BURÓMC
SEGURIDAD INFORMÁTICA

DATASHEET

SOC

ANTECEDENTES

Los ataques cibernéticos están creciendo más rápido que nunca. Añadido a eso, los servicios en la nube y el Internet de las Cosas (IOT) son complejos y es difícil de encontrar la ciberseguridad experta que necesitan.
Con una fuerza laboral cada vez más enfocada en el teletrabajo, las empresas ya no pueden confiar en las soluciones de detección y recopilación de registros tradicionales. La visibilidad avanzada de los terminales es un componente crucial para asegurar la fuerza de trabajo remota y los teletrabajadores, por lo que incluimos CybrHawk Endpoint como tecnología central para todas nuestras soluciones.

¿POR QUÉ NOSOTROS?

Pocas organizaciones tienen los recursos para mantener soluciones costosas y complejas de gestión de eventos e información de seguridad (SIEM) y no cuentan con un centro de operaciones de seguridad que pueda investigar y responder a los incidentes las 24 horas del día. En este caso, CybrHawk y BuróMC son la solución. Nuestro sistema de automatización y orquestación de seguridad basado en la nube reduce la carga de trabajo y prioriza los riesgos para nuestro SOC, con analistas de seguridad experimentados que trabajan con una amplia gama de experiencia en ciberseguridad. El SOC-as-a-Service puede ser un SOC completamente administrado, para brindarle la tranquilidad y la seguridad que necesita a una fracción del costo para respaldarlo a usted mismo y a sus clientes

SERVICIOS

Usted y su organización obtendrán visibilidad de los siguientes servicios mencionados, desde los diferentes reportes de posibles incidentes, para cada proceso de la operación, desde el monitoreo hasta el seguimiento y mitigación de incidentes, así como también recomendaciones por parte de nuestro grupo de ingenieros especializados.

SIEM-XDR

Obtener acceso a una visibilidad completa para detectar y prevenir ataques sofisticados

Seguridad en la nube

Responda a las amenazas avanzadas dirigidas a su Cloud Apps, O365, Gsuite, y mas.

Seguridad engañosa

Te ayudamos a manejar y desplegar distintos Honeypots para burlar a hackers!

BURÓMC
SEGURIDAD INFORMÁTICA

DATASHEET

SOC

SERVICIOS

Assessment de seguridad

Te ayudamos a cumplir con distintos requisitos CMMC/NIST al proveer amenazas y detección por toda tu red.

Búsqueda de amenazas

Nuestros expertos continuamente buscan amenazas haciendo uso de inteligencia especializada.

- MONITOREO SIEM
- CORRELACIÓN DE EVENTOS
- RESPUESTA A INCIDENTES DE SEGURIDAD
- REGISTRO DE LOGS
- DASHBOARDS
- SERVICIOS DE MANOS EN SITIOS POR EVENTO
- REPORTE MENSUAL SEGURIDAD
- SEMINARIOS VIRTUALES
- ALERTAS VIA EMAIL
- CONTROL DE ALTAS BAJAS Y CAMBIOS

¿CÓMO LO HACEMOS?

Para nosotros los procesos son lo más importante, nos permiten entregar servicios de calidad que dan certeza a nuestros clientes, es por ello que se han desarrollado metodologías propias basadas en los más altos estándares de la ciberseguridad. Otra de nuestras ventajas es contar con un laboratorio de ciberseguridad que nos permite analizar amenazas fortaleciendo los conocimientos del personal que se encuentra en constante capacitación, ejecutando ejercicios que apoyan al desarrollo de las capacidades de reacción y contención de incidentes siempre bajo un marco de normatividad.

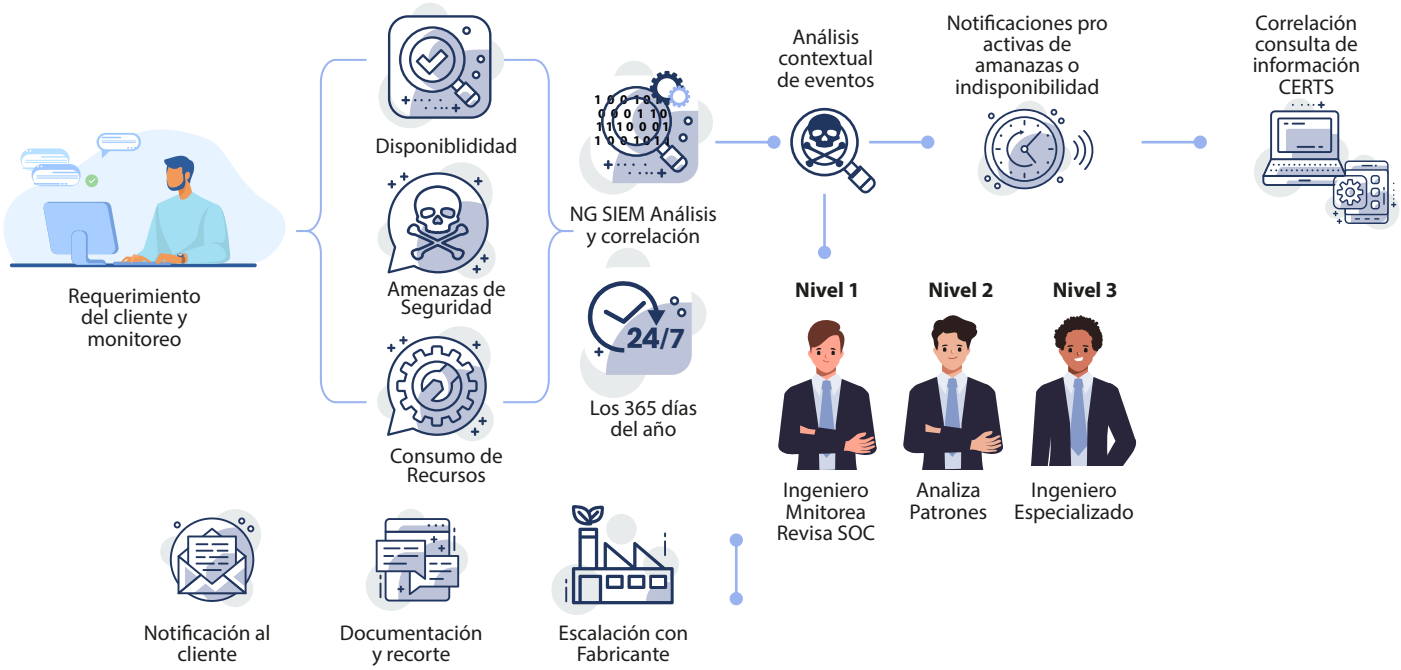
BURÓMC SEGURIDAD INFORMÁTICA

DATASHEET

SOC

NUESTRO ACCIONAR A GRANDES RASGOS FUNCIONA DE LA SIGUIENTE MANERA

- La plataforma de SIEM es 100% en la nube.
- Esta plataforma consume la información que los equipos en alcance nos envían.
- Toda la información se analiza, categoriza, y es presentada a los operadores.
- La información procesada por el SIEM es analizada por los operadores del SOC y en se determina si la alerta procede a ser reportada y clasificada como incidente de seguridad.
- Las amenazas reportadas como positivas disparan un proceso de notificación, investigación y contención.
- Una vez resuelto el incidente de seguridad, se realiza la documentación del incidente en la base de conocimientos para cada vez ser más ágil en las atenciones.



REPORTE

De manera Mensual o bajo demanda se entregan reportes con todas las incidencias que se generaron en el mes, se emiten recomendaciones, mejoras y tendencias que ayudan a tomar decisiones y generan un valor agregado.

buromc.com
BuróMC Seguridad Informática
55 5432 0349
contacto@buromc.com
@BuroMC
@BuroMC