# Security Analysis API Documentation

## Initial Security Analysis API

**Endpoint:** https://97e2-2406-7400-1c3-6062-c91a-dbe0-4c3-7428.ngrok-free.app/analyze\_security  
**Method:** POST  
**Content-Type:** application/json

**Sample Input:**

{  
 "text": "cognizant"  
}

**Sample Response:**

{  
 "analysis": "Cognizant has faced several security breaches, including a ransomware attack in 2020 that affected its operations.",  
 "risk\_level": "These incidents highlight the need for Cognizant to enhance its cybersecurity measures to protect client and employee data."  
}

## 2. Document Analysis API

**Endpoint:** https://97e2-2406-7400-1c3-6062-c91a-dbe0-4c3-7428.ngrok-free.app/analyze\_documents  
**Method:** POST  
**Content-Type:** multipart/form-data

**Sample Input:** - files: [soc2\_policy.txt] - questions: [“What is the password policy?”, “How is customer data protected?”, “What is the incident response timeframe?”]

**Sample Response:**

{  
 "risk\_score": "LOW",  
 "explanation": "Based on the provided document, the overall security risk level can be assessed as follows:\n\n1. \*\*Password Policy\*\*: The password requirements include a minimum of 12 characters, complexity rules, and"  
}

## 3. Vulnerability Check API

**Endpoint:** https://97e2-2406-7400-1c3-6062-c91a-dbe0-4c3-7428.ngrok-free.app/check\_vulnerability  
**Method:** POST  
**Content-Type:** application/x-www-form-urlencoded

**Sample Input:** - software: log4j - version: 2.14.1

**Sample Response:**

{  
 "is\_vulnerable": "YES",  
 "severity": "HIGH",  
 "explanation": "Contains Log4Shell vulnerability (CVE-2021-44228) allowing remote code execution"  
}

## 4. Chat Interface API

**Endpoint:** https://97e2-2406-7400-1c3-6062-c91a-dbe0-4c3-7428.ngrok-free.app/chat  
**Method:** POST  
**Content-Type:** application/x-www-form-urlencoded

**Sample Input:** - query: “Can you check on OpenAI security breaches in recent years?”

**Sample Response:**

{  
 "response": "OpenAI has reported no major security breaches in recent years, but its ChatGPT model was hacked in 2022 to bypass content filters."  
}