



El Soporte de ciberseguridad a la medida de sus necesidades, con Centro de Operaciones de Seguridad propio de Tigloo incluyendo Servicios Gestionados

Soporte de alto nivel ofrecido directamente por expertos en ciberseguridad que monitorizarán sus sistemas únicos de negocio, su infraestructura de IT y sus procesos.

Con un SIEM tendrá:

- Una relación de soporte personalizada, liderada por un especialista que monitoriza su negocio y sus procesos.
- Un servicio de soporte, incluyendo servicios proactivos, servicios de resolución de problemas
- Servicios dirigidos a la prevención de problemas y a la optimización de su seguridad IT.
- Cobertura de soporte 24x7, con los SLAs de respuesta indicados por el cliente en función de la criticidad de la incidencia.

¿Qué servicios de soporte podrían aportar a su negocio el máximo valor? ¿Una monitorización continua de posibles anomalías y brechas de seguridad? ¿Tiene un plan de respuesta ante incidencia? ¿Auditoria de seguridad? ¿Amplio soporte proactivo incluyendo revisiones de soporte para ayudarle a mejorar la eficiencia y evitar potenciales incidentes críticos? ¿Campañas de concienciación para mantener a sus empleados al día? ¿Gestión de los Servicios para asegurar el bastionado de equipos y la formación necesaria para su personal IT?

TIGLOO ofrece todos esos servicios y más. El servicio es personalizable de acuerdo a sus necesidades: el soporte **CIBERSEGURIDAD** le da la flexibilidad de elegir las opciones de soporte que mejor se adapten a su organización. ¿El resultado de todo lo anterior? Reducir al mínimo el riesgo en su infraestructura de IT; aumentar la productividad y la eficiencia, y maximizar los beneficios de sus inversiones en tecnología.

Dedicación para asegurar que se cubren sus necesidades de Ciberseguridad

El **SOC** de **TIGLOO** es su punto de contacto para cualquier tema relacionado con la gestión de los eventos de ciberseguridad. Como representante de sus intereses dentro de **TIGLOO**, dispondrá de un contacto con un profesional altamente cualificado que se asegurará de que se cumplen todas sus necesidades de soporte.

- Colaborará con su área de IT para soportar de forma efectiva su SIEM de Manage Engine. Ayudará a su organización a planificar servicios preventivos en cualquier sistema de accesos; le dará acceso a ingenieros especializados en Ciberseguridad que le proporcionarán asesoramiento y recomendaciones en lo relativo a la seguridad y concienciación. En última instancia, le ayudarán a que obtenga mejoras de seguridad en todas sus tecnologías IT, gracias a auditorías de seguridad internas y externas.
- Le proporcionará asesoramiento legal y recomendaciones tras una posible incidencia de seguridad. Y del mismo modo, tener un acompañamiento cercano para elaborar un plan de respuesta ante incidencia.

Planificación proactiva para ayudarle a evitar paradas críticas y pérdidas de datos

TIGLOO trabajará con usted para ayudarle a identificar y solucionar problemas potenciales antes de que ocurran. La disponibilidad de sus sistemas crece, cada vez más fabricante, ma vulnerabilidades. Objetivo: lograr más tiempo para que su área de tecnología se pueda centrar en actividades estratégicas para su organización. Los servicios proactivos incluyen:

Monitorización desde el SOC:

- Instalación SIEM de seguridad OnPremise
- Monitorización eventos de seguridad.
- Revisión periódica de log para localización de brechas.
- Control de alertas críticas.
- Servicio 24x7.
- Gestión de incidencias con técnicos de ciberseguridad.

Administración de eventos e información de seguridad (SIEM):

- Instalación de Manage Engine Log360 como SIEM
- Monitorización de los logs del Firewall.
- Monitorización de los eventos de los usuarios.
- Monitorización comportamiento de Domain Admin.
- Monitorización de los logs de M365
- Monitorización y auditoria del FileServer.
- Monitorización posible fuga de datos DLP
- Regeneración periódica de índices y estadísticas.
- Control de eventos anómalos.
- Revisiones para implementar mejoras.

Servicios de transferencia de conocimiento para aumentar la seguridad de IT.

MANAGE ENGINE ofrece cantidad de herramientas para ayudar a su personal de IT a desarrollar las habilidades y recursos necesarios para mitigar potenciales incidentes antes de que ocurran. Ponemos a su disposición gran cantidad de herramientas de referencia técnica, con asesoramiento de expertos para cubrir todas las necesidades a nivel de ciberseguridad.

TIGLOO ofrece también Pentesting que proporcionan a su personal de IT visibilidad completa de las brechas de seguridad y vulnerabilidades para ayudarles a solucionar problemas de forma más eficiente. Y una parte muy importante es la de construir una guía para un plan de respuesta ante incidencia.

Rápida y experta resolución de incidentes ciber- néticos

En el caso de que se produzca una incidente seguridad, recibirá el soporte necesario para una rápida recuperación. Nuestro servicio de resolución de problemas le asegura que sus incidentes críticos reciben toda la atención necesaria hasta que estén resueltos y su negocio esté funcionando de nuevo.

Podrá reportar a TIGLOO mediante el soporte del SOC, incidentes de cualquier producto que esté dentro del servicio gestionado de ciberseguridad, también herramientas ya implementadas con anterioridad por el equipo IT. Algunas características:

- Registre sus incidentes en cualquier momento a través de nuestro soporte, por correo electrónico o por teléfono.
- Los tiempos de respuesta se priorizan en base a la severidad del problema y el impacto que tenga para su negocio. La severidad la define usted.
- Escalación rápida de incidentes críticos hasta el más alto nivel de las organizaciones técnicas.
- Coordinación multi-fabricante para la resolución de problemas.

Maximice el valor de sus inversiones en tecnología

La misión de **TIGLOO** es asegurar que obtiene el máximo valor de sus inversiones en tecnología. Ya sea porque usted está tratando de mejorar su cuenta de resultados, mejorar su productividad o utilizar la tecnología para introducirse en nuevas oportunidades de negocio, **TIGLOO** está preparado para ayudarle.

Preguntas y respuestas de los especialistas



Unai Uranga
Director de Ciberseguridad



Gurutz Munduate
Consultor Ciberseguridad

P: ¿Qué son los servicios preventivos y cómo se complementan con los servicios de resolución de problemas?

R: En el ámbito de la ciberseguridad, los servicios preventivos y los servicios de resolución de problemas son dos enfoques esenciales que se complementan entre sí para proteger los sistemas y datos de una organización. Los servicios preventivos se centran en evitar que ocurran incidentes de ciberseguridad. Incluyen una serie de prácticas, herramientas y políticas diseñadas para identificar y mitigar las amenazas antes de que puedan causar daño. En cambio, los servicios de resolución de problemas están diseñados para responder a incidentes de seguridad cuando ocurren, con el objetivo de minimizar el impacto y restarar la normalidad lo más rápido posible

P: ¿Qué es un Pentesting?

R: El pentesting, o prueba de penetración (penetration testing en inglés), es una evaluación de seguridad autorizada y simulada de un sistema informático, red o aplicación web. El objetivo es identificar y explotar vulnerabilidades de seguridad para comprender mejor los riesgos y mejorar las defensas de la organización.

P: ¿Qué valor proporciona a mi organización tener un plan de respuesta ante incidencia?

R: Tener un plan de respuesta ante incidencias proporciona a tu organización múltiples valores críticos, como la minimización del impacto, ya que permite una reacción rápida que reduce el tiempo de inactividad y protege datos sensibles, además de mitigar daños financieros al controlar costos y prevenir multas por incumplimiento normativo. Mejora la reputación y la confianza, mostrando a clientes y socios que se toman en serio la seguridad, y asegura el cumplimiento de regulaciones y estándares de la industria. Aumenta la eficiencia operativa al definir roles y responsabilidades claras, y establece procedimientos estandarizados, promoviendo una cultura de seguridad y preparación continua. Facilita la detección temprana y una respuesta proactiva, reduciendo la superficie de ataque y protegiendo tanto al personal como a los recursos físicos y digitales. En esencia, un plan de respuesta ante incidencias fortalece la resiliencia organizacional, asegurando que se manejen y se recuperen de los incidentes de seguridad de manera efectiva y rápida, protegiendo así los activos, datos y la continuidad operativa de la organización.

P: ¿Cuáles son los beneficios del soporte gestionado de ciberseguridad con un SOC?

R: El soporte gestionado de ciberseguridad con un Centro de Operaciones de Seguridad (SOC) ofrece numerosos beneficios, incluyendo monitoreo continuo 24/7 para detectar y responder rápidamente a amenazas, acceso a expertos especializados y conocimientos actualizados, reducción de costos a través de economías de escala, y cumplimiento normativo con documentación para auditorías. Además, mejora continuamente la seguridad mediante evaluaciones de riesgos y actualizaciones, proporciona inteligencia de amenazas para una protección proactiva, y ofrece escalabilidad y flexibilidad para adaptarse a las necesidades cambiantes de la organización. También facilita una respuesta coordinada y rápida a incidentes, minimizando el tiempo de recuperación y asegurando la continuidad del negocio.

Para más información o para adquirir el Soporte de Ciberseguridad, contacte con: marketing@tigloo.es