1.Incident planning

Antes de um incidente de segurança real ocorrer, é sempre recomendável realizar testes para avaliar a eficácia dos planos de resposta e aprimorar as habilidades da equipe. Esses testes devem ser conduzidos em sistemas de teste para evitar impactos nos ambientes de produção. Além disso, é importante considerar que há um tempo limitado para a realização dos exercícios, pois os envolvidos possuem outras responsabilidades. O objetivo desses exercícios é testar processos, procedimentos e habilidades técnicas, sendo essencial realizar uma avaliação posterior para identificar possíveis melhorias.

Um dos tipos de teste mais utilizados é o **exercício de mesa** (***tabletop exercise***), onde **os participantes se reúnem para discutir, passo a passo, como lidariam com um incidente hipotético**. Esse método é eficiente porque permite revisar as políticas e procedimentos sem precisar mobilizar recursos para um teste em larga escala. Durante a discussão, cada integrante explica o que faria em diferentes momentos do incidente, permitindo identificar falhas e oportunidades de aprimoramento.

Outra abordagem comum são as simulações de ataque, nas quais ameaças são encenadas para testar a resposta da organização. Um exemplo é o envio de e-mails de *phishing* para avaliar quais funcionários clicariam em links suspeitos ou forneceriam credenciais. Outra simulação pode envolver tentativas de engenharia social, como ligar para o suporte técnico e tentar alterar senhas de contas. Essas práticas ajudam a medir a conscientização dos funcionários e a eficácia dos sistemas de defesa. Se a simulação for conduzida por uma empresa terceirizada, também permite testar se filtros automáticos conseguem bloquear as tentativas antes de chegarem aos usuários.

Quando ocorre um incidente real, geralmente há uma série de eventos menores dentro de um ataque maior. Um invasor pode explorar uma vulnerabilidade em um servidor, extrair dados, implantar *malware* e expandir sua presença na rede. Para compreender como isso aconteceu, é necessário realizar uma **análise da causa raiz** (root cause analysis). **Esse processo envolve a revisão de logs, registros de servidores e outros indícios para reconstruir a trajetória do invasor**. Muitas vezes, ataques bem-sucedidos não possuem uma única causa raiz, mas sim múltiplas falhas que permitiram a invasão.

O fator humano também é um ponto crítico na segurança, pois erros dos usuários podem facilitar ataques. Em muitos casos, um simples clique em um link malicioso pode comprometer um sistema inteiro. Por isso, além de corrigir vulnerabilidades técnicas, é essencial investir em treinamentos para que os funcionários reconheçam ameaças e adotem práticas seguras.

Uma forma de evitar que atacantes explorem vulnerabilidades é através da **caça a ameaças** (***threat hunting***), **um processo proativo de busca por sinais de**

atividades maliciosas. Isso pode incluir a revisão de regras de firewall, a verificação de novas vulnerabilidades divulgadas recentemente e a atualização de sistemas com os patches mais recentes. O desafio é que muitas vezes só se identifica um ataque quando ele já está em andamento, por isso, a automação de segurança é essencial para detectar e bloquear ameaças antes que causem danos.

Ferramentas de monitoramento avançadas podem analisar padrões de comportamento e interromper ataques antes que eles comprometam a infraestrutura. Essa automação é fundamental para proteger a organização continuamente, mesmo quando a equipe de segurança não está ativamente monitorando os sistemas.