

Por que a prevenção baseada em intenção gera menos ruído de alertas do que a detecção baseada em assinaturas?

Resposta curta: Porque ela faz uma pergunta mais restrita. As ferramentas de assinatura e heurística emitem alertas sempre que algo *se assemelha* a um padrão conhecido como malicioso e deixam para os humanos a tarefa de resolver a questão. A prevenção baseada em intenção pergunta se um programa específico está, neste exato momento, fazendo algo malicioso em um ponto de entrada conhecido de roubo de dados — uma pergunta com muito menos respostas ambíguas.

“ Para a taxa de falsos positivos medida da Cyber Crucible, consulte o artigo existente **"Vocês têm falsos positivos? Qual é a sua taxa de falsos positivos?"** Esta página explica a razão arquitetural pela qual o perfil de ruído é diferente.

Por que o perfil de ruído é diferente

As ferramentas de assinatura e heurística geram alertas quando algo *se assemelha* a um padrão conhecido como malicioso e, em seguida, dependem da triagem humana para separar o que é real do que é irrelevante. É isso que produz mais de 100 alertas por endpoint por dia em muitos ambientes.

A avaliação baseada em intenção faz uma pergunta mais restrita: este programa está, neste exato momento, fazendo algo malicioso em um ponto de entrada conhecido de roubo de identidade ou de dados? Essa pergunta tem muito menos respostas ambíguas.

O que isso significa na prática operacional

- Os analistas não precisam perseguir alertas de baixa confiança.
- Não é necessário ajustar regras YARA nem realizar caça manual a ameaças para manter o ruído sob controle.
- Como a resposta suspende apenas o processo infrator, mesmo uma interceptação incorreta não derruba o sistema.

Para as taxas atuais medidas em um ambiente semelhante ao seu, pergunte ao seu representante da Cyber Crucible — e consulte o artigo existente "Vocês têm falsos positivos?" para detalhes em nível de produto.

Revision #1

Created 2026-07-24 05:53:00 UTC by Dennis Underwood

Updated 2026-07-24 05:53:00 UTC by Dennis Underwood