SIRT / SOC – Opis dla SOC24.PL

[TLP:CLEAR]

1. Informacje o tym dokumencie

Niniejszy dokument opisuje SOC24.PL zgodnie z RFC 2350 ("Expectations for Computer Security Incident Response").
Dokument jest przeznaczony dla klientów, partnerów biznesowych oraz współpracujących zespołów bezpieczeństwa działających w polskim i europejskim ekosystemie cyberbezpieczeństwa.
Celem dokumentu jest zapewnienie przejrzystego opisu zakresu usług, zasad operacyjnych i kanałów komunikacji SOC24.PL jako komercyjnego Security Operations Center.

1.1 Data ostatniej aktualizacji

Wersja 4.00 – opublikowana 19 marca 2026 r.

1.2 Dystrybucja powiadomień

Informacje o aktualizacjach tego dokumentu mogą być przekazywane do:
- Trusted Introducer (ti@trusted-introducer.org)
- wybranych klientów i partnerów przez kanały komunikacji określone umownie

1.3 Publikacja dokumentu

Aktualna i obowiązująca wersja dokumentu jest dostępna pod adresem: https://www.nomios.pl/soc24-rfc-2350
Wersją referencyjną (kanoniczną) jest dokument w języku angielskim. W przypadku rozbieżności interpretacyjnych wiążąca jest wersja angielska.

1.4 Uwierzytelnianie dokumentu

Dokument jest cyfrowo podpisany przy użyciu klucza PGP SOC24.PL. Odpowiadający klucz publiczny opisano w sekcji 2.8.

2. Informacje kontaktowe

2.1 Nazwa zespołu

SOC24.PL

2.2 Adres

NOMIOS Poland Sp. z o.o.
ul. Puławska 537
02-844 Warszawa
Polska

2.3 Strefa czasowa

Czas Środkowoeuropejski (CET, UTC+1)
Czas Środkowoeuropejski Letni (CEST, UTC+2)

2.4 Numer telefonu

+48 22 460 07 85

2.5 Numer faksu

Nie dotyczy

2.6 Inne kanały komunikacyjne
W zależności od postanowień umownych SOC24.PL wykorzystuje również bezpieczną komunikację z klientami poprzez dedykowany portal klienta oraz platformę Microsoft Teams.

2.7 Adres poczty elektronicznej
Podstawowy kontakt operacyjny:
soc@soc24.pl

2.8 Klucze publiczne i informacje dotyczące szyfrowania
SOC24.PL wykorzystuje OpenPGP do ochrony poufności i integralności wrażliwej komunikacji.
Identyfikator użytkownika: SOC24 <soc@soc24.pl>
Odcisk klucza (fingerprint):
4073 F86E 09CF 0D09 A49C D271 1993 1641 6D50 56E6
Klucz publiczny dostępny pod adresem:
https://www.nomios.pl/soc24-publicpgpkey

2.9 Informacje dodatkowe
Informacje ogólne o SOC24.PL i usługach są dostępne pod adresem:
https://www.nomios.pl/soc24

2.10 Punkty kontaktu dla klientów
SOC24.PL przyjmuje zgłoszenia incydentów poprzez e-mail na adres soc@soc24.pl oraz przez portal zgłoszeń udostępniany klientom zgodnie z zawartymi umowami.
Pierwszy kontakt z SOC24.PL może być nawiązany również za pomocą formularza: https://www.nomios.pl/kontakt/

SOC24.PL działa w trybie 24/7/365.

3. Statut

3.1 Misja
Misją SOC24.PL jest ochrona infrastruktury klientów poprzez ciągłe monitorowanie, szybkie reagowanie na incydenty oraz proaktywne zarządzanie zagrożeniami.
SOC24.PL świadczy wysokiej jakości usługi bezpieczeństwa, zapewnia kadrę doświadczonych specjalistów, wykorzystuje automatyzację oraz rzeczywiste informacje o aktualnych zagrożeniach.

3.2 Obszar działania
Zakres podmiotowy obejmuje organizacje prywatne, publiczne i rządowe, które zawarły umowę na usługi SOC24.PL.
Dotyczy to m.in. podmiotów podlegających: ustawie KSC, dyrektywie NIS2, regulacjom sektorowym ICT oraz – w sektorze finansowym – rozporządzeniu DORA (UE) 2022/2554.
Obsługiwane są m.in. sektory finansowy, ubezpieczeniowy, telekomunikacyjny i infrastruktury krytycznej.

3.3 Powiązania organizacyjne
SOC24.PL działa w ramach NOMIOS Poland Sp. z o.o. oraz Grupy Nomios.

3.4 Uprawnienia
SOC24.PL działa w imieniu klientów w zakresie określonym umową oraz zgodnie z obowiązującymi przepisami prawa.
SOC24.PL nie posiada uprawnień i nie działa w imieniu organów regulacyjnych, nadzorczych ani organów ścigania.

4. Zasady

4.1 Rodzaje incydentów i poziom wsparcia
SOC24.PL obsługuje incydenty cyberbezpieczeństwa dotyczące infrastruktury klientów, m.in.:
- działanie złośliwego oprogramowania,
- nieautoryzowany dostęp i włamania,
- phishing i socjotechnika,
- ataki typu denial-of-service,
- naruszenia bezpieczeństwa danych,
- naruszenia polityk bezpieczeństwa.

Priorytety, czasy reakcji i zasady eskalacji są określone umową; w przypadku braku postanowień szczególnych obowiązują standardowe zasady.

4.2 Współpraca, współdziałanie i udostępnianie informacji
Wszystkie informacje związane z incydentami są traktowane jako poufne.
Wymiana informacji odbywa się zgodnie z zasadami Traffic Light Protocol (TLP).
Informacje mogą być przekazywane zaufanym stronom wyłącznie w zakresie niezbędnym do obsługi incydentu lub ograniczenia skutków incydentu oraz zgodnie z warunkami umownymi.
SOC24.PL nie powiadamia organów ścigania, chyba że wymagają tego przepisy prawa lub jest to zlecone lub wyraźnie dozwolone przez klienta.

4.3 Komunikacja i uwierzytelnianie
Do ochrony poufności i integralności wrażliwej komunikacji stosowany jest OpenPGP; zaleca się szyfrowanie informacji o incydentach.
SOC24.PL zastrzega sobie prawo do weryfikacji autentyczności informacji i źródła, w granicach prawa.

4.4 Ochrona danych osobowych (RODO)
SOC24.PL przetwarza dane osobowe wyłącznie w zakresie niezbędnym do świadczenia usług określonych w umowie oraz zgodnie z Rozporządzeniem (UE) 2016/679 (RODO).
O ile umowa nie stanowi inaczej, SOC24.PL działa jako podmiot przetwarzający, a klient jako administrator danych.
Szczegółowe warunki są określone w umowie i/lub DPA.

5. Usługi

5.1 Reagowanie na incydenty
SOC24.PL wspiera organizacje w pełnym cyklu obsługi incydentów: przygotowanie (playbooki, runbooki, SOAR), detekcja i analiza (monitoring, triage, korelacja), ograniczanie/usuwanie/odtwarzanie

(działania automatyczne i manualne), działania poincydentalne (wnioski, analiza, raportowanie), wsparcie regulacyjne na wniosek klienta (KSC, NIS2, DORA, RODO).

5.2 Działania proaktywne
Cyber Threat Intelligence; Detection Engineering; Threat Hunting; SOAR; powiadomienia o podatnościach i zagrożeniach; wsparcie zgodności (KSC, NIS2, DORA, RODO) bez przejmowania obowiązków nałożonych przez organy regulacyjne.

6. Zgłaszanie incydentów

Nie jest wymagany dedykowany formularz, zgłoszenia przyjmowane są poprzez szyfrowaną pocztę e-mail lub portal zgłoszeń.

7. Zastrzeżenia

SOC24.PL dokłada uzasadnionych starań, aby zapewnić poprawność i jakość przekazywanych informacji; nie ponosi odpowiedzialności za błędy, pominięcia ani skutki wynikające z wykorzystania informacji z niniejszego dokumentu.

8. Podpis PGP i weryfikacja autentyczności

Dokument RFC2350 SOC24.PL jest cyfrowo podpisany z użyciem PGP.
Publiczny klucz PGP:
https://www.nomios.pl/soc24-publicpgpkey
Odcisk klucza:
4073 F86E 09CF 0D09 A49C D271 1993 1641 6D50 56E6
Autentyczność dokumentu można zweryfikować za pomocą standardowych narzędzi OpenPGP (np. GnuPG).