KASPERSKY lab

SOC con tecnología de Kaspersky Lab

www.kaspersky.es

Al mismo tiempo que las empresas aprenden a protegerse mejor, los delincuentes conciben técnicas aún más sofisticadas para penetrar en sus protecciones de seguridad. Atraídos por las oportunidades de generación de ingresos sin precedentes que proporcionan los ciberataques, cada vez más atacantes buscan y dirigen activamente sus ataques a las deficiencias de seguridad no detectadas.

Cada vez se crean más centros de operaciones de seguridad (SOC) para combatir los problemas de seguridad a medida que estos aparecen, y para ofrecer respuestas y soluciones rápidas.

"Los centros de operaciones de seguridad deben estar diseñados para la inteligencia, mediante la incorporación de una arquitectura de seguridad adaptable que permita atender al contexto y centrarse en la inteligencia. Los responsables de seguridad deben saber cómo los SOC basados en inteligencia emplean las herramientas, los procesos y las estrategias con el fin de protegerse frente a las amenazas modernas".

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center (Las cinco características de un centro de operaciones de seguridad basado en la inteligencia), noviembre de 2015

EL SOC OFRECE UNA FUNCIÓN CENTRALIZADA PARA LA SUPERVISIÓN Y EL ANÁLISIS CONSTANTES DE AMENAZAS, Y PARA LA MITIGACIÓN Y PREVENCIÓN DE INCIDENTES DE CIBERSEGURIDAD

En un estudio reciente llevado a cabo por B2B International (publicado a finales de 2016), en el que participaron más de 4000 empresas de 25 países, se determinó que:

- El **38 %** de los encuestados había experimentado **problemas** graves **con virus y malware** en los 12 meses anteriores, con lo que se produjo una pérdida de productividad.
- El **21 %** había experimentado **pérdida o exposición de datos debido a ataques dirigidos**.
- Alrededor del 40 % de los encuestados resaltó estos desafíos como un problema específico.
- El **17 %** de las empresas había sufrido un **ataque DDoS** en los 12 meses anteriores, y en muchos casos más de una vez.
- El **42 %** de los encuestados que experimentaron **ataques de phishing** eran grandes empresas.
- El **26 %** de todos los eventos de seguridad **no se detectaron** hasta pasadas semanas o periodos de tiempo más prolongados, y solo se revelaron mediante auditorías de seguridad externas.
- En el caso de las grandes empresas que sufrieron al menos un robo de datos, **el impacto financiero medio** fue de **891 000 $** (esto incluye los salarios del personal interno, los daños en las calificaciones crediticias y las primas de seguros, la pérdida de negocio, las relaciones públicas adicionales para reparar los daños a la marca y la contratación de asesores externos).
- Las cifras de este **impacto** en las grandes empresas **oscilaron entre 393 000 $ y 1 100 000 $**, en función del momento en el que se detectó el robo (una detección rápida redunda en un menor coste para el negocio).
- El número total de registros confidenciales de clientes y empleados que se vio comprometido también dependió del tiempo, que varió entre 9000, con una detección casi instantánea (gracias a un sistema de detección), y 240 000, cuando el robo no se detectó en más de un año.

De acuerdo con el modelo de arquitectura de seguridad adaptable de Gartner, si los equipos de SOC pretenden combatir con éxito la ciberdelincuencia en el entorno de amenazas actual, deben ser capaces de:

- PREDECIR
- DETECTAR
- PREVENIR
- RESPONDER

Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks (Diseño de una arquitectura de seguridad adaptable para la protección frente a ataques avanzados), febrero de 2014, Foundational enero de 2016

LOS CUATRO ELEMENTOS CLAVE

Para conseguir aplicar con éxito este enfoque tan reconocido en el sector es necesario implementar cuatro elementos clave, junto con procesos claramente definidos y tecnologías relevantes. Estos elementos son los siguientes:

- **GESTIÓN DE CONOCIMIENTOS.** Las personas (los miembros del equipo de SOC) deben contar con una buena formación en ciencia forense digital y respuesta ante incidentes con el fin de prevenir y responder con éxito a unos ataques cada vez más sofisticados.
- **INTELIGENCIA FRENTE A AMENAZAS**, recopilada a partir de diferentes fuentes (cuantas más mejor), esencial para detectar a tiempo las amenazas que surgen:
  1. Datos sobre amenazas internos
  2. Inteligencia obtenida de fuentes abiertas (OSINT)
  3. CERT del sector
  4. Proveedores de antimalware globales
- **BÚSQUEDA DE AMENAZAS** con el fin de buscar de forma proactiva las amenazas que no detectan los sistemas de seguridad tradicionales, como firewall, IPS/IDS, SIEM, etc.
- **UN MARCO DE RESPUESTA ANTE INCIDENTES** implementado para limitar los daños y reducir los gastos de corrección.

Cada uno de estos elementos reviste la misma importancia y debe estudiarse de forma independiente.

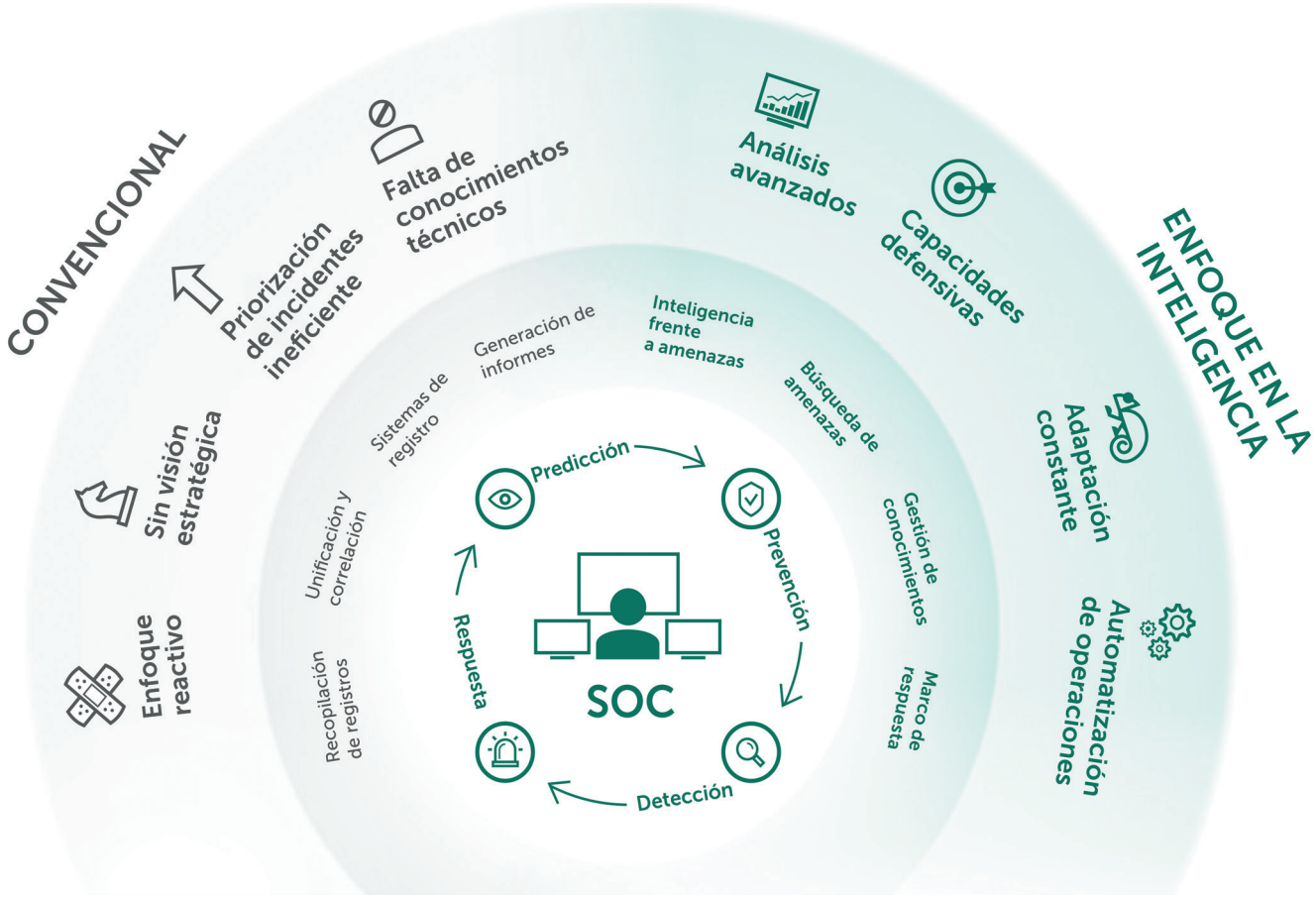


Figura 1:
Los cuatro elementos clave del SOC

GESTIÓN DE CONOCIMIENTOS

El SOC debe proporcionar un grupo de recursos de conocimientos prácticos y experiencia que sea suficiente para analizar una amplia cantidad de datos y para identificar si es necesario llevar a cabo una investigación en mayor profundidad.

Los presupuestos limitados convierten en un desafío la contratación de personal para el SOC.

En la actualidad, el mercado está experimentando una escasez de profesionales de la ciberseguridad con buena formación, lo que genera un aumento de la contratación y los costes derivados de esta.

Un miembro eficiente del equipo de SOC debe tener las cualidades siguientes:

- Una mente curiosa, capaz de construir una imagen general integrada a partir de fragmentos de datos diseminados.
- Capacidad para mantener una concentración constante mientras está sometido a altos niveles de estrés.
- Un buen conocimiento general de IT y ciberseguridad, a poder ser que incluya una amplia experiencia práctica.

Tanto si su objetivo es cubrir los puestos del SOC mediante contratación externa como mediante promoción interna, no es fácil encontrar directamente a los miembros del equipo con las habilidades deseadas. Será necesario contar con formación continua, no solo para salvar las brechas entre el conjunto de habilidades actual y el necesario, sino también para equipar a los miembros con los recursos necesarios para gestionar las tecnologías de seguridad en constante cambio y un entorno de amenazas en continua evolución.

La respuesta ante incidentes, la ciencia forense digital y el análisis de malware son competencias indispensables.

RESPUESTA ANTE INCIDENTES Y CIENCIA FORENSE DIGITAL	ANÁLISIS DE MALWARE
• Respuesta puntual y precisa al incidente • Análisis de las pruebas (imágenes del disco duro, volcados de memoria y rastros de actividad de red) y reconstrucción del historial y la lógica del incidente • Detección de las supuestas fuentes del ataque y otros sistemas potencialmente comprometidos (si es posible) • Comprensión de la causa primordial del incidente para evitar que surja cualquier incidente similar	• Conocimiento de la muestra de software sospechosa y sus capacidades • Definición de si se trata de hecho de malware • Determinación del potencial impacto que puede tener la muestra en los sistemas comprometidos dentro de la organización • Creación de un plan de corrección completo en función del comportamiento del malware detectado

Kaspersky Lab ofrece:
Servicios de formación sobre ciberseguridad

Durante más de 17 años, la experiencia práctica en ciberseguridad de Kaspersky Lab (que incluye detección de amenazas, investigación de malware, ingeniería inversa y ciencia forense digital) ha evolucionado y avanzado continuamente. Nuestros expertos saben cómo optimizar la gestión de las amenazas presentadas por las 325 000 muestras de malware que encontramos a diario y cómo impartir los conocimientos y la experiencia práctica para las organizaciones que se enfrentan a los nuevos peligros de la ciberrealidad contemporánea.

Nuestro programa de formación sobre ciberseguridad ha sido diseñado y desarrollado por las autoridades de seguridad que ayudaron a crear los laboratorios antivirus de Kaspersky y que en la actualidad inspiran y guían a la nueva generación de expertos mundiales.

La estructura de los cursos combina una parte teórica y otra práctica. Al finalizar cada curso, los estudiantes pueden validar sus conocimientos mediante una evaluación.

Los cursos son adecuados para profesionales relacionados con IT que posean habilidades generales o avanzadas de administración de sistemas y programación. Todos los cursos están disponibles a través de clases en las instalaciones del cliente o en una oficina de Kaspersky Lab local o regional, según sea aplicable.

DESCRIPCIÓN DEL PROGRAMA

TEMAS	DURACIÓN	HABILIDADES ADQUIRIDAS
CIENCIA FORENSE DIGITAL		
• Introducción a la ciencia forense digital • Respuesta activa y obtención de pruebas • Datos internos del registro de Windows • Análisis de artefactos de Windows • Ciencia forense de navegadores • Análisis de correo electrónico	5 días	• Desarrollo de un laboratorio de ciencia forense digital • Recopilación de pruebas digitales y gestión de forma correcta • Reconstrucción de un incidente y uso de marcas de tiempo • Localización de rastros de intrusión basados en artefactos de sistemas operativos Windows • Localización y análisis del historial del navegador y el correo electrónico • Aplicación con confianza de las herramientas y técnicas de ciencia forense digital
ANÁLISIS DE MALWARE E INGENIERÍA INVERSA		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Datos internos, archivos ejecutables, ensamblador x86 de Windows • Técnicas de análisis estáticos básicas (extracción de cadenas, análisis de importación, puntos de entrada PE de un vistazo, descompresión automática, etc.) • Técnicas de análisis dinámicos básicas (depuración, herramientas de supervisión, interceptación de tráfico, etc.) • Análisis de archivos .NET, Visual Basic, Win64 • Técnicas de análisis de scripts y no PE (archivos por lotes; AutoIt; Python; JScript; JavaScript; VBS)	5 días	• Creación de un entorno seguro para el análisis de malware: implementación de sandbox y todas las herramientas necesarias • Compresión de los principios de la ejecución del programa de Windows • Descompresión, depuración y análisis de objetos maliciosos; identificación de sus funciones • Detección de sitios maliciosos a través del análisis de malware de scripts • Realización de análisis de malware urgentes

TEMAS	DURACIÓN	HABILIDADES ADQUIRIDAS
CIENCIA FORENSE DIGITAL AVANZADA		
• Ciencia forense detallada de Windows • Recuperación de datos • Ciencia forense de red y nube • Ciencia forense de memoria • Análisis de la escala de tiempo • Práctica de ciencia forense de ataque con un objetivo en el mundo real	5 días	• Capacidad para realizar análisis detallados del sistema de archivos • Capacidad para recuperar archivos eliminados • Capacidad para analizar el tráfico de red • Detección de actividades maliciosas de volcados • Reconstrucción de la escala de tiempo del incidente
ANÁLISIS AVANZADO DE MALWARE E INGENIERÍA INVERSA		
• Técnicas de análisis estático avanzado (análisis estadístico del shellcode, análisis del encabezado PE, TEB, PEB, funciones de carga mediante diferentes algoritmos de hash) • Técnicas de análisis dinámico avanzado (estructura de PE, descompresión manual y avanzada, descompresión de empaquetadores maliciosos que almacenan todo el archivo ejecutable en formato cifrado) • Ingeniería inversa de APT (cubre un escenario de ataque de APT, desde el correo electrónico de phishing hasta profundizar al máximo posible) • Análisis de protocolos (análisis del protocolo de comunicación C2 cifrado y cómo descifrar el tráfico) • Análisis de rootkits y bootkits (depuración del sector de inicio mediante Ida y VMWare, depuración de kernel mediante dos máquinas virtuales y análisis de muestras de rootkit)	5 días	• Capacidad para seguir las prácticas recomendadas de ingeniería inversa mientras se reconocen las técnicas contrarias a la ingeniería inversa (ofuscación, antidepuración) • Capacidad para aplicar análisis de malware avanzado para la disección de rootkits y bootkits • Capacidad para analizar shellcode de exploits incrustado en diferentes tipos de archivos y malware no Windows
RESPUESTA ANTE INCIDENTES		
• Introducción a la respuesta ante incidentes • Detección y análisis primario • Análisis digital • Creación de reglas de detección (YARA, Snort, Bro)	5 días	• Diferenciación de las APT del resto de amenazas • Comprensión de las distintas técnicas y la anatomía de ataque dirigido de los atacantes • Aplicación de métodos específicos de supervisión y detección • Seguimiento del flujo de trabajo de respuesta ante incidentes • Reconstrucción de la cronología y lógica del incidente • Creación de reglas e informes de detección

Las herramientas cambian con el tiempo, pero los conocimientos básicos y los métodos de trabajo siguen siendo los mismos. Los participantes no solo recibirán un conjunto de herramientas e instrucciones, sino también conocimientos sobre los principios básicos y las funciones. Todas las tareas prácticas se basan en casos reales siempre que sea posible sin atentar contra la confidencialidad del cliente.

INTELIGENCIA FRENTE A AMENAZAS Y BÚSQUEDA DE AMENAZAS

El SOC se diseñó tradicionalmente para ofrecer lo siguiente:

- Gestión de dispositivos de seguridad, mantenimiento del perímetro y tecnologías de seguridad preventiva, como IPS, firewalls, proxies, etc.
- Supervisión de eventos de seguridad a través de un sistema de información relacionada con la seguridad y gestión de eventos (SIEM).
- Ciencia forense y corrección de incidentes.
- Cumplimiento interno o normativo (por ejemplo, PCI-DSS).

Muchas organizaciones están planificando cómo obtener una mayor visibilidad de las amenazas mediante el establecimiento de sus propios SOC. Sin embargo, algunas de las que ya cuentan con un SOC se enfrentan a muchos de los mismos problemas.
Esto puede tener varios motivos:

- Priorización deficiente, con lo que las amenazas reales quedan enterradas entre las miles de alertas de seguridad insignificantes que se reciben y analizan cada día.
- Corrección de incidentes sin un conocimiento adecuado de las tácticas, técnicas y procedimientos (TTP) de los actores de amenazas asociados, con lo que se pasan por alto los ataques avanzados.
- Falsos negativos debido a la falta de datos correspondientes a las amenazas.
- Un enfoque reactivo ante los incidentes, en lugar de una "caza" proactiva de las amenazas que no son detectadas pero están activas dentro de la organización.
- Falta de una visión general estratégica del panorama actual de amenazas o falta de conocimiento de ataques en empresas similares, así como las tácticas defensivas disponibles.

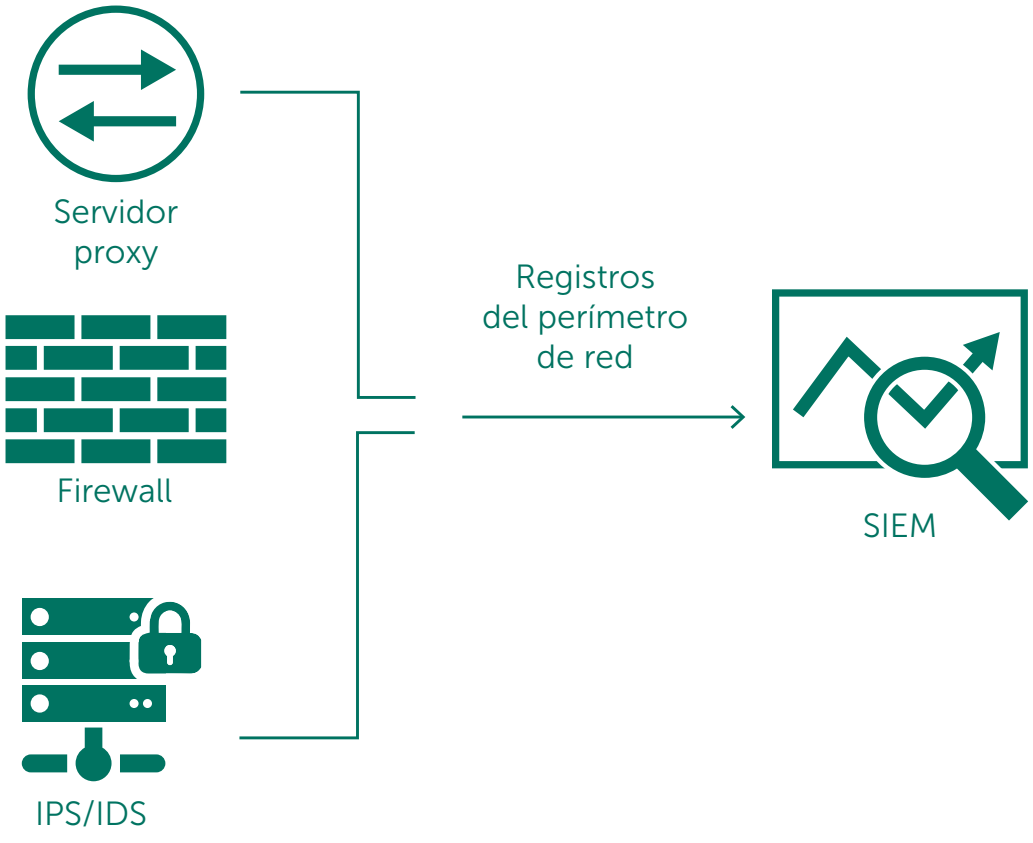


Figura 2:
Un SOC convencional

- Problemas para atraer una inversión interna adecuada a las tecnologías específicas de seguridad, debido a las dificultades para comunicar los riesgos para los procesos empresariales asociados con las brechas de seguridad a los ejecutivos de alto nivel que no son técnicos.

Gartner define la inteligencia frente a amenazas de la forma siguiente:
"Conocimiento basado en pruebas, que incluye contexto, mecanismos, indicadores, implicaciones y consejos viables, sobre una amenaza o un peligro existente o emergente para los activos que pueden utilizarse para tomar decisiones fundamentadas sobre la respuesta del sujeto a dicha amenaza o peligro".

Gartner, How Gartner Defines Threat Intelligence (Cómo define Gartner la inteligencia frente a amenazas), febrero de 2016

Teniendo en cuenta estas consideraciones, los responsables de seguridad deben estar bien asesorados para seguir un enfoque del SOC basado en la inteligencia. Para que el SOC sea eficiente, debe permitir la adopción continua de nuevas tecnologías y controles adecuados a los cambios generalizados que se producen en el entorno actual de amenazas.

La combinación de datos internos sobre amenazas con información recopilada de varias fuentes diferentes (por ejemplo, OSINT o proveedores de antimalware globales) permite conocer las técnicas de ataque y sus potenciales indicadores. A su vez, esto permite a las organizaciones desarrollar estrategias defensivas eficaces frente a ataques genéricos y avanzados dirigidos contra organizaciones específicas.

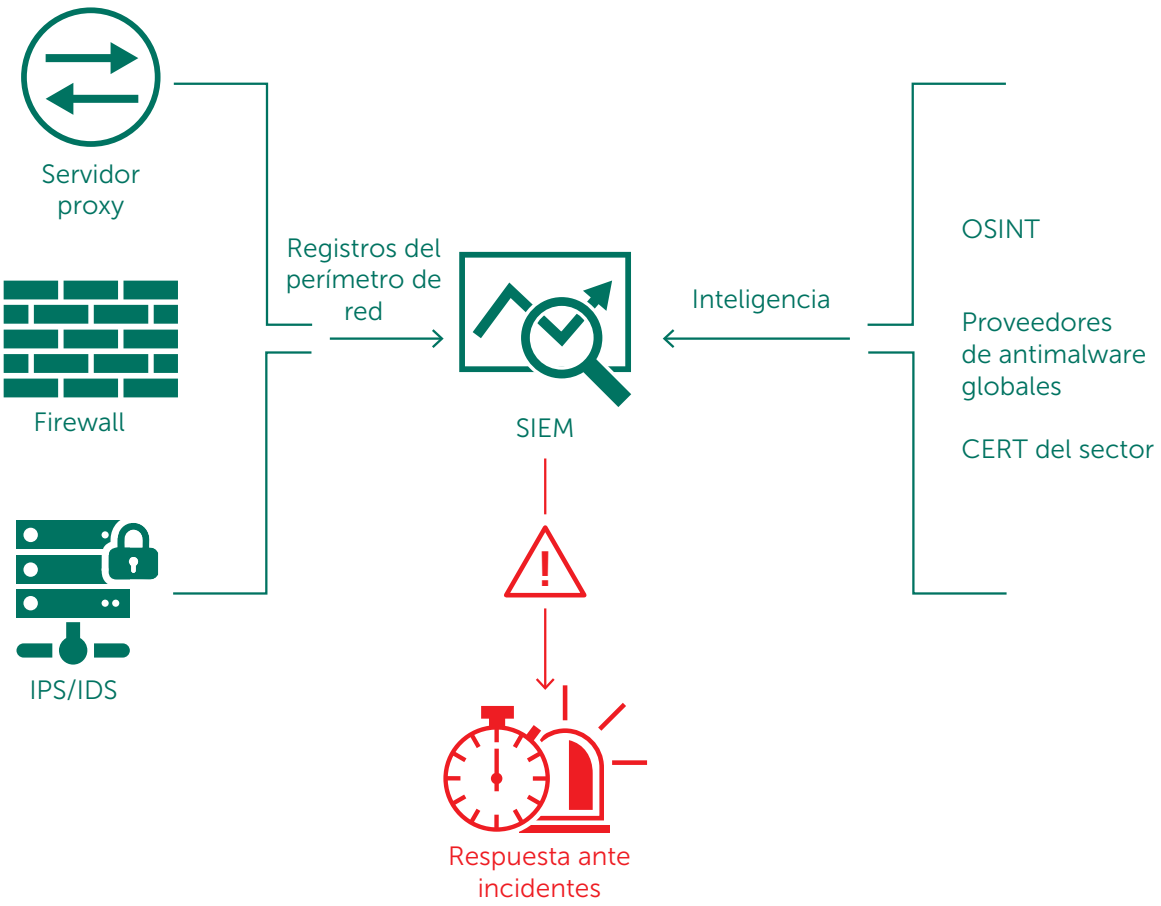


Figura 3:
El SOC basado en la inteligencia

Las fuentes de inteligencia se deben seleccionar cuidadosamente. Existe una correlación directa entre la calidad de la inteligencia utilizada y la eficiencia de las decisiones tomadas en función de esta inteligencia. Si confía en inteligencia irrelevante, imprecisa o no adaptada a los objetivos de su sector o negocio, o si la información sobre amenazas no se recibe rápidamente, la calidad de la toma de decisiones en su organización puede verse gravemente comprometida.

Los datos sin procesar sin contexto no ofrecen la relevancia necesaria para que los equipos de SOC sean totalmente eficientes. Por ejemplo, saber que una URL específica es maliciosa es muy diferente a saber también que se utiliza para alojar un exploit o un tipo de malware específico. Este nivel de inteligencia adicional indica a los expertos de seguridad lo que deben buscar cuando exploran un equipo infectado.

Qué buscar en el caso de fuentes externas de inteligencia frente a amenazas:

- Inteligencia con alcance mundial, que ofrezca la visibilidad más amplia de los ataques.
- Un proveedor con un historial demostrado de detección temprana de nuevos indicadores de amenaza.
- Inteligencia que resulte útil de forma inmediata y tenga un buen contexto.
- Formatos y mecanismos de entrega que permitan una integración fácil en los controles de seguridad presentes.

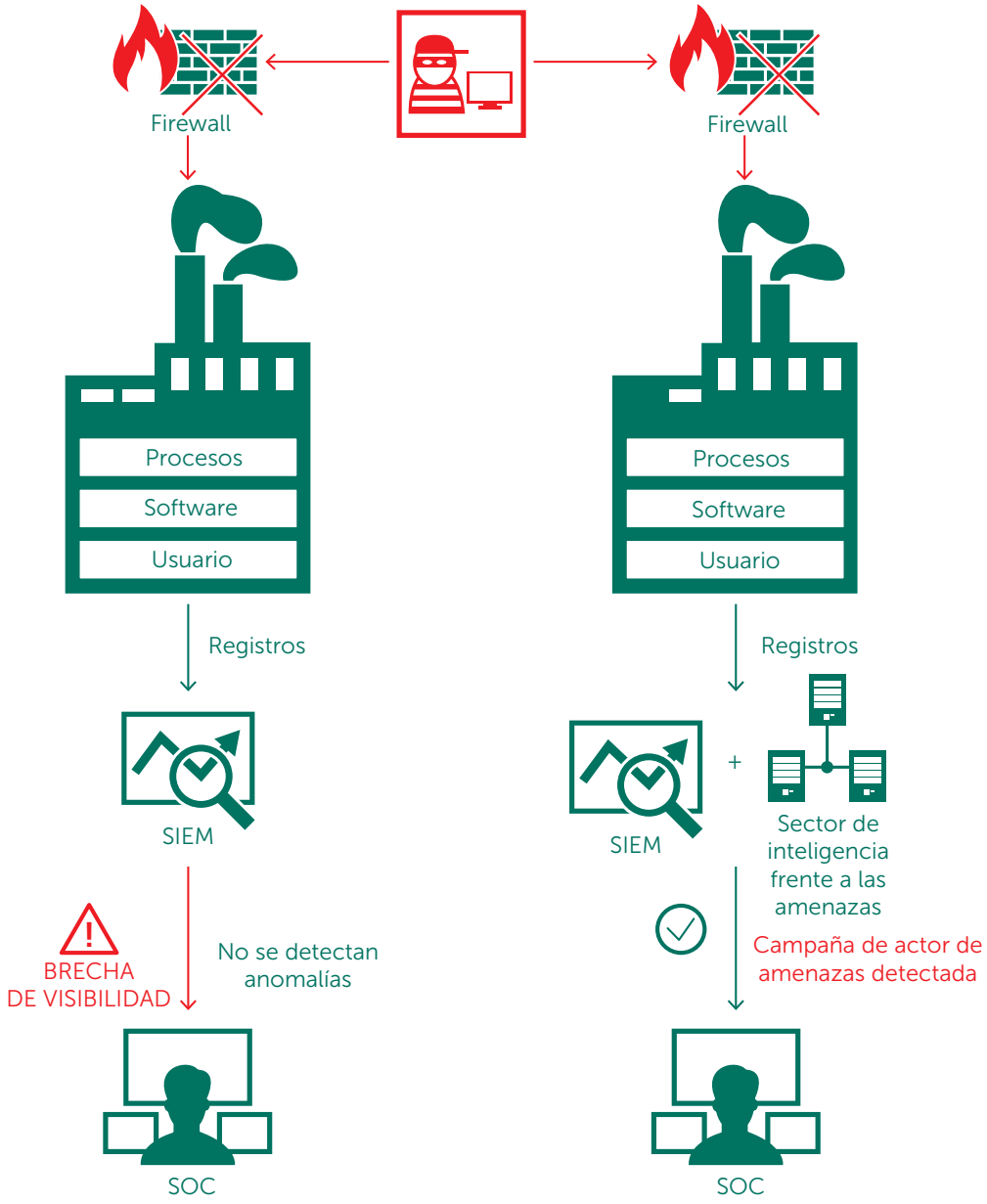


Figura 4:
Modelo de inteligencia frente a amenazas

La búsqueda de amenazas es también un elemento importante de las operaciones diarias del SOC. No se trata de un concepto nuevo. La detección de amenazas desconocidas y avanzadas depende de los arduos esfuerzos prácticos de los analistas de seguridad, en lugar de reglas automatizadas o mecanismos de detección basados en firmas.

Este proceso conlleva la recopilación y aplicación de diferentes técnicas (como el análisis estadístico, el aprendizaje mecánico y la visualización) a todos los datos disponibles obtenidos de los endpoints, las redes, los controles de seguridad implementados, los sistemas de autenticación, etc. El objetivo es confirmar una hipótesis existente con respecto a la posible brecha. Las tecnologías de búsqueda de amenazas que puede emplear el analista incluyen las ya mencionadas (soluciones SIEM, OSINT, plataformas de inteligencia frente a amenazas y otras fuentes de datos).

El analista de búsqueda de amenazas consultará los indicadores de compromiso (IOC) obtenidos de forma externa y aplicará herramientas especializadas para buscar estos artefactos (en forma de direcciones IP, hash de archivos, URL, etc.) dentro de los hosts de la organización. Cuando se detecta un claro signo de que la seguridad se ha visto comprometida, se pueden iniciar los procedimientos de respuesta ante incidentes.

El rastreo de altos volúmenes de datos con el fin de identificar los artefactos que las medidas automatizadas no han podido detectar es una tarea dirigida a profesionales altamente cualificados y experimentados.

Kaspersky Lab ofrece:
Fuentes de datos de inteligencia frente a amenazas

Kaspersky Lab ofrece fuentes de datos de inteligencia frente a amenazas que se actualizan de forma constante con el fin de informar a su equipo de SOC sobre los riesgos y las implicaciones que se asocian a las ciberamenazas, lo que le ayuda a mitigar las amenazas de forma más eficiente y a defenderse de los ataques incluso antes de que se inicien.

DESCRIPCIÓN DE LAS FUENTES DE DATOS

Fuentes de reputación de IP: conjunto de direcciones IP con contexto que cubre los hosts sospechosos y maliciosos.

URL maliciosas: conjunto de URL que abarca enlaces y sitios web maliciosos. Hay registros enmascarados y no enmascarados disponibles.

URL de phishing: conjunto de URL identificadas por Kaspersky Lab como sitios de phishing. Hay registros enmascarados y no enmascarados disponibles.

URL de mando y control de botnets: conjunto de URL de servidores de mando y control (C&C) de botnets y objetos maliciosos relacionados.

Fuentes de datos de listas blancas: conjunto de hash de archivos que ofrece a las soluciones y los servicios de terceros un conocimiento sistemático del software legítimo.

Fuentes de hash maliciosas: cubren el malware más peligroso, frecuente y emergente.

Fuentes de hash maliciosas móviles: conjunto de hash de archivos para detectar objetos maliciosos que infectan plataformas móviles.

Fuentes de datos de troyanos P-SMS: conjunto de hash de troyanos con el contexto correspondiente para detectar troyanos de SMS que conllevan llamadas con cargos premium para los usuarios de móviles y que permiten a un atacante robar, eliminar y responder a mensajes de SMS.

URL de mando y control de botnets móviles: conjunto de URL con contexto que abarca los servidores de mando y control de botnets móviles.

CARACTERÍSTICAS DESTACADAS DEL SERVICIO

- Las fuentes de datos se generan automáticamente a tiempo real, en función de las conclusiones recopiladas a nivel mundial (Kaspersky Security Network ofrece visibilidad de un importante porcentaje de todo el tráfico de Internet, con decenas de millones de usuarios finales en más de 200 países), lo que ofrece unos altos índices de detección y precisión.
- Todos los registros de cada fuente de datos se mejoran con contexto útil (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hash, popularidad, etc.). Los datos contextuales ayudan a revelar una "visión de conjunto", lo que mejora la validación y complementación de un uso variado de los datos. Cuando están en contexto, los datos se pueden utilizar de forma más inmediata para responder a quién, qué, dónde y cuándo, lo que permite identificar a los adversarios y ayuda a tomar decisiones puntuales y emprender las acciones que protegerán específicamente su organización.
- Los formatos de divulgación ligeros sencillos (JSON, CSV, OpenIoC, STIX) a través de HTTPS o mecanismos de entrega específicos permiten una integración fácil de las fuentes en las soluciones de seguridad.
- La inteligencia frente a amenazas se genera y supervisa mediante una infraestructura muy tolerante a fallos, lo que garantiza una disponibilidad continua y un rendimiento constante.
- Integración inmediata con HP ArcSight, IBM QRadar, Splunk y más.

Kaspersky Threat Lookup

Kaspersky Threat Lookup ofrece todos los conocimientos adquiridos por Kaspersky Lab sobre ciberamenazas y sus relaciones, reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de SOC el mayor número de datos posible, evitando los ciberataques antes de que afecten a su organización. La plataforma recupera la inteligencia frente a amenazas más reciente y detallada sobre URL, dominios, direcciones IP, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes, que le ayuda a proteger su organización y mejorar la respuesta ante incidentes.

CARACTERÍSTICAS DESTACADAS DEL SERVICIO

- Inteligencia de confianza: un atributo clave de Kaspersky Threat Lookup es la fiabilidad de nuestros datos de inteligencia frente a amenazas, que se mejoran con contexto útil. Los productos de Kaspersky Lab lideran el campo de las pruebas antimalware[1], demostrando la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.
- Altos niveles de cobertura en tiempo real: la inteligencia frente a amenazas se genera en tiempo real, en función de las conclusiones recopiladas a nivel mundial, respaldadas por Kaspersky Security Network.
- Búsqueda de amenazas: hay que ser proactivo en la prevención, detección y respuesta a los ataques, para minimizar su impacto y frecuencia. Se debe realizar un seguimiento y eliminar drásticamente los ataques lo antes posible. Cuanto antes se detecte una amenaza, menos daños provocará, antes será posible llevar a cabo las reparaciones necesarias y con mayor prontitud podrán volver a la normalidad las operaciones de red.
- Datos enriquecidos: la inteligencia frente a amenazas de Kaspersky Threat Lookup abarca una amplia variedad de tipos de datos diferentes, que incluyen hash, URL, IP, WHOIS, pDNS, GeoIP, atributos de archivos, datos estadísticos y de comportamiento, cadenas de descargas, marcas de tiempo y mucho más. Con la ayuda de estos datos, puede sondear el variado panorama de amenazas de seguridad a las que se enfrenta.
- Disponibilidad continua: la inteligencia frente a amenazas se genera y supervisa mediante una infraestructura muy tolerante a fallos, lo que garantiza una disponibilidad continua y un rendimiento constante.
- Revisión continua por parte de expertos en seguridad: cientos de expertos, incluidos analistas de seguridad de todo el mundo, y expertos en seguridad de fama mundial de nuestro equipo GReAT y de equipos de I+D de vanguardia, contribuyen de forma conjunta a generar valiosa inteligencia frente amenazas del mundo real.

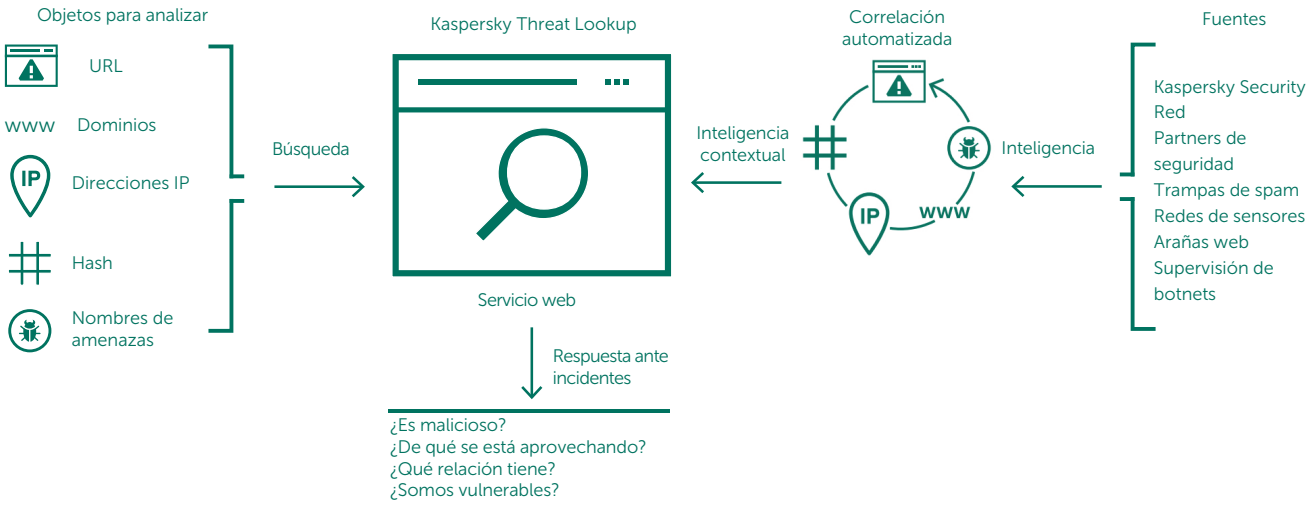
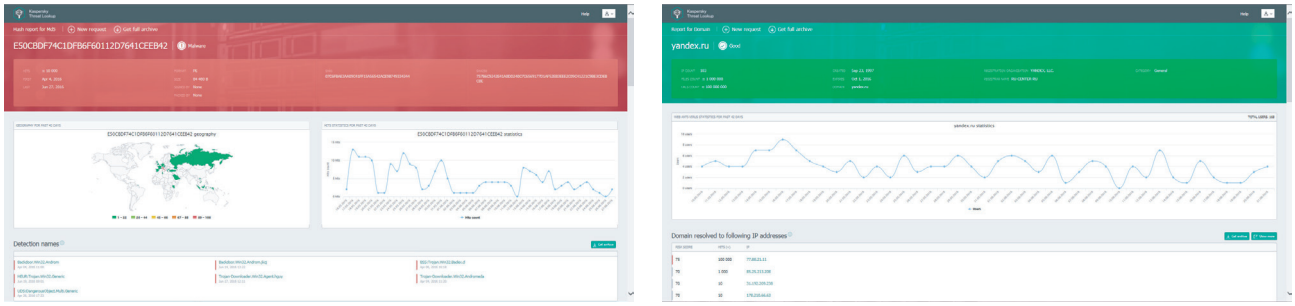


Figura 5:
Kaspersky Threat Lookup

1 http://www.kaspersky.es/top3

- Análisis sandbox: detección de amenazas desconocidas mediante la ejecución de los objetos sospechosos en un entorno seguro y revisión del alcance completo del comportamiento de la amenaza y los artefactos mediante informes de fácil lectura.
- Amplia gama de formatos de exportación: indicadores de compromiso (IOC) o contexto útil sobre los formatos de uso compartido legibles por máquina más ampliamente utilizados y más organizados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para disfrutar de todas las ventajas de la inteligencia frente a amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.
- Interfaz web o API RESTful fáciles de usar: uso del servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceso a través de una sencilla API RESTful, según las preferencias.



Informes de inteligencia APT

No todas las amenazas persistentes avanzadas (APT) se notifican de inmediato y muchas ni siquiera se anuncian públicamente. Sea el primero en conocer nuestras últimas investigaciones a través de nuestros informes de inteligencia procesables en profundidad sobre las APT.

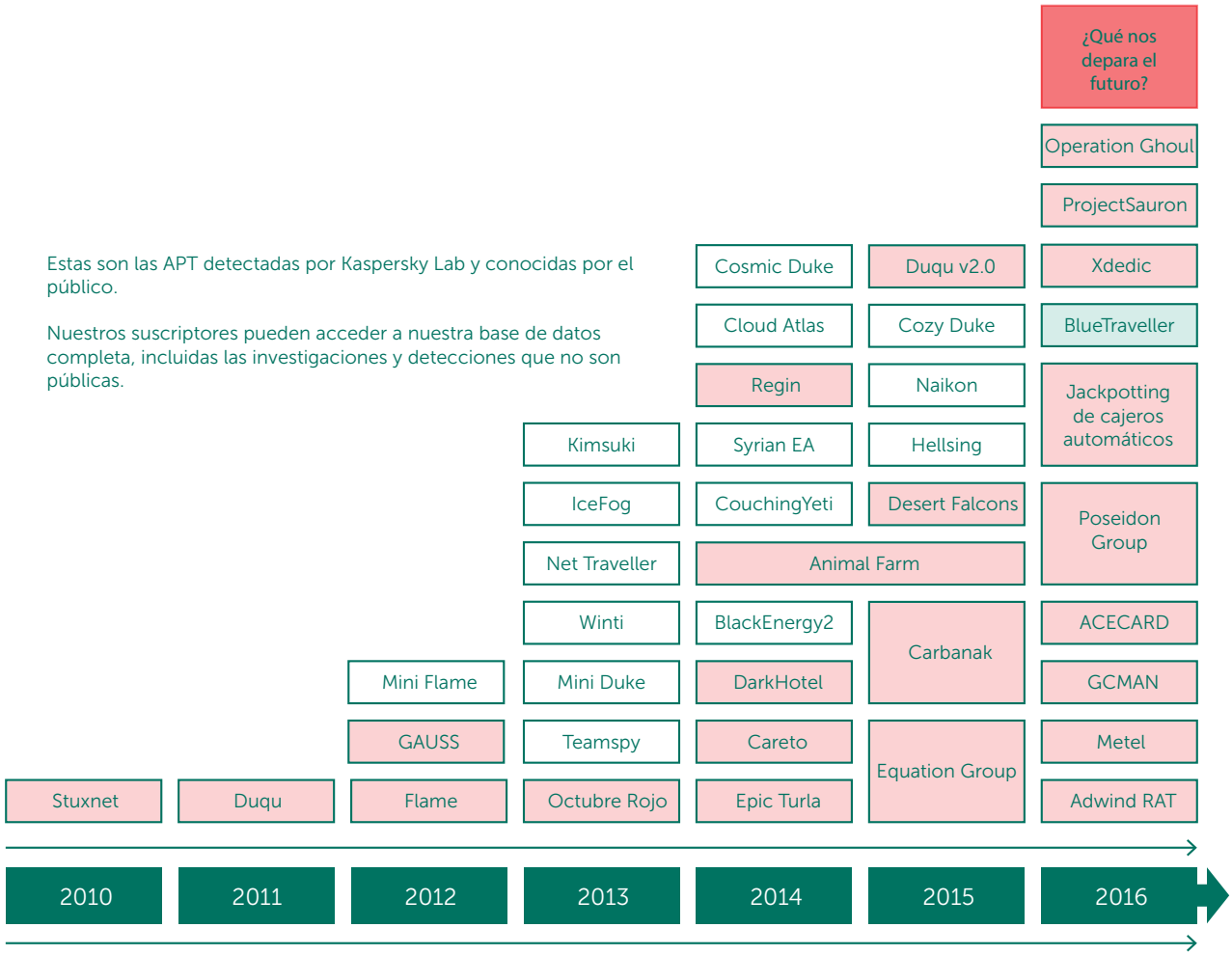


Figura 6:
APT detectadas por Kaspersky Lab

Como suscriptor de los informes de inteligencia de APT de Kaspersky, le proporcionamos acceso permanente y en exclusiva a nuestras investigaciones y descubrimientos sobre las APT detectadas al instante, así como a todos los datos técnicos relevantes en una amplia variedad de formatos. Entre dicha información también se incluirán las amenazas que nunca se harán públicas. Nuestros expertos, los cazadores de APT más cualificados y competentes del sector, también le alertarán de inmediato de los cambios que detecten en las tácticas de los grupos cibercriminales y ciberterroristas. Además, contará con acceso a toda la base de datos de informes de APT de Kaspersky Lab, otro eficaz componente de investigación y análisis de su defensa de seguridad corporativa.

CARACTERÍSTICAS DESTACADAS DEL SERVICIO

- Acceso exclusivo a descripciones técnicas de amenazas de vanguardia durante la investigación en curso, antes de hacerse públicas.
- Información sobre APT no públicas. No todas las amenazas de alto perfil están sujetas a notificación pública. Algunas, debido a las víctimas afectadas, la confidencialidad de los datos, la naturaleza del proceso de reparación de vulnerabilidades o las actividades de orden público asociadas, nunca se hacen públicas. Sin embargo, todas se comunican a nuestros clientes.
- Herramientas, muestras y datos técnicos complementarios detallados, incluida una lista ampliada de indicadores de compromiso (IOC), disponible en formato openIOC, y acceso a nuestras reglas Yara.
- Vigilancia continua de campañas de APT. Acceso a inteligencia procesable durante la investigación (información sobre la distribución de APT, IOC e infraestructura C&C).
- Análisis retrospectivo: acceso a todos los informes privados publicados con anterioridad durante todo el periodo de su suscripción.

Desde un punto de vista práctico, los indicadores de compromiso son la parte más procesable del informe para los expertos del SOC. Esta información estructurada se proporciona para su posterior uso con herramientas automatizadas específicas, que ayudan a comprobar si hay signos de infección en su infraestructura.

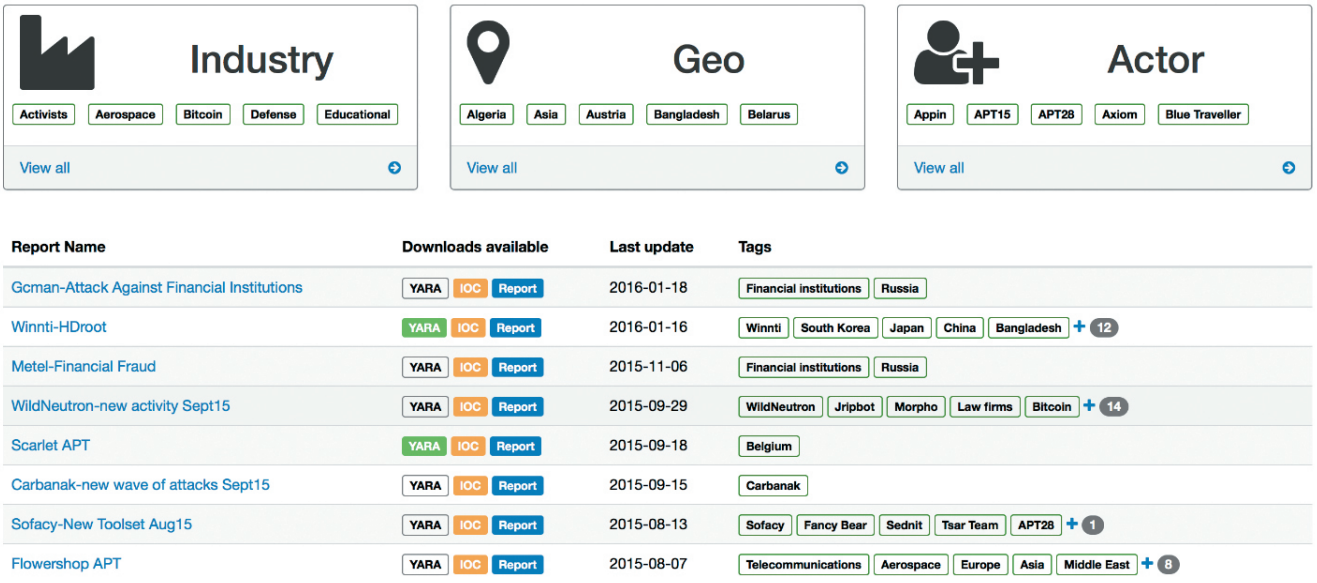


Figura 7:
Portal de inteligencia de APT

Informes sobre amenazas personalizados

Informes sobre amenazas específicos del cliente

¿Cuál es la mejor manera de organizar un ataque contra su empresa? ¿Qué rutas y qué información están disponibles para un atacante que se dirija específicamente a usted? ¿Ya se ha organizado un ataque o está a punto de enfrentarse a una amenaza?

Los informes sobre amenazas específicos del cliente de Kaspersky responden a estas y otras preguntas, ya que nuestros expertos componen una imagen exhaustiva de su actual estado de ataque e identifican puntos débiles a punto para exploits y revelan pruebas de ataques pasados, presentes y previstos.

Con ayuda de toda esta información, podrá centrar su estrategia de defensa en las áreas identificadas como los principales objetivos de los cibercriminales, y actuar rápidamente y con precisión para repeler a los intrusos y minimizar el riesgo de éxito de un ataque.

Desarrollados con inteligencia de fuente abierta (OSINT), el análisis en profundidad de los sistemas y bases de datos especializados de Kaspersky Lab y nuestros conocimientos sobre las redes clandestinas de cibercriminales, estos informes abarcan áreas como:

- **Identificación de vectores de amenazas**: identificación y análisis de estado de los componentes críticos de la red disponibles externamente, incluidos cajeros automáticos, sistemas de videovigilancia y otros sistemas que utilizan tecnologías móviles, perfiles de sus empleados en las redes sociales y cuentas de correo electrónico personales, que son posibles blancos de ataque.
- **Análisis de seguimiento de malware y ciberataques**: identificación, supervisión y análisis de muestras de malware activas o inactivas dirigidas a su empresa, actividad pasada o actual de botnets y actividades sospechosas basadas en la red.
- **Ataques de terceros**: pruebas de amenazas y actividad de botnets específicamente dirigidas a sus clientes, partners y suscriptores, cuyos sistemas infectados podrían utilizarse para atacarle.
- **Filtración de información**: por medio de la vigilancia discreta de foros y comunidades online clandestinos, descubrimos si los hackers están hablando de planes de ataque dirigidos a usted o, por ejemplo, si un empleado sin escrúpulos comercia con información.
- **Estado actual de los ataques**: los ataques de APT pueden continuar de manera inadvertida durante muchos años. Si detectamos un ataque actual que afecta a su infraestructura, le asesoramos sobre su corrección eficaz.

INICIO RÁPIDO – FÁCIL DE UTILIZAR – SIN NECESIDAD DE RECURSOS

Una vez que se establecen los parámetros (para informes específicos del cliente) y los formatos de datos preferidos, no se necesita ninguna infraestructura adicional para empezar a usar este servicio de Kaspersky Lab.

Los informes de inteligencia de amenazas de Kaspersky no afectan a la integridad y la disponibilidad de recursos, incluidos los recursos de red.

Informes sobre amenazas específicos del país

La ciberseguridad de un país comprende la protección de todas sus principales instituciones y organizaciones. Las amenazas persistentes avanzadas (APT) contra autoridades gubernamentales pueden afectar a la seguridad nacional. Los posibles ciberataques contra los sectores de la fabricación, el transporte, las telecomunicaciones, la banca y otros sectores fundamentales pueden conllevar importantes daños en el nivel estatal, como pérdidas financieras, accidentes de producción, bloqueo de las comunicaciones en red y descontento popular.

Disponer de una visión general de la superficie de ataque actual y las tendencias actuales de malware y ataques de hackers dirigidos contra su país le permitirá centrar su estrategia de defensa en las áreas identificadas como los principales objetivos de los ciberdelincuentes, y actuar rápidamente y con precisión para repeler a los intrusos y minimizar el riesgo de éxito de un ataque.

Creados mediante enfoques que van de la inteligencia de fuente abierta (OSINT) al análisis en profundidad de los sistemas y bases de datos especializados de Kaspersky Lab y nuestros conocimientos sobre las redes clandestinas de cibercriminales, estos informes sobre amenazas específicos del país abarcan áreas como:

- **Identificación de vectores de amenazas**: identificación y análisis de estado de los recursos de IT críticos del país disponibles de forma externa, lo que incluye aplicaciones gubernamentales vulnerables, equipos de telecomunicaciones, componentes de sistemas de control industrial (como SCADA, PLC, etc.), cajeros automáticos, etc.
- **Análisis de seguimiento de malware y ciberataques**: identificación y análisis de campañas de APT, muestras de malware activas o inactivas, actividad de botnets pasados o presentes, y otras amenazas destacadas dirigidas contra su país, en función de los datos disponibles en nuestros exclusivos recursos de supervisión internos.
- **Filtraciones de información**: por medio de la supervisión discreta de foros y comunidades online clandestinos, detectamos si los hackers están hablando de planes de ataque dirigidos contra determinadas organizaciones. También revelamos importantes cuentas comprometidas, que pueden suponer riesgos para las organizaciones e instituciones afectadas (por ejemplo, cuentas que pertenecen a empleados de organismos gubernamentales disponibles en el robo de Ashley Madison, que se pueden emplear para operaciones de chantaje).

Los informes de inteligencia frente a amenazas de Kaspersky no afectan a la integridad y la disponibilidad de los recursos de red inspeccionados. El servicio se basa en métodos de reconocimiento de red no intrusivos y en el análisis de la información disponible en fuentes abiertas y recursos de acceso limitado.

Como conclusión del servicio se le proporcionará un informe que incluirá la descripción de las amenazas destacadas para diferentes sectores e instituciones estatales, además de información adicional sobre los resultados del análisis técnico detallado. Los informes se entregan mediante mensajes cifrados por correo electrónico.

El servicio se puede prestar como proyecto puntual o de forma periódica mediante suscripción (por ejemplo, trimestralmente).

Protección gestionada de Kaspersky

El servicio de protección gestionada de Kaspersky ofrece a los usuarios de Kaspersky Security for Business y Kaspersky Anti Targeted Attack Platform una combinación única de medidas técnicas avanzadas para detectar y evitar ataques dirigidos. El servicio incluye supervisión continua por parte de los expertos de Kaspersky Lab y análisis constante de datos de ciberamenazas (inteligencia frente a ciberamenazas), lo que garantiza la detección en tiempo real de campañas de ciberespionaje y ciberdelincuencia nuevas y conocidas dirigidas contra sistemas de información críticos.

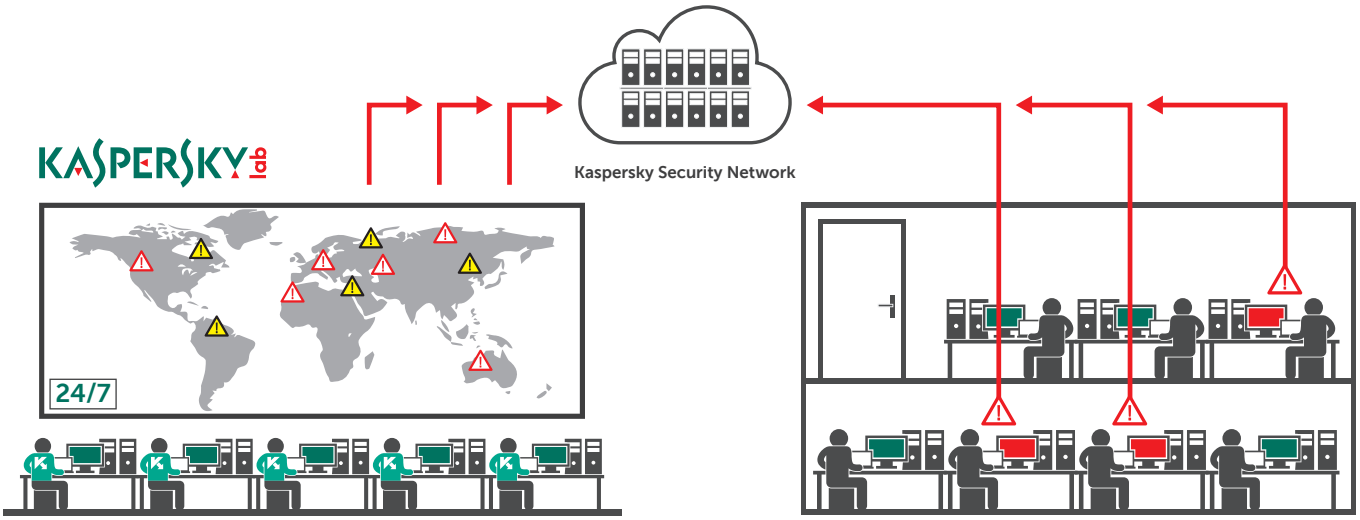


Figura 8:
Protección gestionada de Kaspersky

CARACTERÍSTICAS DESTACADAS DEL SERVICIO

- Un alto nivel de protección contra ataques dirigidos y malware con asistencia permanente de los analistas de Kaspersky Lab.
- Información sobre los atacantes, su motivación, sus métodos y herramientas, así como los posibles daños que pueden infligir, lo que respalda el desarrollo de una estrategia de protección totalmente fundamentada y eficiente.
- Detección de ataques que no son de malware, ataques que incluyen herramientas conocidas anteriormente y ataques que explotan las vulnerabilidades de día cero.
- Análisis retrospectivo de incidentes y búsqueda de amenazas.
- Reducción de los costes de seguridad generales, a la vez que se mejora la calidad de la protección. Se trata de un servicio muy profesional ofrecido por el líder mundial en análisis de ciberataques, que incluye el análisis de los métodos y las tecnologías que utilizan los actores de amenazas. La obtención de este nivel de información a través de un servicio externo resulta mucho más económica que el empleo de especialistas altamente especializados.
- Enfoque integrado: nuestra amplia gama de soluciones Kaspersky Security for Business integradas permite a Kaspersky Lab ofrecer todas las tecnologías y los servicios necesarios para implementar un ciclo de protección completo frente a ataques dirigidos: Preparación — Detección — Investigación — Análisis de datos — Protección automatizada.

VENTAJAS DEL SERVICIO

- Detecta rápidamente los incidentes.
- Recopila información suficiente para permitir la clasificación (entre falsos positivos o detección correcta).
- Identifica la frecuencia de los mecanismos recopilados, lo que permite determinar el nivel de peculiaridad de un ataque.
- Inicia el proceso de respuesta a un incidente de seguridad de la información.
- Inicia las actualizaciones necesarias de las bases de datos antivirus, con el fin de bloquear la difusión de las amenazas.

Más información sobre las fuentes de inteligencia frente a amenazas de Kaspersky

La inteligencia frente a amenazas se incorpora a partir de una fusión de fuentes heterogéneas de alta fiabilidad, que incluyen Kaspersky Security Network (KSN) y nuestras propias arañas web, nuestro servicio de supervisión de botnets (supervisión ininterrumpida de botnets y sus objetivos y actividades), trampas de spam, equipos de investigación, partners y otros datos históricos sobre objetos maliciosos recopilados por Kaspersky Lab a lo largo de más de dos décadas. A continuación, todos los datos agregados se inspeccionan cuidadosamente en tiempo real mediante varias técnicas de procesamiento previo; por ejemplo, criterios estadísticos, sistemas especializados de Kaspersky Lab (sandboxes, motores heurísticos, herramientas de similitud, creación de perfiles de análisis), validación de análisis y verificación de listas blancas.

Una vez que se disponga del personal con las habilidades y la formación adecuadas, y la inteligencia frente a amenazas adquirida a partir de fuentes fiables e implementada en los controles de seguridad existentes, es momento de considerar la respuesta ante incidentes.

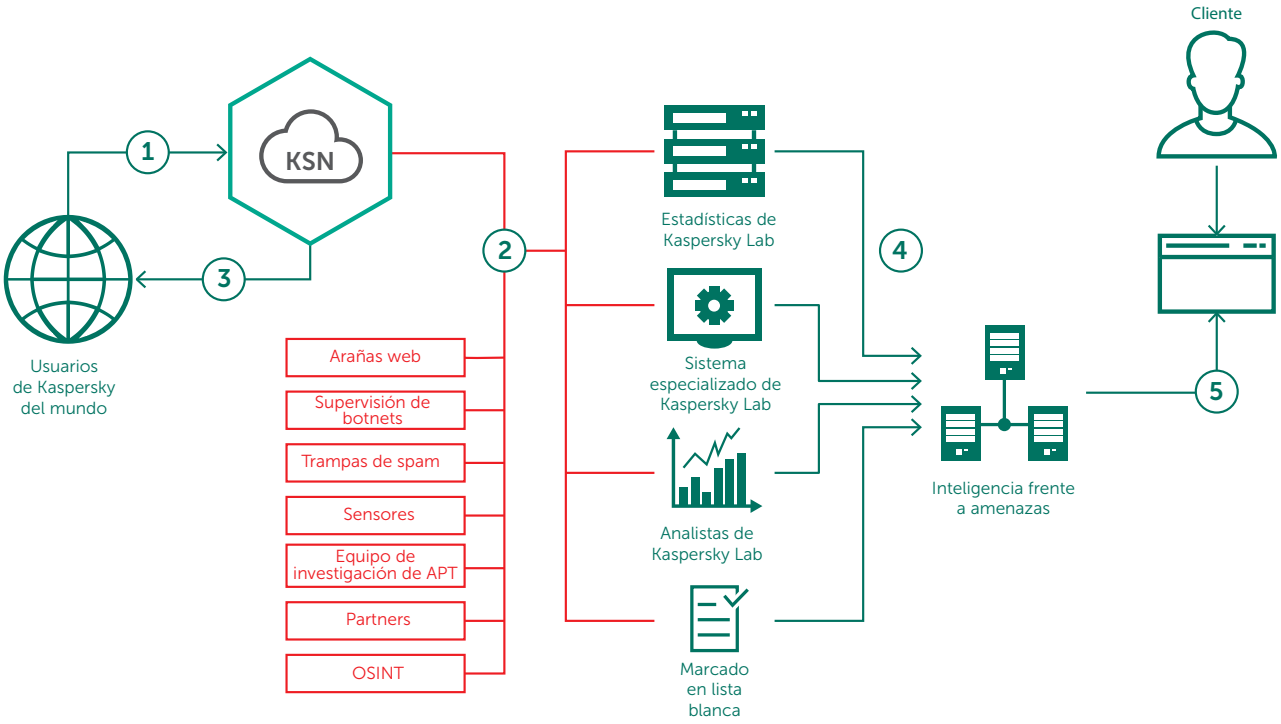


Figura 9:
Fuentes de inteligencia frente a amenazas de Kaspersky Lab

MARCO DE RESPUESTA ANTE INCIDENTES

La ciencia forense y la respuesta ante incidentes requieren la asignación de importantes recursos internos sin que apenas se note. Los especialistas con buenos conocimientos, y provistos de una amplia experiencia práctica en la lucha contra las ciberamenazas, deben actuar rápidamente para identificar, aislar y bloquear las actividades maliciosas. Si es necesario minimizar las consecuencias y los gastos de corrección, la velocidad es algo esencial.

Dominar este nivel de experiencia práctica con poca antelación puede ser difícil, incluso para un equipo de SOC bien establecido. Pocas organizaciones cuentan con suficientes recursos internos para detener un ataque avanzado antes de que se desarrolle. Además, puede haber casos, por ejemplo amenazas patrocinadas de estado complejo o APT, en los que el equipo de SOC carezca de conocimientos especializados sobre el enfoque y las tácticas específicas que utilizan los actores de APT implicados.

En esos casos, puede resultar más rentable o productivo colaborar con un proveedor de respuestas ante incidentes externo o un servicio de asesoría, que estarán equipados para aplicar una respuesta rápida y totalmente fundamentada.

Un marco de respuesta ante incidentes completo debe incluir lo siguiente:

- **Identificación de incidentes**
  Análisis inicial del incidente y aislamiento de los sistemas infectados.
- **Obtención de pruebas**
  En función del tipo de incidente, se requerirá la inspección de diferentes fuentes para obtener las pruebas necesarias.
- **Análisis de ciencia forense (si es necesario)**
  En esta etapa, se puede establecer una imagen detallada del incidente.
- **Análisis de malware (si es necesario)**
  Para conocer las capacidades de un malware determinado.
- **Plan de corrección**
  Desarrollo de un plan para erradicar tanto la causa primordial del problema como todos los rastros del código malicioso.
- **Lecciones aprendidas**
  Revisión y actualización de los controles de seguridad existentes para evitar incidentes similares.

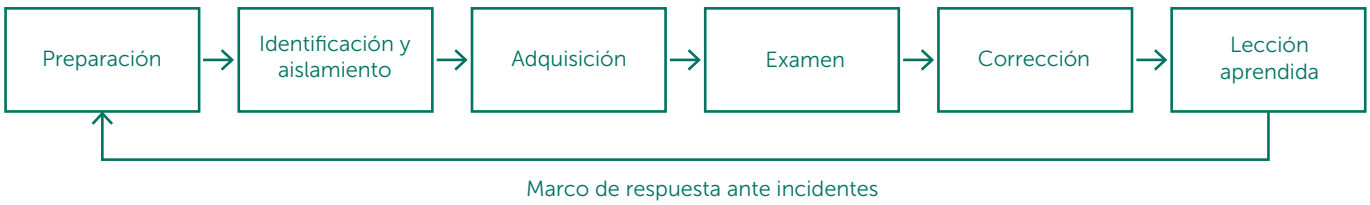


Figura 10:
Marco de respuesta ante incidentes

Kaspersky Lab ofrece:
Servicios de respuesta ante incidentes

La respuesta ante incidentes es uno de nuestros servicios premium, y abarca todo el ciclo de investigación del incidente, desde la adquisición de pruebas in situ hasta la identificación de indicadores adicionales de compromiso, con la preparación de un plan de corrección y la eliminación completa de la amenaza para su organización. Las investigaciones de Kaspersky Lab las llevan a cabo analistas e investigadores de detección de ciberintrusiones muy experimentados. Todo el peso de nuestra experiencia práctica mundial en ciencia forense digital y análisis de malware se aplica a la resolución del incidente de seguridad.

Durante la ejecución del servicio, se pretenden alcanzar los siguientes objetivos:

- Identificación de los recursos comprometidos.
- Aislamiento de la amenaza.
- Prevención de la propagación del ataque.
- Búsqueda y recopilación de pruebas.
- Análisis de las pruebas y reconstrucción de la cronología y la lógica del incidente.
- Análisis del malware utilizado en el ataque (si se detecta algún malware).
- Detección de las fuentes del ataque y otros sistemas potencialmente comprometidos (si es posible).
- Realización de análisis asistidos por herramientas de su infraestructura de IT para revelar posibles signos de compromiso.
- Análisis de las conexiones actuales entre su red y los recursos externos con el fin de detectar cualquier elemento sospechoso (como posibles servidores de comandos y control).
- Eliminación de la amenaza.
- Recomendación de acciones de corrección adicionales que puede emprender.

En función de si cuenta o no con su propio equipo de respuesta ante incidentes, puede pedir a nuestros expertos que lleven a cabo el ciclo de investigación completo, para identificar y aislar de forma sencilla los equipos comprometidos y evitar la distribución de la amenaza, o para realizar un análisis de malware o ciencia forense digital.

ANÁLISIS DE MALWARE

El análisis de malware ofrece una comprensión completa del comportamiento y los objetivos de los archivos de malware específicos dirigidos a su empresa. Los expertos de Kaspersky Lab llevan a cabo un análisis exhaustivo de la muestra de malware que proporciona, y crean un informe detallado que incluye:

- Propiedades de la muestra: una breve descripción de la muestra y una decisión sobre su clasificación como malware.
- Descripción detallada del malware: un análisis en profundidad de las funciones de la muestra de malware, el comportamiento y los objetivos de la amenaza (incluidos los indicadores de compromiso, IOC), para que disponga de la información necesaria para neutralizar sus actividades.
- Acción correctiva: en el informe se incluirán sugerencias para proteger totalmente a su empresa frente a este tipo de amenaza.

CIENCIA FORENSE DIGITAL

La ciencia forense digital puede incluir análisis de malware como se ha descrito anteriormente, si se ha detectado cualquier malware durante la investigación. Los expertos de Kaspersky Lab ensamblan las pruebas para entender exactamente lo que está sucediendo, incluidas las imágenes del disco duro, los volcados de memoria y los rastros de red. El resultado es una aclaración detallada del incidente. Como cliente, usted inicia el proceso con la recopilación de pruebas y una exposición del incidente. Los expertos de Kaspersky Lab analizan los síntomas del incidente, identifican el binario del malware (si lo hay) y realizan el análisis de malware con el fin de proporcionar un informe detallado con acciones correctivas.

OPCIONES DE DISTRIBUCIÓN

Los servicios de respuesta ante incidentes de Kaspersky Lab están disponibles de la siguiente forma:

- Mediante suscripción
- Como respuesta a un único incidente

Ambas opciones se basan en la cantidad de tiempo que emplean nuestros expertos en la resolución del incidente. Esto se negocia con el cliente antes de la firma del contrato. El cliente puede incluir de forma flexible tantas horas de trabajo como piense que es necesario o seguir las recomendaciones de nuestros expertos, personalizadas para cada caso específico.

¿POR QUÉ KASPERSKY LAB?

Porque ofrecemos lo siguiente:
- Relaciones de colaboración con organismos encargados de hacer cumplir las leyes, como Interpol y CERT.
- Herramientas en la nube que supervisan millones de ciberamenazas en todo el mundo en tiempo real.
- Equipos globales que analizan y comprenden todos los tipos de amenazas de Internet.

Porque somos:
- La mayor empresa de software de seguridad independiente del mundo, centrada en la inteligencia frente a amenazas y el liderazgo en tecnología.
- Líder indiscutible en más pruebas independientes de detección de malware que cualquier otro proveedor.
- Una empresa identificada como líder por Gartner, Forrester e IDC.

Acerca de Kaspersky Lab

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints. A lo largo de sus más de 18 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Con una sociedad de cartera registrada en el Reino Unido, Kaspersky Lab opera en casi 200 países y territorios de todo el mundo, y brinda protección a más de 350 millones de usuarios a nivel global.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab España
www.kaspersky.es

Todo sobre la seguridad
en Internet:
https://securelist.lat/

Encuentre un partner próximo:
www.kaspersky.com/buyoffline

KASPERSKY lab