
KASPERSKY lab
Centros de operaciones de seguridad con tecnología Kaspersky Lab
http://latam.kaspersky.com/

Aunque las empresas están aprendiendo a protegerse mejor, los criminales idean técnicas más y más sofisticadas cada día para penetrar sus barreras de seguridad. Atraídos por las ganancias sin precedentes que los ciberataques pueden ofrecer, cada vez son más los cibercriminales que buscan, identifican y aprovechan nuevas fallas de seguridad.

"Los centros de operaciones de seguridad deben diseñarse para la inteligencia, sobre la base de una arquitectura de seguridad adaptable que sea sensible al contexto y que esté potenciada por la inteligencia. Los encargados de la seguridad deben comprender cómo los centros de operaciones de seguridad potenciados por la inteligencia usan herramientas, procesos y estrategias para brindar protección contra las amenazas modernas".

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, noviembre de 2015

Se están estableciendo cada vez más centros de operaciones de seguridad (SOC, por sus siglas en inglés) para contrarrestar los problemas de seguridad a medida que surgen, así como para ofrecer una capacidad de respuesta y resolución rápida.

EL SOC ES UNA FUNCIÓN CENTRALIZADA PARA CONTROLAR Y ANALIZAR CONSTANTEMENTE LAS AMENAZAS, ASÍ COMO PARA PREVENIR Y MITIGAR INCIDENTES DE CIBERSEGURIDAD

En una encuesta reciente, que se publicará a fines de 2016 e incluyó a más de 4000 empresas de 25 países, B2B International descubrió lo siguiente:

- En los doce meses anteriores al estudio, el **38 %** de los encuestados había experimentado problemas **graves con virus y software malicioso** y una consiguiente pérdida de productividad.
- El **21 %** había experimentado **una pérdida o filtración de datos debido a ataques dirigidos**.
- Cerca del 40 % de los encuestados siente especial preocupación por estos desafíos.
- En el mismo período de doce meses, el **17 %** de las empresas había sido víctima de al menos un **ataque DDoS**. En muchos casos, el número de ataques fue incluso mayor.
- El **42 %** de los encuestados que experimentaron **ataques de phishing** fueron grandes empresas.
- El **26 %** de los eventos de seguridad **no se detectó** durante varias semanas o más; los problemas solo quedaron al descubierto debido a auditorías de seguridad externas.
- Para una gran empresa, el **impacto financiero promedio** de sufrir al menos una vulneración de datos fue de **USD 891 000** (este monto incluye los salarios del personal interno adicional, el perjuicio para la solvencia o las primas de seguro, la pérdida de negocios, la contratación de consultores externos y el trabajo de relaciones públicas adicional para reparar el daño a la marca).
- El monto del **impacto** para una gran empresa **osciló entre USD 393 000 y USD 1 100 000**, dependiendo de cuándo se detectó el problema de seguridad: la detección temprana significó un costo menor.
- El tiempo también repercutió en el total de registros afectados: con detección prácticamente instantánea (con sistema de detección instalado), el daño se limitó a 9000 registros de clientes/empleados; la cifra ascendió a 240 000 cuando el ataque se mantuvo sin detectar por más de un año.

Según el modelo de arquitectura de seguridad adaptable de Gartner, para lograr combatir el delito cibernético en el panorama de amenazas actual, el equipo del SOC debe poder:

- PREDECIR
- DETECTAR
- PREVENIR
- RESPONDER

Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, febrero de 2014, Foundational enero de 2016

CUATRO ELEMENTOS CLAVE

Es necesario aplicar cuatro elementos clave, junto con procesos claramente definidos y tecnologías relevantes, para respaldar este enfoque reconocido por la industria. Estos son:

- **GESTIÓN DE CONOCIMIENTOS.** El personal (los miembros del equipo del SOC) debe estar bien capacitado en análisis forense digital, análisis de malware y respuesta a incidentes para prevenir y responder en forma correcta a ataques cada vez más sofisticados.
- **INTELIGENCIA DE AMENAZAS.** Esta información, fundamental para detectar a tiempo las últimas amenazas, debe recopilarse de numerosas fuentes (mientras más, mejor):
    1. Datos de amenazas internos
    2. Inteligencia de códigos abiertos (OSINT)
    3. CERT de la industria
    4. Proveedores de soluciones antimalware globales
- **BÚSQUEDA DE AMENAZAS.** Búsqueda proactiva de amenazas que los sistemas de seguridad tradicionales (firewalls, IPS/IDS, SIEM, etc.) no logren detectar.
- **MARCO DE RESPUESTA A INCIDENTES.** Se implementa para limitar el perjuicio y reducir los costos de corrección.

Cada uno de estos elementos tiene la misma importancia, por lo que merecen considerarse por separado.

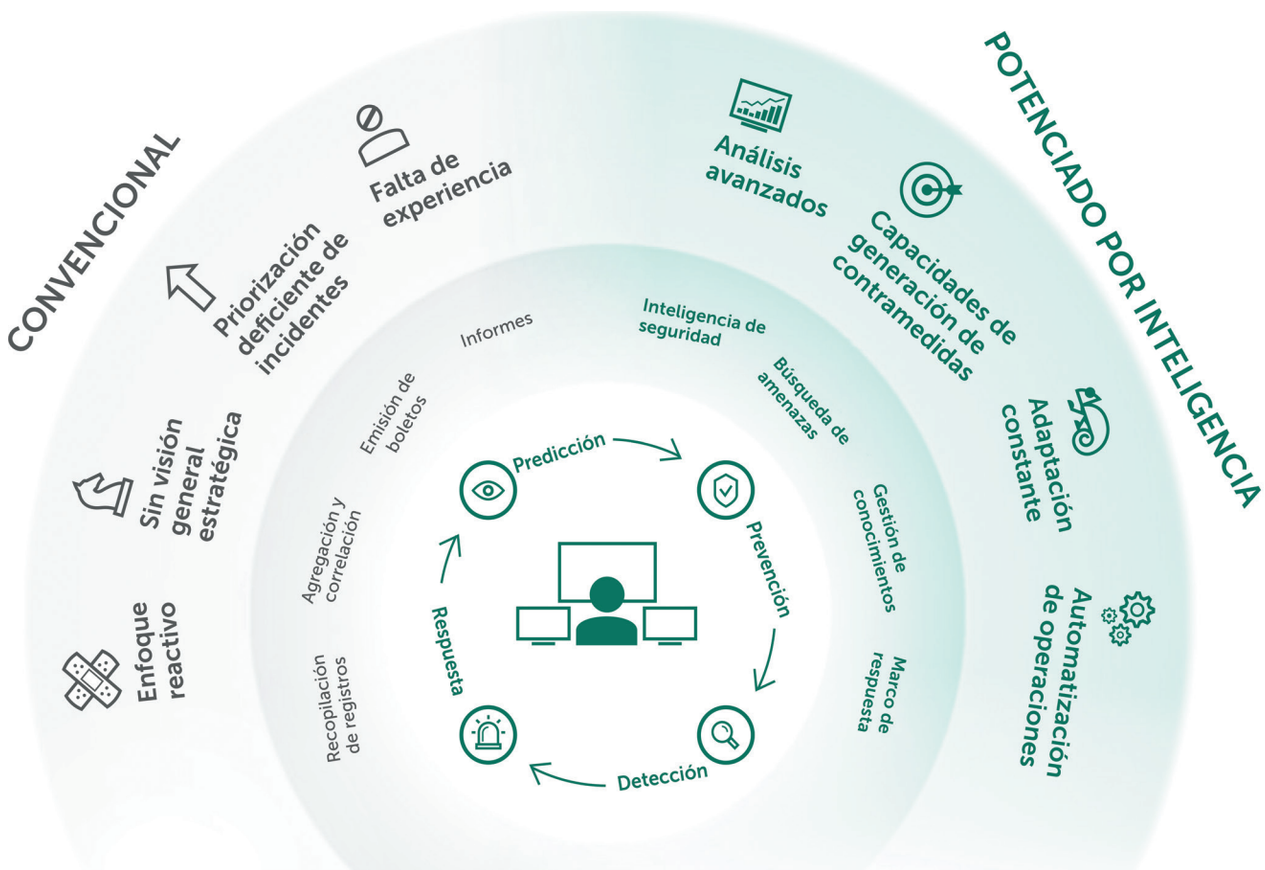


Figura 1:
Los cuatro elementos clave del SOC

GESTIÓN DE CONOCIMIENTOS

El SOC debe ofrecer un repositorio de conocimientos prácticos y la experiencia necesaria para analizar una enorme cantidad de datos e identificar dónde es necesario investigar en mayor profundidad.

Los presupuestos limitados hacen que contratar personal para un SOC sea un desafío.

Actualmente, el mercado está experimentando una escasez de profesionales de ciberseguridad bien capacitados, lo que genera costos mayores de selección y contratación.

La persona ideal para formar parte de un SOC debe tener las siguientes características:
- Una mente curiosa, capaz de elaborar un panorama general y cohesivo a partir de fragmentos de datos dispersos.
- La capacidad de mantenerse enfocada bajo altos niveles de estrés.
- Conocimientos generales relevantes de TI y ciberseguridad, de preferencia con una vasta experiencia práctica.

Ya sea que planee llenar las vacantes del SOC a través de búsquedas externas o ascensos internos, encontrar personas que ya posean todas las habilidades deseadas no es fácil. Deberá ofrecer capacitación constante, no solo para subsanar las deficiencias entre las habilidades existentes y las necesarias, sino también para que los miembros del equipo estén en condiciones de trabajar con tecnologías de seguridad y un entorno de amenazas en constante evolución.

La respuesta a incidentes, el análisis forense digital y el análisis de malware son competencias indispensables.

RESPUESTA A INCIDENTES Y ANÁLISIS FORENSE DIGITAL

- Brindar una respuesta oportuna y precisa ante un incidente
- Analizar evidencia (imágenes de disco duro, volcados de memoria, trazas de actividad en la red) y reconstruir la cronología y la lógica del incidente
- Hallar los presuntos orígenes del ataque, así como otros sistemas que puedan haberse visto afectados (si es posible)
- Comprender la causa raíz del incidente para evitar casos similares en el futuro

ANÁLISIS DE MALWARE

- Comprender la muestra de software sospechoso y sus capacidades
- Determinar si en verdad se trata de malware
- Determinar el impacto que la muestra podría tener en los sistemas afectados de la organización
- Elaborar un plan de corrección integral basado en el comportamiento del malware descubierto

Kaspersky Lab ofrece:
Servicios de capacitación en ciberseguridad

Kaspersky Lab lleva más de 17 años ampliando y desarrollando sus conocimientos en distintas áreas de la ciberseguridad, como la detección de amenazas, la investigación de malware, la ingeniería inversa y el análisis forense digital. Nuestros expertos conocen la mejor manera de contrarrestar las amenazas que suponen las 325 000 muestras de malware que detectamos cada día, así como la forma de transmitir esos conocimientos a organizaciones expuestas a los nuevos peligros de la realidad cibernética actual.

Nuestro programa de capacitación en seguridad es obra de las mismas personas que ayudaron a crear los laboratorios antivirus de Kaspersky, autoridades que hoy inspiran y orientan a la siguiente generación de expertos globales.

Los cursos están diseñados para incluir tanto clases teóricas como prácticas en "laboratorios". Al término de cada curso, se invita a los participantes a validar sus conocimientos mediante una evaluación.

Los cursos de capacitación son ideales para profesionales de TI que poseen habilidades generales o avanzadas de administración de sistemas y programación. Todos los cursos pueden dictarse en las instalaciones del cliente o en las oficinas locales o regionales de Kaspersky Lab, según corresponda.

DESCRIPCIÓN DEL PROGRAMA

TEMAS	DURACIÓN	HABILIDADES ADQUIRIDAS
ANÁLISIS FORENSE DIGITAL		
• Introducción al análisis forense digital • Respuesta inmediata y adquisición de evidencia • El Registro de Windows por dentro • Análisis de artefactos de Windows • Análisis forense de navegadores • Análisis de correo electrónico	5 días	• Construir un laboratorio de análisis forense digital • Recopilar evidencia digital y procesarla correctamente • Recrear un incidente y utilizar marcas de fecha y hora • Detectar una intrusión valiéndose de artefactos de Windows • Encontrar y analizar el historial de navegación y de correo electrónico • Aplicar con confianza herramientas y técnicas de análisis forense digital
ANÁLISIS DE MALWARE E INGENIERÍA INVERSA		
• Objetivos y técnicas del análisis de malware y la ingeniería inversa • Aspectos internos de Windows, archivos ejecutables y ensamblador x86 • Técnicas de análisis estático básico (extracción de cadenas, análisis de importación, puntos de entrada de PE en un solo vistazo, desempaquetado automático, etc.) • Técnicas de análisis dinámico básico (depuración, herramientas de monitoreo, interceptación de tráfico, etc.) • Análisis de archivos de .NET, Visual Basic, Win64 • Técnicas de análisis de scripts y archivos no PE (archivos por lotes, Autoit, Python, JScript, JavaScript, VBS)	5 días	• Crear un entorno seguro para el análisis de malware: implementar espacios aislados y todas las herramientas necesarias • Comprender los principios de ejecución de programas de Windows • Desempaquetar, depurar y analizar objetos maliciosos e identificar sus funciones • Detectar sitios maliciosos a través del análisis de script de malware • Realizar análisis rápidos de malware

TEMAS	DURACIÓN	HABILIDADES ADQUIRIDAS
ANÁLISIS FORENSE DIGITAL AVANZADO		
• Análisis forense profundo de Windows • Recuperación de datos • Análisis forense de red y nube • Análisis forense de la memoria • Análisis cronológico • Práctica de análisis forense de ataques dirigidos reales	5 días	• Ser capaz de realizar análisis profundos del sistema de archivos • Ser capaz de recuperar archivos eliminados • Ser capaz de analizar el tráfico de red • Revelar actividades maliciosas a partir de volcados de memoria • Recrear la cronología de un incidente
ANÁLISIS DE MALWARE E INGENIERÍA INVERSA AVANZADOS		
• Técnicas de análisis estático avanzado (analizar código shell estáticamente, analizar el encabezado PE, TEB, PEB, cargar funciones de distintos algoritmos de hash) • Técnicas de análisis dinámico avanzado (estructura PE, desempaquetado manual y avanzado, desempaquetado de empaquetadores maliciosos que almacenan el ejecutable completo en formato cifrado) • Ingeniería inversa de APT (contempla una situación de ataque de APT, desde el correo electrónico de phishing hasta el nivel más profundo posible) • Análisis de protocolos (se analiza el protocolo de comunicación cifrado de C2 y cómo descifrar el tráfico) • Análisis de rootkits y bootkits (depuración del sector del arranque usando IDA y VMware, depuración de un kernel usando dos máquinas virtuales, análisis de muestras de rootkits)	5 días	• Ser capaz de seguir las prácticas recomendadas de ingeniería inversa y reconocer los trucos que se utilizan en su contra (ofuscación, antidepuración) • Ser capaz de aplicar técnicas de análisis de malware avanzadas para diseccionar un rootkit o bootkit • Ser capaz de analizar el código shell de un exploit incorporado en distintos tipos de archivos, así como malware para sistemas distintos de Windows
RESPUESTA A INCIDENTES		
• Introducción a la respuesta a incidentes • Detección y análisis primario • Análisis digital • Creación de reglas de detección (Yara, Snort, Bro)	5 días	• Diferenciar las APT de otras amenazas • Comprender las técnicas de diversos atacantes y la anatomía de un ataque dirigido • Aplicar métodos específicos de monitoreo y detección • Seguir el flujo de trabajo para responder a un incidente • Reconstruir la cronología y la lógica de un incidente • Crear reglas de detección e informes

Las herramientas cambian con el tiempo, pero los aspectos básicos y los métodos de trabajo siguen siendo los mismos. Los participantes no solo recibirán un conjunto de herramientas e instrucciones, también lograrán comprender los principios fundamentales y la funcionalidad. Todas las tareas prácticas se basan en casos reales, siempre que esto pueda hacerse sin infringir la confidencialidad del cliente.

INTELIGENCIA DE AMENAZAS Y BÚSQUEDA DE AMENAZAS

Tradicionalmente, el SOC tenía a su cargo lo siguiente:

- Gestión de los dispositivos de seguridad, mantenimiento del perímetro y administración de las tecnologías de seguridad preventiva, como los sistemas IPS/IDS, los firewalls, los servidores proxy, etc.
- Control de los eventos de seguridad, a través de un sistema de administración de eventos e información de seguridad (SIEM, por sus siglas en inglés).
- Análisis forense y aplicación de medidas correctivas ante un incidente.
- Cumplimiento de las normativas internas y reglamentarias (por ejemplo, PCI DSS).

En la actualidad, numerosas organizaciones tienen planificado obtener mayor visibilidad de las amenazas estableciendo sus propios SOC. Sin embargo, algunas organizaciones que ya cuentan con un SOC descubren que aún enfrentan muchos de los mismos problemas.
Esto sucede por varios motivos:

- Priorización deficiente, que se traduce en que las amenazas reales quedan sepultadas bajo los miles de alertas insignificantes que se reciben y analizan todos los días.
- Aplicación de medidas correctivas tras un incidente sin comprender a cabalidad los TTP (tácticas, técnicas y procedimientos) de los atacantes, lo que lleva a pasar por alto ataques avanzados.
- Falsos negativos por no contar con datos adecuados sobre las amenazas.
- Una actitud reactiva en lugar de proactiva, es decir, una tendencia a reaccionar a un incidente en lugar de buscar activamente amenazas que aún no se hayan descubierto, pero que puedan estar activas en la organización.
- La falta de una visión general y estratégica del panorama de amenazas existente, así como un desconocimiento de los ataques que sufren otras empresas y de las contramedidas disponibles.

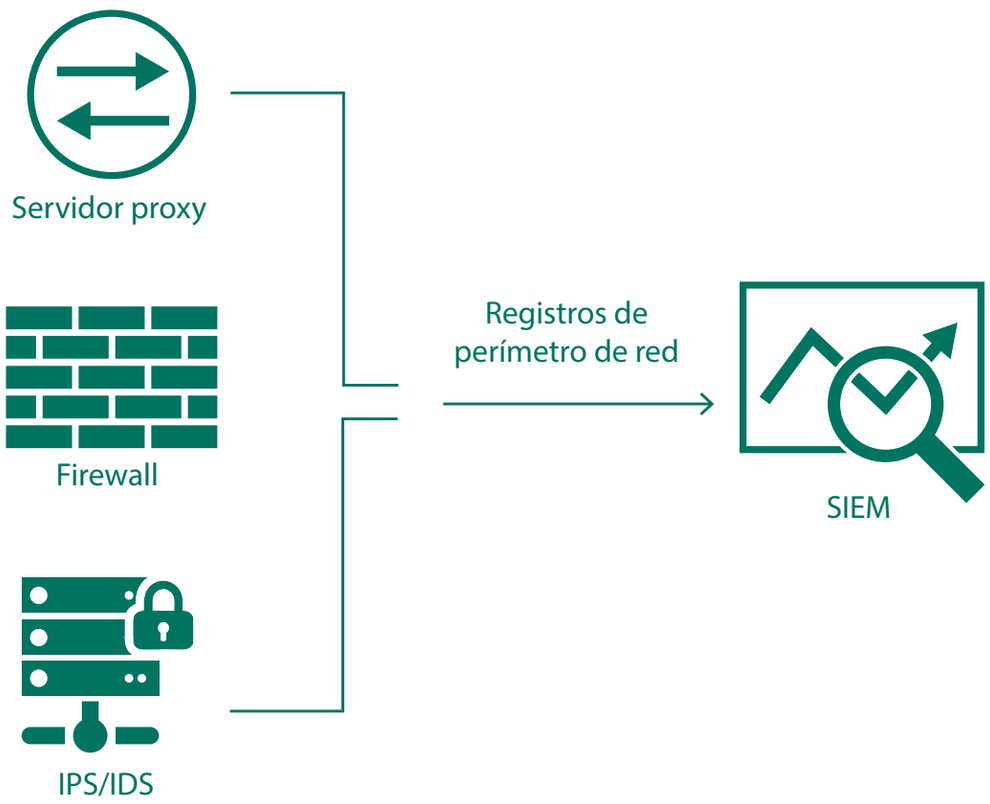


Figura 2:
Un SOC convencional

- Problemas para conseguir financiación interna para tecnologías de seguridad específicas; esto suele deberse a una incapacidad para comunicar, a ejecutivos no técnicos, el riesgo que una vulneración implicaría para los procesos de negocios.

Gartner define la inteligencia de amenazas como:
"Conocimiento basado en evidencias, con contexto, mecanismos, indicadores, implicaciones y asesoramiento práctico, sobre una amenaza o un riesgo existente o emergente para los activos, y que se puede utilizar para tomar decisiones fundamentadas sobre la respuesta del sujeto a la amenaza o el riesgo".

Gartner, How Gartner Defines Threat Intelligence, febrero de 2016

Dadas estas consideraciones, es recomendable que los encargados de la seguridad se adhieran a un enfoque de SOC potenciado por la inteligencia. Para que el SOC sea eficaz, debe poder incorporar nuevas tecnologías y controles de manera continua, en respuesta a los grandes cambios que experimenta el panorama de amenazas.

La combinación de datos de amenazas internos con información recopilada de distintas fuentes (por ejemplo, OSINT o proveedores de soluciones antimalware globales) permite comprender las técnicas de ataque y sus indicadores potenciales. A su vez, esto permite a las organizaciones desarrollar estrategias de defensa eficientes, que les permitan protegerse de ataques básicos y avanzados dirigidos puntualmente a ellas.

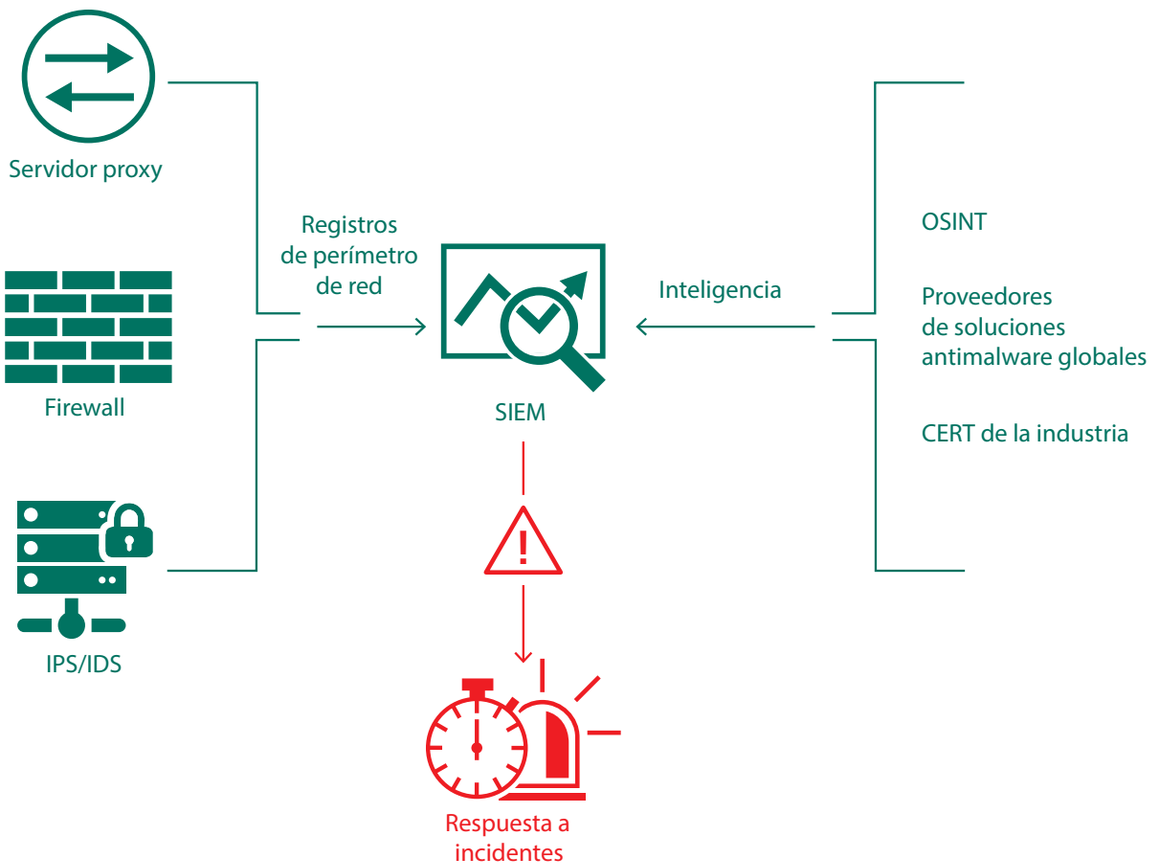


Figura 3:
El SOC potenciado por la inteligencia

Es necesario seleccionar cuidadosamente las fuentes de inteligencia. Existe una correlación directa entre la calidad de la inteligencia y la eficacia de las decisiones que se basan en ella. Si confía en inteligencia irrelevante, imprecisa o inadecuada para las metas de su industria o empresa, o si no recibe información sobre amenazas en forma oportuna, la calidad del proceso de toma de decisiones de su organización se puede ver gravemente afectada.

Los datos sin procesar y sin contexto no ofrecerán la relevancia necesaria para que el equipo del SOC trabaje con total eficacia. Por ejemplo, saber solamente que una URL es maliciosa dista mucho de saber también que se la usa para albergar un exploit o un tipo específico de malware. Esta capa adicional de inteligencia les indicará a sus expertos en seguridad a que deberán estar atentos mientras exploren un equipo infectado.

Esto es lo que debe buscar en una fuente externa de inteligencia de amenazas:

- Inteligencia de alcance global, que ofrezca una visión lo más completa posible de los ataques.
- Un proveedor con antecedentes sólidos en la detección temprana de nuevos indicadores de amenazas.
- Inteligencia contextualizada, que pueda usar de inmediato para tomar una decisión.
- Formatos y mecanismos de entrega que faciliten la integración con los controles de seguridad existentes.

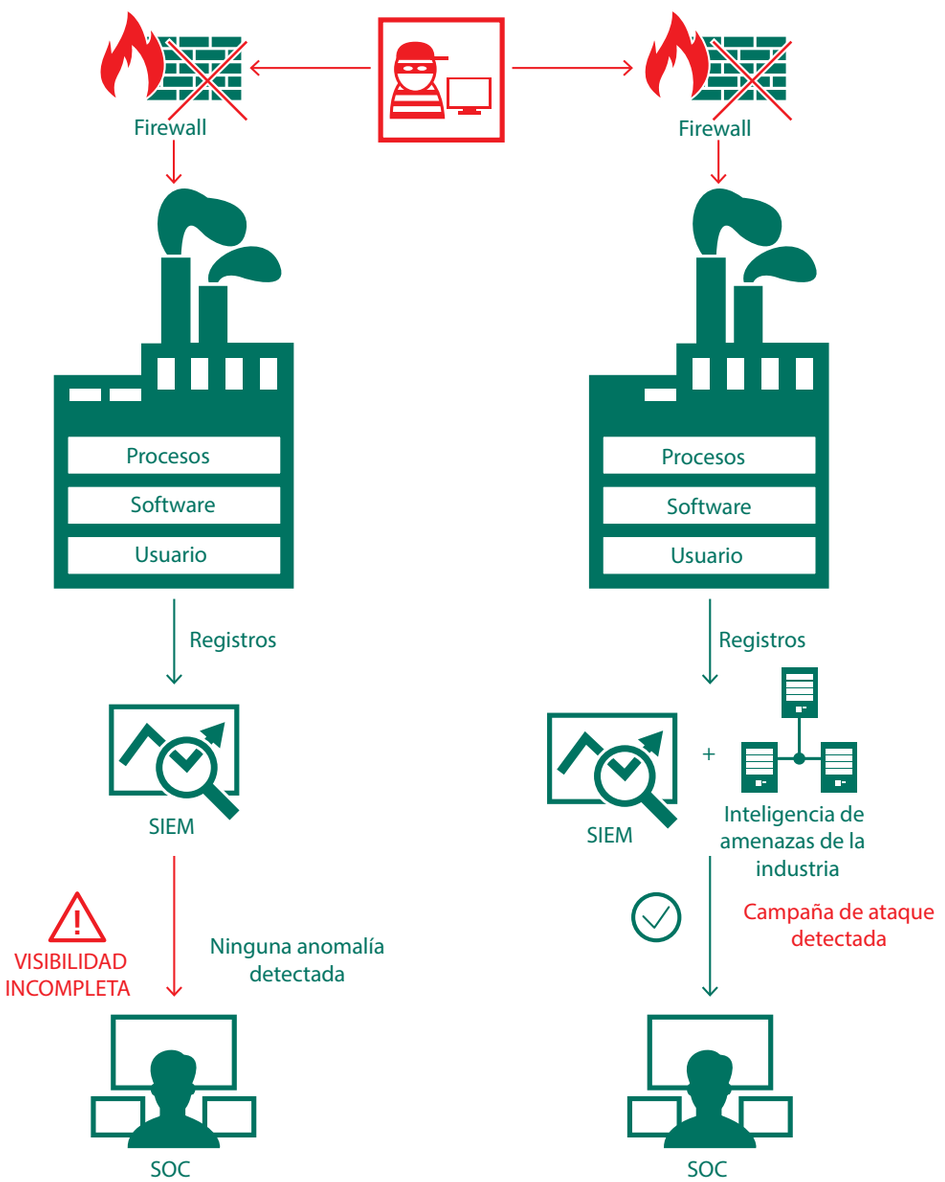


Figura 4:
Modelo de inteligencia de amenazas

La búsqueda de amenazas también es un elemento importante de las operaciones cotidianas de un SOC. Este no es un concepto nuevo. La detección de amenazas desconocidas y avanzadas depende del arduo trabajo manual de los analistas de seguridad, no de mecanismos automatizados basados en reglas o firmas.

Este proceso involucra la recopilación y aplicación de distintas técnicas (como análisis estadístico, aprendizaje computarizado y visualización) a todos los datos disponibles obtenidos de endpoints, redes, controles de seguridad implementados, sistemas de autenticación, etc. El propósito es confirmar una hipótesis existente sobre la posible fuga de datos. Las tecnologías de búsqueda de amenazas que el analista puede utilizar incluyen las ya mencionadas: soluciones SIEM, OSINT, plataformas de inteligencia de amenazas y otras fuentes de datos.

Para hallar las amenazas, el analista consulta IOC obtenidos de fuentes externas y, por medio de herramientas especializadas, busca los respectivos artefactos (direcciones IP, hashes de archivo, URL, etc.) en los hosts de la organización. Cuando encuentra una señal evidente de que la seguridad se ha visto vulnerada, puede dar inicio a los procedimientos para responder al incidente.

Realizar una búsqueda en enormes volúmenes de datos para identificar artefactos que las medidas automatizadas no pudieron detectar es una tarea solo para profesionales altamente calificados y experimentados.

Kaspersky Lab ofrece:
Fuentes de datos de inteligencia de amenazas

Kaspersky Lab ofrece fuentes de datos de inteligencia de amenazas que se actualizan en forma continua para informar al equipo del SOC sobre los riesgos e implicaciones asociados a las ciberamenazas. La información lo ayudará a evitar riesgos con mayor eficacia y a preparar sus defensas para ataques que aún no hayan tenido lugar.

DESCRIPCIÓN DE LAS FUENTES DE DATOS

Fuentes de reputación de IP: conjunto de direcciones IP con contexto para protegerse de hosts sospechosos y maliciosos.

Direcciones URL maliciosas: conjunto de direcciones URL formado por vínculos y sitios web maliciosos. Hay registros enmascarados y no enmascarados.

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

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

Fuentes de datos de whitelisting: conjunto de hashes de archivo que permite a las soluciones y servicios de terceros contar con un catálogo sistemático de software legítimo.

Fuentes de hashes maliciosos: comprenden los tipos de malware más peligrosos, frecuentes y emergentes.

Fuentes de hashes maliciosos para plataformas móviles: conjunto de hashes de archivo para detectar objetos maliciosos que infectan plataformas móviles.

Fuentes de datos de troyanos P-SMS: conjunto de hashes de troyanos, con su contexto correspondiente, para detectar troyanos SMS que le generan cargos al usuario y que además permiten a un atacante robar, eliminar y responder mensajes SMS.

Direcciones URL de C&C de botnets móviles: conjunto de direcciones URL con contexto para protegerse de servidores de C&C utilizados en botnets móviles.

ASPECTOS DESTACADOS DEL SERVICIO

- Las fuentes de datos se generan en forma automática y en tiempo real, a partir de descubrimientos registrados en todo el mundo (Kaspersky Security Network nos facilita una visión de un porcentaje significativo del tráfico total de Internet, ya que conecta a decenas de millones de usuarios finales en más de 200 países). Combinados, estos factores permiten obtener altas tasas de detección y precisión.
- Cada registro de cada fuente de datos está enriquecido con contexto práctico (nombres de amenazas, marcas de fecha y hora, ubicación geográfica, direcciones IP de recursos web infectados, hashes, popularidad, etc.). La información contextual ayuda a revelar el "panorama general" tras los datos, a validarlos y a ampliar sus posibilidades de uso. Con datos contextualizados, tendrá mayor facilidad para responder las preguntas "quién", "qué", "dónde" y "cuándo", que le permitirán identificar a sus adversarios y tomar decisiones y medidas oportunas para proteger específicamente a su organización.
- Los formatos de difusión ligeros y básicos (JSON, CSV, OpenIOC, STIX) y el uso de HTTPS o mecanismos de entrega ad-hoc facilitan la integración de las fuentes con las soluciones de seguridad.
- La inteligencia de amenazas se genera y controla a través de una infraestructura altamente tolerante a fallas, que garantiza una disponibilidad continua y un rendimiento uniforme.
- Integración inmediata con HP ArcSight, IBM QRadar, Splunk y más.

Kaspersky Threat Lookup

Kaspersky Threat Lookup ofrece todos los conocimientos que ha adquirido Kaspersky Lab sobre las ciberamenazas y sus relaciones, reunidos en un único y poderoso servicio web. El objetivo es proporcionar al equipo del SOC la mayor cantidad posible de datos para prevenir ciberataques antes de que afecten a la organización. La plataforma recupera la última inteligencia disponible sobre direcciones URL, dominios, direcciones IP, hashes de archivo, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, etc. Con ello se obtiene una visión global y completa de las amenazas nuevas y emergentes, que lo ayudará a proteger su organización y a optimizar la respuesta ante un incidente.

ASPECTOS DESTACADOS DEL SERVICIO

- Inteligencia de confianza: un atributo clave de Kaspersky Threat Lookup es la confiabilidad de sus datos de inteligencia, enriquecidos con información contextual práctica. Los productos de Kaspersky Lab son líderes en las pruebas antimalware[1], lo que demuestra la calidad sin igual de nuestra inteligencia de seguridad, ya que ofrecemos las más altas tasas de detección, con casi cero falsos positivos.
- Altos niveles de cobertura en tiempo real: la inteligencia de amenazas se genera automáticamente y en tiempo real, con base en descubrimientos de todo el mundo y con el respaldo de Kaspersky Security Network.
- Búsqueda de amenazas: sea proactivo en la prevención, la detección y la respuesta a ataques a fin de minimizar su impacto y frecuencia. Rastree y elimine ataques en forma agresiva y con la mayor antelación posible. Mientras más pronto descubra una amenaza, menor será el daño resultante, más rápido se efectuarán las reparaciones y más pronto volverán a la normalidad las operaciones de la red.
- Datos enriquecidos: la inteligencia de amenazas que ofrece Kaspersky Threat Lookup consta de toda clase de datos: hashes, URL, IP, whois, pDNS, GeoIP, atributos de archivo, datos estadísticos y de comportamiento, cadenas de descarga, marcas de fecha y hora, y mucho más. Con la ayuda de estos datos, podrá sondear el diverso panorama de amenazas que atentan contra su seguridad.
- Disponibilidad continua: la inteligencia de amenazas se genera y controla a través de una infraestructura altamente tolerante a fallas, que garantiza una disponibilidad continua y un rendimiento uniforme.
- Revisión continua por parte de expertos en seguridad: nuestra inteligencia cuenta con el aval y aporte de cientos de expertos, como los afamados investigadores de nuestro equipo de seguridad GReAT, equipos de I+D de vanguardia y analistas de seguridad de todo el mundo.

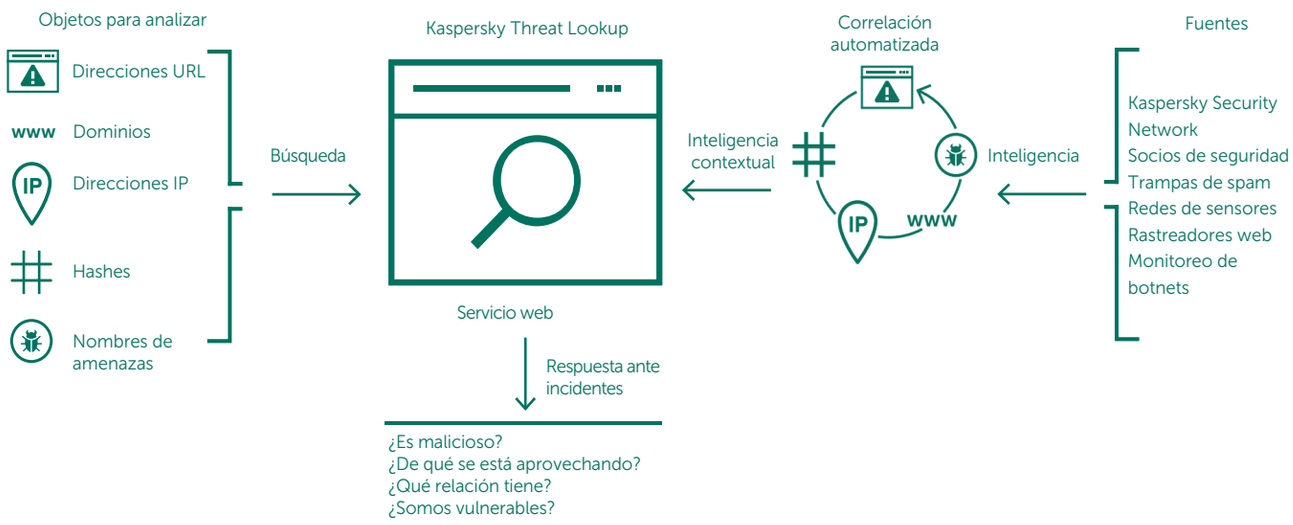
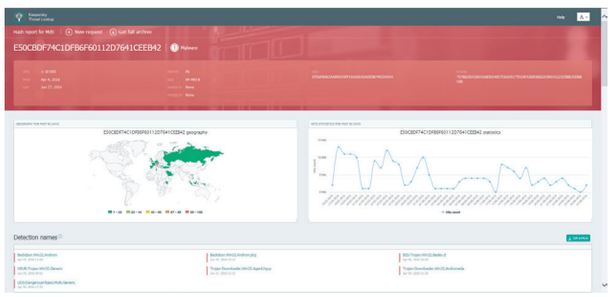
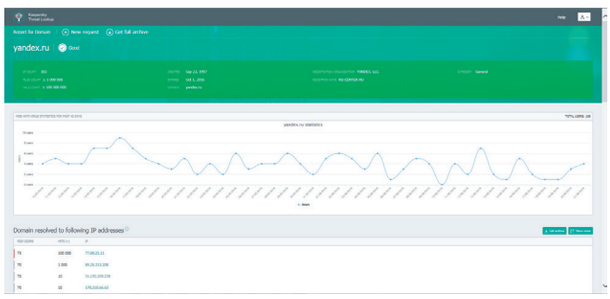


Figura 5:
Kaspersky Threat Lookup

1 https://latam.kaspersky.com/top3

- Análisis en "sandbox": detecte amenazas desconocidas ejecutando objetos sospechosos en un entorno seguro y revise el alcance completo del comportamiento y los artefactos de las amenazas a través de informes de fácil lectura.
- Amplia gama de formatos de exportación: los IOC (indicadores de compromiso) y la información contextual pueden exportarse en formatos muy utilizados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV. Con ello, podrá disfrutar de todos los beneficios de la inteligencia de amenazas en formatos organizados y procesables, que le permitirán automatizar el flujo de trabajo de operaciones o integrar la información en un sistema SIEM u otros controles de seguridad.
- Interfaz web o API RESTful fáciles de usar: use el servicio en modo manual con una interfaz web (a través de un navegador) o acceda a él mediante una sencilla API RESTful, según lo prefiera.





APT Intelligence Reporting

Cuando se descubre una amenaza persistente avanzada (APT), el hallazgo no siempre se da a conocer de inmediato. De hecho, muchos descubrimientos jamás se hacen públicos. Usted puede ser el primero en conocer nuestras investigaciones más recientes, gracias a nuestros exclusivos, prácticos y exhaustivos informes de inteligencia sobre las APT.

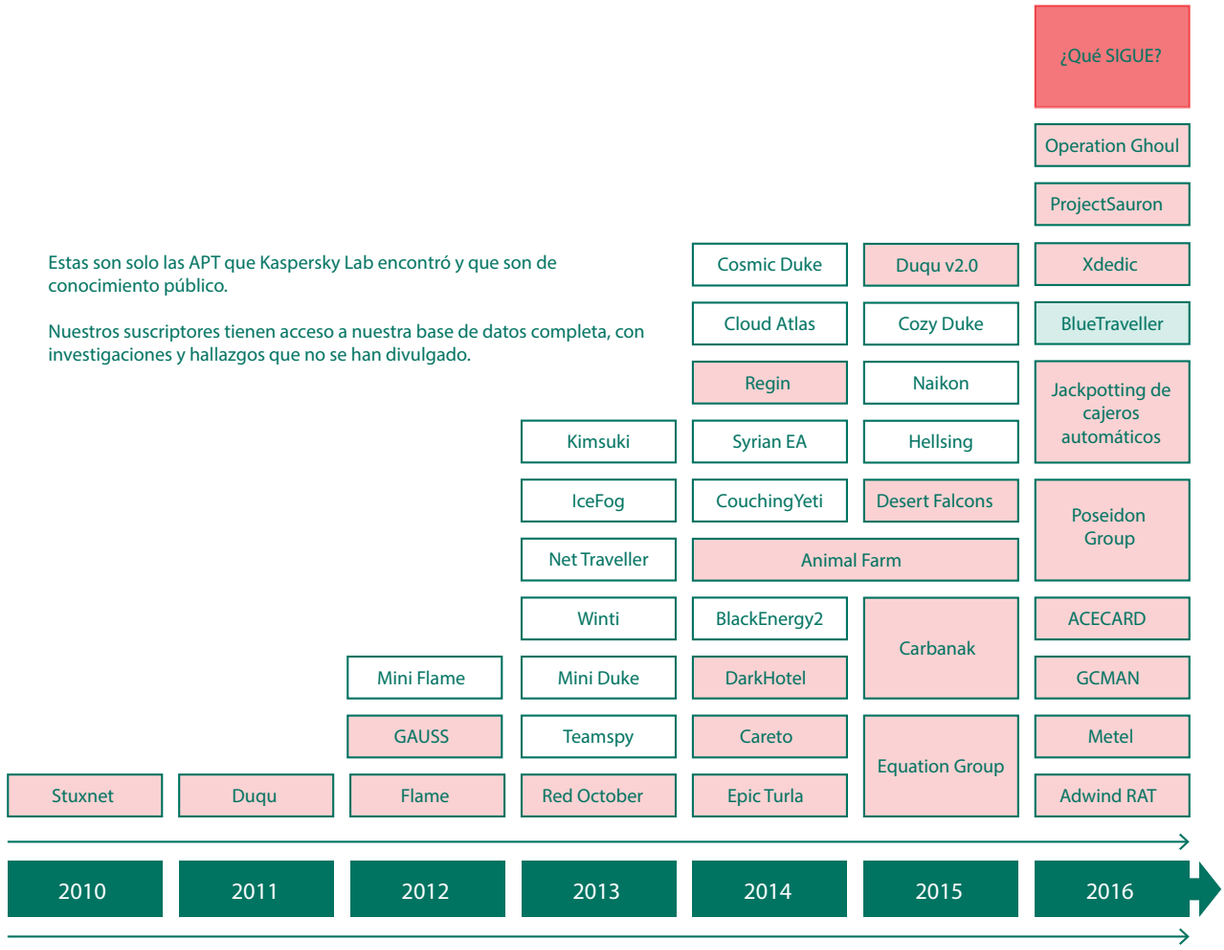


Figura 6:
APT descubiertas por Kaspersky Lab

Al suscribirse a APT Intelligence Reporting de Kaspersky, obtendrá acceso especial y continuo a nuestras investigaciones, hallazgos y datos técnicos (en una gran variedad de formatos) sobre cada APT descubierta, incluidas las que nunca se divulgarán públicamente. Nuestros expertos, los cazadores de APT más hábiles y eficaces de la industria, además le avisarán de inmediato sobre cualquier cambio que detecten en las tácticas de los cibercriminales y los grupos de ciberterroristas. También podrá acceder a la base de datos de informes de APT completa, un formidable componente de investigación y análisis para sumar al arsenal de seguridad corporativo.

ASPECTOS DESTACADOS DEL SERVICIO

- Acceso exclusivo a descripciones técnicas de las amenazas avanzadas que estemos investigando, antes de que divulguemos la información.
- Información sobre APT no públicas. No todas las amenazas de alto perfil están sujetas a notificación pública. Algunas de ellas, debido a la identidad de las víctimas afectadas, lo delicado de los datos, la naturaleza del proceso de corrección de la vulnerabilidad o la actividad policial asociada, nunca se divulgan al público. Sin embargo, todas se divulgan a nuestros clientes.
- Detalles técnicos auxiliares, muestras y herramientas, una lista completa de indicadores de compromiso (IOC) en formato OpenIOC y acceso a nuestras reglas de Yara.
- Vigilancia continua de las campañas de APT. Acceso a inteligencia práctica durante la investigación (información sobre distribución de APT, IOC, infraestructura de C&C).
- Análisis retrospectivo: durante el período de suscripción, tendrá acceso a todos los informes privados que se hayan preparado en el pasado.

Desde un punto de vista práctico, para los expertos de un SOC, el componente más útil de un informe son los IOC. Esta información estructurada puede usarse con herramientas automatizadas específicas que ayudan a analizar una infraestructura en busca de señales de infección.
Todos los informes se entregan a través del Portal de inteligencia de APT, como se ilustra a continuación.

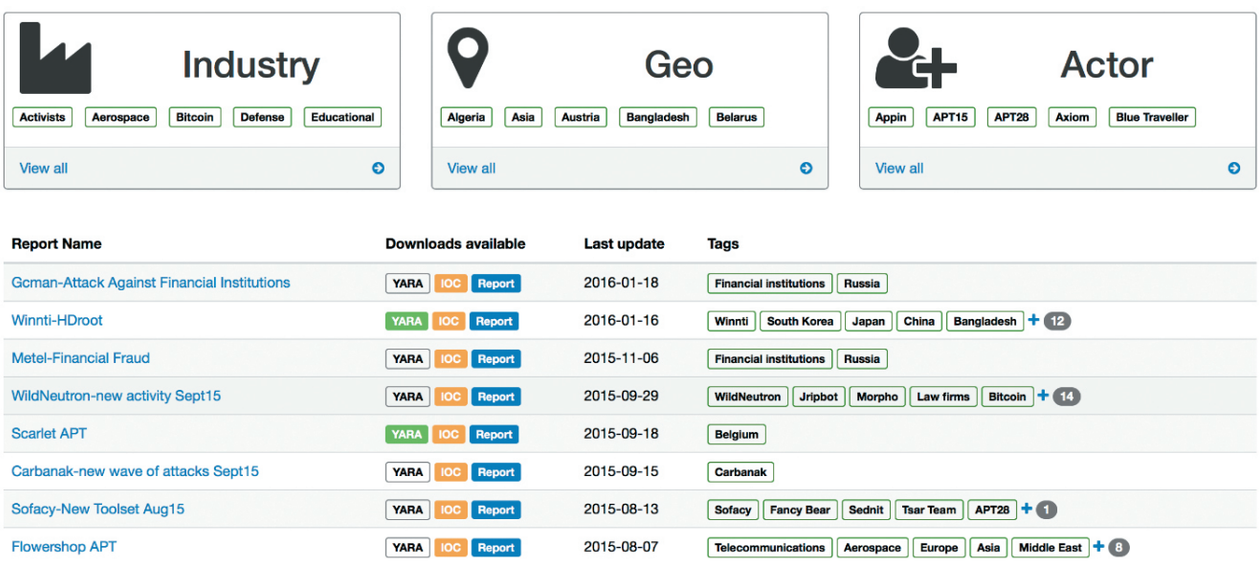


Figura 7:
Portal de inteligencia de APT

Informes Personalizados de Amenazas

Informes de amenazas por cliente

¿Cuál es la mejor manera de montar un ataque contra su organización? ¿Qué rutas y qué información están disponibles para un criminal que dirige un ataque específicamente contra usted? ¿Ya se ha montado un ataque o están a punto de atacarlo?

Con sus informes de amenazas por cliente, Kaspersky lo ayudará a responder estas y otras preguntas. Nuestros expertos identificarán los puntos débiles que un atacante podría aprovechar en su contra, revelarán evidencia de ataques pasados, presentes y planificados, y le ofrecerán un panorama general de su situación de ataque.

Con esta información exclusiva, usted puede concentrar su estrategia de defensa en las áreas señaladas como objetivos principales de los cibercriminales, y actuar con rapidez y precisión para repeler a los intrusos y minimizar la posibilidad de éxito de un ataque.

Los informes se crean mediante inteligencia de fuentes abiertas (OSINT), análisis detallado de los sistemas expertos y las bases de datos de Kaspersky Lab y nuestro conocimiento de las redes clandestinas de cibercriminales. Se abordan áreas como las siguientes:

- **Identificación de vectores de riesgo**. Identificación y análisis de estado de componentes críticos de la red a los que se pueda acceder en forma externa y que puedan ser objeto de ataque, como cajeros automáticos, sistemas de videovigilancia y otras clases de sistemas en las que se usen tecnologías móviles, perfiles de redes sociales de empleados y cuentas de correo electrónico personales.
- **Análisis de rastreo de malware y ciberataques**. Identificación, monitoreo y análisis de cualquier muestra de malware activo o inactivo dirigido a su organización, cualquier actividad de botnets anterior o actual y cualquier actividad sospechosa basada en la red.
- **Ataques de terceros**. Evidencia de amenazas y actividad de botnets dirigidos específicamente a sus clientes, socios y suscriptores, cuyos sistemas infectados luego se pueden utilizar para atacarlo a usted.
- **Fuga de información**. Mediante la vigilancia discreta de foros clandestinos y otras comunidades en línea, descubrimos si los hackers están planeando un ataque en su contra o, por ejemplo, si un empleado inescrupuloso está divulgando información.
- **Situación actual de ataque**. Los ataques de APT pueden continuar muchos años sin detectarse. Si detectamos un ataque en curso que esté afectando a su infraestructura, le recomendaremos las medidas adecuadas para solucionar el problema.

INICIO RÁPIDO – FÁCIL DE USAR – NO NECESITA RECURSOS

Para comenzar a usar este servicio de Kaspersky Lab, solo es necesario definir una serie de parámetros (para los informes adaptados al cliente) y los formatos de datos preferidos. No se requiere de infraestructura adicional.

Nuestro servicio de informes de inteligencia de amenazas no afecta la integridad ni la disponibilidad de ninguna clase de recurso, incluidos los de red.

Informes específicos de amenazas por país

La ciberseguridad de un país incluye la protección de todas sus instituciones y organizaciones principales. Las amenazas persistentes avanzadas (APT) contra autoridades gubernamentales pueden afectar la seguridad nacional. Un ciberataque que impacte en industrias clave (como la manufactura, el transporte, las telecomunicaciones o la banca) puede redundar en pérdidas financieras, accidentes de producción, bloqueo de las comunicaciones de red, protestas sociales y otras consecuencias que repercutan en toda la nación.

Tener un panorama claro y actualizado de la superficie de ataque, y de las tendencias en malware y ataques dirigidos al país, le permitirá focalizar su estrategia de defensa en las áreas que los cibercriminales sean más propensos a atacar, actuar con rapidez y precisión para repeler a los intrusos y minimizar el riesgo de que un ataque sea exitoso.

Los informes de amenazas por país se crean usando enfoques que abarcan desde la inteligencia de fuentes abiertas (OSINT) y el análisis detallado de nuestras bases de datos y sistemas expertos hasta nuestro conocimiento de las redes clandestinas de cibercriminales. Cubren áreas como las siguientes:

- **Identificación de vectores de riesgo**. Identificación y análisis de estado de los recursos de TI críticos para el país a los que se tiene acceso externo, como aplicaciones gubernamentales vulnerables, equipos de telecomunicaciones, componentes de sistemas de control industrial (SCADA, PLC, etc.) y cajeros automáticos.
- **Análisis de rastreo de malware y ciberataques**. Identificación y análisis de campañas de APT, de muestras de malware activo o inactivo, de la actividad actual o pasada de botnets y de otras amenazas importantes dirigidas al país, a través de datos disponibles en nuestros recursos internos de monitoreo de Internet.
- **Fugas de información**. Mediante la vigilancia discreta de foros clandestinos y otras comunidades en línea, descubrimos si los hackers están hablando de atacar organizaciones específicas. También podemos revelar cuentas importantes que hayan sido vulneradas y que puedan plantear riesgos a las organizaciones e instituciones de las víctimas. Un ejemplo de esto son las cuentas de empleados gubernamentales que quedaron expuestas en el ataque de Ashley Madison y que podrían utilizarse para chantaje.

Nuestros informes de inteligencia de amenazas no afectan la integridad ni la disponibilidad de los recursos de red inspeccionados. El servicio se basa en métodos de reconocimiento de red no intrusivos, así como en el análisis de información disponible en códigos abiertos y recursos de acceso limitado.

Como conclusión del servicio, se le proporcionará un informe con una descripción de las amenazas importantes para distintas industrias e instituciones del Estado, así como información adicional sobre los resultados de los análisis técnicos detallados. Los informes se entregan a través de mensajes de correo electrónico cifrados.

El servicio se puede prestar como un proyecto único o periódicamente de acuerdo con un plan de suscripción (por ejemplo, en forma trimestral).

Kaspersky Managed Protection

El servicio Kaspersky Managed Protection ofrece a los usuarios de Kaspersky Security for Business y Kaspersky Anti Targeted Attack Platform una combinación exclusiva de medidas técnicas avanzadas para detectar y prevenir ataques dirigidos. El servicio incluye monitoreo las 24 horas por parte de expertos de Kaspersky Lab y el análisis continuo de datos de ciberamenazas (inteligencia de ciberamenazas) para garantizar la detección en tiempo real de campañas de ciberespionaje y cibercrimen nuevas y conocidas que estén dirigidas a sistemas de información crítica.

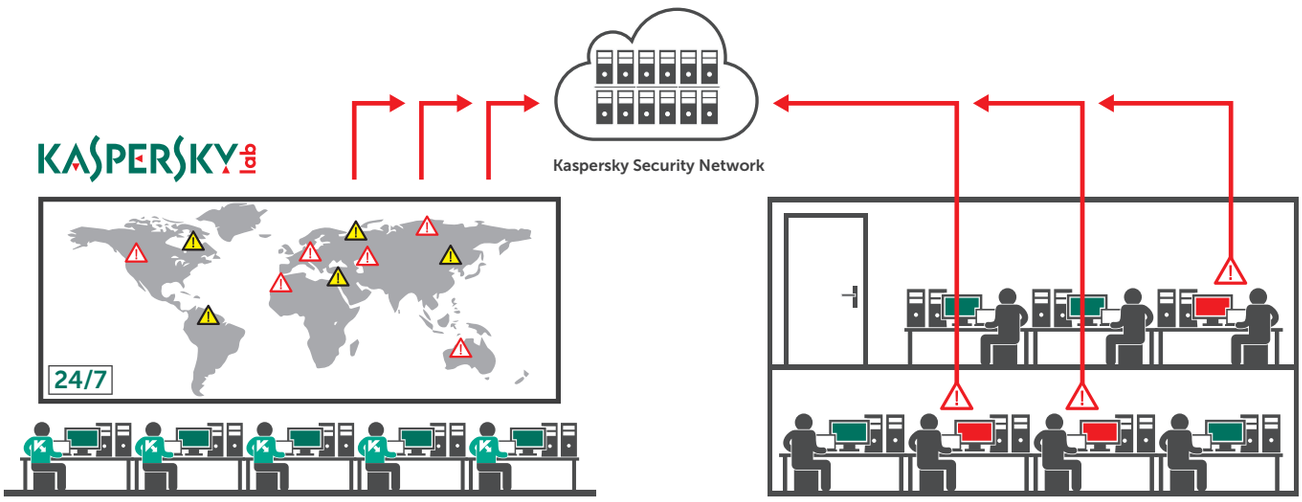


Figura 8:
Kaspersky Managed Protection

ASPECTOS DESTACADOS DEL SERVICIO

- Un alto nivel de protección contra malware y ataques dirigidos, con el soporte ininterrumpido de los analistas de Kaspersky Lab.
- Información sobre los atacantes, su motivación, sus métodos y herramientas y el daño que podrían ocasionarle, para que pueda desarrollar una estrategia de protección calculada y eficaz.
- Detección de ataques en los que no se utilice malware, ataques que involucren herramientas desconocidas y ataques que aprovechen vulnerabilidades de día cero.
- Análisis retrospectivo de incidentes y búsqueda proactiva de amenazas.
- Reducción de los costos generales de seguridad y optimización de la calidad de la protección. Este es un servicio altamente profesional que ofrece el líder mundial en análisis de ciberataques e incluye el análisis de los métodos y las tecnologías que usan los atacantes. Obtener este nivel de información a través de un servicio externo resulta mucho más económico que emplear a especialistas con un enfoque más acotado.
- Enfoque integrado. Nuestra amplia variedad de soluciones Kaspersky Security for Business integradas nos permite ofrecer todas las tecnologías y servicios necesarios para implementar un ciclo completo de protección contra ataques dirigidos: Preparación — Detección — Investigación — Análisis de datos — Protección automatizada.

VENTAJAS DEL SERVICIO

- Detecta incidentes con rapidez.
- Recopila información suficiente para permitir la clasificación (como falso positivo o detección correcta).
- Identifica qué tan comunes son los artefactos recopilados para determinar qué tan singular es el ataque.
- Inicia el proceso de respuesta cuando se registra un incidente de seguridad de la información.
- Inicia el proceso de actualización de las bases de datos antivirus a fin de bloquear la propagación de amenazas.

Más información sobre las fuentes de inteligencia de amenazas de Kaspersky

La inteligencia de amenazas se recopila a partir de una fusión de fuentes heterogéneas y altamente confiables, que incluyen Kaspersky Security Network (KSN), nuestros propios rastreadores web, nuestro servicio de supervisión de botnets (monitoreo constante de las botnets, sus objetivos y sus actividades), trampas de spam, equipos de investigación, socios y otros datos históricos sobre objetos maliciosos que Kaspersky Lab ha reunido durante casi dos décadas. Una vez recopilados, los datos se inspeccionan y refinan cuidadosamente en tiempo real, utilizando diversas técnicas de preprocesamiento: criterios estadísticos, sistemas expertos de Kaspersky Lab (sandboxes, motores heurísticos, herramientas de similitud, perfiles de comportamiento, etc.), validación de analistas, verificación con whitelisting y más.

Una vez que cuente con personal adecuado y debidamente capacitado, e inteligencia de amenazas adquirida de fuentes confiables e implementada en los controles de seguridad existentes, deberá considerar su respuesta ante un incidente.

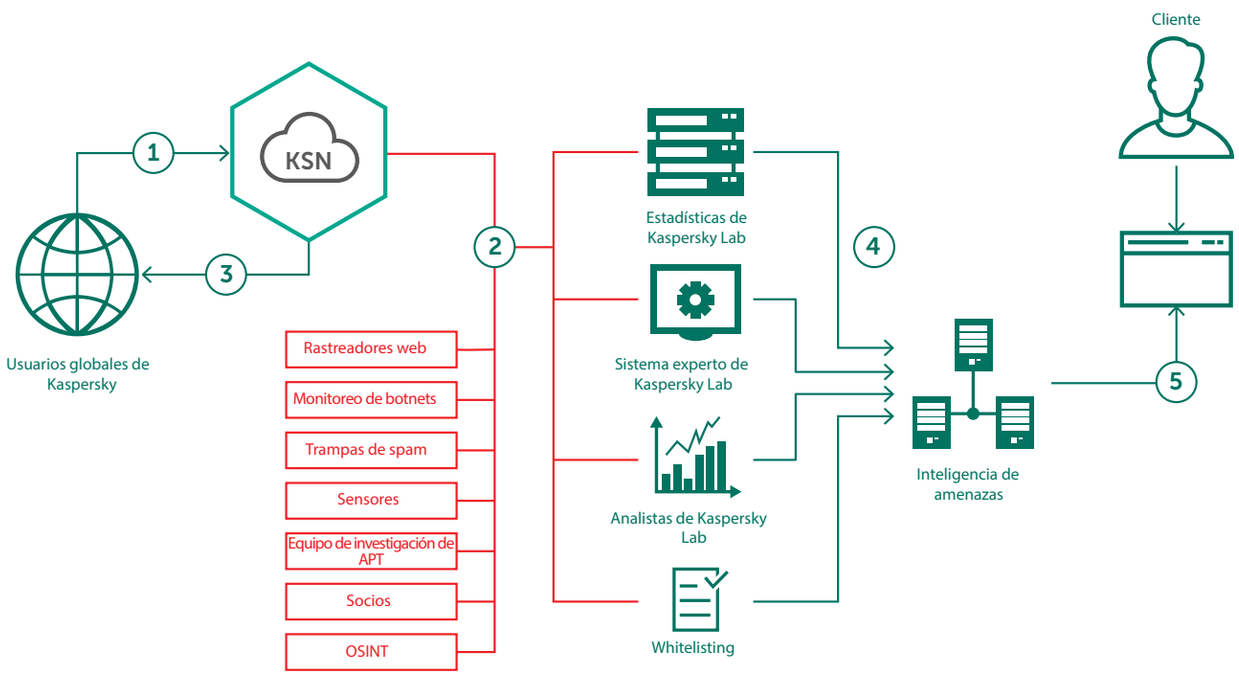


Figura 9:
Fuentes de inteligencia de amenazas de Kaspersky Lab

MARCO DE RESPUESTA A INCIDENTES

El análisis forense y la respuesta a incidentes exigen asignar una cantidad considerable de recursos internos con poca o ninguna anticipación. Los especialistas expertos, equipados con una vasta experiencia práctica en combatir ciberamenazas, deberán actuar con rapidez para identificar, aislar y bloquear la actividad maliciosa. La velocidad es fundamental si el objetivo es minimizar las consecuencias y los costos de corrección.

Alcanzar este nivel de desempeño con tan poca anticipación puede ser un desafío, incluso para el equipo de un SOC consolidado: pocas organizaciones cuentan con recursos internos suficientes para detener en el acto un ataque avanzado. Además, en ciertos casos (por ejemplo, ante APT o amenazas complejas patrocinadas por gobiernos), el SOC puede carecer de conocimientos expertos sobre los enfoques y las tácticas puntuales de los que se ha valido el atacante.

En casos como estos, puede ser más rentable y productivo colaborar con un proveedor o asesor de respuesta a incidentes externo, que cuente con la capacidad de aplicar una respuesta rápida y calculada.

Un marco de respuesta a incidentes integral debe incluir lo siguiente:

- **Identificación del incidente**
  Análisis inicial del incidente y aislamiento de los sistemas infectados.
- **Adquisición de evidencia**
  Dependiendo del tipo de incidente, será necesario revisar distintas fuentes para obtener la evidencia necesaria.
- **Análisis forense (si es necesario)**
  En esta etapa, es posible establecer un panorama detallado del incidente.
- **Análisis de malware (si es necesario)**
  El objetivo es comprender las capacidades del malware específico.
- **Plan de corrección**
  Desarrollo de un plan para erradicar tanto la causa raíz del problema como todos los rastros del código malicioso.
- **Lecciones aprendidas**
  Los controles de seguridad existentes se revisan y actualizan para prevenir incidentes similares.

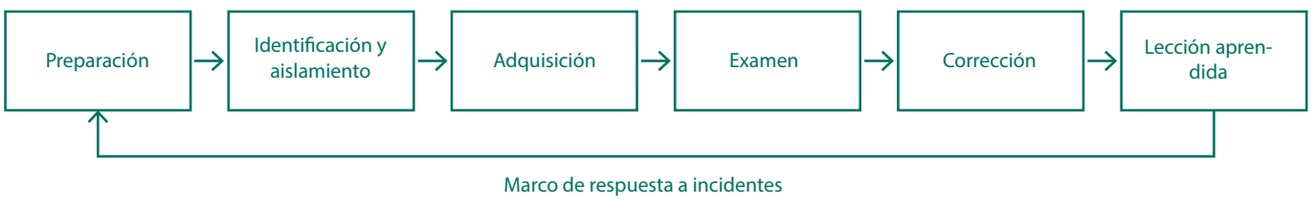


Figura 10:
Marco de respuesta a incidentes

Kaspersky Lab ofrece:
Servicios de respuesta a incidentes

El servicio de respuesta a incidentes es nuestra propuesta premium. Contempla el ciclo completo de investigación de incidentes, desde la adquisición de evidencia in situ hasta la identificación de indicios de vulneración adicionales, la preparación de un plan de corrección y la eliminación total de la amenaza para su organización. Nuestros analistas e investigadores, altamente experimentados en la detección de ciberintrusiones, son quienes llevan a cabo las investigaciones. Toda nuestra experiencia global en análisis de malware y análisis forense digital se puede dedicar a resolver su incidente de seguridad.

Durante la prestación del servicio, se persiguen las siguientes metas:

- Identificar los recursos afectados.
- Aislar la amenaza.
- Evitar la propagación del ataque.
- Buscar y recopilar evidencia.
- Analizar la evidencia y reconstruir la cronología y la lógica del incidente.
- Analizar el malware utilizado en el ataque (si se descubre malware).
- Descubrir los orígenes del ataque y otros sistemas que puedan haberse visto afectados (si es posible).
- Analizar la infraestructura de TI con herramientas específicas para revelar posibles indicios de vulneración.
- Analizar las conexiones salientes entre su red y recursos externos para detectar cualquier señal sospechosa (como posibles servidores de comando y control).
- Eliminar la amenaza.
- Recomendar otras medidas de corrección que puede tomar.

Dependiendo de si cuenta o no con su propio equipo de respuesta a incidentes, puede solicitar a nuestros expertos que lleven a cabo todo el ciclo de investigación, que se limiten a identificar y aislar los equipos afectados y a evitar la propagación de la amenaza, o que realicen tareas de análisis de malware o de análisis forense digital.

ANÁLISIS DE MALWARE

El análisis de malware le permitirá obtener una explicación completa del comportamiento y los objetivos concretos de los archivos de malware dirigidos a su organización. Los expertos de Kaspersky Lab llevan a cabo un análisis exhaustivo de la muestra de malware que usted proporciona y crean un informe detallado que incluye lo siguiente:

- Propiedades de la muestra: una breve descripción de la muestra y un veredicto sobre la clasificación del malware.
- Descripción detallada del malware: un análisis minucioso de las funciones de la muestra de malware, el comportamiento y los objetivos de la amenaza e, incluso, sus IOC. Esto le dará la información necesaria para neutralizar las actividades del malware.
- Medidas de corrección: en el informe se propondrán medidas para proteger completamente a la organización contra la clase de amenaza analizada.

ANÁLISIS FORENSE DIGITAL

El servicio de análisis forense digital puede incluir las tareas de análisis de malware que se acaban de describir; esto dependerá de si se descubre malware durante la investigación. Los expertos de Kaspersky Lab reúnen y examinan las pruebas recopiladas (imágenes de disco duro, volcados de memoria, trazas de red y más) para comprender con exactitud lo que sucede. El resultado es una aclaración detallada del incidente. Como cliente, usted inicia el proceso recopilando evidencia y ofreciendo una descripción del incidente. Los expertos de Kaspersky Lab analizan los síntomas del incidente, identifican el binario de malware (si corresponde) y realizan el análisis de malware con el fin de proporcionar un informe detallado que incluye acciones correctivas.

OPCIONES DE ENTREGA

Los servicios de respuesta a incidentes de Kaspersky Lab están disponibles en dos modalidades:

- Por suscripción
- En respuesta a un incidente único

Ambas opciones se basan en la cantidad de tiempo que nuestros expertos dedican a resolver el incidente. Esto se negocia con el cliente antes de firmar el contrato. El cliente tiene la flexibilidad de incluir cuantas horas de trabajo considere necesarias o seguir las recomendaciones de nuestros expertos para cada caso específico.

¿POR QUÉ KASPERSKY LAB?

Porque tenemos:
- Una relación de trabajo conjunto con fuerzas de seguridad internacionales, como la Interpol y diversos CERT.
- Herramientas basadas en la nube para vigilar millones de ciberamenazas en todo el mundo y en tiempo real.
- Equipos globales que analizan y descifran el funcionamiento de toda clase de amenazas de Internet.

Porque somos:
- La empresa independiente de software de seguridad más grande del mundo y estamos enfocados en la inteligencia de amenazas y el liderazgo tecnológico.
- Líderes indiscutibles en las pruebas de detección de malware independientes, con un historial de aciertos al que no se acerca ningún otro proveedor.
- Líderes de acuerdo con Gartner, Forrester e IDC.

Acerca de Kaspersky Lab

Kaspersky Lab es el proveedor privado más grande del mundo en el área de las soluciones de protección para endpoints. La empresa se encuentra entre los principales cuatro proveedores del mundo de soluciones de seguridad para usuarios de endpoints. Durante sus más de 18 años de historia, Kaspersky Lab ha innovado en seguridad de TI y ha proporcionado las soluciones de seguridad digital más efectivas para grandes empresas, pymes y consumidores. Kaspersky Lab, que tiene su holding registrado en el Reino Unido, opera en casi 200 países y territorios de todo el planeta, y brinda protección a más de 350 millones de usuarios a lo largo y ancho del globo.

Kaspersky Lab, Moscú, Rusia
http://latam.kaspersky.com/

Todo sobre la seguridad en Internet:
www.securelist.com

Encuentre un socio cerca de usted:
www.kaspersky.com/buyoffline

KASPERSKY lab