21 LISTOPADA 2022

Deklaracja
RFC 2350 | wersja 1.0

Smartech IT Sp. z o.o.
ul. Irysowa 1
55-040 Bielany Wrocławskie
NIP: 8961562660

tel. +48 71 727 71 00, www.smartech-it.eu

Spis treści

1. Informacje na temat dokumentu

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

1.1 Data ostatniej aktualizacji

Wersja 1.0 z dnia 21 listopada 2022r.

1.2 Lista dystrybucyjna powiadomień

Nie dotyczy.

1.3 Lokalizacje, w których można znaleźć ten dokument.

Aktualna wersja dokumentu dostępna jest:
https://smartech-it.eu/rfc/

1.4 Uwierzytelnianie tego dokumentu.

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

2. Dane kontaktowe

2.1 Nazwa zespołu

SmartSOC – Smart Security Operations Center

2.2 Adres

Smartech IT Sp. z o.o.
SmartSOC
Irysowa 1
55-040 Bielany Wrocławskie
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 71 727 71 00

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: sekretariat@smartech-IT.eu
Bezpośredni kontakt z zespołem możliwy jest po otrzymaniu indywidualnego adresu członka zespołu, który po można otrzymać poprzez kontakt na adres: sekretariat@smartech-IT.eu

2.8 Klucze publiczne i inne informacje o szyfrowaniu

W celu ochrony wrażliwych informacji korzystamy z szyfrowania PGP.
e-mail: sekretariat@smartech-IT.eu
Odcisk klucza: 580F DC39 D897 8034 6B48 B191 6A07 FA4C 0FA7 36E2
Klucz publikowany jest na stronie: https://smartech-it.eu/kontakt/

2.9 Członkowie zespołu

Zespół SmartSOC tworzą młodzi ludzie, których pasją jest pogłębianie swojej wiedzy i umiejętności w zakresie cyberbezpieczeństwa. Naszym celem jest wykorzystanie posiadanych zasobów do skutecznego podnoszenia świadomości oraz bezpieczeństwa cybernetycznego za pomocą stałego monitorowania i szybkiej reakcji na wykrywane incydenty, przeprowadzania testów

penetracyjnych oraz analizy zagrożeń. Jesteśmy zainteresowani wsparciem przedsiębiorstw oraz administracji w budowaniu bezpiecznych środowisk przetwarzania danych zarówno od strony technologicznej jak i odpowiednio uświadomionych pracowników.

2.10 Inne informacje

Dodatkowe informacje można znaleźć na stronie: https://smartech-it.eu

2.11 Punkty kontaktu z Klientem

Zespół SmartSOC pracuje całodobowo. Preferowaną metodą kontaktu ze SmartSOC jest e-mail, rekomendujemy wykorzystanie PGP w celu zapewnienia integralności i poufności.
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 naszym klientom, że ich wartościowe zasoby zachowują swoją poufność, są zintegrowane i dostępne, gdy są potrzebne. Celem jest utrzymywanie najwyższej satysfakcji naszych klientów, którą mierzymy ich dobrymi opiniami o naszych usługach cyberbezpieczeństwa.

3.2 Obszar działania

Obszar działania SmartSOC obejmuje klientów z sektora prywatnego oraz publicznego, z którymi Smartech IT Sp. z.o.o. ma zawartą umowę z w zakresie wsparcia w monitorowaniu, wykrywaniu oraz reagowaniu na incydenty bezpieczeństwa komputerowego jak również stałego podnoszenia świadomości pracowników u klientów.

3.3 Sponsorowanie i przynależność

SmartSOC funkcjonuje w ramach Smartech IT Sp. z o.o.

3.4 Upełnomocnienie

SmartSOC działa w ramach struktury organizacyjnej firmy Smartech IT Sp. z.o.o. z upoważnieniem kierownictwa oraz na podstawie umów z klientami Smartech IT Sp. z.o.o. i na warunkach wynikających z tych umów.

4. Polityki

4.1 Typy incydentów i poziom wsparcia

Wszystkie incydenty automatycznie priorytetyzuje system Smartech IT w kategoriach zagrożenia: małe, średnie oraz wysokie. Przed rozpoczęciem działania zespół SmartSOC przeprowadza analizę każdego incydentu i weryfikuje klasyfikację w oparciu o warunki umowę zawartą z klientem.

4.2 Współpraca, interakcja i ujawnienie informacji

Smartech IT oświadcza, że wszystkie informacje dotyczące obsługi incydentów są rozpatrywane jako poufne oraz zabezpieczane umowami NDA

Informacje od klientów, są przetwarzane w bezpiecznym środowisku w szczególnych przypadkach są również szyfrowane. Zalecamy, przy zgłaszaniu incydentu i podawaniu poufnych informacji, użycie szyfrowania lub kontakt z Smartech IT w celu ustalenia innego bezpiecznego kanału komunikacyjnego.

Informacje przekazywane do Smartech IT mogą być przesyłane do zaufanych podmiotów (takich jak dostawca usług internetowych, inne zespoły CERT) w zakresie niezbędnej wiedzy i wyłącznie w celu obsługi incydentów. Smartech IT nie zgłasza incydentów do organów ścigania, jeżeli nie wymaga tego prawo krajowe. Smartech IT współpracuje z organami ścigania tylko w trakcie oficjalnego dochodzenia.

4.3 Komunikacja i uwierzytelnianie

W celu zapewnienia poufności i integralności komunikacji Smartech IT używa szyfrowania PGP. Wszystkie wrażliwe informacje, które są przesyłane, powinny być szyfrowane. Wiadomości

dotyczące incydentów przesyłane przez personel Smartech IT są podpisane naszym głównym kluczem PGP (patrz punkt 2.8) i szyfrowane, gdy zawierają wrażliwe informacje.
Smartech IT zastrzega sobie prawo do weryfikacji autentyczności informacji lub jej źródła w zakresie dozwolonym przez prawo.

5. Usługi

5.1 Reagowanie na incydenty

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

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

5.2 Działania aktywne

Smartech IT dokłada wszelkich starań, aby zwiększyć odporność na incydenty bezpieczeństwa oraz ograniczyć ich wpływ. Eksperci Smartech IT pomagają organizacjom rozwijać świadomość na temat zagrożeń cybernetycznych, sposobów zabezpieczania się przed nimi oraz reakcji na nie poprzez przeprowadzanie specjalistycznych szkoleń dla pracowników firm, kadr menadżerskich oraz zarządów oraz uczestnictwem i organizacją konferencji z zakresu cyberbezpieczeństwa.

Na bieżąco przeprowadzamy analizę zabezpieczeń naszych klientów, aby optymalizować nasze działania i skutecznie podnosić poziom bezpieczeństwa. Analizy przeprowadzane są w oparciu o testy penetracyjne, audyty oraz logi klienta.
Szczegółowy opis wymienionych usług wraz z innymi informacjami są dostępne na stronie internetowej Smartech IT: https://smart-soc.com

5.3 Formularze zgłaszania incydentów

Nie ma specjalnych formularzy zgłaszania incydentów do Smartech IT.

5.4 Zastrzeżenia

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