SOKNOW
MONITORING & CYBERSECURITY

TECNOVAN LATAM PERU
del Grupo Araya & Cía.

LA IMPORTANCIA DEL SOC EN LAS ORGANIZACIONES.

Las organizaciones, independiente del tamaño o sector al que pertenezcan, constantemente deben combatir en dos frentes debido a que su exposición es cada vez mayor. Por un lado, se deben enfrentar a constantes amenazas y ataques de ciberseguridad. Por otro lado, cada día las empresas tienen que cumplir con legislaciones y reglamentos relativos a la seguridad de la información que son cada vez más exigentes y restrictivos.

A pesar de las medidas de seguridad que puedan tomar a nivel interno las organizaciones, los ataques son cada vez más complejos y sofisticados, manteniéndose en constante evolución con la única finalidad de cumplir su objetivo: Romper la seguridad de la empresa, por lo que la ciberseguridad se ha convertido en una prioridad y un reto para las empresas.

La mejor solución para proteger de forma integral la ciberseguridad de la empresa es un SOC (Security Operations Center), un centro de seguridad dónde un conjunto de expertos detecta en forma temprana los incidentes de ciberseguridad, disminuyendo considerablemente el impacto de los ataques y respondiendo en forma proactiva ante los eventos de este tipo.

Por lo anterior, TECNOVAN LATAM pone a disposición nuestro SOC, SOKNOW, otro servicio compuesto por especialistas en ciberseguridad con el único objetivo de ayudar a nuestros clientes a estar en constante monitoreo de sus sistemas, minimizando al máximo posible los incidentes en Ciberseguridad y seguridad de la información.

POR QUÉ TENER UN SOC

La principal ventaja de disponer de un centro de operaciones de seguridad es la mejora de la detección de incidentes de seguridad mediante la supervisión y el análisis continuos de la actividad de los datos de manera preventiva, sin embargo, la creación y operación de un SOC es complicada y costosa.

Las empresas los establecen por varias razones, tales como:

- Proteger los datos confidenciales.
- Prevención de incidentes de seguridad.
- Cumplir con las normas de la industria, como PCI DSS
- Cumplir con las normas gubernamentales como la GPG53 CESG

La supervisión ininterrumpida de la actividad de datos en las redes, terminales, servidores y bases de datos de una organización ofrece a las organizaciones una ventaja a la hora de defenderse de incidentes e intrusiones, independientemente de la fuente, la hora del día o el tipo de ataque. Un centro de operaciones de seguridad ayuda a las empresas a salvar la distancia entre el tiempo que tarda el hacker en comprometer el sistema y el tiempo que tarda en detectar la amenaza, así como en mantener a su entorno al tanto de las amenazas.

COMO SE COMPONE

Se encuentra compuesto por un equipo humano con más de 10 años de experiencia en implementación, administración y soporte de tecnologías dedicadas a la Ciberseguridad, siendo nuestro foco principal la proactividad, conocimiento y compromiso con cada uno de nuestros clientes, logrando siempre la entrega de un servicio de monitoreo y ciberseguridad de primer nivel, disminuyendo los impactos de incidentes.
SOKNOW está conformado por los siguientes profesionales y especialista:

1. **Nivel 1:** Se encuentra la primera y única línea de contacto hacia nuestros clientes, quienes se encuentran capacitados para cumplir las siguientes actividades:
    a. Registro de requerimientos de clientes
    b. Atención de primer nivel
    c. Escalamiento de incidentes y/o requerimientos a segundo y tercer nivel
    d. Análisis de Alertas
    e. Monitoreo constante de las alertas recibidas en el SOC, evaluando cada alerta y escalando a nivel 2 dependiendo de la criticidad de esta.

2. **Nivel 2:** Determinan si los datos o el sistema se han visto afectados y, de ser así, recomendarán una respuesta.

3. **Nivel 3:** Está compuesto por profesionales altamente capacitados, que se encargan de resolver los incidentes, pero también analizar los antecedentes con el fin de prevenirlos.

CÓMO OPERA

Los principales servicios que se prestan desde SOKNOW son:

- Monitoreo de redes y servidores: Somos capaces de monitorear toda la infraestructura de red de nuestros clientes, independiente de la tecnología utilizada.
- Inventario de Activos y redes: Basados en ISO 27001 e ISO 22301, realizamos un control y levantamiento de todos los de seguridad y redes de nuestros clientes con la finalidad de poder realizar la matriz de riesgo de los distintos dispositivos.
- Monitoreo de Ciberseguridad: Poseemos tecnología capaz de monitoreo temprano ante un evento malicioso que pueda afectar la disponibilidad de los servicios de nuestros clientes.
- Correlación de eventos.
- Análisis proactivo de eventos y clasificación.
- Investigación de incidentes y trabajo predictivo.
- SIEM y gestión de logs (Correlación).
- Respuesta ante incidentes de Ciberseguridad
- Detección de intrusos.
- Informes de seguridad y cumplimiento.

Adicionalmente, como parte del compromiso que tenemos con nuestros clientes, se ofrecen los siguientes servicios adicionales:

- Análisis de vulnerabilidades/Ethical Hacking
- Servicio de administración, gestión y concientización de usuarios.
- Servicio de seguridad Wordpress.
- Administración de solución de parchado de sistemas operativos y software.
- Administración de seguridad Endpoints.
- Consultoría de seguridad y redes.
- Gestión de hardening.