CyberSOC

Seguridad gestionada 24/7

Creado para organizaciones que buscan una estrategia de ciberseguridad proactiva, CyberSOC de Gtd ofrece servicios gestionados desde una plataforma centralizada con SOC propio, infraestructura TIER III y equipos especializados operando 24/7, que permiten anticipar las amenazas y minimizar su impacto.

SERVICIOS

- **Monitoreo de Salud de Plataformas:** Revisión continua y en detalle de vulnerabilidades y eventos críticos.
- **Monitoreo SIEM (Eventos Correlacionados)**: Plataforma con inteligencia automatizada de amenazas integrada.
- **Threat Hunting – Standard:** Análisis proactivo basado en IOC's, identificando y notificando indicadores de compromiso (IP, dominios, URLs, etc.).
- **Threat Hunting – Avanzado:** nvestigación avanzada de patrones anómalos y amenazas con TTP's, herramientas del cliente (EDR, NTA, Cloud) y SLAs definidos.
- **Respuesta a Incidentes (CIRU):** Gestión integral del ciclo del incidente: detección, contención, análisis forense y recuperación, incluyendo la entrega de un informe final.
- **SecureThreat – Vigilancia Externa:** Monitoreo de amenazas externas en ámbitos como reputación y marca, disrupción del negocio y fraude online.
- **SOAR (Orquestación y Automatización):** Servicio de SOAR e implementación de Playbooks automatizados, que permiten responder de forma rápida y eficiente, minimizando riesgos.
- **Boletines de Seguridad:** Reportes con recomendaciones para decisiones informadas.

FORTALEZAS

- ISO 9001 y 27001 (+10 años)
- Miembros de First CIRU (+8 años)
- Certificación de madurez SOC-CMM 4.7/5
- +2500 Certificaciones a nivel regional
- Únicos en la region con 5 CSOC HA
- Servicio flexible y personalizado
- Dashboard ejecutivo patentado
- Equipo de respueta ante incidentes (CIRU) con experiencia regional
- Automatización de procesos minimiza el error humano
- Casos de uso basados en 3 frameworks: Mitre ATT & CK, Magma y SOC-CMM

CIRU

Cyber Incident Response Unit

Ante un incidente de ciberseguridad que pueda afectar los activos críticos de una organización, nuestro equipo de respuesta CIRU pone a disposición toda su experiencia y capacidades para lograr una recuperación rápida, segura y efectiva.

CARACTERÍSTICAS Y BENEFICIOS

- **Respuesta inmediata y especializada:** Equipo con experiencia en atención de incidentes críticos, capaz de movilizar recursos rápidamente en cualquier ubicación.
- **Expertise técnico comprobado:** Más de 390 especialistas en SIEM, protección y seguridad ofensiva, con 35.700+ horas en gestión de ciberataques en Latinoamérica.
- **Cobertura integral:** 9 disciplinas complementarias que aseguran una respuesta efectiva en todas las fases del incidente.
- **Centro de excelencia en ciberseguridad:** Asegura una amplia experiencia en inteligencia de amenazas en sectores clave como finanzas, telecomunicaciones, retail y minería. Contamos con autorización ATC Check Point e ISC2.

CONOCE **MÁS**