Problema

- Gran volumen de ciberamenzas.
- Falta de concienciación de los empleados en ciberseguridad.
- Falta de procedimientos de actuación y conocimientos operativos en las diferentes plataformas IT.

Alternativas existentes

- Herramientas de protección (AV,IPS,FW,..).
- Programas de concienciación.
- Guías de actuación antes incidentes.

Solución

- Uso de Herramientas SIEM para centralizar eventos.
- Actuación temprana antes de que se materialicen los incidentes (Prevención).
- Procedimientos automatizados y documentados.

Recursos clave

- Equipos de SOC.
- Herramientas específicas de ciberseguridad.
- SIEM par recolección de eventos.
- Canales rápidos de comunicación.
- Procesos automatizados.

Propuesta de valor única

- Respuesta rápida ante incidentes.
- Reducción de impacto de las amenazas
- Procedimientos estandarizados.
- Mayor capacidad de tratamiento de incidentes
- Mejor postura en materia de ciberseguridad ante incidentes.
- Adaptación a las necesidades especificas de ciberseguridad de la organización.

Relación con clientes

- Servicios automatizados de peticiones a SOC de seguridad: (análisis de phishing, obtención de logs de Firewall, análisis de ficheros)
- Procedimientos automáticos y estandarizado de respuesta a incidentes

Canales

- Reportes
- Cuadros de mandos
- Servicios de mensajeria (mail, sms, teams, slack,..)

Segmentos de clientes

- Organizaciones con equipos de SOC dedicados a cuestiones de seguridad

Clientes

- Personal Operativo
- Servicios de ciberseguridad SOC

Estructura de costes

- Coste de Herramienta e infraestructura.
- Coste de equipo de ingeniería y analítica.
- Coste equipos de terceros para conectar la herramienta.

Flujos de ingresos

Se requeiere de un analisis de riesgos junto con un analisis detallado para porder estimar el retorno de la inversión (ROI) que puede generara una herramietna SOAR al igual que cualquier otra herramienta de seguridad