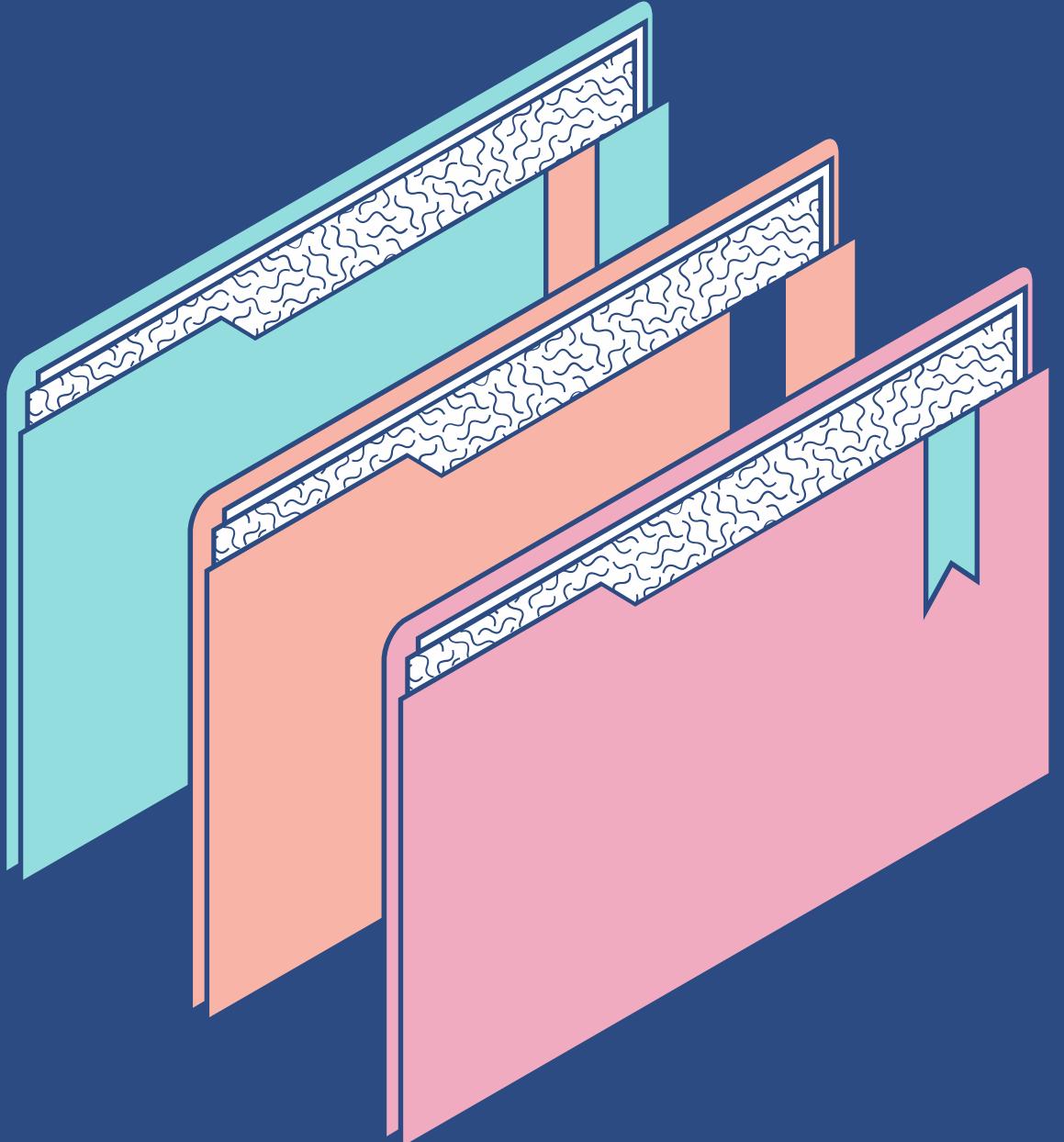




EDR (Endpoint Detection and Response)

Tecnologia de detecção, investigação e resposta em tempo real.



Características

- Detecção avançada de ameaças (Machine Learning).
- Tempo real (zero-day).
- Feedback investigatório.
- Analise forense pôs captura.
- Trabalha com sistemas SIEM (Coleta de dados).



EDR vs Antivirus Tradicional

EDR

Detecção: Analise de comportamento e detecção.

Resposta: Age proativamente em tempo real.

Visibilidade: Monitora totalmente o endpoint.

Automação: IA para analise comportamental.

Proteção avançada: Eficaz contra ataques complexos.

Antivirus

Detecção: Baseada em assinaturas conhecidas.

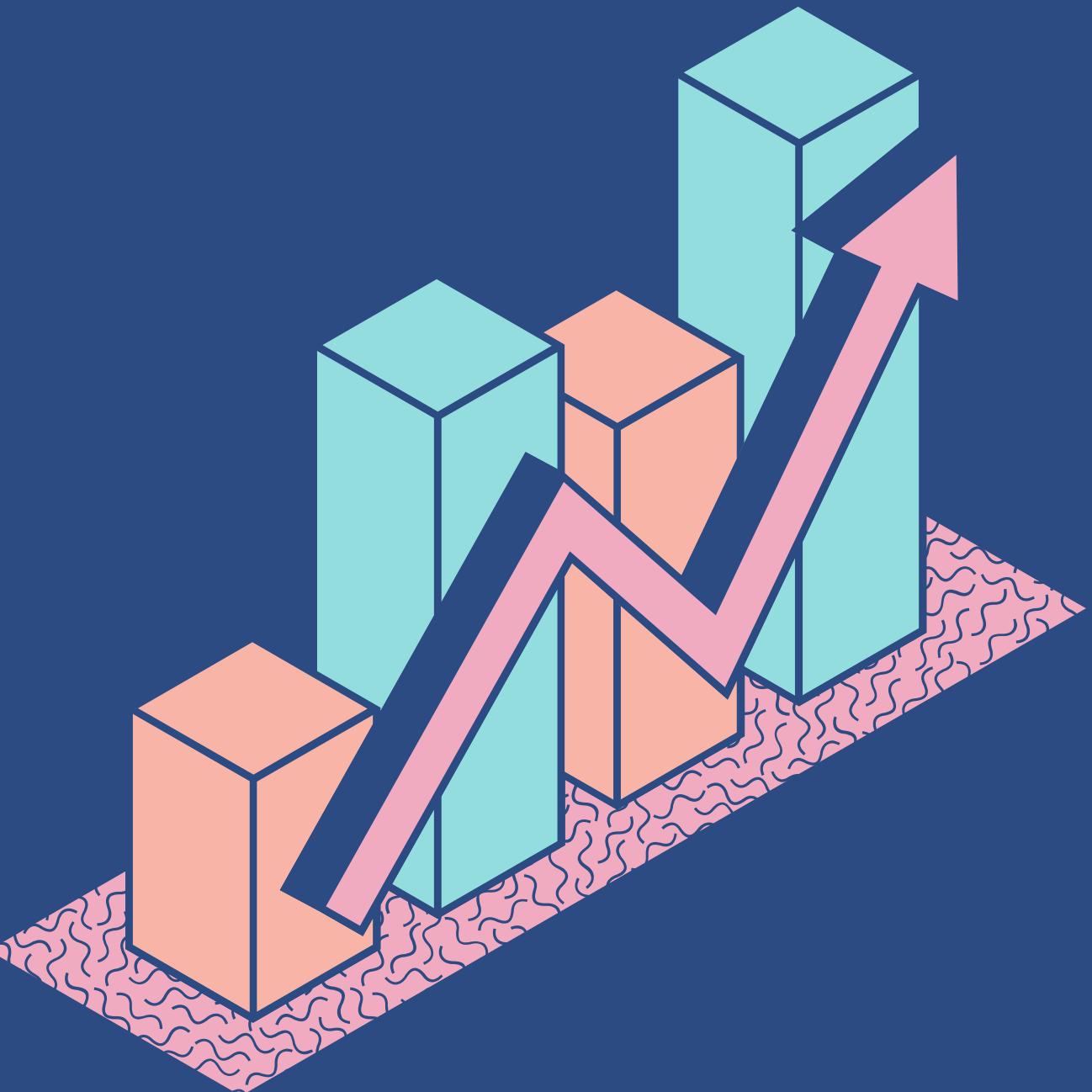
Resposta: Remove malware após infecção.

Visibilidade: Limitada.

Automação: Nula ou pouca eficaz.

Proteção avançada: Ineficaz contra ransomware.

Setor de TI não da lucros?!?





Um caso de uso

Um funcionário clicou em um e-mail.

O antivírus não detectou, pois a falha zero-day.

O virus se espalhou e criptografou tudo.

O desastre

Na segunda planilhas e banco de dados
estavam criptografados e dados vazados.

E o antivírus não tem registro do que aconteceu.

Custo: Produção por hora x Horas paralisados.

A photograph of a man with short brown hair, wearing a white t-shirt, sitting at a desk and working on a laptop. He is looking down at the screen. The background shows an office environment with other desks and equipment.

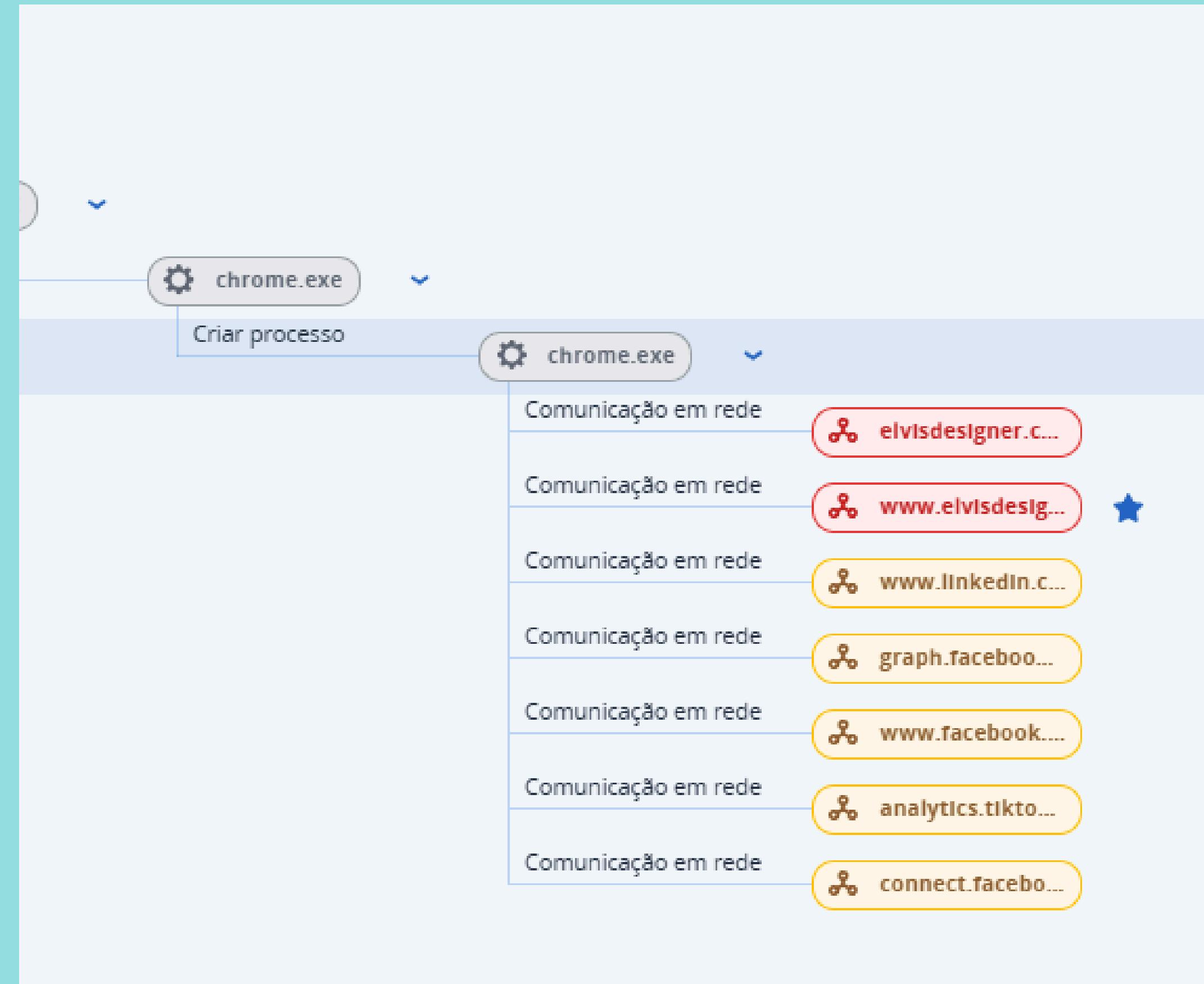
Com EDR

Um funcionário clicou em um e-mail.
EDR flagra o comportamento suspeito, tentando
acessar arquivos e abrindo conexão com a
Rússia.

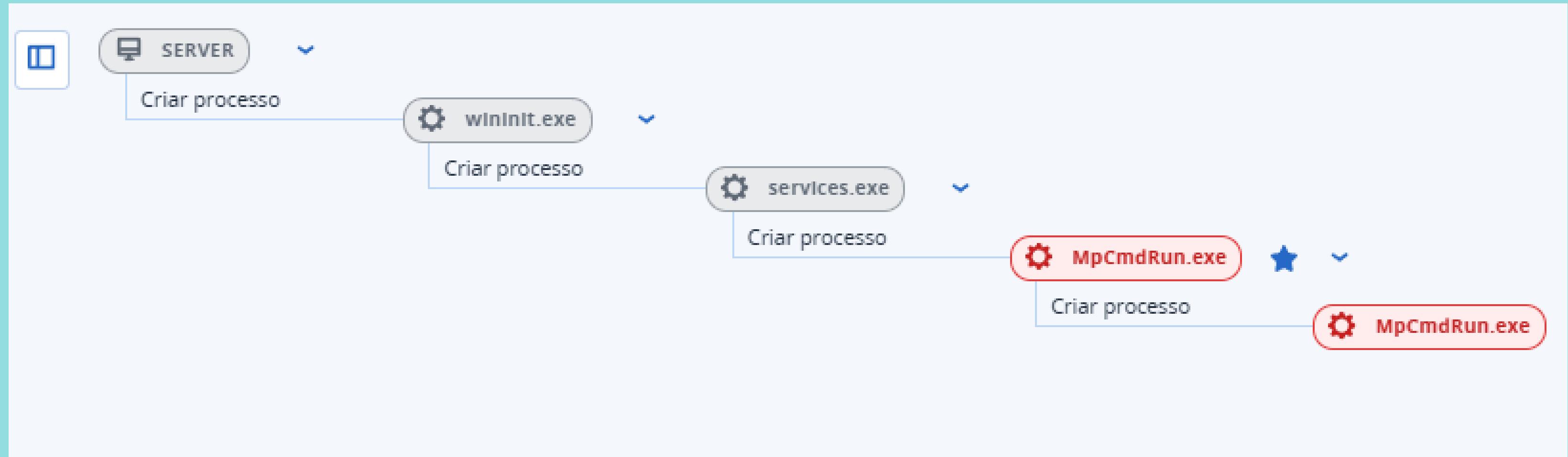
A ação

EDR isolou o endpoint, matou o processo
malicioso e disparou os alertas de segurança.
Zero danos, tempo de ação 30 minutos.

Detecções reais



Detecções reais





5 Passos para Implantar EDR com Sucesso

1

PASSO

Mapeie todos os dispositivos e identifique sistemas críticos.

2

PASSO

Escolha uma ferramenta com detecção comportamental

3

PASSO

Teste em um grupo piloto antes, para evitar falhas

4

PASSO

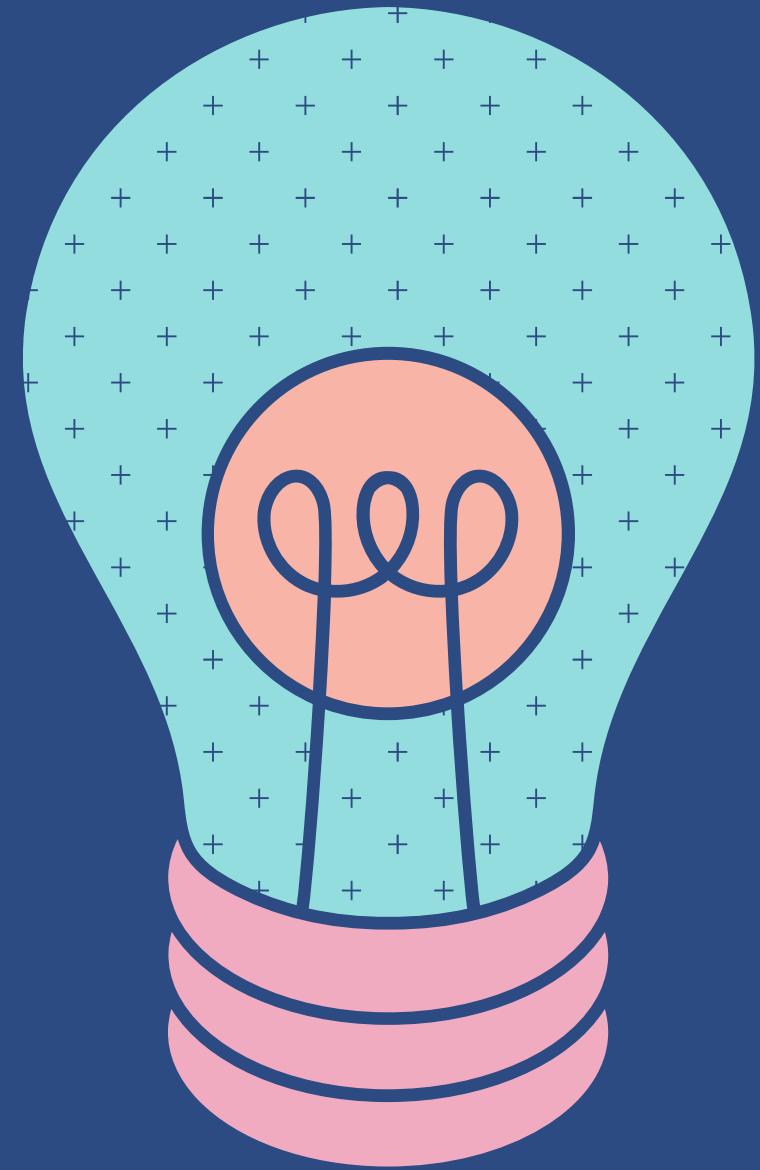
Treine o time de TI e usuários finais

5

PASSO

Ajuste políticas com base em relatórios e ameaças

**EDR não é "magia" – é
engenharia reversa + big data
aplicados.**



Você tem alguma
pergunta?

