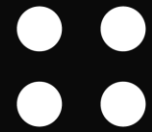


ABOX

Servicios Informáticos



CYBEROO



EL NÚMERO DE ATAQUES HACKING REGISTRADOS ESTÁN CONSTANTEMENTE CRECIENDO POR TODO EL MUNDO, NO FORMES PARTE DE ELLOS

2.779

ataques severos
(+12%
comparado
al 2022)

81%

Ataques con
impacto severo y/o
crítico en 2023

83%

Ataques
ciber-
criminales
(2316 en total)

36%

Ataques Malware,
el tipo de ataque
principal registrado en
2023

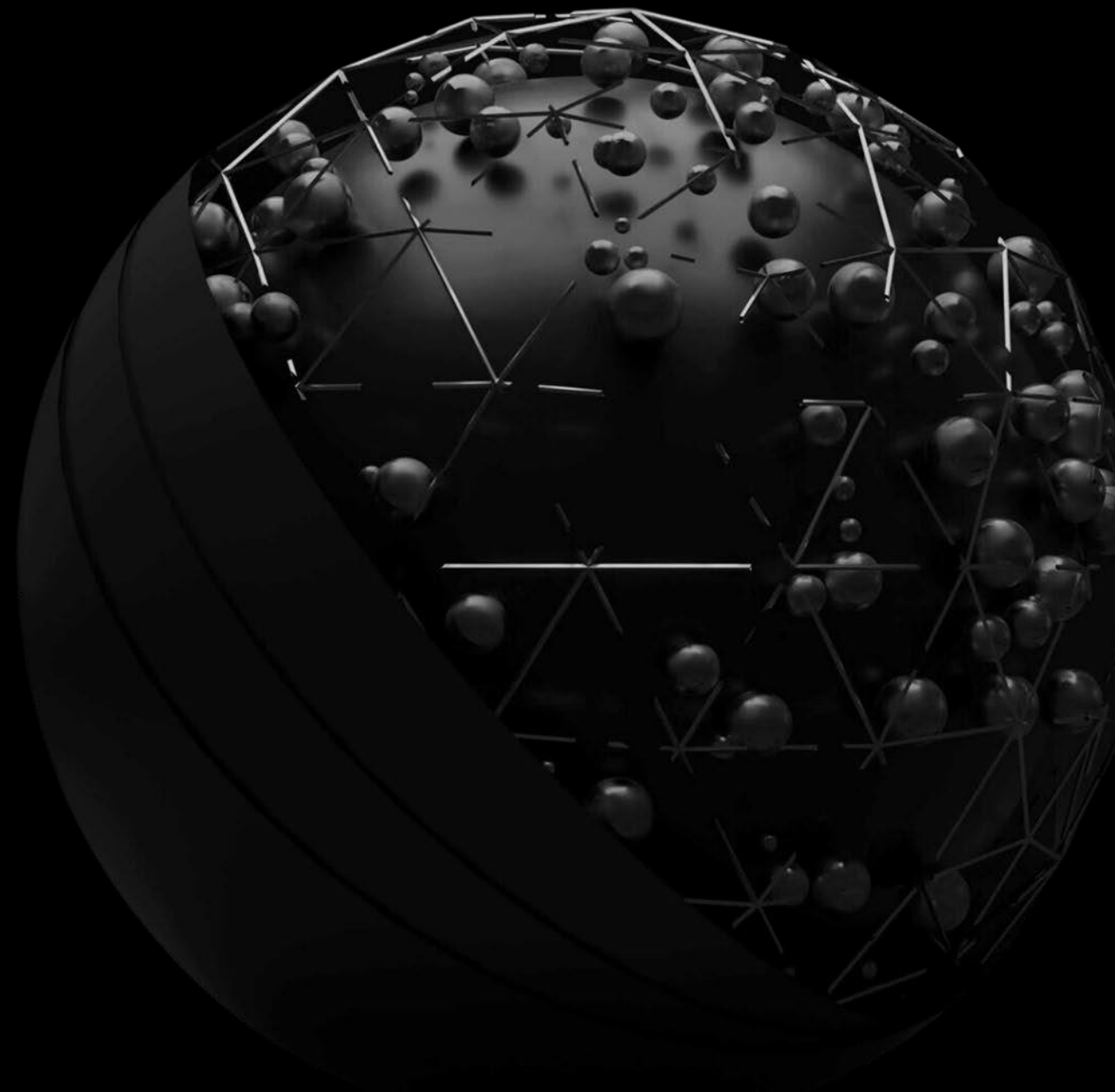


SU SEGURIDAD ES UN PROBLEMA QUE AFECTA A TODA LA CADENA DE SUMINISTRO

En muchos casos, se explota a las pymes para acceder a la red más amplia a la que prestan servicio.

Por lo tanto, las auditorías y certificaciones se convierten en una importante ventaja competitiva.

A partir de octubre de 2024, una buena postura de seguridad no solo es obligatoria y valorada por clientes y proveedores, sino que se convierte en una directiva con la aplicación de la NIS2. Esta directiva de la Comunidad Europea tiene como objetivo garantizar una gestión adecuada de riesgos en la cadena de suministro.



CÓMO PUEDES INCREMENTAR TU NIVEL DE RESILIENCIA?



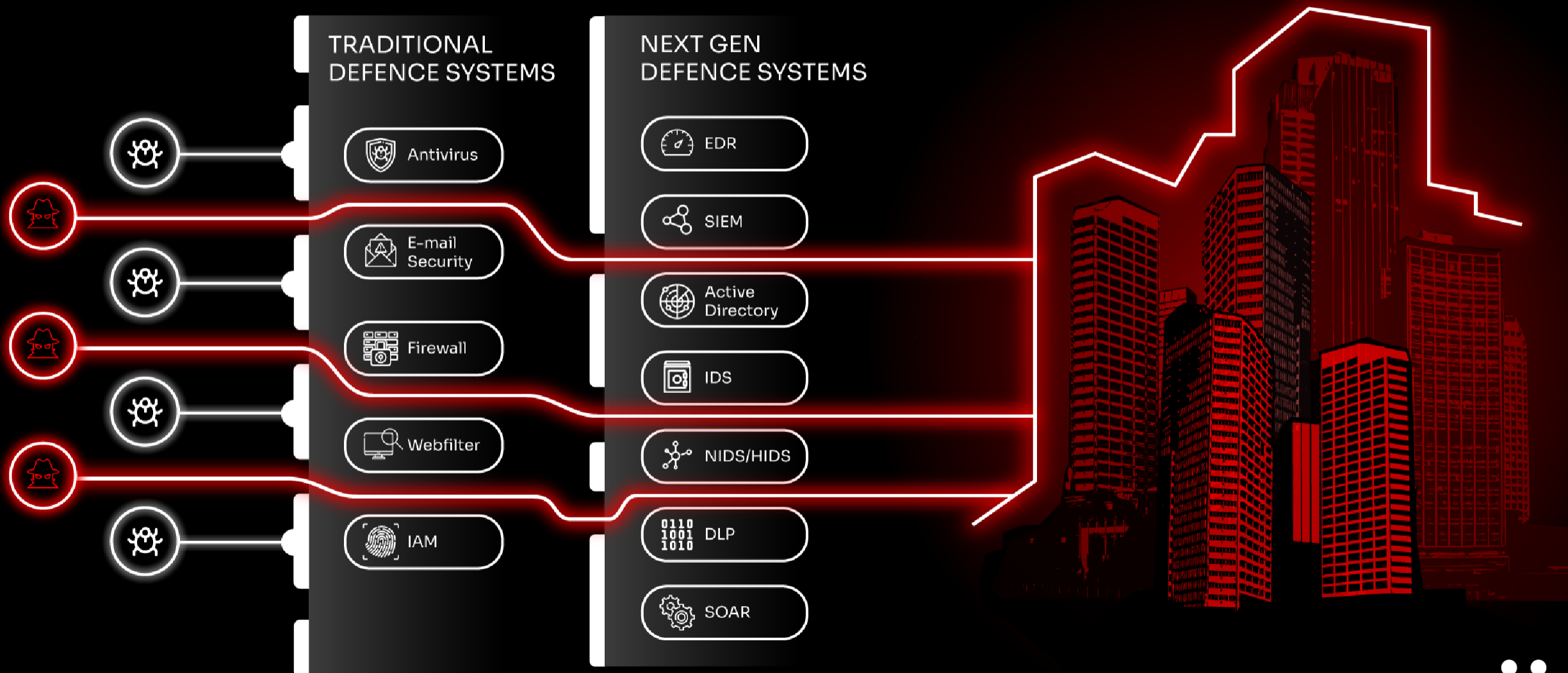
ERES SEGURO, ESPECIALMENTE EN LAS TECNOLOGÍAS DONDE CREES QUE ERES INSEGURO



Known
threats



Advanced
threats



LA CADENA DE ATAQUES CIBERNÉTICOS

Los ciberataques son procesos complejos compuestos de tácticas, técnicas y procedimientos.



PARA SER GANADOR, NECESITAS DESAFIAR EL COMPORTAMIENTO DE TUS Oponentes

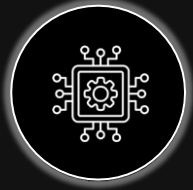
La capacidad de contrarrestar a un hacker criminal varía según el nivel de acción. Su complejidad influye en la capacidad de poner al hacker en dificultades.



SEGÚN GARTNER, EXISTE LA NECESIDAD DE UN SERVICIO AVANZADO QUE FUSIONE ESTOS TRES PILARES



Escanea el Código QR
para descargar el reporte Gartner



ADVANCED TECH

Tecnología Agnóstica

Sólo un sistema basado en una tecnología completamente agnóstica, permite la correlación de innumerables fuentes de información, y por tanto una visión holística.



PERSONAS

Especialista de Ciberseguridad

La ciberseguridad ya no se limita a la TI. Se requieren competencias específicas para identificar y mitigar todas las amenazas en un entorno empresarial determinado.



SIEMPRE ACTIVO

Proceso 24/7/365

El 76% de los ataques de ransomware ocurridos entre 2017 y 2019 tuvieron lugar durante la noche o el fin de semana.



SOMOS CYBEROO



1r proveedor de
ciberseguridad que cotiza en
la Bolsa de Valores de Italia



+200 recursos
altamente
calificados



+700 clientes de
tamaño mediano y
empresas



5 ubicaciones
en EMEA



Guía de Mercado de
Gartner para Servicios
MDR



CYBEROO
es CERT



Tecnologías
propias y
certificadas



Cumple con
GDPR

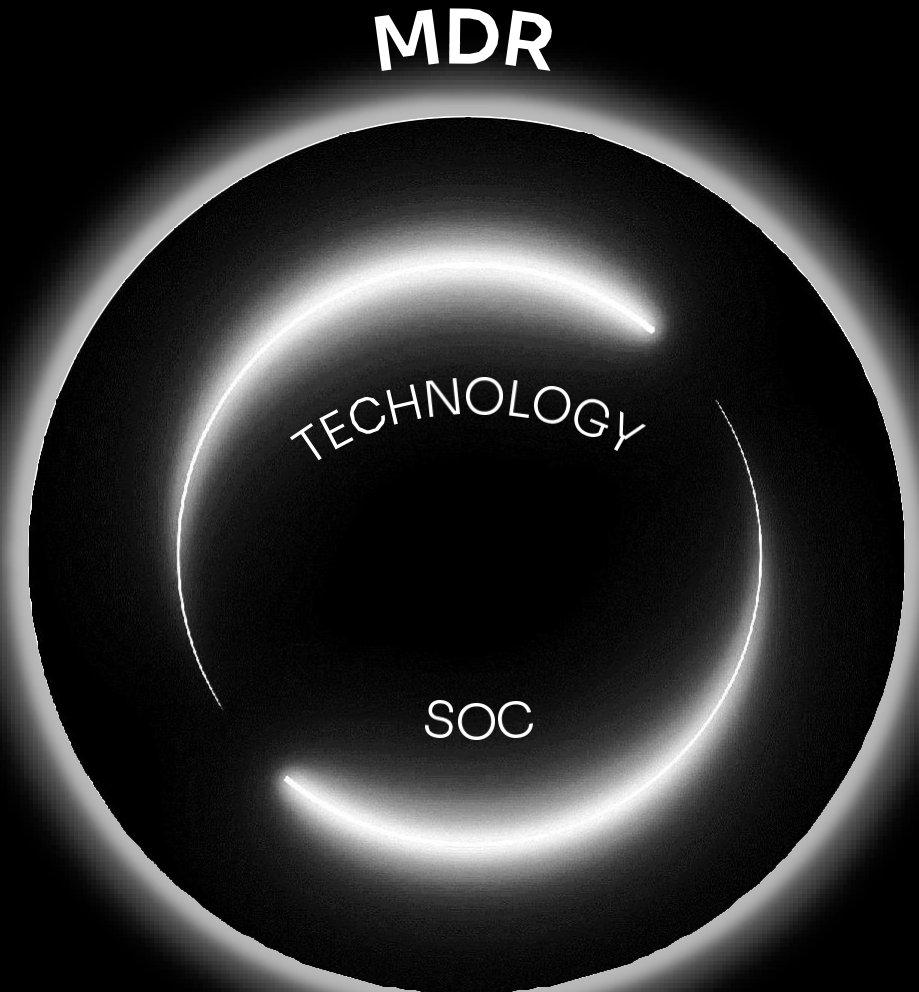


EL TODO ES MAYOR QUE LA SUMA DE SUS PARTES

CYBEROO fusiona los tres pilares fundamentales en un **único servicio**, que va mucho más allá de la gestión de simples tecnologías heterogéneas.

Nuestra solución **va más allá del concepto de tecnología** y analiza contextos complejos para identificar técnicas, tácticas y procedimientos de los piratas informáticos criminales.

PARA DERROTARLOS SIEMPRE.



DETECCIÓN 24/7

Nuestro sistema MDR monitorea y analiza su ciberseguridad las 24/7



ANÁLISIS 24/7

Nuestro equipo de especialistas estudia cualquier posible anomalía detectada por nuestros sistemas para identificar cualquier posible tipo de amenaza.



REMEDIACIÓN 24/7

Si se detecta una amenaza, tomamos medidas inmediatas las 24/7, para resolver el problema lo antes posible.



EN UN SÓLO SERVICIO





CYBER
SECURITY
SUITE

**NUESTRO MDR LE PROTEGE DE AMENAZAS INTERNAS Y EXTERNAS.
NO DEJAMOS ESPACIO PARA ZONAS DE SOMBRA.**

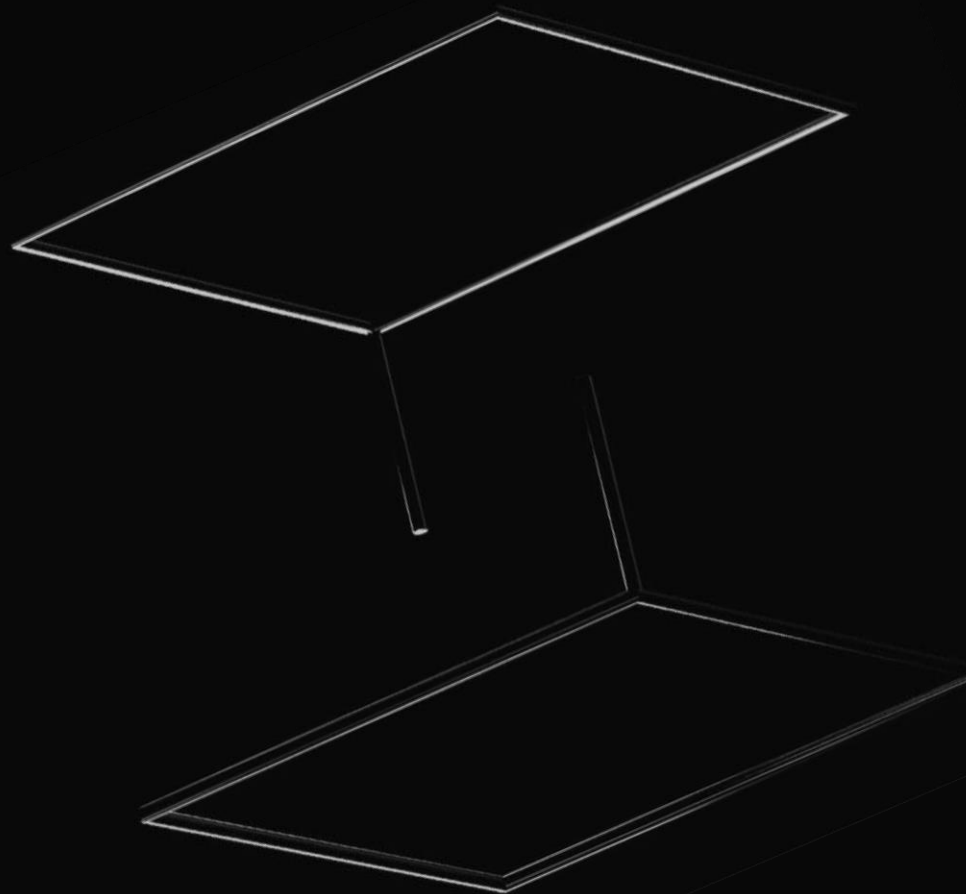


CY

**Plataforma de detección inteligente de
próxima generación**

Gestiona tu seguridad interna

Cypeer integra y monitorea sistemas
y servicios de TI críticos dentro de su
ecosistema corporativo para
protegerlo en todos los frentes.



CSI



**Solución de inteligencia contra
amenazas cibernéticas**

Protege de amenazas externas

Nuestros hackers éticos exploran de
forma encubierta la Deep y Dark
Web para identificar posibles
amenazas y defender sus fronteras.



I-SOC ES EL CORAZÓN DE NUESTRAS OPERACIONES. EL LUGAR DONDE PERSONAS Y TECNOLOGÍA SE UNEN PARA DEFENDERTE 24/7/365.

I-SOC

TIER 0 AUTOMATIZACIÓN

ANÁLISIS DE INTELIGENCIA ARTIFICIAL

Identifica patrones de ataque al correlacionar múltiples datos generados por los sistemas del cliente, reduciendo los **falsos positivos**.

TIER 1 i-SOC

ANALISTA DE CIBERSEGURIDAD

Analistas activos las 24 horas del día, capaces de comprender patrones de ataque y localizar la respuesta.

TIER 2 h-SOC

ESPECIALISTA DE CIBERSEGURIDAD

Apoyan a los analistas en caso de que necesiten investigaciones especializadas de productos.

TIER 3 α-SOC

ESPECIALISTA EXPERTO DE CIBERSEGURIDAD

Personal altamente especializado y vertical en actividades de investigación y pre-incidentes.

RESPUESTA A INCIDENTES

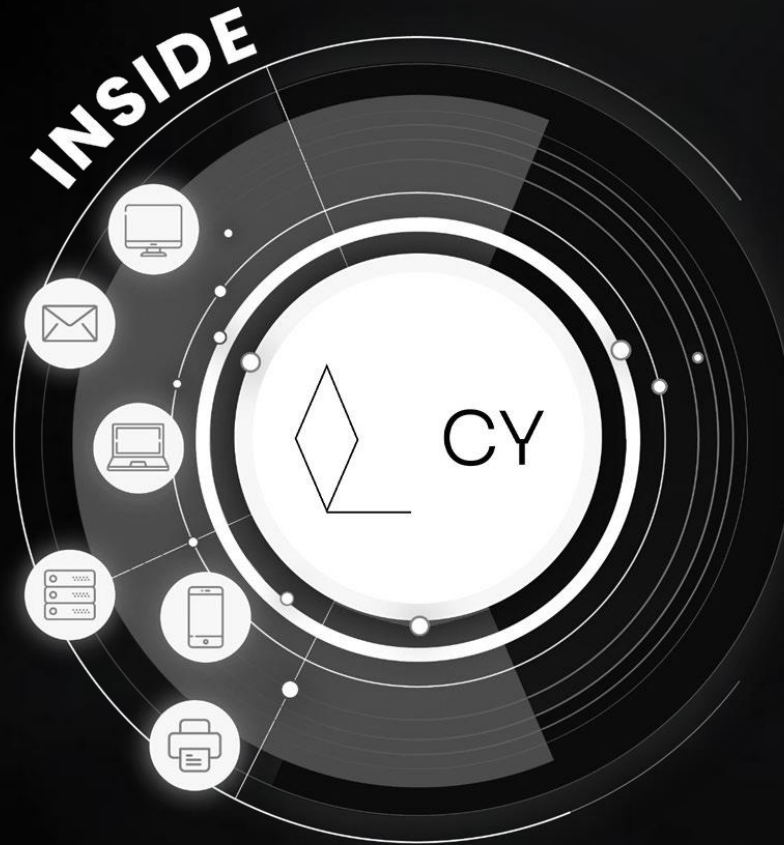
EQUIPO RESPUESTA A INCIDENTES

Expertos en intervención en incidentes con capacidades de análisis forense.



DESCRIPCIÓN

El servicio se basa en una **Plataforma de Detección Inteligente** patentada, que recopila y correlaciona todos los eventos y registros del sistema de las aplicaciones de seguridad existentes en el ecosistema de TI del cliente.



1

DETECCIÓN

Integramos y monitorizamos todos los datos de los sistemas y servicios existentes en el **ecosistema TI de su empresa.**

2

ANÁLISIS

El equipo **I-SOC** de CYBEROO analiza datos.

3

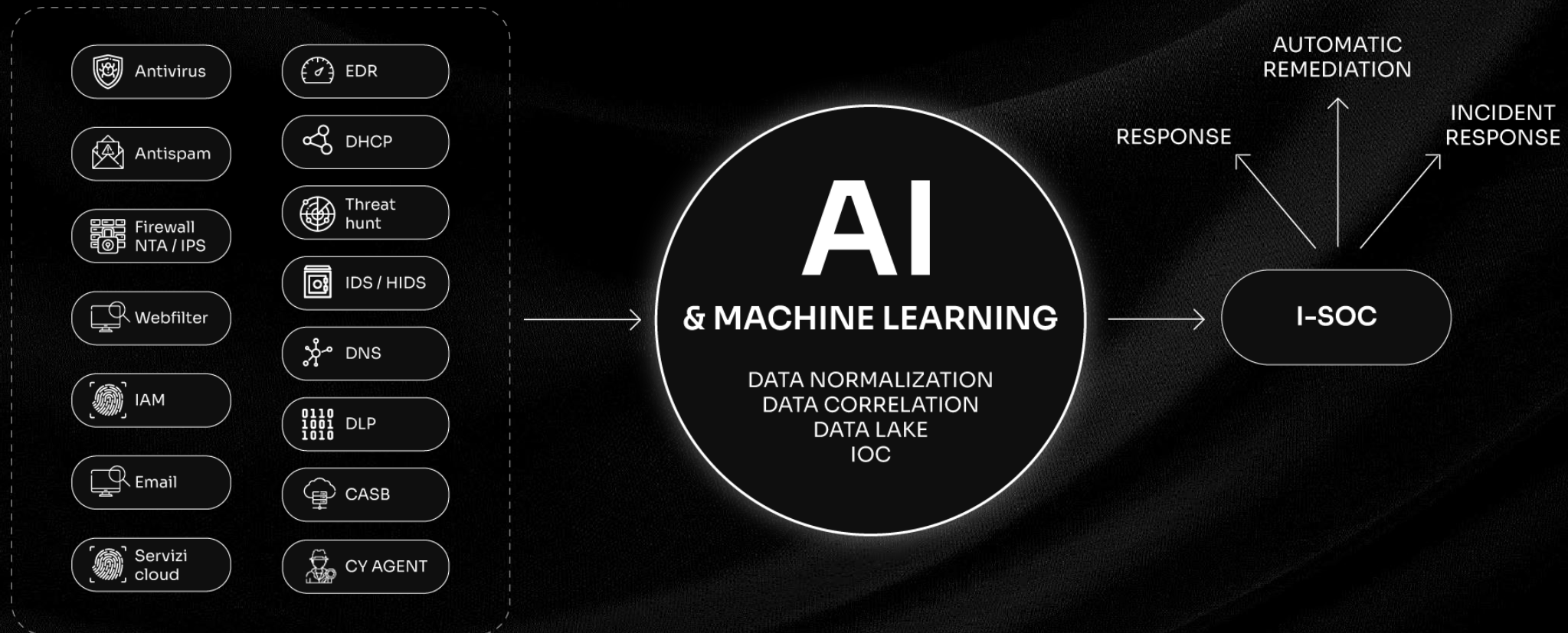
RESPUESTA

REMEDIACIÓN
MANUAL

REMEDIACIÓN
AUTOMÁTICA



CYPEER: TECNOLOGÍA 360°



BENEFICIOS

Detección automática inteligente

Detección temprana de amenazas

Implementación e integración agnósticas



MISMA DETECCIÓN DIFERENTE REMEDIACIÓN



CY_{DEK}



CY_{SONIC}



CY_{KEERA}



CY_{KEERA⁺}



DETECCIÓN CYPEER



AGENTE CYPEER X

Un agente para apoyar la detección de amenazas y el análisis de seguridad con diferentes volúmenes de acción según el contexto del cliente.



SONDA CYPEER X

Una sonda que monitorea el tráfico de la red y respalda la recopilación de datos para detectar configuraciones incorrectas de infraestructura que de otro modo serían indetectables.



CYPEER POT

Una instancia virtual que, en entornos poco protegidos, expone un sistema que emula un servidor y que también es capaz de detectar amenazas internas.



ESCANEEO CONTÍNUO

Identificación automática de nuevas vulnerabilidades en aplicaciones, sistemas y servicios internos.



BLACK BOX

Un hardware que garantiza que los sistemas de Cypeer (Cypeer Manager, Cyper Probe X, Continuous Scanning) se mantengan operativos a pesar de un escenario de compromiso total.



ALARMAS DE IA GENERATIVAS

Una vez identificada la amenaza, el sistema de IA generativa proporciona un análisis detallado que apoya la comprensión de las alarmas, con conocimientos útiles para la descripción y mitigación del riesgo y el fortalecimiento de las defensas corporativas.



PORTAL DEL CLIENTE

1

GESTIÓN DE
CASOS

2

PANEL

3

REPORT
AJE

4

BÚSQUEDA



3 ACERCAMIENTOS A LA REMEDIACIÓN

CADENA RESCATE

La cadena de rescate implica el contacto directo entre I-SOC, el cliente y/o los socios que gestionan la infraestructura.

METODOLOGÍA DE APLICACIÓN

Durante la fase de integración, se define un manual de estrategias, según el esquema MITRE ATT&CK. Este manual identifica, por tipo de ataque, urgencia e importancia, a los propietarios de los activos a los que se debe contactar en caso de intervención, según su disponibilidad.

REMEDIACIÓN AUTOMÁTICA

En contextos acordados, el sistema puede actuar de forma autónoma con manuales de juego preestablecidos en los sistemas integrados del cliente.

TECNOLOGÍAS SOBRE LAS QUE ACTÚA

Firewall
Solución Endpoint
E-mail
Active Directory
Cypeer Agent X

Filtrado Web
IaaS/SaaS
Base de Datos
NIDS
HIDS
IAM
VPN

REMEDIACIÓN CERTIFICADA

Cyberoo realiza manualmente la actividad sobre las tecnologías integradas del cliente sin tener acceso de administrador del sistema, a través de playbooks preestablecidos.

TECNOLOGÍAS SOBRE LAS QUE ACTÚA

Firewall
Protección Email
E-mail
Active Directory
PPE

Proxy Reserva
Wi-Fi
Seguridad Basada en Cloud
Filtrado URL
Agente Cypeer X





La remediación se produce únicamente a través de la cadena de rescate.





La remediación se lleva a cabo a través de una cadena automática de remediación y rescate creada sobre la base del esquema MITRE ATT&CK.

Dependiendo del tipo de ataque, la cadena de rescate identifica, a través de la compilación del playbook, los propietarios de porciones de la infraestructura a contactar en caso de intervención.

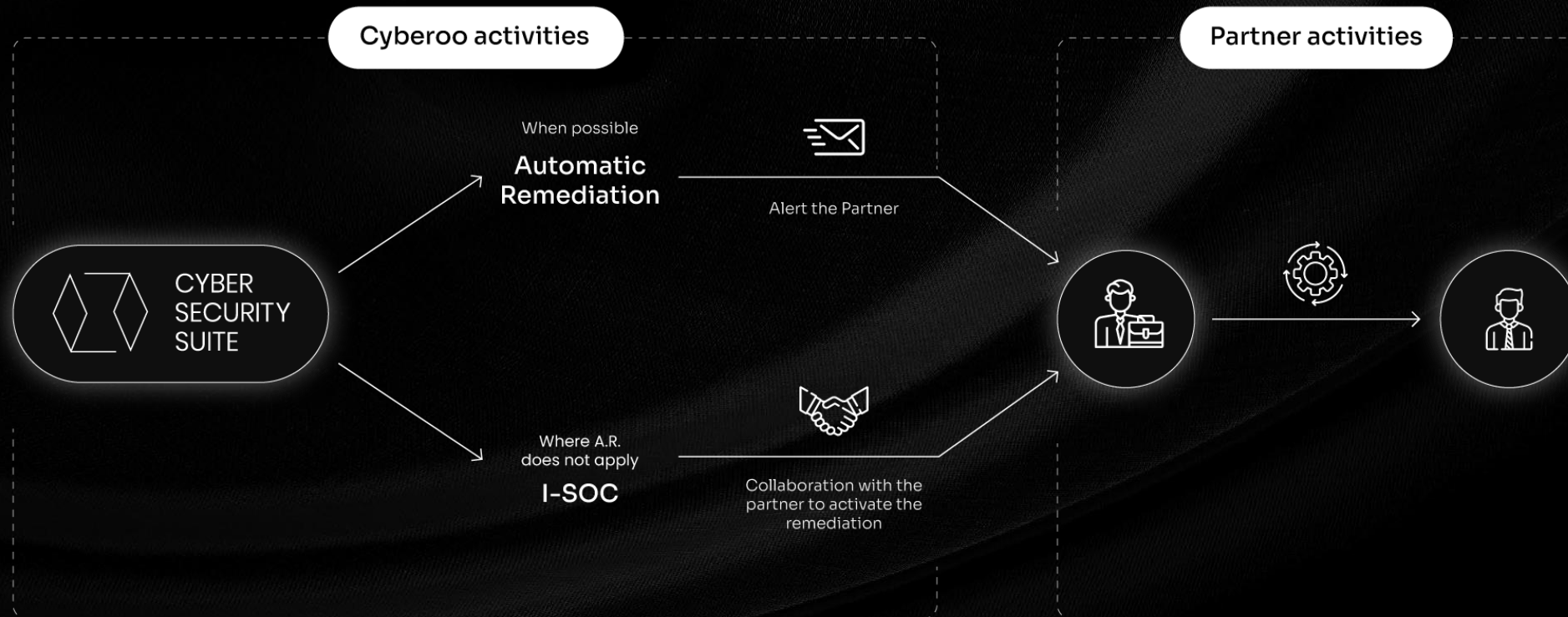


LA CADENA DE RESCATE NECESITA 3 REQUERIMIENTOS

PARTNER SOC O NOC
CON REAL 24/7

AUTONOMÍA EN LA
INTERVENCIÓN

CIBER-
COMPETENCIAS





Cuando la cadena de rescate no cumple con los requisitos correctos o solo los cumple parcialmente, CYPEER KEERA y KEERA+ certifican la calidad de toda la cadena de detección y remediación.





Gestión de actividades de remediación en Cyberoo.

Gestión de infraestructuras por parte del partner.



Interfaz virtual de gestión de remediación de actividades operativas y de mitigación del cliente.

Sin acceso administrativo.



Implementación de **toda la cadena de suministro** desde la detección hasta la remediación.

Aplicación de todas las actividades de mitigación requeridas desde Cyberoo I-SOC.



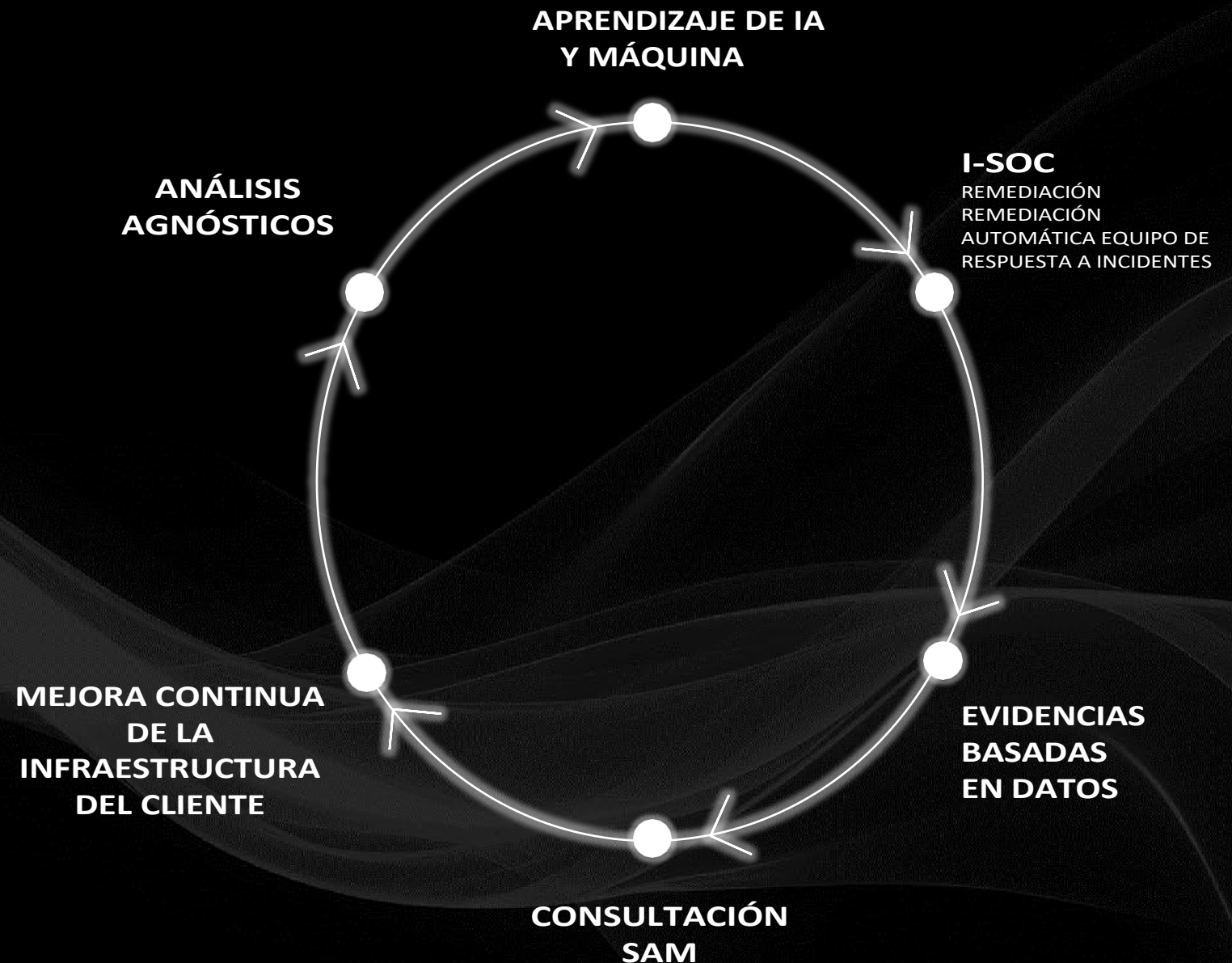
	 CY _{DEK}	 CY _{SONIC}	 CY _{KEERA}	 CY _{KEERA+}
I-SOC 1° Tier 2° Tier 3° Tier	✓	✓	✓	✓
Contacto Email Llamada Portal	✓	✓	✓	✓
Cadena rescate vía partner/cliente	✓	✓	✓ (HORAS TRABAJADAS)	
Remediación Automática		✓	✓	✓
Cadena Rescate certificada por Cyberoo NOCHE Y FINDE			✓	
Cadena Rescate certificada por Cyberoo 24/7				✓



MDR

Un proceso continuo que pone al cliente en el centro de la atención.

La recopilación y el análisis de evidencias basadas en datos, combinados con la ayuda de especialistas como expertos de I-SOC y gerentes de asesoría de seguridad, garantizan que la infraestructura se mantenga resiliente y en constante mejora.



ACTIVIDADES INCLUIDAS EN EL SERVICIO



EVALUACIÓN DE INTEGRACIÓN

Estudiamos cuidadosamente la integración en las soluciones existentes de la empresa antes del proyecto.

INSTALACIÓN

Nuestros especialistas se encargarán de la configuración, proporcionando un servicio completo llave en mano.

GESTIÓN DE ASESORAMIENTO EN SEGURIDAD

Verificamos con constancia la calidad del servicio prestado y optimizamos procesos de seguridad informática a lo largo del tiempo.

ACTUALIZACIONES

La versión comprada incluye actualizaciones gratuitas.

GESTIÓN DE CASOS ILIMITADOS

Nuestro equipo maneja constantemente reportes y alertas sin límites.

ACCESO PRIVILEGIADO AL IRT

Los clientes de MDR se benefician de la intervención de especialistas de IRT, que actúan según el SLA de intervención acordado durante la etapa del contrato.



DESCRIPCIÓN

Servicio de **Inteligencia de Amenazas** realizado por nuestro equipo de Especialistas en Ciberseguridad y **Hackers Éticos** basado en **INTELIGENCIA DE CÓDIGO ABIERTO**, que implica la recopilación y análisis de datos y amenazas de la deep web y la dark web.



1

DETECCIÓN

Los datos de la Deep y Dark Web que representan una amenaza para su empresa son identificados por nuestros Hackers Éticos.

2

ANÁLISIS

El equipo I-SOC de CYBEROO analiza datos.

3

RESPUESTA

En caso de amenaza, el cliente recibe una alerta.





IDENTIFICACIÓN DE VIOLACIÓN DE DATOS Y FUGA DE DATOS

Visibilidad sobre violaciones de datos y fugas de datos para identificar inmediatamente la fuga de datos privados o sensibles de la empresa.



ESCÁNER DE SUMINISTROS

Monitorea pasivamente la exposición de servicios y aplicaciones a Internet e identifica cualquier vulnerabilidad o nuevos servicios para la postura de seguridad de los proveedores.



VIGILANCIA VIP ULTRA

Orquestador de datos: garantiza su interacción y correlación. Permite la monitorización completa de la presencia en línea mediante la comparación de información de diferentes fuentes.



SHADOW IT

Almacenamiento de información que permite la evaluación de la postura de seguridad, el conocimiento en tiempo real sobre los sistemas expuestos y sobre cualquier posible amenaza.



MONITOREO DE MARCA

Protección de la marca y la reputación del cliente mediante múltiples actividades de inteligencia (por ejemplo, comprobación de dominios clonados).



ESCANEEO CONTÍNUO

El análisis automático de la exposición de servicios casi en tiempo real identifica de forma proactiva la presencia de nuevas vulnerabilidades.



ACTIVIDADES INCLUIDAS EN EL SERVICIO



CONFIGURACIÓN INICIAL

Al inicio del proyecto, se recopilará la información necesaria para la activación del servicio. La solución no requiere agentes, ya que su propósito es únicamente consultar la información en la web.

NOTIFICACIÓN DE EVENTOS MALICIOSOS

En caso de evento malicioso, nuestro equipo informará oportunamente sobre las actividades realizadas y los detalles de las amenazas.

OPERABILIDAD EN CASO DE SERVICIOS INTEGRADOS

En base a la evidencia detectada, CSI habilita los siguientes procesos de remediación automática a través de Cypeer Sonic.

EVIDENCIA DE OPERACIONES

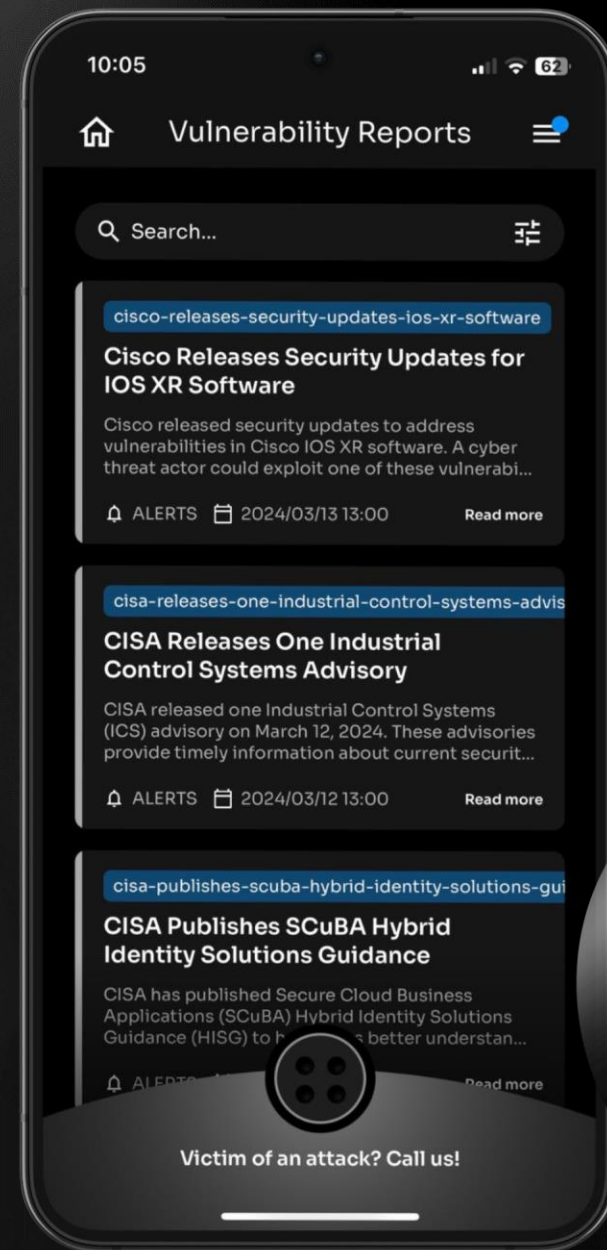
A través del panel es posible consultar los registros desde el inicio del servicio.



VÍCTIMA DE UN ATAQUE? CYBEROO ESTÁ AQUÍ

DESCARGA LA **APP** DE RESPUESTA
A INCIDENTES DE CYBEROO
Y PULSA EL **BOTÓN NEGRO**

El BOTÓN NEGRO también está disponible en
la web CYBEROO.COM o contáctanos al
número **+39 0522.388160** disponible las **24/7**



ABOVE THE REST

Hemos creado la nueva campaña
ABOVE THE REST.

Con el nuevo comercial, Cyberoo se **presenta desde una perspectiva diferente.**



*Mira el
nuevo spot*



CONTÁCTANOS



Cyberoo S.p.A.
Via Brigata Reggio, 37
42124 Reggio Emilia



Tel. 0522.388111



LinkedIn: CYBEROO



Mail: info@cyberoo.com



YouTube: CYBEROO



Web: www.cyberoo.com



X: CYBEROO



Instagram:
[@cyberoo_official](https://www.instagram.com/cyberoo_official)

