Risk Generation Prompt Engineering Notes

Since the risk generation is something we are adding to our project to help visualize the current risks an organization has, there is no initial data, examples, or templates. We will have to research and generate our own examples.

Luckily, the risks are easier to read in a tabular format. Therefore, a JSON schema will work best.

In [1]:

```
import os
import google.generativeai as genai
from dotenv import load_dotenv, find_dotenv

load_dotenv(find_dotenv())
genai.configure(api_key=os.environ["GEMINI_API_KEY"])
model = genai.GenerativeModel('gemini-2.5-pro')
```

```
c:\Users\victo\anaconda3\envs\sd2\lib\site-packages\tqdm\auto.py:21: TqdmWarning: IP
rogress not found. Please update jupyter and ipywidgets. See https://ipywidgets.read
thedocs.io/en/stable/user_install.html
  from .autonotebook import tqdm as notebook_tqdm
```

In [2]:

```
def export_html_to_files(full_html_content, html_output_filename="output.html"):
    """
    Takes the generated HTML string and performs the file export to HTML

    Args:
        full_html_content (str): The HTML content generated by generate_html_from_m
        html_output_filename (str): The path to save the intermediate HTML file.
    """
    if not full_html_content:
        print("Export failed: HTML content is empty or None.")
        return

    try:
        with open(html_output_filename, "w", encoding="utf-8") as f:
            f.write(full_html_content)
        print(f"✅ Successfully exported HTML: {html_output_filename}")

    except Exception as e:
        print(f"❌ An unexpected error occurred during file export: {e}")
```

In [3]:

```
proModel = genai.GenerativeModel('gemini-2.5-pro')
flashModel = genai.GenerativeModel('gemini-2.5-flash')
```

In [4]:

```
def get_severity(score: float) -> tuple[str, str, str]:
    """Determines the color (hex), label, and Tailwind color class based on the CVS
    if score >= 9.0:
        return '#EF4444', 'CRITICAL', 'vuln-critical'
    if score >= 7.0:
        return '#F59E0B', 'HIGH', 'vuln-high'
    if score >= 4.0:
        return '#3B82F6', 'MEDIUM', 'vuln-medium'
    return '#10B981', 'LOW', 'vuln-low'

def json_to_html_cards(json_data: dict) -> str:
    """
    Converts the JSON vulnerability report into styled HTML cards.

    Args:
        json_data: A dictionary representing the parsed JSON vulnerability report.

    Returns:
        A string containing the HTML markup for the vulnerability cards.
    """
    if not json_data or not json_data.get('vulnerabilities'):
        return '<div class="text-center p-8 text-gray-500">No vulnerabilities found

    html_cards = []

    for vuln in json_data['vulnerabilities']:
        hex_color, label, tw_color_class = get_severity(vuln['severity_cvss_score']

        # 1. Resources List HTML
        resources_html = ""
        for res in vuln['recommendations']['resources']:
            resources_html += f"""
                <li class="mb-1">
                    <a href="{res['url']}" target="_blank" class="text-blue-600 hov
                        <i class="fas fa-external-link-alt mr-2 text-xs"></i>
                        {res['type'].upper()}: {res['description']}
                    </a>
                </li>
            """

        # 2. Affected Elements HTML
        affected_html = "".join([
            f'<span class="inline-block bg-gray-100 text-gray-700 text-xs px-3 py-1
            for el in vuln['affected_elements']
        ])

        # 3. Long-Term Fix HTML (Conditional)
        long_term_fix_html = ""
        if vuln['recommendations'].get('long_term_fix'):
            long_term_fix_html = f"""
                <div class="mb-4 p-4 bg-red-100 rounded-lg shadow-sm">
                    <p class="font-semibold text-red-800 flex items-center mb-1">
                        <i class="fas fa-cogs mr-2"></i> Long-Term/Strategic Fix:
                    </p>
                    <p class="text-sm text-red-900">{vuln['recommendations']['long_
                </div>
            """

        # 4. Main Card Structure
        card = f"""
            <div class="bg-white shadow-xl rounded-2xl overflow-hidden transform tr
```

```
                <!-- Header and Score -->
                <div class="p-6">
                    <div class="flex justify-between items-start mb-4">
                        <h2 class="text-2xl font-bold text-gray-900">{vuln['risk_na
                        <div class="text-center p-2 rounded-lg text-white font-extr
                            <span class="block">{label}</span>
                            <span class="text-xs">CVSS {vuln['severity_cvss_score']
                        </div>
                    </div>

                    <!-- Overview -->
                    <p class="text-gray-600 mb-6 border-l-4 border-gray-200 pl-4 it
                        {vuln['overview']}
                    </p>

                    <!-- Affected Elements -->
                    <h3 class="text-lg font-semibold text-gray-800 mb-2 mt-4">Affec
                    <div class="flex flex-wrap mb-6">
                        {affected_html}
                    </div>
                </div>

                <!-- Recommendations Section -->
                <div class="bg-gray-50 p-6">
                    <h3 class="text-lg font-bold text-gray-800 mb-4">Mitigation Rec

                    <!-- Easy Fix -->
                    <div class="mb-4 p-4 bg-yellow-100 rounded-lg shadow-sm">
                        <p class="font-semibold text-yellow-800 flex items-center m
                            <i class="fas fa-hammer mr-2"></i> Quick/Easy Fix:
                        </p>
                        <p class="text-sm text-yellow-900">{vuln['recommendations']
                    </div>

                    <!-- Long Term Fix (Conditional) -->
                    {long_term_fix_html}

                    <!-- Resources -->
                    <h4 class="font-semibold text-gray-700 mt-4 mb-2 border-t pt-4"
                    <ul class="list-none space-y-2">
                        {resources_html}
                    </ul>
                </div>
            </div>
        """
        html_cards.append(card)

    return "".join(html_cards)

def generate_full_report_html(vulnerability_data: dict) -> str:
    """Generates the full, standalone HTML page including header, styles, and card

    card_content = json_to_html_cards(vulnerability_data)

    # We must use inline styles (style="border-top-color: #EF4444;") for the dynami
    # since external Tailwind classes (like border-[${severity.color}]) cannot be u
    # The Python function is now generating the specific hex codes inline for color

    full_html = f"""
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Vulnerability Report Visualizer (Python Generated)</title>
    <!-- Load Tailwind CSS -->
    <script src="https://cdn.tailwindcss.com"></script>
    <!-- Load Font Awesome for icons -->
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesom
    <script>
        // Configuration needed for custom colors
        tailwind.config = {{
            theme: {{
                extend: {{
                    fontFamily: {{
                        sans: ['Inter', 'sans-serif'],
                    }},
                    // Note: These colors are also applied via inline style in Pyth
                    colors: {{
                        'vuln-critical': '#EF4444',
                        'vuln-high': '#F59E0B',
                        'vuln-medium': '#3B82F6',
                        'vuln-low': '#10B981',
                    }}
                }}
            }}
        }}
    </script>
</head>
<body class="bg-gray-100 min-h-screen p-4 sm:p-8 font-sans">
    <div class="max-w-7xl mx-auto">
        <header class="text-center py-6 mb-8 bg-white shadow-lg rounded-xl">
            <h1 class="text-4xl font-extrabold text-gray-900 tracking-tight">
                Cybersecurity Vulnerability Dashboard
            </h1>
            <p class="text-lg text-gray-500 mt-2">Innovatech Dynamics - Cloud Secur
        </header>

        <!-- Container for the generated vulnerability cards -->
        <div class="grid grid-cols-1 md:grid-cols-2 lg:grid-cols-3 gap-8">
            {card_content}
        </div>

    </div>
</body>
</html>
"""
    return full_html
```

In [ ]:

```
import textwrap
import json
```

```
example_report = "risk_template/example.tex"
example_risk_list = "risk_template/example_risk_list.json"
context_report = "risk_template/context.tex"

# Prompt
risk_prompt_text = textwrap.dedent(r'''You are an expert cybersecurity analyst task
Your goal is to extract all explicit and implicit risks and map them precisely to t

Focus Areas for Extraction:
    - Risk Name & Overview: Identify distinct vulnerabilities (e.g., exposed ports,
    - Affected Elements: Note the specific IP addresses, ports, domains, or control
    - Recommendations: Match the fixes mentioned in the report's Recommendations se
    - CVSS Score: Assign an appropriate severity score (1-10) based on the report's
    - Resources: Since the report does not provide links, use your knowledge to pro
''')

risk_example_text = 'Example Task:\nFollow the structure, formatting, and analytica

# Example/Template Report
with open(example_report, 'r') as file:
  data = file.read()
  risk_example_text += data

risk_example_text += "\n\nExample Risk List:\n"

# Example Risk List
with open(example_risk_list, 'r') as file:
  data = json.load(file)
  risk_example_text += f"{json.dumps(data,indent=2)}"

# Context Report
report_response = ''
with open(context_report, 'r') as file:
  data = file.read()
  report_response += data

print(risk_example_text)
print("========================")
print(report_response)
```

Example Task:
Follow the structure, formatting, and analytical style of this example precisely.

Example report:

~~~
```latex
\documentclass[12pt]{article}
\usepackage[letterpaper, margin=1in]{geometry}
\usepackage{amsmath, amssymb}
\usepackage{pifont} % For the checkmark symbol \ding{51}
\usepackage{booktabs} % For professional-looking tables
\usepackage{hyperref} % For links
\usepackage{fontawesome5}
\usepackage{setspace} % For line spacing
\usepackage{url} % Included and applied to domains
\usepackage{seqsplit} % Applied to long code/IP strings

\hypersetup{
    colorlinks=true,
    urlcolor=blue,
    linkcolor=black
}

\title{\textbf{Cybersecurity Readiness Report for G.A.S. Inc.}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report provides a cybersecurity assessment for G.A.S. Inc., based on a combination of a self-reported questionnaire and external technical scans. The analysis reveals critical vulnerabilities in network perimeter security, email authentication, and internal security policies. The findings indicate a high-risk posture that requires immediate attention to mitigate significant threats such as unauthorized access, data breaches, and phishing attacks.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: G.A.S. Inc.
    \item \textbf{Email Domain}: \url{gasinc.net}
    \item \textbf{Website Domain}: \url{www.gasinc.net}
    \item \textbf{External IP / Web Host}: 104.28.1.189
    \item \textbf{DNS Hosting}: Self-hosted or privately managed (\url{dns1.gasinc.net}, \url{dns2.gasinc.net})
\end{itemize}

\section{Security Questionnaire Review}
\begin{table}[h!]
\centering
\caption{Security Control Status}
\label{tab:security_controls}
\begin{tabular}{l c}
\toprule
\textbf{Security Control} & \textbf{Status} \\
~~~

```
\midrule
MFA for Email & No \\
MFA for Computer Login & No \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & No \\
New Employee Security Awareness Training & No \\
Annual All-Employee Security Training & No \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: The organization reports significant gaps in foundationa
l cybersecurity policies and controls. The absence of mandatory Multi-Factor Authent
ication (MFA) for email and computer access, coupled with a lack of employee securit
y training and an acceptable use policy, creates a substantial risk of security inci
dents originating from compromised user credentials and lack of security awareness.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item The domain's A record points to a single IP address, \texttt{104.28.1.18
9}, which serves as both the primary external IP and the web host.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The organization uses a third-party email provider, as indicated by the MX
records: \seqsplit{\texttt{mx.mailhostbox.com}} and \seqsplit{\texttt{mx2.mailhostbo
x.com}}.
    \item \textbf{SPF record} is present but configured with a softfail: \seqsplit
{\texttt{v=spf1 include:spf.mailhostbox.com ~all}}. This configuration advises recei
ving servers to accept but mark potentially forged emails, which is less secure than
a hardfail (`-all`) policy.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item \textbf{No DMARC record was found for the \url{gasinc.net} domain.}
    \item The absence of a DMARC policy significantly weakens the organization's def
ense against email spoofing and phishing attacks, as there is no instruction for rec
ipient servers on how to handle fraudulent emails claiming to be from \url{gasinc.ne
t}.
\end{itemize}

\noindent \textbf{Conclusion}: Email security is weak. The lack of a DMARC record an
d the use of a softfail SPF policy leave the organization highly susceptible to emai
l-based attacks.

\section{Port Scanning Results}

\subsection*{External IP / Web Host (104.28.1.189)}
A scan of the primary external IP address revealed numerous open ports, indicating m
ultiple services are directly exposed to the internet.
\begin{itemize}
    \item \textbf{Port 21 (FTP)}: Open
    \item \textbf{Port 22 (SSH)}: Open
    \item \textbf{Port 25 (SMTP)}: Open
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 110 (POP3)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
    \item \textbf{Port 3389 (RDP)}: Open
\end{itemize}
This configuration represents a critical security risk. Exposing services like FTP,
SSH, and RDP directly to the public internet dramatically increases the attack surfa
ce and makes the network a prime target for brute-force attacks and exploitation of
potential vulnerabilities.

\section{Risk Assessment \& Readiness Summary}
\begin{table}[h!]
\centering
\caption{Readiness Summary}
\label{tab:readiness_summary}
\begin{tabular}{l c l}
\toprule
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\midrule
Authentication Security & Weak & No MFA for email or computer logins \\
Email Security & High Risk & No DMARC record; weak SPF policy \\
Network Exposure & Critical & Multiple high-risk services exposed (RDP, SSH, FTP) \\
Web Hosting & At Risk & Hosted on the same IP as critical exposed services \\
Policy \& Training & Deficient & Lacks AUP and security awareness training programs
\\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
Immediate action is required to address the identified critical vulnerabilities. We
recommend prioritizing the following:
\begin{enumerate}
    \item \textbf{Harden Network Perimeter}: Immediately close all unnecessary ports
on the external firewall (\texttt{104.28.1.189}). Access to services like RDP and SS
H should be restricted to trusted IP addresses or, preferably, placed behind a VPN.
FTP should be replaced with a secure alternative like SFTP.
    \item \textbf{Implement DMARC}: Deploy a DMARC record for the \url{gasinc.net} d
omain, starting with a monitoring policy (\texttt{p=none}) and progressing to a quar
antine or reject policy (\texttt{p=reject}) to prevent domain spoofing.
    \item \textbf{Strengthen SPF Record}: Update the SPF record to use a hardfail me
chanism (`-all`) instead of a softfail (`~all`) to instruct receiving mail servers t
o reject messages from unauthorized senders.
    \item \textbf{Enforce Multi-Factor Authentication (MFA)}: Mandate MFA for all us
ers for email access, remote access (VPN), and computer logins to protect against cr
edential theft.
    \item \textbf{Develop and Implement Security Policies}: Establish a formal Accep
table Use Policy (AUP) and create a mandatory security awareness training program fo
r all employees, to be conducted upon hiring and at least annually thereafter.
\end{enumerate}

\section{Conclusion}
G.A.S. Inc. currently exhibits a high-risk cybersecurity posture characterized by a
severely exposed network perimeter, inadequate email security, and a lack of fundame
```

~~~~
ntal security policies and user training. The combination of these weaknesses create
s a high probability of a successful cyberattack. The recommendations outlined in th
is report are critical and should be implemented without delay to build a foundation
al security program and protect the organization's assets and reputation.

\vspace{1cm}
\noindent Prepared by: \\
Cybersecurity Assessment Team\\
Date: October 14, 2025

\end{document}
```
~~~~

Example Risk List:

```
{
  "vulnerabilities": [
    {
      "risk_name": "Critical Network Service Exposure",
      "overview": "The external IP address 104.28.1.189 has multiple high-risk servi
ces exposed directly to the public internet, including FTP (Port 21), SSH (Port 22),
and RDP (Port 3389). This dramatically increases the attack surface, making the netw
ork vulnerable to brute-force attacks and service exploitation.",
      "severity_cvss_score": 9.3,
      "affected_elements": [
        "External IP: 104.28.1.189",
        "Port 21 (FTP)",
        "Port 22 (SSH)",
        "Port 3389 (RDP)"
      ],
      "recommendations": {
        "easy_fix": "Immediately close all unnecessary ports on the external firewal
l. Services like RDP and SSH must be restricted to trusted IP addresses only.",
        "long_term_fix": "Implement a Virtual Private Network (VPN) solution and req
uire all remote access (RDP, SSH) to pass through the VPN. Replace FTP with a secure
alternative like SFTP or FTPS.",
        "resources": [
          {
            "type": "website",
            "url": "https://docs.microsoft.com/en-us/windows-server/remote/remote-de
sktop-services/rds-security-guidance",
            "description": "Microsoft's security guidance for securing Remote Deskto
p Services (RDP)."
          },
          {
            "type": "youtube",
            "url": "https://www.youtube.com/watch?v=example-secure-ssh",
            "description": "Video tutorial on hardening SSH configurations."
          }
        ]
      }
    },
    {
      "risk_name": "Missing DMARC Policy (Email Spoofing)",
      "overview": "No DMARC record was found for the gasinc.net domain. This absence
is a High Risk vulnerability, as it allows attackers to easily spoof emails claiming
to be from G.A.S. Inc., significantly increasing the likelihood of successful phishi
```

```
ng and impersonation attacks.",
      "severity_cvss_score": 8.0,
      "affected_elements": [
        "Email Domain: gasinc.net",
        "DMARC Record"
      ],
      "recommendations": {
        "easy_fix": "Deploy a DMARC record immediately, starting with a monitoring p
olicy (`p=none`) to collect reports without affecting email delivery.",
        "long_term_fix": "Progress the DMARC policy to quarantine (`p=quarantine`) o
r reject (`p=reject`) after verifying all legitimate sending sources, ensuring prote
ction against spoofing.",
        "resources": [
          {
            "type": "website",
            "url": "https://dmarcian.com/dmarc-record-creation/",
            "description": "Online tool and guide for generating a DMARC record."
          },
          {
            "type": "documentation",
            "url": "https://www.agari.com/email-security-blog/dmarc-guide/",
            "description": "Comprehensive guide to DMARC implementation and policy p
rogression."
          }
        ]
      }
    },
    {
      "risk_name": "Weak SPF Record Configuration",
      "overview": "The Sender Policy Framework (SPF) record is configured with a sof
tfail (`~all`) mechanism. This instructs receiving servers to accept and mark potent
ially forged emails, instead of rejecting them outright, weakening the defense again
st unauthorized email sending.",
      "severity_cvss_score": 6.5,
      "affected_elements": [
        "Email Domain: gasinc.net",
        "SPF Record"
      ],
      "recommendations": {
        "easy_fix": "Update the SPF record to use a hardfail mechanism (`-all`) to i
nstruct receiving mail servers to reject messages from unauthorized servers immediat
ely.",
        "long_term_fix": "Review all legitimate third-party senders and ensure their
includes are correct before moving to hardfail to prevent false positives.",
        "resources": [
          {
            "type": "website",
            "url": "https://mxtoolbox.com/spf.aspx",
            "description": "SPF record testing and diagnostic tool."
          }
        ]
      }
    },
    {
      "risk_name": "Absence of Mandatory Multi-Factor Authentication (MFA)",
      "overview": "The organization does not mandate Multi-Factor Authentication for
```

```
email access or computer logins. This foundational gap leaves the organization highl
y susceptible to credential theft and account takeover via phishing or leaked passwo
rds.",
      "severity_cvss_score": 8.8,
      "affected_elements": [
        "MFA for Email",
        "MFA for Computer Login",
        "Employee User Accounts"
      ],
      "recommendations": {
        "easy_fix": "Mandate MFA for all users on critical services, starting with e
mail access and remote access (VPN).",
        "long_term_fix": "Implement a Single Sign-On (SSO) solution with mandatory M
FA for all corporate applications and systems to create a unified, secure login expe
rience.",
        "resources": [
          {
            "type": "youtube",
            "url": "https://www.youtube.com/watch?v=example-mfa-importance",
            "description": "Explanation of MFA and its importance in modern cybersec
urity."
          },
          {
            "type": "documentation",
            "url": "https://www.cisa.gov/stop-ransomware/mandatory-mfa",
            "description": "CISA guidance on enforcing Multi-Factor Authentication."
          }
        ]
      }
    },
    {
      "risk_name": "Deficient Security Policy and Training",
      "overview": "The organization lacks foundational policies, including an Accept
able Use Policy (AUP) and mandatory security awareness training for all employees (n
ew hires and annual). This deficiency creates a high risk of security incidents orig
inating from human error or lack of security awareness.",
      "severity_cvss_score": 7.0,
      "affected_elements": [
        "Acceptable Use Policy (AUP)",
        "New Employee Security Awareness Training",
        "Annual All-Employee Security Training"
      ],
      "recommendations": {
        "easy_fix": "Implement a basic, mandatory security awareness training sessio
n for all current employees immediately.",
        "long_term_fix": "Develop a formal Acceptable Use Policy (AUP) and establish
a recurring, mandatory security awareness training program with phishing simulations
to build a strong security culture.",
        "resources": [
          {
            "type": "website",
            "url": "https://www.sans.org/security-awareness-training/",
            "description": "Resources and guidance for building effective security a
wareness programs."
          }
        ]
      }
    }
  ]
}
========================
\documentclass[12pt]{article}
\usepackage[letterpaper, margin=1in]{geometry}
\usepackage{amsmath, amssymb}
\usepackage{pifont} % For the checkmark symbol \ding{51}
\usepackage{booktabs} % For professional-looking tables
\usepackage{hyperref} % For links
\usepackage{fontawesome5}
\usepackage{setspace} % For line spacing
\usepackage{url} % Included and applied to domains
\usepackage{seqsplit} % Applied to long code/IP strings
\hypersetup{
    colorlinks=true,
    urlcolor=blue,
    linkcolor=black
}
\title{\textbf{Cloud Security Audit Report: Innovatech Dynamics}}
\author{Date: October 25, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Executive Summary}
This audit assessed the security posture of Innovatech Dynamics' cloud-native applic
ation infrastructure, which utilizes AWS, Kubernetes for orchestration, and a micros
ervices architecture. While the use of modern tools is commendable, the audit identi
fied \textbf{three critical vulnerabilities} stemming from cloud misconfigurations,
weak Identity and Access Management (IAM), and unpatched container images. The most
significant finding is the public exposure of the S3 data storage bucket, which requ
ires immediate remediation.

\section{Organizational and Technical Context}
\begin{itemize}
    \item \textbf{Organization Name}: Innovatech Dynamics
    \item \textbf{Primary Cloud Provider}: Amazon Web Services (AWS)
    \item \textbf{Architecture}: Microservices deployed on AWS EKS (Managed Kubernet
es)
    \item \textbf{Main Application Domain}: \url{app.innovatech-dyn.com}
    \item \textbf{Development Language}: Python/Go microservices
\end{itemize}

\section{Key Audit Findings}

\subsection*{Cloud Misconfiguration: S3 Bucket Public Exposure}
\begin{itemize}
    \item \textbf{Vulnerability}: The S3 bucket named \texttt{innovatech-prod-logs-s
torage}, used for storing application logs and analytics data, was found to be publi
cly accessible due to an incorrect bucket policy setting.
    \item \textbf{Affected Element}: AWS S3 Bucket \seqsplit{\texttt{arn:aws:s3:::in
novatech-prod-logs-storage}}.
```

```
    \item \textbf{Data Impact}: The bucket contains customer analytics records, incl
uding anonymized session IDs and geolocation data, which is a breach of compliance s
tandards if exposed.
    \item \textbf{Severity}: \textbf{Critical}.
\end{itemize}

\subsection*{Kubernetes (EKS) Security Issues}
\begin{itemize}
    \item \textbf{Vulnerability}: Multiple container images in the \texttt{product-c
atalog-service} deployment are running with known, unpatched vulnerabilities (CVE-20
24-XXXXX) and, critically, are running with \texttt{root} privileges within the cont
ainer.
    \item \textbf{Affected Elements}: Kubernetes Deployment \texttt{product-catalog-
service}, specifically the container image \texttt{prod-cat-v2.1} (running as root).
    \item \textbf{Exploitation Path}: A successful attack could exploit the image vu
lnerability to escape the container and potentially compromise the EKS worker node.
    \item \textbf{Severity}: \textbf{High}.
\end{itemize}

\subsection*{Weak IAM and Credential Management}
\begin{itemize}
    \item \textbf{Vulnerability}: A development-focused IAM user, \texttt{dev\_deplo
yer}, has been granted the \texttt{AdministratorAccess} policy instead of a more res
trictive custom policy. This user is actively used by a CI/CD pipeline script stored
in a private GitHub repository.
    \item \textbf{Affected Element}: AWS IAM User \texttt{arn:aws:iam::123456789012:
user/dev\_deployer}.
    \item \textbf{Risk}: If the GitHub repository or the CI/CD pipeline is compromis
ed, the attacker gains full administrative control over the entire AWS environment.
The Principle of Least Privilege is violated.
    \item \textbf{Severity}: \textbf{High}.
\end{itemize}

\section{Recommendations for Immediate Action}
Immediate action is required to address these critical findings.

\begin{enumerate}
    \item \textbf{Fix S3 Public Access}: The bucket policy for \texttt{innovatech-pr
od-logs-storage} must be modified to block all public access. The policy should only
allow access via specific IAM roles tied to the application services that require lo
gging access.
    \item \textbf{Secure Kubernetes Containers}: Update the \texttt{product-catalog-
service} deployment to use a patched container image and enforce the \texttt{runAsNo
nRoot: true} setting via a Pod Security Standard (or policy engine like OPA/Kyvern
o).
    \item \textbf{Implement Least Privilege}: Revoke the \texttt{AdministratorAcces
s} policy from the \texttt{dev\_deployer} IAM user. Replace it with a custom, fine-g
rained policy that only permits the specific actions necessary for the CI/CD deploym
ent process (e.g., only update EKS deployments, not create new S3 buckets).
\end{enumerate}

\section{Conclusion}
Innovatech Dynamics' reliance on cloud and container technologies has led to new sec
urity challenges primarily centered around misconfiguration and over-privileged acce
ss. While the core microservices design offers resilience, the current configuration
exposes the entire environment to critical data breach and account takeover risks. P
```

```
rompt execution of the outlined recommendations is mandatory to secure the platform.

\vspace{1cm}
\noindent Prepared by: \\CloudSec Audit Team\\Date: October 25, 2025
\end{document}
```

In [16]:

```python
risk_response = proModel.generate_content(
    contents=[risk_prompt_text, report_response + "\n" + risk_example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            "type": "object",
            "properties": {
                "vulnerabilities": {
                    "type": "array",
                    "description": "A list of identified cybersecurity risks/vulner
                    "items": {
                        "type": "object",
                        "properties": {
                            "risk_name": {
                                "type": "string",
                                "description": "A concise, descriptive name for the
                            },
                            "overview": {
                                "type": "string",
                                "description": "A text summary of the risk, its imp
                            },
                            "severity_cvss_score": {
                                "type": "number",
                                "description": "The calculated severity score (1-10
                            },
                            "affected_elements": {
                                "type": "array",
                                "description": "A list of system components, files,
                                "items": {
                                    "type": "string"
                                }
                            },
                            "recommendations": {
                                "type": "object",
                                "description": "Specific recommendations for mitiga
                                "properties": {
                                    "easy_fix": {
                                        "type": "string",
                                        "description": "A quick, immediate, or easy
                                    },
                                    "long_term_fix": {
                                        "type": "string",
                                        "description": "A more difficult, time-cons
                                    },
                                    "resources": {
                                        "type": "array",
                                        "description": "Links to external resources
                                        "items": {
                                            "type": "object",
                                            "properties": {
                                                "type": {
                                                    "type": "string",
                                                    "enum": ["youtube", "website",
                                                    "description": "The type of res
                                                },
                                                "url": {
                                                    "type": "string",
                                                    "format": "uri",
                                                    "description": "The URL of the
                                                },
                                                "description": {
                                                    "type": "string",
                                                    "description": "A brief descrip
                                                }
                                            },
                                            "required": ["type", "url"]
                                        }
                                    }
                                },
                                "required": ["easy_fix", "resources"]
                            }
                        },
                        "required": [
                            "risk_name",
                            "overview",
                            "severity_cvss_score",
                            "affected_elements",
                            "recommendations"
                        ]
                    }
                }
            },
            "required": ["vulnerabilities"]
        }
    }
)

print(risk_response.text)
```

```
{
  "vulnerabilities": [
    {
      "risk_name": "Publicly Accessible S3 Bucket",
      "overview": "The S3 bucket 'innovatech-prod-logs-storage', which contains customer analytics, session IDs, and geolocation data, was found to be publicly accessible due to an incorrect bucket policy. This direct exposure of sensitive data constitutes a critical security risk and a potential compliance breach.",
      "severity_cvss_score": 9.8,
      "affected_elements": [
        "AWS S3 Bucket: arn:aws:s3:::innovatech-prod-logs-storage"
      ],
      "recommendations": {
        "easy_fix": "Immediately modify the S3 bucket policy for 'innovatech-prod-logs-storage' to block all public access using the AWS S3 Block Public Access feature.",
        "resources": [
          {
            "type": "documentation",
            "url": "https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html",
            "description": "Official AWS documentation on S3 security best practices, including blocking public access."
          },
          {
            "type": "youtube",
            "url": "https://www.youtube.com/watch?v=f-aGv1i35gY",
            "description": "A video guide from AWS on how to use S3 Block Public Access to secure your buckets."
          }
        ],
        "long_term_fix": "Refactor the bucket policy to follow the principle of least privilege, allowing access only from specific IAM roles associated with the application services that require log data access."
      }
    },
    {
      "risk_name": "Insecure Kubernetes Container Configuration",
      "overview": "The 'product-catalog-service' deployment in the EKS cluster is using container images with known, unpatched vulnerabilities (e.g., CVE-2024-XXXXX). Critically, these containers are also configured to run with root privileges, which could allow an attacker to exploit an image vulnerability, escape the container, and compromise the underlying EKS worker node.",
      "severity_cvss_score": 8.5,
      "affected_elements": [
        "Kubernetes Deployment: product-catalog-service",
        "Container Image: prod-cat-v2.1"
      ],
      "recommendations": {
        "easy_fix": "Update the 'product-catalog-service' deployment to use a newer, patched version of the container image that resolves the known vulnerabilities.",
        "resources": [
          {
            "type": "documentation",
            "url": "https://kubernetes.io/docs/concepts/security/pod-security-standards/",
            "description": "Official Kubernetes documentation on Pod Security Standa
rds, which includes preventing containers from running as root."
          },
          {
            "type": "website",
            "url": "https://www.redhat.com/en/blog/practical-guide-running-openshift
-non-root-containers",
            "description": "A guide explaining the risks of running containers as ro
ot and how to avoid it."
          }
        ],
        "long_term_fix": "Implement a policy-as-code engine like OPA Gatekeeper or K
yverno to enforce security best practices across the cluster, such as requiring all
pods to have 'runAsNonRoot: true' and blocking images with known critical vulnerabil
ities."
      }
    },
    {
      "risk_name": "Over-privileged IAM User in CI/CD Pipeline",
      "overview": "The IAM user 'dev_deployer', which is used by the CI/CD pipeline,
has been assigned the 'AdministratorAccess' policy. This violates the principle of l
east privilege. If the CI/CD system or its associated code repository were compromis
ed, an attacker would gain full administrative control over the entire AWS accoun
t.",
      "severity_cvss_score": 9.1,
      "affected_elements": [
        "AWS IAM User: arn:aws:iam::123456789012:user/dev_deployer"
      ],
      "recommendations": {
        "easy_fix": "Immediately revoke the 'AdministratorAccess' policy from the 'd
ev_deployer' IAM user to contain the risk.",
        "resources": [
          {
            "type": "documentation",
            "url": "https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.
html#grant-least-privilege",
            "description": "AWS documentation on the best practice of granting least
privilege for IAM users and roles."
          },
          {
            "type": "website",
            "url": "https://www.datadoghq.com/blog/aws-iam-best-practices/",
            "description": "A comprehensive guide to AWS IAM best practices for secu
ring cloud environments."
          }
        ],
        "long_term_fix": "Create a new, fine-grained IAM policy that only grants the
'dev_deployer' user the specific permissions required for its CI/CD tasks (e.g., upd
ating EKS deployments, pushing images to ECR) and attach it to the user."
      }
    }
  ]
}
```

In [ ]:

```
risk_response = flashModel.generate_content(
    contents=[risk_prompt_text, report_response + "\n" + risk_example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            "type": "object",
            "properties": {
                "vulnerabilities": {
                    "type": "array",
                    "description": "A list of identified cybersecurity risks/vulner
                    "items": {
                        "type": "object",
                        "properties": {
                            "risk_name": {
                                "type": "string",
                                "description": "A concise, descriptive name for the
                            },
                            "overview": {
                                "type": "string",
                                "description": "A text summary of the risk, its imp
                            },
                            "severity_cvss_score": {
                                "type": "number",
                                "description": "The calculated severity score (1-10
                            },
                            "affected_elements": {
                                "type": "array",
                                "description": "A list of system components, files,
                                "items": {
                                    "type": "string"
                                }
                            },
                            "recommendations": {
                                "type": "object",
                                "description": "Specific recommendations for mitiga
                                "properties": {
                                    "easy_fix": {
                                        "type": "string",
                                        "description": "A quick, immediate, or easy
                                    },
                                    "long_term_fix": {
                                        "type": "string",
                                        "description": "A more difficult, time-cons
                                    },
                                    "resources": {
                                        "type": "array",
                                        "description": "Links to external resources
                                        "items": {
                                            "type": "object",
                                            "properties": {
                                                "type": {
                                                    "type": "string",
                                                    "enum": ["youtube", "website",
                                                    "description": "The type of res
                                                },
                                                "url": {
                                                    "type": "string",
                                                    "format": "uri",
                                                    "description": "The URL of the
                                                },
                                                "description": {
                                                    "type": "string",
                                                    "description": "A brief descrip
                                                }
                                            },
                                            "required": ["type", "url"]
                                        }
                                    }
                                },
                                "required": ["easy_fix", "resources"]
                            }
                        },
                        "required": [
                            "risk_name",
                            "overview",
                            "severity_cvss_score",
                            "affected_elements",
                            "recommendations"
                        ]
                    }
                }
            },
            "required": ["vulnerabilities"]
        }
    }
)
print(risk_response.text)
```

{"vulnerabilities":[{"risk_name":"S3 Bucket Public Exposure","overview":"The S3 bucket named innovatech-prod-logs-storage, used for storing application logs and analytics data, was found to be publicly accessible due to an incorrect bucket policy setting. This exposes customer analytics records, including anonymized session IDs and geolocation data, which constitutes a breach of compliance standards.","severity_cvss_score":9.8,"affected_elements":["AWS S3 Bucket arn:aws:s3:::innovatech-prod-logs-storage"],"recommendations":{"easy_fix":"The bucket policy for innovatech-prod-logs-storage must be modified to block all public access. The policy should only allow access via specific IAM roles tied to the application services that require logging access.","resources":[{"type":"documentation","url":"https://docs.aws.amazon.com/AmazonS3/latest/userguide/configuring-block-public-access.html","description":"AWS documentation on blocking public access to S3 buckets."},{"type":"website","url":"https://aws.amazon.com/s3/features/security/","description":"Overview of S3 security features and best practices."}],"long_term_fix":"Implement S3 Block Public Access at the account level to prevent future accidental public exposures across all buckets. Regularly audit S3 bucket policies using AWS Config rules to ensure ongoing compliance."}},{"risk_name":"Unpatched Container Image and Root Privileges in EKS","overview":"Multiple container images in the product-catalog-service deployment are running with known, unpatched vulnerabilities (CVE-2024-XXXXX) and, critically, are running with root privileges within the container. A successful attack could exploit the image vulnerability to escape the container and potentially compromise the EKS worker node.","severity_cvss_score":8.5,"affected_elements":["Kubernetes Deployment product-catalog-service","Container Image prod-cat-v2.1 (running as root)"],"recommendations":{"easy_fix":"Update the product-catalog-service deployment to use a patched container image and enforce the runAsNonRoot: true setting.","resources":[{"type":"documentation","url":"https://kubernetes.io/docs/concepts/security/pod-security-standards/","description":"Kubernetes Pod Security Standards documentation on security best practices."},{"type":"youtube","url":"https://www.youtube.com/watch?v=Xz2Cg1jW4iI","description":"Video explaining container security best practices, including running as non-root."}],"long_term_fix":"Implement a robust container image scanning and vulnerability management process within the CI/CD pipeline. Use policy engines like OPA Gatekeeper or Kyverno to enforce Pod Security Standards across the EKS cluster, ensuring containers always run as non-root and from approved, patched images."}},{"risk_name":"Over-privileged IAM User for CI/CD","overview":"A development-focused IAM user, dev_deployer, used by a CI/CD pipeline script, has been granted the AdministratorAccess policy instead of a more restrictive custom policy. If the GitHub repository or the CI/CD pipeline is compromised, the attacker would gain full administrative control over the entire AWS environment, violating the Principle of Least Privilege.","severity_cvss_score":8.9,"affected_elements":["AWS IAM User arn:aws:iam::123456789012:user/dev_deployer"],"recommendations":{"easy_fix":"Revoke the AdministratorAccess policy from the dev_deployer IAM user immediately. Replace it with a custom, fine-grained policy that only permits the specific actions necessary for the CI/CD deployment process (e.g., only update EKS deployments, not create new S3 buckets).","resources":[{"type":"documentation","url":"https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege","description":"AWS IAM best practices, focusing on the principle of least privilege."},{"type":"youtube","url":"https://www.youtube.com/watch?v=Q-1d0-D7r5E","description":"Video tutorial on creating custom IAM policies for least privilege in AWS."}],"long_term_fix":"Transition away from using long-lived IAM user credentials in CI/CD pipelines. Implement AWS IAM Roles for Service Accounts (IRSA) for Kubernetes workloads or use AWS IAM Identity Center for centralized identity management, coupled with regular IAM access reviews and automated policy validation."}}]}

Summary:

The Pro model was able to generate correct links to recommended fixes. However, the Flash model did not generate a correct YouTube video link on how to secure s3 buckets on AWS.