perceptus
BEZPIECZEŃSTWO IT

RFC 2350

Security Operations Center

Wersja 1.0

Perceptus sp. z o. o.

ul. Nowy Kisielin – A. Wysockiego 10
66-002 Zielona Góra

soc@perceptus.pl

Spis treści / table of content

1. Informacje na temat dokumentu

Ten dokument zawiera opis zespołu SOC Perceptus zgodnie z RFC 2350. Dostarcza podstawowych informacji o SOC Perceptus, sposobach kontaktu, opisuje obowiązki zespołu i oferowane usługi.

1.1. Data ostatniej aktualizacji
Wersja dokumentu 1.0, opublikowano 2024-04-19.

1.2. Lista dystrybucyjna powiadomień
SOC Perceptus nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

1.3. Lokalizacje, w których można znaleźć dokument
Aktualna wersja dokumentu publikowana jest na stronie:
www.perceptus.pl/soc-perceptus/ w dokumencie dwujęzycznym, zawierającym wersję w j. polskim i w j. angielskim

1.4. Uwierzytelnianie tego dokumentu
Dokument został podpisany algorytmem sha256RSA z kluczem RSA 2048Bits
Weryfikacja podpisu dostępna jest pod adresem OSCP:
http://ocsp1.uanataca.com/public/pki/ocsp/
lub http://ocsp2.uanataca.com/public/pki/ocsp/

2. Dane kontaktowe

2.1. Nazwa zespołu
SOC Perceptus

2.2. Adres
Park Naukowo-Technologiczny
Perceptus Sp. z o.o.
ul. Nowy Kisielin – Antoniego Wysockiego 10
66-002 Zielona Góra

2.3. Strefa czasowa
Czas środkowoeuropejski UTC+1
Czas środkowoeuropejski UTC+2 (od kwietnia do października; w roku 2024 zmiana czasu na letni wypada na 30/31 marca)

2.4. Numer telefonu
N/D

2.5. Adres poczty elektronicznej
soc@perceptus.pl – w sprawach technicznych i biznesowych

2.6. Klucze publiczne i inne informacje o szyfrowaniu
SOC Perceptus korzysta z klucza podpisanego przez wewnętrzny Urząd Certyfikacji oparty o CA o parametrach:

Algorytm podpisu sha512RSA
Klucz typu RSA 4096Bits
Odcisk klucza 835a8c305c665dba2015cdea412fab09a5418205
Klucz można znaleźć pod adresem Perceptus Sp. z o.o. - Root CA

2.7. Członkowie zespołu

Zespół SOC Perceptus tworzą doświadczeni eksperci w dziedzinie cyberbezpieczeństwa, którzy dbają o bezpieczeństwo usług dostarczanych przez spółkę Perceptus.
Zespół składa się ogółem z 8 osób.

2.8. Inne informacje

Inne informacje na temat SOC Perceptus, a także różnych innych zalecanych sposobów proponowanych przez Perceptus do zabezpieczenia zasobów zamieszczone poniżej pod wskazanymi linkami:
https://perceptus.pl/soc-perceptus/
https://perceptus.pl/category/wiedza-o-cyberbezpieczenstwie/

2.9. Punkty kontaktu z klientem

Preferowaną metodą kontaktu z SOC Perceptus jest e-mail na adres soc@perceptus.pl. Rekomendujemy wykorzystanie szyfrowania, aby zachować integralność i poufność przekazywanych informacji. E-mail przesłany pod ten adres zostanie natychmiast przesłany do odpowiedniej osoby lub automatycznie przekazany do odpowiedniej osoby rezerwowej. Jeśli potrzebujesz pilnej pomocy, wpisz "pilne" w temacie wiadomości.
Standardowe godziny pracy spółki Perceptus to 0800-1600 od poniedziałku do piątku z wyłączeniem świąt. Jednak Zespół SOC Perceptus pracuje całodobowo 365 dni w roku.

3. Statut

3.1. Misja

Celem, który przyświeca działalności SOC Perceptus jest wspieranie podmiotów współpracujących, zmniejszenie szansy na zmaterializowanie ryzyk związanych z cyberbezpieczeństwem oraz pomaganie swoim beneficjentom w przypadku zaistnienia cyber incydentu.

SOC Perceptus świadczy usługi cyberbezpieczeństwa klientom prywatnym oraz podmiotom publicznym.

3.2. Obszar działania

SOC Perceptus zapewnia wsparcie w zakresie obsługi zdarzeń bezpieczeństwa dla spółki Perceptus oraz klientów z sektora prywatnego i publicznego, z którymi SOC Perceptus ma zawartą umowę w zakresie wsparcia w monitorowaniu, wykrywaniu oraz reagowaniu na incydenty bezpieczeństwa komputerowego jak również stałego podnoszenia poziomu świadomości na temat zagrożeń pośród pracowników u klientów.

3.3. Sponsorowanie i przynależność

SOC Perceptus funkcjonuje w ramach Perceptus sp. z o.o.

3.4. Upełnomocnienie

SOC Perceptus działa pod auspicjami i upoważnieniem Zarządu Perceptus sp. z o.o. Ponadto SOC Perceptus działa na podstawie umów z klientami biznesowymi i na warunkach wynikających z tych umów.

SOC Perceptus obsługuje i koordynuje incydenty w imieniu swoich klientów, z którymi związany jest warunkami umowy. Ponadto regularnie wydaje rekomendacje z zakresu procesu obsługi incydentów, zainteresowanym stronom, które nie są klientami dla SOC Perceptus.

4. Polityki

4.1. Typy incydentów i poziom wsparcia

Poziom wsparcia zapewniany naszym klientom zależy od ich potrzeb i może różnić się w zależności od nagłości sytuacji i powiązanych umów SLA uzgodnionych wspólnie.

Poziom wsparcia udzielanego przez SOC Perceptus będzie różny w zależności od rodzaju i powagi incydentu lub problemu, elementów na które oddziałuje zdarzenie, ilości użytkowników, którzy są objęci działaniem incydentu oraz dostępności zasobów Perceptus w tym czasie. Dla zdarzeń określa się priorytety stosownie do ich dotkliwości i rozmiaru. Dla wszystkich przypadków pewna reakcja zostanie podjęta według poziomu krytyczności incydentu ujętego w klasyfikacji incydentów zgodnie z umowami zawartymi z klientami.

4.2. Współpraca, interakcja i ujawnienie informacji

SOC Perceptus oświadcza, że wszystkie informacje dotyczące obsługi incydentów są rozpatrywane jako poufne oraz zabezpieczone umowami NDA.
Informacje od klientów są przetwarzane w bezpiecznym środowisku, w szczególnych przypadkach są również szyfrowane.
Zalecamy przy zgłaszaniu incydentu i podawaniu poufnych informacji, użycia szyfrowania lub kontakt z SOC Perceptus w celu ustalenia bezpiecznego kanału.

SOC Perceptus nie zgłasza incydentów do organów ścigania, jeżeli nie wymaga tego prawo krajowe. SOC Perceptus współpracuje z organami ścigania tylko w trakcie oficjalnego dochodzenia. Szczegółowe informacje na ten temat można znaleźć w umowie NDA.

4.3. Komunikacja i uwierzytelnianie

SOC Perceptus jest zobowiązany do przestrzegania przepisów i zasad obowiązujących w Polsce i w Unii Europejskiej w sprawach dot. informacji wrażliwych. Ponadto SOC Perceptus chroni dane zgodnie z wdrożonymi regulacjami wewnętrznymi wynikającymi m. in. z SZBI ISO 27001.
Z SOC Perceptus można skontaktować się za pomocą poczty elektronicznej (patrz pkt.2.5).

W celu zapewnienia poufności i integralności komunikacji SOC Perceptus zaleca korzystanie z narzędzi kryptograficznych podczas przesyłania wrażliwych informacji.

SOC Perceptus zastrzega sobie prawo do weryfikacji autentyczności informacji lub jej źródła w zakresie dozwolonym przez prawo.

5. Usługi

SOC Perceptus świadczy kompleksową ochronę środowiska ICT klienta przed zagrożeniami, polegającą na monitorowaniu bezpieczeństwa infrastruktury teleinformatycznej, systemów i działań użytkowników Klienta, informowaniu go o incydentach, a także reagowaniu na incydenty poprzez ich szczegółową analizę. Obejmuje ona przekazywanie Klientowi rekomendacji mających na celu możliwie najbardziej efektywną mitygację zagrożeń. Usługa realizowana jest przez wykwalifikowany zespół specjalistów bezpieczeństwa teleinformatycznego SOC Perceptus przy wykorzystaniu odpowiednich systemów (w tym systemu SIEM) i właściwie określonych procesów i procedur.

SOC Perceptus oferuje szeroki zakres usług, w tym:

- Analiza przedwdrożeniowa
- Zarządzanie i utrzymanie usługi
- Monitoring bezpieczeństwa systemów IT;
- Weryfikacja alarmów generowanych na skutek zaimplementowanych reguł korelacyjnych i scenariuszy bezpieczeństwa
- Ocena incydentów (triage);
- Wstępna analiza incydentu na podstawie logów w Systemie SIEM
- Informowanie o incydentach zgodnie z ustalonym procesem i SLA osoby upoważnionej. W zależności od dostępności danych, informacja ta może zawierać takie dane jak: data i godzina wykrycia Incydentu, poziom krytyczności Incydentu, sposób / miejsce przełamania zabezpieczeń, Indicators of Compromise,
- Raporty okresowe

Usługi profesjonalne:

- testy penetracyjne i audyty bezpieczeństwa
- testy podatności/skanowanie sieci
- budowanie świadomości
- konfiguracja i zarządzanie platformami bezpieczeństwa
- doradztwo w zakresie bezpieczeństwa IT
- konsultacje z ekspertem

Szczegółowy opis wymienionych usług wraz z innymi informacjami można uzyskać pod adresem soc@perceptus.pl.

6. Formularze zgłaszania incydentów

Klient jest zobowiązany zgłaszać awarie i incydenty do Perceptus niezwłocznie po ich stwierdzeniu. Perceptus przyjmuje zgłoszenia 24/7 i można się z nim skontaktować poprzez soc@perceptus.pl i analitycy@perceptus.pl
Klient zgłasza awarię lub incydent podając następujące informacje:

1. Nazwę Klienta
2. Rodzaj usługi i numer umowy
3. Rodzaj i krótki opis awarii lub incydentu
4. Czas wystąpienia awarii lub incydentu
5. Zasięg problemu, jeśli jest znany
6. Szczegółowe dane kontaktowe na wypadek potrzeby współpracy w zakresie usunięcia awarii czy mitygacji incydentu w przypadku, gdy jest to inna osoba niż osoba upoważniona
7. Zastrzeżenia

Pomimo, że podczas przygotowywania informacji, powiadomień i ostrzeżeń dokładamy wszelkiej staranności, SOC Perceptus nie ponosi odpowiedzialności za błędy lub pominięcia, ani za szkody powstałe w wyniku wykorzystania informacji w nich zawartych.

ENGLISH VERSION

1. About this document

This document describes in detail the SOC Perceptus team, in accordance with the RFC 2350 standard. It contains basic information about SOC Perceptus, including the provided services, the team's responsibilities and contact information.

1.1. Date of last update

The 1.0 version of this document was published on 2024-04-19.

1.2. Notification distribution list

SOC Perceptus does not use any distribution list to notify about changes made to this document.

1.3. Locations where this document may be found

The current version of this document is available on the following website: Perceptus.pl/soc-perceptus/ in two language document, with the Polish and English language version.

1.4. Authentication of this document

This document has been digitally signed using the sha256RSA algorithm and the RSA 2048Bits key.
Verification of the signature is accessible via the following OSCP address:
http://ocsp1.uanataca.com/public/pki/ocsp/
lub http://ocsp2.uanataca.com/public/pki/ocsp/

2. Contact Information

2.1. Name of the team

SOC Perceptus

2.2. Address
Park Naukowo - Technologiczny
Perceptus Sp. z o.o.
ul. Nowy Kisielin - Antoniego Wysockiego 10
66-002 Zielona Góra

2.3. Time zone
Central European Time UTC+1
Central European Time UTC+2 (from April to October; in 2024 the shift to summertime is set to happen on the 30/31 of March

2.4. Telephone number
N/A

2.5. Electronic mail address
soc@perceptus.pl - concerning technical/business matters.

2.6. Public keys and other information about encryption
The key used by SOC Perceptus is signed by the internal Certification Authority with the following parameters:
Signature algorithm sha512RSA
Key type RSA 4096Bits
Key print 835a8c305c665dba2015cdea412fab09a5418205
The key is available at Perceptus Sp. z o.o. - Root CA

2.7. Team members
The SOC Perceptus team is made up of experienced cybersecurity specialists who oversee the security of the services provided by Perceptus.
The team consists of 8 people in total.

2.8. Other information
Further information about SOC Perceptus, as well as other ways of securing resources, recommended by Perceptus are available in the following links:
https://perceptus.pl/soc-perceptus/
https://perceptus.pl/category/wiedza-o-cyberbezpieczenstwie/

2.9. Point of contact for clients.
The preferred method for contacting SOC Perceptus is via email at soc@perceptus.pl. We recommend encrypting the message in order to maintain the integrity and confidentiality of the transmitted information. An e-mail sent to this address is immediately forwarded to the applicable person or automatically forward to the applicable reserve person. If you require urgent assistance, type "urgent" in the subject line of the e-mail.

The standard working hours of Perceptus are 8.00 a.m. - 4 p.m., Monday to Friday, not including holidays. However, the SOC Perceptus Team works around the clock, 365 days a year.

3. Charter

3.1. Mission Statement

The aim of SOC Perceptus is to support its beneficiaries by minimizing the risk of cybersecurity threats materializing and assisting them in the event of a cyber incident. SOC Perceptus provides cybersecurity services to private clients and public entities.

3.2. Constituency

SOC Perceptus provides support in the handling of security incidents for Perceptus and clients from the public and private sectors with whom SOC Perceptus has an agreement; SOC Perceptus provides support in monitoring, detecting and reacting to cybersecurity incidents, as well as consistently raising the awareness of risk among employees and clients.

3.3. Sponsorship and Affiliation

SOC Perceptus operates as part of Perceptus sp. z o.o.

3.4. Authority

SOC Perceptus operates under the authority of the Perceptus sp. z o.o. management, and within the terms and conditions of the contracts concluded with business clients. SOC Perceptus handles incidents on behalf of the clients with whom they are bound in terms of contract. Furthermore, SOC Perceptus also makes recommendations on incident handling processes to interested entities who are not clients of SOC Perceptus.

4. Policies

4.1. Incident types and level of support

SOC Perceptus can respond to any type of IT security incident. Our team does whatever it takes to investigate, contain, fix and monitor incidents, as well as advise those affected.
The level of support provided to our clients depends on their needs and may vary depending on the urgency of the situation and the service-level agreement (SLA).
The level of support provided by SOC Perceptus varies depending on the type and severity of the incident, the elements affected by the incident, the number of users affected by the incident and the availability of resources at the time. Priority is set according to the severity and extent of the incidents. However, all incidents, depending on the level of criticality, receive a response within the following time period:
Response time according to the criticality level of the Incident:
CRITICAL: 30 minutes
HIGH: 90 minutes
MEDIUM: 3 hours
LOW: 5 hours
Elimination of the incident: 24 business hours

Reconfiguration request: 72 business hours

4.2. Co-operation, Interaction and Disclosure of Information

SOC Perceptus states that all information concerning the handling of incidents is confidential under a non-disclosure agreement (NDA).
Information received form clients is processed in a secure environment and encrypted in specified cases.
We recommend encrypting messages when reporting an incident and/or providing confidential information or contacting SOC Perceptus in order to establish a secure channel.
SOC Perceptus does not report incidents to law enforcement authorities unless required to do so by national law. SOC Perceptus only cooperates with law enforcement authorities during an official investigation. Detailed information about this can be found in the NDA agreement.

4.3. Communication and Authentication

SOC Perceptus is obliged to comply with the rules and regulations applicable in Poland and the European Union in matters concerning sensitive information.
SOC Perceptus can be contacted via e-mail (see Section 2.5).

To ensure the confidentiality and integrity of communication, SOC Perceptus recommends the use of cryptographic tools when transmitting sensitive information.
SOC Perceptus reserves the right to verify the authenticity of the information or its source to the extent permitted by law.

5. Services

SOC Perceptus provides comprehensive protection of the client's ICT environment against threats, involving monitoring the security of the client's ICT infrastructure, systems, and user activities, informing the client about incidents and responding to them through detailed analysis, as well as recommending the most effective ways to mitigate threats.
The service is carried out by a qualified team of SOC Perceptus ICT security specialists, using the appropriate systems (i.a. the SIEM system) and defined processes and procedures.
SOC Perceptus offers a wide range of services, including:

- Pre-implementation analysis
- Management and maintenance of the service;
- Monitoring of IT system security;
- Verification of alarms generated through implemented correlation rules and security scenarios;
- Incident assessment (triage);
- Initial incident analysis based on logs in the SIEM system.
- Notifying about incidents according to the established process and SLA of the authorized person. Depending on the available data, the notifications may include the following information: date and time of incident detection, level of criticality of the incident, method / location of security breach, Indicators of Compromise.
- Periodic reports

Professional services:

- penetration testing and security audits
- vulnerability testing/network scanning
- awareness building
- configuration and management of security platforms
- consultation on IT security
- consultation with specialists

A detailed description of the listed services, along with further information is available at soc@perceptus.pl.

6. Incident Reporting Forms

The client is obliged to report failures and incidents to Perceptus immediately. Perceptus accepts reports 24/7 and can be contacted via soc@perceptus.pl or analitycy@perceptus.pl.

When reporting an emergency or incident, provide the following information:

1. Client name
2. Type of service and contract number
3. Type and brief description of the incident
4. The time at which the incident occurred
5. The extent of the problem, if known
6. Contact details, if the necessity to cooperate in resolving or mitigating the incident with someone other than the authorised person arises.

7. Disclaimers

Although every precaution is taken in the preparation of information, notifications and alerts, SOC Perceptus assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.