monitoring i analizę informacji o ruchu sieciowym w *ustalonych* węzłach komunikacyjnych sieci *zamawiającego*. Analiza wyżej wymienionych danych będzie prowadzona w zestawieniu ze wskaźnikami IOC oraz źródłami Threat Intelligence w kontekście zdarzeń z punktów końcowych oraz logów i będzie obejmowała zdarzenia bieżące oraz historyczne*co najmniej z 30 dni*.

1.47. *Dostawca* będzie prowadził ciągły monitoring i analizę danych na podstawie logów zdarzeń z *ustalonych* systemów operacyjnych, aplikacji, systemów bezpieczeństwa oraz urządzeń sieciowych. Analiza wyżej wymienionych danych będzie prowadzona w zestawieniu ze wskaźnikami IOC oraz źródłami Threat Intelligence w kontekście zdarzeń z punktów końcowych oraz informacji o ruchu sieciowym i będzie obejmowała zdarzenia bieżące oraz historyczne*co najmniej z 30 dni*.

1.48. Wszelkie prace związane ze świadczoną usługą, z wyłączeniem reakcji na incydenty w siedzibie zamawiającego, będą prowadzone w dedykowanym pomieszczeniu SOC pod wskazanym przez *dostawcę* adresem. Wszyscy członkowie zespołu *dostawcy* zaangażowani w pracę na rzecz *zamawiającego* w zakresie monitoringu systemów, analizy zdarzeń i obsługi incydentów będą przebywali we wskazanym pomieszczeniu w czasie wykonywania tych prac.

1.49. W przypadku poważnych incydentów dostawca zapewni pomieszczenie umożliwiające spotkanie i wspólną pracę wydzielonego zespołu powołanego w celu reakcji na incydent.

1.50. *Dostawca* umożliwi wskazanym przedstawicielom *zamawiającego* przeprowadzenie niezapowiedzianych wizyt kontrolnych w pomieszczeniu w którym wykonywane będą prace na rzecz *zamawiającego* co najmniej raz w miesiącu.

1.51. W zakresie monitoringu systemów bezpieczeństwa oraz analizy i selekcji zdarzeń *dostawca* zagwarantuje dostępność min. 3 osób w godzinach 7:00 - 21:00 w dni robocze, min. 2 osób w godzinach 7:00 - 21:00 w dni wolne od pracy oraz min. 2 osób w godzinach 21:00 - 7:00.

1.52. *Dostawca* dostarczy listę członków zespołu zaangażowanego w świadczenie usługi.

1.53. Dostęp do systemów *zamawiającego* oraz systemów wykorzystywanych przez *dostawcę* do świadczenia usług na rzecz *zamawiającego* mogą mieć jedynie osoby uwzględnione na liście.

1.54. Każda zmiana w składzie zespołu świadczącego usługę musi być niezwłocznie zgłaszana *zamawiającemu*

1.55. *Zamawiający* dopuszcza możliwość zaangażowania osób/podmiotów, które nie są pracownikami *dostawcy* w przypadku gdy prace związane z analizą i reakcją na incydenty wymagają kompetencji specyficznych dla incydentu, których *dostawca* nie posiada . W takich przypadkach *dostawca* niezwłocznie poinformuje *zamawiającego* o zaangażowaniu osób trzecich. W informacji tej zawarta będzie również informacja o podstawie prawnej współpracy dostawcy z tymi osobami/podmiotami.

1.56. Każdorazowy dostęp osób/podmiotów trzecich do systemów *zamawiającego* oraz systemów wykorzystywanych przez *dostawcę* do świadczenia usług na rzecz *zamawiającego* może odbywać się jedynie w pomieszczeniu wskazanym przez *dostawcę* jako miejsce świadczenia usługi oraz w obecności przedstawicieli *dostawcy*. W przypadku realizacji zadań związanych z reakcją na incydenty w miejscu ich wystąpienia wszelkie prace prowadzone będą pod kontrolą przedstawicieli *wykonawcy*.

NDR (Network Detection and Response) - Usługa Monitoringu Bezpieczeństwa Sieci ruchu sieciowego.

1) System analizy bezpieczeństwa sieci Rozwiązanie umożliwiające monitorowanie aktywności sieci w czasie rzeczywistym, identyfikowanie potencjalnych zagrożeń i anomalii oraz tworzenie natychmiastowych alertów w przypadku ich wykrycia.
2) Rozwiązanie sieciowe z pełną inspekcją ruchu Rozwiązanie umożliwiające analizę ruchu sieciowego w oparciu o dostarczoną z sieci pełną kopię tego ruchu (nie bazuje na rozwiązaniach typu NetFlow, IPFIX lub podobnych), bez konieczności instalowania jakichkolwiek agentów na stacjach końcowych lub węzłach sieci.
3) Rejestrowanie i przechowywanie metadanych ruchu sieci Rozwiązanie musi przechowywać metadane ruchu sieciowego w obydwu kierunkach, zawierające co najmniej informacje z warstw L2, L3, L4 i L7 modelu ISO/OSI, oraz zapytania i odpowiedzi w danych z pojedynczego przepływu. Rozwiązanie musi umożliwiać przechowywanie metadanych historycznych ruchu sieciowego z okresu co najmniej 30 dni, z możliwością przywrócenia danych z dowolnego okresu i możliwością ich ponownej analizy Rozwiązanie musi umożliwiać przeszukiwanie i filtrowanie wszystkich zgromadzonych danych historycznych i zagregowanych statystyk w czasie rzeczywistym
4) Przechowywanie danych Wszystkie dane muszą być przechowywane i przetwarzane lokalnie na urządzeniu, a nie w "chmurze" lub udostępnionej bazie danych klientów
5) Kompleksowe monitorowanie urządzeń i usług

Rozwiązanie musi wykrywać urządzenia IP podłączone do sieci, w tym: laptopy, telefony komórkowe, serwery. Rozwiązanie musi także wykrywać takie zdarzenia, jak zmieniony / zduplikowany adres IP lub MAC, połączenie nowego hosta w monitorowanych segmentach sieci, brak dostępności krytycznych usług, korzystanie z zabronionych usług, adresów IP itp..
6) Uczenie maszynowe Rozwiązanie musi posiadać funkcjonalność samodzielnego uczenia się (z wykorzystaniem nienadzorowanych algorytmów uczenia maszynoweo) standardowej aktywności sieciowej i adaptacji do normalnej działalności organizacji oraz zdolność do rozpoznawania niestandardowej aktywności sieci. Rozwiązanie powinno z użyciem nadzorowanych mechanizmów uczenia maszynowego takich jak takich jak Bayesian EM and Gaussian MM wykrywać na wszystkich portach TCP / UDP anomalie w co najmniej następujących obszarach: transfer danych, liczba połączeń, liczba pakietów , liczba hostów biorących udział w komunikacji sieciowej, liczba portów, wydajność aplikacji i sieci.
7) Nadzorowana nauka i korelacja zdarzeń Rozwiązanie musi umożliwiać ręczną adaptację uczenia się bez nadzoru za pomocą granularnych środków wykorzystywanych przez użytkowników końcowych (takich jak np. priotetyzowanie konkretnych zasobów). Ponadto aplikacja musi być w stanie skorelować zdarzenia wykryte za pomocą różnych metod wykrywania.
8) Umiejętność rozpoznawania zagrożeń typu zero-day oraz machine behaviour Rozwiązanie musi umożliwiać wykrywanie zagrożeń, które nie zostałyby zidentyfikowane przez standardowe sygnatury i wykrywanie komunikacji trojanów, botnetów itp., wykrywając w co najmniej w następujących obszarach: • skanowania sieci • potencjalne wycieki danych • zachowania maszynowe (komunikacja botów) tworzone automatycznie wewnątrz monitorowanej sieci
9) Wyróżnianie podejrzanych działań w oparciu o wzorce zachowań Rozwiązanie musi być w stanie wyróżnić podejrzane działania, takie jak powtarzające się wzorce w komunikacji, techniki skanowania portów, próby brute force itp.
10) **Wykrywanie incydentów w oparciu o sygnatury** Rozwiązania musi umożliwiać zgłaszanie incydentów na podstawie wykrycia komunikacji od: znanych lub przewidywalnych zagrożeń, złośliwego oprogramowania i ataków takich jak C&C, P2P, złośliwego oprogramowania na telefony komórkowe, trojanów, aplikacji do czatu, sieci Web, exploitów, podatnych aplikacji, skanowania sieci, naruszenia zasad bezpieczeństwa itp. Zestaw reguł wykrywania musi zawierać co najmniej 30 000 aktywnych reguł, oraz umożliwiać ich co najmniej codzienną i automatyczną aktualizację. Użytkownik musi mieć możliwość tworzenia własnych reguł IDS w składni zgodnej ze snort/Suricata.
11) **Automatyzacja wykrywania oraz szczegółowa informacja** o **zdarzeniach** System powinien w sposób automatyczny identyfikować zagrożenia, przedstawiać ich opis wraz z rekomendacjami umożliwiającymi świadome podjęcie właściwej akcji przeciwdziałającej atakom
12) Deep Packet Inspection

Wykrywanie usług w oparciu o DPI, a nie tylko poprzez numer portu usługi, np. wykrywanie HTTPS na porcie 80 lub SSH na porcie 443. Rozpoznawanie komunikacji tunelowanej lub enkapsulowanej, np. ipv6 w ipv4, GRE itp. Zgromadzone w systemie metadane muszą zawierać przynajmniej metadane aplikacji (warstwa 7 modelu OSI) dla tych protokołów: HTTP, DNS, HTTPS, SMB, SMB2, DHCP, TLS, SSH, MS-SQL, SMTP, POP3, SIP, FTP, NFS, DNP3, ModBus, IEC 60870-5-101 / 104.
13) Przechwytywanie pakietów Rozwiązanie musi umożliwiać nagrywanie ruchu sieciowego na żądanie i przechwytywania pakietów, konfigurowalne co najmniej na podstawie: źródłowego i docelowego adresu IP, MAC, podsieci, protokołu, portu/usługi, wersji protokołu IP (IPv4, IPv6).
14) Czarne listy adresów IP - Blacklists Rozwiązanie musi obsługiwać możliwość pobierania adresów IP z wielu źródeł z serwisów reputacyjnych (czarnych list) wraz z co najmniej codzienną automatyczną aktualizacją. .
15) Analiza pakietów w wielu podsieciach i usługach Rozwiązanie musi analizować pakiety danych w czasie rzeczywistym i działać w różnych podsieciach i VLAN-ach. Musi być w stanie sprawdzić metadane pakietu niezależnie od protokołu lub aplikacji za pomocą silnika Deep Packet Inspection.
16) Deszyfrowanie SSL Rozwiązanie musi być w stanie odszyfrować i zaszyfrowany ruch za pomocą deszyfrowania SSL, jeśli zapewniony jest prywatny klucz RSA i certyfikat (HTTPS, SMTP, FTP itp.).
17) Widoczność serwera proxy Rozwiązanie musi być w stanie zapewnić bezpośrednią widoczność do docelowego adresu IP z hostów źródłowych, gdy serwer proxy HTTP jest używany zgodnie z elementem X-Forwarding-for zawartym w nagłówkach HTTP.
18) Powiadamianie o zagrożeniach i automatyczne raporty w czasie rzeczywistym Rozwiązanie musi umożliwiać wysyłanie powiadomień pocztą e-mail w oparciu o filtr (np. Adres IP lub MAC, typ zdarzenia, istotność zdarzenia, użytkownik, usługa, numer portu itp.). Alerty muszą być również eksportowane do systemów zewnętrznych (np. SIEM) w konfigurowalnym formacie syslog.
19) **Pojedynczy graficzny interfejs użytkownika** Rozwiązanie musi być dostępne i możliwe do zarządzania za pomocą jednego interfejsu graficznego użytkownika. Użytkownicy muszą mieć możliwość dostosowania własnych pulpitów i filtrów. Rozwiązanie powinno posiadać polską wersję językową interfejsu użytkownika
20) Wyszukiwanie i filtrowanie zdarzeń, informacji o przepływie i zbiorczych statystyk Rozwiązanie musi mieć możliwość wyszukiwania i filtrowania pełnej historii wykrytych zdarzeń i rekordów przepływów sieciowych. Rozwiązanie musi mieć możliwość wyszukiwania i filtrowania zagregowanych statystyk przepływu. Wyszukiwanie i filtrowanie muszą być dostępne na podstawie przynajmniej jednego z następujących parametrów: adres IP, adres MAC, nazwa hosta, nazwa użytkownika, usługa lokalna lub zdalna, ruch przychodzący i wychodzący, port, usługa sieciowa, autonomiczny numer systemu, identyfikator VLAN i kraj. Utworzone niestandardowe filtry muszą być przechowywane i udostępniane użytkownikom.

21) **Świadomość kontekstualna**

Rozwiązanie musi być w stanie pobierać, wizualizować i integrować informacje kontekstowe dla wykrytych zdarzeń oraz adresy wewnętrzne i zewnętrzne w graficznym interfejsie użytkownika. Minimalne wymagania są następujące:

• Nazwy użytkowników i poświadczenia użytkownika z kontrolera domeny

• Wyświetlanie nazw hostów w oparciu o bieżące rekordy DNS i DHCP
• Geolokalizacja IP

• Reputacja IP, w tym, jeśli adres IP jest na czarnej liście

• Rekordy Network flow z uszczegółowieniem do wykrytych zdarzeń

22) Profile użytkowników

Rozwiązanie musi umożliwiać tworzenie praw dostępu użytkownika (tylko do odczytu, do odczytu i zapisu, brak) dla poszczególnych użytkowników i grup użytkowników, funkcji administracyjnych i segmentów sieci.

23) Zarządzanie zdarzeniami

Rozwiązanie musi zapewniać narzędzia do współpracy w zakresie wykrywania zagrożeń i reagowania z możliwością przyporządkowywania zadań pomiędzy różnymi użytkownikami.

24) Integracja

Rozwiązanie powinno zapewniać narzędzia umożliwiające integrację z oprogramowaniem innych firm, takim jak SIEM bez pracochłonnego interfejsu API, przy użyciu co najmniej:
• syslog, CEF i LEEF dla eksportu zdarzeń

• bezpośrednie linki do URL-i zdarzeń i filtrowane wyświetlenia w GUI

• eksport informacji o przepływie w IPFIX lub podobnych formatach

25) Skalowalność

Rozwiązanie musi korzystać z architektury typu sonda + kolektor, umożliwiając jej rozbudowę zarówno o sondy jak i kolektory oraz kolektor zbierający informacje ze wszystkich kolektorów w organizacji lub wielu organizacjach np. na potrzeby SOC.

Komunikacja między sondami i kolektorami musi być zaszyfrowana przynajmniej przy użyciu protokołu SSL / TLS.

26) Raportowanie

Rozwiązanie musi umożliwiać cykliczne generowanie raportów w formacie PDF i DOCS i przesyłanie ich na wskazany adres e-mail.

Raporty powinny być generowane w języku polskim

27) Analiza śledcza

Rozwiązanie powinno umożliwiać prowadzenie analizy śledczej na bazie danych historycznych oraz funkcjonalności nagrywania pakietów ruchu sieciowego.

28) Systemy kluczowe

Rozwiązanie powinno umożliwiać zdefiniowanie urządzeń kluczowych w infrastrukturze Klienta i indywidualizację interfejsu dla tych urządzeń. System powinien umożliwiać ręczne podniesienie priorytetu zdarzeń bezpieczeństwa dla tych urządzeń.

29) Priorytetyzacja zdarzeń System powinien posiadać funkcjonalność automatycznej priorytetyzacji zdarzeń bezpieczeństwa i automatycznego przypisywania poziomu ryzyka dla każdego zdarzenia oraz funkcjonalność oznaczania zdarzeń jako false positive bez ich usuwania z systemu.
30) Blokowanie zagrożeń System powinien dawać możliwość blokowania wychwyconych zagrożeń poprzez integrację z rozwiązaniami klasy Firewall przy czym blokowanie nie powinno odbywać się w sposób automatyczny.

Wymagania dla Wykonawcy – co najmniej:

a) 7 osób z certyfikatem CRTP (Certified Red Team Professional) lub równoważny,
b) 5 osób z certyfikatem CIHE (Certified Incident Handling Engineer) lub równoważny,
c) 3 osoby z certyfikatem PNTP (Professional Network Penetration Tester) lub równoważny.

Zamawiający informuje, iż jedna osoba posiadająca więcej niż jeden z wymaganych certyfikatów, może być wykazana odpowiednio w więcej niż jednym z powyższych punktów.

Przez certyfikat równoważny Zamawiający rozumie certyfikat, który jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako:

a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
b) analogiczny stopień poziomu kompetencji,
c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,