



Servicios Avanzados de Ciberseguridad

CiberVigilancia: Completando la respuesta efectiva



Cifras CiberSOC



Años de vida

ICA 35

SOC 14



Personas

ICA 670

Ciber 120



Clientes

ICA 200

Ciber 90



Alta Cualificación y Especialización

Desarrollo de Plataformas Propias

Certificaciones

Alianzas Tecnológicas

100 % Español : Empresa y Productos

Certificaciones





Servicios Avanzados de Ciberseguridad: CyberSOC

Servicios desde el CyberSOC 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.



- 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 NGSIM, LogICA Cibervigilancia, LogICA EndPoint Protection.
- Expertos en hacking ético, auditoría de código fuente, ingeniería inversa, ciberinteligencia y vulnerabilidades.
- Servicio de emergencias ante amenazas con presencia 24x7x365.
- Prestación de servicios remota o insitu.



Productos propios de Ciberseguridad y CiberSOC



LogICA NGSiem

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



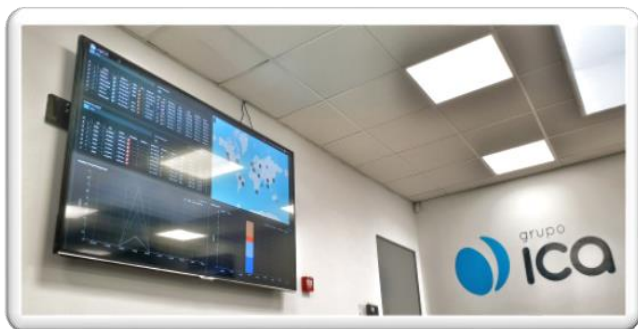
BoxICA

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



PubICA

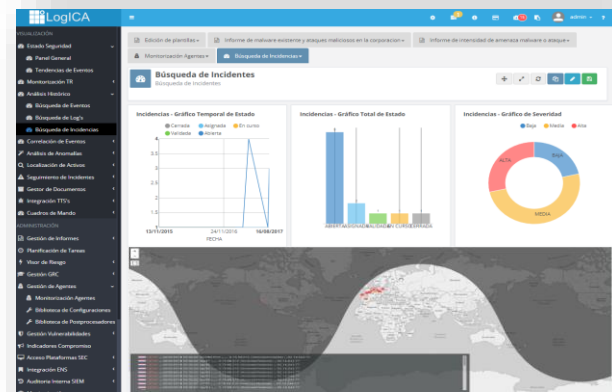
Plataforma que evalúa Normas ISO, Leyes o Buenas Prácticas y mide el estado del cumplimiento de forma rápida e intuitiva.





LogICA Security Analytics

- Detección, Contención y Mitigación de Ciberamenazas.
- Basado en la plataforma de Security Analytics LogICA.
- CyberSOC de Grupo ICA: Servicios de valor añadido.
- Modalidad On Premise o en CyberSOC.
- 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 educacional.



Feeds de Amenazas 65+

Casi cualquier suscripción de valor añadido disponibles en web.



50+ Sitios de “Pasteado”

Publicaciones sobre Debilidades, Brechas de Seguridad, Publicaciones de Credenciales, Listados de Ips.



Recolección en DARK WEB

Miles de Referencias nuevas diarias, Canales IRC 400+.



Medios Sociales y Blogs

Comunidades de Seguridad, Tweets públicos, Facebook, y otras muchas.



Repositorios de Código

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



Investigación y Análisis

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



Recolecciones Técnicas

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



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, 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.**

The image displays three screenshots of the LogICA security dashboard. The top-left screenshot shows a 'Cyber Exploit CVE-2017-14243' vulnerability summary for the week of September 18, 2017, with a severity score of 25. It lists references to US-CERT and other sources. The top-right screenshot shows a '161.111.232.10 - IP Address' analysis with a severity score of 90, indicating a high risk of a risk factor being triggered. The middle-left screenshot shows a '7887c94eb38c436dbb385acdd084e9999e9e73d...' hash analysis with a severity score of 65, identifying it as a Malicious Risk Score 65. The middle-right screenshot shows a 'Windows Server Exploit' alert posted in an exploit forum, with a severity score of 65. The bottom-left screenshot shows a 'Triggered Risk Rules' section with a severity score of 25, listing rules like 'Positive Malware Verdict' and 'Linked to Malware'. The bottom-right screenshot shows a 'References Breakdown' section with a severity score of 291, indicating 291 total references from information security sources.



Actores (740,000+)

APT28 Pawn Storm - Tsar Team - Threat Actor of

1000+ References to This Entry
First Seen Sep 3, 2015
Last Seen Jun 17, 2016
Country: Russia
Curated Entry

Category: Russia Nation State Sponsored, Nation State Sponsored (APT)

Show all events involving APT28 Pawn Storm - Tsar Team in Table | <

Print | Request Data Review | Add to List | EXPORT ENTITIES

Total Reference Count: 53 601 Total References: 18 202 In the Last 60 Days: 16 767 In the Last 7 Days: 424 In the Last 24 Hours: 150

References Breakdown: 29 216 in Social Media, 2 605 from Information Security Sources, 27 609 including Malicious Language

Attackers in Cyber Events: 2 478 Total References: 2 519 References in the last 60 days (including future events): 1 502

Malware (60,000+)

Angler Exploit Kit - Malware of

10 000+ References to This Entry
First Seen Mar 15, 2006
Curated Entry

Malware Category: Exploit Kit

Show all events involving Angler Exploit Kit in Table | <

Print | Request Data Review | Add to List | EXPORT ENTITIES

Total Reference Count: 53 601 Total References: 18 202 In the Last 60 Days: 16 767 In the Last 7 Days: 424 In the Last 24 Hours: 150

References Breakdown: 29 216 in Social Media, 2 605 from Information Security Sources, 27 609 including Malicious Language

Related Entries: Attack Vector 6 of 30, Zero day exploit 1 of 9, Malware 1 of 9, Cmsmware 1 of 9

Hashes (90,000,000+)

9b79b29d7914a090668b71bd0fe922d - Hash of

Malicious Risk Score: 89 (1 of 3 Risk Rules Triggered)

20 References to This Entry
First Seen Apr 3, 2016
Last Seen Apr 12, 2016

Risk Score Evidence: **Linked to Intrusion Method** - Linked to 7 intrusion methods including Nuclei Pack Exploit Kit, Magnitude Exploit Kit, CVE-2016-1019, AFS-16-01, CVE-2014-0569

File Analysis: Wildfire Verdict: Malware, SHA256: 94023315830ba49162b7c39c45215b4399664e2ca0a1e214545792f83c, SHA1: 83699c2f170acabab450038f72f6b32727299, MD5: 9b79b29d7914a090668b71bd0fe922d, sha256: 207c217m5y9zw7ow70ncw3jwckvcqkgq/gz5frcc3lqz3rdyvisopawckv4z3fr, ImpHash: 4ef28c667f91949610ff114a2b2655, Risk Type: PE, Size: 278,528 bytes, Created: Apr 2, 2016, 01:32, Finished: Apr 2, 2016, 01:09, Virtualized: Unavailable as of 2016-04-02T20:09:00, MultiScanner: C/C++ of 2016-04-02T05:09:00, Link to Autofocus: https://autofocus.palantir.com/#/sample/9b79b29d7914a090668b71bd0fe922d

Vulnerabilidades (120,000+)

Java Object Deserialization Vulnerability - Vulnerability of

Very Severe Risk Score: 99 (4 of 7 Risk Rules Triggered)

1 000+ References to This Entry
First Seen Jan 8, 2011
First Seen May 18, 2016
Curated Entry

Show all events involving Java Object Deserialization Vulnerability in Table | <

Print | Request Data Review | Add to List | EXPORT ENTITIES

Risk Score Evidence: **Linked to Recent Cyber Exploit** - 210 sightings on 46 sources including CVE-2016-0755, Trend, packstack.com, Metasploit Web, web2team, Recur Inc (May 17, 2016), http://trops.wowjagroups.com/15000/1-1690, **Linked to Ransomware** - 42 sightings on 3 sources: Telnet, CyberWatch, wopress.com, Recur Inc (Apr 5, 2016), https://thecloud.com/our/news/2016/07/14/5510223-0738, **Recently Linked to Intrusion Method** - 300 sightings on 42 sources including CSO Online, Security Response Arty Labs, SecurityFocus Vulnerabilities, wordcloud.com, WebCodecs, Recur Inc (May 17, 2016), http://netbug.mediaviva.net/2016/12/learning-to-java-deserialization-vulnerabilities-in-web-applications-with-burp-suit/, **Recent Scanner Update** - 14 sightings on 8 sources including goste.com, intel.com, Telnet, security.com, mediaviva.net, Recur Inc (May 17, 2016), http://reacted.us/2016-deserialization-exploit-released.html

Total Reference Count: 3 074 Total References: 1 481 In the Last 60 Days: 271 In the Last 7 Days: 204 Including Malicious Language: 340

References Breakdown: 1 404 in Social Media, 271 from Information Security Sources, 204 including Malicious Language, 340 including Exploit Language

Cyber Events Involving This Vulnerability: 29 Total References: 29 In the last 60 days (including future events): 17 In the Last 7 Days: 0 References Today

Related Entries: Attack Vector 6 of 11, Arbitrary Code Execution 10 of 15, Remote Code Execution 11 of 15, DNS site scripting 1 of 1, Zero-day exploit 1 of 1, Remote Code Execution 11 of 15, DDoS 1 of 1, ShellCode 1 of 1, Product 6 of 15, CommonJS Framework 4 of 30, CVE-2013-5186 1 of 30, CVE-2015-4820 1 of 30, CVE-2015-8103 1 of 7, CVE-2015-4674 1 of 3, CVE-2016-0776 1 of 3, CVE-2016-1114 1 of 3

Dominios (50,000,000+)

photobucket.com - Domain of

Suspicious Risk Score: 25 (1 of 14 Risk Rules Triggered)

1 000+ References to This Entry
First Seen Mar 13, 2012
Last Seen May 31, 2017

Show all events involving photobucket.com in Table | <

Print | Request Data Review | Add to List | EXPORT ENTITIES

Triggered Risk Rules: **Recent Malware Analysis DNS Name** - 3 sightings on 1 source: Water.com, Most recent link (Apr 17, 2017), https://water.com/analysis/2016/22/mehh9n1y1nd0m3w6/e123u11w2ywyw7/, **Learn more about domain risk rules**

In Threat Lists

Subdomains of photobucket.com

2 138 subdomains of photobucket.com

1088.photobucket.com 78 of 25	1129.photobucket.com 11 of 5
1091.photobucket.com 17 of 5	110.photobucket.com 4 of 5
1106.photobucket.com 41 of 5	109.photobucket.com 2 of 5
737.photobucket.com 18 of 5	88.photobucket.com 1 of 5
1108.photobucket.com 15 of 5	1251.photobucket.com 1 of 5

Direcciones IP (70,000,000+)

51.255.131.66 - IP Address of

Malicious Risk Score: 89 (2 of 17 Risk Rules Observed)

32 References to This Entry
First Seen Dec 18, 2015

Show all events involving 51.255.131.66 in Timeline | <

Print | Flag for Review | Add to List | STIX Export | EXPORT ENTITIES

Risk Score Evidence: **Linked to Intrusion Method** - 29 sightings on 24 sources including @secwiki, Cissland Twitter link, @VirusShareBot, @CIS, security, @Hacker, Recur Incet 07: @hacker, Recur Incet 07: @hacker, traffic, 2015-12-14, Angler EK from 51.255.131.66 sends CryptWall - postexploit/malware available at https://c0d3r04h171 https://... , Recur Inc, https://twitter.com/commsint/updates/7191242657804, **Trojan Responder** - 1 sighting on 1 source: @Dynamis Blog, Recur Inc, http://blog.dynamis.com/2015/12/hatched-network-dropt-whatstake.html, **Positive Malware Verdict** - 1 sighting on 1 source: MalwareTrafficAnalysis.net Blog Entry, Recur Inc, http://www.malware-traffic-analysis.net/2015/12/17/4.html

In Threat Lists

Not on any threat list.

CDR 51.255.131.024 Details

2 of 2 Addresses in CDR 51.255.131.024 with Risk Score 1 or More

51.255.131.66 1 of 3 | 51.255.131.64/30 1 of 3

File Reputation Status: MALICIOUS

Sample Type: PE32 executable (GUI) Intel x86, for MS Windows
Sample Size: 278,528 bytes
Malware Family Name: Center
Threat Name: Win32/Trojan.Center
Type: Trojan
Platform: Win32

File Hashes: SHA1: 83699c2f170acabab450038f72f6b327299, SHA256: 94023315830ba49162b7c39c45215b4399664e2ca0a1e214545792f83c, SHA384: 846c4775f2028c48c40b700172707593432823238992964c079646b40b9e55b7e..., SHA512: 250110f73c9397f2ba689534b7c187184089791fd6d7e4d0467653741be341a4e42c..., ripemd160: 80559a8a28f2c02076964c68ba08026d9, MD5: 9b79b29d7914a090668b71bd0fe922d

Total Reference Count: 20 Total References: 20 In the Last 60 Days: 0 In the Last 7 Days: 3

References Breakdown: 0 in Social Media, 4 from Information Security Sources, 3 including Malicious Language

Recent References: Most Recent Reference: **Killing a Zero-Day in the Egg: Adobe CVE-2016-1019 | Proofpoint** "9b79b29d7914a090668b71bd0fe922d" In: In on Apr 12, 2016, 15:31



Ventajas



Aumentar Visibilidad

Escalable
Orígenes
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



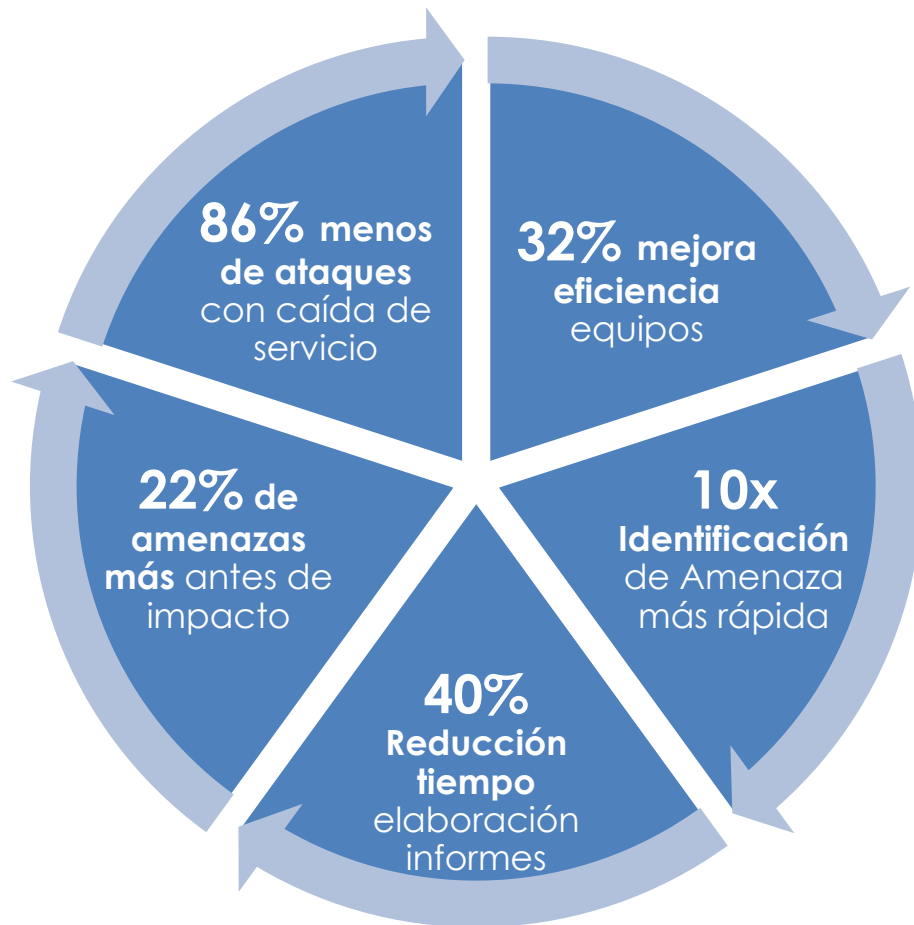
INNOVACIÓN CONTÍNUA

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



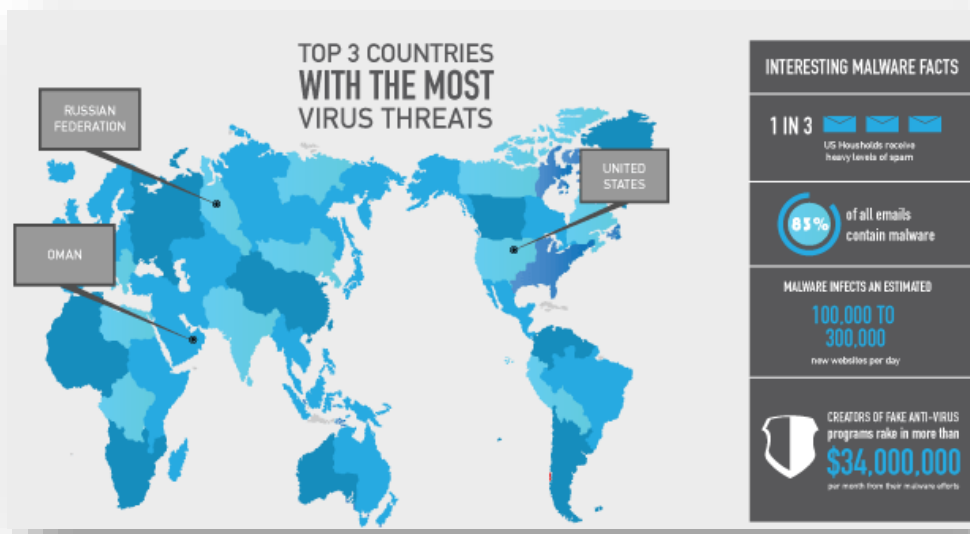
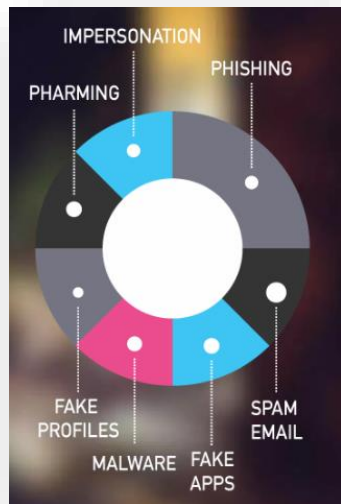


Servicio Avanzado de LogICA Cibervigilancia – *Defensa Activa*

¿Qué es la Defensa Activa?

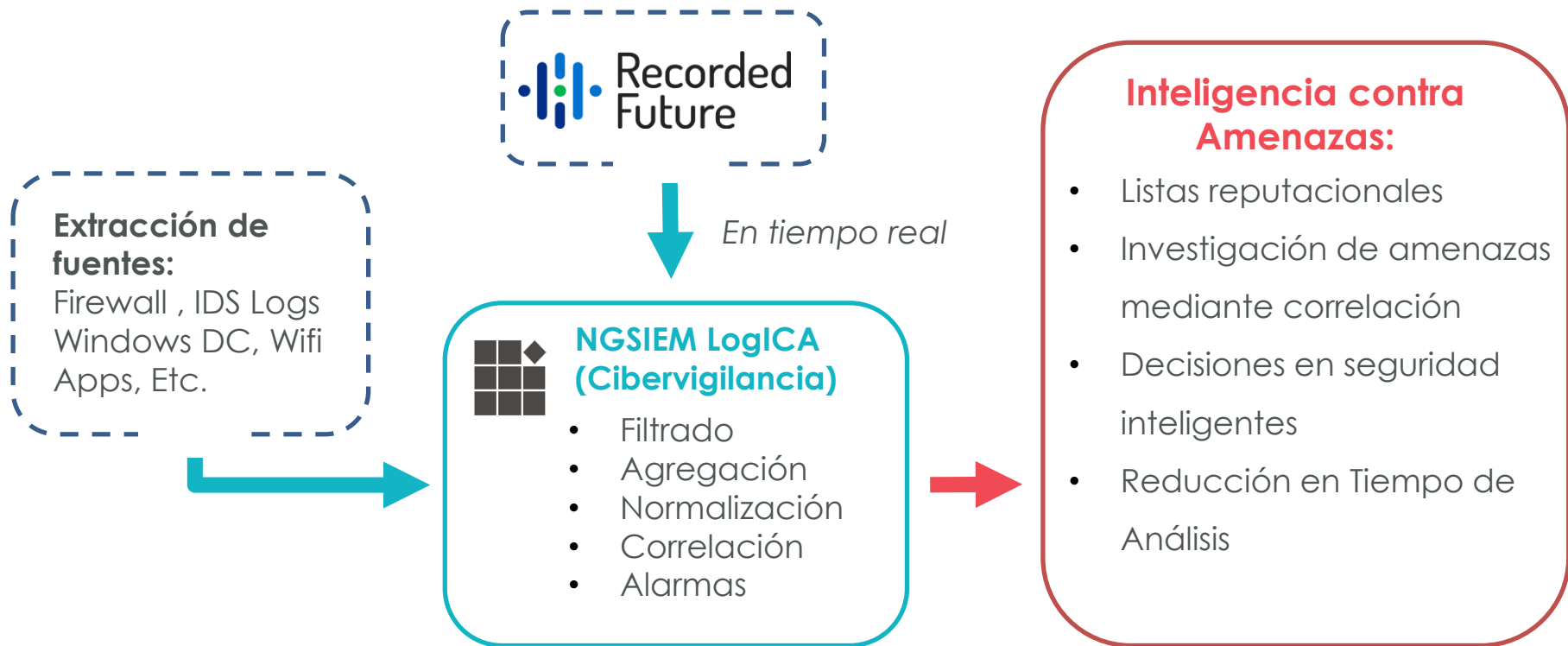
Es una **solicitud emitida** a un ISP, hosting de web, compañía de redes sociales, registrador de dominios u operador de la tienda de aplicaciones móviles **para eliminar contenido malicioso o fraudulento o dominios que abusan de la marca de una empresa.**

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

Recorded Future

Recorded Future

Recorded Future

Título	Descripción
<p>5.32.65.50</p> <p>IP Address 5.32.65.50</p> <p>Total Referencias: 111 Primera referencia recopilada: 8 Jul 2017 Última referencia recopilada: 21 Nov 2018</p> <p>ASN: AS15802</p> <p>ORG: Emirates Integrated Telecommunications Company PJSC (EITC-DU) GEO: Dubai, United Arab Emirates, Asia</p>	<p>Current risk: Very Malicious.Triggers 5 of 49 rules</p> <div style="text-align: center; margin: 20px 0;"> <p>96 %</p> </div> <p>Triggered Risk Rules</p> <div style="background-color: #f8d7da; padding: 5px; margin-bottom: 5px;"> <p>Very Malicious</p> <p>Current C&C Server 1 sightings on 1 source: Abuse.ch: Feodo IP Blocklist. 22 Nov 2018</p> </div> <div style="background-color: #fff3f3; padding: 5px; margin-bottom: 5px;"> <p>Malicious</p> <p>Recently Linked to Intrusion Method 15 sightings on 1 source: PasteBin. 3 related intrusion methods: Banking Trojan, Emotet, Trojan. Most recent link (Nov 14, 2018): https://pastebin.com/q8M7TUBZ 14 Nov 2018</p> </div> <div style="background-color: #fff3f3; padding: 5px;"> <p>Malicious</p> <p>Recent Threat Researcher 4 sightings on 2 sources: CERT-EU, We Live Security. Most recent link (Nov 18, 2018): https://www.welivesecurity.com/br/2018/11/13/trojan-emotet-lanca-nova-campanha-massiva-de-spam/ 18 Nov 2018</p> </div>

Ejecutar acción

Acción
▼

- module
- command
- Ping
- Whois
- Port Scan
- Nmap
- Blacklist
- IntegrationITOP
- Insert into Mongo Collection Test
- Related Log Lines
- IgnoreCVE
- IP Threat Detail (Event)
- URL Threat Detail (Event)
- Domain Threat Detail (Event)
- Threat Check (Event)

■ ▶



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**



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
Ecurban
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

