¿Por qué la prevención basada en la intención genera menos ruido de alertas que la detección basada en firmas?

Respuesta breve: Porque plantea una pregunta más acotada. Las herramientas de firmas y heurísticas generan alertas cuando algo *se asemeja* a un patrón conocido como malicioso y dejan que los humanos determinen si es relevante. La prevención basada en la intención pregunta si un programa específico está, en ese momento, realizando algo malicioso en un punto de entrada conocido de robo de datos, una pregunta con muchas menos respuestas ambiguas.

> Para conocer la tasa de falsos positivos medida por Cyber Crucible, consulte el artículo existente **"¿Tiene falsos positivos? ¿Cuál es su tasa de falsos positivos?"** Esta página explica la razón arquitectónica por la que el perfil de ruido difiere.

Por qué el perfil de ruido es diferente

Las herramientas de firmas y heurísticas generan alertas cuando algo *se asemeja* a un patrón conocido como malicioso, y luego dependen de la clasificación humana para distinguir lo real de lo irrelevante. Eso es lo que produce más de 100 alertas por endpoint al día en muchos entornos.

La evaluación basada en la intención plantea una pregunta más acotada: ¿está este programa, en este momento, realizando algo malicioso en un punto de entrada conocido de robo de identidad o de datos? Esa pregunta tiene muchas menos respuestas ambiguas.

Qué significa esto en términos operativos

- Los analistas no tienen que perseguir alertas de baja confianza.

- No se requiere ajuste de reglas YARA ni búsqueda manual de amenazas para mantener el ruido bajo control.
- Dado que la respuesta suspende únicamente el proceso infractor, incluso una intercepción incorrecta no provoca la caída de un sistema.

Para conocer las tasas actuales medidas en un entorno como el suyo, consulte a su representante de Cyber Crucible, y vea el artículo existente "¿Tiene falsos positivos?" para más detalles a nivel de producto.

Revision #1
Created 2026-07-24 01:54:29 UTC by Dennis Underwood
Updated 2026-07-24 01:54:29 UTC by Dennis Underwood