Kaspersky MXDR

kaspersky preparados para el futuro

Capas de Kaspersky Next MXDR Optimum

Características de protección en endpoints

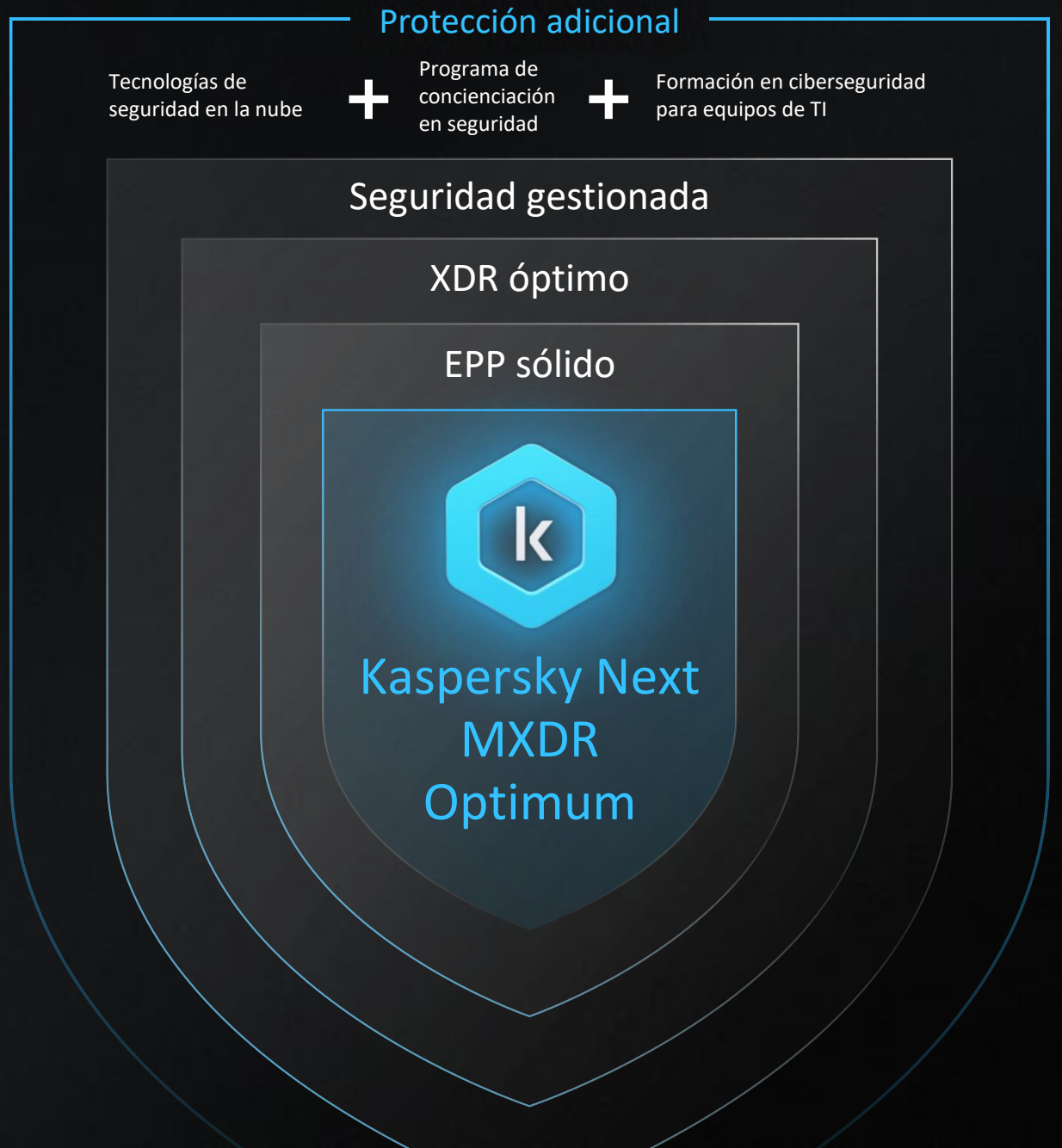
- Antimalware mejorado
- Refuerzo ampliado
- Valoración de las vulnerabilidades
- Controles de endpoints
- Protección de datos
- Gestión de parches

Detección, análisis y respuesta

- Detección de comportamientos
- Unificación de alertas
- Sandbox basado en la nube
- Descubrimiento de pruebas de amenazas (IoC) e IoC personalizados
- Análisis de la causa raíz
- Rango de acciones de respuesta

Protección gestionada

- Supervisión y detección de amenazas continuas
- Vista general de todos los recursos protegidos
- Almacenamiento de telemetría sin procesar durante 3 meses
- Comunicarse directamente con el equipo SOC sobre los incidentes
- Envío de incidentes
- Respuesta guiada automatizada



Reducción de la superficie de ataque

Refuerzo del sistema

Los diversos componentes de control (entre ellos, Control de Anomalías Adaptativo y algoritmos de ML) permiten adaptar el refuerzo del sistema y la configuración de las directivas de seguridad de forma automática según el comportamiento de los usuarios.

Gestión de parches y vulnerabilidades

La administración de vulnerabilidades y parches simplifica las actualizaciones y optimiza las operaciones de seguridad y TI al admitir la instalación de SO y software de terceros en los hosts.

Características de detección y respuesta en endpoints

Indicadores IoC

Búsqueda de indicadores de vulneración (IoC) con respuesta automática en todos los endpoints.

Análisis de la causa raíz

Datos y herramientas de visualización para confirmar la causa raíz de la amenaza y la necesidad de tomar acciones de respuesta adicionales.

Respuesta automática

Guía de respuestas y automatización incorporadas.

Enriquecimiento

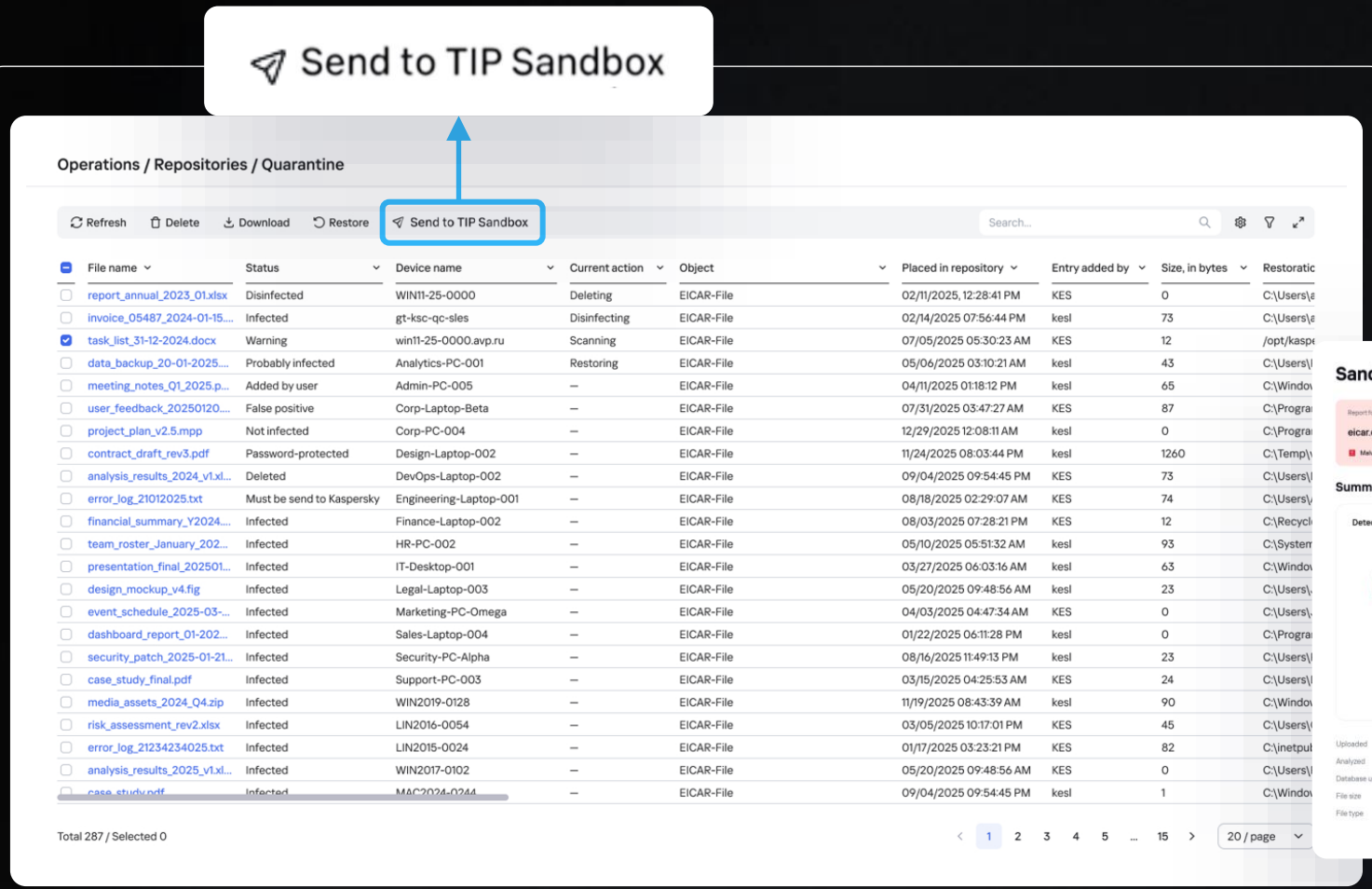
Acceso a Threat Intelligence Portal

Consultas en sandbox basado en la nube

La integración con Kaspersky Cloud Sandbox permite realizar diversas acciones mediante Kaspersky Threat Intelligence Portal.

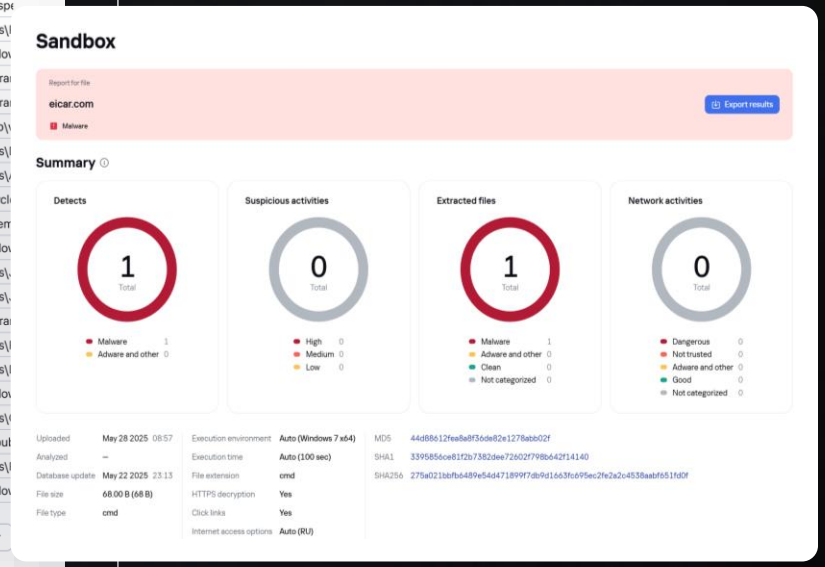
- Detección automática de tipos de archivos
- Administración de tareas ejecutables obsoletas
- Carga y ejecución de archivos en Cloud Sandbox
- Carga de un archivo desde una dirección web y posterior ejecución en Cloud Sandbox
- Características de antievasión para contrarrestrar el malware diseñado para eludir entornos aislados
- Ejecución de un archivo extraído del informe de Cloud Sandbox
- Exportación de resultados de los análisis

Consultas en sandbox basado en la nube

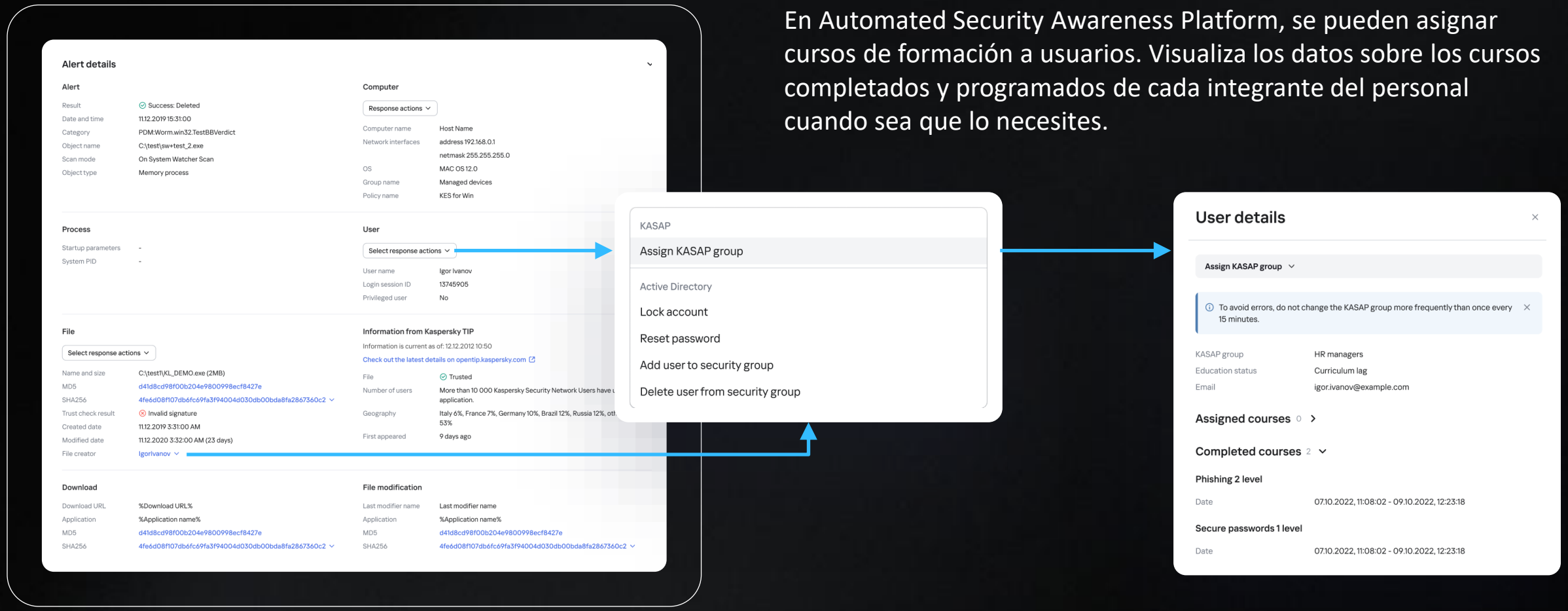


Para investigar archivos maliciosos con facilidad y obtener un contexto más amplio y más detalles, ofrecemos la integración con Cloud Sandbox. Desde la interfaz del producto, el usuario puede cargar muestras que puedan ser maliciosas para verificar su reputación en segundos.

Los datos generados pueden usarse para analizar IoC posteriormente.

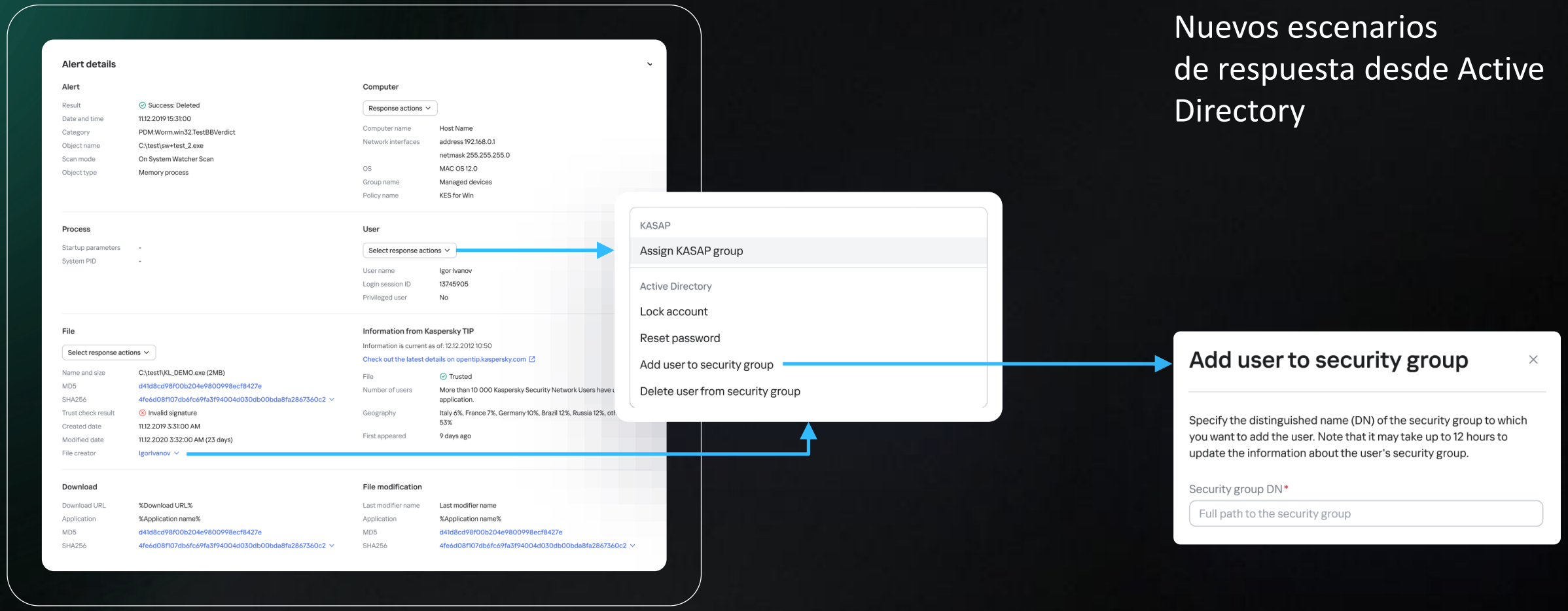


Integración de Security Awareness



En Automated Security Awareness Platform, se pueden asignar cursos de formación a usuarios. Visualiza los datos sobre los cursos completados y programados de cada integrante del personal cuando sea que lo necesites.

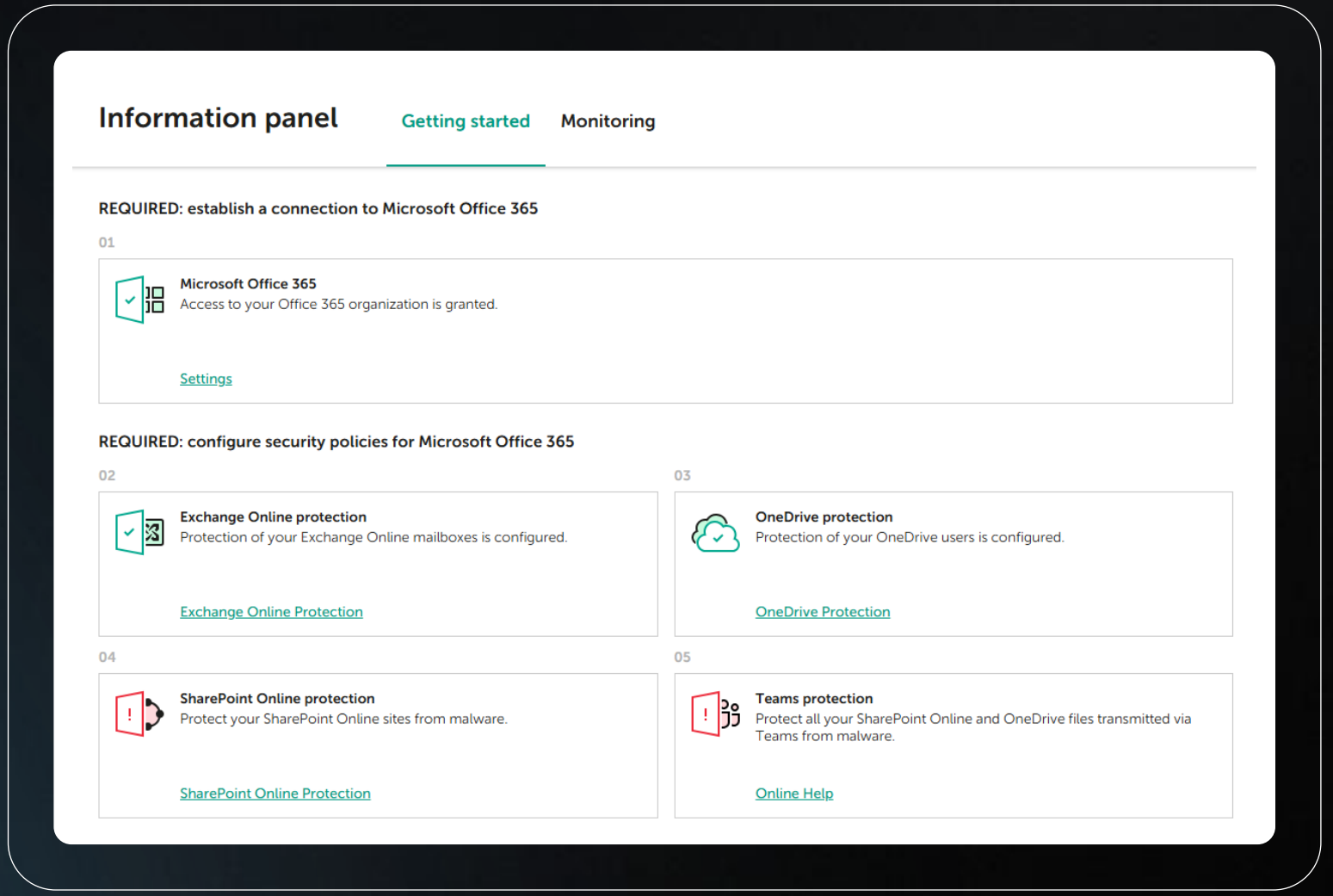
Integración con Active Directory



Nuevos escenarios de respuesta desde Active Directory

Seguridad de Office 365

- Protección avanzada frente a amenazas
- Antiphishing, antimalware, antispam y eliminación de archivos adjuntos maliciosos
- Para las principales aplicaciones de MS Office 365



La Joya de La Corona…

Kaspersky MDR

Es una solución integral que ofrece protección avanzada y continua incluso contra las amenazas más innovadoras

Supervisión continua las 24 horas del día, los 7 días de la semana
en busca de actividades sospechosas

Detección y análisis de amenazas
para evitar posibles sistemas vulnerados

Priorización de alertas
para filtrar falsos positivos y asignar recursos de forma eficiente

Búsqueda de amenazas y respuesta
por expertos en seguridad de Kaspersky

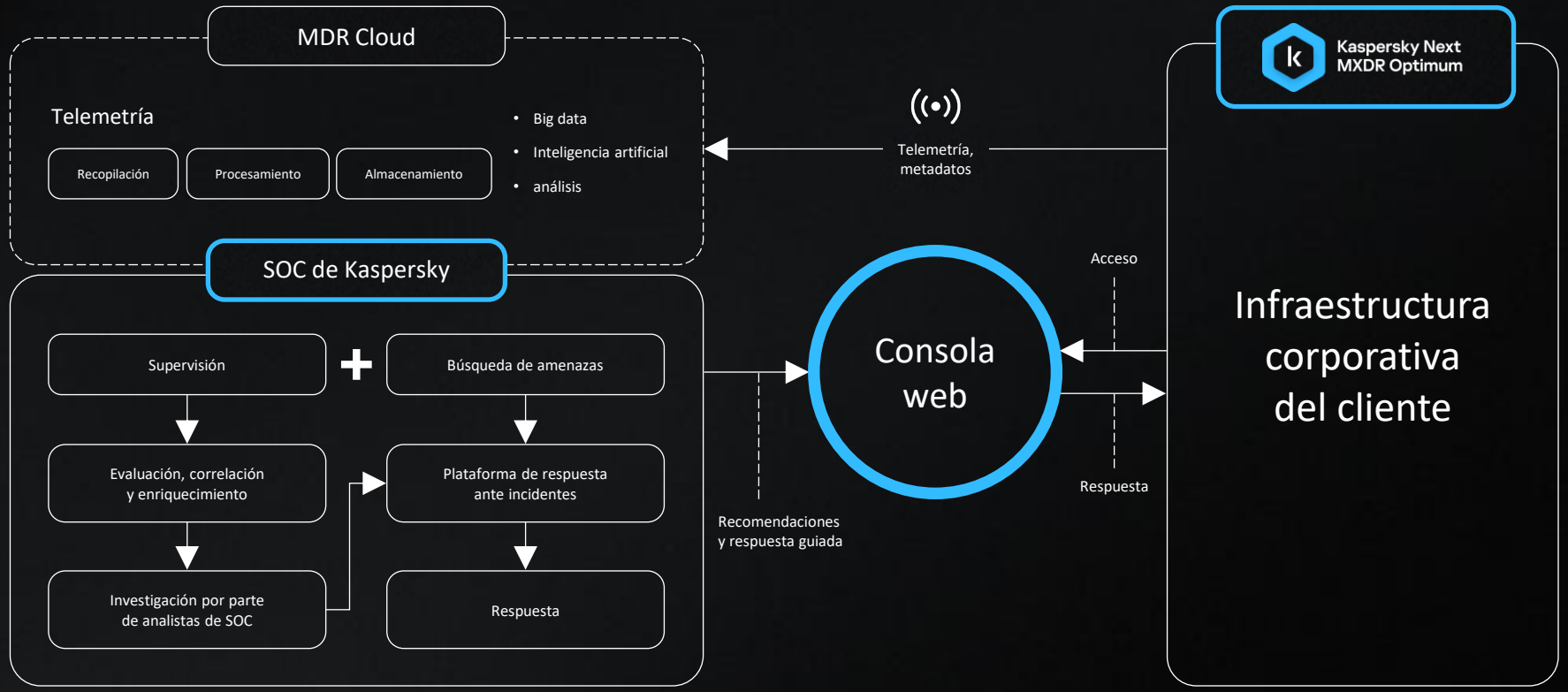
Seguridad gestionada

1 Kaspersky Next MXDR Optimum captura y envía los datos al SOC de Kaspersky.

2 La telemetría, los metadatos y la priorización de alertas se analizan con herramientas de ML/IA, con la participación activa de los expertos del SOC de Kaspersky.

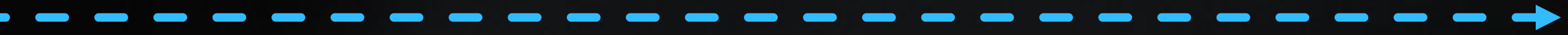
3

El equipo del SOC de Kaspersky investiga alertas e informa al cliente acerca de actividad maliciosa, además de ofrecer recomendaciones y respuesta guiada paso a paso.



Motores de inteligencia artificial (IA)

Los mecanismos de IA filtran automáticamente los falsos positivos, lo que permite mejorar considerablemente la productividad de los analistas y reduce el tiempo medio de priorización, detección y respuesta (MTTD/MTTR)



Eventos

Alertas

Correlación de datos

Análisis de IA

Priorización de alertas

Desglose de alertas

Incidentes

Confirmación del estado del disparador: Verdadero/Falso

Capacidades de las tecnologías de IA

1

Detección más rápida

La IA analiza objetos sospechosos en el momento en que ingresan los datos

2

Resuelven entre el 35 y 40 % de alertas

Aumenta de forma significativa el rendimiento de los analistas, lo que genera SLA de tiempo de reacción reducidos

3

Priorización de alertas

Permite a nuestros analistas enfocarse en las alertas más importantes

4

Resolución de alertas automática

No es necesario recurrir a analistas humanos

Escenarios de respuesta

Nuestro equipo examina incidentes y crea respuestas que puedes aceptar o rechazar, como:

Tipo de respuesta	Description
Obtener archivo	Copiar un archivo de tu infraestructura al SOC de Kaspersky
Aislar	Aislar el activo especificado de la red
Desactivar aislamiento	Desactivar el aislamiento de la red del activo especificado
Eliminar clave de registro	Eliminar una clave de registro o una rama de registro en el activo especificado
Volcado de memoria	Crear un volcado de memoria y enviarlo al SOC de Kaspersky
Terminar proceso	Terminar un proceso en el activo especificado con Kaspersky Endpoint Security for Windows

SLA

Nivel de prioridad	Tiempo de reacción	Valor objetivo
Alto (ejemplo: ataque dirigido)	1 hora	90 %
Medio (ejemplo: malware común)	4 hora	90 %
Bajo (por ejemplo: software publicitario, riskware, etc.)	24 horas	90 %

Tiempo de reacción

El tiempo que transcurre desde la detección del incidente (“Hora de creación”) hasta su publicación en la consola de MDR (“Hora de actualización”).

Valor objetivo

Porcentaje de incidentes en los que el tiempo de reacción y el tiempo de respuesta satisfacen el valor objetivo.

Puede encontrar más información, como los criterios de los incidentes, en los Términos y condiciones

kaspersky

¡Muchas Gracias!

Javier Sanz