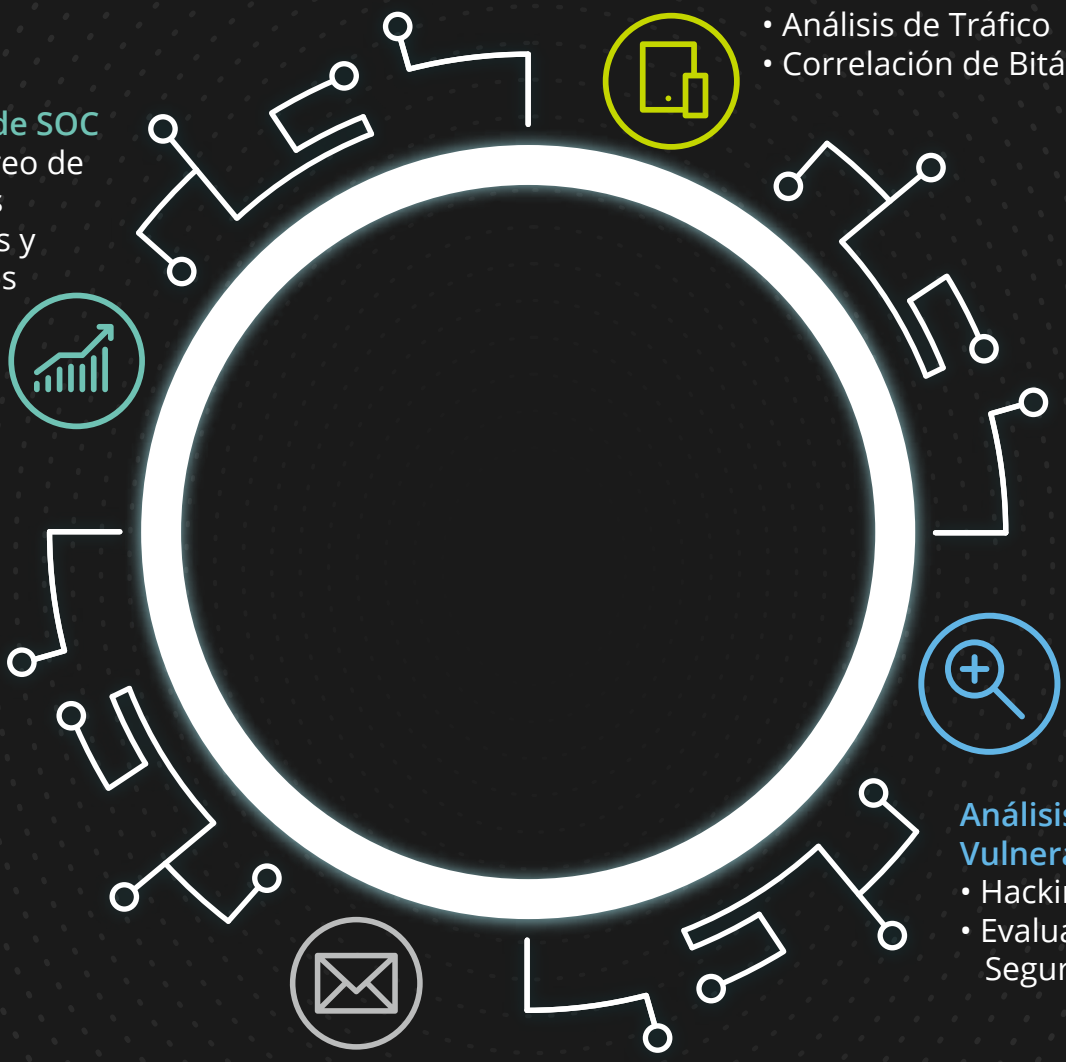
Deloitte.

Servicios SOC/CERT

Ciberseguridad

Nuestro Servicio
Security Operation Center



Sensores
- Análisis de Tráfico
- Correlación de Bitácoras/Logs

Servicio de SOC
- Monitoreo de eventos Internos y Externos

Análisis de Vulnerabilidades
- Hacking Ético
- Evaluación de Seguridad

DEMARC/Secure Email

Diferencias de Nuestro Servicio

- Monitoreo de Riesgo Global
- Gestión de Infraestructura
- Único Dashboard de Gestión
  - Logs
  - Tráfico anómalo
- Correlación en Línea
- Fácil seguimiento a la mitigación
- Automatización de Alertas y Reportes en tiempo Real

Nuestro Servicio
SOC/CERT

El CERT provee un sistema único de Inteligencia de Seguridad y capacidades de Data Mining:

- Gestión de Riesgo Tecnológico
- Correlación
- Métricas de Riesgo
- Escaneo de vulnerabilidades
- Data Mining
- Monitoreo en Tiempo Real

Los servicios del SOC debido a su capacidad de correlación y data mining, poseen alto rendimiento y escalabilidad de millones de eventos por día, debido a que su detección es distribuida y diseñada para alto desempeño.

La responsabilidad del análisis y almacenamiento de la información puede asignarse a los diferentes nodos los cuales gestión sus alarmas generadas desde el SOC, para mantener la confidencialidad e integridad de la información que procesan.
Esto permite tener una vista global de la seguridad y el índice de exposición al riesgo en tiempo real.

Roles en la Gestión del SOC
La gestión de accesos se encuentra definida acorde a los servicios que serán solicitados, y los perfiles de los roles son definidos para:

- Funcionalidades de usuarios que pueden accesar las alertas
- Activos que pueden ser accesibles por cada funcionalidad
- Gestión exclusiva de Alarmas generadas y almacenadas en los Sensores/Colectores
- Generación de Tickets según la Exposición al riesgo generado por las Alarma recibidas.

El Gestor de la Seguridad ubicado en el CERT posee una vista global mientras los analistas únicamente tienen acceso a información técnica de específicos sistemas.

El sistema de control permite que el SOC ofrezca los servicios de MSSP (Managed Security Service Provider), lo cual permite que multiples clientes utilicen dicha infraestructura, pero debido a exigencias corporativas; Es posible colectar y almacenar toda la información técnica en la infraestructura del cliente y el SOC únicamente presta los servicios de inteligencia y monitoreo en tiempo real, para garantizar un nivel extra de confidencialidad.

Nuestro Servicio
SOC/CERT 24/7

El CERT provee un sistema único de tickets y acceso a los sistemas de monitoreo de cada uno de sus clientes, para garantizar la efectividad de los servicios que ofrece, siendo estos:

- Gestión de Riesgo Tecnológico
- Correlación de Logs
- Monitoreo de Uptime
- Help Desk
- Monitoreo en tiempo real

Los servicios del SOC debido a su capacidad de gestión, poseen alto rendimiento y escalabilidad apropiada para cumplir con los SLA'S establecidos.

Y la responsabilidad del análisis y almacenamiento de la información se realiza desde el SOC, para mantener la confidencialidad e integridad de la información que procesan.

Roles en la Gestión del SOC 24/7

La gestión de accesos se encuentra definida acorde a los servicios que serán solicitados, y los perfiles de los roles son definidos para:

- Funcionalidades de usuarios que pueden accesar las alertas
- Activos que pueden ser accesibles por cada funcionalidad
- Gestión exclusiva de Alarmas generadas y almacenadas en el sistema de tickets
- Generación de Tickets según la Exposición al riesgo y Gestión de Cambios.

Contáctenos

Renato Campos
Socio de Risk Advisory
+503 2524 4177 ext. 4177
rencampos@deloitte.com

Herbert Vargas
Gerente Risk Advisory
2384 6500
hevargas@deloitte.com

Edificio Europlaza
5a Avenida 5-55 zona 14
Torre 4 nivel 15, oficinas 1501-1502
Ciudad de Guatemala

www.deloitte.com/gt

Deloitte.