2018

grupo ICA · CiberSOC

Servicios Avanzados de Ciberseguridad

CiberVigilancia: Completando la respuesta efectiva

LogICA NGSIEM

Recorded Future

Cifras CiberSOC

Años de vida	Personas	Clientes
ICA 35	ICA 670	ICA 200
SOC 14	Ciber 120	Ciber 90

Certificaciones

grupo ica · CiberSOC

Alta Cualificación y Especialización

Desarrollo de Plataformas Propias

Certificaciones

Alianzas Tecnológicas

100 % Español : Empresa y Productos

Servicios Avanzados de Ciberseguridad: CiberSOC

Servicios desde el CiberSOC y en el cliente

LogICA Security Analytics

Detecta, contiene y mitiga las más sofisticadas ciberamenazas en tiempo real.

LogICA End Point Protection

Securiza y descubre las amenazas del endpoint en tiempo real de manera centralizada: comportamientos, procesos, goodware y badware.

LogICA Cibervigilancia

Servicio personalizado de ciber alertas y amenazas para la prevención y detección de incidentes en tiempo real. Servicio de Defensa Activa.

Auditoría de seguridad

Servicio avanzado de auditoría y propuesta de mejoras y servicios tipo Red Team/ Blue Team/ Purple Team.

LogICA Atalaya

Servicio de auditoría externa que permite identificar y gestionar vulnerabilidades encontradas desde el perímetro de la organización.

LogICA Achilles

Servicio de gestión de vulnerabilidades y alerta temprana de red interna.

grupo ICA · CiberSOC

- *Monitorización, operación, contención y mitigación de amenazas.*
- *Gestión de eventos de seguridad 24x7x365.*
- *Personal de nivel 2 y 3 con más de 10 años de experiencia.*
- *LogICA NGSIEM, LogICA Cibervigilancia, LogICA EndPoint Protection.*
- *Expertos en hácking ético, auditoría de código fuente, ingeniería inversa, ciberinteligencia y vulnerabilidades.*
- *Servicio de emergencias ante amenazas con presencia 24x7x365.*
- *Prestación de servicios remota o insitu.*

panda

Recorded Future

Productos propios de Ciberseguridad y CiberSOC

LogICA NGSIEM

Reconocida plataforma Next Generation SIEM *permite gestionar la seguridad en tiempo real y forense.*

BoxICA

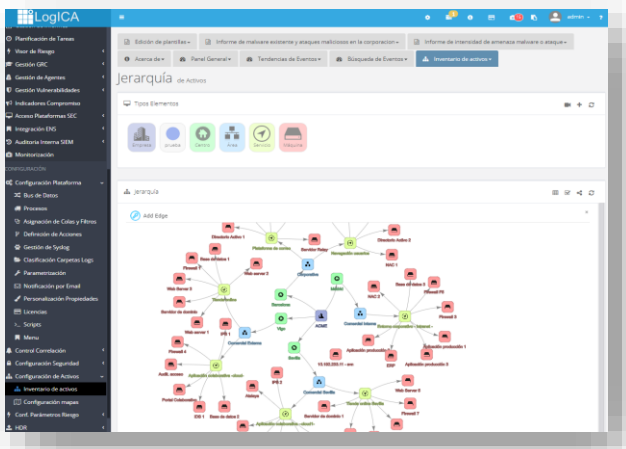
Sistema de detección de intrusiones *que permite la integración de reglas de terceros y a medida.*

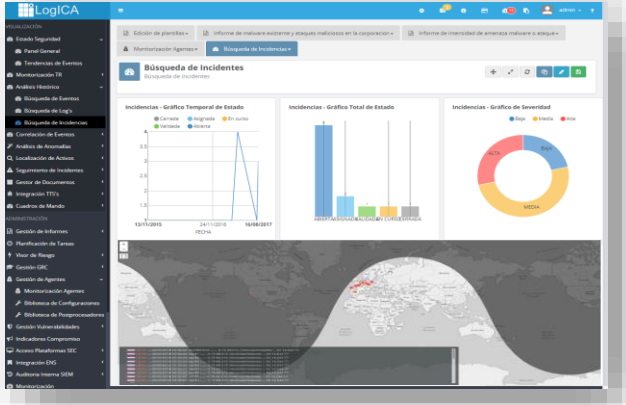
PublICA

Plataforma que evalúa Normas ISO*, Leyes o Buenas Prácticas y mide el estado del cumplimiento de forma rápida e intuitiva.*

LogICA Security Analytics

- Detección, Contención y Mitigación de Ciberamenazas.
- Basado en la plataforma de Security Analytics LogICA.
- CiberSOC de Grupo ICA: Servicios de valor añadido.
- Modalidad On Premise o en CiberSOC.
- Permite detectar, contener y mitigar ciberamenazas.
- Correlaciones complejas.
- Tecnología BigData.





Servicio Avanzado de LogICA Cibervigilancia

Métodos Tradicionales

- Humano, Recolección Limitada
- Retrasos, Paradas
- No Escala
- Basado en Reportes
- Acceso muy limitado a datos

Servicio LogICA Cibervigilancia

- Automático, recopilación masiva
- Real-time, dinámico
- Altamente escalable
- Integrado en la infraestructura y procesos de seguridad
- Acceso directo a la información y analistas expertos

Análisis por Tecnología de Aprendizaje Automático

Fuentes de información masiva

1,500+ Forums
Hacker, criminal y delincuencia, extremismo, investigación y eduacional.

50+ Sitios de "Pasteado"
Publicaciones sobre Debilidades, Brechas de Seguridad, Publicaciones de Credenciales, Listados de Ips.

Medios Sociales y Blogs
Comunidades de Seguridad, Tweets públicos, Facebook, y otras muchas.

Investigación y Análisis
Investigación y Análisis Líderes en la Industria al alcance del cliente.

Feeds de Amenazas 65+
Casi cualquier suscripción de valor añadido disponibles en web.

Recolección en DARK WEB
Miles de Referencias nuevas diarias, Canales IRC 400+.

Repositorios de Código
Compartición de código, Pruebas de Concepto, Almacenes de Aplicaciones, BDs de Vulnerabilidades y Malware PoC.

Recolecciones Técnicas
Shodan RATs, Command and Control, Google dorking, GEO IP.

Recorded Future

Alertas en tiempo real contextualizadas.

Fuentes de información en cualquier idioma.

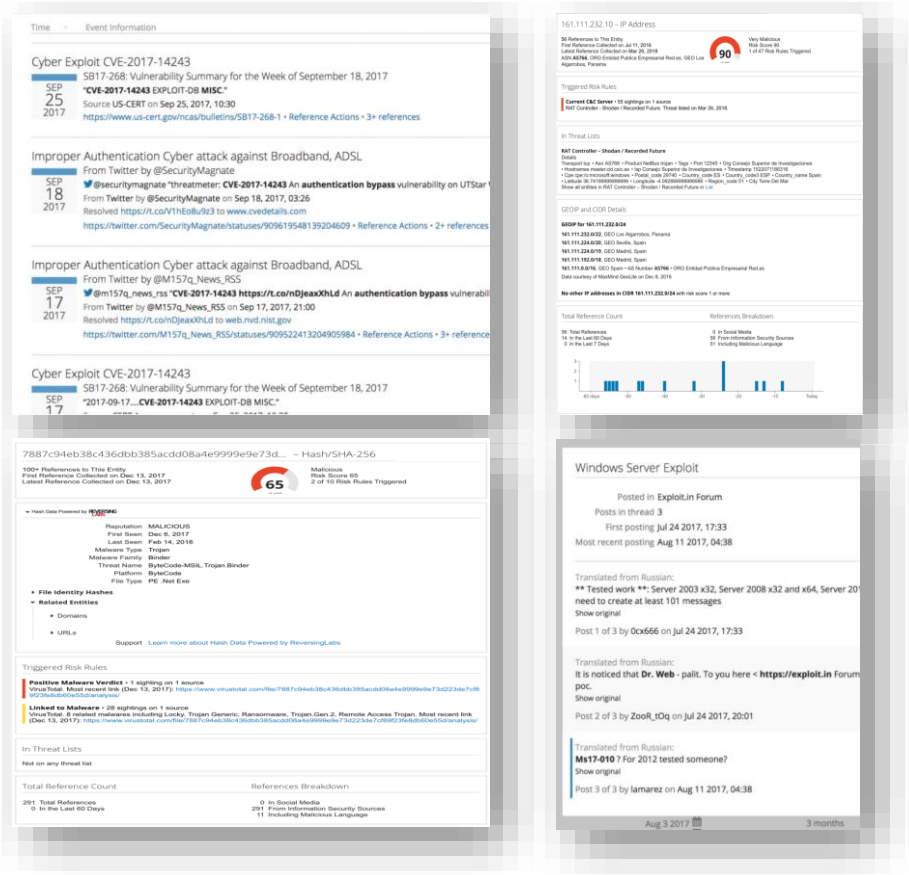
Cientos de nuevas fuentes.
Cada semana con enlace directo a los sites.

Fuentes de información masiva

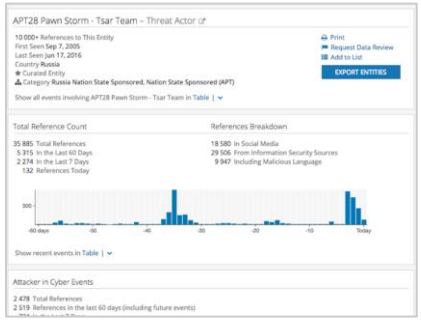
- **Análisis de amenazas en tiempo real de más de 780,000 fuentes de web**, en todos los idiomas, con **procesamiento de lenguaje natural en 12 idiomas** de alto valor (Español, Inglés, Árabe, Farsí, Iraní, Chino+, Ruso+, Francés, Alemán, Italiano, Japonés, Portugués, Sueco…)

- **Recolección automatizada de datos de fuentes globales y foros privados**: actores de amenazas, nuevas vulnerabilidades e indicadores emergentes.

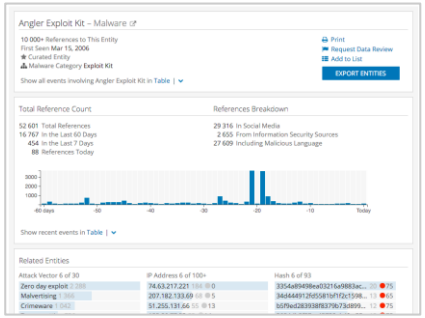
- **Alertas personalizadas sobre amenazas de ciberseguridad potenciales y de tendencias.**



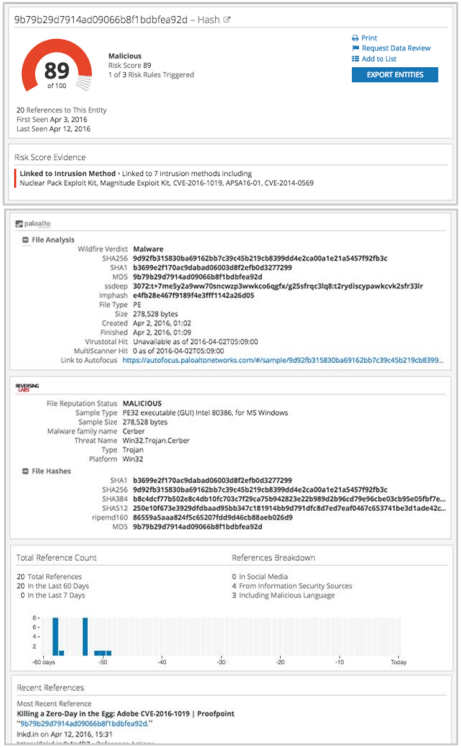
Actores (740,000+)



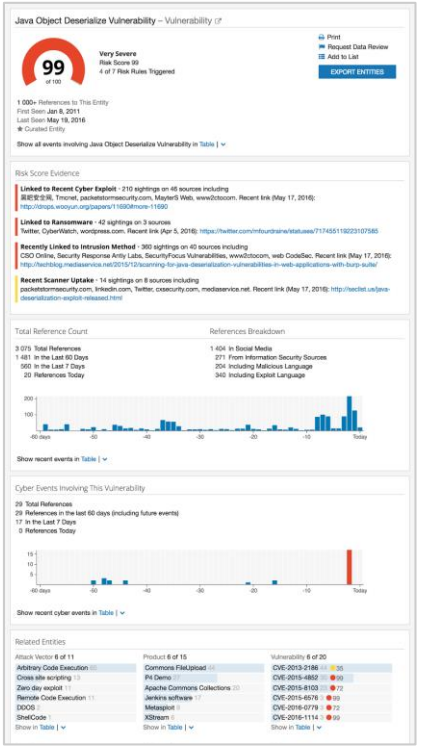
Malware (60,000+)



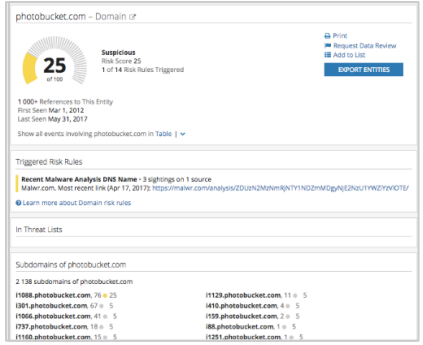
Hashes (90,000,000+)



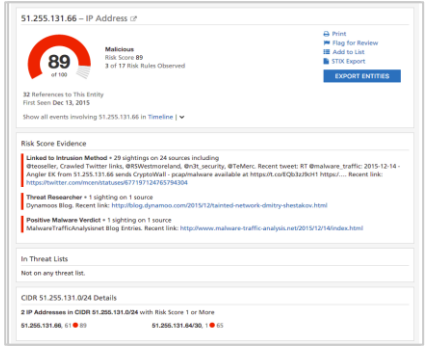
Vulnerabilidades (120,000+)



Dominios (50,000,000+)



Direcciones IP (70,000,000+)



Ventajas

Aumentar Visibilidad

Escalable

Origenes Múltiples

Soporte en multitud de lenguajes

Tiempo Real

Alertas y actualizaciones

Puntuación Dinámica del Riesgo

Integraciones SIEM

Sencillez Uso y mantenimiento

No requiere instalación

Vista global

Diálogo directo desde LogICA

Análisis Automático

Intel Cards automáticas

Acceso a expertos bajo demanda

Análisis específicos de referencias

INNOVACIÓN CONTÍNUA

Machine-learning Patentado

Analítica Predictiva

Actualizaciones de funcionalidad automáticas

Beneficios

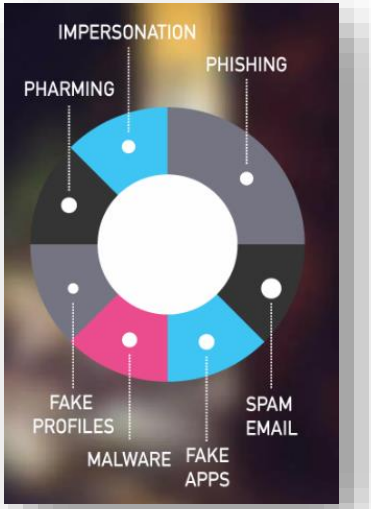
- Contexto único de trabajo
- Mejora de triaje y priorización
- Reducción de tiempo final de respuesta

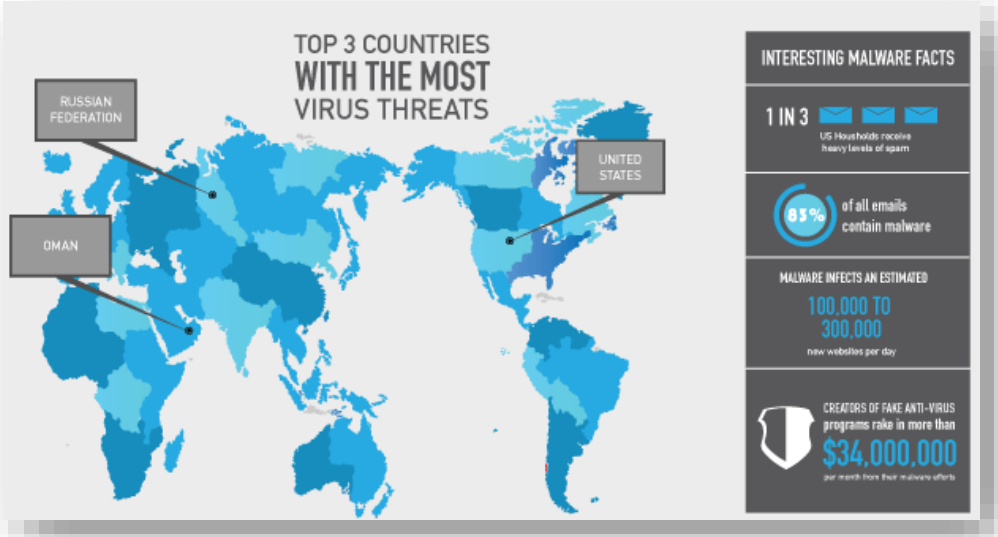
Servicio Avanzado de LogICA Cibervigilancia – *Denfensa Activa*

¿Qué es la Defensa Activa?

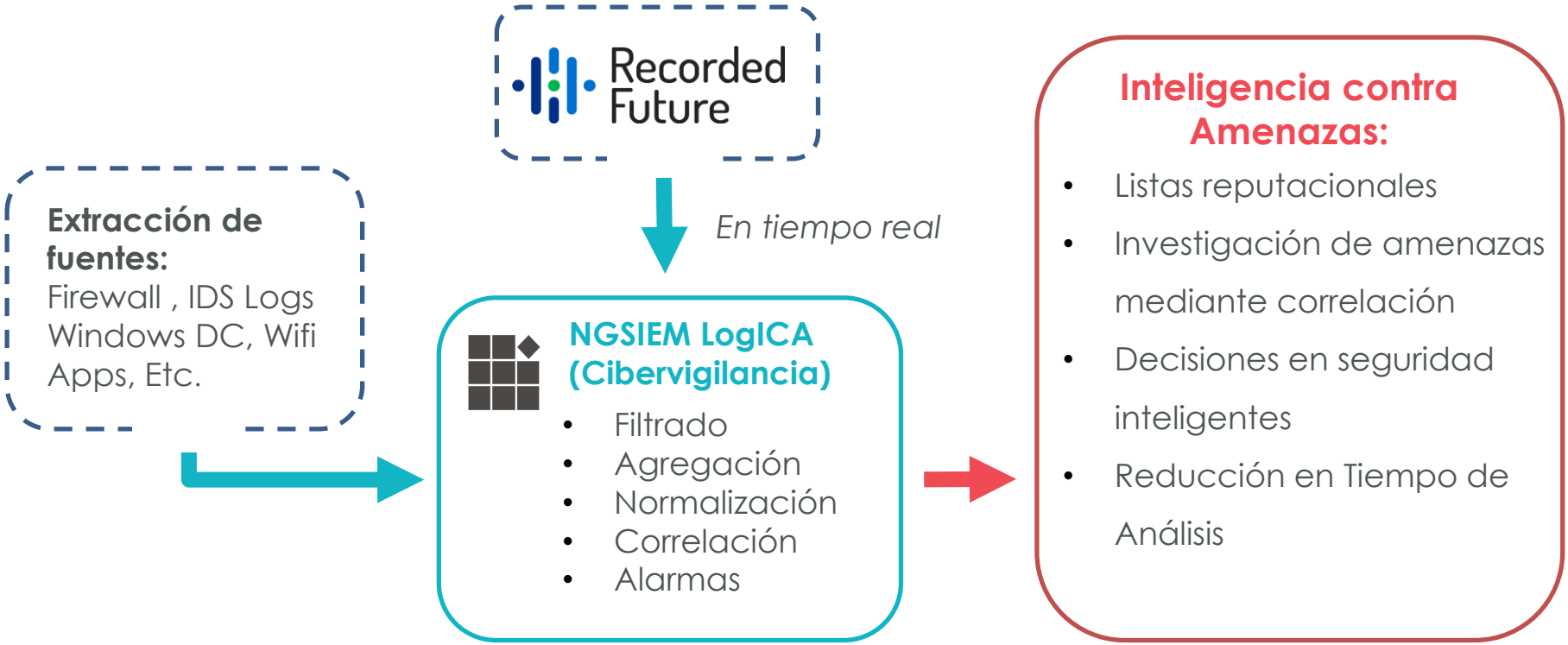
Es una **solicitud emitida** a un ISP, hosting de web, compañía de redes sociales, registrador de dominios u operador de la tienda de aplicaciones móviles **para eliminar contenido malicioso o fraudulento o dominios que abusan de la marca de una empresa**.

Un cliente necesita un *takedown* cuando **existe un dominio malicioso o una página web que utiliza su marca** (por ejemplo, un sitio de phishing), **alguien que abusa de su marca en las redes sociales o una aplicación móvil no autorizada en una App Store**.

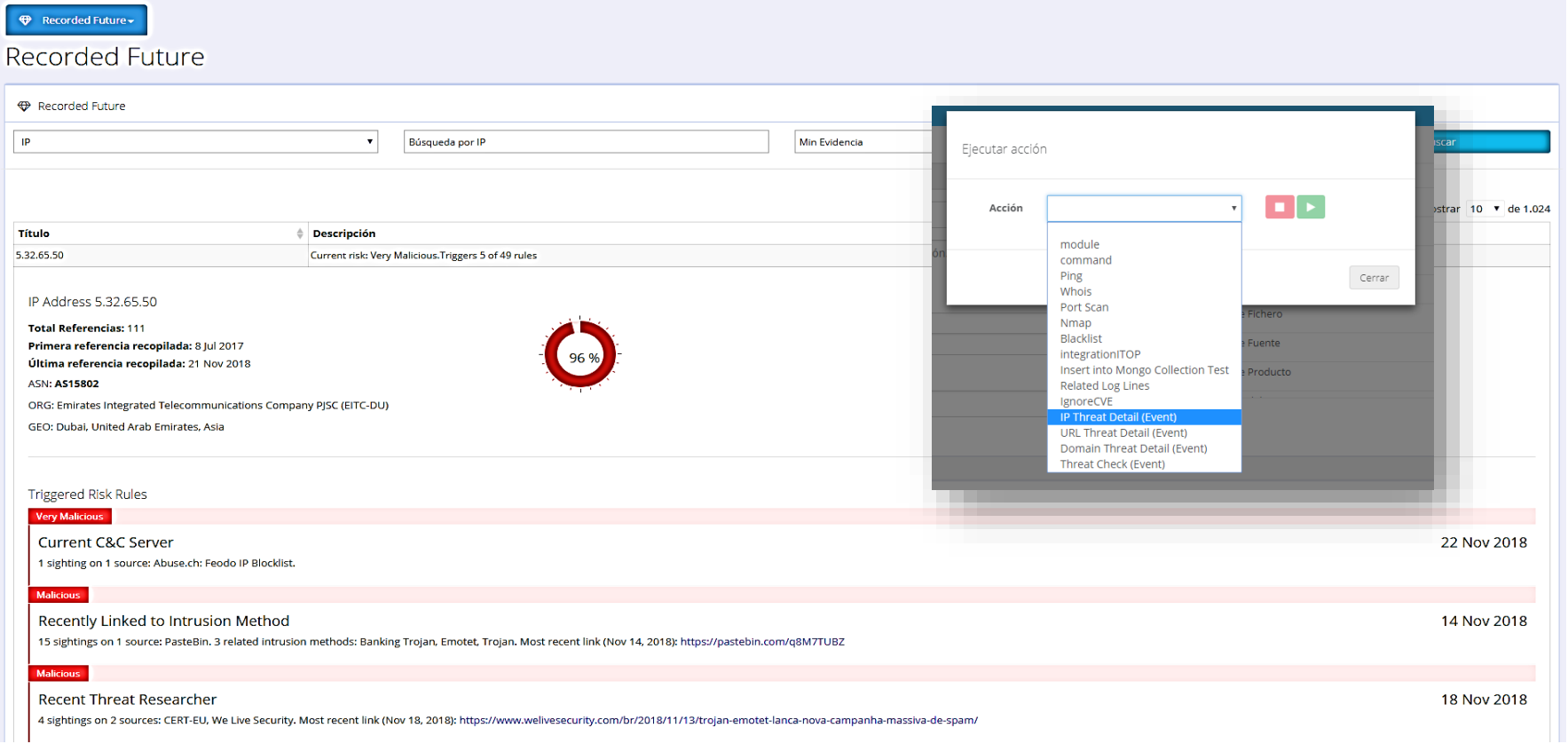




NGSIEM LogICA - Recorded Future. Integración



NGSIEM LogICA - Recorded Future. Integración



Servicios Avanzados de Ciberseguridad – Valor diferencial

Grupo ICA como empresa nacional y experta en el ámbito de la ciberseguridad aporta una serie de valores diferenciales:

- **Fabricante 100% español de los afamados productos LogICA Next Generation SIEM (más de 15 años en el mercado) y BoxICA IDS (más de 15 años en el mercado)**
- **Equipo de desarrolladores en productos de ciberseguridad** con **más de 15 años** de experiencia
- **Equipo de implantación en productos de ciberseguridad** con **más de 15 años** de experiencia
- **Experiencia en implantaciones en los más importantes organismos de la AAPP y empresa privada**, y conocedores de la casuística y problemática de la misma.
- **Implantaciones de SIEM LogICA desde 100 GB a más de 1 TB** de información diaria **tratada en tiempo real y forense**.
- **Acuerdo de Seguridad** con el **Ministerio de Defensa**
- **Habilitaciones de Personal hasta nivel NATO Secret**
- **Capacidad de adaptación de sus soluciones a necesidades del cliente**

Contacto

Sede Social

C/ La Rábida, 27
28039 Madrid
Tel: 91 311 04 87

Sede Madrid

C/ Alejandro Rodríguez, 32
Plta , 2ª-5ª-6ª
28039 Madrid
Tel: 91 311 98 44

Sede Barcelona

C/Almogàvers 119-123
Complejo Empresarial
Ecourban
Distrito 22@ - Edificio Azul
Plta 3ª Oficina 4ª
08018 Barcelona
Tel: 93 452 02 65

Sede Sevilla

C/ Gramil 18-2
Polígono Store
41008 Sevilla
Tel: 674 366 299

seguridad@grupoica.com

www.grupoica.com