PLATINUM
CIBER-SEGURIDAD

Servicios de **SOC-SIEM-CERT**

Platinum provee el ciclo completo de servicios de SOC/CERT (Security Operation Center/Computer Emergency Response Team) mediante un equipo de profesionales con gran experiencia en ciberse- guridad, con la utilización de herramientas propias y de terceros que logran proporcionar el más alto nivel de servicio.
Cubrimos las tres áreas estándar de un SOC/CERT: equipo de profesionales altamente capacitados; procesos eficientes y probados, y tecnologías adecuadas y de última generación.
Como diferencial, nuestro servicio incluye una cuarta área: información de Contexto de Negocio.

EQUIPO

Nuestro equipo de trabajo cuenta con gran experiencia en la realización de las tareas del SOC/CERT. Desde las más básicas como el monitoreo de alertas o el triage, hasta las más avanza- das como el análisis, la correlación y la caza de amenazas (Threat Hunting).

CONTEXTO DE NEGOCIO

Consideramos que la información de contexto de negocio de la compañía, es fundamental a la hora de tomar decisiones sobre las medidas de protección de activos. Nuestra expererienciа de más de 10 años en el mercado desarrollando análisis de riesgo, nos permite ofrecer este componente adicional único para un SOC/CERT, de gran valor a la hora de establecer las medidas de protección y las acciones necesarias.

TECNOLOGÍA

Nuestros partners nos permiten contar con la última tecnología para atender los requerimientos necesarios en el ciber-ambiente actual, la que complementamos con otros componentes para brindar el servicio preciso que nuestros clientes necesitan. Protegen y alertan en tiempo real sobre riesgos y amenazas. Almacenan información de trazabilidad para su análisis, investigación y evidencia. Además, ofrece muchas posibilidades de análisis gráfico y matemático, permitiendo búsquedas complejas de amenazas persistentes avanzadas (APT).

PROCESOS

Poseemos procesos probados y eficientes en la definición de un SOC/CERT en la operación diaria, definiendo subprocesos de preparación, identificación, contención, erradicación y recupera- ción; inmersos en un esquema de mejora continua.
Asimismo nuestros procesos de operación están optimizados para contar con visibilidad sobre el ciber-entorno de la compañía, análisis de los eventos y acciones de respuestas rápidas y adecuadas.

IBM QRadar

PRELUDE Smart Security