Contents

1. Informacje na temat dokumentu

Dokument ten zawiera informacje na temat zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) Sii SOC w formacie zgodnym z RFC 2350.

1.1 Data ostatniej aktualizacji

Wersja 1.0 z dnia 27 sierpnia 2025r.

1.2 Lista dystrybucyjna powiadomień

Nie dotyczy.

1.3 Lokalizacje, w których można znaleźć ten dokument.

Aktualna wersja dokumentu dostępna jest: 360 Managed Detection & Response (MDR) | Sii Polska

1.4 Uwierzytelnianie tego dokumentu.

Dokument został podpisany przy użyciu klucza PGP, poświadczenie dokumentu może być zweryfikowane poprzez klucz [Sii] PGP opublikowany w punkcie 2.8 dokumentu.

2. Dane kontaktowe

2.1 Nazwa zespołu

Sii Security Operations Center

2.2 Adres

Sii Polska Sp. z o.o.
Sii SOC
al. Niepodległości 69
02-626 Warszawa
Polska

2.3 Strefa czasowa

Czas środkowoeuropejski UTC+1 Czas środkowoeuropejski letni UTC+2 (od ostatniej niedzieli marca do ostatniej niedzieli października).

2.4 Numer telefonu

+48 22 486 37 37

2.5 Numer faksu

Nie dotyczy

2.6 Inna komunikacja

Nie dotyczy

2.7 Adres poczty elektronicznej

Pytania dotyczące oferty, zakresu świadczonych usług oraz kwestii biznesowych prosimy przesyłać na adres: contact@sii.pl
Bezpośredni kontakt z zespołem możliwy jest po otrzymaniu indywidualnego adresu członka zespołu, który po można otrzymać poprzez kontakt na adres: contact@sii.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

e-mail: contactSOC@sii.pl.

2.9 Członkowie zespołu

Zespół SOC w Sii tworzą specjaliści z pasją do cyberbezpieczeństwa, stale rozwijający swoją wiedzę i kompetencje w tej dziedzinie. Naszą misją jest podnoszenie poziomu ochrony i świadomości w obszarze bezpieczeństwa cyfrowego poprzez ciągłe monitorowanie środowisk IT, szybką i skuteczną reakcję na incydenty, realizację testów penetracyjnych oraz zaawansowaną analizę zagrożeń. Wspieramy przedsiębiorstwa oraz instytucje publiczne w budowaniu odpornych i bezpiecznych środowisk przetwarzania danych, łącząc nowoczesne rozwiązania technologiczne z edukacją i zwiększaniem świadomości pracowników.

2.10 Inne informacje

Dodatkowe informacje można znaleźć na stronie: https://sii.pl/oferta/cybersecurity

2.11 Punkty kontaktu z Klientem

Zespół Sii SOC pracuje całodobowo. Preferowaną metodą kontaktu ze Sii SOC jest e-mail:

contactSOC@sii.pl. Standardowe godziny obsługi klientów to 9:00-16:00 od poniedziałku do piątku z wyłączeniem świąt.

3. Statut

3.1 Misja

Naszą misją jest zapewnienie klientom pełnej ochrony ich kluczowych zasobów – gwarantując poufność, integralność oraz dostępność danych zawsze wtedy, gdy są potrzebne. Dążymy do utrzymywania najwyższego poziomu satysfakcji, którą mierzymy nie tylko wysoką jakością świadczonych usług w obszarze cyberbezpieczeństwa, ale również zaufaniem i pozytywnymi opiniami naszych klientów.

3.2 Obszar działania

Obszar działania Sii SOC obejmuje klientów zarówno z sektora prywatnego, jak i publicznego, z którymi Sii Polska Sp. z o.o. zawarła umowy w zakresie wsparcia w monitorowaniu, wykrywaniu i reagowaniu na incydenty bezpieczeństwa. Nasze usługi obejmują również stałe podnoszenie świadomości pracowników w obszarze cyberbezpieczeństwa, co stanowi kluczowy element budowania odporności organizacji na zagrożenia.

3.3 Sponsorowanie i przynależność

Sii SOC funkcjonuje w ramach Sii Polska Sp. z o.o.

3.4 Upełnomocnienie

Sii SOC działa w ramach struktury organizacyjnej firmy Sii Polska Sp. z o.o. z upoważnieniem kierownictwa oraz na podstawie umów z klientami Sii Polska Sp. z o.o. i na warunkach wynikających z tych umów.

4. Polityki

4.1 Typy incydentów i poziom wsparcia

Wszystkie incydenty są automatycznie klasyfikowane przez system według poziomu zagrożenia: niskiego, średniego oraz wysokiego. Następnie, przed podjęciem działań, zespół Sii SOC dokonuje szczegółowej analizy każdego zdarzenia i weryfikuje nadaną kategorię, uwzględniając postanowienia umowy zawartej z klientem.

4.2 Współpraca, interakcja i ujawnienie informacji

Sii Polska Sp. z o.o. oświadcza, że wszystkie informacje dotyczące obsługi incydentów bezpieczeństwa traktowane są jako poufne i objęte stosownymi umowami o zachowaniu poufności (NDA). Dane przekazywane przez klientów przetwarzane są w bezpiecznym środowisku, a w szczególnych przypadkach poddawane dodatkowo procesowi szyfrowania.

Przy zgłaszaniu incydentów oraz przekazywaniu informacji o charakterze poufnym rekomendujemy stosowanie mechanizmów szyfrowania bądź kontakt z Sii Polska w celu ustalenia alternatywnego, bezpiecznego kanału komunikacyjnego.

Informacje przekazywane do Sii Polska mogą być udostępniane wyłącznie zaufanym podmiotom trzecim (np. dostawcom usług internetowych, innym zespołom CERT) w zakresie niezbędnym do obsługi incydentu.

Sii Polska nie zgłasza incydentów do organów ścigania, chyba że obowiązek taki wynika bezpośrednio z przepisów prawa krajowego. Współpraca z organami ścigania realizowana jest wyłącznie w ramach oficjalnie prowadzonych postępowań.

4.3 Komunikacja i uwierzytelnianie

W celu zapewnienia poufności oraz integralności komunikacji Sii Polska stosuje mechanizmy szyfrowania oparte na technologii PGP. Wszystkie wrażliwe informacje przekazywane w ramach współpracy powinny być szyfrowane.

Sii Polska zastrzega sobie prawo do weryfikacji autentyczności otrzymanych informacji oraz ich źródła, w zakresie dozwolonym obowiązującymi przepisami prawa.

5. Usługi

5.1 Reagowanie na incydenty

Sii Polska Sp. z o.o. wspomaga organizacje w obsłudze incydentów związanych z bezpieczeństwem teleinformatycznym zarówno w aspekcie technicznym jak i organizacyjnym. Zdolności Sii Polska Sp. z o.o. obejmują cały proces reagowania na incydenty:

- przygotowanie
- wykrycie i analiza
- ograniczenia, likwidacja i odtwarzanie
- wyciąganie wniosków, analiza zebranych dowodów i rekomendacje.

5.2 Usługi cyberbezpieczeństwa

Sii Polska dokłada wszelkich starań, aby zwiększać odporność organizacji na incydenty bezpieczeństwa oraz minimalizować ich potencjalny wpływ. Nasi eksperci wspierają klientów w budowaniu świadomości cyberzagrożeń oraz sposobów ich skutecznego ograniczania poprzez realizację specjalistycznych szkoleń dla pracowników, kadry menedżerskiej i zarządów.

Na bieżąco prowadzimy analizy zabezpieczeń naszych klientów w celu optymalizacji procesów ochrony i podnoszenia poziomu bezpieczeństwa.

Świadczymy usługi w ramach:

- Dostosowania do wymogów regulacyjnych NIS2, DORA
- Wdrażania rozwiązań bezpieczeństwa: EDR/XDR, NDR, DLP, IAM/PAM
- Weryfikacji bezpieczeństwa i testów penetracyjnych
- Bezpieczeństwa OT

Szczegółowy opis wymienionych usług wraz z innymi informacjami są dostępne na stronie internetowej Sii Polska: https://sii.pl/oferta/cybersecurity

5.3 Formularze zgłaszania incydentów

Nie ma specjalnych formularzy zgłaszania incydentów do Sii Polska.

5.4 Zastrzeżenia

Podczas przygotowywania wszelkich informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności. Sii Polska nie ponosi odpowiedzialności za błędy lub pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.