

RELATÓRIO MODELO · EXEMPLO FICTÍCIO

Agent Security Review

Relatório executivo e técnico · Empresa Exemplo S.A.

Exemplo fictício para demonstrar o formato do entregável. Empresa, dados e achados são inventados.

Resumo executivo

Avaliamos 3 agentes em produção da Empresa Exemplo: atendimento por e-mail, triagem de contratos e assistente interno de vendas. Encontramos 13 pontos de atenção, sendo 1 crítico e 3 altos. O risco principal é a combinação de permissões amplas com conteúdo externo processado sem isolamento.

SEVERIDADE	QUANTIDADE	PRAZO RECOMENDADO
Crítico	1	Imediato
Alto	3	Até 30 dias
Médio	5	Até 90 dias
Baixo	4	Próximo ciclo

Prioridades

1. Restringir o envio externo do agente de e-mail (SR-01).
2. Isolar o processamento de anexos (SR-02).
3. Trocar a credencial compartilhada por uma conta de serviço (SR-03).

Achados técnicos (seleção)

SR-01 · Crítico Agente de e-mail pode enviar mensagens para qualquer destinatário

O que encontramos: A ferramenta de envio não restringe destinatários. Um e-mail recebido com instruções ocultas levou o agente a encaminhar uma planilha para um endereço externo.

Correção recomendada: Restringir destinatários a domínios aprovados; envio externo passa por aprovação humana (AC-03).

SR-02 · Alto Injeção indireta via anexo PDF

O que encontramos: Um anexo com texto oculto fez o agente consultar dados de outro cliente.

Correção recomendada: Processar anexos em etapa sem ferramentas de consulta (AC-05, AC-06).

SR-03 · Alto Credencial compartilhada com um funcionário

O que encontramos: O agente usa a conta de uma pessoa com acesso de escrita a todo o CRM.

Correção recomendada: Conta de serviço própria com escopo de leitura (AC-02).

SR-04 · Médio Logs guardam dados pessoais sem mascaramento

O que encontramos: CPF e telefone aparecem em texto claro nos registros de execução.

Correção recomendada: Mascaramento automático e prazo de retenção (AC-07, AC-12).

Este é um exemplo fictício do formato do relatório. avadlabs.com.br/solucoes/agent-security-review