**CANVAS MVP**

[O Canvas MVP detalha o MVP e suas funcionalidades.]

|  |  |  |
| --- | --- | --- |
| **PERSONAS SEGMENTADAS:**  **1.** Phished (Usuário Alvo do Ataque)   * + Recebe e-mail   + É convencido a clicar   + Interage com o curso  1. Phisher (Atacante)    * Envia e-mail    * Visualiza dashboard    * Analisa relatórios 2. Sistema (Ferramenta utilizada no ataque)    * Gera relatórios    * Coleta dados | **PROPOSTA DO MVP:**  O projeto "Campanha de Phishing" tem como principal objetivo educar os colaboradores da instituição PUC sobre os riscos de ataques de engenharia social, com foco na conscientização sobre a importância da segurança digital. A iniciativa visa simular um ataque de phishing realista, no qual funcionários e alunos receberão e-mails maliciosos disfarçados de notificações legítimas, com o objetivo de instigar o clique em links comprometidos que, ao serem acessados, levam os usuários a uma página falsa de captura. Esta ação é parte de um processo educacional que inclui a realização de um curso obrigatório de conscientização sobre phishing. | **RESULTADO ESPERADO:**  **Aumento da conscientização sobre phishing e ataques de engenharia social.**   * Identificação de vulnerabilidades entre os usuários-alvo. * Geração de relatórios detalhados para melhoria contínua da segurança. * Engajamento dos usuários no curso de conscientização. |
| **JORNADAS**  **Jornada do Phished (Usuário Alvo do Ataque):**   * + Recebe um e-mail disfarçado de notificação oficial.   + Acredita que a solicitação é verdadeira e clica no link fornecido.   + Ao acessar a página falsa, tem seus dados capturados pelo sistema.   + É imediatamente informado de que caiu em um golpe de phishing.   + É redirecionado para o curso de conscientização.   + Conclui o curso e recebe um certificado de participação.  1. Jornada do Phisher (Atacante - Coordenador do Projeto):    * Desenvolve e-mails maliciosos convincentes.    * Define os alvos do ataque (alunos e colaboradores da PUC).    * Envia os e-mails em ondas programadas.    * Monitora a taxa de abertura e cliques nos links.    * Analisa quais usuários caíram no golpe.    * Coleta dados para compilar relatórios detalhados.    * Avalia os resultados e propõe melhorias na campanha. 2. Jornada do Sistema (Ferramenta utilizada no ataque):    * Dispara os e-mails maliciosos conforme programado.    * Captura e armazena os dados dos usuários que clicaram nos links.    * Redireciona automaticamente os phished para a página de conscientização.    * Gera um CSV com as informações coletadas para análise posterior.    * Fornece dashboards para que os organizadores visualizem os resultados da campanha. | **FUNCIONALIDADES:**  **Envio de E-mail Malicioso:**  Disparo de 5 tipos diferentes de e-mails maliciosos de forma aleatória.   1. Página de Phishing:   Exibe mensagem informando que o usuário caiu no golpe.  Redireciona automaticamente para um curso de conscientização obrigatório.  Curso composto por slides informativos, vídeos educativos e quizzes interativos.   1. Monitoramento de Cliques:   Uso de scripts Python para rastrear quem clicou nos e-mails.  Geração de um CSV com os dados para posterior análise.   1. Relatórios e Análises:   Relatórios detalhados sobre cliques, interações e adesão ao curso.  Dados utilizados para ajustar futuras campanhas. | **MÉTRICAS PARA VALIDAR A HIPÓTESE DE NEGÓCIO:**  Número de usuários que clicaram nos e-mails maliciosos.   * Percentual de usuários que concluíram o curso de conscientização. * Comparação do nível de conscientização antes e depois da campanha. * Feedback qualitativo dos participantes sobre a eficácia da campanha. |
| **CUSTO E CRONOGRAMA:**  **Desenvolvimento dos e-mails e scripts de monitoramento: 2 semanas.**   * Configuração da página de phishing e do curso: 3 semanas. * Período de execução da campanha: 1 mês. * Análise de resultados e ajustes: 2 semanas. * Total estimado: 2 meses para a implementação completa. |