PROJECT CHARTER

Data Safe AI

Componentes do grupo:

1) Ana Flavia Ribeiro Lorêdo dos Santos No 23025092

2) Fernanda Mayumi Kuba Kato No 23024484

3) Guilherme Medeiros No 23024555

4) Kevin Makoto Shiroma No 20020925

5) Lorena Bernardo No 23025048

6) Matheus Sampaio Duarte No 23024588

7) Renato Riichi Kato No 23024516

8) Paulo Carvalho No 23024564

São Paulo, 18/11/2024

1.Organização - Resumir das condições do projeto

Problema: As organizações enfrentam um risco crescente de ataques cibernéticos, especialmente de phishing, que têm como alvo os colaboradores despreparados. Muitos funcionários não sabem identificar e reagir adequadamente a esses tipos de ataques, o que pode comprometer a segurança da empresa. O comportamento inadequado ao clicar em links maliciosos em e-mails de phishing é uma das principais vulnerabilidades exploradas pelos cibercriminosos. Isso evidencia a falta de conscientização e treinamento sobre práticas seguras de cibersegurança, expondo a empresa a riscos consideráveis de comprometimento de dados e infraestruturas.

2. Project Charter – Termo de Compromisso

Nome do projeto: Data Safe AI

Cronograma básico - Data: Início: 04/08/2024 Fim: 22/11/2024

Organização: Data Safe AI

Gerente do Projeto, Responsabilidades e autoridade:

Gerente de Projeto e PO (Paulo Carvalho): Responsável por definir o escopo inicial do projeto, os stakeholders envolvidos, coordenar as partes interessadas, gerenciar conflitos e monitorar os indicadores do projeto.

Engenheiro de Dados (Kevin Makoto Shiroma): Responsável pela tratação, armazenamento de análise dos dados coletados e modelagem do banco de dados.

Analista de Dados (Ana Flavia Lorêdo e Fernanda Mayumi Kuba Kato): Responsável pela análise exploratória de dados, criação de dashboards e relatórios, integração com ferramentas de visualização de dados.

Desenvolvedor (Matheus Sampaio Duarte): Responsável pelo desenvolvimento da arquitetura do site e pela codificação e implementação da interface front e back end.

Ux Designer (Lorena Bernardo): Responsável pelo desenvolvimento da experiência do usuário, desempenhando papel fundamental na criação de um produto que proporcione uma experiência intuitiva e eficaz para os usuários finais enquanto navegam pela plataforma da Data Safe AI.

Desenvolvedor de IA e ML (Guilherme Medeiros): Responsável pelo desenvolvimento e implementação de algoritmos de Processamento de Linguagem Natural (NLP) e Regressão, com o objetivo de analisar e prever incidentes de phishing, bem como gerar insights a partir dos dados coletados.

Controle de Qualidade (Renato Riichi Kato): Responsável pela garantia dos padrões de qualidade estabelecidos durante o levantamento dos requisitos do sistema e na garantia de que o software apresente alta qualidade.

Declaração do escopo

Objetivo do projeto

O objetivo central do Data Safe AI é detectar e corrigir as vulnerabilidades de comportamento dos colaboradores no que diz respeito à segurança digital, simulando de forma controlada ataques de phishing. O projeto tem como metas específicas:

- Educar os colaboradores sobre as melhores práticas de cibersegurança, ajudando-os a identificar e evitar ataques de phishing reais no futuro.
- Promover uma cultura de segurança digital dentro da organização, estimulando o comportamento consciente e a adoção de práticas mais seguras por parte de todos.

- Gerar dados e insights sobre o nível de conscientização e a exposição da empresa a riscos de phishing, fornecendo informações valiosas para a implementação de treinamentos direcionados e ações corretivas.
- Fortalecer a resiliência organizacional contra ameaças cibernéticas, capacitando os colaboradores a proteger dados e utilizar tecnologias de forma segura.

O projeto contribui para a criação de um ambiente corporativo mais seguro, minimizando vulnerabilidades humanas e fortalecendo as defesas digitais da empresa frente aos riscos cibernéticos.

Metas do projeto

As metas do Data Safe AI são centradas na educação dos colaboradores, na detecção de vulnerabilidades comportamentais e na promoção de uma cultura de segurança digital. O projeto busca alcançar:

1. Educação contínua sobre práticas de cibersegurança.
2. Criação de uma cultura de segurança digital.
3. Coleta e análise de dados para identificar vulnerabilidades.
4. Desenvolvimento de treinamentos direcionados para corrigir falhas de comportamento.
5. Fortalecimento da resiliência organizacional contra ameaças cibernéticas.
6. Automatização do processo de testes e treinamentos.
7. Geração de relatórios e insights para a gestão da segurança digital.
8. Melhoria contínua do sistema com base no desempenho dos colaboradores.

Essas metas são essenciais para garantir que o Data Safe AI seja eficaz na melhoria da postura de segurança cibernética da organização e na proteção contra ataques de phishing e outras ameaças cibernéticas.

Justificativa para o projeto:

A justificativa do Data Safe AI é baseada na crescente ameaça de ataques de phishing, que representam um risco significativo para as organizações, e na vulnerabilidade humana que muitas vezes serve como ponto de entrada para essas ameaças. Ao oferecer uma solução que educa os colaboradores, promove a conscientização contínua, melhora a segurança digital e reduz a exposição a riscos, o projeto se torna uma ferramenta crucial para fortalecer a segurança cibernética da empresa e garantir que ela esteja melhor preparada para enfrentar as ameaças cibernéticas no futuro.

Stakeholders - (Principais partes interessadas)

Desenvolvedores, Engenheiro de dados, Analistas de dados, QA, UX designer, Desenvolvedor de IA, PO, Gerente de Projeto, Usuários Finais, Investidores e Colaboradores.

Estimativa Inicial de Investimento (R$)

226.000,00

Fonte (inicial) de recursos que serão usados no projeto
Recursos Humanos: Gerente de Projeto e PO, Engenheiro de Dados, Analistas de Dados, Desenvolvedor, UX Designer, Desenvolvedor de IA e ML, Controle de Qualidade. Recursos Financeiros: Investimento inicial, programas para análise de dados, programas para gerenciamento de projeto, ferramentas para desenvolvimento do software. Recursos Materiais: Locação de um imóvel, aquisição de equipamentos, computadores e móveis.

Descrição resumida do produto ou serviço que o projeto irá produzir.

O Data Safe AI é uma plataforma que simula ataques de phishing para treinar os colaboradores a identificar e prevenir essas ameaças. Através de simulações, coleta de dados e relatórios, a ferramenta visa educar os funcionários sobre cibersegurança, identificar vulnerabilidades comportamentais e fortalecer a cultura de segurança digital na empresa.

Principais fases (MARCOS) do projeto
1. **Planejamento e Definição do Projeto** Definir metas, prazos e as necessidades do projeto. 2. **Pesquisa e Análise de Riscos** Estudar os principais riscos de phishing e como a plataforma pode ajudar a prevenir. 3. **Desenvolvimento da Plataforma** Criar a estrutura técnica e a base do sistema. 4. **Desenvolvimento da Interface (Design)** Criar o visual da plataforma e garantir que seja fácil de usar. 5. **Criação de Algoritmos de IA** Desenvolver algoritmos que detectem e simulem ataques de phishing. 6. **Coleta de Dados e Testes Iniciais** Coletar dados sobre o comportamento dos colaboradores e testar as primeiras simulações. 7. **Teste da Plataforma** Testar a plataforma para garantir que tudo funcione corretamente. 8. **Treinamento de Colaboradores** Ensinar os colaboradores a usar a plataforma e identificar phishing. 9. **Acompanhamento e Ajustes** Monitorar o uso da plataforma e fazer melhorias com base no feedback. 10. **Entrega Final e Avaliação** Finalizar o projeto, entregar a plataforma e avaliar os resultados.

Principais Riscos	Contingências que serão adotadas
Atrasos no desenvolvimento da plataforma	Aumentar os recursos da equipe ou ajustar o cronograma, priorizando as funcionalidades essenciais para o lançamento inicial.
Baixa adesão dos colaboradores aos treinamentos	Implementar uma abordagem de gamificação e reforçar a comunicação interna sobre a importância do treinamento.
Identificação inadequada de comportamentos de phishing	Ajustar os algoritmos de IA após a análise de dados e feedback, realizando testes contínuos e melhorias.
Falta de comunicação entre as equipes do projeto	Estabelecer reuniões regulares de acompanhamento, além de usar ferramentas de comunicação e gestão de projetos para manter todos alinhados.
Inadequação da plataforma a diferentes perfis de usuários	Realizar testes de usabilidade com grupos diversos de usuários e ajustar a interface conforme o feedback recebido.
Falha na coleta e análise de dados	Revisar os processos de coleta de dados, melhorar a qualidade das fontes e integrar novas ferramentas de análise, se necessário.

Premissas

Recursos humanos, financeiros e materiais e um planejamento inicial.

Restrições (limites)

As restrições do projeto incluem um orçamento limitado, que exige controle rigoroso de custos, e um prazo fixo para a entrega da solução, o que limita a flexibilidade nas fases de desenvolvimento. O projeto também depende do uso de tecnologias e ferramentas já existentes na empresa, o que pode restringir a adoção de novas soluções ou inovações. Além disso, deve-se garantir a conformidade legal com regulamentos de privacidade de dados, como a LGPD, o que impõe limites ao tipo de dados que podem ser coletados e utilizados. A capacidade de infraestrutura de TI também pode ser uma restrição, limitando o desempenho e escalabilidade da solução. Ter um escopo bem definido é essencial para gerenciar essas limitações, pois ajuda a estabelecer claramente os objetivos, entregáveis e limites do projeto, garantindo que todos os envolvidos estejam alinhados e possam trabalhar de forma focada, dentro dos recursos e prazos disponíveis.

Exclusões

As exclusões do projeto Data Safe AI incluem a integração com sistemas externos não previstos, o desenvolvimento de versões para dispositivos móveis, e a consultoria jurídica detalhada sobre regulamentações, embora a plataforma siga as leis de proteção de dados. O projeto também não prevê mudanças na infraestrutura de TI da empresa, operando com os recursos existentes, e não abrange treinamentos presenciais extensivos para todos os colaboradores, mas sim treinamentos virtuais. Além disso, a manutenção pós-lançamento não faz parte do escopo, sendo responsabilidade de outra iniciativa, se necessário. Essas exclusões ajudam a manter o foco no escopo original e nas entregas essenciais do projeto.

Comentários e informações relevantes para o desenvolvimento do projeto:

É de extrema importância de manter uma comunicação contínua com os stakeholders para garantir que as expectativas estejam alinhadas. É fundamental realizar testes regulares nas simulações de phishing para assegurar sua eficácia e coletar feedback dos usuários para aprimorar a experiência e a interface. A segurança de dados é uma prioridade, com medidas rigorosas para proteger informações sensíveis. Além disso, a plataforma precisa ser escalável, acompanhando o crescimento da empresa, e o projeto deve ser monitorado regularmente para ajustes no andamento e garantir que a educação contínua em cibersegurança seja sempre relevante e eficaz.