THE SECURITY SENTINEL

SOLUCIONES ON SECURITY_

El panorama global de amenaza cibernética está en constante evolución, con un flujo permanente de nuevas y avanzadas amenazas que ponen a prueba nuestra seguridad: virus que corrompen o secuestran datos, software espía que roba información valiosa, ataques de denegación de servicio (DoS) sobre webs de comercio electrónico, fugas de información, etc. Mantenerse al día puede ser un trabajo duro. Y a esto hay que añadir un entorno organizacional cada vez más dinámico y deslocalizado: teletrabajo, movilidad, servicios en la nube, etc. que aumenta la complejidad y donde cualquier grieta podría significar un desastre.

The Security Sentinel proporciona, a través de su unidad de negocio On Security, soluciones y servicios de ciberseguridad para la identificación, protección, detección, respuesta y recuperación de cualquier tipo de amenaza a la seguridad de la información.

SECURIZE SUS SISTEMAS CON NUESTRA SOLUCION INTEGRAL_

SECURITY OPERATION CENTER (SOC)

Nuestro centro de respuesta a incidentes trabaja 24x7 monitorizando, detectando y respondiendo a eventos de ciberseguridad que puedan ocurrir en su organización.

SECURITY EXPERT CONSULTING (SEC)

Nuestros expertos en seguridad pueden apoyarle en el diseño e implementación de soluciones que aumenten la seguridad en su organización.

Nuestro enfoque hacia la ciberseguridad está basado las 5 funciones definidas en el Cyber Security Framework, desarrollado por el NIST con el objetivo de proporcionar a las organizaciones métodos para proteger adecuadamente sus activos ante ciberataques.

Nuestro portafolio de servicios y productos se enmarca dentro de estas cinco funciones críticas cubriendo así los aspectos más relevantes del entorno de amenazas actual.

IDENTIFICAR
Entender el contexto organizacional para manejar el riesgo de la ciberseguridad.

PROTEGER
Implementar las salvaguardias apropiadas para asegurar la correcta provisión de servicios.

DETECTAR
Identificar la aparición de un evento de ciberseguridad.

RESPONDER
Tomar las medidas adecuadas con respecto a un evento de ciberseguridad detectado.

RECUPERAR
Restaurar cualquier capacidad o servicio afectado por un problema de ciberseguridad.

915 792 426 · info@thesecuritysentinel.es · thesecuritysentinel.es

IDENTIFICAR

NO PUEDE PROTEGERSE LO QUE NO SE CONOCE_

La identificación es fundamental para la correcta gestión de la ciberseguridad. Comprender el contexto empresarial, los sistemas que dan soporte a los servicios críticos, los activos relacionados, la criticidad de la información, las personas implicadas y los riesgos relacionados con la ciberseguridad permite a una organización priorizar sus esfuerzos en consonancia con su estrategia de gestión de riesgos y las necesidades del negocio.

GESTIÓN DE ACTIVOS

La correcta identificación de la información, el personal, los dispositivos y sistemas de la organización, así como sus relaciones y la importancia para los objetivos del negocio es el primer paso imprescindible para la correcta gestión de la ciberseguridad. The security Sentinnel proporciona herramientas automáticas que permiten que esta información sea completa y esté correctamente actualizada.

ENTORNO DE NEGOCIO

Las organizaciones están sujetas a un entorno sumamente complejo en el que desarrollan su labor. La legislación aplicable, los grupos de interés, los posibles competidores, las aplicaciones en la nube, los proveedores, los socios de negocio... son elementos que influyen también y de manera directa en la gestión de la ciberseguridad. La amplia experiencia de The security Sentinnel colabora con su organización para que esta gestión se realice correctamente.

GOBIERNO

Las tecnologías de la información sólo aportan valor al negocio en la medida en que están alineadas con los objetivos de negocio. En este ámbito la ciberseguridad debe garantizar, además de los requisitos organizacionales, el cumplimento legal, de riesgo, ambiental, económico... Para posibilitar el cumplimiento de estos objetivos, el equipo de expertos en seguridad de The security Sentinnel (SEC) le apoyan la implantación de estándares y buenas prácticas del mercado de demostrada solvencia como son COBIT, ISO 27000, ITIL, ISO 20000, PRINCE2, LOPD...

GESTIÓN DE RIESGOS

Un correcto análisis de riesgos de la organización alineado con su perfil tecnológico, el apetito y la tolerancia al riesgo permite dirigir de manera correcta las actuaciones e inversiones en materia de ciberseguridad. The security Sentinnel le ayudará en la realización tanto de este análisis como de los planes directores que le permitan obtener sus objetivos.

PROTEGER

UNA CADENA ES TAN FUERTE COMO SU MÁS DÉBIL ESLABÓN_

La protección posibilita limitar o contener el impacto de un posible evento de ciberseguridad, consiguiendo así minimizar el efecto que dicho evento puede producir sobre la actividad de la organización.

CONTROL DE ACCESO

El acceso a la información, activos, dispositivos e instalaciones debe estar limitado a los usuarios autorizados si queremos garantizar la ciberseguridad. Los procesos y actividades deben ser además correctamente autorizados y monitorizados. The Security Sentinnel ofrece soluciones para la correcta identificación de usuarios, seguridad de la red (cortafuegos, NAC...) herramientas de monitorización y auditoría... que le permiten realizar correctamente esta tarea.

FORMACIÓN Y CONCIENCIACIÓN

El factor humano es clave en el éxito de la ciberseguridad, por lo que la correcta formación de los usuarios tanto a nivel técnico (herramientas, amenazas, atacantes...) como organizacional (normas, políticas, responsabilidades...) se convierte en una tarea vital en la que The Security Sentinnel puede aportar su experiencia y contrastado know-how.

SEGURIDAD DE DATOS

La información debe protegerse en sus tres aspectos fundamentales (disponibilidad, confidencialidad e integridad) en todo su ciclo de vida. La ciberseguridad debe garantizar que la información se obtiene de manera correcta, se custodia adecuadamente, se transporta de forma segura, se actualiza puntualmente, está disponible cuando se necesite, se facilita sólo a las personas autorizadas (evitando fugas de información) y se destruye de manera eficaz. Para conseguir este objetivo, The Security Sentinel aporta tecnologías de autenticación fuerte, cifrado, alta disponibilidad, anti fugas de información...

OPERACIONES

Las operaciones y los distintos procedimientos de mantenimiento y gestión de las infraestructuras TI deben realizarse garantizando la seguridad y la resiliencia de los sistemas y cumpliendo con las políticas de la organización. The Security Sentinnel ofrece herramientas de monitorización y auditoría, cumplimiento de políticas, gestión de dispositivos extraíbles, actualización de software, control remoto, gestión de la red, gestión de la capacidad...

DETECTAR

SE PUEDE PERDONAR EL SER DERROTADO, PERO NUNCA EL SER SORPRENDIDO_

La detección más temprana, completa y veraz posible de la ocurrencia de un evento de ciberseguridad permite responder adecuadamente a dicho evento, priorizando las actuaciones y utilizando adecuadamente los recursos disponibles.

ANOMALÍAS Y EVENTOS

Es necesario establecer la línea base de los sistemas y detectar desviaciones de la misma. Nuestro SOC utiliza sistemas de correlación de logs que pueden analizar y correlar datos de múltiples fuentes y detectar comportamientos anómalos que pasarían desapercibidos si son analizados de manera aislada.

MONITORIZACIÓN CONTINUA DE LA SEGURIDAD

Sistemas automáticos de monitorización de la red, monitorización de accesos, análisis de malware, análisis de vulnerabilidades... así como análisis periódicos con inteligencia (auditorías de seguridad, pentesting...) son utilizados por el SOC de The Security Sentinnel para alertar de posibles problemas de seguridad que deben ser correctamente atendidos.

PROCESOS DE DETECCIÓN

Las auditorías, pentesting y análisis de vulnerabilidades que realiza The Security Sentinnel no sólo deben probar la fortaleza de los mecanismos de seguridad. También deben ser adecuadamente utilizados para probar la eficacia de los sistemas de detección, así como el correcto tratamiento de los eventos de seguridad.

RESPONDER

LA RAPIDEZ DE ACCIÓN ES EL FACTOR CRUCIAL PARA VENCER_

Tomar las medidas adecuadas tras detectar un evento de ciberseguridad, de manera rápida y utilizando eficazmente los recursos disponibles, permite contener el impacto de un potencial problema de ciberseguridad.

PLANES DE RESPUESTA

La estrategia de respuesta ante un incidente debe ser planificada y puesta en marcha antes de la aparición de los mismos. The Security Sentinnel pone a su disposición la experiencia de su SOC, preparado para responder 24x7 a los incidentes de seguridad que puedan acaecer.

ANÁLISIS Y COMUNICACIÓN

Ante de la detección de un incidente, es necesario un análisis preciso del mismo y la comunicación adecuada con todos los agentes implicados. Nuestro SOC dispone de la solvencia técnica para analizar los incidentes que pudieran producirse y coordinar las tareas de comunicación necesarias.

MITIGACIÓN

Tras la detección y el análisis de un incidente, es necesario desplegar las medidas adecuadas para la erradicación del mismo. The Security Sentinnel pone a su disposición su SOC para realizar estas tareas o asesorar a su equipo técnico en las mismas.

RECUPERAR

NO SE SALE ADELANTE CELEBRANDO ÉXITOS SINO SUPERANDO FRACASOS_

Poner en práctica planes para resiliencia y superar oportunamente cualquier problema de ciberseguridad restaurando las operaciones normales de cualquier capacidad o servicio que se haya visto afectado.

PLANES DE RECUPERACIÓN

Ante un incidente de seguridad, uno o varios servicios pueden verse afectados. Se hace necesario por tanto la existencia de planes de recuperación, previamente probados, que garanticen la recuperación lo más temprana posible de los servicios afectados. The Security Sentinnel le apoya en el diseño, implementación y pruebas de dichos planes, así como a su puesta en marcha en caso de incidente.

CONTINUIDAD

Más allá de la intervención reactiva ante un incidente, la gestión de la continuidad se organiza proactivamente día a día para prevenir y limitar los posibles efectos de un incidente. The Security Sentinnel dispone de soluciones para aumentar la resiliencia y disponibilidad de sus sistemas ante potenciales incidentes.

MEJORA CONTINUA

Todo el proceso de identificación, protección, detección, respuesta y recuperación debe estar sometido a mejora continua. Tras la aparición de un incidente hay que responder a las preguntas de por qué se ha producido el incidente, cómo podemos mejorar la detección, cómo disminuir su impacto, cómo recuperar antes los servicios... The Security Sentinnel le aportar toda su experiencia y know-how para mejorar día a día su ciberseguridad.