DETECTION AND RESPONSE ADVANCED

Gracias por elegir las soluciones y los servicios de ESET. Este documento proporciona una descripción general sobre el servicio ESET Detection and Response Advanced, incluyendo sus procesos básicos y sus fases.

Progress. Protected.

ESPECIFICACIÓN DEL SERVICIO

RESUMEN DEL SERVICIO

ESET Detection and Response Advanced va más allá del soporte estándar de los productos, proporcionando asistencia eficaz en la investigación de incidentes y desafíos de seguridad. Analiza archivos potencialmente dañinos y propone pasos de respuesta y remediación para asegurar la continuidad del negocio. Además, está diseñado específicamente para satisfacer las necesidades de las organizaciones que desean elevar su nivel de seguridad y añaden nuestra solución XDR, ESET Inspect (EI), a su infraestructura. ESET Detection and Response Advanced garantiza que aprovecharán al máximo los beneficios de EI desde el momento de su implementación.

Es el servicio más adecuado para organizaciones que cuentan con el personal necesario para gestionar las operaciones diarias de ESET Inspect por sí mismas, pero que desean asegurarse de que el producto está correctamente optimizado y personalizado para su empresa. También permite consultar a los expertos en ciberseguridad de ESET cuando sea necesario.

A pesar de que nuestros multipremiados productos están ampliamente reconocidos como unos de los mejores del sector, el máximo nivel de seguridad solo puede alcanzarse cuando se combina una tecnología potente con la experiencia humana. Ninguna capa preventiva es eficaz al 100%. Para una verdadera tranquilidad, las organizaciones reconocen cada vez más la necesidad de contar con un sólido plan de respaldo en caso de incidentes. Aquí es exactamente donde entra en juego ESET Detection and Response Advanced: para garantizar a las organizaciones que los expertos en ciberseguridad de ESET están a su disposición y los ayudarán a investigar, identificar y resolver cualquier evento potencialmente dañino.

FASES DEL SERVICIO

1. Fase de evaluación inicial e inscripción

Cada servicio comienza con una evaluación del entorno, la infraestructura, la estructura organizativa y la postura general de seguridad digital del cliente. Con estos datos se completa el Formulario de Evaluación específico del servicio.

Si ESET Inspect se implementó mediante el servicio ESET Deployment and Upgrade, el equipo de Servicios de Seguridad ya dispondrá de una gran cantidad de detalles y solo solicitará la información faltante.

Si falta información relevante para una toma de decisiones eficiente durante la investigación de posibles amenazas, el equipo de Servicios de Seguridad realizará una entrevista completa con el personal designado por el cliente hasta recopilar toda la información necesaria.

El resultado de esta fase es la creación de un Perfil de Seguridad de la Organización, que sirve para que nuestros operadores de Servicios de Seguridad lo consulten en el futuro si necesitan

detalles relacionados con el entorno, la infraestructura, la composición de la organización y la postura general de seguridad digital del cliente.

El último paso es verificar los datos de contacto y los canales de comunicación de ambas partes (consulta la Guía de Contacto).

2. Fase operativa estándar

Una vez finalizada la evaluación inicial y la inscripción, nuestro equipo de Servicios de Seguridad queda a la espera para responder a cualquier posible problema de seguridad e incidente notificado a través de los canales de comunicación definidos (consulta la sección Contactos y Canales de Comunicación). Los tickets deben enviarse a través del formulario de contacto web designado y deben incluir una licencia de producto ESET válida para que pueda asociarse correctamente a la cuenta del cliente.

El alcance del soporte durante la fase operativa estándar se describe en la siguiente sección.

Los tiempos de respuesta y resolución (si corresponden) se basan en los Contratos de Nivel de Servicio definidos en el presente documento (consulta la sección Contrato de Nivel de Servicio).

ALCANCE DEL SERVICIO

Este servicio se centra fundamentalmente en problemas y preguntas relacionados con la seguridad digital. Su objetivo principal es determinar si existe alguna actividad maliciosa y, de confirmarse, ofrecer sugerencias para mitigarla y resolverla eficazmente. El alcance del servicio incluye asistencia para las siguientes áreas principales y tipos de problemas:

Tipo de problema	Descripción del problema	Descripción de la actividad	Datos de entrada requeridos y resultado o salida
Asistencia en Respuesta a incidentes forenses digitales (DFIR)	Asistencia en Respuesta a incidentes forenses digitales / Asistencia en DFIR, es decir, se necesita investigar un incidente, es un incidente en curso y se proporciona interacción (llamada telefónica, conexión remota). No se trata de una solución de DFIR en sí misma, sino de asistencia en DFIR.	El incidente se investiga online. Se ofrece una asesoría sobre temas relacionados con la ciberseguridad desde un punto de vista técnico. Esto puede dar lugar a un análisis de archivos y/o un análisis forense digital. Las actividades se limitan únicamente a casos relacionados con ataques de malware/ciberseguridad, y no a casos como la mitigación de problemas de relaciones públicas y áreas similares.	Entrada: Datos del entorno, acceso al entorno; se especifican las preguntas y/o el nivel de detalle; información sobre hechos ya investigados/identificados. Salida: Cualquiera de los siguientes: consultoría, cambios en el entorno, informe, redirección a otro servicio.

Asistencia para la detección de malware	Malware: falta la detección, es decir, no se detecta el malware.	Se analiza el archivo, URL, dominio o IP enviado y, si se considera malicioso, se añade la detección y se proporciona información sobre la familia del malware.	Entrada: Versión del producto, archivo/URL/dominio/IP. Salida: Si la entrada se considera maliciosa, se proporciona información sobre la detección añadida (incluyendo el nombre de la detección); en caso contrario, se confirma el estado de no infectado.
Asistencia para la detección de malware	Malware: problema de desinfección, es decir, se detecta malware pero no se puede desinfectar.	Se comprueba que se desinfecte el archivo enviado y se mejora si se detecta algún problema. En casos especiales, se puede proporcionar una aplicación de desinfección independiente.	Entrada: Versión del producto, archivo, registros, información sobre el entorno. Salida: Si se mejora la desinfección, se proporciona información sobre la solución prevista; aplicación o procedimiento de desinfección independiente, en caso necesario.
Asistencia para la detección de malware	Malware: infección de ransomware, es decir, el sistema está infectado con ransomware.	Se evalúa la infección por ransomware y, si es posible descifrar los archivos, se proporciona un descifrador (existente o nuevo). En caso contrario, se ofrecen consejos básicos de mitigación y prevención.	Entrada: Versión del producto, ejemplos de archivos cifrados, archivo de información de pago, registros, muestra de malware. Salida: Programa de descifrado (si es posible); en caso contrario, consejos básicos de mitigación y prevención.
Asistencia para la detección de malware	Falso positivo, es decir, un archivo, URL, dominio o IP se detecta erróneamente como malicioso.	Se analiza el archivo, URL, dominio o dirección IP enviados y, si se determina que la detección es incorrecta, se elimina dicha detección.	Entrada: Versión del producto, archivo/URL/dominio/IP, registros, capturas de pantalla. Salida: Si la entrada se considera maliciosa, se proporciona información sobre la detección eliminada.
Asistencia para la detección de malware	General: Investigación de comportamientos sospechosos	A partir de la descripción del comportamiento sospechoso y otros datos proporcionados, se analiza el comportamiento y se sugiere una posible solución.	Entrada: Versión del producto, descripción del comportamiento sospechoso, registros, información sobre el entorno, datos adicionales a petición, incluye conexión remota en casos específicos.

			Salida: Si es posible, se resuelve el problema y se proporciona información básica.
Análisis de archivos de malware por expertos	Análisis básico del archivo, es decir, se necesita información básica sobre el archivo.	¿El archivo enviado es malicioso? Si no lo es, se proporciona información básica. Si es malicioso, se proporcionan los motivos de la detección, la familia del malware e información básica sobre su funcionalidad.	Entrada: Archivo; preguntas específicas. Salida: Resultado del análisis, junto con información básica.
Análisis de archivos de malware por expertos	Análisis detallado del archivo, es decir, se necesita información detallada sobre el malware.	¿El archivo enviado es malicioso? Si no lo es, se proporciona información básica. Si es malicioso, se proporcionan los motivos de la detección, la familia del malware e información detallada sobre su funcionalidad.	Entrada: Archivo. Salida: Resultado del análisis, junto con información detallada.
Cacería de Amenazas personalizada para todas las amenazas actuales	EI: Cacería de Amenazas.	Se inspecciona el entorno utilizando EI. Se suministra información sobre cualquier amenaza o punto débil. Se ofrece asesoramiento. Los pasos individuales se definen en una lista de verificación.	Entrada: Formulario de Evaluación, acceso al entorno. Salida: Informe de Cacería de Amenazas.
Optimización de reglas y exclusiones personalizadas	EI: asistencia sobre uso de reglas, es decir, asistencia relacionada con la creación, modificación o mal funcionamiento de reglas, por ejemplo, para detectar comportamientos específicos de malware.	Se analiza la regla o el comportamiento especificado y se ofrece consultoría.	Entrada: Versión de EI, reglas, especificación del problema; si resulta ser una falla o incompatibilidad, registros, base de datos o acceso a la base de datos. Salida: Asesoramiento y recomendación sobre cómo configurar la norma deseada.
Optimización de reglas y exclusiones personalizadas	EI: asistencia sobre uso de exclusiones, es decir, asistencia relacionada con la creación, modificación o mal funcionamiento de exclusiones.	Se analiza la exclusión o el comportamiento especificado y se ofrece consultoría.	Entrada: Versión de EI, exclusiones, especificación del problema; si resulta ser una falla o incompatibilidad, registros, base de datos o acceso a la base de datos. Salida: Asesoramiento y recomendación sobre cómo configurar la exclusión deseada.
Optimización de reglas y	EI: Optimización inicial.	Cuando se instala ESET Inspect en un nuevo entorno, genera un gran	Entrada: Formulario de Evaluación, acceso al entorno o datos exportados.

exclusiones personalizadas	número de falsos positivos (FP). Acción que se realiza una sola vez. Se revisan las detecciones de FP más frecuentes en el entorno de EI. Se crean exclusiones. Se pueden crear reglas personalizadas o modificar las reglas existentes para reflejar las expectativas.	Salida: Informe de optimización, cambios en el entorno de EI, como la creación o modificación de reglas y exclusiones.

CONTRATO DE NIVEL DE SERVICIO (SLA)

Grupo de actividades del servicio	Actividad del servicio	Tipo de solicitud/ Problema	SLA según la gravedad A/B/C
Asistencia en Respuesta a incidentes forenses digitales (DFIR)	Asistencia en la investigación	Se necesita investigar un incidente, es un incidente en curso y se proporciona interacción (llamada telefónica, conexión remota). No se trata de una solución DFIR en sí misma, sino de asistencia en DFIR.	**2/4/24 horas**
Asistencia para la detección de malware	Malware: Falta la detección	No se detecta el malware.	**2/4/24 horas**
	Malware: Problema de desinfección	Se detecta malware pero no se puede desinfectar.	**2/4/24 horas**
	Malware: Infección de ransomware	El sistema está infectado con ransomware.	**2/4/24 horas**
	Falso positivo	Un archivo, URL, dominio o IP se detecta erróneamente como malicioso.	**2/4/24 horas**
	General: Investigación de comportamientos sospechosos	Comportamiento sospechoso no relacionado con ninguna otra categoría de la lista.	**2/4/24 horas**
Análisis de archivos de malware por expertos	Análisis básico del archivo	Se necesita información básica sobre el archivo.	**2/4/24 horas**
	Análisis detallado del archivo	Se necesita información detallada sobre el malware.	**2/4/24 horas**
Cacería de Amenazas personalizada para todas las amenazas actuales	EI: Cacería de Amenazas	El cliente quiere que se inspeccione su entorno para detectar la presencia de amenazas (inspección única).	**2/4/24 horas**

Optimización de reglas y exclusiones personalizadas	EI: asistencia sobre uso de reglas	Asistencia relacionada con la creación, modificación o mal funcionamiento de reglas.	**2/4/24 horas**
	EI: asistencia sobre uso de exclusiones	Asistencia relacionada con la creación, modificación o mal funcionamiento de exclusiones.	**2/4/24 horas**
	EI: Optimización inicial	Cuando se instala ESET Inspect en un nuevo entorno, genera un gran número de falsos positivos.	**N/D (actividad planificada realizada por expertos de ESET)**

NIVELES DE GRAVEDAD

Los niveles de gravedad se utilizan para especificar la naturaleza y la urgencia de las solicitudes o los problemas notificados y solo son aplicables a algunos subtipos específicos de problemas o actividades.

A. Críticos

Problemas y solicitudes de naturaleza crítica, especialmente cuando se ha confirmado que afectan la continuidad del negocio. Algunos ejemplos típicos de problemas críticos son la infección activa de ransomware, la respuesta en tiempo real a incidentes y situaciones similares. Los problemas o solicitudes de gravedad crítica tienen un SLA garantizado de dos horas para la Respuesta Humana Inicial.

B. Serios

Problemas o solicitudes de naturaleza seria cuando existe una fuerte sospecha de que pueden afectar la continuidad del negocio. Algunos ejemplos típicos son la notificación de falsos positivos, la investigación de comportamientos potencialmente sospechosos, etc. Los problemas o solicitudes de gravedad seria tienen un SLA garantizado de cuatro horas para la Respuesta Humana Inicial.

C. Comunes

Problemas y solicitudes de naturaleza común en los que el tiempo de respuesta inicial no afecta al resultado final ni a la continuidad del negocio. Algunos ejemplos típicos son la investigación retrospectiva de un incidente histórico, la ayuda con la configuración de reglas o exclusiones de ESET Inspect, el análisis detallado de malware planificado, etc. Este nivel de gravedad también abarca actividades planificadas con antelación (por ejemplo, la Cacería de Amenazas programada) y cualquier problema o solicitud que pueda surgir durante su ejecución. Los problemas o solicitudes de gravedad común tienen un SLA garantizado de veinticuatro horas para la Respuesta Humana Inicial.

TIPOS DE RESPUESTA

1. Respuesta Automática del Sistema

Correo electrónico automático generado por el sistema. Este correo se genera en unos minutos como máximo y sirve simplemente para confirmar que el ticket se ha creado correctamente.

2. Respuesta Humana Inicial

Esta es la respuesta principal a la que se aplican los SLA. Es la primera respuesta generada por un operador humano, quien realiza una comprobación básica de la solicitud o el problema notificado y proporciona uno o varios de los siguientes elementos:

- Comprobación de la gravedad: Al crear un ticket, debe seleccionarse la gravedad del problema, ya que esto puede afectar los tiempos reales del SLA. Sin embargo, hay que tener en cuenta que la gravedad seleccionada inicialmente puede cambiar en función del análisis inicial (por ejemplo, un problema que se consideraba A. Crítico puede resultar ser solo B. Grave o C. Común y viceversa). ESET se reserva el derecho de modificar la gravedad en función de los resultados del análisis inicial.
- Solución o solución alternativa: a menudo, el problema notificado es conocido y existe una solución o solución alternativa temporal que puede proporcionarse de inmediato.
- Análisis inicial: análisis básico del problema notificado.
- Verificación de la integridad de los datos: en los casos en los que se requieren datos contextuales adicionales (archivo de muestra, registro del sistema, registro del producto en la endpoint, etc.), el operador comprueba la integridad y exactitud de los datos proporcionados.
- Solicitud de datos adicionales: si la comprobación de integridad de los datos y el análisis básico mencionados anteriormente muestran que los datos facilitados en el ticket son incompletos o insuficientes para seguir investigando, los operadores pueden solicitar datos adicionales.
- Tiempo estimado necesario para el resultado final: el SLA solo garantiza el tiempo necesario para la respuesta humana inicial, ya que el tiempo necesario para el resultado final real varía en cada caso en función de la solicitud o el problema notificado. En la medida de lo posible, los operadores tratarán de proporcionar una estimación del tiempo necesario para completar el trabajo. Sin embargo, esta estimación no es una garantía y, en algunos casos, no es posible ofrecer una estimación exacta.

3. Resultado Final

Se trata del resultado final o la solución ofrecida como respuesta a la solicitud o el problema notificado en el ámbito del servicio específico. El tipo de resultado (salida) varía en función de las actividades relacionadas con los distintos tipos de problemas (por ejemplo, un informe, una recomendación, etc.).

VISTA GENERAL DEL PROCESO