

WHITE PAPER TÉCNICO

Engenharia de detecção e automação de alta fidelidade

Ciclo de vida de detecção, cobertura ATT&CK; validada e promoção de resposta automática

Metodologia de hipótese, teste, medição de falso positivo e promoção estatística de automação, com protocolo de exercício adversário e indicadores de cobertura por tática.

Documento técnico xFabric · revisão 2026.2 · uso corporativo

Contexto e fundamentação

Automação sem fidelidade medida transfere o erro para a velocidade. Engenharia de detecção define hipótese, cobertura, teste e critério de promoção antes de qualquer ação automática.

Detecção é produto, não regra

Uma detecção tem ciclo de vida: hipótese de comportamento adversário, fonte de telemetria necessária, lógica, conjunto de teste positivo e negativo, taxa de falso positivo observada em produção e critério de aposentadoria.

Regras adotadas sem esse ciclo acumulam-se e degradam. A métrica relevante não é quantidade de regras ativas, e sim cobertura validada por tática e técnica com falso positivo dentro de limite acordado.

Onde a IA agrega e onde não agrega

Modelos são eficazes em compressão de contexto, agrupamento de eventos correlacionados em um único caso, priorização por similaridade com incidentes anteriores e geração de linha do tempo narrada a partir de evidência estruturada.

Modelos não substituem lógica determinística onde a decisão precisa ser reproduzível e auditável — contenção de host, revogação de credencial e bloqueio de rota são ações que exigem condição explícita e trilha verificável.

Critério de promoção para automação

Uma resposta só é automatizada depois de operar em modo de recomendação por período determinado, com decisão humana registrada. A promoção é estatística e reversível.

- Volume mínimo de ocorrências observadas para significância
- Precisão medida contra decisão humana no mesmo período
- Raio de impacto delimitado por escopo de ativo e janela de execução
- Reversão automática e notificação obrigatória ao dono do ativo
- Revisão amostral periódica das execuções automáticas

Validação por exercício adversário

Cobertura declarada e cobertura efetiva divergem. Exercícios de emulação executam técnicas conhecidas contra o ambiente real e medem detecção, alerta e resposta ponta a ponta, incluindo o handoff entre turnos.

O resultado do exercício alimenta o backlog de engenharia de detecção com lacunas específicas por técnica, e não com uma pontuação agregada que não indica ação.

Ficha de detecção

Cada detecção é registrada como artefato versionado, com autor, hipótese e condição de aposentadoria. Detecções sem ficha não entram em produção.

Campo	Conteúdo
-------	----------

Hipótese	Comportamento adversário esperado e contexto
Técnica	Tática e técnica ATT&CK; mapeadas
Telemetria	Fontes exigidas e cobertura mínima de frota
Teste	Conjunto positivo e negativo reproduzível
Fidelidade	Falso positivo observado e limite acordado
Aposentadoria	Condição objetiva de desativação

Escala de maturidade de automação

Nível	Comportamento	Condição de avanço
0 — Observação	Alerta sem ação	Volume mínimo de ocorrências registrado
1 — Recomendação	Ação sugerida ao analista	Precisão medida contra decisão humana
2 — Sombra	Ação simulada e registrada	Divergência abaixo do limite acordado
3 — Automática restrita	Execução em escopo delimitado	Reversão testada e notificação ativa
4 — Automática ampla	Execução no escopo pleno	Revisão amostral periódica sem exceção crítica

Protocolo de exercício adversário

- Seleção de técnicas por relevância para o setor e para a superfície do cliente
- Execução em ambiente real com janela e escopo autorizados por escrito
- Medição de detecção, alerta, atribuição de caso e ação de resposta
- Registro de handoff entre turnos no regime follow-the-sun
- Lacunas convertidas em itens de backlog por técnica, com prazo
- Reexecução da técnica após a correção para confirmar cobertura

Indicadores do programa

- Cobertura validada por tática, com data da última verificação
- Falso positivo por detecção e por fonte de telemetria
- Tempo médio entre detecção e atribuição de caso
- Percentual de ações executadas por nível de maturidade de automação
- Detecções aposentadas por ciclo, com justificativa

Pontos de decisão

- Cobertura validada por exercício substitui contagem de regras como indicador.
- IA comprime contexto e prioriza; a ação de contenção permanece determinística e auditável.
- Automação promovida sem período de sombra e sem reversão é risco operacional, não eficiência.