REGULAMIN ŚWIADCZENIA USŁUG 3S SECURITY DLA KLIENTÓW B2B ŚWIADCZONY PRZEZ SPÓŁKĘ P4 SP. Z O.O.

Niniejszy dokument reguluje zasady świadczenia usług 3S Security przez P4 Sp. z o.o. z siedzibą w Warszawie.

§ 1 Definicje

1. **Operator, Usługodawca, P4** - **P4 Sp. z o.o.** z siedzibą w Warszawie, ul. Wynalazek 1, 02-677 Warszawa, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla miasta stołecznego Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000217207, której kapitał zakładowy wynosi: 48.856.500 PLN, NIP 951-21-20-077.
2. **Abonent, Klient, Usługobiorca** – osoba inna niż fizyczna nieprowadząca działalności gospodarczej, zawierająca z Operatorem umowę obejmującą Usługę.

„Abonent, Klient, Usługobiorca, Zamawiający" – osoba inna niż fizyczna nieprowadząca działalności gospodarczej, zawierająca z Operatorem umowę obejmującą Usługę

3. **Usługa** – usługa świadczona przez Operatora związana z szeroko pojętym bezpieczeństwem teleinformatycznym przez Operatora na rzecz Abonenta, świadczona na podstawie niniejszego Regulaminu, Ogólnego Regulaminu Świadczenia Usług, umowy łączącej Strony, jak również (jeśli dotyczy danego przypadku) Zamówienia.
4. **Ogólny Regulamin Świadczenia Usług** - dokument mający zastosowanie do Usług. W razie kolizji postanowień niniejszego dokumentu z Ogólnym Regulaminem Świadczenia Usług, stosuje się postanowienia niniejszego dokumentu.
5. **Regulamin**, Regulamin 3S Security – niniejszy dokument.
6. **Zamówienie -** Zamówienie w rozumieniu Ogólnego Regulaminu Świadczenia Usług**.**
7. **False Positive** – potwierdzone przez analityków SOC Zdarzenie będące fałszywym alarmem.
8. **Incydent bezpieczeństwa (Incydent)** – Zdarzenie , będące potwierdzonym przez analityków SOC Naruszeniem bezpieczeństwa systemów informatycznych Zamawiającego w zakresie dostępności, poufności lub integralności na poziomie danych zasobów informacyjnych lub usług Zamawiającego. Incydenty mogą mieć następujący status: LOW, MEDIUM, HIGH, CRITICAL.
9. **Incident handling** – proces obsługi Incydentu mający na celu jak najszybsze rozwiązanie danego Incydentu .
10. **Mitygacja** – zespół środków i działań podejmowanych w celu zmniejszenia skutków, utrudniania przebiegu lub powstrzymania Incydentu oraz przygotowania zaleceń mających na celu niedopuszczenie do jego ponowienia w przyszłości.
11. **Naruszenie bezpieczeństwa** – Zdarzenie, co do którego istnieje podejrzenie, iż może być Incydentem bezpieczeństwa, nie będące takim Incydentem bezpieczeństwa (lub do czasu uzyskania statusu Incydentu bezpieczeństwa). Wykrycie Naruszenia bezpieczeństwa odbywa się automatycznie przez System w wyniku działania Reguł korelacyjnych lub poprzez zgłoszenie Usługobiorcy. Naruszenie bezpieczeństwa jest analizowane przez specjalistów SOC i jest klasyfikowane jako False Positive lub Incydent bezpieczeństwa.
12. **Raport** – dokument sporządzony w formie elektronicznej przez Usługodawcę z czynności wykonanych w ramach Usługi. Raport może zawierać rekomendacje w zakresie monitorowanych systemów Usługobiorcy. Raporty udostępniane są w formie zaszyfrowanej poprzez e-mail. Wzór Raportu określa załącznik do Zamówienia.
13. **Audyt Bezpieczeństwa** - Usługa, której efektem jest raport opisujący stan infrastruktury IT Usługobiorcy wraz z wykazem znalezionych błędów i luk bezpieczeństwa oraz rekomendacją działań mających na celu usunięcie luk i podniesienie poziomu bezpieczeństwa infrastruktury IT Usługobiorcy.
14. **Reguła korelacyjna** – logiczne powiązanie Zdarzeń przychodzących ze Źródeł (np.: firewalli, urządzeń końcowych, systemów typu anty-malware, IDS/IPS, WAF) w celu ich holistycznej analizy oraz identyfikacji potencjalnych Incydentów bezpieczeństwa .
15. **System** - SIEM (Security Information and Event Management) – narzędzie wspierające Usługi poprzez zbieranie, monitorowanie i analizę w czasie rzeczywistym Zdarzeń generowanych przez systemy Usługobiorcy. Rozwiązanie to jest niezbędne do świadczenia Usługi na rzecz Usługobiorcy. Podstawowymi funkcjami SIEM są:
    a) agregacja – polega na gromadzeniu i przechowywaniu danych w sposób pozwalający na możliwość odtworzenia danych w dowolnym momencie;
    b) normalizacja – polega na ustandaryzowaniu wielu formatów dostarczanych danych do jednego formatu;
    c) korelacja – zestawienie logów z wielu Źródeł w postaci jednego Zdarzenia. Korelacja dokonywana jest na podstawie Reguł korelacyjnych, które mogą być dostarczane przez producentów oprogramowania SIEM lub też definiowane przez Usługobiorcę, pozwalając na dostosowanie platformy do monitorowania własnych systemów.

16. **Zagrożenie** – potencjalna możliwość naruszenia bezpieczeństwa systemów informatycznych Usługobiorcy.
17. **Zdarzenie** – każdy rodzaj aktywności w ruchu sieciowym podlegającym monitorowaniu w ramach Usługi, która to aktywność jest rejestrowana w logach Systemu.
18. **Zalecenia** – aktywność polegająca na dostarczeniu Usługobiorcy szczegółowych wytycznych dotyczących możliwości jak najszybszej i najbardziej efektywnej Mitygacji, będących wynikiem dogłębnej analizy Incydentu. Zalecenia przekazywane są etapami (drogą mailową lub telefonicznie), w miarę postępu prac nad analizą Incydentu. Usługobiorca jest odpowiedzialny za implementację Zaleceń we własnym zakresie.

19. **Zmiana konfiguracji** – oznacza zmianę ustawień w Systemie (np. stworzenie nowej lub modyfikacja dotychczasowej Reguły korelacyjnej, dodanie nowego Źródła). Żądania Zmiany konfiguracji realizowane są w Dni robocze w godz. 8.00-16.00 w terminie do 3 Dni roboczych od daty zgłoszenia przez Usługobiorcę. Zmiany konfiguracji dostępne są w usłudze niestandardowej.
20. **Źródła** – elementy infrastruktury sieciowej i bezpieczeństwa Usługobiorcy, wysyłające logi i monitorowane przez System, publikowane przez producenta Systemu jako wspierane standardowo. Jako Źródło rozumiany jest pojedynczy strumień logów generowany przez dany komponent Systemu z pojedynczego adresu IP. Przykładowymi Źródłami mogą być systemy typu: IDS/IPS, firewall, anty-malware, DLP, AD/LDAP, DNS, DHCP, Proxy.
21. **Dni robocze** – dni od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy;
22. **Dodatkowe opcje Usługi** – wszelkie dodatkowe opcje Usługi, które wymagają złożenia przez Usługobiorcę Zamówienia. Dodatkowe opcje usługi wprowadza się do Umowy po zaakceptowaniu przez Usługodawcę.
23. **Gwarancja Jakości Świadczonych Usług SLA** – dokument określający parametry jakościowe i niezawodnościowe poszczególnych Usług oraz zasady i warunki naliczania bonifikat z tytułu niedotrzymania gwarantowanych parametrów.
24. **Siła wyższa** – wydarzenie o charakterze nadzwyczajnym, niemożliwe do przewidzenia i zapobieżenia, a w szczególności wojny, zamknięcia granic, epidemie, katastrofalne działanie sił przyrody, strajki generalne oraz skutki powyższych, w tym, przerwy w łańcuchu dostaw, nadzwyczajne braki kadr, nadzwyczajne zmiany cen, nadzwyczajne przerwy w dostawach surowców lub mediów, wpływające na możliwość realizacji Umowy .

25. **SOC** (Security Operations Center) – zbiór procesów, procedur, kompetencji, narzędzi oraz wykwalifikowanych ekspertów zorganizowany tak, aby w ciągły sposób prowadzić monitoring, wykrywanie, analizę oraz reakcję w formie rekomendacji działań w odpowiedzi na ataki cybernetyczne.
26. **Zespół SOC** – dedykowany przez Usługodawcę do świadczenia Usługi zespół wykwalifikowanych ekspertów. Ilekroć w Regulaminie lub Umowie używa się określeń takich jak: analitycy SOC, specjaliści SOC, konsultanci SOC, eksperci SOC lub innych wyrażeń o tożsamym znaczeniu, Strony będą przez to rozumiały Zespół SOC.

§ 2 Ogólne zasady świadczenia Usług

1. Operator oświadcza, że posiada wiedzę, doświadczenie oraz zasoby niezbędne do prawidłowego wykonywania Umów, oraz że wprowadził adekwatne środki bezpieczeństwa w odniesieniu do Usług, jednakże z uwagi na charakter Usług nie może on wykluczyć w całości ingerencji osób trzecich, których ingerencja może wpłynąć na bezpieczeństwo korzystania z Usług.
2. Operator nie dopuszcza anonimowego korzystania z Usług.
3. Usługi świadczone są na podstawie Zamówienia składanego na podstawie umowy w rozumieniu Ogólnego Regulaminu Świadczenia Usług.
4. Opis Usług znajduje się w Załącznikach do Regulaminu. Abonenta wiąże tylko ten załącznik, który obejmuje zamówioną przez niego Usługę.
5. Wykonywanie Umów i niniejszego Regulaminu pozostaje bez wpływu na zobowiązania i uprawnienia Stron wynikające z innych łączących je porozumień i umów, o ile nie wskazano inaczej w niniejszym Regulaminie lub Zamówieniu.
6. Usługa o charakterze jednorazowym jest wykonywana przez okres do 30 dni roboczych (lub, odpowiednio, w ciągu 30 dni roboczych) od dnia złożenia Zamówienia obejmującego Usługę, o ile Strony nie wskażą innej daty rozpoczęcia Usługi. W przypadku, gdy Usługa ma zostać rozpoczęta na żądanie Abonenta, wówczas:
   a) Żądanie takie może być zgłoszone w terminie 14 dni od dnia Zamówienia, oraz
   b) Żądanie musi być zgłoszone na co najmniej 3 dni robocze przed planowaną datą rozpoczęcia.
7. Usługa o charakterze ciągłym/powtarzającym się jest uruchamiana w dniu wskazanym w Zamówieniu.

8. Każdorazowe uruchomienie Usługi ciągłej / powtarzalnej będzie potwierdzone wiadomością e-mail wysłaną na uprzednio wskazany przez Abonenta adres. Brak uwag w ciągu 3 dni od dnia wysłania takiej wiadomości traktowany będzie jak potwierdzenie poprawności uruchomienia Usługi. Dla Usług jednorazowych wiadomość taka będzie potwierdzeniem przyjęcia Usługi do realizacji.
9. Zakończenie Usług jednorazowych – z wyłączeniem usług, co do których nie będzie to wymagane lub będzie to niemożliwe - będzie potwierdzone protokołem lub wiadomością email przesłaną przez Operatora na adres wskazany przez Abonenta. Brak uwag w ciągu 3 dni od dnia wysłania takiej wiadomości traktowany będzie jak potwierdzenie poprawności zrealizowania Usługi.
10. Dla Usług ciągłych/powtarzalnych, Operator na żądanie Abonenta będzie wysyłał raporty z okresowego wykonywania Usługi, na adres e-mail wskazany przez Abonenta.
11. Operator, w miarę posiadanych możliwości technicznych, może udostępnić Abonentowi narzędzie informatyczne do samodzielnego zarządzania Usługą lub narzędzie informujące o stanie Usługi. W takim wypadku:
    a) Abonent zobowiązany jest przestrzegać wszelkich postanowień licencyjnych związanych z takim narzędziem,
    b) Operator nie odpowiada za zdalny dostęp do takiego narzędzia (tj. za łącza osób trzecich).
12. Abonent zobowiązany jest do zapewnienia dostępu Operatorowi do wskazanych przez niego narzędzi, systemów lub zasobów teleinformatycznych Abonenta, na poziomie wskazanym przez Operatora oraz utrzymywania takiego dostępu przez czas świadczenia Usługi, w szczególności połączenia sieciowego niezbędnego do realizacji Usługi.
13. Operator jest uprawniony do korzystania z usług osób trzecich lub usług osób trzecich w celu poprawnego świadczenia Usług, jednak odpowiada za działania lub zaniechania takich osób jak za działania lub zaniechania własne.
14. Niniejszy Regulamin ani Zamówienie nie będą stanowić same z siebie całości dokumentacji dotyczącej powierzenia przez Abonenta danych osobowych do przetwarzania Operatorowi i na żądanie Abonenta, Operator w uzasadnionych prawnie przypadkach zawrze z Abonentem stosowną umowę regulującą materię danych osobowych. Operator odmawia przetwarzania danych osobowych, jeśli nie zostanie zawarta stosowna umowa w tym przedmiocie, co może wpłynąć na niemożność świadczenia Usług.
15. O ile Umowa lub Zamówienie wyraźnie tak stanowi, Operator będzie świadczył Usługę na rzecz podmiotu wskazanego przez Abonenta (osoby trzeciej), przy czym w takim wypadku Abonent odpowiada za działania i zaniechania takiej osoby trzeciej jak za działania lub zaniechania własne, w szczególności odpowiada za przestrzeganie przez taką osobę zasad wykonywania Zamówienia (Umowy).

§ 3 Ograniczenia odpowiedzialności

1. Strony przyjmują do wiadomości, że nawet prawidłowe wykonywanie Usługi może prowadzić do zakłóceń funkcjonowania infrastruktury czy oprogramowania, z którego korzysta Abonent. W związku z powyższym, Operator nie odpowiada za wystąpienie w/w zdarzeń, chyba, że doprowadził do nich z winy umyślnej.
2. Operator nie odpowiada za niewykonanie lub nienależyte wykonanie Usługi w przypadku, gdy do takiego niewykonania lub nienależytego wykonania doszło z przyczyn leżących po stronie Abonenta (w szczególności Abonent nie udostępnia wskazanych przez Operatora systemów, nie zabezpiecza on swoich systemów w należyty sposób etc.).
3. Operator nie odpowiada za niewykonanie lub nienależyte wykonanie Usługi w przypadku, gdy prawidłowe wykonanie Usługi nie jest możliwe z przyczyn technicznych lub prawnych lezących poza Operatorem, w szczególności niedostępności urządzeń Abonenta (brak zasilania, brak dostępu do Internetu od dostawcy Abonenta itp.) czy obostrzeniami licencyjnymi urządzeń czy oprogramowania Abonenta.
4. Operator zobowiązuje się do dochowania należytej staranności przy wykonywaniu Usług, ale nie gwarantuje, że zapewnią one pełnię bezpieczeństwa Abonentowi, ani że będą one całkowicie skuteczne. Dla uniknięcia wątpliwości Strony akceptują, że odpowiedzialność Operatora dotyczy prawidłowego wykonywania zamówionych Usług, nie zaś skuteczności Usług.

§ 4 Postanowienia końcowe

1. Zmiany Regulaminu będą komunikowane Abonentowi z co najmniej 30 –dniowym wyprzedzeniem. Przy braku akceptacji zmian, Abonent będzie uprawniony do odstąpienia od umowy w części dotyczącej Usługi bez negatywnych konsekwencji.
2. Niniejszy Regulamin wchodzi w życie z dniem 01.12.2022 r.

Załącznik 1a

Przedmiot Usługi Audyt Bezpieczeństwa i zasady jej świadczenia

1. Usługa może mieć charakter jednorazowy lub cykliczny, zależnie od ustaleń Stron.
2. Audyt Bezpieczeństwa polega na analizie udzielonych przez Usługobiorcę informacji oraz dostarczonych dokumentów wskazanych uprzednio przez Usługodawcę, a dotyczących infrastruktury Zamawiającego. Audyt Bezpieczeństwa ma na celu:
   a. przeprowadzenie analizy aktualnej infrastruktury Usługobiorcy,
   b. dokonanie (w postaci raportu ze Skanu podatności) inwentaryzacji i weryfikacji urządzeń i systemów wykorzystywanych przez Usługobiorcę w ramach infrastruktury Usługobiorcy oraz inwentaryzacji i weryfikacji sprzętu i oprogramowania systemowego na podstawie informacji pozyskanych przez oprogramowanie Skanera podatności,
   c. weryfikację zastosowanych środków technicznych chroniących zasoby informatyczne i wewnętrzną sieć Usługobiorcy przed nieautoryzowanym dostępem.
4. Wynikiem Audytu Bezpieczeństwa infrastruktury Usługobiorcy jest Raport.

1. Zlecając przeprowadzenie Usługi Audytu Bezpieczeństwa, Usługobiorca jedocześnie oświadcza, iż:
   a. świadomy jest, że wykonanie Audytu Bezpieczeństwa, może skutkować uzyskaniem przez Usługodawcę dostępu do systemu informatycznego Usługobiorcy, w tym również do poszczególnych urządzeń połączonych z systemem informatycznym Usługobiorcy. Dostęp do systemów informatycznych Usługobiorcy realizowany może być bezpośrednio z siedziby Usługobiorcy lub za pomocą połączenia zdalnego. Uzyskanie dostępu do systemu informatycznego oraz poszczególnych urządzeń połączonych z tym systemem może skutkować uzyskaniem przez Usługobiorcę dostępu do danych przechowywanych w testowanym systemie informatycznym;
   b. świadomy jest, że podczas wykonywania Usługi istnieje możliwość uzyskania przez Usługodawcę dostępu do danych Usługobiorcy, w tym danych poufnych stanowiących tajemnicę przedsiębiorstwa lub chronionych na podstawie odrębnych przepisów prawa, przechowywanych w systemie informatycznym będącym przedmiotem Audytu Bezpieczeństwa i nie będzie zgłaszał względem Usługodawcy jakichkolwiek roszczeń cywilnych ani zawiadomień o popełnieniu przestępstwa przez Usługodawcę w związku z należytym wykonywaniem Usługi.
   c. dostarczy Usługodawcy wszelkie niezbędne informacje i dokumenty żądane przez Usługodawcę niezbędne do przeprowadzenia Audytu Bezpieczeństwa , w szczególności topologię sieci, dostęp do infrastruktury, informacje o urządzeniach bezpieczeństwa lub innych kluczowych urządzeń.
5. Rekomendowane działania zawarte w Raporcie mogą wiązać się z potrzebą nabycia przez Usługobiorcę dodatkowego oprogramowania lub urządzeń na własny koszt.
6. Mogą wystąpić przypadki, w których wykonanie rekomendacji Usługodawcy przez Zamawiającego będzie stanowiło warunek konieczny dla Aktywacji innych Usług dla danego Systemu. W takim przypadku zostanie to wyraźnie wskazane w rekomendacji zawartej w Raporcie.

Załącznik 1b
Przedmiot Usługi Monitoring i Raportowanie (SOC) i zasady jej świadczenia

1. Przedmiot Usługi polega na bieżącym, całodobowym monitorowaniu ruchu sieciowego oraz zdarzeń systemowych Abonenta w Systemie, pod kątem znanych i podejrzewanych zagrożeń cybernetycznych.
2. Warunkiem koniecznym świadczenia Usługi SOC jest uprzednie wykonanie przez Usługodawcę Audytu Bezpieczeństwa w stosunku do przedmiotu, którego ma dotyczyć ta Usługa. Usługodawca może odmówić świadczenia Usługi SOC w przypadku braku wykonania takiej uprzedniej Usługi Audytu Bezpieczeństwa, lub niepełnego zakresu takiego Audytu. Usługa Audytu Bezpieczeństwa może być osobno płatna.
3. Abonent otrzyma stosowne informacje o wykrytych Naruszeniach bezpieczeństwa, za pomocą systemu powiadomień lub kontaktu dyżurnego pracownika Operatora na adres e-mail lub numer telefonu wskazany przez Abonenta, w zależności o zakresu wsparcia dla danego rodzaju usługi 3S SOC. W razie braku połączenia telefonicznego, pracownik dokona powiadomienia e-mail lub sms. Na zamówienie Usługobiorcy pracownik może ponowić próbę połączenia do dwóch razy, po nieudanej próbie połączenia. W zależności od charakteru Naruszenia, pracownik Operatora może przedstawić sugerowane działania zapobiegawcze.
4. Usługa ma charakter ciągły i posiada zakres wsparcia i specyfikację określoną w Umowie lub Zamówieniu.
5. Usługodawca oświadcza, że:
   a. w toku realizacji przedmiotu Umowy lub Zamówienia wykorzystuje aktualne technologie z zakresu bezpieczeństwa IT;
   b. ze względu na zmienny charakter i stopień zaawansowania Zagrożeń Usługodawca nie gwarantuje, że wszystkie Naruszenia bezpieczeństwa oraz Incydenty zostaną wykryte;
   c. z uwagi na ciągły rozwój nowych technik włamywania się i atakowania infrastruktur IT oraz sieci internetowej, a także czynnik ludzki, który niejednokrotnie jest przyczyną włamania bądź ataku, Usługodawca nie ponosi odpowiedzialności za zapewnienie pełnego bezpieczeństwa systemów i usług Usługobiorcy.
6. Usługobiorca zobowiązuje się do:
   a. zapewnienia Usługodawcy dostępu do systemów i infrastruktury IT Usługobiorcy w zakresie niezbędnym do realizacji Usługi;
   b. w czasie realizacji przedmiotu Usługi będzie współdziałał z Usługodawcą;
   c. zapewnienia, że wykonanie Usługi nie naruszy żadnych umów, ani zobowiązań Usługobiorcy w stosunku do osób trzecich;
   d. nie zmieniania konfiguracji urządzeń sieciowych, systemów i aplikacji przesyłających do Usługodawcy logi z listy systemów objętych Usługą bez uprzedniego zawiadomienia Usługodawcy na co najmniej 3 (słownie: trzy) Dni robocze przed planowaną zmianą.
7. Usługodawca zapewnia przechowywanie logów napływających z systemów objętych Usługą na zasobach Usługodawcy przez okres ustalony z Usługobiorcą w Specyfikacji Usługi lub w Zamówieniu. Po upływie okresu określonego powyżej informacje zapisane w Systemie Usługodawcy zostaną usunięte.
8. W przypadku rozwiązania lub wygaśnięcia Umowy, logi przechowywane na zasobach Usługodawcy mogą zostać zwrócone Usługobiorcy na jego wyraźną prośbę dostarczoną Usługodawcy za pośrednictwem poczty elektronicznej przed datą rozwiązania lub wygaśnięcia Umowy i pod warunkiem dostarczenia w tym celu Usługodawcy przez Usługobiorcę odpowiedniego nośnika danych. W przypadku braku prośby o dostarczenie logów przez Usługobiorcę logi zostaną niezwłocznie usunięte z serwerów Usługodawcy z dniem rozwiązania lub wygaśnięcia Umowy.
9. Usługa SOC będzie świadczona przez Usługodawcę dla stanu bezpieczeństwa systemów i usług Usługobiorcy określonego w Specyfikacji Usługi lub w Zamówieniu.
10. Obowiązki Usługobiorcy:
    a. Zamawiający zobowiązany jest dostarczyć Usługodawcy wszelkie niezbędne informacje i dokumenty żądane przez Usługodawcę niezbędne do przeprowadzenia analizy przedwdrożeniowej infrastruktury, w szczególności topologię sieci, dostęp do infrastruktury, informacje o urządzeniach bezpieczeństwa.
    b. dodatkowe obowiązki Usługobiorcy uzależnione są od wyniku Audytu Bezpieczeństwa, a także każdorazowo precyzowane będą w rekomendacjach zawartych w Raporcie.
    c. Niezależnie od wyników Audytu, Usługobiorca po Aktywacji Usługi zobowiązany jest współpracować z Usługodawcą w celu należytej realizacji Usługi przez Usługodawcę, zwłaszcza w celu dostosowania Systemu do osiągnięcia maksymalnego poziomu ochrony infrastruktury IT Zamawiającego przy minimalnym poziomie obciążenia łącza, zakłóceń w ruchu, przetwarzaniu danych i w celu eliminacji jak największej liczby błędów typu False Positives;

d. dostarczyć i na bieżąco aktualizować dane osób upoważnionych do kontaktów technicznych z Usługodawcą, dostępnych przez 24 h na dobę przez 7 dni w tygodniu;
e. na bieżąco informować Usługodawcę o wszelkich zmianach w swojej sieci i infrastrukturze IT, które mogą mieć wpływ na świadczenie Usługi, w tym w zakresie zmiany parametrów, zmiany adresów sieciowych, zmian w metodach dostępu do Internetu, zmiany w aplikacjach, informacji o nowych urządzeniach i usługach dostępnych dla klienta zewnętrznego, nowej podsieci, nowej placówce zdalnej podłączonej do infrastruktury;
f. udzielić każdorazowo w ciągu 24 h odpowiedzi na zapytania Usługodawcy dotyczące świadczonych usług (np. poprzez dostarczenie dodatkowych informacji związanych z danym Incydentem bezpieczeństwa), przy zastrzeżeniu, iż każde opóźnienie może mieć wpływ na przebieg procesu reakcji na Incydent;
g. wyznaczyć przynajmniej jedną osobę odpowiedzialną za kontakt z SOC, dostępną telefonicznie lub poprzez e-mail w trybie 24/7/365;
h. niezwłocznie informować o podejrzanych zdarzeniach związanych z cyberbezpieczeństwem, np. o zgubionym laptopie, upublicznionym haśle, skompromitowanym systemie, itp;
i. dostarczyć po zakończeniu własnego śledztwa raport końcowy lub informację zwrotną o statusie Naruszenia lub Incydentu – co pozwoli na zamknięcie przypadku w systemie Usługodawcy.

11. W przypadku niewykonania lub nienależytego wykonania przez Usługobiorcę jakiegokolwiek zobowiązania określonego w ust. powyżej, Usługodawca nie gwarantuje dalszego procesowania wykrytego Naruszenia lub Incydentu.
12. W ramach procesu Incident handling w usłudze SOC, Incydenty zamykane są automatycznie w przeciągu 72 godzin od momentu potwierdzenia Incydentu przez Usługodawcę i poinformowania o nim Usługobiorcy. Usługobiorca ma prawo do zgłoszenia przez e-mail pytań lub zastrzeżeń dotyczących przesłanych przez Usługodawcę informacji o wystąpieniu Incydentu.
13. Usługodawca zastrzega sobie prawo do odmowy Zmiany konfiguracji, jeżeli zmiana taka wykracza poza zakres wybranego wariantu Usługi lub w opinii Usługodawcy może mieć negatywny wpływ na systemy lub sieć Usługobiorcy albo Usługodawcy.
14. Raport Okresowy SOC. Raz w miesiącu lub w innym ustalonym terminie, Usługodawca przygotuje i dostarczy Usługobiorcy za pośrednictwem poczty elektronicznej Raport Okresowy w zaszyfrowanej wersji elektronicznej (plik PDF) jako podsumowanie danego okresu funkcjonowania Usługi SOC.

Załącznik 1c
Przedmiot Usługi Skaner Podatności i zasady jej świadczenia

1. Przedmiot Usługi polega na wykonaniu testu infrastruktury teleinformatycznej zlokalizowanej w miejscu wskazanym przez Abonenta, w zakresie testu penetracyjnego infrastruktury stanowiącej styk sieci lokalnej z siecią Internet.
2. Po przeprowadzeniu testów penetracyjnych, Operator przedstawia Abonentowi raport z przeprowadzonych testów, zawierający co najmniej: opis wykonanych testów, wyniki testów, wnioski, zalecenia i rekomendacje dotyczące zdiagnozowanych problemów lub podatności. Raport stanowi także protokół wykonania Usługi w rozumieniu Regulaminu.
3. Raport, o którym mowa w ust. 2 będzie przekazany za pomocą poczty e-mail na wskazany przez Abonenta adres, a ja żądanie Abonenta może być także dodatkowo zabezpieczony (np. plik z założonym hasłem) lub wysłany w formie papierowej na adres wskazany przez Abonenta.
4. Niemożność dostarczenia raportu, o którym mowa w ust. 2 lub bezzasadna odmowa jego przyjęcia przez Abonenta traktowane będą jak jego odbiór bez zastrzeżeń.
5. Abonent, w terminie do 7 dni od dnia otrzymania raportu, o którym mowa w ust. 2 może zgłaszać zastrzeżenia co do jego treści, wnieść o sprostowanie lub wyjaśnienie jego treści, pod warunkiem, że zastrzeżenia takie nie rozszerzą zakresu Usługi. Operator odpowie na zastrzeżenia w terminie do 14 dni roboczych, w taki sam sposób, w jaki przekazał raport.
6. Usługa może mieć charakter jednorazowy lub cykliczny, zależnie od ustaleń Stron.

Załącznik 1d
Przedmiot Usługi Anty-DDoS i zasady jej świadczenia

1. Przedmiot Usługi polega na wpięciu pomiędzy sieć Abonenta a sieć Internet urządzenia mającego na celu ochronę wolumetryczną łącza internetowego przed atakami typu Distributed Denial of Service (DDoS).
2. Urządzenie wskazane w ust. 1 jest zarządzane przez Operatora i reaguje na faktyczne lub podejrzewane ataki DDoS.
3. Prawidłowe działanie Usługi może powodować okresowe i krótkotrwałe spowolnienie łącza internetowego lub brak połączenia z określonymi adresami (portami).
4. Operator dołoży wszelkich starań, by Usługa chroniła przed wszelkimi atakami DDoS, ale nie jest w stanie zagwarantować 100% skuteczności, ani tego, że urządzenie nie zadziała w przypadku tzw. false positive (brak faktycznego ataku).
5. Usługa ma charakter cykliczny i posiada zakres wsparcia i specyfikację określoną w Umowie w Załączniku – Specyfikacja Ochrony Anty-DDoS.