RFC 2350 OCCENTUS NETWORK

1 Información del documento

1.1 Fecha de la última actualización

Lunes 21 de agosto de 2023

1.2 Listas de distribución

soc-csirt@occentus.net

1.3 Ubicación del documento

https://www.occentus.net/RFC2350-es.pdf

1.4 Autenticación del documento

Este documento ha sido firmado digitalmente por Occentus Network S.L.

2 Información de contacto

2.1 Nombre del Equipo

OCCENTUS SOC

2.2 Dirección

Occentus Network S.L.
C/ Vila de Madrid 44. Pol. Ind. Fuente del Jarro.
ES46988, Paterna. Valencia, España.

2.3 Zona Horaria

CET / CEST

2.4 Número de teléfono

+34 961 19 08 01 (24/365)

2.5 Número de Fax

No existente

2.6 Otras comunicaciones

Dirección de correo electrónico: soc@occentus.net

2.7 Claves públicas y cifrado de información

Los correos de contacto y claves PGP asociadas se encuentran publicadas en:
https://misp.occentus.net/gpg.asc

2.8 Miembros del equipo

- Miembros del equipo de SOC de Occentus Network
- Miembros del equipo de Sistemas de Occentus Network
- Miembros del equipo de Soporte 24x7 de Occentus Network

2.9 Más información

La información general sobre los servicios proporcionados por Occentus Network y sobre la compañía se encuentra publicada en su web: https://www.occentus.net y en https://edgewatch.com

Occentus Network SL
C/ Villa de Madrid 44
Pol. Ind. Fuente del Jarro
ES46988 Paterna,Valencia

Call center +34 902 88 44 25 24h/365d
Valencia +34 96 119 08 01
Barcelona +34 93 184 67 31
www.occentus.net

2.10 Horario de atención

El equipo de respuesta a incidentes está disponible en los siguientes horarios:

- Consultas sobre servicios: horario de oficina (9.00h-17.00h)
- Incidentes catalogados con peligrosidad baja o media: horario de oficina (6.00h - 22.00h)
- Incidentes catalogados con peligrosidad alta, muy alta o crítica: 24x7x365.

2.11 Puntos de contacto para la comunidad

El método preferido para la comunicación con el CERT de Occentus Network es el correo electrónico.

Por favor, escríbanos a la cuenta: soc@occentus.net . Esto creará un caso en nuestro sistema de tickets y será tratado por nuestro personal.

3 Constitución

3.1 Misión

La misión fundamental de OCCENTUS SOC es ayudar a las empresas a disminuir los riesgos a que se exponen a causa de la gestión de su información.

OCCENTUS SOC ofrece un servicio integral en dimensiones como securización de infraestructuras TI, auditoría en seguridad global, servicios de hacking ético, consultoría, formación, asesoría, y adecuación en Derecho de las TIC y adecuación a procesos y Gobierno IT.

Ofrecemos servicios de seguridad de gestión, administración y alerta temprana de eventos de seguridad que facilitan el control total del estado de seguridad y salud de los activos de información para infraestructuras críticas, instituciones educativas, organismos públicos y entidades privadas.

Todo ello, con el fin último de conseguir la compleja tarea de gestionar la seguridad de las organizaciones, mediante la implementación conjunta de medidas preventivas, de vigilancia y de respuesta rápida ante incidentes de seguridad.

3.2 Comunidad a la que brinda servicios

Occentus Network es una empresa española dedicada a las Tecnologías de la Información y Comunicaciones que ayuda a sus clientes en cuatro áreas:

- Telecomunicaciones, Sistemas de Información y Seguridad Lógica
- Gestión 24x7x365 de Sistemas IT, Telecomunicaciones y Seguridad.
- Auditoría, Consultoría, Formación, Adecuación a Procesos y Gobierno IT a través de nuestra marca Edgewatch.
- Recopilación y tratamiento de fuentes de ciber-ínteligencia a través de nuestra marca Edgewatch.

OCCENTUS SOC presta, en sus cuatro líneas de negocio, sus servicios tanto a grandes, medianas y pequeñas organizaciones, privadas o públicas.

3.3 Patrocinio y/o afiliación

OCCENTUS SOC es el equipo de respuesta ante incidentes de seguridad de la compañía Occentus Network S.L. de capital español íntegramente privado.

3.4 Autoridad

OCCENTUS SOC colabora, a estos efectos, con CCN-CERT, CERT Gubernamental Nacional e INCIBE

Occentus Network SL
C/ Villa de Madrid 44
Pol. Ind. Fuente del Jarro
ES46988 Paterna,Valencia
Call center +34 902 88 44 25 24h/365d
Valencia +34 96 119 08 01
Barcelona +34 93 184 67 31
www.occentus.net

4 Políticas

4.1 Tipo de incidentes y nivel de soporte

El equipo de OCCENTUS SOC evaluará los incidentes que les sean reportados y desplegará, progresivamente, sus servicios dependiendo de la peligrosidad del incidente.

El nivel de apoyo que brinde OCCENTUS SOC y el tiempo de respuesta del mismo, dependerá de la gravedad del incidente reportado, la carga de trabajo del equipo y la integridad de la información disponible. La gravedad de los mismos se determinará haciendo uso de criterios establecidos por el CCN-CERT:

- Tipo de amenaza (código dañino, intrusiones, fraude, etc.)
- Origen de la amenaza: interna o externa.
- La categoría de seguridad de los sistemas afectados.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.
- El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
- Los requerimientos legales y regulatorios.

La respuesta se realizará en base al uso de una metodología contrastada para la gestión de incidentes.

OCCENTUS SOC ofrece consejos de seguridad a sus clientes, con el fin de reducir las vulnerabilidades técnicas y las provenientes de las amenazas internas de las organizaciones. De manera periódica a través de su boletín o puntual cuando se recibe alguna alerta notificada por entidades gubernamentales, como el CCN-CERT o INCIBE.

4.2 Cooperación, interacción y divulgación de la información

La información manejada por OCCENTUS SOC es tratada con absoluta confidencialidad acorde a las políticas y procedimientos para la Gestión de Incidentes establecidos para el OCCENTUS SOC mediante los pertinentes acuerdos de cooperación establecidos previamente con otros equipos CSIRTs.

4.3 Comunicación y autenticación

Los medios disponibles para la comunicación con OCCENTUS SOC son:

- Correo electrónico cifrado con las claves públicas dedicadas para ello y publicadas en: https://misp.occentus.net/gpg.asc
- Portal normalizado de intercambio de información (MISP): https://misp.occentus.net
- Portal de soporte de Occentus Network: https://marvin.occentus.net
- Portal de soporte de Edgewatch: https://support.edgewatch.com/

Occentus Network SL
C/ Villa de Madrid 44
Pol. Ind. Fuente del Jarro
ES46988 Paterna,Valencia

Call center +34 902 88 44 25 24h/365d
Valencia +34 96 119 08 01
Barcelona +34 93 184 67 31
www.occentus.net

5 Servicios

El servicio fundamental de OCCENTUS SOC es que, en caso de que se materialice algún ataque, la respuesta sea inmediata, las consecuencias puedan ser mitigadas y el impacto para la organización sea mínimo. El equipo de expertos que ponemos a disposición de la entidad afectada, asesora a la compañía con el objetivo de recuperar la normalidad en las operaciones o conseguir que se prevengan nuevos incidentes en el futuro. La evolución de las amenazas, así como la aparición de normativa dirigida a proteger la información, han hecho que los equipos de respuesta ante incidentes sean de vital importancia para las compañías.

5.1 Prevención

Desde OCCENTUS SOC se promueven iniciativas de divulgación de información con el objetivo de concienciar y prevenir incidentes de seguridad, entre las que destacan:

- Elaboración de políticas de seguridad.
- Formación y concienciación en materia de ciberseguridad, derecho tecnológico y estándares relacionados con la gestión de la información.
- Alertas y avisos a su comunidad sobre nuevas amenazas y vulnerabilidades, recopiladas de fuentes reconocidas.
- Confección de procedimientos y buenas prácticas.
- Organización y participación en jornadas y eventos de ciberseguridad.

5.2 Respuesta a incidentes

La respuesta ante incidentes es una tarea compleja para las organizaciones, ya que es necesario disponer de recursos capaces de atender y ofrecer soluciones a los eventos que puedan ocurrir.

5.2.1 Clasificación del incidente

- Investigación en profundidad del incidente acaecido.
- Determinación de la extensión del incidente.

5.2.2 Coordinación del incidente

- Categorización del incidente
- Determinación de la causa inicial del incidente (vulnerabilidad explotada)
- Coordinación con otras organizaciones involucradas en el incidente
- Informar, si procede, a otros equipos CSIRT.

5.2.3 Resolución del incidente

- Resolución y erradicación del incidente, en base a la metodología implementada por el equipo.

5.3 Análisis forense y de malware

OCCENTUS SOC dispone de equipamiento y personal especializado para realizar el análisis forense de equipos implicados en incidentes

6 Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- Buzón de correo específico: soc@occentus.net
- Teléfonos proporcionados en la información de contacto.

7 Exclusión de responsabilidad

El Equipo CSIRT de OCCENTUS SOC no se responsabiliza del mal uso que pueda darse de la información aquí contenida.

Occentus Network SL
C/ Villa de Madrid 44
Pol. Ind. Fuente del Jarro
ES46988 Paterna,Valencia

Call center +34 902 88 44 25 24h/365d
Valencia +34 96 119 08 01
Barcelona +34 93 184 67 31
www.occentus.net