NOTA DE PRENSA
20 / 10 / 2020

Rapid7 incorpora Telemetría de Endpoint Mejorada en su solución InsightIDR

> InsightIDR es la solución de Rapid7 que permite detectar los comportamientos sigilosos que hay detrás de las infracciones de seguridad

Rapid7, proveedor líder en análisis de seguridad y automatización, ha anunciado la disponibilidad de Telemetría de Endpoint Mejorada (EET, por sus siglas en inglés) en InsightIDR, la solución líder en el mercado de Gestión de Información y Eventos de Seguridad (SIEM) de Rapid7. Con EET, los clientes tendrán una cobertura más amplia e investigaciones sin fricciones de los incidentes de seguridad, así como una visibilidad robusta de la actividad del endpoint, incluidos los nombres y dominios del host, las líneas de comando de los procesos y las rutas de ejecución.

Las organizaciones de hoy en día se enfrentan a amenazas en constante evolución con una complejidad, tamaño y alcance cada vez mayor. A medida que las compañías continúan dando soporte a su creciente fuerza remota, los endpoints se amplían creando más oportunidades para la explotación de los atacantes, y en última instancia, cargando a los equipos de seguridad de más alertas y detecciones. Para combatir estas amenazas, estos equipos necesitan una visión más holística de la actividad de los endpoints.

EET permite a los clientes de InsightIDR ver lo que ocurre antes, durante y después de una amenaza, además de saber cómo un atacante ha podido acceder a un endpoint, lo que puede ayudar a informar sobre las futuras acciones de remediación y respuesta. EET unifica esta valiosa visibilidad de los endpoints junto con los datos de la red, los usuarios y el cloud en InsightIDR, haciendo posible que los equipos aumenten continuamente el nivel de seguridad de sus programas y monitoricen la superficie de ataque desde una única interfaz.

“Las herramientas de detección y respuesta son conocidas por inundar a los usuarios con datos desde

el principio y dejar que los equipos configuren reglas y averigüen cómo hacer que la información sea procesable. Como resultado, muchas de estas herramientas desafortunadamente terminan acumulándose y dejan a los equipos vulnerables a los ataques", comenta Rich Perkett, Vicepresidente Senior de la Práctica de Detección y Respuesta en Rapid7. "La prioridad número uno de InsightIDR es realizar detecciones tempranas y confiables para que nuestros clientes tengan información procesable desde el primer día. A medida que los equipos crecen y se preparan para una seguridad más proactiva, nosotros nos sentimos entusiasmados por hacer que estos conjuntos de datos –como el análisis de tráfico de la red, y ahora la telemetría de endpoint mejorada– estén disponibles para proporcionar una visibilidad centralizada y extendida, y aumentar así la caza de amenazas, las detecciones personalizadas y los casos de uso de remediación", señala Perkett.

> ## Nuevos casos de uso

Con EET, se envía un registro detallado para anotar la búsqueda cada vez que se inicia un proceso en un endpoint monitorizado, permitiendo a los usuarios realizar trabajos forenses adicionales más allá del incidente inicial. Los casos de uso añadidos incluyen:

- Investigación de la actividad maliciosa en profundidad para entender la probabilidad de una amenaza real.
- Identificar cuándo los usuarios están ejecutando otro software no probado en el endpoint.
- Consultar todos los datos del endpoint para identificar si los problemas fueron aislados o no.
- Crear alertas personalizadas únicas para organizaciones individuales.

Las capacidades de Rapid7 EET están disponibles como una función adicional para los clientes de InsightIDR. Para obtener más información, haga clic aquí.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net