SHIELD FORCE T-RESPONDO

Servicios Administrados de Ciber Seguridad **Virtual CSOC**

Beneficios

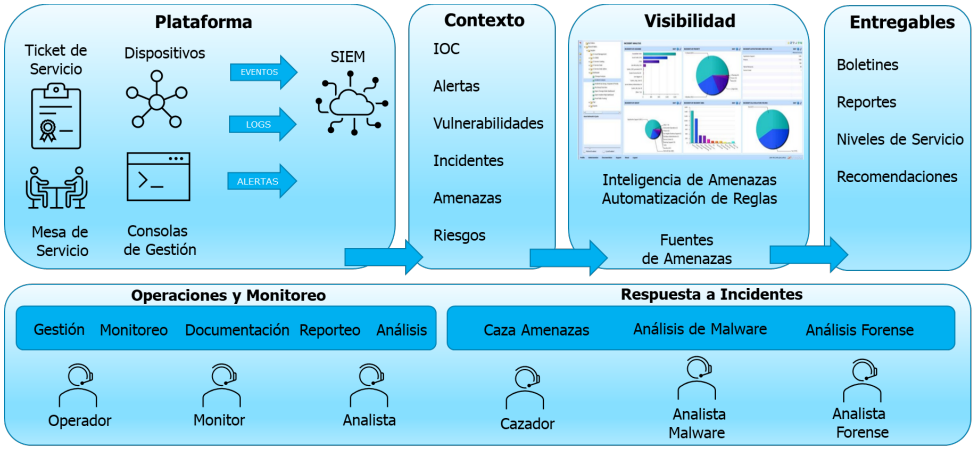
- Mejora la visibilidad.
- Optimiza el tiempo de respuesta.
- Reduce los Costos
- Reduce el riesgo y el impacto de los incidentes.
- Mejora la postura de seguridad y el nivel cumplimiento.

"*Cuanto más rápido se pueda identificar y contener un incidente, menor será el impacto y por consecuencia los costos*".

- Ponemon Institute

Servicios Gestionados de Detección y Respuesta (MDR)

Con **T-RESPONDO**, nuestro equipo de especialistas del V-CSOC diseñan, planean, implementan y operan la Consola de Gestión de las plataforma EDR, extendiendo sus capacidades, realizando detección y caza de amenazas, respuesta a incidentes, así como remediación y fortalecimiento de la postura de seguridad.



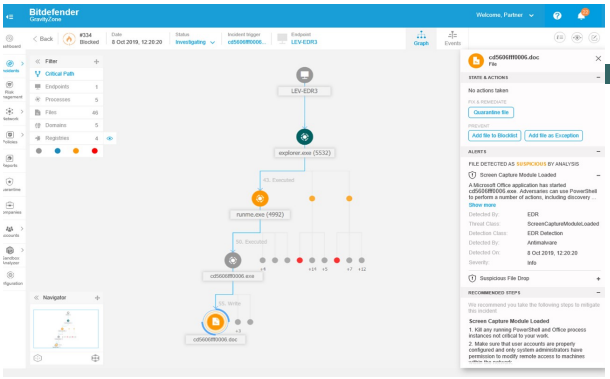
El Reto para las empresas:

- Se requiere contar con personal especialista que tenga capacitación continua.
- Hay un escasez de recursos entrenados, certificados y con experiencia
- El personal dedicado (si lo hay), debe ocuparse en labores de planeación, presupuesto, gestión del servicio orientado al negocio y no perderse en el detalle operativo.
- Los requerimientos de auditoría y cumplimiento se multiplican, lo cual incrementa la carga de trabajo
- Puede haber un exceso de alertas / notificaciones generadas por las herramientas (que pueden resultar falsos positivos).

Nuestro servicio:

- Orientado a Estaciones de Trabajo, Servidores, On Premise / VM / Cloud y Dispositivos Móviles.
- Gestión de Dispositivos protegidos por el EDR.
- Monitoreo de eventos de Seguridad, detección, investigación y alertamiento.
- Caza de Amenazas , mapeo de incidentes en "Kill Chain" y al Framework ATT&CK de MITRE.
- Respuesta a Incidentes, incluyendo análisis de malware y análisis forense.
- Gestión de Inteligencia de Amenazas (Colección, Fusión y Diseminación)
- Entregables: Reportes Mensuales, SLA's, Recomendaciones de Mejora, Boletines de Seguridad.

SHIELD FORCE



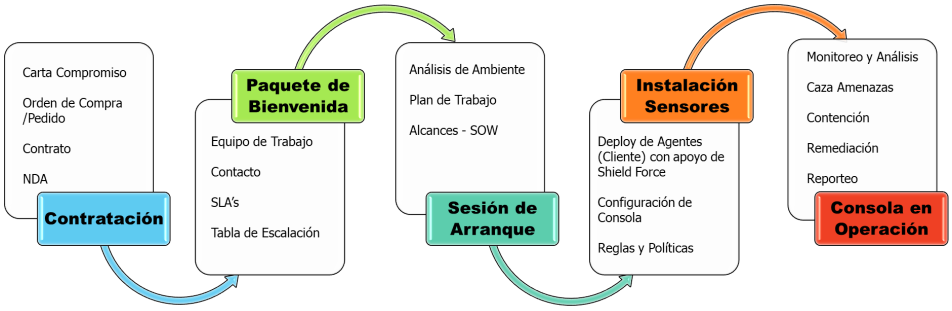
End Point Detection and Response (EDR)

Somos socios de negocio de los fabricantes Bitdefender (MSP), Blackberry , Crowdstrike, FireEye, McAfee (MSP) y Open Text, todos ellos ofrecen plataformas EDR, de las cuales estamos entrenados y certificados, tenemos experiencia, las hemos implementado y las operamos desde nuestro V-CSOC. El EDR permite realizar detección rápida e intuitiva con visibilidad de 360° desde el punto final hasta la red, y la nube. El Sensor EDR que registra datos sin procesar de los puntos finales, datos que se correlacionan con la información de las otras capas de seguridad. Proporciona visibilidad casi en tiempo real de todas las actividades sospechosas, creando automáticamente incidentes para que los equipos de seguridad los analicen más a fondo. La detección y respuesta avanzadas muestra con precisión cómo funciona una amenaza potencial y su contexto en su entorno. Las técnicas de ataque MITRE y los indicadores de compromiso brindan información actualizada al minuto sobre las amenazas con nombre y otros programas maliciosos que pueden estar involucrados. Las capacidades de búsqueda avanzada de nuestras soluciones EDR permiten realizar búsquedas de información sobre amenazas basadas en IOC, etiquetas MITRE, procesos, archivos, registro y otros parámetros durante un período prolongado (90 días) para identificar rastros de ataques o actividades sospechosas.

Expertos: los expertos certificados de **SHIELD FORCE** incluidos analistas e ingenieros de seguridad, cazadores de amenazas, analistas, investigadores y expertos en respuesta a incidentes, están directamente accesibles para usted, colaborando para su equipo de seguridad, para garantizar aún más la detección y protección oportuna, así como

Servicios T-Respondo
Arquitectura y Planeación
Implementación Remota
Soporte y Asistencia Remota
Cobertura 5x8 / 7x12 / 7x24
Reportes
Gestión Consola / Dispositivos
Monitoreo y Análisis
Caza Amenazas / Análisis de Malware (EDR)
Respuesta a Incidentes
Contención de Amenaza
Erradicación de Incidente
Análisis de Vulnerabilidades
Análisis de Malware (Profundo)
Análisis Forense

Proceso de Adopción



Contratación Simple

Activamos el servicio, aseguramos que pague por los servicios y licencias que consume cada mes

Pago sobre demanda

Facturación Mensual

Pago por consumo

No Capex

Contrato Firmado

Contrato Negociado

Mínimo un año

Descuento multianual