### **Título: Sistema de Resposta Automatizada a Incidentes de Phishing em E-mails usando IA**

### 

### **Contexto e Justificativa:**

### O phishing é uma das principais ameaças cibernéticas, responsável por grande parte dos vazamentos de dados e prejuízos financeiros em organizações. Ataques de phishing são frequentemente realizados via e-mail, onde os criminosos se passam por entidades confiáveis para enganar os usuários e roubar informações sensíveis. A detecção manual de e-mails de phishing é ineficiente e sujeita a erros humanos, especialmente em ambientes com grande volume de mensagens. Este projeto visa utilizar técnicas de Inteligência Artificial (IA) e Processamento de Linguagem Natural (NLP) para automatizar a detecção e resposta a e-mails de phishing, reduzindo o tempo de resposta e aumentando a eficácia da defesa.

### 

### **Objetivo Geral:**

### Desenvolver um sistema automatizado de detecção e resposta a incidentes de phishing em e-mails, utilizando IA para analisar e classificar mensagens suspeitas.

### **Objetivos Específicos:**

### Integração com APIs de e-mail:

### Conectar-se às APIs do Gmail e Microsoft Graph para coletar e-mails em tempo real, extraindo metadados (remetente, assunto, corpo da mensagem, links, anexos).

### Análise de conteúdo com NLP:

### Aplicar técnicas de NLP para identificar padrões de phishing, como:

### Análise de sentimentos: Detectar tom urgente ou ameaçador comum em e-mails de phishing.

### Detecção de entidades nomeadas: Identificar nomes de empresas, pessoas ou serviços falsos.

### Análise de links: Verificar se URLs são maliciosos ou suspeitos.

### Análise de similaridade de texto: Comparar o conteúdo do e-mail com modelos conhecidos de phishing.

### 

### Classificação de e-mails:

### Usar modelos de machine learning (como redes neurais ou algoritmos de classificação) para categorizar e-mails como "seguros", "suspeitos" ou "maliciosos".

### Resposta automatizada:

### Mover e-mails classificados como phishing para uma pasta de quarentena.

### Bloquear remetentes maliciosos.

### Enviar alertas para o usuário e a equipe de segurança.

### Mecanismo de alerta:

### Criar um sistema de notificação em tempo real para informar usuários e equipes de segurança sobre e-mails classificados como phishing.

### 

### **Escopo do Projeto:**

### O projeto se concentrará exclusivamente na detecção e resposta a e-mails de phishing, utilizando as APIs do Gmail e Microsoft Graph para coleta de dados e técnicas de NLP para análise de conteúdo. O sistema será capaz de:

### Coletar e-mails em tempo real.

### Analisar o conteúdo dos e-mails para identificar indicadores de phishing.

### Classificar e-mails como seguros, suspeitos ou maliciosos.

### Tomar ações automatizadas, como quarentena e bloqueio.

### Notificar usuários e equipes de segurança sobre incidentes.

