BASE4
SECURITY

Tu ciber aliado

CSIRT

Responde rápidamente a incidentes críticos de ciberseguridad

DIFERENCIALES

01

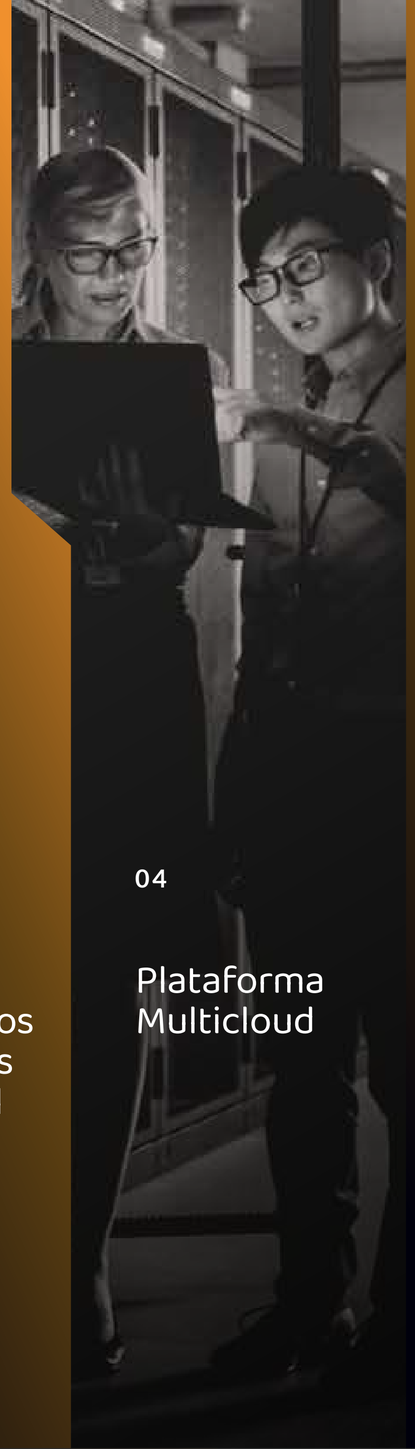
Servicio continuo 24/7/365

02

Reportes en tiempo real

03

Servicios personalizados y gestionados por Technical Account Manager



04

Plataforma Multicloud

05

Equipo de Respuesta ante Incidentes - CSIRT

06

Servicios modulares

Forensic

Análisis forense digital para la gestión de incidentes. Recoge, analiza y determina las causas e impactos de los incidentes críticos que han afectado a tu organización

CARACTERÍSTICAS DESTACADAS

- Análisis exhaustivo: Evaluación completa de las causas y el impacto del incidente
- Recolección rigurosa de evidencias: Garantizamos la integridad de las pruebas
- Informe técnico y ejecutivo: Hallazgos detallados y sugerencias para mitigar riesgos futuros

PROCESO

1. Threat Hunting: Búsqueda activa de amenazas ocultas para neutralizarlas antes del impacto
2. Detección y Análisis: Identificación e investigación de indicadores de compromiso (IoCs)
3. Contención Automática: Mitigación inmediata mediante respuestas automáticas y dirigidas
4. Informe de Resultados: Reportes periódicos dinámicos con análisis detallado

¿Por qué contratar este servicio?

- Detección proactiva y enriquecida
- Contención de incidentes en tiempo real
- Reducción de riesgos y exposición
- Cumplimiento normativo

Contáctanos

IRA Emergency

Respuesta rápida ante incidentes críticos. Nuestro servicio Emergency Incident Response está diseñado para activar rápidamente un equipo multidisciplinario de CSIRT, certificado en FIRST. Con tiempos de respuesta urgentes (SLA), garantizamos una acción inmediata para minimizar el impacto de los ataques

CARACTERÍSTICAS DESTACADAS

- Tiempos de respuesta urgentes (SLA): Compromiso de acción inmediata
- CSIRT certificado en FIRST: Equipo con amplia experiencia en gestión de incidentes
- Cobertura global: Disponibilidad sin importar la ubicación o zona horaria

PROCESO

1. Activación inmediata: Solicitud de intervención en cuestión de minutos
2. Análisis inicial: Identificación del tipo de ataque y su alcance
3. Contención y mitigación: Aislamiento del incidente para evitar propagación
4. Resolución y reporte: Informe final con hallazgos y recomendaciones

¿Por qué contratar este servicio?

- SLA inmediato
- Acceso on-demand a expertos
- Minimización de impacto financiero

Contáctanos

IRA Retainer

Análisis forense digital para la gestión de incidentes. El servicio Retainer Incident Response proporciona cobertura 24x7 y disponibilidad inmediata en caso de incidentes declarados, garantizando una respuesta continua ante ciberamenazas críticas

CARACTERÍSTICAS DESTACADAS

- Monitoreo y análisis proactivos: Evaluación constante del entorno de amenazas
- Planes personalizados: Adaptación del servicio a las necesidades específicas de la organización
- Reportes periódicos: Informes ejecutivos con recomendaciones preventivas

PROCESO

1. Evaluación inicial: Identificación de riesgos y planificación de respuesta
2. Monitoreo continuo: Supervisión 24x7 para detectar y responder a incidentes
3. Intervención inmediata: Activación del equipo CSIRT al declarar un incidente
4. Mejora continua: Revisión periódica de incidentes y actualización de estrategias

¿Por qué contratar este servicio?

- Cobertura 24x7
- Disponibilidad garantizada
- Acceso continuo a expertos

Contáctanos

Sandbox

Análisis avanzado de archivos sospechosos en entornos aislados. Detecta y analiza archivos y programas sospechosos en un entorno controlado y seguro, identificando amenazas avanzadas

CARACTERÍSTICAS DESTACADAS

- Entorno controlado y seguro: Evaluación sin riesgo para tu red o sistemas
- Análisis dinámico y detallado: Seguimiento del comportamiento de archivos sospechosos
- Detección de amenazas evadidas: Identificación de malware que escapa a otras soluciones

PROCESO

1. Carga de archivos sospechosos: Los archivos se ejecutan en un entorno aislado
2. Monitoreo del comportamiento: Observamos el impacto del archivo sobre el entorno virtual
3. Análisis detallado: Identificación de amenazas y generación de indicadores
4. Informe final: Resultados del análisis y recomendaciones para mitigar riesgos.

¿Por qué contratar este servicio?

- Detección proactiva de amenazas sofisticadas
- Protección contra ataques avanzados
- Reducción de falsos positivos
- Fortalecimiento de defensas

Contáctanos