Gemini Prompt Engineering Notes

Prompt engineering helps improve the quality, relevance, and consistency of AI outputs. To increase the likelihood of the Gemini API to generate a similar report to the one our sponsor provided, we will be testing structured, specific prompts to control the model's randomness and prevent having to expend resources to train a model.

Gemini API Structure:

- User Inputs: Multimodal, allows prompts to include text, images, video, and audio
- System Instructions: Guide the model's behavior and provide context for the entire user interaction. We will definetly specify the output format to ensure it is saved into the database correctly.
  - Plan to test: Persona/role, output style/tone
- Configuration Parameters: Control content generation and fine-tune the model's reponse.

Data From Sponsor

Questionnaire / Organization Profile Example

Org Name	Email Domain	Website Domain	External IP	Do you require MFA to access email?	Do you require MFA to log into computers?	Do you require MFA to access sensitive data systems?
Valier School District	valier.k12.mt.us	www.valier.k12.mt.us	216.220.16.170	Yes	Yes	Yes

DNS DIG on Email Domain

```
id 49113
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
valier.k12.mt.us. IN ANY
;ANSWER
```

```
valier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-request.umt.edu.
2024030501 21600 900 1209600 86400
valier.k12.mt.us. 3600 IN NS ens-o1.umt.edu.
valier.k12.mt.us. 3600 IN NS cudess2.umt.edu.
valier.k12.mt.us. 3600 IN NS cudess1.umt.edu.
valier.k12.mt.us. 3600 IN A 216.239.38.21
valier.k12.mt.us. 3600 IN A 216.239.32.21
valier.k12.mt.us. 3600 IN A 216.239.34.21
valier.k12.mt.us. 3600 IN A 216.239.36.21
valier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.
valier.k12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.
valier.k12.mt.us. 3600 IN MX 10 aspmx3.googlemail.com.
valier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.
valier.k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.
valier.k12.mt.us. 3600 IN TXT "v=spf1 include:_spf.google.com
include:mg.infinitecampus.org -all"
;AUTHORITY
;ADDITIONAL
```

DNS DIG on Email DMARC Domain

```
id 45565
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
_dmarc.valier.k12.mt.us. IN ANY
;ANSWER
_dmarc.valier.k12.mt.us. 3600 IN TXT "v=DMARC1; p=reject;
rua=mailto:dmarc@valier.k12.mt.us"
;AUTHORITY
;ADDITIONAL
```

Port Scan on Web

```
-------------------------------------------------
Scanning Target: 216.239.32.21
Scanning started at:2025-07-18 22:09:34.408091
-------------------------------------------------
Port 80 is open
Port 443 is open
```

Port Scan on External IP

```
-------------------------------------------------
Scanning Target: 216.220.16.170
Scanning started at:2025-07-18 22:12:17.055226
```

```
------------------------------------------------
no ports open
```

Sample Prompt from Sponsor

Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the answers to the security questionnaire, write a report on the cybersecurity readiness of the organization.

Example Report from Sponsor, Generated from ChatGPT

Cybersecurity Readiness Report for Valier School District

Date: July 18, 2025

1. Overview

This report evaluates the cybersecurity posture of Valier School District based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings reflect a strong commitment to foundational cybersecurity practices across user access, email protection, network exposure, and staff awareness.

2. Organizational Information

- **Organization Name:** Valier School District
- **Email Domain:** valier.k12.mt.us
- **Website Domain:** www.valier.k12.mt.us
- **External IP (Firewall):** 216.220.16.170
- **Website Hosting IPs:** 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21
- **DNS Hosting:** Managed by University of Montana (umt.edu nameservers)

3. Security Questionnaire Review

Security Control	Status
MFA for Email	Yes
MFA for Computer Login	Yes
MFA for Sensitive Systems	Yes
Acceptable Use Policy	Yes
New Employee Security Awareness Training	Yes
Annual All-Employee Security Training	Yes

Summary: The district reports complete implementation of basic cyber hygiene practices, especially user authentication (Multi-Factor Authentication) and routine training. This indicates a proactive and policy-driven approach to risk mitigation.

4. DNS & Email Security

DNS Records

- DNS is managed by the University of Montana (cudess1.umt.edu, cudess2.umt.edu), suggesting centralized and professionally administered DNS.
- A records point to IPs within Google's network (likely Google Sites hosting for web content). **MX Records (Email)**
- The district uses Google Workspace (Gmail) for email, as shown by multiple aspmx.l.google.com MX records.
- SPF record is correctly configured: v=spf1 include:_spf.google.com include:mg.infinitecampus.org -all
    - This helps mitigate spoofing by defining authorized mail senders. **DMARC Record**
- A valid DMARC record exists with a **reject** policy: v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us
    - This instructs receiving servers to reject unauthenticated mail, providing strong protection against phishing. **Conclusion:** DNS and email protections (SPF, DMARC, and hosting security) are configured correctly and follow best practices.

5. Port Scanning Results

Website Hosting (Google IP: 216.239.32.21)

- **Port 80 (HTTP):** Open
- **Port 443 (HTTPS):** Open These are expected for a publicly accessible website and are typical for Google-hosted services.

Firewall / External IP (216.220.16.170)

- **All scanned ports are closed** This is a strong sign of network perimeter hardening and good firewall configuration. No externally exposed services were found on the organization's primary IP.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	Strong	MFA is required across key systems
Email Security	Strong	SPF and DMARC with "reject" policy in place
Network Exposure	Secure	No exposed services on the external firewall IP
Web Hosting	Secure	Google-hosted; limited attack surface
Policy & Training	Comprehensive	Acceptable use policies and regular training in place

7. Recommendations Although the cybersecurity readiness is solid, continuous improvement is essential. We recommend the following:

1. **Verify DKIM**: While SPF and DMARC are configured, ensure **DKIM** is also active for all sending domains.
2. **Vulnerability Scanning**: Consider regular internal and external vulnerability assessments of network devices and servers.
3. **Incident Response Plan**: Document and regularly test a cybersecurity incident reponse and disaster recovery plan.
4. **Asset Inventory**: Maintain a regularly updated inventory of hardware/software assets and monitor for unauthorized changes.
5. **Third-party Risk**: Evaluate vendors (e.g., Infinite Campus) for their security psture, especially since they're included in SPF.

8. Conclusion

Valier School District demonstrates a strong cybersecurity foundation, particularly in authentication, email protection, staff training, and perimeter security. Continued vigilance and regular audits will help maintain and improve this strong security posture.

Prepared by:

Cybersecurity Assessment Team

Date: July 18, 2025

Testing Gemini API

Gemini Models

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]:
```
import json
import re
import markdown

def generate_html_from_markdown(text_content):
    """
    Extracts Markdown content and converts it into a full, styled HTML string.
    This function contains all the text processing logic.
```

```
    Args:
        text_content (str): The raw text content.

    Returns:
        str or None: The complete HTML string, or None if extraction fails.
    """
    markdown_content = text_content

    # 1. Content Extraction Logic
    try:
        # Check for code-fenced JSON structure first
        json_match = re.search(r'```json\s*(.*?)\s*```', text_content, re.DOTALL)
        if json_match:
            json_string = json_match.group(1).strip()
            try:
                data = json.loads(json_string)
                markdown_content = data.get("text", "")
            except json.JSONDecodeError:
                print("Warning: JSON inside the code block is not valid. Treating e
                markdown_content = text_content
        else:
            # Try to load the entire content as plain JSON
            try:
                data = json.loads(text_content)
                markdown_content = data.get("text", "")
            except json.JSONDecodeError:
                # If neither works, treat the entire input as Markdown text
                markdown_content = text_content

        if not isinstance(markdown_content, str):
            print(f"Error: Markdown content is not a string, it's a {type(markdown_
            return None

        # 2. Markdown to HTML Conversion
        html_output = markdown.markdown(markdown_content, extensions=['tables', 'fe

        # 3. Full HTML Structure with CSS for PDF Styling (WeasyPrint needs this st
        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>Markdown Export</title>
    <style>
        @page {{
            size: A4;
            margin: 1in;
            @top-center {{ content: element(header); }}
        }}
        body {{
            font-family: 'Noto Sans', sans-serif;
            line-height: 1.6;
            color: #333;
        }}
        h1, h2, h3, h4, h5, h6 {{ color: #1a1a1a; margin-top: 1.5em; }}
```

```
        pre {{
            background-color: #f4f4f4;
            padding: 1rem;
            border-radius: 4px;
            overflow-x: auto;
            border: 1px solid #ddd;
            font-family: monospace;
        }}
        code {{ font-family: monospace; }}
        blockquote {{
            border-left: 5px solid #007bff;
            padding-left: 1.5rem;
            color: #555;
            margin: 1rem 0;
        }}
        table {{
            border-collapse: collapse;
            width: 100%;
            margin: 1.5rem 0;
        }}
        th, td {{
            border: 1px solid #ddd;
            padding: 10px;
            text-align: left;
        }}
        th {{
            background-color: #e9ecef;
            font-weight: bold;
        }}
        img {{ max-width: 100%; height: auto; }}
    </style>
</head>
<body>
{html_output}
</body>
</html>
"""
        return full_html

    except Exception as e:
        print(f"An unexpected error occurred during content generation: {e}")
        return None
```

In [3]:

```
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 [4]:
```
proModel = genai.GenerativeModel('gemini-2.5-pro')
flashModel = genai.GenerativeModel('gemini-2.5-flash')
flashLiteModel = genai.GenerativeModel('gemini-2.5-flash-lite')
```

In [ ]:
```
import json

prompt_text = 'Prompt:\nGiven this DNS DIG, Port scan of the website, Port scan of

context1_text = 'Context:\n'
context2_text = 'Context:\n'

example_text = 'Example:\n' + prompt_text

filepaths = ["report_template/test_questionnaire.json", "report_template/test_port_
sample1_filepaths = ["report_sample1/sample1_questionnaire.json", "report_sample1/s
sample2_filepaths = ["report_sample2/sample2_questionnaire.json", "report_sample2/s

for file in filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            example_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("=======  Example ==========")
print(example_text)
print("============================")

for file in sample1_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context1_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 1 =========")
```

```
print(prompt_text)
print(context1_text)
print("============================")

for file in sample2_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context2_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 2 =========")
print(prompt_text)
print(context2_text)
print("============================")
```

======= Example ==========
Example:
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization.template/test_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Valier School District",
    "Email Domain": "valier.k12.mt.us",
    "Website Domain": "www.valier.k12.mt.us",
    "External IP": "216.220.16.170",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
--
template/test_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
220.16.170\nScanning started at:2025-07-18 22:12:17.055226\n-----------------------
--------------------------\nno ports open\n"
}
--
template/test_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
239.32.21\nScanning started at:2025-07-18 22:09:34.408091\n-------------------------
------------------------\nPort 80 is open\nPort 443 is open\n"
}
--
template/test_dns_dig_email.json:
{
  "text": "id 49113\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\nvalier.
k12.mt.us. IN ANY\n;ANSWER\nvalier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-reque
st.umt.edu. 2024030501 21600 900 1209600 86400\nvalier.k12.mt.us. 3600 IN NS ens-o1.
umt.edu.\nvalier.k12.mt.us. 3600 IN NS cudess2.umt.edu.\nvalier.k12.mt.us. 3600 IN N
S cudess1.umt.edu.\nvalier.k12.mt.us. 3600 IN A 216.239.38.21\nvalier.k12.mt.us. 360
0 IN A 216.239.32.21\nvalier.k12.mt.us. 3600 IN A 216.239.34.21\nvalier.k12.mt.us. 3
600 IN A 216.239.36.21\nvalier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.\nvalier.k
12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 10 aspm
x3.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.\nvalier.
k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.\nvalier.k12.mt.us. 3600 IN TXT \"v=
spf1 include:_spf.google.com include:mg.infinitecampus.org -all\"\n;AUTHORITY\n;ADDI
TIONAL\n"
}
--
template/test_dns_dig_email_dmarc.json:
{
  "text": "id 45565\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
```

valier.k12.mt.us. IN ANY\n;ANSWER\n_dmarc.valier.k12.mt.us. 3600 IN TXT \"v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us\"\n;AUTHORITY\n;ADDITIONAL\n"
}
--
template/test_sample_report.json:

{
  "text": "**Cybersecurity Readiness Report for Valier School District**\n\n**Date:** July 18, 2025\n\n**1. Overview**\n\nThis report evaluates the cybersecurity posture of Valier School District based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings reflect a strong commitment to foundational cybersecurity practices across user access, email protection, network exposure, and staff awareness.\n\n**2. Organizational Information**\n- **Organization Name:** Valier School District\n- **Email Domain:** valier.k12.mt.us\n- **Website Domain:** www.valier.k12.mt.us\n- **External IP (Firewall):** 216.220.16.170\n- **Website Hosting IPs:** 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21\n- **DNS Hosting:** Managed by University of Montana (umt.edu nameservers)\n\n**3. Security Questionnaire Review**\n| Security Control | Status |\n| :--------------: | :-----: |\n| MFA for Email | Yes |\n| MFA for Computer Login | Yes |\n| MFA for Sensitive Systems | Yes |\n| Acceptable Use Policy | Yes |\n| New Employee Security Awareness Training | Yes |\n| Annual All-Employee Security Training | Yes |\n\n**Summary:** The district reports complete implementation of basic cyber hygiene practices, especially user authentication (Multi-Factor Authentication) and routine training. This indicates a proactive and policy-driven approach to risk mitigation.\n\n**4. DNS & Email Security**\n\n**DNS Records**\n- DNS is managed by the University of Montana (cudess1.umt.edu, cudess2.umt.edu), suggesting centralized and professionally administered DNS.\n- A records point to IPs within Google's network (likely Google Sites hosting for web content).\n**MX Records (Email)**\n- The district uses Google Workspace (Gmail) for email, as shown by multiple aspmx.l.google.com MX records.\n- SPF record is correctly configured: v=spf1 include:_spf.google.com include:mg.infinitecampus.org -all\n\t- This helps mitigate spoofing by defining authorized mail senders./n**DMARC Record**/n- A valid DMARC record exists with a **reject** policy: v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us\n\t- This instructs receiving servers to reject unauthenticated mail, providing strong protection against phishing./n**Conclusion:** DNS and email protections (SPF, DMARC, and hosting security) are configured correctly and follow best practices.\n\n**5. Port Scanning Results**\n\n**Website Hosting (Google IP: 216.239.32.21)**\n- **Port 80 (HTTP):** Open\n- **Port 443 (HTTPS):** Open\nThese are expected for a publicly accessible website and are typical for Google-hosted services.\n\n**Firewall / External IP (216.220.16.170)**\n- **All scanned ports are closed**\nThis is a strong sign of network perimeter hardening and good firewall configuration. No externally exposed services were found on the organization's primary IP.\n\n**6. Risk Assessment & Readiness Summary**\n| Category | Status | Notes |\n| :------: | :----: | :---: |\n| Authentication Security | Strong | MFA is required across key systems |\n| Email Security | Strong | SPF and DMARC with \"reject\" policy in place |\n| Network Exposure | Secure | No exposed services on the external firewall IP |\n| Web Hosting | Secure | Google-hosted; limited attack surface |\n| Policy & Training | Comprehensive | Acceptable use policies and regular training in place |\n\n**7. Recommendations**\nAlthough the cybersecurity readiness is solid, continuous improvement is essential. We recommend the following:\n1. **Verify DKIM**: While SPF and DMARC are configured, ensure **DKIM** is also active for all sending domains.\n2. **Vulnerability Scanning**: Consider regular internal and external vulnerability assessments of network devices and servers.\n3. **Incident Response Plan**: Document and regularly test a cybersecurity incident reponse and disaster recovery plan.\n4. **Asset Inventory**: Maintain a regularly updated inventory of hardware/software assets and monitor for unauthorized changes.\n5. **Third-party Risk**: Evaluate vendors (e.g., Infinite Campus) for their security psture, especially since they're included in SPF.\n\n**8. Conclusion**\n\nValier School District demonstrates

a strong cybersecurity foundation, particularly in authentication, email protection, staff training, and perimeter security. Continued vigilance and regular audits will help maintain and improve this strong security posture.\n\n**Prepared by:**\n\nCyber security Assessment Team\n\n**Date:** July 18, 2025"
}
--

==========
======== Sample 1 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the answers to the security questionnaire, write a report on the cybersecurity readiness of the organization.
Context:
sample1/sample1_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Apex Innovations",
    "Email Domain": "apexinnovations.com",
    "Website Domain": "www.apexinnovations.com",
    "External IP": "72.21.196.160",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Yes",
    "Does your organization do security awareness training for all employees at least once per year?": "Yes"
  }
}
```

--
sample1/sample1_dns_dig_email_dmarc.json:

```
{
  "text": "id 31890\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.apexinnovations.com. IN ANY\n;ANSWER\n_dmarc.apexinnovations.com. 3600 IN TXT \"v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\""
}
```

--
sample1/sample1_dns_dig_email.json:

```
{
  "text": "id 52417\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\napexinnovations.com. IN ANY\n;ANSWER\napexinnovations.com. 3600 IN SOA ns1.apexinnovations.com. hostmaster.apexinnovations.com. 2025101401 21600 3600 604800 3600\napexinnovations.com. 3600 IN NS ns1.apexinnovations.com.\napexinnovations.com. 3600 IN NS ns2.apexinnovations.com.\napexinnovations.com. 3600 IN A 72.21.196.160\napexinnovations.com. 3600 IN MX 10 mx1.apexinnovations.com.\napexinnovations.com. 3600 IN MX 20 mx2.apexinnovations.com.\napexinnovations.com. 3600 IN TXT \"v=spf1 include:spf.protection.outlook.com -all\""
}
```

--
sample1/sample1_port_scan_external_ip.json:

```
{
  "text": "-------------------------------------------------\nScanning Target: 72.21.196.160\nScanning started at: 2025-10-14 14:09:42.589112\n-------------------------\nPort 80 is open\nPort 443 is open"
```

```
}
--
sample1/sample1_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:08:15.223456\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--
```


```
============================
======== Sample 2 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization.
Context:
sample2/sample2_questionnaire.json:
```


```
{
  "text": {
    "Organization Name": "G.A.S. Inc.",
    "Email Domain": "gasinc.net",
    "Website Domain": "www.gasinc.net",
    "External IP": "104.28.1.189",
    "Do you require MFA to access email?": "No",
    "Do you require MFA to log into computers?": "No",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "No",
    "Does your organization do security awareness training for new employees?": "N
o",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "No"
  }
}
--
sample2/sample2_dns_dig_email_dmarc.json:
{
  "text": "id 28911\nopcode QUERY\nrcode NXDOMAIN\nflags QR AA RD RA\n;QUESTION\n_dm
arc.gasinc.net. IN ANY\n;AUTHORITY\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmas
ter.gasinc.net. 2025101402 14400 3600 604800 3600\n;ADDITIONAL"
}
--
sample2/sample2_dns_dig_email.json:
{
  "text": "id 47123\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\ngasinc.
net. IN ANY\n;ANSWER\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmaster.gasinc.ne
t. 2025101402 14400 3600 604800 3600\ngasinc.net. 3600 IN NS dns1.gasinc.net.\ngasin
c.net. 3600 IN NS dns2.gasinc.net.\ngasinc.net. 3600 IN A 104.28.1.189\ngasinc.net.
3600 IN MX 10 mx.mailhostbox.com.\ngasinc.net. 3600 IN MX 20 mx2.mailhostbox.com.\ng
asinc.net. 3600 IN TXT \"v=spf1 include:spf.mailhostbox.com ~all\""
}
--
sample2/sample2_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:16:11.890123\n-------------------------
```

```
------------------------\nPort 21 is open\nPort 22 is open\nPort 25 is open\nPort 8
0 is open\nPort 110 is open\nPort 443 is open\nPort 3389 is open"
}
--
sample2/sample2_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:15:30.456789\n-----------------------
------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
```

In [6]:
```python
# === SAMPLE 1 ===

# input markdown-formatted text, output markdown
response = proModel.generate_content(contents=[prompt_text, context1_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations

Date: October 14, 2025

1. Overview

This report provides a cybersecurity readiness assessment for Apex Innovations. The evaluation is based on a review of the organization's self-reported security practices via a questionnaire, combined with technical analysis of its public-facing DNS records and network port scans. The findings indicate a strong commitment to user authentication and email security, with some areas for improvement in network perimeter hardening.

2. Organizational Information
- **Organization Name:** Apex Innovations
- **Email Domain:** apexinnovations.com
- **Website Domain:** www.apexinnovations.com
- **External IP / Web Server:** 72.21.196.160

3. Security Questionnaire Review

Security Control	Status
MFA for Email	Yes
MFA for Computer Login	Yes
MFA for Sensitive Systems	Yes
Acceptable Use Policy	Yes
New Employee Security Awareness Training	Yes
Annual All-Employee Security Training	Yes

Summary: Apex Innovations reports a comprehensive implementation of crucial cybersecurity policies. The mandatory use of Multi-Factor Authentication (MFA) across all key access points significantly reduces the risk of credential-based attacks. The presence of an acceptable use policy and regular security awareness training demonstrates a mature approach to managing human-related security risks.

4. DNS & Email Security

MX Records (Email)
- Email is handled by `mx1.apexinnovations.com` and `mx2.apexinnovations.com`.
- The SPF record indicates the use of Microsoft's email infrastructure (`include:spf.protection.outlook.com`).

SPF Record
- The SPF record is correctly configured with a hard fail policy: `"v=spf1 include:spf.protection.outlook.com -all"`
- This policy strictly defines authorized sending servers and helps prevent unauthorized email spoofing from the apexinnovations.com domain.

DMARC Record
- A strong DMARC record is in place with a **reject** policy: `"v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1"`
- This instructs receiving email servers to reject any messages that fail SPF or DKIM authentication, providing robust protection against phishing and domain impersonation attacks.

Conclusion: The organization's email security configuration is excellent and adh
eres to modern best practices. The combination of SPF (hard fail) and DMARC (reject)
provides a high level of defense against email-based threats.

5. Port Scanning Results

External IP / Web Server (72.21.196.160)
- **Port 80 (HTTP):** Open
- **Port 443 (HTTPS):** Open

The scan of the organization's primary external IP reveals open ports for web traffi
c. This is expected for a public-facing website. However, it indicates that the web
server is directly exposed on the same IP as the primary network egress point. This
configuration concentrates risk on this single asset, making its security and mainte
nance critical.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	Strong	Comprehensive MFA implementation is in place.
Email Security	Strong	SPF and DMARC with a "reject" policy provide excellent p
rotection.
Network Exposure	Moderate	The web server is exposed on the primary external I
P, increasing the attack surface.
Policy & Training	Strong	Policies and regular training programs are establishe
d.

7. Recommendations

While Apex Innovations has a solid security foundation, the following actions are re
commended for continuous improvement:

1. **Harden Web Server:** Since the web server at `72.21.196.160` is a primary poin
t of exposure, it is crucial to ensure it is aggressively hardened. This includes ti
mely patching, secure configuration, and implementation of a Web Application Firewal
l (WAF).
2. **Verify DKIM:** While SPF and DMARC are properly configured, ensure that Domain
Keys Identified Mail (DKIM) is also enabled and aligned for all outgoing email. This
completes the trifecta of modern email authentication.
3. **Implement Vulnerability Scanning:** Conduct regular, automated vulnerability s
cans against the external IP (`72.21.196.160`) to proactively identify and remediate
potential security flaws in the web server and its applications.
4. **Develop an Incident Response Plan:** Ensure a formal, documented Incident Resp
onse (IR) plan is in place. This plan should be tested regularly through tabletop ex
ercises to ensure a swift and effective response to any potential security breach.
5. **Review Network Segmentation:** Consider placing the public-facing web server i
n a segregated network zone (DMZ) to prevent a potential compromise from impacting t
he internal corporate network.

8. Conclusion

Apex Innovations demonstrates a strong and mature cybersecurity posture in the criti
cal areas of user authentication, email security, and employee training. Their polic
ies effectively mitigate common and high-impact risks like phishing and account take
overs. The primary area for improvement lies in managing the network perimeter, spec

ifically by hardening the exposed web server and considering greater network segment ation to minimize the potential impact of a compromise. By addressing the recommenda tions in this report, Apex Innovations can further enhance its already robust securi ty defenses.

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample1_markdown_markdown.html")
```

✅ Successfully exported HTML: pro_sample1_markdown_markdown.html

In [8]:
```
response = flashModel.generate_content(contents=[prompt_text, context1_text + "\n"
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations

Date: October 14, 2025

1. Overview

This report assesses the cybersecurity posture of Apex Innovations based on DNS reco
rds, email security configurations (SPF, DMARC), external port scans, and responses
to a security questionnaire. The organization demonstrates a strong foundation in se
veral key areas, particularly in user authentication, email security, and employee a
wareness. Network exposure appears well-managed, with only essential web services op
enly accessible.

2. Organizational Information
-   **Organization Name:** Apex Innovations
-   **Email Domain:** apexinnovations.com
-   **Website Domain:** www.apexinnovations.com
-   **External IP:** 72.21.196.160
-   **DNS Hosting:** Self-managed or hosted by a provider using Apex Innovations' na
meservers (ns1.apexinnovations.com, ns2.apexinnovations.com).
-   **Email Service:** Microsoft 365 / Outlook.com (based on SPF record).

3. Security Questionnaire Review

Security Control	Status
MFA for Email	Yes
MFA for Computer Login	Yes
MFA for Sensitive Systems	Yes
Employee Acceptable Use Policy	Yes
New Employee Security Awareness Training	Yes
Annual All-Employee Security Training	Yes

Summary: Apex Innovations reports comprehensive implementation of foundational c
ybersecurity practices. The widespread use of Multi-Factor Authentication (MFA) acro
ss critical systems significantly enhances protection against unauthorized access. F
urthermore, the existence of an acceptable use policy and consistent security awaren
ess training for all employees indicates a proactive and policy-driven approach to h
uman-centric security risks.

4. DNS & Email Security

DNS Records
-   **Nameservers (NS):** ns1.apexinnovations.com, ns2.apexinnovations.com. This sug
gests Apex Innovations either manages their own DNS infrastructure or uses a private
label DNS hosting service.
-   **A Record:** apexinnovations.com resolves to 72.21.196.160, which is the organi
zation's external IP address.
-   **MX Records:** mx1.apexinnovations.com, mx2.apexinnovations.com. While these po
int to the organization's own domain, the SPF record provides further clarity on the
actual email service.

SPF Record (Sender Policy Framework)
-   The SPF record is correctly configured: `"v=spf1 include:spf.protection.outlook.
com -all"`
    -   This indicates that Apex Innovations uses Microsoft 365 or Outlook.com for s

ending emails.
    -   The `-all` mechanism specifies that only the listed servers (Microsoft's) ar
e authorized to send email on behalf of apexinnovations.com. Any email originating f
rom other servers will be hard-failed, providing strong protection against email spo
ofing.

DMARC Record (Domain-based Message Authentication, Reporting, & Conformance)
-   A valid DMARC record exists with a strong policy: `"v=DMARC1; p=reject; rua=mail
to:dmarc_reports@apexinnovations.com; fo=1"`
    -   The `p=reject` policy is excellent, instructing receiving mail servers to re
ject messages that fail DMARC authentication (i.e., not aligned with SPF or DKIM). T
his provides the highest level of protection against phishing, spoofing, and busines
s email compromise (BEC) attacks.
    -   The `rua` tag is configured to receive aggregate reports, which are crucial
for monitoring email authentication status and identifying potential abuse.

Conclusion: DNS and email security configurations (SPF and DMARC with a "reject"
policy) are well-implemented and follow best practices, offering robust protection a
gainst email-based threats.

5. Port Scanning Results

The external IP address `72.21.196.160` (which hosts the website and is identified a
s the external IP/firewall) was scanned.

-   **Port 80 (HTTP):** Open
-   **Port 443 (HTTPS):** Open

Summary: Only standard web ports (HTTP and HTTPS) are open on the external-facin
g IP address. This is expected for a publicly accessible website. The absence of oth
er open ports indicates a strong network perimeter, suggesting that the firewall is
effectively blocking access to internal services. This minimal exposure reduces the
overall attack surface significantly.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
--:
Authentication Security	Strong	MFA is required across email, computer logi
ns, and sensitive data systems.
Email Security	Strong	SPF and DMARC with a "reject" policy are correctly i
mplemented.
Network Exposure	Secure	Only ports 80/443 (for web services) are open on t
he external IP.
Web Presence Security	Fair	Minimal exposure but the web application itself
needs continuous security validation.
Policy & Training	Strong	Acceptable use policy and regular security awaren
ess training are in place.

7. Recommendations

While Apex Innovations demonstrates a strong cybersecurity posture, continuous impro
vement is vital. We recommend the following:

1. **Verify DKIM Implementation:** While SPF and DMARC are robust, ensure DomainKey

s Identified Mail (DKIM) is also properly configured and actively signing outgoing e
mails from Microsoft 365. This provides an additional layer of email authentication.
2. **Regular Web Application Security Assessments:** As ports 80 and 443 are open f
or the website, conduct periodic vulnerability scanning and penetration testing spec
ifically targeting the web application itself. This will help identify and mitigate
potential application-layer vulnerabilities.
3. **Develop/Test Incident Response Plan:** Ensure a comprehensive Incident Respons
e Plan is documented, regularly reviewed, and tested through tabletop exercises to p
repare for potential security incidents.
4. **Continuous Firewall Rule Review:** Periodically audit firewall rules and confi
gurations to ensure that only absolutely necessary ports are open and that all rules
are optimally configured and strictly enforced.
5. **Consider a Web Application Firewall (WAF):** Implementing a WAF can provide an
additional layer of protection for the publicly exposed web services (ports 80/443)
by filtering and monitoring HTTP traffic, helping to block common web attacks.

8. Conclusion

Apex Innovations has established a commendable cybersecurity readiness posture, espe
cially in user authentication, email protection, and employee security awareness. Th
e limited external network exposure further strengthens its defense. By addressing t
he recommendations for continuous monitoring and advanced application security, Apex
Innovations can further enhance its resilience against evolving cyber threats.

Prepared by:

Cybersecurity Assessment Team

Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample1_markdown_markdown.html")
```

✅ Successfully exported HTML: flash_sample1_markdown_markdown.html

In [10]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context1_text + "
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations

Date: October 14, 2025

1. Overview

This report assesses the cybersecurity readiness of Apex Innovations based on provid
ed DNS DIG records, port scan results for the website and firewall, and responses to
a security questionnaire. The findings indicate a generally sound cybersecurity post
ure with strong foundational controls, particularly in user authentication and email
security.

2. Organizational Information

*   **Organization Name:** Apex Innovations
*   **Email Domain:** apexinnovations.com
*   **Website Domain:** www.apexinnovations.com
*   **External IP (Firewall):** 72.21.196.160
*   **Website Hosting IP:** 72.21.196.160
*   **DNS Hosting:** Managed by Apex Innovations' own nameservers (ns1.apexinnovatio
ns.com, ns2.apexinnovations.com)

3. Security Questionnaire Review

Security Control	Status
MFA for Email	Yes
MFA for Computer Login	Yes
MFA for Sensitive Data Systems	Yes
Acceptable Use Policy	Yes
New Employee Security Awareness Training	Yes
Annual All-Employee Security Training	Yes

Summary: Apex Innovations reports a robust implementation of key security polici
es and practices. The mandatory use of Multi-Factor Authentication (MFA) across all
critical access points significantly strengthens their defense against unauthorized
access. The presence of an Acceptable Use Policy and comprehensive security awarenes
s training for all employees further demonstrates a proactive approach to managing h
uman-related security risks.

4. DNS & Email Security

DNS Records:
*   The DNS records for `apexinnovations.com` indicate that the organization manages
its own nameservers, `ns1.apexinnovations.com` and `ns2.apexinnovations.com`.
*   The A record for `apexinnovations.com` resolves to the external IP address `72.2
1.196.160`, which is also identified as the firewall's external IP. This suggests th
e website might be hosted on or behind this directly accessible IP.
*   MX records point to `mx1.apexinnovations.com` and `mx2.apexinnovations.com`, ind
icating that Apex Innovations handles its own email infrastructure or uses a service
that is configured under these hostnames.
*   The SPF record is configured as `v=spf1 include:spf.protection.outlook.com -all
`. This correctly leverages Microsoft 365 (Outlook.com protection) for email authent
ication, a strong practice for preventing email spoofing.

DMARC Record:

*   The DMARC record for `_dmarc.apexinnovations.com` is configured with a `p=reject` policy and a report-to address: `v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1`.
*   This is an excellent configuration. The `reject` policy instructs receiving mail servers to reject any emails claiming to be from `apexinnovations.com` that do not pass SPF or DKIM checks, providing strong protection against phishing and email spoofing. The `fo=1` tag indicates that failure reporting should occur if any authentication check (SPF or DKIM) fails.

Conclusion: Apex Innovations has implemented strong email security measures with a correctly configured SPF record pointing to Microsoft 365 and a strict DMARC `reject` policy. This indicates a high level of readiness to combat email-based threats.

5. Port Scanning Results

Website Hosting (IP: 72.21.196.160)
*   **Port 80 (HTTP):** Open
*   **Port 443 (HTTPS):** Open
These are standard ports for a publicly accessible website. The presence of both indicates that the website is likely served over HTTP and HTTPS.

Firewall / External IP (IP: 72.21.196.160)
*   **Port 80 is open**
*   **Port 443 is open**
The port scan of the external IP (which is the same as the website hosting IP) shows that ports 80 and 443 are open. This implies that the firewall is configured to allow traffic to these ports, likely for the web server. It is important to note that no other ports were reported as open.

Conclusion: The external network perimeter appears to be minimally exposed, with only essential ports for web services (HTTP/HTTPS) accessible. This suggests a well-configured firewall that limits the attack surface.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	Strong	MFA mandated for email, computers, and sensitive data systems.
Email Security	Strong	SPF configured for Microsoft 365; DMARC with `reject` policy implemented.
Network Exposure	Secure	Only standard web ports (80, 443) exposed on the external IP.
Web Hosting	Moderate	Website directly accessible on the external IP. While standard ports are open, specific services running on these ports require careful configuration and patching.
Policy & Training	Strong	Acceptable Use Policy and regular security awareness training are in place for all employees.
DNS Management	Adequate	Self-managed DNS, with appropriate SPF and DMARC records.

7. Recommendations

While Apex Innovations demonstrates a commendable cybersecurity posture, the followi

ng recommendations could further enhance its readiness:

1. **Verify DKIM Implementation:** The DMARC policy recommends checking both SPF an d DKIM. Ensure that DKIM is also properly configured and enabled for `apexinnovation s.com` to align with the `fo=1` setting in the DMARC record and maximize email authe ntication strength.
2. **Web Server Hardening:** Since ports 80 and 443 are open on the external IP, en sure that the web server software is regularly patched, configured securely (e.g., d isabling unnecessary modules, implementing TLS 1.2/1.3), and that any sensitive info rmation is not directly exposed. Consider using a Web Application Firewall (WAF) for additional protection.
3. **Vulnerability Scanning:** Implement regular internal and external vulnerabilit y scanning to proactively identify and remediate potential weaknesses in network inf rastructure and web applications.
4. **Incident Response Plan:** Develop and regularly test a comprehensive cybersecu rity incident response plan to ensure a swift and effective reaction to any security breaches.
5. **Asset Management:** Maintain a detailed and up-to-date inventory of all hardwa re and software assets, including web server configurations, to facilitate better se curity management and incident response.

8. Conclusion

Apex Innovations exhibits a strong cybersecurity readiness, particularly in its impl ementation of multi-factor authentication, robust email security controls (SPF and D MARC), and comprehensive employee training programs. The limited exposure of its ext ernal network perimeter is also a positive indicator. By addressing the minor recomm endations, particularly concerning web server hardening and proactive vulnerability management, Apex Innovations can further solidify its security posture and maintain a resilient defense against evolving cyber threats.

Prepared by:

Cybersecurity Assessment Team

Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample1_markdown_markdown.html")
```

✅ Successfully exported HTML: flash_lite_sample1_markdown_markdown.html

In [12]:
```
# === SAMPLE 2 ===

# input markdown-formatted text, output markdown
response = proModel.generate_content(contents=[prompt_text, context2_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.

Date: October 14, 2025

1. Overview

This report provides an assessment of the cybersecurity readiness of G.A.S. Inc. bas ed on a security questionnaire and technical scans of the organization's public-faci ng digital assets. The evaluation reveals critical deficiencies across network secur ity, email authentication, user access controls, and security policies. The organiza tion's current posture presents a high risk of unauthorized access, data breach, and business email compromise. Immediate and comprehensive remediation efforts are stron gly advised.

2. Organizational Information
- **Organization Name:** G.A.S. Inc.
- **Email Domain:** gasinc.net
- **Website Domain:** www.gasinc.net
- **External / Website IP:** 104.28.1.189

3. Security Questionnaire Review
The self-reported questionnaire indicates a lack of fundamental cybersecurity polici es and controls.

Security Control	Status
MFA for Email	No
MFA for Computer Login	No
MFA for Sensitive Systems	Yes
Acceptable Use Policy	No
New Employee Security Awareness Training	No
Annual All-Employee Security Training	No

Summary: The absence of Multi-Factor Authentication (MFA) for email and computer access is a critical vulnerability, making user accounts highly susceptible to compr omise through phishing or password reuse. The lack of security policies and employee training creates a high-risk environment where human error is more likely to lead to a security incident.

4. DNS & Email Security

MX Records (Email)
- Email is handled by `mx.mailhostbox.com` and `mx2.mailhostbox.com`.

SPF Record
- The SPF record is: `"v=spf1 include:spf.mailhostbox.com ~all"`
- The `~all` (softfail) qualifier is a weak configuration. It allows unauthenticated emails to be delivered to the recipient's inbox, albeit potentially marked as spam, reducing protection against email spoofing.

DMARC Record
- A DNS query for the DMARC record (`_dmarc.gasinc.net`) returned `NXDOMAIN`, indica ting that **no DMARC record exists**.
- This is a critical security gap, as it leaves the `gasinc.net` domain highly vulne rable to direct domain spoofing used in sophisticated phishing and business email co mpromise attacks.

Conclusion: The organization's email security posture is weak. The combination of a softfail SPF policy and the complete absence of DMARC provides inadequate protection against impersonation and phishing attacks.

5. Port Scanning Results

Firewall / External IP (104.28.1.189)
The organization's primary external IP address, which also hosts the public website, has numerous high-risk services exposed directly to the internet.

- **Port 21 (FTP):** Open - Insecure protocol that transmits credentials in plaintext.
- **Port 22 (SSH):** Open - A primary target for automated brute-force attacks.
- **Port 25 (SMTP):** Open - Can be abused by attackers for spam relaying.
- **Port 80 (HTTP):** Open - Expected for a website.
- **Port 110 (POP3):** Open - Insecure email protocol that transmits credentials in plaintext.
- **Port 443 (HTTPS):** Open - Expected for a website.
- **Port 3389 (RDP):** Open - A major and frequent attack vector for ransomware and unauthorized remote access.

Conclusion: The network perimeter is dangerously exposed. Exposing services like RDP, SSH, and FTP directly to the internet is a severe security risk and contrary to all best practices. This configuration suggests the absence of a properly configured firewall and a high likelihood that a single compromised service could lead to a full network breach.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	Weak	Lack of MFA on email and computers creates a high risk of account takeover.
Email Security	Weak	Missing DMARC and a weak SPF record leave the organization vulnerable to spoofing.
Network Exposure	Critical	Multiple high-risk services (RDP, SSH, FTP) are exposed directly to the internet.
Policy & Training	Non-existent	No reported policies or security awareness training, leading to a high risk of human error.

7. Recommendations

Urgent action is required to address these critical vulnerabilities. We recommend the following, in order of priority:

1. **Immediate Network Remediation:**
    * **Close Exposed Ports:** Immediately close ports 21 (FTP), 22 (SSH), 110 (POP3), and especially 3389 (RDP) on your external firewall.
    * **Implement VPN:** If remote access is required for these services, it must be secured behind a Virtual Private Network (VPN) that requires MFA.

2. **Implement Multi-Factor Authentication (MFA):**
    * Immediately enable MFA for all user accounts, prioritizing email, remote access (VPN), and administrative accounts.
    * Develop a plan to roll out MFA for all computer logins.

3. **Strengthen Email Security:**
    * **Implement DMARC:** Create and publish a DMARC record, starting with a monitoring policy (`p=none`) and progressing quickly to a quarantine or reject policy (`p=reject`).
    * **Strengthen SPF:** Change the SPF record from `~all` (softfail) to `-all` (hardfail) to instruct receiving servers to reject mail from unauthorized sources.
    * **Implement DKIM:** Ensure DKIM is configured for your email provider to digitally sign outgoing messages.

4. **Develop Foundational Policies and Training:**
    * **Acceptable Use Policy (AUP):** Create and implement an AUP for all employees.
    * **Security Awareness Training:** Immediately enroll all employees in a security awareness training program, with mandatory annual refreshers.

8. Conclusion

G.A.S. Inc. currently exhibits a very low level of cybersecurity readiness. The combination of an exposed network perimeter, weak authentication controls, inadequate email security, and a lack of security policies places the organization at an extremely high risk of a significant cyberattack. The recommendations outlined in this report should be treated as urgent priorities to mitigate these immediate threats.

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample2_markdown_markdown.html")
```

✅ Successfully exported HTML: pro_sample2_markdown_markdown.html

In [15]:
```
response = flashModel.generate_content(contents=[prompt_text, context2_text + "\n"
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.

Date: October 14, 2025

1. Overview

This report assesses the cybersecurity posture of G.A.S. Inc. based on technical sca
ns (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The f
indings indicate a significantly low level of cybersecurity readiness across multipl
e critical areas, presenting substantial risks to the organization's data, systems,
and operations. Urgent action is required to address these vulnerabilities.

2. Organizational Information
- **Organization Name:** G.A.S. Inc.
- **Email Domain:** gasinc.net
- **Website Domain:** www.gasinc.net
- **External IP:** 104.28.1.189
- **DNS Hosting:** Self-managed (dns1.gasinc.net, dns2.gasinc.net)
- **Email Hosting:** Mailhostbox.com

3. Security Questionnaire Review

Security Control	Status
MFA for Email	No
MFA for Computer Login	No
MFA for Sensitive Data Systems	Yes
Acceptable Use Policy	No
New Employee Security Awareness Training	No
Annual All-Employee Security Training	No

Summary: The organization's self-assessment reveals a severe lack of fundamental
cybersecurity controls. Multi-Factor Authentication (MFA) is largely absent, being o
nly applied to sensitive data systems, leaving email and computer logins vulnerable.
Furthermore, there is no employee acceptable use policy and no security awareness tr
aining for new or existing employees. This indicates a significant gap in security c
ulture and foundational policy enforcement.

4. DNS & Email Security

DNS Records
- DNS is managed internally by G.A.S. Inc. (dns1.gasinc.net, dns2.gasinc.net). Whi
le possible, this requires robust internal management and redundancy to ensure relia
bility and security.
- The A record for gasinc.net points to 104.28.1.189, indicating that the website
is hosted on the same external IP as the primary network perimeter.

MX Records (Email)
- G.A.S. Inc. utilizes Mailhostbox.com for email services, as shown by the MX reco
rds: `mx.mailhostbox.com` and `mx2.mailhostbox.com`.
- **SPF Record:** The SPF record is configured as `v=spf1 include:spf.mailhostbox.
com ~all`.
    - The `~all` (softfail) policy indicates that unauthenticated emails from the
domain should be treated with suspicion but not necessarily rejected. While better t
han no SPF, it is not as strong as a `-all` (fail) policy in preventing spoofing.

DMARC Record
- A DMARC record for `_dmarc.gasinc.net` does not exist (NXDOMAIN).
    - **Critical Finding:** The absence of a DMARC record means there is no policy to guide receiving mail servers on how to handle emails that fail SPF or DKIM authentication. This leaves the `gasinc.net` domain highly vulnerable to email spoofing, phishing, and Business Email Compromise (BEC) attacks, as malicious actors can easily send emails purporting to be from G.A.S. Inc. without detection.

Conclusion: G.A.S. Inc.'s email security posture is critically weak due to the complete lack of a DMARC policy and a permissive SPF policy. This exposes the organization to significant email-based threats.

5. Port Scanning Results

The port scans against the external IP 104.28.1.189 (which hosts both the website and serves as the external firewall) reveal an alarmingly wide-open network perimeter.

Open Ports on External IP (104.28.1.189)
- **Port 21 (FTP):** Open - File Transfer Protocol is often insecure, transmitting credentials in plaintext, and can be exploited for unauthorized access or file manipulation.
- **Port 22 (SSH):** Open - Secure Shell access should ideally be restricted to trusted IPs or via VPN. Direct exposure to the internet is a common target for brute-force attacks.
- **Port 25 (SMTP):** Open - While email is hosted by Mailhostbox, an open SMTP port on the external IP could indicate an internal mail server, relay, or an unnecessary exposure that can be abused for spam or other attacks.
- **Port 80 (HTTP):** Open - Standard for web traffic.
- **Port 110 (POP3):** Open - Post Office Protocol version 3 is an insecure, unencrypted email retrieval protocol. Its external exposure is a severe vulnerability for credential theft. Modern email clients should use secure POP3S (Port 995) or IMAPS (Port 993).
- **Port 443 (HTTPS):** Open - Standard for secure web traffic.
- **Port 3389 (RDP):** Open - Remote Desktop Protocol is a *critical* security risk when exposed directly to the internet. RDP is a frequent target for brute-force attacks and exploitation, which can lead to full system compromise.

Conclusion: The exposure of multiple high-risk services (FTP, SSH, POP3, RDP, potentially SMTP) directly to the internet on the organization's primary external IP creates an extremely broad and vulnerable attack surface. This configuration dramatically increases the likelihood of unauthorized access, data breaches, and system compromise.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	Weak	MFA missing for email and computer logins; only present for sensitive systems.
Email Security	Poor	No DMARC record, and SPF is `~all` (softfail), leaving the domain highly susceptible to spoofing and phishing.
Network Exposure	Critical	Numerous high-risk services (FTP, SSH, POP3, RDP) directly exposed to the internet, creating a massive attack surface.
Web Hosting	Moderate	Website on same external IP as firewall, but 80/443 expec

ted. Other open ports on this IP are the concern. |
| Policy & Training | Non-Existent | No Acceptable Use Policy; no security awareness training for new or existing employees. |

7. Recommendations

Given the significant vulnerabilities identified, G.A.S. Inc. should prioritize and immediately implement the following recommendations:

1. **Implement Multi-Factor Authentication (MFA) Broadly:**
    * **Urgent:** Mandate MFA for all email accounts.
    * **Urgent:** Mandate MFA for all computer logins, especially for users with administrative privileges.
2. **Enhance Email Security:**
    * **Critical:** Implement a DMARC record for `gasinc.net`. Start with a `p=quarantine` policy and move towards `p=reject` after monitoring DMARC reports to ensure legitimate emails are not affected.
    * **Stronger SPF:** Consider changing the SPF policy from `~all` to `-all` once DMARC is stable and all legitimate email senders are accounted for.
    * **Verify DKIM:** Ensure DKIM is properly configured for Mailhostbox.com and any other services sending email on behalf of `gasinc.net`.
3. **Reduce Network Exposure (Firewall Hardening):**
    * **Critical:** Immediately close or restrict access to **Port 3389 (RDP)**. Remote access should only be allowed through a securely configured Virtual Private Network (VPN) with MFA.
    * **Critical:** Close **Port 110 (POP3)**. Use secure email retrieval protocols like IMAPS (Port 993) or POP3S (Port 995) if local client access is required, or encourage webmail via HTTPS.
    * **Urgent:** Close **Port 21 (FTP)**. Migrate to secure file transfer protocols like SFTP or FTPS, or utilize secure cloud-based file sharing solutions.
    * **Review Port 22 (SSH):** If SSH access is necessary, restrict it to known source IP addresses, disable password authentication in favor of key-based authentication, change the default port, and ensure strong logging and monitoring. Ideally, SSH access should also be behind a VPN.
    * **Review Port 25 (SMTP):** As email is handled by Mailhostbox, determine if Port 25 on the external IP is truly necessary. If not, close it. If it is for an internal server, ensure it is configured securely and only relays authorized mail.
4. **Establish and Enforce Security Policies:**
    * Develop and implement an **Employee Acceptable Use Policy (AUP)** outlining expectations for secure technology usage.
5. **Implement Security Awareness Training:**
    * Develop and deliver **mandatory security awareness training** for all new employees upon hire.
    * Conduct **annual mandatory security awareness training** for all employees, covering topics like phishing, malware, password hygiene, and data handling.
6. **Regular Vulnerability Management:**
    * Conduct regular internal and external vulnerability assessments and penetration testing to identify and remediate weaknesses proactively.
7. **Develop an Incident Response Plan:**
    * Create a documented and tested incident response plan to effectively handle security breaches, minimize damage, and ensure business continuity.

8. Conclusion

G.A.S. Inc. currently operates with critical cybersecurity deficiencies across multiple domains, including user authentication, email security, and network perimeter de

fense. The absence of basic security policies and employee training further exacerba
tes these risks. Without immediate and comprehensive action to address the identifie
d vulnerabilities, G.A.S. Inc. faces an exceptionally high risk of cyberattacks, dat
a breaches, and operational disruption. It is imperative that the organization commi
ts to improving its cybersecurity posture as an urgent priority.

Prepared by:

Cybersecurity Assessment Team

Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample2_markdown_markdown.html")
```

✅ Successfully exported HTML: flash_sample2_markdown_markdown.html

In [17]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context2_text + "
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.

Date: October 14, 2025

1. Overview

This report assesses the cybersecurity readiness of G.A.S. Inc. based on the provided DNS DIG information, port scan results for the website and firewall, and answers to a security questionnaire. The findings indicate several areas of concern and opportunities for significant improvement in the organization's security posture.

2. Organizational Information

*   **Organization Name:** G.A.S. Inc.
*   **Email Domain:** gasinc.net
*   **Website Domain:** www.gasinc.net
*   **External IP (Firewall):** 104.28.1.189
*   **Website Hosting IP:** 104.28.1.189 (also appears to be the firewall IP)

3. Security Questionnaire Review

Security Control	Status
MFA to access email?	No
MFA to log into computers?	No
MFA to access sensitive data systems?	Yes
Employee acceptable use policy?	No
Security awareness training for new employees?	No
Security awareness training for all employees (at least once per year)?	No

Summary: G.A.S. Inc. has significant gaps in fundamental security practices. The absence of Multi-Factor Authentication (MFA) for email and computer logins, coupled with a lack of an acceptable use policy and any form of security awareness training, leaves the organization highly vulnerable to common cyber threats like phishing, credential stuffing, and social engineering. While MFA is present for sensitive data systems, its absence elsewhere is a critical weakness.

4. DNS & Email Security

DNS Records (gasinc.net)

*   **SOA Record:** Indicates DNS is managed by `dns1.gasinc.net` and `dns2.gasinc.net`.
*   **A Record:** `gasinc.net` resolves to IP `104.28.1.189`. This IP appears to be both the website hosting and potentially the external firewall IP.
*   **MX Records:** The email is handled by `mx.mailhostbox.com` and `mx2.mailhostbox.com`.
*   **SPF Record:** `v=spf1 include:spf.mailhostbox.com ~all`. This is a basic SPF record, indicating that mail originating from `spf.mailhostbox.com` is authorized.

DMARC Records (_dmarc.gasinc.net)

*   **DMARC Record:** `NXDOMAIN` (Non-Existent Domain). This signifies that no DMARC record is published for `gasinc.net`.

Conclusion: The absence of a DMARC record is a significant oversight. While SPF

is present, DMARC provides crucial instructions to receiving mail servers on how to handle emails that fail SPF (and potentially DKIM, which is not evaluated here but i s also a common component). Without DMARC, the organization is more susceptible to e mail spoofing and phishing attacks targeting its domain.

5. Port Scanning Results

Website Hosting (IP: 104.28.1.189)

*   **Port 80 (HTTP):** Open
*   **Port 443 (HTTPS):** Open
    These are standard ports for web servers and are expected for a public website.

External IP / Firewall (IP: 104.28.1.189)

*   **Port 21 (FTP):** Open
*   **Port 22 (SSH):** Open
*   **Port 25 (SMTP):** Open
*   **Port 80 (HTTP):** Open
*   **Port 110 (POP3):** Open
*   **Port 443 (HTTPS):** Open
*   **Port 3389 (RDP):** Open

Conclusion: The external firewall/IP address exposes a significant number of ser vices to the internet. Open ports for FTP, SSH, SMTP, POP3, and RDP are particularly concerning. These services, if not properly secured, hardened, and monitored, can be entry points for attackers. SSH and RDP are often targeted for brute-force attacks, and unencrypted FTP and POP3 are highly insecure for transmitting sensitive informat ion.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	**Poor**	Critical lack of MFA for email and compu ter logins.
Email Security	**Fair**	SPF is present, but the absence of DMARC and DKIM (not checked) weakens protection against spoofing.
Network Exposure	**Poor**	Numerous unnecessary ports are open on t he external firewall, presenting a large attack surface.
Web Hosting	**Fair**	Standard web ports (80, 443) are open, a s expected.
Policy & Training	**Poor**	No acceptable use policy and no security awareness training for employees.
Sensitive Data Access	**Good**	MFA is required for sensitive data syste ms, which is a positive control.

7. Recommendations

G.A.S. Inc. has significant cybersecurity vulnerabilities that require immediate att
ention. The following recommendations are prioritized to improve the organization's
readiness:

1. **Implement Multi-Factor Authentication (MFA):**
    * **High Priority:** Enforce MFA for all email accounts and computer logins. T
his is the single most effective control against compromised credentials.
2. **Harden Firewall and Network Exposure:**
    * **High Priority:** Close all unnecessary open ports on the external firewall
(Ports 21, 22, 25, 110, 3389).
    * Restrict access to only essential services and use strong access controls
(e.g., VPN for SSH/RDP access, specific IP whitelisting if possible).
    * If FTP is still required, migrate to SFTP or FTPS and ensure strong authenti
cation.
    * Consider a managed firewall service if internal expertise is limited.
3. **Implement DMARC and DKIM:**
    * **High Priority:** Publish a DMARC record for `gasinc.net` with a clear poli
cy (e.g., `p=reject` or `p=quarantine`) and a reporting address.
    * Ensure DKIM is configured and active for all outgoing email.
4. **Develop and Enforce an Acceptable Use Policy (AUP):**
    * **High Priority:** Create a clear policy outlining acceptable and unacceptab
le use of company IT resources, including internet, email, and devices. Ensure emplo
yees acknowledge and adhere to it.
5. **Conduct Regular Security Awareness Training:**
    * **High Priority:** Implement a comprehensive security awareness training pro
gram for all employees, covering topics like phishing, password security, social eng
ineering, and data handling. This training should be mandatory for new hires and con
ducted annually for all staff.
6. **Review and Secure Email Services:**
    * While using `mailhostbox.com` is noted, ensure their security practices are
robust and that all email security features (like encryption options) are utilized.
7. **Regular Vulnerability Scanning and Patch Management:**
    * Implement a schedule for regular internal and external vulnerability scans t
o identify and address weaknesses.
    * Maintain a robust patch management process for all systems and applications.

8. Conclusion

G.A.S. Inc. currently exhibits a low level of cybersecurity readiness. The lack of b
asic security controls like MFA for email and logins, a proper acceptable use polic
y, and employee training creates a highly vulnerable environment. The exposed networ
k services on the external IP further exacerbate these risks. Addressing the recomme
ndations outlined above, particularly the implementation of MFA, network hardening,
and employee training, is critical to mitigating immediate threats and establishing
a more secure operational foundation. Continuous monitoring and periodic security as
sessments will be necessary to maintain an improved security posture.

Prepared by:

Cybersecurity Assessment Team

Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample2_markdown_markdown.html")
```

✅ Successfully exported HTML: flash_lite_sample2_markdown_markdown.html

In [39]:
```
# === SAMPLE 1 ===

#input markdown-formatted text, output JSON
response = proModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report provides a cybersecurity readiness assessment for Apex In
novations, based on a review of their self-reported security questionnaire, DNS and
email security configurations, and external port scans. The assessment reveals a str
ong commitment to security fundamentals, particularly in user authentication and ema
il protection. However, a potential misconfiguration in email records presents a not
able risk that requires attention.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External / Website IP: 72.21.196.160"
  ],
  "Security Questionnaire Review": [
    "MFA Implementation: The organization reports mandatory Multi-Factor Authenticat
ion (MFA) for email access, computer logins, and access to sensitive data systems. T
his significantly strengthens user account security.",
    "Security Policies: An employee acceptable use policy is in place.",
    "Awareness Training: Security awareness training is conducted for all new employ
ees and is repeated annually for all staff, indicating a solid foundation for human-
layer security."
  ],
  "DNS & Email Security": [
    "SPF Record: An SPF record exists ('v=spf1 include:spf.protection.outlook.com -a
ll'). The use of '-all' (hard fail) is a security best practice. However, this recor
d authorizes Microsoft Outlook servers, which conflicts with the organization's MX r
ecords pointing to self-hosted servers (mx1/mx2.apexinnovations.com).",
    "DMARC Record: A strong DMARC policy is implemented ('v=DMARC1; p=reject; ...').
This policy instructs receiving mail servers to reject emails that fail authenticati
on checks, providing robust protection against email spoofing and phishing.",
    "MX Records: Mail Exchange (MX) records point to 'mx1.apexinnovations.com' and
'mx2.apexinnovations.com', indicating that the organization manages its own email se
rvers or uses a third party not reflected in the SPF record."
  ],
  "Port Scanning Results": [
    "External IP Scan (72.21.196.160): The scan identified Port 80 (HTTP) and Port 4
43 (HTTPS) as open.",
    "Website Scan (72.21.196.160): The scan confirmed that Port 80 and Port 443 are
open, which is expected for a public-facing web server.",
    "Summary: The attack surface on the scanned IP address is minimal, with only sta
ndard web traffic ports exposed. This indicates effective firewall configuration."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Strong. Comprehensive MFA deployment is a critical str
ength.",
    "Email Security: Strong, but with a notable configuration risk. The 'p=reject' D
MARC policy is excellent, but the mismatch between SPF and MX records could lead to
legitimate email delivery failures and undermines the full effectiveness of the cont
rol.",
    "Network Perimeter Security: Good. The external IP exposes only necessary servic
es, minimizing the risk of network-based attacks.",
    "Policy and Training: Strong. The organization has foundational policies and a r
ecurring training program in place."
  ],
  "Recommendations": [
    "Reconcile SPF and MX Records: Urgently investigate and correct the discrepancy
```

```
between the SPF record (authorizing Microsoft) and the MX records (pointing to apexi
nnovations.com). If Microsoft 365 is the email provider, update the MX records. If e
mail is self-hosted, update the SPF record to authorize the correct sending IP addre
sses.",
    "Implement DKIM: Ensure that DomainKeys Identified Mail (DKIM) is configured and
aligned with SPF and DMARC. DKIM provides cryptographic verification of email integr
ity and is a crucial component of modern email security.",
    "Enforce HTTPS: Although Port 443 (HTTPS) is open, ensure that the web server is
configured to automatically redirect all traffic from Port 80 (HTTP) to HTTPS. This
guarantees that all user connections are encrypted.",
    "Conduct Regular Vulnerability Scanning: Implement a program of regular internal
and external vulnerability scanning to proactively identify and remediate security w
eaknesses in systems and software."
  ],
  "Conclusion": "Apex Innovations demonstrates a mature cybersecurity posture, excel
ling in user authentication controls, security training, and network perimeter defen
se. The implementation of a restrictive DMARC policy is commendable. The most critic
al finding is the conflict between the organization's SPF and MX records, which pose
s a risk to email deliverability and security. Addressing this misconfiguration shou
ld be the top priority to solidify their otherwise robust security framework."
}
```

In [41]:

```
response = flashModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report assesses the cybersecurity readiness of Apex Innovations, incorporating findings from DNS records, DMARC configuration, port scans of their external IP and website, and responses from a security questionnaire. The organization demonstrates a robust foundational security posture, particularly in user authentication, email security, and employee training. Key areas of strength include widespread Multi-Factor Authentication (MFA) and comprehensive email authentication protocols (SPF and DMARC with a 'reject' policy). The network perimeter shows expected openings for web services, indicating a need for continued vigilance on web application security.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External IP (Firewall & Website): 72.21.196.160",
    "DNS Hosting: Self-managed via ns1.apexinnovations.com and ns2.apexinnovations.com"
  ],
  "Security Questionnaire Review": [
    "MFA for Email Access: Yes",
    "MFA for Computer Login: Yes",
    "MFA for Sensitive Data Systems: Yes",
    "Employee Acceptable Use Policy: Yes",
    "New Employee Security Awareness Training: Yes",
    "Annual All-Employee Security Training: Yes",
    "Summary: Apex Innovations exhibits a strong commitment to fundamental cybersecurity practices, with robust implementation of Multi-Factor Authentication across critical access points and a proactive approach to security awareness training and policy development."
  ],
  "DNS & Email Security": [
    "DNS Records: DNS is managed by Apex Innovations' own nameservers (ns1.apexinnovations.com, ns2.apexinnovations.com). The A record for apexinnovations.com points to 72.21.196.160, which is also the external IP, indicating direct hosting or a single point of entry.",
    "MX Records (Email): MX records (mx1.apexinnovations.com, mx2.apexinnovations.com) point to internal or dedicated email infrastructure, complemented by an SPF record indicating Office 365 as an authorized sender.",
    "SPF Record: The SPF record \"v=spf1 include:spf.protection.outlook.com -all\" is correctly configured. It authorizes Microsoft Outlook (likely Office 365) to send emails on behalf of apexinnovations.com and explicitly rejects all other senders, effectively combating email spoofing.",
    "DMARC Record: A strong DMARC record \"v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\" is in place. The 'p=reject' policy instructs receiving mail servers to reject unauthenticated emails, providing robust protection against phishing and brand impersonation. The 'rua' tag ensures aggregate reports are sent for monitoring.",
    "Conclusion: DNS and email security configurations (SPF, DMARC with a reject policy) are excellent, providing strong protection against email-based threats."
  ],
  "Port Scanning Results": [
    "Website Hosting & External IP (72.21.196.160):",
    "Port 80 (HTTP): Open",
    "Port 443 (HTTPS): Open",
    "These ports are expected to be open for a publicly accessible website. Given that the external IP and website IP are identical, the web server is directly exposed
```

```
at the organization's primary network perimeter. No other unexpected ports were foun
d open on the scanned external IP, indicating a well-managed firewall configuration
with services limited to essential web traffic."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Strong (MFA is comprehensively implemented across emai
l, computer logins, and sensitive systems).",
    "Email Security: Strong (Well-configured SPF and DMARC with a 'reject' policy pr
ovide robust protection against email spoofing and phishing).",
    "Network Exposure: Moderate (While only essential web ports 80/443 are open, the
web server is directly exposed on the primary external IP, increasing the attack sur
face on this specific host).",
    "Web Hosting: Appears to be self-hosted or dedicated server hosting at the exter
nal IP, requiring Apex Innovations to manage web server security proactively.",
    "Policy & Training: Comprehensive (Acceptable use policy and regular security aw
areness training demonstrate a proactive approach to human-centric security)."
  ],
  "Recommendations": [
    "1. Implement a Web Application Firewall (WAF): Given the direct exposure of the
web server on the external IP, deploying a WAF would provide an additional layer of
defense against common web application vulnerabilities and attacks.",
    "2. Regular Vulnerability Assessments: Conduct periodic vulnerability scans and
penetration testing on the public-facing web server (72.21.196.160) to identify and
remediate potential security flaws.",
    "3. Verify DKIM Configuration: While SPF and DMARC are robust, ensure DomainKeys
Identified Mail (DKIM) is also correctly configured for all outgoing emails via Offi
ce 365 to further enhance email authenticity and prevent tampering.",
    "4. Develop/Review Incident Response Plan: Ensure a well-documented and regularl
y tested incident response plan is in place to manage and mitigate the impact of pot
ential cybersecurity incidents effectively.",
    "5. Network Segmentation: Consider internal network segmentation to isolate the
web server from other critical internal systems, limiting potential lateral movement
in case of a breach."
  ],
  "Conclusion": "Apex Innovations demonstrates a strong cybersecurity foundation, pa
rticularly in user authentication, email protection, and employee security awarenes
s. The proactive implementation of MFA, SPF, and a DMARC 'reject' policy positions t
he organization favorably against common cyber threats. While the direct exposure of
the web server on the external IP presents a specific focus area, the overall perime
ter security appears well-managed with minimal unnecessary open ports. Continued adh
erence to best practices and the implementation of the recommended enhancements will
further strengthen the organization's cybersecurity posture."
}
```

In [42]:
```
response = flashLiteModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
```

```
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report evaluates the cybersecurity posture of Apex Innovations b
ased on technical scans (DNS, DMARC, and port scanning) and a self-reported security
questionnaire. The findings indicate a strong implementation of foundational cyberse
curity controls across user authentication, email security, and network exposure.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External IP (Firewall): 72.21.196.160",
    "Website Hosting IP: 72.21.196.160",
    "DNS Hosting: Implicitly managed by the organization, with authoritative nameser
vers likely within their control."
  ],
  "Security Questionnaire Review": [
    "MFA for Email: Yes",
    "MFA for Computer Login: Yes",
    "MFA for Sensitive Systems: Yes",
    "Acceptable Use Policy: Yes",
    "New Employee Security Awareness Training: Yes",
    "Annual All-Employee Security Training: Yes",
    "Summary: Apex Innovations reports a comprehensive adoption of essential securit
y practices, including mandatory Multi-Factor Authentication across critical access
points and robust security awareness training programs for all employees. This demon
strates a proactive approach to user-based security risks."
  ],
  "DNS & Email Security": [
    "DNS Records:",
    "The apexinnovations.com domain has A, MX, NS, and TXT records.",
    "An A record points to 72.21.196.160, which is likely the web server.",
    "MX records point to mx1.apexinnovations.com and mx2.apexinnovations.com, indica
ting self-hosted or managed email infrastructure.",
    "The TXT record for the main domain includes an SPF record: \"v=spf1 include:sp
f.protection.outlook.com -all\". This suggests the organization uses Microsoft 365 f
or email and is correctly configured to prevent email spoofing.",
    "DMARC Record:",
    "A DMARC record exists for _dmarc.apexinnovations.com: \"v=DMARC1; p=reject; rua
=mailto:dmarc_reports@apexinnovations.com; fo=1\".",
    "The 'p=reject' policy enforces strict email authentication, significantly reduc
ing the risk of phishing and email impersonation.",
    "Conclusion: DNS and email security configurations, including SPF and DMARC, are
robust and follow best practices, indicating strong protection against email-based t
hreats."
  ],
  "Port Scanning Results": [
    "External IP Scan (72.21.196.160):",
    "Port 80 (HTTP): Open",
    "Port 443 (HTTPS): Open",
    "Website Scan (72.21.196.160):",
    "Port 80 (HTTP): Open",
    "Port 443 (HTTPS): Open",
    "Summary: The external IP address and the website hosting IP both show only port
s 80 and 443 open. These are standard ports for web services (HTTP and HTTPS) and ar
e expected for a publicly accessible website. The absence of other open ports on the
external IP suggests good firewall configuration, limiting the attack surface."
  ],
```

```
  "Risk Assessment & Readiness Summary": [
    "Category | Status | Notes",
    "---|---|---",
    "Authentication Security | ✅ Strong | MFA is mandated across email, computer l
ogins, and sensitive data systems.",
    "Email Security | ✅ Strong | SPF record is correctly configured (likely for Mi
crosoft 365), and a DMARC record with a 'reject' policy is in place, providing excel
lent protection against spoofing and phishing.",
    "Network Exposure | ✅ Secure | Only standard web ports (80 and 443) are open o
n the external IP, indicating effective firewall management.",
    "Web Hosting | ✅ Secure | Ports 80 and 443 are open, as expected for a websit
e.",
    "Policy & Training | ✅ Comprehensive | An acceptable use policy is in place, a
nd both new and existing employees receive regular security awareness training."
  ],
  "Recommendations": [
    "1. Regular Audits: Continue periodic reviews of DNS records, firewall rules, an
d security configurations to ensure ongoing compliance and identify potential drif
t.",
    "2. Vulnerability Management: Implement a schedule for regular vulnerability sca
nning of external and internal systems to proactively identify and remediate weaknes
ses.",
    "3. Incident Response Plan: Develop or refine an incident response plan, includi
ng testing and regular updates, to ensure preparedness for security incidents.",
    "4. Email Security Enhancement: While DMARC 'reject' is strong, monitor the DMAR
C reports (mailto:dmarc_reports@apexinnovations.com) to understand mail flow and pot
ential issues.",
    "5. Asset Management: Maintain an accurate inventory of all IT assets, including
software and hardware, to better manage security risks."
  ],
  "Conclusion": "Apex Innovations demonstrates a high level of cybersecurity readine
ss, characterized by strong authentication controls, robust email security measures,
and a well-hardened network perimeter. The organization's commitment to security awa
reness training and policy enforcement further strengthens its security posture. Con
tinuous monitoring and proactive vulnerability management are recommended to maintai
n this effective level of defense."
}
```

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample1_markdown_json.html")
```

In [43]:
```
# === SAMPLE 2 ===

#input markdown-formatted text, output JSON
response = proModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
```

```
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report assesses the cybersecurity readiness of G.A.S. Inc. based on a security questionnaire and technical scans of its public-facing infrastructure. The findings reveal critical deficiencies in fundamental security controls, including user authentication, email security, network perimeter defense, and employee security awareness. The organization currently exhibits a high-risk security posture and requires immediate remediation to protect against common cyber threats.",
  "Organizational Information": [
    "Organization Name: G.A.S. Inc.",
    "Email Domain: gasinc.net",
    "Website Domain: www.gasinc.net",
    "External IP: 104.28.1.189"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: No - This is a critical weakness, leaving email accounts vulnerable to takeover via credential theft.",
    "MFA for Computer Login: No - The lack of MFA on workstations increases the risk of unauthorized access to the internal network.",
    "MFA for Sensitive Systems: Yes - While positive, its effectiveness is reduced by the lack of MFA on email and computers, which are common initial access vectors.",
    "Employee Acceptable Use Policy: No - The absence of a formal policy creates ambiguity regarding secure practices and employee responsibilities.",
    "Security Awareness Training: No - The organization does not conduct security awareness training for new or existing employees, leaving the workforce highly susceptible to phishing and social engineering attacks."
  ],
  "DNS & Email Security": [
    "SPF Record: A Sender Policy Framework (SPF) record exists ('v=spf1 include:spf.mailhostbox.com ~all'). However, it uses a '~all' (SoftFail) qualifier, which allows unauthorized emails to be delivered to the inbox, reducing its effectiveness against spoofing.",
    "DMARC Record: The domain gasinc.net is missing a Domain-based Message Authentication, Reporting, and Conformance (DMARC) record. This is a critical security gap that leaves the organization highly vulnerable to email spoofing and phishing attacks impersonating its domain.",
    "Conclusion: Email security is weak. The lack of a DMARC policy and a permissive SPF record significantly increases the risk of successful phishing attacks and brand impersonation."
  ],
  "Port Scanning Results": [
    "A scan of the external IP address (104.28.1.189) revealed numerous open ports, indicating multiple services are directly exposed to the internet:",
    "Port 21 (FTP): Open - Insecure file transfer protocol.",
    "Port 22 (SSH): Open - Secure Shell, a common target for brute-force attacks.",
    "Port 25 (SMTP): Open - Simple Mail Transfer Protocol, can be exploited for spam relay.",
    "Port 80 (HTTP): Open - Expected for web traffic.",
    "Port 110 (POP3): Open - Insecure email retrieval protocol.",
    "Port 443 (HTTPS): Open - Expected for secure web traffic.",
    "Port 3389 (RDP): Open - Remote Desktop Protocol, a primary target for ransomware attacks.",
    "Conclusion: The network perimeter is dangerously exposed. Exposing services like FTP, SSH, and RDP directly to the internet presents a severe and immediate risk of compromise."
  ],
  "Risk Assessment & Readiness Summary": [
```

```
    "Authentication Security: Weak - Lack of mandatory MFA for email and computer ac
cess creates a high risk of account compromise.",
    "Email Security: Weak - The absence of DMARC and a permissive SPF record makes t
he organization highly susceptible to phishing and domain spoofing.",
    "Network Exposure: Critical Risk - Multiple high-risk services (RDP, SSH, FTP) a
re exposed directly to the internet, creating a large and vulnerable attack surfac
e.",
    "Policy & Training: Non-Existent - The lack of basic security policies and emplo
yee training indicates a low level of security maturity and high susceptibility to h
uman-centric attacks."
  ],
  "Recommendations": [
    "1. Immediately Implement MFA: Enforce MFA for all user access, starting with em
ail (Office 365/Google Workspace) and computer logins.",
    "2. Harden the Network Perimeter: Close all unnecessary ports on the firewall (1
04.28.1.189). Access to services like RDP and SSH should be restricted to a Virtual
Private Network (VPN) only.",
    "3. Strengthen Email Security: Implement a DMARC policy, starting with 'p=none'
for monitoring and progressing to 'p=quarantine' or 'p=reject'. Change the SPF recor
d qualifier from '~all' (SoftFail) to '-all' (HardFail).",
    "4. Develop and Implement Security Policies: Create a formal Employee Acceptable
Use Policy that outlines responsibilities for protecting company data and systems.",
    "5. Establish Security Awareness Training: Implement a mandatory security awaren
ess training program for all new and existing employees, conducted at least annuall
y, with a focus on phishing identification."
  ],
  "Conclusion": "G.A.S. Inc. currently has a very poor cybersecurity posture with cr
itical vulnerabilities across its network, user authentication, and email systems. T
he combination of exposed high-risk services, lack of MFA, and inadequate email secu
rity controls places the organization at an immediate and high risk of a significant
security breach. The recommendations provided in this report should be prioritized a
nd implemented without delay to establish a foundational level of security."
}
```

In [44]:

```
response = flashModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
 "Overview": "This report evaluates the cybersecurity posture of G.A.S. Inc. based o
n technical scans (DNS, DMARC, and port scanning) and a self-reported security quest
ionnaire. The findings indicate a critically weak cybersecurity posture across multi
ple domains, including user authentication, email security, and network perimeter ex
posure. The lack of basic security policies, employee training, and the presence of
numerous open and potentially insecure ports on their external IP collectively point
to a high-risk environment.",
 "Organizational Information": [
  "Organization Name: G.A.S. Inc.",
  "Email Domain: gasinc.net",
  "Website Domain: www.gasinc.net",
  "External IP: 104.28.1.189"
 ],
 "Security Questionnaire Review": [
  "MFA for Email: No",
  "MFA for Computer Login: No",
  "MFA for Sensitive Data Systems: Yes",
  "Acceptable Use Policy: No",
  "New Employee Security Awareness Training: No",
  "Annual All-Employee Security Training: No",
  "Summary: G.A.S. Inc. lacks fundamental user-centric security controls and policie
s. The absence of Multi-Factor Authentication (MFA) for email and computer logins, c
oupled with no security awareness training and no acceptable use policy, creates a h
ighly vulnerable internal environment. This significantly increases the risk of phis
hing, account compromise, and insider threats."
 ],
 "DNS & Email Security": [
  "MX Records: The MX records point to mx.mailhostbox.com and mx2.mailhostbox.com, i
ndicating email services are hosted externally.",
  "SPF Record: A valid SPF record is present (v=spf1 include:spf.mailhostbox.com ~al
l). This helps to prevent email spoofing by authorizing mail servers. The ~all (soft
fail) policy is a reasonable starting point.",
  "DMARC Record: No DMARC record was found for _dmarc.gasinc.net. This absence leave
s the organization susceptible to advanced email spoofing and phishing attacks that
could impersonate their domain, leading to brand damage and potential financial loss
es.",
  "Summary: While an SPF record is in place to provide some protection against email
spoofing, the complete absence of DMARC creates a significant gap in email security,
making the organization vulnerable to sophisticated phishing and impersonation attem
pts."
 ],
 "Port Scanning Results": [
  "Scanning Target: 104.28.1.189 (External IP / Firewall)",
  "Port 21 (FTP): Open - High risk. FTP often transmits credentials in cleartext and
is prone to various vulnerabilities. Direct exposure of FTP is rarely advisable.",
  "Port 22 (SSH): Open - Moderate risk. While SSH is encrypted, direct internet expo
sure increases the attack surface, especially without strong authentication and IP r
estrictions.",
  "Port 25 (SMTP): Open - Expected for mail servers, but represents a high risk if n
ot properly secured against open relay, brute-force attacks, and unauthenticated acc
ess.",
  "Port 80 (HTTP): Open - Expected for public web services, but should be redirected
to HTTPS.",
  "Port 110 (POP3): Open - High risk. POP3 often transmits credentials in cleartext
and is an outdated protocol. Secure alternatives like POP3S (encrypted POP3) should
```

be used if POP3 is necessary.",
  "Port 443 (HTTPS): Open - Expected for secure public web services.",
  "Port 3389 (RDP): Open - Extremely high risk. Remote Desktop Protocol (RDP) is a f
requent target for ransomware and brute-force attacks. Direct internet exposure of R
DP is a critical security vulnerability.",
  "Summary: The organization has a highly exposed external network perimeter with se
veral critical and high-risk services directly accessible from the internet. The exp
osure of FTP, POP3, SSH, and especially RDP, without reported MFA for computer login
s, represents a severe attack surface that could lead to unauthorized access, data b
reaches, and system compromise."
 ],
 "Risk Assessment & Readiness Summary": [
  "Authentication Security: Weak - Critical lack of MFA for email and computer login
s. MFA is only applied to sensitive data systems, leaving significant attack vectors
open.",
  "Email Security: Moderate - An SPF record exists, but the complete absence of DMAR
C leaves a significant vulnerability to email spoofing and phishing.",
  "Network Exposure: Very High Risk - Numerous critical services (FTP, SSH, SMTP, PO
P3, RDP) are openly exposed to the internet, creating a large attack surface.",
  "Policy & Training: Very Weak - No acceptable use policy is in place, and there is
no security awareness training for new or existing employees, fostering a low-securi
ty culture.",
  "Overall Posture: Critically Vulnerable - The combination of weak internal control
s, a highly exposed external network, and a lack of essential email security protoco
ls creates a substantial and immediate risk to G.A.S. Inc.'s data, systems, and repu
tation."
 ],
 "Recommendations": [
  "Implement Multi-Factor Authentication (MFA) Broadly: Immediately implement MFA fo
r all email accounts and computer logins to significantly enhance user account secur
ity.",
  "Review and Secure Exposed Services: Conduct an urgent review of all exposed servi
ces on the external IP (104.28.1.189). Close Port 21 (FTP) and Port 110 (POP3) and m
igrate to secure alternatives (e.g., SFTP/SCP, IMAPS/SMTPS). Restrict access to Port
22 (SSH) and Port 3389 (RDP) to only trusted IPs via a firewall or implement a VPN f
or secure remote access, combined with strong, complex passphrases and MFA.",
  "Implement DMARC for Email Domain: Configure a DMARC record with at least a 'quara
ntine' policy (p=quarantine) for gasinc.net to protect against email spoofing and ph
ishing, gradually moving to a 'reject' policy (p=reject) after monitoring.",
  "Develop and Enforce Security Policies: Immediately create and implement an employ
ee acceptable use policy to define expected security behaviors.",
  "Conduct Regular Security Awareness Training: Introduce mandatory security awarene
ss training for all new hires and conduct annual refresher training for all employee
s to build a security-conscious culture.",
  "Regular Vulnerability Scanning and Penetration Testing: Implement a program for r
egular external and internal vulnerability assessments and periodic penetration test
ing to proactively identify and address security weaknesses.",
  "Review and Implement Principle of Least Privilege: Ensure that all users, account
s, and services are configured with the minimum necessary access and permissions req
uired for their function."
 ],
 "Conclusion": "G.A.S. Inc. currently operates with a critically weak cybersecurity
posture. The lack of foundational security policies, absence of employee security tr
aining, insufficient multi-factor authentication, and a highly exposed external netw
ork perimeter with several high-risk open services collectively present a significan
t and immediate threat landscape. Urgent and comprehensive action is required across

```
all identified areas to address these vulnerabilities and enhance the organization's
cyber resilience to an acceptable level."
}
```

In [45]:

```
response = flashLiteModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report assesses the cybersecurity readiness of G.A.S. Inc. based on provided DNS, port scanning, and security questionnaire data. The assessment reveals several critical areas of concern, particularly regarding basic security controls and network exposure.",
  "Organizational Information": [
    "Organization Name: G.A.S. Inc.",
    "Email Domain: gasinc.net",
    "Website Domain: www.gasinc.net",
    "External IP: 104.28.1.189"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: No - Significant risk of account compromise.",
    "MFA for Computer Login: No - Poses a risk to endpoint security.",
    "MFA for Sensitive Data Systems: Yes - Positive control, but lack of MFA for email/computers is a major weakness.",
    "Acceptable Use Policy: No - Lacks foundational policy for user conduct and security.",
    "New Employee Security Awareness Training: No - Increases risk of initial security oversights.",
    "Annual All-Employee Security Training: No - Employees are not kept up-to-date on current threats and best practices."
  ],
  "DNS & Email Security": [
    "Email Domain (gasinc.net):",
    "MX Records: mx.mailhostbox.com, mx2.mailhostbox.com - Indicates use of a third-party email provider.",
    "SPF Record: \"v=spf1 include:spf.mailhostbox.com ~all\" - This record is present and correctly configured to authorize mailhostbox.com as a sender, which is good.",
    "DMARC Record: NXDOMAIN (Non-Existent Domain) for _dmarc.gasinc.net - This is a critical deficiency. The absence of a DMARC record leaves the domain vulnerable to email spoofing and phishing attacks."
  ],
  "Port Scanning Results": [
    "External IP Scan (104.28.1.189):",
    "Open Ports: 21 (FTP), 22 (SSH), 25 (SMTP), 80 (HTTP), 110 (POP3), 443 (HTTPS), 3389 (RDP).",
    "Analysis: The exposure of numerous services, including FTP, SSH, SMTP, POP3, and RDP, directly to the internet is a significant security risk. These services, if not properly secured and monitored, can be entry points for attackers.",
    "Website Scan (104.28.1.189):",
    "Open Ports: 80 (HTTP), 443 (HTTPS) - Standard for web servers.",
    "Analysis: While expected, the overall exposure of the external IP needs to be considered in conjunction with the web ports."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Low - Lack of MFA for email and computer logins is a critical vulnerability.",
    "Email Security: Low - Absence of DMARC record makes the domain highly susceptible to spoofing.",
    "Network Exposure: High Risk - Numerous unnecessary ports open on the external IP.",
    "Policy & Training: Low - Absence of an acceptable use policy and security awareness training for all employees.",
    "Overall Readiness: Low - Multiple foundational security controls are missing or
```

```
inadequately implemented."
  ],
  "Recommendations": [
    "Implement MFA immediately for email access and computer logins.",
    "Implement a DMARC record for the gasinc.net domain with a reject or quarantine
policy.",
    "Review and close all unnecessary open ports on the external IP address (104.28.
1.189). Specifically, ports 21, 22, 25, 110, and 3389 should not be directly exposed
if not absolutely required and secured.",
    "Develop and implement an Acceptable Use Policy for all employees.",
    "Establish and conduct regular security awareness training for all employees, in
cluding new hires and annual refreshers.",
    "Consider disabling or restricting access to non-essential services like FTP (po
rt 21) and RDP (port 3389) from the public internet.",
    "If FTP or SSH must be exposed, ensure they are secured with strong credentials
and potentially through a VPN or bastion host."
  ],
  "Conclusion": "G.A.S. Inc. currently presents a low cybersecurity readiness postur
e. The lack of multi-factor authentication for critical systems like email and compu
ters, the absence of a DMARC record, and the extensive exposure of network services
present significant risks. Immediate implementation of the recommended security cont
rols is crucial to mitigate these vulnerabilities and improve the organization's ove
rall security."
}
```

In [4]:
```python
from pypdf import PdfReader

def extract_text_from_pdf(pdf_path):
    text = ""
    try:
        reader = PdfReader(pdf_path)
        for page in reader.pages:
            text += page.extract_text() + "\n"
    except Exception as e:
        print(f"Error reading PDF: {e}")
        return None
    return text
```

In [ ]:
```python
prompt_text = 'Prompt:\nGiven this DNS DIG, Port scan of the website, Port scan of

context1_text = 'Context:\n'
context2_text = 'Context:\n'
example_text = 'Example:\n' + prompt_text

filepaths = ["report_template/test_questionnaire.json", "report_template/test_port_
pdfFile = "report_template/test_report.pdf"

sample1_filepaths = ["report_sample1/sample1_questionnaire.json", "report_sample1/s
sample2_filepaths = ["report_sample2/sample2_questionnaire.json", "report_sample2/s

for file in filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            example_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"
```

```
    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

example_text += extract_text_from_pdf(pdfFile)

print("=======  Example ==========")
print(example_text)
print("============================")

for file in sample1_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context1_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 1 =========")
print(prompt_text)
print(context1_text)
print("============================")

for file in sample2_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context2_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 2 =========")
print(prompt_text)
print(context2_text)
print("============================")
```

======= Example ==========
Example:
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization.template/test_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Valier School District",
    "Email Domain": "valier.k12.mt.us",
    "Website Domain": "www.valier.k12.mt.us",
    "External IP": "216.220.16.170",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
--
template/test_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
220.16.170\nScanning started at:2025-07-18 22:12:17.055226\n-----------------------
--------------------------\nno ports open\n"
}
--
template/test_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
239.32.21\nScanning started at:2025-07-18 22:09:34.408091\n-------------------------
------------------------\nPort 80 is open\nPort 443 is open\n"
}
--
template/test_dns_dig_email.json:
{
  "text": "id 49113\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\nvalier.
k12.mt.us. IN ANY\n;ANSWER\nvalier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-reque
st.umt.edu. 2024030501 21600 900 1209600 86400\nvalier.k12.mt.us. 3600 IN NS ens-o1.
umt.edu.\nvalier.k12.mt.us. 3600 IN NS cudess2.umt.edu.\nvalier.k12.mt.us. 3600 IN N
S cudess1.umt.edu.\nvalier.k12.mt.us. 3600 IN A 216.239.38.21\nvalier.k12.mt.us. 360
0 IN A 216.239.32.21\nvalier.k12.mt.us. 3600 IN A 216.239.34.21\nvalier.k12.mt.us. 3
600 IN A 216.239.36.21\nvalier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.\nvalier.k
12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 10 aspm
x3.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.\nvalier.
k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.\nvalier.k12.mt.us. 3600 IN TXT \"v=
spf1 include:_spf.google.com include:mg.infinitecampus.org -all\"\n;AUTHORITY\n;ADDI
TIONAL\n"
}
--
template/test_dns_dig_email_dmarc.json:
{
  "text": "id 45565\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
```

valier.k12.mt.us. IN ANY\n;ANSWER\n_dmarc.valier.k12.mt.us. 3600 IN TXT \"v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us\"\n;AUTHORITY\n;ADDITIONAL\n"
}
--

Cybersecurity Readiness Report for Valier School District Date: July 18, 2025

1. Overview

This report evaluates the cybersecurity posture of Valier School District based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings reflect a strong commitment to foundational cybersecurity practices across user access, email protection, network exposure, and staff awareness.

2. Organizational Information

● Organization Name: Valier School District ● Email Domain: valier.k12.mt.us ● Website Domain: www.valier.k12.mt.us ● External IP (Firewall): 216.220.16.170 ● Website Hosting IPs: 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21 ● DNS Hosting: Managed by University of Montana (umt.edu nameservers)

3. Security Questionnaire Review Security Control Status

MFA for Email ✅ Yes
MFA for Computer Login ✅ Yes
MFA for Sensitive Systems ✅ Yes
Acceptable Use Policy ✅ Yes
New Employee Security Awareness Training ✅ Yes
Annual All-Employee Security Training ✅ Yes

Summary: The district reports complete implementation of basic cyber hygiene practices, especially
user authentication (Multi-Factor Authentication) and routine training. This indicates a proactive and policy-driven approach to risk mitigation.

4. DNS & Email Security

DNS Records

● DNS is managed by the University of Montana (cudess1.umt.edu, cudess2.umt.edu), suggesting centralized and professionally administered DNS. ● A records point to IPs within Google's network (likely Google Sites hosting for web content).

MX Records (Email)

● The district uses Google Workspace (Gmail) for email, as shown by multiple aspmx.l.google.com MX records. ● SPF record is correctly configured: v=spf1 include:_spf.google.com include:mg.infinitecampus.org -all This helps mitigate spoofing by defining authorized mail senders.

DMARC Record

● A valid DMARC record exists with a reject policy: v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us This instructs receiving servers to reject unauthenticated mail, providing strong protection against phishing.

Conclusion: DNS and email protections (SPF, DMARC, and hosting security) are configured correctly and follow best practices.

5. Port Scanning Results

Website Hosting (Google IP: 216.239.32.21)

● Port 80 (HTTP): Open ● Port 443 (HTTPS): Open These are expected for a publicly accessible website and are typical for Google-hosted services.

Firewall / External IP (216.220.16.170)

● All scanned ports are closed This is a strong sign of network perimeter hardening and good firewall configuration. No externally exposed servic

es were found on the organization’s primary IP.

6. Risk Assessment & Readiness Summary Category Status Notes
Authentication Security ✅ Strong MFA is required across key systems
Email Security ✅ Strong SPF and DMARC with “reject” policy in place
Network Exposure ✅ Secure No exposed services on the external firewall IP
Web Hosting ✅ Secure Google-hosted; limited attack surface
Policy & Training ✅ Comprehensive Acceptable use policies and regular tr aining in place

7. Recommendations
Although the cybersecurity readiness is solid, continuous improvement is es sential. We recommend the following:
1. Verify DKIM : While SPF and DMARC are configured, ensure DKIM is also active for all sending domains. 2. Vulnerability Scanning : Consider regul ar internal and external vulnerability assessments of network devices and servers. 3. Incident Response Plan : Document and regularly test a cybers ecurity incident response and disaster recovery plan. 4. Asset Inventory : Maintain a regularly updated inventory of hardware/software assets and moni tor for unauthorized changes. 5. Third-party Risk : Evaluate vendors (e. g., Infinite Campus) for their security posture, especially since they're included in SPF.

8. Conclusion
Valier School District demonstrates a strong cybersecurity foundation, parti cularly in authentication, email protection, staff training, and perimeter security. Continued vigilance and regular audits will help maintain and im prove this strong security posture.

Prepared by: Cybersecurity Assessment Team Date: July 18, 2025

==========
======== Sample 1 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans wers to the security questionnaire, write a report on the cybersecurity readiness of the organization.
Context:
sample1/sample1_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Apex Innovations",
    "Email Domain": "apexinnovations.com",
    "Website Domain": "www.apexinnovations.com",
    "External IP": "72.21.196.160",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
```

```
}
--
sample1/sample1_dns_dig_email_dmarc.json:
{
  "text": "id 31890\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
apexinnovations.com. IN ANY\n;ANSWER\n_dmarc.apexinnovations.com. 3600 IN TXT \"v=DM
ARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\""
}
--
sample1/sample1_dns_dig_email.json:
{
  "text": "id 52417\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\napexinn
ovations.com. IN ANY\n;ANSWER\napexinnovations.com. 3600 IN SOA ns1.apexinnovations.
com. hostmaster.apexinnovations.com. 2025101401 21600 3600 604800 3600\napexinnovati
ons.com. 3600 IN NS ns1.apexinnovations.com.\napexinnovations.com. 3600 IN NS ns2.ap
exinnovations.com.\napexinnovations.com. 3600 IN A 72.21.196.160\napexinnovations.co
m. 3600 IN MX 10 mx1.apexinnovations.com.\napexinnovations.com. 3600 IN MX 20 mx2.ap
exinnovations.com.\napexinnovations.com. 3600 IN TXT \"v=spf1 include:spf.protectio
n.outlook.com -all\""
}
--
sample1/sample1_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:09:42.589112\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--
sample1/sample1_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:08:15.223456\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
======== Sample 2 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization.
Context:
sample2/sample2_questionnaire.json:
{
  "text": {
    "Organization Name": "G.A.S. Inc.",
    "Email Domain": "gasinc.net",
    "Website Domain": "www.gasinc.net",
    "External IP": "104.28.1.189",
    "Do you require MFA to access email?": "No",
    "Do you require MFA to log into computers?": "No",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "No",
    "Does your organization do security awareness training for new employees?": "N
o",
```

```
    "Does your organization do security awareness training for all employees at leas
t once per year?": "No"
  }
}
--
sample2/sample2_dns_dig_email_dmarc.json:
{
  "text": "id 28911\nopcode QUERY\nrcode NXDOMAIN\nflags QR AA RD RA\n;QUESTION\n_dm
arc.gasinc.net. IN ANY\n;AUTHORITY\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmas
ter.gasinc.net. 2025101402 14400 3600 604800 3600\n;ADDITIONAL"
}
--
sample2/sample2_dns_dig_email.json:
{
  "text": "id 47123\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\ngasinc.
net. IN ANY\n;ANSWER\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmaster.gasinc.ne
t. 2025101402 14400 3600 604800 3600\ngasinc.net. 3600 IN NS dns1.gasinc.net.\ngasin
c.net. 3600 IN NS dns2.gasinc.net.\ngasinc.net. 3600 IN A 104.28.1.189\ngasinc.net.
3600 IN MX 10 mx.mailhostbox.com.\ngasinc.net. 3600 IN MX 20 mx2.mailhostbox.com.\ng
asinc.net. 3600 IN TXT \"v=spf1 include:spf.mailhostbox.com ~all\""
}
--
sample2/sample2_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:16:11.890123\n-------------------------
-------------------------\nPort 21 is open\nPort 22 is open\nPort 25 is open\nPort 8
0 is open\nPort 110 is open\nPort 443 is open\nPort 3389 is open"
}
--
sample2/sample2_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:15:30.456789\n-------------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
```


In [23]:

```python
# === SAMPLE 1 ===

# input PDF, output markdown
response = proModel.generate_content(contents=[prompt_text, context1_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations
Date: October 14, 2025

1. Overview

This report provides an evaluation of the cybersecurity readiness of Apex Innovations, based on a combination of a self-reported security questionnaire and external technical scans, including DNS analysis and port scanning. The findings indicate a strong commitment to identity management, employee awareness, and email security. However, the network architecture, which exposes web services on the primary external IP address, presents a notable area for improvement and a potential risk to the organization.

2. Organizational Information

*   **Organization Name:** Apex Innovations
*   **Email Domain:** apexinnovations.com
*   **Website Domain:** www.apexinnovations.com
*   **External / Website IP:** 72.21.196.160 (Note: The primary external IP and the web server IP are the same)

3. Security Questionnaire Review

Security Control	Status
MFA for Email	✅ Yes
MFA for Computer Login	✅ Yes
MFA for Sensitive Systems	✅ Yes
Acceptable Use Policy	✅ Yes
New Employee Security Awareness Training	✅ Yes
Annual All-Employee Security Training	✅ Yes

Summary: Apex Innovations reports a strong internal security culture. The mandatory use of Multi-Factor Authentication (MFA) across all key access points significantly reduces the risk of credential-based attacks. This is complemented by a solid foundation of employee policies and regular security awareness training.

4. DNS & Email Security

DNS Records
*   DNS is managed on self-hosted nameservers (`ns1.apexinnovations.com`, `ns2.apexinnovations.com`), indicating direct control over their DNS infrastructure.

MX Records (Email)
*   The organization uses Microsoft 365 for its email services, as indicated by the SPF record pointing to `spf.protection.outlook.com`.
*   The SPF record is correctly configured with a `-all` (hard fail) mechanism, which helps prevent unauthorized servers from sending email on behalf of their domain:
    `v=spf1 include:spf.protection.outlook.com -all`

DMARC Record
*   A strong DMARC policy is in place, instructing receiving mail servers to **reject** emails that fail authentication checks. This provides excellent protection against direct domain spoofing and phishing attacks.
    `v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1`

Conclusion: The organization's email security configuration is robust and adheres to modern best practices. The combination of SPF and a DMARC "reject" policy is a significant strength.

5. Port Scanning Results

External Firewall / Website IP (72.21.196.160)
*   **Port 80 (HTTP): Open**
*   **Port 443 (HTTPS): Open**

The port scan reveals that the primary external IP address for the organization is also hosting the public-facing website. While these ports are necessary for web traffic, exposing them directly on the main corporate firewall IP increases the network's attack surface. Any vulnerability in the web server, its applications, or its configuration could potentially provide a pivot point into the internal network.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	✅ Strong	Comprehensive MFA implementation across all critical systems.
Email Security	✅ Strong	SPF and DMARC with a "reject" policy are correctly configured.
Network Exposure	⚠️ Moderate	The public website is exposed on the primary external firewall IP, creating a direct attack vector that should be isolated.
Web Hosting	⚠️ Moderate	Hosting the website on the primary network perimeter places the burden of security (patching, hardening) entirely on the organization.
Policy & Training	✅ Comprehensive	All foundational policies and training programs are in place.

7. Recommendations

While Apex Innovations has many strong security controls, the following recommendations are made to address the identified risks and further mature its cybersecurity posture:

1. **Network Segmentation:** The highest priority should be to isolate the web server from the internal corporate network. This can be achieved by:
    *   Placing the web server in a segregated network zone (a DMZ).
    *   Migrating the website to a reputable third-party cloud hosting provider.
    This will ensure that a compromise of the web server does not lead to an immediate compromise of internal systems.

2. **Web Application Security:** Given its direct exposure, the web server requires heightened security. Implement a Web Application Firewall (WAF) to protect against common web-based attacks and conduct regular vulnerability scans of the web application and server.

3. **Verify DKIM Implementation:** While SPF and DMARC are in place, ensure that DKIM (DomainKeys Identified Mail) is also configured for Microsoft 365 to complete the trifecta of email authentication standards.

4. **Develop an Incident Response Plan:** Formalize, document, and test an incident response plan to ensure the organization can respond effectively and efficiently in the event of a security breach.

8. Conclusion

Apex Innovations demonstrates a very strong cybersecurity foundation in terms of policy, user authentication, and email security. These proactive measures significantly reduce risk from phishing and credential theft. The primary area of concern is the network architecture, where the public-facing website is co-located with the main network perimeter. By implementing the recommendation to segment the web server, Apex Innovations can substantially reduce its attack surface and elevate its overall security posture from strong to excellent.

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample1_pdf_markdown.html")
```

✅ Successfully exported HTML: pro_sample1_pdf_markdown.html

In [25]:
```
response = flashModel.generate_content(contents=[prompt_text, context1_text + "\n"
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations

Date: October 14, 2025

1. Overview
This report assesses the cybersecurity posture of Apex Innovations based on information gathered from DNS records (DIG), port scans of the external IP and website, and responses to a security questionnaire. The findings indicate a robust commitment to essential cybersecurity practices, particularly in user access controls, email security, and staff awareness. The organization appears to directly host its website on its external-facing IP address.

2. Organizational Information
*   **Organization Name:** Apex Innovations
*   **Email Domain:** apexinnovations.com
*   **Website Domain:** www.apexinnovations.com
*   **External IP / Website IP:** 72.21.196.160
*   **DNS Hosting:** Self-managed (ns1.apexinnovations.com, ns2.apexinnovations.com)

3. Security Questionnaire Review
Apex Innovations reports a strong adherence to foundational cybersecurity policies and controls:

Security Control	Status
MFA for Email	✅ Yes
MFA for Computer Login	✅ Yes
MFA for Sensitive Data Systems	✅ Yes
Employee Acceptable Use Policy	✅ Yes
New Employee Security Awareness Training	✅ Yes
Annual All-Employee Security Training	✅ Yes

Summary: The organization has fully implemented critical security measures concerning multi-factor authentication (MFA) across key access points, established an acceptable use policy, and conducts regular security awareness training for all employees. This demonstrates a proactive and policy-driven approach to reducing insider threats and unauthorized access.

4. DNS & Email Security

DNS Records
*   DNS is managed internally by Apex Innovations (ns1.apexinnovations.com, ns2.apexinnovations.com), suggesting direct control over DNS infrastructure.
*   The primary A record for apexinnovations.com points to 72.21.196.160, indicating the main website and external services are hosted on this IP.

MX Records (Email)
*   Email is configured to use internal mail exchange servers (mx1.apexinnovations.com, mx2.apexinnovations.com).
*   **SPF Record:** `v=spf1 include:spf.protection.outlook.com -all`
    *   The SPF record is correctly configured, including Microsoft Outlook's SPF for legitimate email sending. The `-all` mechanism specifies a "hard fail" policy, instructing receiving mail servers to reject mail from unauthorized senders, providing strong protection against email spoofing.

DMARC Record

*   **DMARC Record:** `v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1`
    *   A valid DMARC record is present with a `p=reject` policy. This is the strongest DMARC policy, directing receiving servers to reject emails that fail DMARC authentication. This significantly mitigates risks from phishing and impersonation attacks. Email reports are configured to be sent to `dmarc_reports@apexinnovations.com`.

Conclusion: DNS and email security configurations (SPF with hard fail and DMARC with a reject policy) are exceptionally strong and follow best practices, significantly reducing the risk of email-based attacks like spoofing and phishing.

5. Port Scanning Results

Website & External IP (72.21.196.160)
*   **Port 80 (HTTP):** Open
*   **Port 443 (HTTPS):** Open

Summary: Both the "Website Scan" and "External IP Scan" targeted the same IP address (72.21.196.160), indicating that the organization's public website is hosted directly on its external IP, likely behind a firewall that only permits HTTP and HTTPS traffic. The open ports 80 and 443 are standard and expected for a publicly accessible web server. No other ports were found open, which is positive for minimizing the attack surface.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	✅ Strong	MFA is a mandatory requirement across email, computer logins, and sensitive data systems, providing robust protection against credential theft.
Email Security	✅ Strong	Comprehensive SPF (`-all`) and DMARC (`p=reject`) policies are in place, significantly reducing the threat of email spoofing and phishing, and directing unauthenticated emails to be rejected. Reporting is also configured.
Network Exposure	✅ Secure	The external IP (72.21.196.160) only exposes necessary web ports (80, 443). This indicates a well-configured perimeter firewall minimizing the external attack surface.
Web Hosting	✅ Good	The website is hosted on the external IP, with only standard web ports open. While this consolidates the external presence, it means the web server is directly exposed and requires vigilant patching and security monitoring.
Policy & Training	✅ Comprehensive	An acceptable use policy is established, and security awareness training is conducted for both new hires and annually for all employees, fostering a security-conscious culture.

7. Recommendations
Apex Innovations exhibits a commendable cybersecurity readiness posture. To further enhance and maintain this strong position, the following recommendations are suggest

ed:

1. **Implement DKIM:** While SPF and DMARC are robust, ensure DomainKeys Identified Mail (DKIM) is also properly configured for all outgoing email to provide an additional layer of email authentication and trust.
2. **Regular Vulnerability Management:** Given the direct exposure of the web server on the external IP, implement regular external and internal vulnerability scanning of this server and underlying infrastructure. Establish a rigorous patch management program for all software, operating systems, and web applications running on this server.
3. **Incident Response Plan:** Develop, document, and regularly test a comprehensive cybersecurity incident response and disaster recovery plan. This ensures the organization can effectively detect, respond to, and recover from security incidents.
4. **Security Information and Event Management (SIEM):** Consider implementing a SIEM solution to centralize log collection, monitor security events in real-time, and facilitate threat detection and analysis, particularly for the externally exposed web server.
5. **Web Application Firewall (WAF):** To protect the public-facing website more effectively, consider deploying a Web Application Firewall (WAF) to defend against common web-based attacks (e.g., SQL injection, cross-site scripting).

8. Conclusion
Apex Innovations has established a strong cybersecurity foundation, particularly in user authentication, email protection, network perimeter security, and employee security awareness. The organization's proactive measures significantly reduce its overall cyber risk. By adopting the recommended continuous improvement strategies, Apex Innovations can further strengthen its defenses and ensure long-term resilience against evolving cyber threats.

Prepared by: Cybersecurity Assessment Team
Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample1_pdf_markdown.html")
```

✅ Successfully exported HTML: flash_sample1_pdf_markdown.html

In [27]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context1_text + "
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations Date: October 14, 2025

1. Overview

This report assesses the cybersecurity readiness of Apex Innovations based on provid
ed DNS information, port scan results for the website and firewall, and responses to
a security questionnaire. The findings indicate a generally strong security posture
with robust practices in place for authentication and email security, coupled with a
well-hardened external network perimeter.

2. Organizational Information

*   **Organization Name:** Apex Innovations
*   **Email Domain:** apexinnovations.com
*   **Website Domain:** www.apexinnovations.com
*   **External IP (Firewall):** 72.21.196.160
*   **Website Hosting IP:** 72.21.196.160 (as indicated by the A record for the doma
in)
*   **DNS Hosting:** Managed internally (indicated by `ns1.apexinnovations.com` and
`ns2.apexinnovations.com` as name servers).

3. Security Questionnaire Review

Security Control	Status
MFA for Email	✅ Yes
MFA for Computer Login	✅ Yes
MFA for Sensitive Data Systems	✅ Yes
Acceptable Use Policy	✅ Yes
New Employee Security Awareness Training	✅ Yes
Annual All-Employee Security Training	✅ Yes

Summary: Apex Innovations demonstrates a strong commitment to foundational cyber
security practices. The mandatory implementation of Multi-Factor Authentication (MF
A) across email, computer logins, and sensitive data systems is a significant streng
th. Furthermore, the existence of an acceptable use policy and regular security awar
eness training for all employees, including new hires, indicates a proactive approac
h to mitigating human-factor risks.

4. DNS & Email Security

DNS Records:
*   The DNS records for `apexinnovations.com` show both NS (Name Server) records poi
nting to `ns1.apexinnovations.com` and `ns2.apexinnovations.com`, suggesting the org
anization manages its own DNS infrastructure.
*   An A record points to `72.21.196.160`, which is consistent with the external IP
address scanned and identified as the firewall.
*   MX records indicate that email is handled by Microsoft 365 (`spf.protection.outl
ook.com`).

SPF Record:
*   The SPF record is correctly configured as: `v=spf1 include:spf.protection.outloo
k.com -all`. This record properly authorizes Microsoft 365 servers to send email on
behalf of `apexinnovations.com`, helping to prevent email spoofing.

DMARC Record:

*   A DMARC record is present with a `reject` policy: `v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1`.
    *   The `p=reject` policy is strong, instructing receiving mail servers to reject emails that fail DMARC authentication.
    *   The `rua` tag indicates that aggregate reports will be sent to `dmarc_reports@apexinnovations.com`, which is crucial for monitoring email authentication and identifying potential spoofing attempts.
    *   The `fo=1` flag requests failure reporting for all checking, providing detailed information on authentication failures.

Conclusion: Apex Innovations has implemented robust email security measures through correctly configured SPF and DMARC records with a strict reject policy. The active use of DMARC reporting is a key indicator of diligent security monitoring.

5. Port Scanning Results

Website Hosting (IP: 72.21.196.160):
*   Port 80 (HTTP): Open
*   Port 443 (HTTPS): Open

These are standard ports for a publicly accessible website and are expected. The presence of both indicates the website is accessible via both unencrypted and encrypted connections.

Firewall / External IP (72.21.196.160):
*   The port scan of the external IP address did not report any open ports.

Conclusion: The external IP address serving as the firewall appears to be well-hardened, with no open ports detected. This indicates a strong network perimeter and effective firewall configuration, significantly reducing the attack surface exposed to the internet.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	✅ Strong	Mandatory MFA across all critical access points.
Email Security	✅ Strong	Properly configured SPF and DMARC with a strict `reject` policy and active reporting.
Network Exposure	✅ Secure	No open ports detected on the external firewall IP, indicating a well-hardened perimeter.
Web Hosting	✅ Sound	Standard ports (80, 443) are open, as expected for a website.
Policy & Training	✅ Comprehensive	Acceptable use policies and regular security awareness training for all employees.

7. Recommendations

Apex Innovations has demonstrated a strong cybersecurity posture. To further enhance readiness, the following recommendations are made:

1. **Verify DKIM:** While SPF and DMARC are in place, ensure that DomainKeys Identified Mail (DKIM) signing is also implemented and configured correctly for outgoing e

mails. DKIM adds another layer of email authentication and strengthens protection ag
ainst spoofing.
2. **Regular Vulnerability Scanning:** Conduct regular, scheduled vulnerability sca
ns (both internal and external) of the network infrastructure and web servers. This
proactive measure helps identify and address potential weaknesses before they can be
exploited.
3. **Incident Response Plan Review:** Ensure that a comprehensive incident response
plan is documented, regularly reviewed, and tested. This plan should outline procedu
res for responding to various security incidents, including data breaches and system
compromise.
4. **Web Application Firewall (WAF):** Given that the website is accessible via por
ts 80 and 443, consider implementing a Web Application Firewall (WAF) to provide an
additional layer of protection against common web-based attacks such as SQL injectio
n and cross-site scripting (XSS).
5. **Log Monitoring and Analysis:** Implement robust log monitoring and analysis so
lutions for critical systems and network devices. This will aid in the early detecti
on of suspicious activities and facilitate faster incident response.

8. Conclusion

Apex Innovations exhibits a high level of cybersecurity readiness. The organization
has successfully implemented strong controls around user authentication, email secur
ity, and network perimeter defense. The commitment to employee training and policy e
nforcement further solidifies its security posture. By considering the additional re
commendations, Apex Innovations can continue to mature its cybersecurity program and
maintain a robust defense against evolving threats.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample1_pdf_markdown.html")
```

✅ Successfully exported HTML: flash_lite_sample1_pdf_markdown.html

In [29]:
```
# === SAMPLE 2 ===

# input PDF, output markdown
response = proModel.generate_content(contents=[prompt_text, context2_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.
Date: October 14, 2025

1. Overview
This report evaluates the cybersecurity posture of G.A.S. Inc. based on a security questionnaire and external technical scans. The findings reveal critical vulnerabilities in network security, email configuration, user authentication, and organizational policy. The organization currently has a very weak security posture and is at high risk of a cyberattack, including ransomware, data breach, and business email compromise. Immediate and decisive action is required to mitigate these risks.

2. Organizational Information
- **Organization Name:** G.A.S. Inc.
- **Email Domain:** gasinc.net
- **Website Domain:** www.gasinc.net
- **External IP Address:** 104.28.1.189

3. Security Questionnaire Review

Security Control	Status
MFA for Email	❌ **No**
MFA for Computer Login	❌ **No**
MFA for Sensitive Systems	✅ Yes
Acceptable Use Policy	❌ **No**
New Employee Security Awareness Training	❌ **No**
Annual All-Employee Security Training	❌ **No**

Summary: The questionnaire reveals a significant lack of foundational security controls. The absence of Multi-Factor Authentication (MFA) for email and computer access exposes the organization to account takeovers from simple password compromises. The lack of security policies and employee training indicates a low level of security maturity, making staff highly susceptible to social engineering and phishing attacks.

4. DNS & Email Security

*   **SPF Record:** An SPF record exists (`v=spf1 include:spf.mailhostbox.com ~all`). However, it uses a soft-fail (`~all`) policy, which only marks unauthorized emails as suspicious rather than blocking them. This provides weak protection against email spoofing.
*   **DMARC Record:** A DMARC record for `_dmarc.gasinc.net` is **missing** (`rcode NXDOMAIN`). Without DMARC, the organization has no ability to instruct receiving email servers on how to handle fraudulent emails sent on its behalf and has no visibility into spoofing campaigns targeting its domain.

Conclusion: Email security is poor. The combination of a weak SPF policy and the complete absence of DMARC leaves G.A.S. Inc. highly vulnerable to phishing, business email compromise, and brand impersonation attacks.

5. Port Scanning Results
A port scan of the external IP address (104.28.1.189) revealed multiple high-risk services exposed directly to the internet.

*   **Port 21 (FTP): Open** - Insecure, unencrypted protocol.
*   **Port 22 (SSH): Open** - Potential access point for attackers.

*   **Port 25 (SMTP): Open** - Potentially an open mail relay, a target for spammers.
*   **Port 80 (HTTP): Open** - Standard for web traffic.
*   **Port 110 (POP3): Open** - Insecure, unencrypted email protocol.
*   **Port 443 (HTTPS): Open** - Standard for secure web traffic.
*   **Port 3389 (RDP): Open** - **CRITICAL RISK.** Exposing Remote Desktop Protocol to the internet is a primary vector for ransomware attacks.

Conclusion: The network perimeter is dangerously misconfigured. Exposing services like RDP, FTP, and POP3 directly to the internet creates an extremely large and vulnerable attack surface.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	❌ **Poor**	Lack of MFA on email and computers is a major weakness.
Email Security	❌ **Poor**	Weak SPF and no DMARC record leave the organization open to spoofing.
Network Exposure	🚨 **Critical**	RDP and other insecure ports are directly exposed to the internet.
Policy & Training	❌ **Non-Existent**	No policies or training programs in place, elevating human risk.

7. Recommendations
The following actions should be taken to address the identified vulnerabilities, prioritized by risk.

Immediate (Critical Priority):
1. **Close Port 3389 (RDP):** Immediately place the RDP service behind a Virtual Private Network (VPN) with MFA. Do not leave it exposed to the public internet.
2. **Close Insecure Ports:** Close ports 21 (FTP) and 110 (POP3) on the firewall. Use secure, encrypted alternatives like SFTP or IMAPS/POP3S, accessible only via VPN.
3. **Restrict Access to Other Ports:** Review the business need for public access to Port 22 (SSH) and Port 25 (SMTP). If required, restrict access to a whitelist of known, trusted IP addresses.

High Priority:
4. **Enforce MFA:** Immediately implement and require MFA for all user accounts, especially for email access (e.g., Office 365, Google Workspace) and computer logins.
5. **Implement DMARC:** Create a DMARC record with a starting policy of `p=none` to begin monitoring, with the goal of moving to `p=quarantine` and ultimately `p=reject`.
6. **Strengthen SPF:** Change the SPF record from a soft-fail (`~all`) to a hard-fail (`-all`) to instruct receiving servers to reject mail from unauthorized sources.

Medium Priority:
7. **Develop Policies:** Establish and distribute a formal Employee Acceptable Use Policy.
8. **Implement Security Training:** Institute a mandatory security awareness training program for all new hires and conduct annual refresher training for all employees.

8. Conclusion
G.A.S. Inc. is currently operating with a critically low level of cybersecurity read

iness. The combination of an insecure network perimeter, weak email protections, and a lack of fundamental user security controls and policies places the organization at an imminent risk of a significant security breach. The recommendations outlined in t his report, particularly the immediate closure of exposed RDP and other insecure por ts, must be addressed urgently to protect the organization's data, finances, and rep utation.

Prepared by:
Cybersecurity Assessment Team
October 14, 2025

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample2_pdf_markdown.html")
```

✅ Successfully exported HTML: pro_sample2_pdf_markdown.html

In [31]:
```
response = flashModel.generate_content(contents=[prompt_text, context2_text + "\n"
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.

Date: October 14, 2025

---

1. Overview

This report provides an assessment of the cybersecurity posture of G.A.S. Inc. based on a review of technical information (DNS records, DMARC status, and external port scans) and self-reported answers to a security questionnaire. The findings indicate significant vulnerabilities and a low level of cybersecurity readiness across several critical areas, necessitating immediate attention and remediation.

2. Organizational Information

*   **Organization Name:** G.A.S. Inc.
*   **Email Domain:** gasinc.net
*   **Website Domain:** www.gasinc.net
*   **External IP:** 104.28.1.189
*   **DNS Hosting:** Self-managed (dns1.gasinc.net, dns2.gasinc.net)
*   **Email Hosting:** Mailhostbox (mx.mailhostbox.com)

3. Security Questionnaire Review

The security questionnaire reveals critical gaps in foundational security practices within G.A.S. Inc.

Security Control	Status	Notes
MFA for Email	❌ No	**Critical Weakness:** Lack of MFA for email significantly increases phishing risk.
MFA for Computer Login	❌ No	**Critical Weakness:** Lack of MFA for computer access increases risk of unauthorized access.
MFA for Sensitive Systems	✅ Yes	**Strength:** MFA is required for sensitive data systems.
Employee Acceptable Use Policy	❌ No	**Weakness:** Absence of a policy leaves the organization vulnerable to misuse and lacks clear guidelines.
New Employee Security Awareness Training	❌ No	**Weakness:** New hires are not onboarded with essential security knowledge.
Annual All-Employee Security Training	❌ No	**Weakness:** Employees lack regular reinforcement of security best practices.

Summary: G.A.S. Inc. demonstrates a significant lack of essential security controls related to user authentication, employee behavior policies, and security awareness training. The only reported strength is the use of MFA for sensitive data systems, which is positive but insufficient given the other deficiencies.

4. DNS & Email Security

DNS Records
*   The organization's DNS is managed by what appear to be internal nameservers (dns1.gasinc.net, dns2.gasinc.net). While this offers direct control, it requires robust security measures to prevent DNS compromise.

*   The `A` record for `gasinc.net` points to `104.28.1.189`, which is the organization's external IP and the target of the port scans.

MX Records (Email)
*   Email services are hosted by Mailhostbox, as indicated by the MX records: `10 mx.mailhostbox.com.` and `20 mx2.mailhostbox.com.`.

SPF Record (Sender Policy Framework)
*   An SPF record exists: `v=spf1 include:spf.mailhostbox.com ~all`.
*   **Weakness:** The `~all` (softfail) mechanism allows mail from unauthorized servers to be delivered but marked as suspicious. A stronger policy, such as `-all` (hardfail), is recommended to prevent email spoofing more effectively.

DMARC Record (Domain-based Message Authentication, Reporting & Conformance)
*   **Critical Weakness:** The DMARC DNS lookup resulted in `NXDOMAIN`, meaning no DMARC record is configured for `gasinc.net`. This is a severe vulnerability as it leaves the organization completely exposed to email spoofing, phishing, and business email compromise (BEC) attacks. Without DMARC, G.A.S. Inc. has no control over how receiving mail servers should handle unauthenticated emails purporting to be from its domain, nor does it receive reports on such activities.

Conclusion: G.A.S. Inc.'s email security posture is poor due to the absence of a DMARC record and a weak SPF policy. This significantly increases the risk of successful phishing and spoofing attacks targeting the organization's reputation and employees.

5. Port Scanning Results

A port scan of the external IP address `104.28.1.189` (which hosts the website and serves as the organization's external network gateway) revealed multiple open and high-risk services directly exposed to the internet.

Port	Service	Risk Level	Notes
21	FTP	**High**	File Transfer Protocol (FTP) is inherently insecure, transmitting credentials and data in plaintext. It's a common target for unauthorized access.
22	SSH	**Medium**	Secure Shell (SSH) allows remote command execution. While secure if properly configured, broad exposure makes it a target for brute-force attacks.
25	SMTP	**Medium**	Simple Mail Transfer Protocol. While necessary for email, it usually only needs to be open to trusted relays or for outbound traffic. Exposing it directly to the internet if not a dedicated mail server is risky.
80	HTTP	Low (Expected)	Standard port for unencrypted web traffic. Typically redirects to HTTPS.
110	POP3	**High**	Post Office Protocol version 3 is an insecure mail retrieval protocol that transmits credentials in plaintext. It should be replaced by IMAP/S or POP3/S.
443	HTTPS	Low (Expected)	Standard port for encrypted web traffic. Essential for secure website communication.
3389	RDP	**Critical**	Remote Desktop Protocol (RDP) directly exposed to

the internet is a severe vulnerability, a primary vector for ransomware, brute-forc
e, and credential theft attacks. |

Summary: The exposure of FTP, POP3, and RDP services directly on the external IP
represents a critical network security failing. These services are frequent targets
for attackers and offer direct access points into the organization's network, potent
ially leading to data breaches, system compromise, and ransomware infections. SSH an
d SMTP exposure also present elevated risks if not meticulously secured.

6. Risk Assessment & Readiness Summary

| Category | Status | Notes
|
| :---------- | :---------- | :----------
---------- |
| **Authentication Security** | **Weak** | Lack of MFA for email and computer log
ins, offset only partially by MFA for sensitive systems. This makes user accounts hi
ghly susceptible to compromise. |
| **Email Security** | **Weak** | Absence of DMARC and a softfail SPF record
(`~all`) makes the organization vulnerable to email spoofing and phishing attacks, e
roding trust and increasing operational risk. |
| **Network Exposure** | **Critical**| Direct exposure of high-risk services (FT
P, POP3, RDP) to the internet creates a wide-open gateway for attackers, severely co
mpromising perimeter security. |
| **Web Hosting** | **Moderate**| Standard web ports (80/443) are open. The
risk is elevated by the presence of other highly vulnerable services on the same ext
ernal IP. |
| **Policy & Training** | **Weak** | Complete absence of an Acceptable Use Poli
cy and any form of security awareness training for employees, leaving a significant
human factor vulnerability. |

7. Recommendations

Given the critical findings, G.A.S. Inc. must take immediate and decisive action to
improve its cybersecurity posture.

Immediate & Critical Actions (Within 24-72 hours):

1. **Close Unnecessary Ports:** Immediately close ports 21 (FTP), 110 (POP3), and 3
389 (RDP) on `104.28.1.189`. If these services are absolutely necessary:
    *   **RDP (3389):** Implement a VPN for all remote access or restrict access to
specific, trusted source IP addresses. Never expose RDP directly to the internet.
    *   **FTP (21) & POP3 (110):** Disable these insecure protocols. Migrate to SFT
P/SCP (port 22 with strong SSH configuration), or use secure email protocols like IM
APS (993) or POP3S (995) *only if necessary* and with strong authentication.
    *   **SSH (22):** If SSH is required, implement key-based authentication, disabl
e password authentication, restrict access to specific IP addresses, change the defa
ult port, and use strong, unique passphrases.
    *   **SMTP (25):** Ensure port 25 is only open to necessary Mailhostbox servers
or an internal mail relay.

2. **Implement DMARC:** Configure a DMARC record for `gasinc.net` with at least a `
p=quarantine` policy, if not `p=reject`, to protect against email spoofing. Monitor
DMARC reports regularly.

```
3.  **Strengthen SPF:** Change the SPF record from `~all` (softfail) to `-all` (hard
fail) to ensure that emails from unauthorized senders are rejected.

**High-Priority Actions (Within 1-2 months):**

4.  **Implement MFA Broadly:**
    *   Require Multi-Factor Authentication (MFA) for all email accounts.
    *   Require MFA for all employee computer logins.

5.  **Develop & Enforce Security Policies:**
    *   Create and disseminate an employee Acceptable Use Policy (AUP).
    *   Develop policies for remote access, password management, and data handling.

6.  **Conduct Security Awareness Training:**
    *   Implement mandatory security awareness training for all new employees.
    *   Establish an annual mandatory security awareness training program for all ex
isting employees, covering topics like phishing, social engineering, password hygien
e, and incident reporting.

**Ongoing Improvements:**

7.  **Vulnerability Management:** Implement a regular schedule for internal and exte
rnal vulnerability scans and penetration testing.
8.  **Incident Response Plan:** Develop and regularly test a comprehensive cybersecu
rity incident response plan and disaster recovery procedures.
9.  **DNS Security Review:** Review the security posture of the self-managed DNS nam
eservers. Consider moving to a managed DNS service for increased resilience and secu
rity if internal resources are limited.

### 8. Conclusion

G.A.S. Inc. currently exhibits a **low to critical cybersecurity readiness**. The di
rect exposure of highly vulnerable services on its external IP, coupled with the abs
ence of fundamental email authentication (DMARC) and critical organizational securit
y policies and training, places the organization at extreme risk of cyberattacks, da
ta breaches, and business disruption.

**Urgent and comprehensive remediation** of the identified vulnerabilities and imple
mentation of the recommended security controls are imperative to protect G.A.S. In
c.'s assets, data, and reputation.

---
**Prepared by:** Cybersecurity Assessment Team
**Date:** October 14, 2025
```

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample2_pdf_markdown.html")
```

✅ Successfully exported HTML: flash_sample2_pdf_markdown.html

In [33]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context2_text + "
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.

Date: October 14, 2025

1. Overview

This report assesses the cybersecurity readiness of G.A.S. Inc. based on the provide
d DNS, port scan results, and answers to a security questionnaire. The findings indi
cate several critical areas of vulnerability and a lack of fundamental security cont
rols, suggesting a low level of cybersecurity readiness.

2. Organizational Information

*   **Organization Name:** G.A.S. Inc.
*   **Email Domain:** gasinc.net
*   **Website Domain:** www.gasinc.net
*   **External IP (Firewall):** 104.28.1.189
*   **Website Hosting IP:** 104.28.1.189

3. Security Questionnaire Review

| Security Control | Status | Notes
|
| :--- | :--- | :---
--- |
| MFA to access email? | No | Critical vulnerability. Lack
of MFA for email significantly increases the risk of account compromise.
|
| MFA to log into computers? | No | Critical vulnerability. With
out MFA for computer logins, any compromised credentials can lead to full system acc
ess. |
| MFA to access sensitive data systems? | Yes | Positive control, but its ef
fectiveness is diminished by the lack of MFA on email and general computer logins.
|
| Employee acceptable use policy? | No | Significant gap. An AUP is f
oundational for setting user expectations and defining responsible technology use.
|
| Security awareness training for new employees? | No | Critical gap. New employ
ees are often prime targets for social engineering. Lack of training leaves them unp
repared. |
| Security awareness training for all employees annually? | No | Critical gap. C
ybersecurity threats evolve constantly. Regular training is essential to keep employ
ees informed and vigilant. |

Summary: G.A.S. Inc. demonstrates a significant lack of fundamental cybersecurit
y controls. The absence of Multi-Factor Authentication (MFA) for email and general c
omputer logins, coupled with no acceptable use policy and no security awareness trai
ning, creates a highly vulnerable environment.

4. DNS & Email Security

DNS Records:

*   The `gasinc.net` domain has A records pointing to `104.28.1.189`.
*   MX records are configured for `gasinc.net`, directing mail to `mx.mailhostbox.co

m` and `mx2.mailhostbox.com`. This indicates an external email hosting provider is b
eing used.
*   A TXT record for SPF is present: `"v=spf1 include:spf.mailhostbox.com ~all"`. Th
is is a positive step in helping to prevent email spoofing.

DMARC Record:

*   The `_dmarc.gasinc.net` query returned an `NXDOMAIN` (Non-Existent Domain) erro
r. This means no DMARC record is configured.

Conclusion: While SPF is present, the lack of a DMARC record is a significant ov
ersight. DMARC, when implemented with SPF and DKIM (which is not confirmed here but
is a common pairing), provides a robust defense against email spoofing and phishing.
The absence of a DMARC record leaves the organization exposed to these threats.

5. Port Scanning Results

Website Hosting (104.28.1.189):

*   Port 80 (HTTP): Open
*   Port 443 (HTTPS): Open

These ports are expected for a publicly accessible website.

Firewall / External IP (104.28.1.189):

*   Port 21 (FTP): Open
*   Port 22 (SSH): Open
*   Port 25 (SMTP): Open
*   Port 80 (HTTP): Open
*   Port 110 (POP3): Open
*   Port 443 (HTTPS): Open
*   Port 3389 (RDP): Open

Conclusion: The firewall scan reveals a disturbingly high number of open ports e
xposed to the internet. This includes ports commonly associated with file transfer
(FTP), remote access (SSH, RDP), email services (SMTP, POP3), and web services (HTT
P, HTTPS). Each open port represents a potential attack vector. The exposure of port
3389 (RDP) is particularly concerning, as it is a frequent target for brute-force at
tacks and exploitation if not secured with strong credentials and MFA.

6. Risk Assessment & Readiness Summary

| Category | Status | Notes
|
| :------------------ | :----- | :--

-- |
| Authentication | Low | Critical vulnerabilities due to the absence of MFA
for email and general computer logins. Sensitive data access has MFA, but the overal
l security is compromised. |
| Email Security | Medium | SPF is configured, which is good. However, the lac
k of a DMARC record significantly weakens defenses against phishing and spoofing.
|
| Network Exposure | Low | Critical vulnerabilities. A large number of ports
are open on the external firewall, creating a broad attack surface. RDP (3389) being

open is a significant risk. |
| Policy & Training | Low | Critical gaps. No acceptable use policy and no security awareness training for any employees leave the organization and its users highly susceptible to human error and social engineering attacks. |
| Website Security | Moderate | Standard web ports (80, 443) are open, which is expected. However, without further information, it's impossible to assess the security of the web application itself. |

7. Recommendations

G.A.S. Inc. is at a **low level of cybersecurity readiness** and requires immediate and significant improvements. The following recommendations are critical:

1. **Implement Multi-Factor Authentication (MFA) Everywhere:**
    * Immediately enforce MFA for all email accounts.
    * Enforce MFA for all user logins to computers and company devices.
    * Ensure strong, unique passwords are also enforced.

2. **Develop and Enforce an Acceptable Use Policy (AUP):**
    * Create a comprehensive AUP that clearly outlines acceptable and prohibited uses of company IT resources.
    * Ensure all employees read, understand, and sign the AUP.

3. **Establish a Robust Security Awareness Training Program:**
    * Implement mandatory security awareness training for all new employees.
    * Conduct annual (at a minimum) security awareness training for all employees. This training should cover phishing, social engineering, password security, and safe browsing habits.

4. **Harden the Network Perimeter:**
    * **Review and restrict open ports:** Critically evaluate every open port on the external firewall. Close any ports that are not absolutely necessary for business operations.
    * **Secure RDP:** If RDP access is required, it must be secured with MFA, strong passwords, and ideally accessed via a VPN rather than directly exposed to the internet. Consider disabling RDP from the public internet entirely.
    * **Implement Network Segmentation:** If possible, segment the network to limit the blast radius of any potential breach.

5. **Configure DMARC:**
    * Implement a DMARC record for `gasinc.net`. Start with a monitoring mode (`p=none`) to analyze reports, then move to quarantine (`p=quarantine`) or reject (`p=reject`) as confidence grows.
    * Ensure DKIM is also configured and aligned with SPF and DMARC for comprehensive email authentication.

6. **Regular Vulnerability Scanning and Penetration Testing:**
    * Conduct regular external and internal vulnerability scans to identify weaknesses.
    * Consider periodic penetration testing to simulate real-world attacks.

7. **Review Email Hosting Security:**
    * While using an external provider is common, ensure G.A.S. Inc. understands the security responsibilities of their chosen email hosting provider (mailhostbox.com).

8. Conclusion

G.A.S. Inc. is currently operating with significant cybersecurity risks due to the absence of fundamental security controls. The open ports on the firewall and the lack of MFA and employee training are critical vulnerabilities that expose the organization to a high risk of data breaches, ransomware, and other cyberattacks. Immediate remediation of the recommended actions is essential to improve the organization's cybersecurity posture and protect its assets and reputation.

In [ ]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample2_pdf_markdown.html")
```

✅ Successfully exported HTML: flash_lite_sample2_pdf_markdown.html

In [47]:
```
# === SAMPLE 1 ===

#input PDF, output JSON
response = proModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

{
  "Overview": "This report provides a cybersecurity readiness assessment for Apex Innovations, based on a security questionnaire and technical scans of their public-facing infrastructure. The findings indicate strong internal security policies, including widespread MFA adoption and security training, coupled with excellent email security configurations. However, the external network perimeter shows open ports for HTTP and HTTPS on the primary external IP, suggesting a web server is directly exposed, which presents a notable area of risk.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External IP / Web Server IP: 72.21.196.160"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: Yes",
    "MFA for Computer Login: Yes",
    "MFA for Sensitive Systems: Yes",
    "Acceptable Use Policy: Yes",
    "New Employee Security Awareness Training: Yes",
    "Annual All-Employee Security Training: Yes",
    "Summary: The organization reports a strong commitment to fundamental security controls, mandating MFA across critical access points and maintaining a regular security training cadence for all employees. This demonstrates a mature approach to user-level security."
  ],
  "DNS & Email Security": [
    "SPF Record: A valid SPF record is in place ('v=spf1 include:spf.protection.outlook.com -all'), authorizing Microsoft Outlook as the sole email sender and instructing receivers to reject mail from other sources.",
    "DMARC Record: A strong DMARC policy is implemented ('v=DMARC1; p=reject; ...'), which protects against domain spoofing by instructing email providers to reject unauthenticated emails.",
    "MX Records: Mail Exchange (MX) records are configured for 'mx1.apexinnovations.com' and 'mx2.apexinnovations.com', consistent with an on-premise or dedicated mail server setup that uses Microsoft's protection services.",
    "Conclusion: Email security is well-configured and follows best practices, significantly reducing the risk of phishing and email-based impersonation attacks."
  ],
  "Port Scanning Results": [
    "External IP / Web Server (72.21.196.160):",
    "Port 80 (HTTP): Open",
    "Port 443 (HTTPS): Open",
    "Summary: The scan reveals that the organization's primary external IP address is also serving web content. While these ports are necessary for a website, having them open on the main corporate firewall IP increases the attack surface. It is positive that no other services are exposed."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Strong. The mandatory use of MFA across email, computers, and sensitive systems greatly reduces the risk of unauthorized access.",
    "Email Security: Strong. The implementation of SPF and a 'reject' DMARC policy provides robust protection against email spoofing.",
    "Policy & Training: Strong. The existence of an acceptable use policy and annual security training indicates a high level of security awareness.",
    "Network Exposure: Moderate Risk. The web server is exposed on the primary exter

```
nal IP. While only standard web ports are open, any vulnerability on this server cou
ld potentially provide a gateway into the internal network."
  ],
  "Recommendations": [
    "1. Enforce HTTPS: Implement a permanent redirect (301) from HTTP (Port 80) to H
TTPS (Port 443) on the web server to ensure all visitor traffic is encrypted.",
    "2. Network Segmentation: If the web server is hosted on-premise, ensure it is p
roperly isolated in a Demilitarized Zone (DMZ) to prevent a potential compromise fro
m affecting the internal corporate network.",
    "3. Regular Vulnerability Scanning: Conduct regular, authenticated vulnerability
scans of the web server (72.21.196.160) to identify and remediate security flaws in
a timely manner.",
    "4. Implement DKIM: While SPF and DMARC are in place, ensure DomainKeys Identifi
ed Mail (DKIM) is also configured for the 'apexinnovations.com' domain to further st
rengthen email authentication.",
    "5. Develop an Incident Response Plan: Create and regularly test an incident res
ponse plan to ensure a coordinated and effective response in the event of a security
breach."
  ],
  "Conclusion": "Apex Innovations has established a robust cybersecurity foundation
with excellent user authentication policies, security training programs, and email s
ecurity protocols. The primary area for improvement lies in managing their external
network exposure. By securing their web server and ensuring it is properly segmented
from the internal network, Apex Innovations can significantly enhance its overall se
curity posture and reduce its attack surface."
}
```

In [48]:

```
response = flashModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

{
  "Overview": "This report assesses the cybersecurity readiness of Apex Innovations, analyzing findings from DNS records, email security configurations, external port scans, and a self-reported security questionnaire. The organization demonstrates a strong foundational security posture with robust user authentication, comprehensive email protection, and a well-managed network perimeter, alongside strong policy and training adherence.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External IP (Website/Firewall): 72.21.196.160",
    "DNS Management: apexinnovations.com (based on SOA and NS records)"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: Yes",
    "MFA for Computer Login: Yes",
    "MFA for Sensitive Data Systems: Yes",
    "Employee Acceptable Use Policy: Yes",
    "New Employee Security Awareness Training: Yes",
    "Annual All-Employee Security Training: Yes",
    "Summary: Apex Innovations reports full compliance with foundational security practices, including multi-factor authentication (MFA) across critical access points and regular security awareness training, indicating a strong policy-driven security culture."
  ],
  "DNS & Email Security": [
    "DNS Records:",
    " DNS is managed by Apex Innovations (ns1.apexinnovations.com, ns2.apexinnovations.com).",
    " A record points to 72.21.196.160, matching the reported External IP, indicating the primary web presence is hosted here.",
    "MX Records (Email):",
    " Email services are configured via mx1.apexinnovations.com and mx2.apexinnovations.com.",
    " SPF record: \"v=spf1 include:spf.protection.outlook.com -all\". This is well-configured, using Outlook.com for email protection and a strict -all policy to prevent spoofing.",
    "DMARC Record:",
    " A valid DMARC record is present with a p=reject policy: \"v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\". This provides strong protection against email impersonation and phishing attempts.",
    "Conclusion: DNS and email security configurations (SPF, DMARC with reject policy) are robust and align with best practices, offering excellent protection against email-based threats."
  ],
  "Port Scanning Results": [
    "Scanning Target (External IP / Website): 72.21.196.160",
    "Open Ports:",
    " Port 80 (HTTP): Open",
    " Port 443 (HTTPS): Open",
    "Analysis: The port scans for both the external IP and the website yielded identical results, indicating that the website is directly accessible via the organization's primary external IP, or through a firewall that exposes only these two ports. The presence of HTTP (80) and HTTPS (443) is expected for a public website. No other unexpected ports were found open, suggesting a well-secured perimeter for the main I

```
P."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Strong (MFA required across email, computer login, sen
sitive systems).",
    "Email Security: Strong (SPF and DMARC with \"reject\" policy implemented, using
Outlook protection).",
    "Network Exposure: Secure (Only essential web ports 80 and 443 are open on the e
xternal IP; no other services exposed).",
    "Policy & Training: Comprehensive (Acceptable use policies and regular security
awareness training in place)."
  ],
  "Recommendations": [
    "1. Enforce HTTPS Redirection: Ensure all HTTP (Port 80) traffic is automaticall
y redirected to HTTPS (Port 443) to guarantee encrypted communication for all websit
e visitors.",
    "2. Regular Vulnerability Scanning: Conduct regular internal and external vulner
ability assessments of the web server and other network devices to identify and reme
diate potential weaknesses proactively.",
    "3. Security Logging and Monitoring: Implement comprehensive logging and monitor
ing solutions for network traffic, server access, and security events to detect and
respond to potential threats in real-time.",
    "4. Web Application Firewall (WAF): Consider deploying a WAF in front of the web
server (72.21.196.160) to provide an additional layer of protection against common w
eb-based attacks.",
    "5. Review Custom MX Records: While the SPF and DMARC are strong, review the use
of custom MX records (mx1/mx2.apexinnovations.com) to ensure they are properly secur
ed and redundant, especially as SPF points to Outlook.com. Confirm the mail flow arc
hitecture."
  ],
  "Conclusion": "Apex Innovations exhibits a commendable cybersecurity posture, part
icularly in its commitment to strong authentication, robust email security, and cont
rolled network exposure. The organization's adherence to security policies and emplo
yee training further strengthens its defenses. By addressing the recommendations for
continuous improvement, Apex Innovations can maintain and further enhance its overal
l cybersecurity readiness."
}
```


In [49]:

```
response = flashLiteModel.generate_content(
    contents=[prompt_text, context1_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
```

```
    }
)
print(response.text)
```

```
{
  "Overview": "This report evaluates the cybersecurity posture of Apex Innovations b
ased on technical scans (DNS, DMARC, and port scanning) and a self-reported security
questionnaire. The findings indicate a strong implementation of foundational securit
y controls, particularly concerning authentication, email security, and staff awaren
ess.",
  "Organizational Information": [
    "Organization Name: Apex Innovations",
    "Email Domain: apexinnovations.com",
    "Website Domain: www.apexinnovations.com",
    "External IP (Firewall): 72.21.196.160",
    "Website Hosting IP: 72.21.196.160"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: Yes",
    "MFA for Computer Login: Yes",
    "MFA for Sensitive Data Systems: Yes",
    "Acceptable Use Policy: Yes",
    "New Employee Security Awareness Training: Yes",
    "Annual All-Employee Security Training: Yes",
    "Summary: Apex Innovations reports a high level of security maturity, with manda
tory MFA across critical systems and comprehensive security awareness training progr
ams. This suggests a proactive approach to mitigating insider threats and unauthoriz
ed access."
  ],
  "DNS & Email Security": [
    "DNS Records:",
    "The domain apexinnovations.com has A records pointing to 72.21.196.160, NS reco
rds for ns1.apexinnovations.com and ns2.apexinnovations.com, and MX records pointing
to mx1.apexinnovations.com and mx2.apexinnovations.com. This indicates a standard DN
S configuration.",
    "SPF Record: The TXT record for apexinnovations.com contains 'v=spf1 include:sp
f.protection.outlook.com -all'. This is a correct SPF configuration, indicating the
use of Microsoft 365 for email and helping to prevent email spoofing.",
    "DMARC Record: The _dmarc.apexinnovations.com record shows 'v=DMARC1; p=reject;
rua=mailto:dmarc_reports@apexinnovations.com; fo=1'. This is a strong DMARC policy,
instructing receiving servers to reject emails that fail DMARC checks, significantly
enhancing email security and preventing phishing.",
    "Conclusion: DNS and email security configurations, including SPF and DMARC, are
robust and align with best practices for preventing email-based threats."
  ],
  "Port Scanning Results": [
    "External IP Scan (72.21.196.160): Port 80 (HTTP) and Port 443 (HTTPS) are open.
Other ports were not specified as open.",
    "Website Scan (72.21.196.160): Port 80 (HTTP) and Port 443 (HTTPS) are open. Thi
s is expected for a publicly accessible website.",
    "Summary: The external IP and website expose only standard web ports (80 and 44
3), indicating a well-configured firewall that limits the attack surface. No unneces
sary services appear to be exposed to the internet."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Strong. Multi-Factor Authentication (MFA) is mandated
for email, computer logins, and sensitive data systems, significantly reducing the r
isk of account compromise.",
    "Email Security: Strong. Correctly configured SPF and a 'reject' policy DMARC re
cord provide excellent protection against email spoofing and phishing.",
```

```
    "Network Exposure: Secure. Only standard web ports (80 and 443) are open on the
external IP and website, indicating effective firewall rules.",
    "Policy & Training: Comprehensive. The organization has an acceptable use policy
and conducts regular security awareness training for all employees, fostering a secu
rity-conscious culture.",
    "Overall Readiness: Apex Innovations demonstrates a high level of cybersecurity
readiness due to strong authentication controls, robust email security measures, and
a commitment to employee training."
  ],
  "Recommendations": [
    "Review Firewall Rules: Regularly review and audit firewall rules to ensure only
necessary ports are open and to detect any unauthorized changes.",
    "Implement Intrusion Detection/Prevention Systems (IDPS): Consider deploying IDP
S solutions to monitor network traffic for malicious activity.",
    "Regular Vulnerability Assessments: Conduct periodic vulnerability assessments a
nd penetration testing to proactively identify and address potential weaknesses in t
he infrastructure.",
    "Develop an Incident Response Plan: Formalize and test an incident response plan
to ensure a swift and effective reaction to security breaches.",
    "Enhance Logging and Monitoring: Implement comprehensive logging across systems
and establish monitoring to detect suspicious activities in real-time."
  ],
  "Conclusion": "Apex Innovations exhibits a strong cybersecurity posture, underpinn
ed by robust authentication, effective email security measures, and a culture of sec
urity awareness cultivated through training and policies. The limited exposure of ne
twork services further strengthens its defense. Continued diligence in regularly rev
iewing security configurations and implementing advanced threat detection mechanisms
will ensure sustained security maturity."
}
```


In [51]:

```python
# === SAMPLE 2 ===

#input PDF, output JSON
response = proModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report assesses the cybersecurity readiness of G.A.S. Inc. based on a security questionnaire and external network scans. The assessment reveals criti cal deficiencies in fundamental security controls, including user authentication, em ail security, network perimeter defense, and employee security awareness. The organi zation currently has a very high-risk security posture and requires immediate action to mitigate significant vulnerabilities.",
  "Organizational Information": [
    "Organization Name: G.A.S. Inc.",
    "Email Domain: gasinc.net",
    "Website Domain: www.gasinc.net",
    "External IP: 104.28.1.189"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: No - CRITICAL RISK. Lack of MFA on email exposes the organizatio n to business email compromise and phishing attacks.",
    "MFA for Computer Login: No - CRITICAL RISK. This significantly increases the ri sk of unauthorized access to endpoints and internal network resources.",
    "MFA for Sensitive Systems: Yes - POSITIVE. However, the security benefit is dim inished by the lack of MFA on email and computers, which are often entry points.",
    "Employee Acceptable Use Policy: No - HIGH RISK. Without a policy, there are no clear guidelines for employees on the safe and acceptable use of company assets.",
    "Security Awareness Training: No - HIGH RISK. The absence of training for new or existing employees makes the organization highly susceptible to social engineering a nd phishing attacks."
  ],
  "DNS & Email Security": [
    "SPF Record: A valid SPF record exists ('v=spf1 include:spf.mailhostbox.com ~al l'), but it is configured with a softfail (~all) instead of a hardfail (-all). This reduces its effectiveness in preventing email spoofing.",
    "DMARC Record: No DMARC record was found (NXDOMAIN). This is a CRITICAL vulnerab ility, as it leaves the organization's domain unprotected against sophisticated emai l spoofing and phishing campaigns.",
    "DKIM: DKIM status could not be determined from the provided data, but it should be implemented alongside SPF and DMARC for comprehensive email authentication."
  ],
  "Port Scanning Results": [
    "External IP (104.28.1.189) Scan: CRITICAL RISK. Numerous high-risk ports are ex posed directly to the internet:",
    "Port 21 (FTP): Open. Unencrypted file transfer protocol, insecure.",
    "Port 22 (SSH): Open. Secure Shell, a primary target for brute-force attacks.",
    "Port 25 (SMTP): Open. Simple Mail Transfer Protocol, can be exploited for spam relay.",
    "Port 110 (POP3): Open. Unencrypted email protocol.",
    "Port 3389 (RDP): Open. Remote Desktop Protocol, a major vector for ransomware a ttacks.",
    "Ports 80 (HTTP) & 443 (HTTPS): Open. Expected for a web server, but the other o pen ports indicate this IP is likely a misconfigured multi-purpose server or firewal l."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication Security: Very Poor. Lack of MFA for email and computer access i s a critical failure.",
    "Email Security: Very Poor. The absence of DMARC and a weak SPF configuration le ave the primary communication channel vulnerable to spoofing.",
    "Network Exposure: Critical. The high number of exposed, high-risk services (FT
```

```
P, SSH, RDP) on the external IP address presents an immediate and severe threat of c
ompromise.",
    "Policy & Training: Non-Existent. The lack of basic policies and security awaren
ess training indicates a low level of security maturity and high susceptibility to h
uman error."
  ],
  "Recommendations": [
    "IMMEDIATE: Close all unnecessary ports on the external firewall (104.28.1.189),
especially ports 21, 22, 25, 110, and 3389. If remote access is required, it must be
secured behind a VPN.",
    "IMMEDIATE: Implement mandatory Multi-Factor Authentication (MFA) for all user a
ccess to email and computer logins.",
    "URGENT: Create and implement a DMARC record for gasinc.net, starting with a mon
itoring policy (p=none) and progressing to a quarantine or reject policy (p=rejec
t).",
    "URGENT: Strengthen the SPF record by changing the qualifier from `~all` (softfa
il) to `-all` (fail).",
    "Develop and enforce an Employee Acceptable Use Policy that outlines rules for t
echnology use.",
    "Establish a mandatory security awareness training program for all employees upo
n hiring and at least annually thereafter."
  ],
  "Conclusion": "G.A.S. Inc. exhibits a critically weak cybersecurity posture. The c
ombination of an exposed network perimeter with multiple insecure services, inadequa
te email security, and a complete lack of MFA and employee training places the organ
ization at an extremely high risk of a significant security breach, such as a ransom
ware attack or business email compromise. The recommendations outlined in this repor
t should be treated as urgent priorities to establish a baseline level of security a
nd protect critical assets."
}
```

In [52]:
```python
response = flashModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

{
"Overview": "This report evaluates the cybersecurity posture of G.A.S. Inc. based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings indicate several critical vulnerabilities and a general lack of foundational cybersecurity practices, posing a significant risk to the organization's data and operations.",
"Organizational Information": [
"Organization Name: G.A.S. Inc.",
"Email Domain: gasinc.net",
"Website Domain: www.gasinc.net",
"External IP: 104.28.1.189"
],
"Security Questionnaire Review": [
"MFA for Email Access: No (Critical Weakness - Leaves email accounts vulnerable to credential theft)",
"MFA for Computer Login: No (Critical Weakness - Increases risk of unauthorized access to internal systems)",
"MFA for Sensitive Data Systems: Yes (Strength - Essential for protecting high-value assets)",
"Employee Acceptable Use Policy: No (Major Weakness - Lack of clear guidelines for employee behavior)",
"New Employee Security Awareness Training: No (Major Weakness - New employees are unprepared for common cyber threats)",
"Annual All-Employee Security Training: No (Major Weakness - Employees are not regularly updated on evolving threats and best practices)",
"Summary: G.A.S. Inc. demonstrates significant gaps in fundamental security controls related to multi-factor authentication for common access points, security policies, and employee training. While MFA for sensitive systems is a positive, the widespread absence of other controls creates a high-risk environment."
],
"DNS & Email Security": [
"Email Domain: gasinc.net",
"MX Records (Email): The domain uses mailhostbox.com for email hosting (mx.mailhostbox.com, mx2.mailhostbox.com).",
"SPF Record: A Sender Policy Framework (SPF) record is present: \"v=spf1 include:spf.mailhostbox.com ~all\". This record helps to prevent email spoofing by authorizing specific senders. However, the '~all' (softfail) policy is less restrictive than '-all' (hardfail), allowing some spoofed emails to potentially be delivered.",
"DMARC Record: No DMARC record was found (_dmarc.gasinc.net returned NXDOMAIN). This is a critical vulnerability. Without DMARC, G.A.S. Inc.'s email domain is highly susceptible to impersonation and phishing attacks, as there is no policy to instruct receiving mail servers on how to handle unauthenticated mail."
],
"Port Scanning Results": [
"Scanning Target: 104.28.1.189",
"Open Ports Identified:",
"Port 21 (FTP): Open - File Transfer Protocol is often insecure, transmitting credentials in cleartext. High risk.",
"Port 22 (SSH): Open - Secure Shell access should be tightly restricted to known IP addresses and use strong authentication (e.g., key-based, MFA). Direct exposure is a significant risk.",
"Port 25 (SMTP): Open - Simple Mail Transfer Protocol. While necessary for mail servers, direct exposure can lead to spam, unauthorized relaying, or vulnerabilities if not properly secured.",
"Port 80 (HTTP): Open - Standard for unencrypted web traffic. Expected for a website, but should redirect to HTTPS.",

"Port 110 (POP3): Open - Post Office Protocol version 3 is a legacy email retrieval protocol that often transmits credentials in cleartext. High risk.",
"Port 443 (HTTPS): Open - Standard for encrypted web traffic. Expected for a secure website.",
"Port 3389 (RDP): Open - Remote Desktop Protocol provides graphical interface to a server. Direct exposure is a critical vulnerability, making the system a prime target for brute-force attacks and unauthorized access.",
"Summary: The external IP (104.28.1.189) has numerous high-risk ports open to the public internet, including FTP, SSH, POP3, and RDP. This indicates a severely exposed network perimeter, significantly increasing the attack surface and the likelihood of a successful breach. Many of these services are inherently insecure or should only be accessible via a VPN or strict IP whitelisting."
],
"Risk Assessment & Readiness Summary": [
"Authentication Security: Poor - Lack of MFA for email and computer logins leaves critical access points vulnerable.",
"Email Security: Critical - Absence of a DMARC record and a softfail SPF policy make the domain highly susceptible to spoofing and phishing.",
"Network Exposure: Critical - Numerous high-risk ports (FTP, SSH, POP3, RDP) are open to the internet, creating severe opportunities for attackers.",
"Policy & Training: Absent - No acceptable use policy and no security awareness training leave employees unprepared and unprotected.",
"Overall Readiness: G.A.S. Inc. has a low cybersecurity readiness. There are critical vulnerabilities across multiple domains, from user authentication and email security to network perimeter protection and employee awareness. The organization is at a very high risk of cyberattack and data breach."
],
"Recommendations": [
"1. Implement Multi-Factor Authentication (MFA): Immediately enforce MFA for all email access and computer logins to prevent unauthorized access even if credentials are stolen.",
"2. Secure Network Perimeter: Review and close all unnecessary open ports on 104.28.1.189. Specifically, disable or restrict access to Ports 21 (FTP), 22 (SSH), 25 (SMTP), 110 (POP3), and 3389 (RDP). For essential services, implement strict firewall rules (IP whitelisting) or require VPN access.",
"3. Enhance Email Security: Publish a DMARC record with an enforcing policy (e.g., 'p=quarantine' or 'p=reject') to prevent email impersonation. Consider hardening the SPF record to '-all' after verifying all legitimate sending sources.",
"4. Develop and Implement Security Policies: Create and enforce an Employee Acceptable Use Policy (AUP) to define expected behaviors and security requirements for all employees.",
"5. Conduct Security Awareness Training: Implement mandatory security awareness training for all new employees and annual refresher training for all staff. This should cover topics like phishing, social engineering, password hygiene, and data handling.",
"6. Regular Vulnerability Scanning: Perform regular vulnerability scans and penetration tests on all internet-facing assets to identify and address weaknesses proactively.",
"7. Secure Email Protocols: Ensure all email clients are configured to use secure protocols like IMAPS/POP3S/SMTPS (ports 993/995/465) instead of insecure POP3/SMTP (ports 110/25) for retrieving and sending mail."
],
"Conclusion": "G.A.S. Inc. faces significant cybersecurity challenges due to widespread vulnerabilities in authentication, email protection, network perimeter, and security awareness. The current posture indicates a high level of risk to organizational assets and data. Immediate and comprehensive action on the recommendations is crucia

```
l to mitigate these risks and establish a more robust cybersecurity defense."
}
```

In [53]:

```
response = flashLiteModel.generate_content(
    contents=[prompt_text, context2_text + "\n" + example_text],
    generation_config={
        'response_mime_type': 'application/json',
        'response_schema': {
            'type':'object',
            'properties': {
                'Overview': {'type': 'string'},
                'Organizational Information': {'type': 'array', 'items': {'type': '
                'Security Questionnaire Review': {'type': 'array', 'items': {'type'
                'DNS & Email Security': {'type': 'array', 'items': {'type': 'string
                'Port Scanning Results': {'type': 'array', 'items': {'type': 'strin
                'Risk Assessment & Readiness Summary': {'type': 'array', 'items': {
                'Recommendations': {'type': 'array', 'items': {'type': 'string'}},
                'Conclusion': {'type': 'string'},
            },
            'required': ['Overview', 'Organizational Information', 'Security Questi
        }
    }
)
print(response.text)
```

```
{
  "Overview": "This report assesses the cybersecurity readiness of G.A.S. Inc. based on provided DNS, port scanning, and security questionnaire data. The findings highlight areas of strength and areas requiring immediate attention to improve the organization's overall security posture.",
  "Organizational Information": [
    "Organization Name: G.A.S. Inc.",
    "Email Domain: gasinc.net",
    "Website Domain: www.gasinc.net",
    "External IP Address (Firewall): 104.28.1.189"
  ],
  "Security Questionnaire Review": [
    "MFA for Email: No",
    "MFA for Computer Login: No",
    "MFA for Sensitive Data Systems: Yes",
    "Acceptable Use Policy: No",
    "Security Awareness Training (New Employees): No",
    "Security Awareness Training (Annual): No",
    "Summary: The organization lacks fundamental security controls such as MFA for email and computer logins, an acceptable use policy, and regular security awareness training for employees. This presents significant risks related to account compromise, data breaches, and insider threats."
  ],
  "DNS & Email Security": [
    "DNS Records for gasinc.net: The 'ANY' query shows an SOA record indicating management by dns1.gasinc.net and NS records for dns1.gasinc.net and dns2.gasinc.net. An A record points to 104.28.1.189, and MX records are configured for mx.mailhostbox.com and mx2.mailhostbox.com. An SPF record is present: \"v=spf1 include:spf.mailhostbox.com ~all\".",
    "DMARC Record for gasinc.net: The DMARC query for _dmarc.gasinc.net resulted in NXDOMAIN (Non-Existent Domain), indicating that no DMARC record is published. This is a critical gap in email security.",
    "Email Security Conclusion: While SPF is configured, the absence of a DMARC record leaves the email system vulnerable to spoofing and phishing attacks. The use of mailhostbox.com for email services is noted."
  ],
  "Port Scanning Results": [
    "External IP Scan (104.28.1.189): Ports 21 (FTP), 22 (SSH), 25 (SMTP), 80 (HTTP), 110 (POP3), 443 (HTTPS), and 3389 (RDP) were found to be open. This wide range of open ports on the external perimeter increases the attack surface.",
    "Website Scan (104.28.1.189): Ports 80 (HTTP) and 443 (HTTPS) are open, which is expected for a web server."
  ],
  "Risk Assessment & Readiness Summary": [
    "Authentication: Weak. Lack of MFA for email and computer logins significantly increases the risk of account compromise.",
    "Email Security: Moderate to Weak. SPF is present, but the absence of DMARC is a critical vulnerability.",
    "Network Exposure: High Risk. Numerous ports (FTP, SSH, SMTP, POP3, RDP) are open on the external IP, presenting a large attack surface.",
    "Policy & Training: Very Weak. Absence of an acceptable use policy and any form of security awareness training leaves the organization highly susceptible to social engineering and policy violations.",
    "Overall Readiness: Low. The combination of missing foundational security controls, lack of policies, inadequate training, and a broad network attack surface indicates a low level of cybersecurity readiness."
```

```
  ],
  "Recommendations": [
    "Implement Multi-Factor Authentication (MFA): Enforce MFA for all email account
s, computer logins, and access to sensitive data systems.",
    "Publish a DMARC Record: Implement a DMARC record for the 'gasinc.net' domain to
protect against email spoofing and phishing.",
    "Review and Harden Firewall Rules: Close all unnecessary open ports on the exter
nal IP address (104.28.1.189). Specifically, restrict access to or disable ports lik
e FTP (21), SSH (22), SMTP (25), POP3 (110), and RDP (3389) unless absolutely requir
ed and properly secured.",
    "Develop and Implement an Acceptable Use Policy: Create a formal policy outlinin
g acceptable use of company IT resources.",
    "Establish Security Awareness Training Programs: Implement mandatory security aw
areness training for all new and existing employees, covering topics such as phishin
g, password security, and safe internet practices.",
    "Review Email Service Provider Security: Ensure the security practices of 'mailh
ostbox.com' align with G.A.S. Inc.'s security requirements."
  ],
  "Conclusion": "G.A.S. Inc. exhibits significant cybersecurity weaknesses across mu
ltiple critical areas, including authentication, email security, network exposure, a
nd organizational policies. The lack of basic security controls and training poses a
substantial risk. Immediate implementation of the recommendations, particularly MFA,
DMARC, and firewall hardening, is crucial to mitigate these risks and improve the or
ganization's cybersecurity posture."
}
```

In [ ]:

```python
prompt_text = 'Prompt:\nGiven this DNS DIG, Port scan of the website, Port scan of

context1_text = 'Context:\n'
context2_text = 'Context:\n'
example_text = 'Example:\n' + prompt_text

filepaths = ["report_template/test_questionnaire.json", "report_template/test_port_
pdfFile = "report_template/test_report.pdf"

sample1_filepaths = ["report_sample1/sample1_questionnaire.json", "report_sample1/s
sample2_filepaths = ["report_sample2/sample2_questionnaire.json", "report_sample2/s

for file in filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            example_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

example_text += extract_text_from_pdf(pdfFile)

print("=======  Example ==========")
print(example_text)
print("==========================")
```

```python
for file in sample1_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context1_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 1 =========")
print(prompt_text)
print(context1_text)
print("==========================")

for file in sample2_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context2_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 2 =========")
print(prompt_text)
print(context2_text)
print("==========================")
```

======= Example ==========
Example:
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization. Output plain text plus TeX only.template/test_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Valier School District",
    "Email Domain": "valier.k12.mt.us",
    "Website Domain": "www.valier.k12.mt.us",
    "External IP": "216.220.16.170",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
--
template/test_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
220.16.170\nScanning started at:2025-07-18 22:12:17.055226\n-----------------------
--------------------------\nno ports open\n"
}
--
template/test_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
239.32.21\nScanning started at:2025-07-18 22:09:34.408091\n-------------------------
------------------------\nPort 80 is open\nPort 443 is open\n"
}
--
template/test_dns_dig_email.json:
{
  "text": "id 49113\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\nvalier.
k12.mt.us. IN ANY\n;ANSWER\nvalier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-reque
st.umt.edu. 2024030501 21600 900 1209600 86400\nvalier.k12.mt.us. 3600 IN NS ens-o1.
umt.edu.\nvalier.k12.mt.us. 3600 IN NS cudess2.umt.edu.\nvalier.k12.mt.us. 3600 IN N
S cudess1.umt.edu.\nvalier.k12.mt.us. 3600 IN A 216.239.38.21\nvalier.k12.mt.us. 360
0 IN A 216.239.32.21\nvalier.k12.mt.us. 3600 IN A 216.239.34.21\nvalier.k12.mt.us. 3
600 IN A 216.239.36.21\nvalier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.\nvalier.k
12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 10 aspm
x3.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.\nvalier.
k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.\nvalier.k12.mt.us. 3600 IN TXT \"v=
spf1 include:_spf.google.com include:mg.infinitecampus.org -all\"\n;AUTHORITY\n;ADDI
TIONAL\n"
}
--
template/test_dns_dig_email_dmarc.json:
{
  "text": "id 45565\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
```

valier.k12.mt.us. IN ANY\n;ANSWER\n_dmarc.valier.k12.mt.us. 3600 IN TXT \"v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us\"\n;AUTHORITY\n;ADDITIONAL\n"
}
--

Cybersecurity Readiness Report for Valier School District Date: July 18, 2025

1. Overview

This report evaluates the cybersecurity posture of Valier School District based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings reflect a strong commitment to foundational cybersecurity practices across user access, email protection, network exposure, and staff awareness.

2. Organizational Information

● Organization Name: Valier School District ● Email Domain: valier.k12.mt.us ● Website Domain: www.valier.k12.mt.us ● External IP (Firewall): 216.220.16.170 ● Website Hosting IPs: 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21 ● DNS Hosting: Managed by University of Montana (umt.edu nameservers)

3. Security Questionnaire Review Security Control Status

MFA for Email ✅ Yes
MFA for Computer Login ✅ Yes
MFA for Sensitive Systems ✅ Yes
Acceptable Use Policy ✅ Yes
New Employee Security Awareness Training ✅ Yes
Annual All-Employee Security Training ✅ Yes

Summary: The district reports complete implementation of basic cyber hygiene practices, especially
user authentication (Multi-Factor Authentication) and routine training. This indicates a proactive and policy-driven approach to risk mitigation.

4. DNS & Email Security

DNS Records

● DNS is managed by the University of Montana (cudess1.umt.edu, cudess2.umt.edu), suggesting centralized and professionally administered DNS. ● A records point to IPs within Google's network (likely Google Sites hosting for web content).

MX Records (Email)

● The district uses Google Workspace (Gmail) for email, as shown by multiple aspmx.l.google.com MX records. ● SPF record is correctly configured: v=spf1 include:_spf.google.com include:mg.infinitecampus.org -all This helps mitigate spoofing by defining authorized mail senders.

DMARC Record

● A valid DMARC record exists with a reject policy: v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us This instructs receiving servers to reject unauthenticated mail, providing strong protection against phishing.

Conclusion: DNS and email protections (SPF, DMARC, and hosting security) are configured correctly and follow best practices.

5. Port Scanning Results

Website Hosting (Google IP: 216.239.32.21)

● Port 80 (HTTP): Open ● Port 443 (HTTPS): Open These are expected for a publicly accessible website and are typical for Google-hosted services.

Firewall / External IP (216.220.16.170)

● All scanned ports are closed This is a strong sign of network perimeter hardening and good firewall configuration. No externally exposed servic

es were found on the organization’s primary IP.

6. Risk Assessment & Readiness Summary Category Status Notes
Authentication Security ✅ Strong MFA is required across key systems
Email Security ✅ Strong SPF and DMARC with “reject” policy in place
Network Exposure ✅ Secure No exposed services on the external firewall IP
Web Hosting ✅ Secure Google-hosted; limited attack surface
Policy & Training ✅ Comprehensive Acceptable use policies and regular tr aining in place

7. Recommendations
Although the cybersecurity readiness is solid, continuous improvement is es sential. We recommend the following:
1. Verify DKIM : While SPF and DMARC are configured, ensure DKIM is also active for all sending domains. 2. Vulnerability Scanning : Consider regul ar internal and external vulnerability assessments of network devices and servers. 3. Incident Response Plan : Document and regularly test a cybers ecurity incident response and disaster recovery plan. 4. Asset Inventory : Maintain a regularly updated inventory of hardware/software assets and moni tor for unauthorized changes. 5. Third-party Risk : Evaluate vendors (e. g., Infinite Campus) for their security posture, especially since they're included in SPF.

8. Conclusion
Valier School District demonstrates a strong cybersecurity foundation, parti cularly in authentication, email protection, staff training, and perimeter security. Continued vigilance and regular audits will help maintain and im prove this strong security posture.

Prepared by: Cybersecurity Assessment Team Date: July 18, 2025

==========
======== Sample 1 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans wers to the security questionnaire, write a report on the cybersecurity readiness of the organization. Output plain text plus TeX only.
Context:
sample1/sample1_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Apex Innovations",
    "Email Domain": "apexinnovations.com",
    "Website Domain": "www.apexinnovations.com",
    "External IP": "72.21.196.160",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
```

```
}
--
sample1/sample1_dns_dig_email_dmarc.json:
{
  "text": "id 31890\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
apexinnovations.com. IN ANY\n;ANSWER\n_dmarc.apexinnovations.com. 3600 IN TXT \"v=DM
ARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\""
}
--
sample1/sample1_dns_dig_email.json:
{
  "text": "id 52417\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\napexinn
ovations.com. IN ANY\n;ANSWER\napexinnovations.com. 3600 IN SOA ns1.apexinnovations.
com. hostmaster.apexinnovations.com. 2025101401 21600 3600 604800 3600\napexinnovati
ons.com. 3600 IN NS ns1.apexinnovations.com.\napexinnovations.com. 3600 IN NS ns2.ap
exinnovations.com.\napexinnovations.com. 3600 IN A 72.21.196.160\napexinnovations.co
m. 3600 IN MX 10 mx1.apexinnovations.com.\napexinnovations.com. 3600 IN MX 20 mx2.ap
exinnovations.com.\napexinnovations.com. 3600 IN TXT \"v=spf1 include:spf.protectio
n.outlook.com -all\""
}
--
sample1/sample1_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:09:42.589112\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--
sample1/sample1_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:08:15.223456\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
======== Sample 2 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization. Output plain text plus TeX only.
Context:
sample2/sample2_questionnaire.json:
{
  "text": {
    "Organization Name": "G.A.S. Inc.",
    "Email Domain": "gasinc.net",
    "Website Domain": "www.gasinc.net",
    "External IP": "104.28.1.189",
    "Do you require MFA to access email?": "No",
    "Do you require MFA to log into computers?": "No",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "No",
    "Does your organization do security awareness training for new employees?": "N
o",
```

```
    "Does your organization do security awareness training for all employees at leas
t once per year?": "No"
  }
}
--
sample2/sample2_dns_dig_email_dmarc.json:
{
  "text": "id 28911\nopcode QUERY\nrcode NXDOMAIN\nflags QR AA RD RA\n;QUESTION\n_dm
arc.gasinc.net. IN ANY\n;AUTHORITY\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmas
ter.gasinc.net. 2025101402 14400 3600 604800 3600\n;ADDITIONAL"
}
--
sample2/sample2_dns_dig_email.json:
{
  "text": "id 47123\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\ngasinc.
net. IN ANY\n;ANSWER\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmaster.gasinc.ne
t. 2025101402 14400 3600 604800 3600\ngasinc.net. 3600 IN NS dns1.gasinc.net.\ngasin
c.net. 3600 IN NS dns2.gasinc.net.\ngasinc.net. 3600 IN A 104.28.1.189\ngasinc.net.
3600 IN MX 10 mx.mailhostbox.com.\ngasinc.net. 3600 IN MX 20 mx2.mailhostbox.com.\ng
asinc.net. 3600 IN TXT \"v=spf1 include:spf.mailhostbox.com ~all\""
}
--
sample2/sample2_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:16:11.890123\n-------------------------
-------------------------\nPort 21 is open\nPort 22 is open\nPort 25 is open\nPort 8
0 is open\nPort 110 is open\nPort 443 is open\nPort 3389 is open"
}
--
sample2/sample2_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:15:30.456789\n-------------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
```


In [9]:
```python
# === SAMPLE 1 ===

# input PDF, output LaTeX
response = proModel.generate_content(contents=[prompt_text, context1_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations
Date: October 14, 2025

1. Overview
This report provides an assessment of the cybersecurity readiness of Apex Innovation s, based on a combination of a self-reported security questionnaire and external tec hnical scans, including DNS record analysis and network port scanning. The evaluatio n indicates a mature and robust security posture, with strong controls implemented a cross email security, user authentication, and network perimeter defense.

2. Organizational Information
- Organization Name: Apex Innovations
- Email Domain: apexinnovations.com
- Website Domain: www.apexinnovations.com
- External IP / Web Host: 72.21.196.160
- DNS Hosting: Self-hosted (ns1.apexinnovations.com, ns2.apexinnovations.com)
- Email Service Provider: Microsoft 365 (as per SPF record)

3. Security Questionnaire Review
Security Control	Status
MFA for Email	Yes
MFA for Computer Login	Yes
MFA for Sensitive Systems	Yes
Acceptable Use Policy	Yes
New Employee Security Awareness Training	Yes
Annual All-Employee Security Training	Yes

Summary: Apex Innovations reports complete adherence to fundamental cybersecurity po licies. The mandatory implementation of Multi-Factor Authentication (MFA) for all cr itical access points, combined with a comprehensive security awareness training prog ram, signifies a strong, policy-driven commitment to mitigating risk.

4. DNS & Email Security
- SPF Record: The organization has a correctly configured SPF record: "v=spf1 includ e:spf.protection.outlook.com -all". The use of "-all" (Hard Fail) is a best practice that helps prevent email spoofing by strictly defining authorized sending sources.
- DMARC Record: A strong DMARC policy is in place: "v=DMARC1; p=reject; rua=mailto:d marc_reports@apexinnovations.com; fo=1". The "p=reject" policy instructs receiving e mail servers to reject messages that fail authentication, providing excellent protec tion against phishing and domain impersonation attacks.
- DNS and MX Records: The organization manages its own DNS and mail exchange (MX) se rvers. This configuration, paired with the use of a secure third-party provider (Mic rosoft 365) for email delivery, demonstrates a well-architected and secure email inf rastructure.

Conclusion: The email security configuration for apexinnovations.com is excellent an d aligns with modern best practices, providing strong defenses against common email-based threats.

5. Port Scanning Results
- Website / External IP (72.21.196.160):
  - Port 80 (HTTP): Open
  - Port 443 (HTTPS): Open
- Summary: The external network scan of the organization's primary IP address shows that only standard web service ports are open. This indicates a properly configured

firewall that limits the external attack surface, adhering to the principle of least privilege.

6. Risk Assessment & Readiness Summary
Category	Status	Notes
Authentication Security	Strong	MFA is consistently required across the organization.
Email Security	Strong	SPF and DMARC are implemented with a strict "reject" policy.
Network Exposure	Secure	Minimal services are exposed; only standard web ports are open.
Policy & Training	Comprehensive	Foundational policies and regular training programs are in place.

7. Recommendations
While Apex Innovations exhibits a strong security posture, the following recommendations are made for continuous improvement:
1. Implement a Web Application Firewall (WAF): Since the organization hosts its own website, a WAF would provide critical protection against application-layer attacks like SQL injection and cross-site scripting.
2. Verify DKIM Implementation: To complete the email authentication triad (SPF, DKIM, DMARC), ensure that DKIM is correctly configured for all authorized sending services.
3. Conduct Regular Vulnerability Scanning: For all self-hosted infrastructure (web server, DNS), perform regular vulnerability assessments to identify and remediate potential security weaknesses before they can be exploited.
4. Develop and Test an Incident Response Plan: Formalize a comprehensive incident response plan and conduct regular tabletop exercises to ensure the organization can respond effectively to a security breach.

8. Conclusion
Apex Innovations demonstrates a high level of cybersecurity readiness. The organization has successfully implemented critical controls for authentication, email security, and network defense. By focusing on the continuous improvement of its self-hosted services and formalizing response procedures, Apex Innovations can further enhance its already robust security posture.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025

```
\documentclass{article}
\usepackage[utf8]{inputenc}
\usepackage{geometry}
\geometry{a4paper, margin=1in}
\usepackage{array}
\usepackage{tabularx}
\usepackage{hyperref}
\usepackage{listings}
\lstset{
  basicstyle=\small\ttfamily,
  breaklines=true,
}

\title{Cybersecurity Readiness Report for Apex Innovations}
```

```
\author{Cybersecurity Assessment Team}
\date{October 14, 2025}

\begin{document}

\maketitle

\section*{1. Overview}
This report provides an assessment of the cybersecurity readiness of Apex Innovation
s, based on a combination of a self-reported security questionnaire and external tec
hnical scans, including DNS record analysis and network port scanning. The evaluatio
n indicates a mature and robust security posture, with strong controls implemented a
cross email security, user authentication, and network perimeter defense.

\section*{2. Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name:} Apex Innovations
    \item \textbf{Email Domain:} apexinnovations.com
    \item \textbf{Website Domain:} www.apexinnovations.com
    \item \textbf{External IP / Web Host:} 72.21.196.160
    \item \textbf{DNS Hosting:} Self-hosted (ns1.apexinnovations.com, ns2.apexinnova
tions.com)
    \item \textbf{Email Service Provider:} Microsoft 365 (as per SPF record)
\end{itemize}

\section*{3. Security Questionnaire Review}
\begin{table}[h!]
\centering
\begin{tabular}{|l|c|}
\hline
\textbf{Security Control} & \textbf{Status} \\
\hline
MFA for Email & Yes \\
MFA for Computer Login & Yes \\
MFA for Sensitive Systems & Yes \\
Acceptable Use Policy & Yes \\
New Employee Security Awareness Training & Yes \\
Annual All-Employee Security Training & Yes \\
\hline
\end{tabular}
\end{table}

\textbf{Summary:} Apex Innovations reports complete adherence to fundamental cyberse
curity policies. The mandatory implementation of Multi-Factor Authentication (MFA) f
or all critical access points, combined with a comprehensive security awareness trai
ning program, signifies a strong, policy-driven commitment to mitigating risk.

\section*{4. DNS \& Email Security}
\begin{itemize}
    \item \textbf{SPF Record:} The organization has a correctly configured SPF recor
d: \texttt{"v=spf1 include:spf.protection.outlook.com -all"}. The use of \texttt{-al
l} (Hard Fail) is a best practice that helps prevent email spoofing by strictly defi
ning authorized sending sources.
    \item \textbf{DMARC Record:} A strong DMARC policy is in place: \texttt{"v=DMARC
1; p=reject; rua=mailto:dmarc\_reports@apexinnovations.com; fo=1"}. The \texttt{p=re
ject} policy instructs receiving email servers to reject messages that fail authenti
```

```
cation, providing excellent protection against phishing and domain impersonation att
acks.
    \item \textbf{DNS and MX Records:} The organization manages its own DNS and mail
exchange (MX) servers. This configuration, paired with the use of a secure third-par
ty provider (Microsoft 365) for email delivery, demonstrates a well-architected and
secure email infrastructure.
\end{itemize}

\textbf{Conclusion:} The email security configuration for apexinnovations.com is exc
ellent and aligns with modern best practices, providing strong defenses against comm
on email-based threats.

\section*{5. Port Scanning Results}
\begin{itemize}
    \item \textbf{Website / External IP (72.21.196.160):}
    \begin{itemize}
        \item Port 80 (HTTP): Open
        \item Port 443 (HTTPS): Open
    \end{itemize}
    \item \textbf{Summary:} The external network scan of the organization's primary
IP address shows that only standard web service ports are open. This indicates a pro
perly configured firewall that limits the external attack surface, adhering to the p
rinciple of least privilege.
\end{itemize}

\section*{6. Risk Assessment \& Readiness Summary}
\begin{table}[h!]
\centering
\begin{tabularx}{\textwidth}{|l|X|X|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication Security & Strong & MFA is consistently required across the organizat
ion. \\
\hline
Email Security & Strong & SPF and DMARC are implemented with a strict "reject" polic
y. \\
\hline
Network Exposure & Secure & Minimal services are exposed; only standard web ports ar
e open. \\
\hline
Policy \& Training & Comprehensive & Foundational policies and regular training prog
rams are in place. \\
\hline
\end{tabularx}
\end{table}

\section*{7. Recommendations}
While Apex Innovations exhibits a strong security posture, the following recommendat
ions are made for continuous improvement:
\begin{enumerate}
    \item \textbf{Implement a Web Application Firewall (WAF):} Since the organizatio
n hosts its own website, a WAF would provide critical protection against application
-layer attacks like SQL injection and cross-site scripting.
    \item \textbf{Verify DKIM Implementation:} To complete the email authentication
triad (SPF, DKIM, DMARC), ensure that DKIM is correctly configured for all authorize
```

```
d sending services.
    \item \textbf{Conduct Regular Vulnerability Scanning:} For all self-hosted infra
structure (web server, DNS), perform regular vulnerability assessments to identify a
nd remediate potential security weaknesses before they can be exploited.
    \item \textbf{Develop and Test an Incident Response Plan:} Formalize a comprehen
sive incident response plan and conduct regular tabletop exercises to ensure the org
anization can respond effectively to a security breach.
\end{enumerate}

\section*{8. Conclusion}
Apex Innovations demonstrates a high level of cybersecurity readiness. The organizat
ion has successfully implemented critical controls for authentication, email securit
y, and network defense. By focusing on the continuous improvement of its self-hosted
services and formalizing response procedures, Apex Innovations can further enhance i
ts already robust security posture.

\end{document}
```

In [10]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample1_pdf_latex.html")
```

✅ Successfully exported HTML: pro_sample1_pdf_latex.html

In [11]:
```
response = flashModel.generate_content(contents=[prompt_text, context1_text + "\n"
print(response.text)
```

```
Cybersecurity Readiness Report for Apex Innovations
Date: October 14, 2025

1. Overview
This report provides an evaluation of Apex Innovations' cybersecurity posture, deriv
ed from a security questionnaire, DNS records analysis (including DMARC), and extern
al port scans of their public-facing infrastructure. The organization demonstrates a
robust foundational security stance across critical areas such as user authenticatio
n, email protection, and employee awareness, with a well-managed external network pr
esence.

2. Organizational Information
\begin{itemize}
    \item Organization Name: Apex Innovations
    \item Email Domain: apexinnovations.com
    \item Website Domain: www.apexinnovations.com
    \item External IP (Website/Firewall): 72.21.196.160
\end{itemize}

3. Security Questionnaire Review
Apex Innovations reports a comprehensive adoption of key cybersecurity policies and
practices:
\begin{center}
\begin{tabular}{|l|l|}
\hline
\textbf{Security Control} & \textbf{Status} \\
\hline
MFA for Email Access & \(\checkmark\) Yes \\
\hline
MFA for Computer Login & \(\checkmark\) Yes \\
\hline
MFA for Sensitive Data Systems & \(\checkmark\) Yes \\
\hline
Employee Acceptable Use Policy & \(\checkmark\) Yes \\
\hline
New Employee Security Awareness Training & \(\checkmark\) Yes \\
\hline
Annual All-Employee Security Training & \(\checkmark\) Yes \\
\hline
\end{tabular}
\end{center}
Summary: The organization has implemented crucial controls for user authentication
(Multi-Factor Authentication), acceptable use, and ongoing security awareness traini
ng. This indicates a strong commitment to managing human risk factors and enforcing
security policies.

4. DNS & Email Security
DNS Records
\begin{itemize}
    \item The primary A record for apexinnovations.com resolves to 72.21.196.160, ma
tching the external IP identified in port scans.
    \item Name Servers (NS) are ns1.apexinnovations.com and ns2.apexinnovations.com,
suggesting self-managed DNS or a provider managing DNS on their behalf with custom n
ameservers.
\end{itemize}
```

MX Records (Email)
\begin{itemize}
    \item MX records (mx1.apexinnovations.com, mx2.apexinnovations.com) indicate email services are handled by Apex Innovations' infrastructure or a dedicated provider.
    \item SPF record is correctly configured: \texttt{v=spf1 include:spf.protection.outlook.com -all}. This record explicitly authorizes Microsoft 365 (Outlook.com) as a legitimate sender for Apex Innovations' email and uses a strict \texttt{-all} policy to reject unauthorized senders, significantly reducing email spoofing risks.
\end{itemize}

DMARC Record
\begin{itemize}
    \item A valid DMARC record is present with a strong enforcement policy: \texttt{v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1}. The \texttt{p=reject} policy instructs receiving mail servers to reject messages that fail DMARC authentication, offering robust protection against phishing and brand impersonation. The \texttt{rua} tag ensures DMARC reports are sent to the organization for monitoring.
\end{itemize}
Conclusion: Apex Innovations demonstrates an excellent email security posture, with correctly configured SPF and DMARC records (using a reject policy), leveraging a reputable email service provider (Microsoft 365).

5. Port Scanning Results
Website / External IP (72.21.196.160)
\begin{itemize}
    \item Port 80 (HTTP): Open
    \item Port 443 (HTTPS): Open
\end{itemize}
These ports are typically open for a publicly accessible website, indicating that Apex Innovations is hosting web services on this IP address. The consistent results from both "port_scan_external_ip" and "port_scan_web" confirm that the external IP is directly associated with the website. While these ports are necessary for web presence, the security of the web server and application behind them is crucial.

6. Risk Assessment & Readiness Summary
\begin{center}
\begin{tabular}{|l|l|l|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication Security & \(\checkmark\) Strong & MFA is required for email, computer login, and sensitive data systems. \\
\hline
Email Security & \(\checkmark\) Strong & Comprehensive SPF and DMARC with a "reject" policy implemented, leveraging Microsoft 365. \\
\hline
Network Exposure & \(\triangle\) Moderate & Ports 80 and 443 are open for web services. This is expected but requires vigilant security practices for the underlying web server and application. No other unnecessary ports appear to be open. \\
\hline
Web Hosting & \(\triangle\) Acceptable & Web services are exposed via HTTP/HTTPS. The security posture depends on the hardening and patching of the web server and web application. \\
\hline

```
Policy & \(\checkmark\) Comprehensive & Acceptable Use Policy is in place. \\
\hline
Training & \(\checkmark\) Comprehensive & Regular security awareness training for al
l employees. \\
\hline
\end{tabular}
\end{center}

7. Recommendations
While Apex Innovations exhibits a strong cybersecurity foundation, continuous improv
ement is vital. We recommend the following:
\begin{enumerate}
    \item \textbf{Web Application Security:} Given that ports 80 and 443 are open, i
mplement a Web Application Firewall (WAF) to protect against common web exploits. Co
nduct regular web application vulnerability scanning and penetration testing. Ensure
web servers are hardened, patched regularly, and configured securely.
    \item \textbf{Verify DKIM:} Although SPF and DMARC are robustly configured, ensu
re DomainKeys Identified Mail (DKIM) is also active for all sending email domains to
provide another layer of email authentication.
    \item \textbf{Incident Response Plan:} Develop, document, and regularly test a c
omprehensive cybersecurity incident response plan and disaster recovery procedures t
o ensure business continuity in the event of a breach.
    \item \textbf{Regular Vulnerability Assessments:} Conduct routine internal and e
xternal vulnerability assessments and penetration tests across the entire network in
frastructure, not just the web presence, to identify and remediate potential weaknes
ses.
    \item \textbf{Asset Inventory and Management:} Maintain a current, detailed inve
ntory of all hardware and software assets, and implement a robust patch management p
rogram to ensure all systems are up-to-date.
\end{enumerate}

8. Conclusion
Apex Innovations demonstrates a commendable level of cybersecurity readiness, partic
ularly in critical areas such as multi-factor authentication, email security, and em
ployee training. The organization's proactive stance on DMARC enforcement (\texttt{p
=reject}) and comprehensive policy framework are significant strengths. While networ
k exposure for web services is a necessary aspect of doing business, continuous vigi
lance and proactive measures for web application security will further enhance their
overall cybersecurity posture. Maintaining these strong practices and addressing the
recommendations will ensure the organization remains resilient against evolving cybe
r threats.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025
```

In [12]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample1_pdf_latex.html")
```

✅ Successfully exported HTML: flash_sample1_pdf_latex.html

In [13]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context1_text + "
print(response.text)
```

Cybersecurity Readiness Report for Apex Innovations
Date: October 14, 2025

---

1. Overview

This report evaluates the cybersecurity readiness of Apex Innovations based on provi
ded technical scan data (DNS, port scanning) and answers to a security questionnair
e. The assessment indicates a generally strong security posture with robust practice
s in place for authentication and email security, alongside necessary website access
ibility.

---

2. Organizational Information

*   **Organization Name:** Apex Innovations
*   **Email Domain:** apexinnovations.com
*   **Website Domain:** www.apexinnovations.com
*   **External IP (Firewall):** 72.21.196.160
*   **Website Hosting IP:** 72.21.196.160

---

3. Security Questionnaire Review

Security Control	Status
MFA to access email?	✅ Yes
MFA to log into computers?	✅ Yes
MFA to access sensitive data systems?	✅ Yes
Employee acceptable use policy?	✅ Yes
Security awareness training for new employees?	✅ Yes
Security awareness training for all employees at least once per year?	✅ Yes

Summary: Apex Innovations demonstrates a commendable commitment to fundamental c
ybersecurity practices. The mandatory use of Multi-Factor Authentication (MFA) acros
s email, computer logins, and sensitive data systems is a significant strength. The
presence of an acceptable use policy and regular security awareness training for all
employees, including new hires, indicates a proactive approach to user-related secur
ity risks.

---

4. DNS & Email Security

DNS Records for `apexinnovations.com`:
*   The domain's A record points to `72.21.196.160`, which is also identified as the
external IP and the web server.
*   MX records point to `mx1.apexinnovations.com` and `mx2.apexinnovations.com`, ind
icating that Apex Innovations manages its own mail servers or a dedicated mail relay
service.
*   The TXT record reveals an SPF configuration: `v=spf1 include:spf.protection.outl
ook.com -all`. This suggests that Apex Innovations utilizes Microsoft 365 for its em
ail services, and the SPF record is correctly configured to authorize Microsoft's se

rvers for sending email on behalf of the domain.

DMARC Record for `_dmarc.apexinnovations.com`:
*   A DMARC record is present: `v=DMARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1`.
*   The `p=reject` policy is a strong measure against email spoofing and phishing attempts, instructing receiving mail servers to reject emails that fail DMARC checks.
*   The `rua` tag indicates that DMARC aggregate reports are being sent to `dmarc_reports@apexinnovations.com`, which is crucial for monitoring and refining email authentication.
*   The `fo=1` flag indicates that reporting should occur if any alignment check fails, providing detailed feedback.

Conclusion: Apex Innovations has implemented strong email security measures with a properly configured SPF record pointing to Microsoft 365 and a robust DMARC policy set to `reject`. This significantly mitigates the risk of email-based attacks like phishing and spoofing.

---

5. Port Scanning Results

External IP (`72.21.196.160`) / Firewall:
*   Port 80 (HTTP) is open.
*   Port 443 (HTTPS) is open.
*   **Observation:** The external IP address, which is also associated with the website, reveals only standard web ports (HTTP and HTTPS) as open. This is expected for a publicly accessible website and suggests that the firewall is configured to allow only necessary traffic for web services. No other unnecessary ports appear to be exposed externally.

Website (`www.apexinnovations.com`):
*   Port 80 is open.
*   Port 443 is open.
*   **Observation:** Consistent with the external IP scan, the website is accessible via HTTP and HTTPS, which are the standard protocols for web browsing.

Conclusion: The external network perimeter appears to be well-secured, with only essential ports for web services exposed. This minimizes the attack surface available to external threats.

---

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	✅ Strong	Mandatory MFA for email, computer logins, and sensitive systems is excellent.
Email Security	✅ Strong	SPF and DMARC with a `reject` policy are effectively implemented, providing strong protection against email spoofing and phishing.
Network Exposure	✅ Secure	Only standard web ports (80, 443) are open o

n the external IP, indicating good firewall configuration and minimal attack surfac
e. |
| Web Hosting | ✅ Secure | Standard web ports are open, as expected for
a functional website.
|
| Policy & Training | ✅ Comprehensive | Acceptable use policy and regular sec
urity awareness training demonstrate a commitment to user education and adherence to
security standards. |

---

7. Recommendations

While Apex Innovations exhibits a strong cybersecurity posture, continuous improveme
nt is key. The following recommendations can further enhance their readiness:

1. **DKIM Implementation:** Ensure that DomainKeys Identified Mail (DKIM) is also c
onfigured and active for `apexinnovations.com`. While SPF and DMARC are in place, DK
IM adds another layer of email authentication, further strengthening email security
and preventing spoofing.
2. **Regular Vulnerability Scanning:** Implement a schedule for regular internal an
d external vulnerability scans of the external IP address and any other exposed infr
astructure. This helps identify and remediate potential weaknesses proactively.
3. **Incident Response Plan:** Develop and document a comprehensive incident respon
se plan. Regularly conduct tabletop exercises or simulations to test the plan's effe
ctiveness and ensure staff are prepared to handle security incidents.
4. **Security Patch Management:** Maintain a robust patch management process for al
l systems, including servers hosting the website and any internal systems that might
be indirectly exposed. Prompt patching of vulnerabilities is critical.

---

8. Conclusion

Apex Innovations demonstrates a high level of cybersecurity readiness. The organizat
ion has successfully implemented critical security controls, including mandatory MF
A, robust email authentication mechanisms (SPF and DMARC with a reject policy), and
a clear security awareness program. The limited exposure of network services on the
external perimeter further contributes to a strong security posture. By continuing t
o monitor security best practices and addressing the recommendations outlined above,
Apex Innovations can maintain and enhance its cybersecurity resilience.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025

```latex
\documentclass{article}
\usepackage{geometry}
\geometry{a4paper, margin=1in}
\usepackage{enumitem}
\usepackage{hyperref}
```

```
\usepackage{xcolor}

\hypersetup{
    colorlinks=true,
    linkcolor=blue,
    filecolor=magenta,
    urlcolor=cyan,
}

\title{Cybersecurity Readiness Report for Apex Innovations}
\author{Cybersecurity Assessment Team}
\date{October 14, 2025}

\begin{document}

\maketitle

\section{Overview}
This report evaluates the cybersecurity readiness of Apex Innovations based on provi
ded technical scan data (DNS, port scanning) and answers to a security questionnair
e. The assessment indicates a generally strong security posture with robust practice
s in place for authentication and email security, alongside necessary website access
ibility.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name:} Apex Innovations
    \item \textbf{Email Domain:} \href{mailto:apexinnovations.com}{apexinnovations.c
om}
    \item \textbf{Website Domain:} \href{https://www.apexinnovations.com}{www.apexin
novations.com}
    \item \textbf{External IP (Firewall):} 72.21.196.160
    \item \textbf{Website Hosting IP:} 72.21.196.160
\end{itemize}

\section{Security Questionnaire Review}
\begin{tabular}{|p{0.6\textwidth}|p{0.1\textwidth}|p{0.2\textwidth}|}
\hline
\textbf{Security Control} & \textbf{Status} & \textbf{Notes} \\
\hline
MFA to access email? & \textcolor{green}{\checkmark} Yes & \\
MFA to log into computers? & \textcolor{green}{\checkmark} Yes & \\
MFA to access sensitive data systems? & \textcolor{green}{\checkmark} Yes & \\
Employee acceptable use policy? & \textcolor{green}{\checkmark} Yes & \\
Security awareness training for new employees? & \textcolor{green}{\checkmark} Yes &
\\
Security awareness training for all employees at least once per year? & \textcolor{g
reen}{\checkmark} Yes & \\
\hline
\end{tabular}

\vspace{0.5em}
\textbf{Summary:} Apex Innovations demonstrates a commendable commitment to fundamen
tal cybersecurity practices. The mandatory use of Multi-Factor Authentication (MFA)
across email, computer logins, and sensitive data systems is a significant strength.
The presence of an acceptable use policy and regular security awareness training for
```

```
all employees, including new hires, indicates a proactive approach to user-related s
ecurity risks.

\section{DNS \& Email Security}

\subsection{DNS Records for \texttt{apexinnovations.com}}
\begin{itemize}
    \item The domain's A record points to \texttt{72.21.196.160}, which is also iden
tified as the external IP and the web server.
    \item MX records point to \texttt{mx1.apexinnovations.com} and \texttt{mx2.apexi
nnovations.com}, indicating that Apex Innovations manages its own mail servers or a
dedicated mail relay service.
    \item The TXT record reveals an SPF configuration: \texttt{v=spf1 include:spf.pr
otection.outlook.com -all}. This suggests that Apex Innovations utilizes Microsoft 3
65 for its email services, and the SPF record is correctly configured to authorize M
icrosoft's servers for sending email on behalf of the domain.
\end{itemize}

\subsection{DMARC Record for \texttt{\_dmarc.apexinnovations.com}}
\begin{itemize}
    \item A DMARC record is present: \texttt{v=DMARC1; p=reject; rua=mailto:dmarc\_r
eports@apexinnovations.com; fo=1}.
    \item The \texttt{p=reject} policy is a strong measure against email spoofing an
d phishing attempts, instructing receiving mail servers to reject emails that fail D
MARC checks.
    \item The \texttt{rua} tag indicates that DMARC aggregate reports are being sent
to \texttt{dmarc\_reports@apexinnovations.com}, which is crucial for monitoring and
refining email authentication.
    \item The \texttt{fo=1} flag indicates that reporting should occur if any alignm
ent check fails, providing detailed feedback.
\end{itemize}

\textbf{Conclusion:} Apex Innovations has implemented strong email security measures
with a properly configured SPF record pointing to Microsoft 365 and a robust DMARC p
olicy set to \texttt{reject}. This significantly mitigates the risk of email-based a
ttacks like phishing and spoofing.

\section{Port Scanning Results}

\subsection{External IP (\texttt{72.21.196.160}) / Firewall:}
\begin{itemize}
    \item Port 80 (HTTP) is open.
    \item Port 443 (HTTPS) is open.
    \item \textbf{Observation:} The external IP address, which is also associated wi
th the website, reveals only standard web ports (HTTP and HTTPS) as open. This is ex
pected for a publicly accessible website and suggests that the firewall is configure
d to allow only necessary traffic for web services. No other unnecessary ports appea
r to be exposed externally.
\end{itemize}

\subsection{Website (\texttt{www.apexinnovations.com}):}
\begin{itemize}
    \item Port 80 is open.
    \item Port 443 is open.
    \item \textbf{Observation:} Consistent with the external IP scan, the website is
accessible via HTTP and HTTPS, which are the standard protocols for web browsing.
```

```
\end{itemize}

\textbf{Conclusion:} The external network perimeter appears to be well-secured, with only essential ports for web services exposed. This minimizes the attack surface available to external threats.

\section{Risk Assessment \& Readiness Summary}
\begin{tabular}{|p{0.4\textwidth}|p{0.15\textwidth}|p{0.35\textwidth}|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication Security & \textcolor{green}{\textbf{Strong}} & Mandatory MFA for email, computer logins, and sensitive systems is excellent. \\
Email Security & \textcolor{green}{\textbf{Strong}} & SPF and DMARC with a \texttt{reject} policy are effectively implemented, providing strong protection against email spoofing and phishing. \\
Network Exposure & \textcolor{green}{\textbf{Secure}} & Only standard web ports (80, 443) are open on the external IP, indicating good firewall configuration and minimal attack surface. \\
Web Hosting & \textcolor{green}{\textbf{Secure}} & Standard web ports are open, as expected for a functional website. \\
Policy \& Training & \textcolor{green}{\textbf{Comprehensive}} & Acceptable use policy and regular security awareness training demonstrate a commitment to user education and adherence to security standards. \\
\hline
\end{tabular}

\section{Recommendations}
While Apex Innovations exhibits a strong cybersecurity posture, continuous improvement is key. The following recommendations can further enhance their readiness:
\begin{enumerate}
    \item \textbf{DKIM Implementation:} Ensure that DomainKeys Identified Mail (DKIM) is also configured and active for \texttt{apexinnovations.com}. While SPF and DMARC are in place, DKIM adds another layer of email authentication, further strengthening email security and preventing spoofing.
    \item \textbf{Regular Vulnerability Scanning:} Implement a schedule for regular internal and external vulnerability scans of the external IP address and any other exposed infrastructure. This helps identify and remediate potential weaknesses proactively.
    \item \textbf{Incident Response Plan:} Develop and document a comprehensive incident response plan. Regularly conduct tabletop exercises or simulations to test the plan's effectiveness and ensure staff are prepared to handle security incidents.
    \item \textbf{Security Patch Management:} Maintain a robust patch management process for all systems, including servers hosting the website and any internal systems that might be indirectly exposed. Prompt patching of vulnerabilities is critical.
\end{enumerate}

\section{Conclusion}
Apex Innovations demonstrates a high level of cybersecurity readiness. The organization has successfully implemented critical security controls, including mandatory MFA, robust email authentication mechanisms (SPF and DMARC with a reject policy), and a clear security awareness program. The limited exposure of network services on the external perimeter further contributes to a strong security posture. By continuing to monitor security best practices and addressing the recommendations outlined above, Apex Innovations can maintain and enhance its cybersecurity resilience.
```

```
\vfill

\textbf{Prepared by:} \\
Cybersecurity Assessment Team \\
\textbf{Date:} October 14, 2025

\end{document}
```

In [14]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample1_pdf_latex.html")
```

✅ Successfully exported HTML: flash_lite_sample1_pdf_latex.html

In [15]:
```
# === SAMPLE 2 ===

# input PDF, output LaTeX
response = proModel.generate_content(contents=[prompt_text, context2_text + "\n" +
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.
Date: October 14, 2025

1. Overview

This report provides an assessment of the cybersecurity readiness of G.A.S. Inc., based on a security questionnaire, DNS record analysis, and external network port scans. The findings reveal critical vulnerabilities across multiple domains, including network perimeter security, email authentication, user access controls, and security policy. These deficiencies place the organization at a high risk of significant cyber incidents, such as data breaches, ransomware attacks, and business email compromise.

2. Organizational Information

- Organization Name: G.A.S. Inc.
- Email Domain: gasinc.net
- Website Domain: www.gasinc.net
- External IP: 104.28.1.189

3. Security Questionnaire Review

The self-reported answers highlight fundamental gaps in security policies and controls.

Security Control	Status
MFA for Email	❌ No
MFA for Computer Login	❌ No
MFA for Sensitive Systems	✅ Yes
Acceptable Use Policy	❌ No
New Employee Security Awareness Training	❌ No
Annual All-Employee Security Training	❌ No

Summary: The absence of Multi-Factor Authentication (MFA) for email and computer access is a critical weakness, making user accounts highly susceptible to compromise through phishing or password theft. The lack of an acceptable use policy and any security awareness training indicates a low level of security maturity and leaves employees unprepared to identify and respond to threats.

4. DNS & Email Security

Analysis of the organization's DNS records for gasinc.net reveals major gaps in email security.

- SPF Record: The organization has an SPF record (`v=spf1 include:spf.mailhostbox.com ~all`). However, it uses a "~all" (SoftFail) qualifier, which instructs mail servers to accept but mark potentially forged emails. This is a weak policy that does not prevent spoofed emails from reaching inboxes.

- DMARC Record: A query for a DMARC record resulted in `NXDOMAIN`, indicating that no DMARC policy exists for the gasinc.net domain.

Conclusion: Without a DMARC record and with a weak SPF policy, G.A.S. Inc. is highly vulnerable to email spoofing. Attackers can easily send malicious emails that appear to originate from the company's domain, targeting employees, customers, and partners in phishing and fraud campaigns.

5. Port Scanning Results

A port scan of the primary external IP address (104.28.1.189) revealed numerous open ports, exposing critical services directly to the internet.

● Port 21 (FTP): Open. File Transfer Protocol is an unencrypted and insecure servic
e.
● Port 22 (SSH): Open. Secure Shell access, a common target for brute-force attacks.
● Port 25 (SMTP): Open. Simple Mail Transfer Protocol, can be abused if misconfigure
d.
● Port 80 (HTTP): Open. Standard for web traffic.
● Port 110 (POP3): Open. An unencrypted and outdated email retrieval protocol.
● Port 443 (HTTPS): Open. Standard for secure web traffic.
● Port 3389 (RDP): Open. Remote Desktop Protocol is a primary vector for ransomware
attacks.

Conclusion: The network perimeter is dangerously exposed. Open RDP, FTP, and POP3 po
rts represent an immediate and critical risk. Exposing these services without the pr
otection of a Virtual Private Network (VPN) or other access controls is a severe sec
urity misconfiguration.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication	❌ Weak	No MFA for email or computers creates a hig h risk of account compromise.
Email Security	❌ Critical Risk	No DMARC and a weak SPF policy allow for tr ivial email spoofing.
Network Exposure	❌ Critical Risk	Direct exposure of RDP, FTP, and other serv ices to the internet.
Policy & Training	❌ Weak	Absence of basic security policies and empl oyee training.

7. Recommendations
The following actions are recommended with the highest priority to address the ident
ified critical risks:

1. **Harden the Network Perimeter Immediately**:
    ● Close all unnecessary ports on the firewall, especially Port 3389 (RDP), Port
21 (FTP), and Port 110 (POP3).
    ● If remote access is required, implement a securely configured Virtual Private
Network (VPN) with MFA.

2. **Implement Mandatory Multi-Factor Authentication (MFA)**:
    ● Enforce MFA for all user access, starting with email accounts, computer login
s, and all remote access systems.

3. **Strengthen Email Authentication**:
    ● Update the SPF record to use a `-all` (HardFail) policy to prevent delivery of
unauthorized email.
    * Deploy a DMARC record, starting with a monitoring policy (`p=none`) and prog
ressing to a full rejection policy (`p=reject`).

4. **Establish a Security Program**:
    ● Develop and implement a formal Acceptable Use Policy for all employees.
    ● Institute mandatory cybersecurity awareness training for all new hires and con
duct annual refresher training for all staff.

8. Conclusion
G.A.S. Inc. currently has a critically deficient cybersecurity posture. The combinat
ion of an exposed network perimeter, inadequate email security, and weak authenticat

ion controls creates an environment highly susceptible to a successful cyberattack. The organization must take immediate and decisive action to implement the recommendations in this report to protect its data, assets, and reputation.

```
\documentclass{article}
\usepackage[utf8]{inputenc}
\usepackage{geometry}
\usepackage{array}
\usepackage{amssymb}
\geometry{a4paper, margin=1in}
\renewcommand{\familydefault}{\sfdefault}

\begin{document}

\title{Cybersecurity Readiness Report for G.A.S. Inc.}
\author{Cybersecurity Assessment Team}
\date{October 14, 2025}
\maketitle

\section*{1. Overview}
This report provides an assessment of the cybersecurity readiness of G.A.S. Inc., based on a security questionnaire, DNS record analysis, and external network port scans. The findings reveal critical vulnerabilities across multiple domains, including network perimeter security, email authentication, user access controls, and security policy. These deficiencies place the organization at a high risk of significant cyber incidents, such as data breaches, ransomware attacks, and business email compromise.

\section*{2. Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name:} G.A.S. Inc.
    \item \textbf{Email Domain:} gasinc.net
    \item \textbf{Website Domain:} www.gasinc.net
    \item \textbf{External IP:} 104.28.1.189
\end{itemize}

\section*{3. Security Questionnaire Review}
The self-reported answers highlight fundamental gaps in security policies and controls.

\begin{center}
\begin{tabular}{|l|c|}
\hline
\textbf{Security Control} & \textbf{Status} \\
\hline
MFA for Email & \text{\Large\bfseries ❌} No \\
MFA for Computer Login & \text{\Large\bfseries ❌} No \\
MFA for Sensitive Systems & \text{\Large\bfseries ✅} Yes \\
Acceptable Use Policy & \text{\Large\bfseries ❌} No \\
New Employee Security Awareness Training & \text{\Large\bfseries ❌} No \\
Annual All-Employee Security Training & \text{\Large\bfseries ❌} No \\
\hline
\end{tabular}
\end{center}
```

```
\textbf{Summary:} The absence of Multi-Factor Authentication (MFA) for email and com
puter access is a critical weakness, making user accounts highly susceptible to comp
romise through phishing or password theft. The lack of an acceptable use policy and
any security awareness training indicates a low level of security maturity and leave
s employees unprepared to identify and respond to threats.

\section*{4. DNS \& Email Security}
Analysis of the organization's DNS records for gasinc.net reveals major gaps in emai
l security.

\begin{itemize}
    \item \textbf{SPF Record:} The organization has an SPF record (\texttt{v=spf1 in
clude:spf.mailhostbox.com \textasciitilde all}). However, it uses a "\texttt{\textas
ciitilde all}" (SoftFail) qualifier, which instructs mail servers to accept but mark
potentially forged emails. This is a weak policy that does not prevent spoofed email
s from reaching inboxes.
    \item \textbf{DMARC Record:} A query for a DMARC record resulted in \texttt{NXDO
MAIN}, indicating that no DMARC policy exists for the gasinc.net domain.
\end{itemize}

\textbf{Conclusion:} Without a DMARC record and with a weak SPF policy, G.A.S. Inc.
is highly vulnerable to email spoofing. Attackers can easily send malicious emails t
hat appear to originate from the company's domain, targeting employees, customers, a
nd partners in phishing and fraud campaigns.

\section*{5. Port Scanning Results}
A port scan of the primary external IP address (104.28.1.189) revealed numerous open
ports, exposing critical services directly to the internet.

\begin{itemize}
    \item \textbf{Port 21 (FTP): Open.} File Transfer Protocol is an unencrypted and
insecure service.
    \item \textbf{Port 22 (SSH): Open.} Secure Shell access, a common target for bru
te-force attacks.
    \item \textbf{Port 25 (SMTP): Open.} Simple Mail Transfer Protocol, can be abuse
d if misconfigured.
    \item \textbf{Port 80 (HTTP): Open.} Standard for web traffic.
    \item \textbf{Port 110 (POP3): Open.} An unencrypted and outdated email retrieva
l protocol.
    \item \textbf{Port 443 (HTTPS): Open.} Standard for secure web traffic.
    \item \textbf{Port 3389 (RDP): Open.} Remote Desktop Protocol is a primary vecto
r for ransomware attacks.
\end{itemize}

\textbf{Conclusion:} The network perimeter is dangerously exposed. Open RDP, FTP, an
d POP3 ports represent an immediate and critical risk. Exposing these services witho
ut the protection of a Virtual Private Network (VPN) or other access controls is a s
evere security misconfiguration.

\section*{6. Risk Assessment \& Readiness Summary}
\begin{center}
\begin{tabular}{|l|c|p{6cm}|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication & \text{\Large\bfseries ❌} Weak & No MFA for email or computers cre
```

```
ates a high risk of account compromise. \\
Email Security & \text{\Large\bfseries ❌} Critical Risk & No DMARC and a weak SPF
policy allow for trivial email spoofing. \\
Network Exposure & \text{\Large\bfseries ❌} Critical Risk & Direct exposure of RD
P, FTP, and other services to the internet. \\
Policy \& Training & \text{\Large\bfseries ❌} Weak & Absence of basic security pol
icies and employee training. \\
\hline
\end{tabular}
\end{center}

\section*{7. Recommendations}
The following actions are recommended with the highest priority to address the ident
ified critical risks:

\begin{enumerate}
    \item \textbf{Harden the Network Perimeter Immediately:}
    \begin{itemize}
        \item Close all unnecessary ports on the firewall, especially Port 3389 (RD
P), Port 21 (FTP), and Port 110 (POP3).
        \item If remote access is required, implement a securely configured Virtual
Private Network (VPN) with MFA.
    \end{itemize}
    \item \textbf{Implement Mandatory Multi-Factor Authentication (MFA):}
    \begin{itemize}
        \item Enforce MFA for all user access, starting with email accounts, compute
r logins, and all remote access systems.
    \end{itemize}
    \item \textbf{Strengthen Email Authentication:}
    \begin{itemize}
        \item Update the SPF record to use a \texttt{-all} (HardFail) policy to prev
ent delivery of unauthorized email.
        \item Deploy a DMARC record, starting with a monitoring policy (\texttt{p=no
ne}) and progressing to a full rejection policy (\texttt{p=reject}).
    \end{itemize}
    \item \textbf{Establish a Security Program:}
    \begin{itemize}
        \item Develop and implement a formal Acceptable Use Policy for all employee
s.
        \item Institute mandatory cybersecurity awareness training for all new hires
and conduct annual refresher training for all staff.
    \end{itemize}
\end{enumerate}

\section*{8. Conclusion}
G.A.S. Inc. currently has a critically deficient cybersecurity posture. The combinat
ion of an exposed network perimeter, inadequate email security, and weak authenticat
ion controls creates an environment highly susceptible to a successful cyberattack.
The organization must take immediate and decisive action to implement the recommenda
tions in this report to protect its data, assets, and reputation.

\end{{document}
```

In [16]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "pro_sample2_pdf_latex.html")
```

✅ Successfully exported HTML: pro_sample2_pdf_latex.html

In [17]:
```
response = flashModel.generate_content(contents=[prompt_text, context2_text + "\n"
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc.
Date: October 14, 2025

\section{1. Overview}
This report evaluates the cybersecurity posture of G.A.S. Inc. based on DNS records (including DMARC), external port scanning, and a self-reported security questionnaire. The findings indicate significant cybersecurity weaknesses across multiple critical areas, including user authentication, email security, network perimeter defense, and employee awareness. The organization faces a high risk of cyberattacks, data breaches, and system compromise due to these identified vulnerabilities.

\section{2. Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name:} G.A.S. Inc.
    \item \textbf{Email Domain:} gasinc.net
    \item \textbf{Website Domain:} www.gasinc.net
    \item \textbf{External IP (Firewall/Web Server):} 104.28.1.189
    \item \textbf{DNS Hosting:} Appears to be self-hosted (dns1.gasinc.net, dns2.gasinc.net)
\end{itemize}

\section{3. Security Questionnaire Review}
\begin{center}
\begin{tabular}{|l|l|l|}
\hline
\textbf{Security Control} & \textbf{Status} & \textbf{Notes} \\
\hline
MFA for Email & \faTimes \textbf{No} & Critical security gap, highly vulnerable to credential stuffing and phishing. \\
\hline
MFA for Computer Login & \faTimes \textbf{No} & Critical security gap, increases risk of unauthorized access via compromised credentials. \\
\hline
MFA for Sensitive Systems & \faCheck \textbf{Yes} & Positive, but limited in scope given other MFA gaps. \\
\hline
Acceptable Use Policy (AUP) & \faTimes \textbf{No} & Lack of clear guidelines for employee behavior, increasing insider threat risk. \\
\hline
New Employee Security Training & \faTimes \textbf{No} & New hires are not properly educated on security best practices, leading to early vulnerabilities. \\
\hline
Annual All-Employee Security Training & \faTimes \textbf{No} & Employees are not regularly updated on evolving threats and security protocols. \\
\hline
\end{tabular}
\end{center}

\subsection*{Summary:}
The questionnaire responses reveal critical deficiencies in fundamental cybersecurity practices. The absence of Multi-Factor Authentication (MFA) for email and computer logins, coupled with a complete lack of security policies (like an AUP) and employee security awareness training, exposes the organization to severe risks from phishing, credential theft, and human error. While MFA is used for sensitive data systems, its limited application undermines overall security posture.

```
\section{4. DNS \& Email Security}
\subsection*{DNS Records:}
\begin{itemize}
    \item DNS is managed by self-hosted nameservers (dns1.gasinc.net, dns2.gasinc.ne
t).
    \item The primary A record for gasinc.net points to 104.28.1.189, confirming thi
s IP as the public facing entry point.
\end{itemize}

\subsection*{MX Records (Email):}
\begin{itemize}
    \item The organization uses Mailhostbox for email services (mx.mailhostbox.com,
mx2.mailhostbox.com).
    \item \textbf{SPF Record:} A Sender Policy Framework (SPF) record is correctly c
onfigured: \texttt{v=spf1 include:spf.mailhostbox.com \~all}. This helps prevent ema
il spoofing by specifying authorized mail senders.
\end{itemize}

\subsection*{DMARC Record:}
\begin{itemize}
    \item \textbf{No DMARC record found (\texttt{NXDOMAIN}).} This is a significant
vulnerability. Without DMARC, email spoofing attempts using the \texttt{@gasinc.net}
domain are not properly authenticated and can bypass recipient email filters. This l
eaves G.A.S. Inc. and its correspondents highly susceptible to phishing, business em
ail compromise (BEC) attacks, and brand impersonation.
\end{itemize}

\subsection*{Conclusion:}
While SPF is in place, the absence of a DMARC record leaves the email domain highly
vulnerable to sophisticated spoofing and phishing attacks. This is exacerbated by th
e lack of MFA for email access, creating a very weak email security posture.

\section{5. Port Scanning Results}
The external IP address 104.28.1.189 serves as both the organization's external netw
ork perimeter (firewall) and hosts the website. This configuration inherently increa
ses risk by consolidating critical services on a single, exposed entry point.

\subsection*{Website Hosting (104.28.1.189):}
\begin{itemize}
    \item \textbf{Port 80 (HTTP): Open}
    \item \textbf{Port 443 (HTTPS): Open}
\end{itemize}
\subsection*{Firewall / External IP (104.28.1.189):}
\begin{itemize}
    \item \textbf{Port 21 (FTP): Open} - Insecure protocol for file transfer, often
susceptible to brute-force attacks and weak credentials.
    \item \textbf{Port 22 (SSH): Open} - Secure shell, but requires stringent access
controls, strong authentication, and regular patching to prevent compromise.
    \item \textbf{Port 25 (SMTP): Open} - Mail transfer protocol, could indicate an
open relay or vulnerability if not properly secured.
    \item \textbf{Port 80 (HTTP): Open} - Standard for web traffic.
    \item \textbf{Port 110 (POP3): Open} - Insecure email retrieval protocol, often
transmits credentials in cleartext.
    \item \textbf{Port 443 (HTTPS): Open} - Standard for secure web traffic.
    \item \textbf{Port 3389 (RDP): Open} - Remote Desktop Protocol, a frequent targe
t for brute-force attacks and credential theft, especially if not secured with MFA o
```

```
r restricted by IP.
\end{itemize}

\subsection*{Conclusion:}
The external IP (104.28.1.189) has an unacceptably large number of open ports, expos
ing several high-risk services directly to the internet. The presence of FTP, POP3,
and RDP on a publicly accessible IP significantly broadens the attack surface and po
ses a critical risk of unauthorized access, data compromise, and remote system contr
ol. This indicates a severe lack of network segmentation and perimeter hardening.

\section{6. Risk Assessment \& Readiness Summary}
\begin{center}
\begin{tabular}{|l|l|l|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication Security & \faTimes \textbf{Weak} & MFA missing for email and compute
r logins; only applied to sensitive systems. \\
\hline
Email Security & \faTimes \textbf{Weak} & No DMARC record, despite SPF presence. Hig
h risk of email spoofing. \\
\hline
Network Exposure & \faTimes \textbf{Critical} & Numerous high-risk ports (FTP, SMTP,
POP3, RDP) open on external IP. \\
\hline
Web Hosting & \faTimes \textbf{Risky} & Website hosted directly on the main external
IP, increasing its exposure to other services. \\
\hline
Policy \& Training & \faTimes \textbf{Non-existent} & No AUP, no security awareness
training for new or existing employees. \\
\hline
\end{tabular}
\end{center}

\section{7. Recommendations}
Urgent and comprehensive action is required to address the critical cybersecurity vu
lnerabilities at G.A.S. Inc.

\begin{enumerate}
    \item \textbf{Implement MFA Broadly:} Mandate Multi-Factor Authentication (MFA)
for all email accounts, computer logins, and any other critical internal or external
systems.
    \item \textbf{Harden Network Perimeter:}
    \begin{itemize}
        \item \textbf{Close Unnecessary Ports:} Immediately close ports 21 (FTP), 25
(SMTP unless absolutely essential for a secure mail relay), 110 (POP3).
        \item \textbf{Restrict Access:} For essential services like Port 22 (SSH) an
d Port 3389 (RDP), restrict access to specific trusted IP addresses or implement a V
PN for access.
        \item \textbf{Separate Services:} Isolate the web server from the primary fi
rewall/server. Implement a dedicated firewall solution with proper segmentation and
Intrusion Prevention System (IPS) capabilities.
        \item \textbf{Replace Insecure Protocols:} Migrate from FTP to SFTP/FTPS and
from POP3 to secure IMAP (IMAPS) or webmail interfaces.
    \end{itemize}
    \item \textbf{Implement DMARC for Email Security:} Configure a DMARC record with
```

```
a policy of \texttt{p=quarantine} or \texttt{p=reject} to prevent unauthorized use o
f the \texttt{@gasinc.net} domain for spoofing and phishing.
    \item \textbf{Develop and Enforce Security Policies:}
    \begin{itemize}
        \item Create and distribute an Acceptable Use Policy (AUP) outlining proper
employee conduct regarding company assets and data.
        \item Develop policies for password management, data handling, incident resp
onse, and remote access.
    \end{itemize}
    \item \textbf{Implement Security Awareness Training:}
    \begin{itemize}
        \item Conduct mandatory security awareness training for all new employees du
ring onboarding.
        \item Implement annual security awareness training for all employees, coveri
ng topics like phishing, social engineering, password hygiene, and incident reportin
g.
    \end{itemize}
    \item \textbf{Regular Vulnerability Management:} Conduct regular external and in
ternal vulnerability scans and penetration tests to identify and remediate security
flaws proactively.
\end{enumerate}

\section{8. Conclusion}
G.A.S. Inc. currently possesses an extremely weak cybersecurity posture with critica
l vulnerabilities in network exposure, a severe lack of fundamental authentication c
ontrols, and non-existent security policies and training programs. The organization
is highly susceptible to various cyber threats, including data breaches, ransomware,
phishing, and unauthorized system access. Immediate and comprehensive implementation
of the recommended security measures is paramount to mitigate these risks and establ
ish a foundational level of cybersecurity readiness. Failure to address these issues
could lead to significant financial, operational, and reputational damage.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025
```

In [18]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_sample2_pdf_latex.html")
```

✅ Successfully exported HTML: flash_sample2_pdf_latex.html

In [19]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context2_text + "
print(response.text)
```

Cybersecurity Readiness Report for G.A.S. Inc. Date: October 14, 2025

1. Overview
This report assesses the cybersecurity readiness of G.A.S. Inc. based on provided DNS, port scanning, and security questionnaire data. The findings indicate several critical areas requiring immediate attention to improve the organization's overall security posture.

2. Organizational Information
* Organization Name: G.A.S. Inc.
* Email Domain: gasinc.net
* Website Domain: www.gasinc.net
* External IP (Firewall): 104.28.1.189
* Website Hosting IP: 104.28.1.189

3. Security Questionnaire Review

Security Control	Status	Notes
MFA for Email	❌ No	Critical vulnerability, leaving email accounts susceptible to compromise.
MFA for Computer Login	❌ No	Significant risk for unauthorized access to internal systems.
MFA for Sensitive Data Systems	✅ Yes	Positive step, but limited by lack of MFA on email and computers.
Acceptable Use Policy	❌ No	Lack of policy increases the risk of misuse and non-compliance.
New Employee Security Training	❌ No	New employees are onboarded without essential security awareness.
Annual All-Employee Training	❌ No	No regular reinforcement of security best practices for all staff.

Summary: The organization demonstrates a significant lack of fundamental security practices, particularly concerning Multi-Factor Authentication (MFA) for email and computer logins, and a complete absence of acceptable use policies and security awareness training. While MFA is implemented for sensitive data systems, the lack of it for email and general computer access creates broad vulnerabilities.

4. DNS & Email Security

DNS Records
* The `gasinc.net` domain is configured with A records pointing to `104.28.1.189`.
* MX records indicate email is handled by `mailhostbox.com` services.
* An SPF record is present: `v=spf1 include:spf.mailhostbox.com ~all`. This is a positive step towards preventing email spoofing.

DMARC Record
* The `_dmarc.gasinc.net` DNS query returned `NXDOMAIN`. This means there is no DMARC record configured for the domain.
Conclusion: While basic SPF is in place, the absence of a DMARC record is a significant security gap. DMARC, in conjunction with SPF and DKIM, provides crucial protection against email phishing and spoofing. The lack of a DMARC record leaves the organization's email infrastructure vulnerable.

5. Port Scanning Results

Website Hosting (IP: 104.28.1.189)
* Port 80 (HTTP): Open
* Port 443 (HTTPS): Open
These are standard ports for a web server and are expected.

Firewall / External IP (104.28.1.189)
* Port 21 (FTP): Open
* Port 22 (SSH): Open
* Port 25 (SMTP): Open
* Port 80 (HTTP): Open
* Port 110 (POP3): Open
* Port 443 (HTTPS): Open
* Port 3389 (RDP): Open

Conclusion: The external IP address, which appears to be acting as both the firewall and hosting the website, exposes a broad range of services. This extensive open port list represents a significant attack surface. Specifically, open ports for FTP, SSH, SMTP, POP3, and RDP are highly concerning without strong authentication mechanisms l ike MFA, which are missing for email and computer logins.

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	🔴 High Risk	Lack of MFA for email and computer log ins is a critical vulnerability. Open services like SSH, RDP, and FTP are exposed wi thout this essential layer of security.
Email Security	🟡 Medium	SPF is configured, which is good. Howeve r, the complete absence of a DMARC record is a major weakness, leaving the organizat ion vulnerable to sophisticated phishing and spoofing attacks.
Network Exposure	🔴 High Risk	A wide array of ports are open on the external IP, significantly increasing the attack surface. This includes potentially vulnerable services like FTP, SSH, POP3, and RDP.
Web Hosting	🟢 Secure	Standard ports for web hosting (80, 443) are open, which is expected.
Policy & Training	🔴 High Risk	The absence of an Acceptable Use Polic y and any form of security awareness training (for new or existing employees) indica tes a severe deficiency in establishing a security-aware culture and guiding user be havior.

7. Recommendations

Given the critical vulnerabilities identified, the following recommendations are pri oritized:

1. **Implement MFA Immediately:**
    *   Mandate MFA for all email accounts (`gasinc.net`).

    *   Enforce MFA for all computer logins (workstations and servers).
    *   This is the most urgent step to mitigate widespread account compromise risk
s.

2. **Configure DMARC:**
    *   Create and publish a DMARC record for `gasinc.net`. Start with a `p=none` or
`p=quarantine` policy to monitor and then move to `p=reject` once confident in SPF a
nd DKIM configuration.
    *   Ensure DKIM is also properly configured and aligned with SPF and DMARC.

3. **Minimize External Attack Surface:**
    *   Review all open ports on the external IP address (`104.28.1.189`).
    *   Close any ports that are not absolutely necessary for external access (e.g.,
FTP, POP3, RDP, and potentially SSH if not managed securely with key-based authentic
ation and rate limiting).
    *   If RDP or SSH must be exposed, ensure they are secured with strong password
s, key-based authentication (for SSH), and ideally accessed only via a VPN with MFA.

4. **Develop and Implement Security Policies:**
    *   Create a comprehensive Employee Acceptable Use Policy that clearly outlines
security expectations and responsibilities.
    *   Formalize and document a cybersecurity awareness training program for all em
ployees.

5. **Establish Security Training Programs:**
    *   Implement mandatory security awareness training for all new employees during
onboarding.
    *   Conduct annual security awareness training for all existing employees, cover
ing topics like phishing, password security, and safe internet practices.

6. **Consider Firewall Segmentation:**
    *   If possible, segment the network to isolate the web server from internal res
ources, and ensure the firewall effectively blocks unsolicited incoming traffic.

8. **Conclusion**
G.A.S. Inc. currently exhibits significant cybersecurity readiness gaps, particularl
y in the areas of authentication, email protection, network exposure, and foundation
al security policies and training. The lack of MFA for email and computer logins, co
upled with a broad range of open ports on the external perimeter and no DMARC recor
d, exposes the organization to a high risk of compromise. Immediate implementation o
f the recommended actions, especially MFA and DMARC configuration, is crucial to est
ablish a more secure operational environment.

Prepared by:
Cybersecurity Assessment Team
Date: October 14, 2025

```tex
\documentclass{article}
\usepackage{geometry}
\geometry{a4paper, margin=1in}
\usepackage{enumitem}
\usepackage{hyperref}

\title{Cybersecurity Readiness Report for G.A.S. Inc.}
\author{Cybersecurity Assessment Team}
```

```
\date{October 14, 2025}

\begin{document}

\maketitle

\section{Overview}
This report assesses the cybersecurity readiness of G.A.S. Inc. based on provided DN
S, port scanning, and security questionnaire data. The findings indicate several cri
tical areas requiring immediate attention to improve the organization's overall secu
rity posture.

\section{Organizational Information}
\begin{itemize}
    \item Organization Name: G.A.S. Inc.
    \item Email Domain: \texttt{gasinc.net}
    \item Website Domain: \texttt{www.gasinc.net}
    \item External IP (Firewall): \texttt{104.28.1.189}
    \item Website Hosting IP: \texttt{104.28.1.189}
\end{itemize}

\section{Security Questionnaire Review}
\subsection{Security Control Status}
\begin{tabular}{|l|c|p{6cm}|}
\hline
\textbf{Security Control} & \textbf{Status} & \textbf{Notes} \\
\hline
MFA for Email & \textcolor{red}{\ding{55}} No & Critical vulnerability, leaving emai
l accounts susceptible to compromise. \\
MFA for Computer Login & \textcolor{red}{\ding{55}} No & Significant risk for unauth
orized access to internal systems. \\
MFA for Sensitive Data Systems & \textcolor{green}{\checkmark} Yes & Positive step,
but limited by lack of MFA on email and computers. \\
Acceptable Use Policy & \textcolor{red}{\ding{55}} No & Lack of policy increases the
risk of misuse and non-compliance. \\
New Employee Security Training & \textcolor{red}{\ding{55}} No & New employees are o
nboarded without essential security awareness. \\
Annual All-Employee Training & \textcolor{red}{\ding{55}} No & No regular reinforcem
ent of security best practices for all staff. \\
\hline
\end{tabular}

\subsection{Summary}
The organization demonstrates a significant lack of fundamental security practices,
particularly concerning Multi-Factor Authentication (MFA) for email and computer log
ins, and a complete absence of acceptable use policies and security awareness traini
ng. While MFA is implemented for sensitive data systems, the lack of it for email an
d general computer access creates broad vulnerabilities.

\section{DNS \& Email Security}
\subsection{DNS Records}
\begin{itemize}
    \item The \texttt{gasinc.net} domain is configured with A records pointing to \t
exttt{104.28.1.189}.
    \item MX records indicate email is handled by \texttt{mailhostbox.com} services.
    \item An SPF record is present: \texttt{v=spf1 include:spf.mailhostbox.com \(\si
```

```
m\)all}. This is a positive step towards preventing email spoofing.
\end{itemize}

\subsection{DMARC Record}
\begin{itemize}
    \item The \texttt{\_dmarc.gasinc.net} DNS query returned \texttt{NXDOMAIN}. This means there is no DMARC record configured for the domain.
\end{itemize}
\textbf{Conclusion:} While basic SPF is in place, the absence of a DMARC record is a significant security gap. DMARC, in conjunction with SPF and DKIM, provides crucial protection against email phishing and spoofing. The lack of a DMARC record leaves th e organization's email infrastructure vulnerable.

\section{Port Scanning Results}
\subsection{Website Hosting (IP: 104.28.1.189)}
\begin{itemize}
    \item Port 80 (HTTP): Open
    \item Port 443 (HTTPS): Open
\end{itemize}
These are standard ports for a web server and are expected.

\subsection{Firewall / External IP (104.28.1.189)}
\begin{itemize}
    \item Port 21 (FTP): Open
    \item Port 22 (SSH): Open
    \item Port 25 (SMTP): Open
    \item Port 80 (HTTP): Open
    \item Port 110 (POP3): Open
    \item Port 443 (HTTPS): Open
    \item Port 3389 (RDP): Open
\end{itemize}
\textbf{Conclusion:} The external IP address, which appears to be acting as both the firewall and hosting the website, exposes a broad range of services. This extensive open port list represents a significant attack surface. Specifically, open ports for FTP, SSH, SMTP, POP3, and RDP are highly concerning without strong authentication me chanisms like MFA, which are missing for email and computer logins.

\section{Risk Assessment \& Readiness Summary}
\begin{tabular}{|l|c|p{8cm}|}
\hline
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\hline
Authentication Security & \textcolor{red}{\textbf{High Risk}} & Lack of MFA for emai l and computer logins is a critical vulnerability. Open services like SSH, RDP, and FTP are exposed without this essential layer of security. \\
Email Security & \textcolor{orange}{\textbf{Medium}} & SPF is configured, which is g ood. However, the complete absence of a DMARC record is a major weakness, leaving th e organization's email vulnerable to sophisticated phishing and spoofing attacks. \\
Network Exposure & \textcolor{red}{\textbf{High Risk}} & A wide array of ports are o pen on the external IP, significantly increasing the attack surface. This includes p otentially vulnerable services like FTP, SSH, POP3, and RDP. \\
Web Hosting & \textcolor{green}{\textbf{Secure}} & Standard ports for web hosting (8 0, 443) are open, which is expected. \\
Policy \& Training & \textcolor{red}{\textbf{High Risk}} & The absence of an Accepta ble Use Policy and any form of security awareness training (for new or existing empl oyees) indicates a severe deficiency in establishing a security-aware culture and gu
```

```
iding user behavior. \\
\hline
\end{tabular}

\section{Recommendations}
Given the critical vulnerabilities identified, the following recommendations are pri
oritized:

\begin{enumerate}
    \item \textbf{Implement MFA Immediately:}
    \begin{itemize}
        \item Mandate MFA for all email accounts (\texttt{gasinc.net}).
        \item Enforce MFA for all computer logins (workstations and servers).
        \item This is the most urgent step to mitigate widespread account compromise
risks.
    \end{itemize}
    \item \textbf{Configure DMARC:}
    \begin{itemize}
        \item Create and publish a DMARC record for \texttt{gasinc.net}. Start with
a \texttt{p=none} or \texttt{p=quarantine} policy to monitor and then move to \textt
t{p=reject} once confident in SPF and DKIM configuration.
        \item Ensure DKIM is also properly configured and aligned with SPF and DMAR
C.
    \end{itemize}
    \item \textbf{Minimize External Attack Surface:}
    \begin{itemize}
        \item Review all open ports on the external IP address (\texttt{104.28.1.18
9}).
        \item Close any ports that are not absolutely necessary for external access
(e.g., FTP, POP3, RDP, and potentially SSH if not managed securely with key-based au
thentication and rate limiting).
        \item If RDP or SSH must be exposed, ensure they are secured with strong pas
swords, key-based authentication (for SSH), and ideally accessed only via a VPN with
MFA.
    \end{itemize}
    \item \textbf{Develop and Implement Security Policies:}
    \begin{itemize}
        \item Create a comprehensive Employee Acceptable Use Policy that clearly out
lines security expectations and responsibilities.
        \item Formalize and document a cybersecurity awareness training program for
all employees.
    \end{itemize}
    \item \textbf{Establish Security Training Programs:}
    \begin{itemize}
        \item Implement mandatory security awareness training for all new employees
during onboarding.
        \item Conduct annual security awareness training for all existing employees,
covering topics like phishing, password security, and safe internet practices.
    \end{itemize}
    \item \textbf{Consider Firewall Segmentation:}
    \begin{itemize}
        \item If possible, segment the network to isolate the web server from intern
al resources, and ensure the firewall effectively blocks unsolicited incoming traffi
c.
    \end{itemize}
\end{enumerate}
```

```
\section{Conclusion}
G.A.S. Inc. currently exhibits significant cybersecurity readiness gaps, particularl
y in the areas of authentication, email protection, network exposure, and foundation
al security policies and training. The lack of MFA for email and computer logins, co
upled with a broad range of open ports on the external perimeter and no DMARC recor
d, exposes the organization to a high risk of compromise. Immediate implementation o
f the recommended actions, especially MFA and DMARC configuration, is crucial to est
ablish a more secure operational environment.

\end{document}
```
```

In [20]:
```
generated_html = generate_html_from_markdown(response.text)
export_html_to_files(generated_html, "flash_lite_sample2_pdf_latex.html")
```

✅ Successfully exported HTML: flash_lite_sample2_pdf_latex.html

In [42]:
```
import pypandoc

def _extract_latex_content(text_content: str) -> str | None:
    """
    Internal helper to extract LaTeX content from raw text or a JSON block.
    """
    latex_content = ""
    try:
        # Check for code-fenced JSON structure first
        json_match = re.search(r'```json\s*(.*?)\s*```', text_content, re.DOTALL)
        if json_match:
            json_string = json_match.group(1).strip()
            try:
                data = json.loads(json_string)
                latex_content = data.get("text", "")
            except json.JSONDecodeError:
                print("Warning: JSON inside the code block is not valid. Treating e
                latex_content = text_content
        else:
            # Try to load the entire content as plain JSON
            try:
                data = json.loads(text_content)
                latex_content = data.get("text", "")
            except json.JSONDecodeError:
                # If neither works, treat the entire input as LaTeX text
                latex_content = text_content

        if not isinstance(latex_content, str):
            print(f"Error: LaTeX content is not a string, it's a {type(latex_conten
            return None

        return latex_content

    except Exception as e:
        print(f"An unexpected error occurred during content extraction: {e}")
        return None
```
```

```python
def _wrap_html_shell(body_content: str, title: str = "LaTeX Export") -> str:
    """
    Internal helper to wrap HTML body content in a full document
    with KaTeX for math rendering.
    """
    return f"""
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>{title}</title>

    <!-- KaTeX CSS -->
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/kat

    <!-- KaTeX JS -->
    <script src="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/katex.min.js" xinte

    <!-- KaTeX Auto-render extension -->
    <script src="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/contrib/auto-render

    <style>
        /* Base styles */
        body {{
            font-family: 'Noto Sans', 'Arial', sans-serif;
            line-height: 1.6;
            color: #333;
            max-width: 800px;
            margin: 2rem auto;
            padding: 0 1rem;
        }}
        h1, h2, h3, h4, h5, h6 {{
            color: #1a1a1a;
            margin-top: 1.5em;
            margin-bottom: 0.5em;
        }}
        p {{
            margin-bottom: 1em;
        }}
        pre {{
            background-color: #f4f4f4;
            padding: 1rem;
            border-radius: 4px;
            overflow-x: auto;
            border: 1px solid #ddd;
            font-family: monospace;
        }}
        code {{
            font-family: monospace;
            background-color: #f0f0f0;
            padding: 2px 4px;
            border-radius: 3px;
        }}
        ul, ol {{
```

```
            padding-left: 2em;
            margin-bottom: 1em;
        }}
        li {{
            margin-bottom: 0.5em;
        }}

        /* KaTeX specific styling for display math */
        .katex-display {{
            overflow-x: auto;
            overflow-y: hidden;
            padding: 0.5em 0;
        }}

        /* Custom LaTeX styles */
        .table-wrapper {{
            margin: 1.5em 0;
            overflow-x: auto;
        }}
        table {{
            border-collapse: collapse;
            width: 100%;
            margin-bottom: 1.5rem;
        }}
        caption {{
            font-weight: bold;
            font-size: 1.1em;
            margin-bottom: 0.5em;
            text-align: left;
        }}
        th, td {{
            border: 1px solid #ddd;
            padding: 10px;
            text-align: left;
            vertical-align: top;
        }}
        th {{
            background-color: #e9ecef;
            font-weight: bold;
        }}
        .latex-url, .seqsplit {{
            word-break: break-all;
        }}
    </style>
</head>
<body>
{body_content}

<!-- KaTeX auto-render script -->
<script>
    document.addEventListener("DOMContentLoaded", function() {{
        renderMathInElement(document.body, {{
            delimiters: [
                {{left: "$$", right: "$$", display: true}},
                {{left: "$", right: "$", display: false}},
                {{left: "\\(", right: "\\)", display: false}},
```

```
                {{left: "\\[", right: "\\]", display: true}}
            ],
            throwOnError : false
        });
    });
</script>
</body>
</html>
"""

def generate_html_from_latex(text_content: str) -> str | None:
    """
    Extracts LaTeX content and converts it into a full, styled HTML string
    using pypandoc.

    This is the most robust method but requires:
    1. `pip install pypandoc`
    2. The Pandoc binary to be installed on the system:
       https://pandoc.org/installing.html

    Args:
        text_content (str): The raw text content (LaTeX or JSON-wrapped).

    Returns:
        str or None: The complete HTML string, or None if conversion fails.
    """

    latex_content = _extract_latex_content(text_content)
    if latex_content is None:
        return None

    if pypandoc is None:
        print("Error: pypandoc library is not imported. Cannot convert.")
        return None

    try:
        # Extract content only between \begin{document} and \end{document}
        # Pandoc is smart enough to handle the full document, but this
        # ensures we only get the body content if needed.
        body_match = re.search(r'\\begin\{document\}(.*?)\\end\{document\}', latex_
        if body_match:
            content_to_convert = body_match.group(1).strip()
        else:
            content_to_convert = latex_content

        # Use pandoc to convert.
        # --katex tells pandoc to format math for KaTeX.
        # --standalone would wrap it in a full HTML doc, but we want
        # to use our own shell to control the CSS and JS.
        html_output = pypandoc.convert_text(
            content_to_convert,
            'html',
            format='latex',
            extra_args=['--katex']
        )
```

```
        # Pandoc will correctly handle \ding and other symbols.
        return _wrap_html_shell(html_output, "Pandoc LaTeX Export")

    except FileNotFoundError:
        print("="*50)
        print("ERROR: Pandoc executable not found.")
        print("Please install Pandoc from https://pandoc.org/installing.html")
        print("="*50)
        return None
    except Exception as e:
        print(f"An unexpected error occurred during Pandoc conversion: {e}")
        return None
```

In [ ]:

```
prompt_text = 'Prompt:\nGiven this DNS DIG, Port scan of the website, Port scan of

context1_text = 'Context:\n'
context2_text = 'Context:\n'
example_text = 'Example:\n' + prompt_text

filepaths = ["report_template/test_questionnaire.json", "report_template/test_port_
latex_file_path = "report_template/test_report.tex"

sample1_filepaths = ["report_sample1/sample1_questionnaire.json", "report_sample1/s
sample2_filepaths = ["report_sample2/sample2_questionnaire.json", "report_sample2/s

for file in filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            example_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

with open(latex_file_path, 'r') as file:
    latex_content = file.read()
    example_text += latex_content

print("=======  Example ==========")
print(example_text)
print("============================")

for file in sample1_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context1_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
```

```
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 1 =========")
print(prompt_text)
print(context1_text)
print("==========================")

for file in sample2_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context2_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 2 =========")
print(prompt_text)
print(context2_text)
print("==========================")
```

======= Example ==========
Example:
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization. Output plain text plus TeX only.template/test_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Valier School District",
    "Email Domain": "valier.k12.mt.us",
    "Website Domain": "www.valier.k12.mt.us",
    "External IP": "216.220.16.170",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
--
template/test_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
220.16.170\nScanning started at:2025-07-18 22:12:17.055226\n-----------------------
--------------------------\nno ports open\n"
}
--
template/test_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 216.
239.32.21\nScanning started at:2025-07-18 22:09:34.408091\n-------------------------
------------------------\nPort 80 is open\nPort 443 is open\n"
}
--
template/test_dns_dig_email.json:
{
  "text": "id 49113\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\nvalier.
k12.mt.us. IN ANY\n;ANSWER\nvalier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-reque
st.umt.edu. 2024030501 21600 900 1209600 86400\nvalier.k12.mt.us. 3600 IN NS ens-o1.
umt.edu.\nvalier.k12.mt.us. 3600 IN NS cudess2.umt.edu.\nvalier.k12.mt.us. 3600 IN N
S cudess1.umt.edu.\nvalier.k12.mt.us. 3600 IN A 216.239.38.21\nvalier.k12.mt.us. 360
0 IN A 216.239.32.21\nvalier.k12.mt.us. 3600 IN A 216.239.34.21\nvalier.k12.mt.us. 3
600 IN A 216.239.36.21\nvalier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.\nvalier.k
12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 10 aspm
x3.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.\nvalier.
k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.\nvalier.k12.mt.us. 3600 IN TXT \"v=
spf1 include:_spf.google.com include:mg.infinitecampus.org -all\"\n;AUTHORITY\n;ADDI
TIONAL\n"
}
--
template/test_dns_dig_email_dmarc.json:
{
  "text": "id 45565\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
```

```
valier.k12.mt.us. IN ANY\n;ANSWER\n_dmarc.valier.k12.mt.us. 3600 IN TXT \"v=DMARC1;
p=reject; rua=mailto:dmarc@valier.k12.mt.us\"\n;AUTHORITY\n;ADDITIONAL\n"
}
--
\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 Valier School District}}
\author{Date: July 18, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report evaluates the cybersecurity posture of Valier School District based on t
echnical scans (DNS, DMARC, and port scanning) and a self-reported security question
naire. The findings reflect a strong commitment to foundational cybersecurity practi
ces across user access, email protection, network exposure, and staff awareness.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Valier School District
    \item \textbf{Email Domain}: valier.k12.mt.us
    \item \textbf{Website Domain}: \url{www.valier.k12.mt.us}
    \item \textbf{External IP (Firewall)}: 216.220.16.170
    \item \textbf{Website Hosting IPs}: \seqsplit{216.239.32.21, 216.239.34.21, 216.
239.36.21, 216.239.38.21}
    \item \textbf{DNS Hosting}: Managed by University of Montana (umt.edu nameserver
s)
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: The district reports complete implementation of basic cy
ber hygiene practices, especially user authentication (Multi-Factor Authentication)
and routine training. This indicates a proactive and policy-driven approach to risk
mitigation.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS is managed by the University of Montana (\url{cudess1.umt.edu}, \url{c
udess2.umt.edu}), suggesting centralized and professionally administered DNS.
    \item A records point to IPs within Google's network (likely Google Sites hostin
g for web content).
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The district uses Google Workspace (Gmail) for email, as shown by multiple
\seqsplit{\texttt{\url{aspmx.l.google.com}}} MX records.
    \item \textbf{SPF record} is correctly configured: \seqsplit{\texttt{v=spf1 incl
ude:\url{spf.google.com} include:\url{mg.infinitecampus.org -all}}}. This helps miti
gate spoofing by defining authorized mail senders.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A valid DMARC record exists with a \textbf{reject policy}: \seqsplit{\text
tt{v=DMARC1; p=reject; rua=\url{mailto:dmarc@valier.k12.mt.us}}}.
    \item This instructs receiving servers to reject unauthenticated mail, providing
strong protection against phishing.
\end{itemize}

\noindent \textbf{Conclusion}: DNS and email protections (SPF, DMARC, and hosting se
curity) are configured correctly and follow best practices.

\section{Port Scanning Results}

\subsection*{Website Hosting (Google IP: 216.239.32.21)}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
These ports are expected for a publicly accessible website and are typical for Googl
e-hosted services.

\subsection*{Firewall / External IP (216.220.16.170)}
```

```
\begin{itemize}
    \item All scanned ports are \textbf{closed}.
\end{itemize}
This is a strong sign of network perimeter hardening and good firewall configuratio
n. No externally exposed services were found on the organization's primary IP.

\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 & Strong & MFA is required across key systems \\
Email Security & Strong & SPF and DMARC with "reject" policy in place \\
Network Exposure & Secure & No exposed services on the external firewall IP \\
Web Hosting & Secure & Google-hosted; limited attack surface \\
Policy \& Training & Comprehensive & Acceptable use policies and regular training in
place \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
Although the cybersecurity readiness is solid, continuous improvement is essential.
We recommend the following:
\begin{enumerate}
    \item \textbf{Verify DKIM}: While SPF and DMARC are configured, ensure DKIM is a
lso active for all sending domains.
    \item \textbf{Vulnerability Scanning}: Consider regular internal and external vu
lnerability assessments of network devices and servers.
    \item \textbf{Incident Response Plan}: Document and regularly test a cybersecuri
ty incident response and disaster recovery plan.
    \item \textbf{Asset Inventory}: Maintain a regularly updated inventory of hardwa
re/software assets and monitor for unauthorized changes.
    \item \textbf{Third-party Risk}: Evaluate vendors (e.g., Infinite Campus) for th
eir security posture, especially since they're included in SPF.
\end{enumerate}

\section{Conclusion}
Valier School District demonstrates a strong cybersecurity foundation, particularly
in authentication, email protection, staff training, and perimeter security. Continu
ed vigilance and regular audits will help maintain and improve this strong security
posture.

\vspace{1cm}
\noindent Prepared by: \\
Cybersecurity Assessment Team\\
Date: July 18, 2025

\end{document}
==========================
======== Sample 1 =========
Prompt:
```

Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the answers to the security questionnaire, write a report on the cybersecurity readiness of the organization. Output plain text plus TeX only.
Context:
sample1/sample1_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Apex Innovations",
    "Email Domain": "apexinnovations.com",
    "Website Domain": "www.apexinnovations.com",
    "External IP": "72.21.196.160",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
```

--
sample1/sample1_dns_dig_email_dmarc.json:

```
{
  "text": "id 31890\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
apexinnovations.com. IN ANY\n;ANSWER\n_dmarc.apexinnovations.com. 3600 IN TXT \"v=DM
ARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\""
}
```

--
sample1/sample1_dns_dig_email.json:

```
{
  "text": "id 52417\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\napexinn
ovations.com. IN ANY\n;ANSWER\napexinnovations.com. 3600 IN SOA ns1.apexinnovations.
com. hostmaster.apexinnovations.com. 2025101401 21600 3600 604800 3600\napexinnovati
ons.com. 3600 IN NS ns1.apexinnovations.com.\napexinnovations.com. 3600 IN NS ns2.ap
exinnovations.com.\napexinnovations.com. 3600 IN A 72.21.196.160\napexinnovations.co
m. 3600 IN MX 10 mx1.apexinnovations.com.\napexinnovations.com. 3600 IN MX 20 mx2.ap
exinnovations.com.\napexinnovations.com. 3600 IN TXT \"v=spf1 include:spf.protectio
n.outlook.com -all\""
}
```

--
sample1/sample1_port_scan_external_ip.json:

```
{
  "text": "--------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:09:42.589112\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
```

--
sample1/sample1_port_scan_web.json:

```
{
  "text": "--------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:08:15.223456\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
```

--

```
==========================
======== Sample 2 =========
Prompt:
Given this DNS DIG, Port scan of the website, Port scan of the firewall, and the ans
wers to the security questionnaire, write a report on the cybersecurity readiness of
the organization. Output plain text plus TeX only.
Context:
sample2/sample2_questionnaire.json:
{
  "text": {
    "Organization Name": "G.A.S. Inc.",
    "Email Domain": "gasinc.net",
    "Website Domain": "www.gasinc.net",
    "External IP": "104.28.1.189",
    "Do you require MFA to access email?": "No",
    "Do you require MFA to log into computers?": "No",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "No",
    "Does your organization do security awareness training for new employees?": "N
o",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "No"
  }
}
--
sample2/sample2_dns_dig_email_dmarc.json:
{
  "text": "id 28911\nopcode QUERY\nrcode NXDOMAIN\nflags QR AA RD RA\n;QUESTION\n_dm
arc.gasinc.net. IN ANY\n;AUTHORITY\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmas
ter.gasinc.net. 2025101402 14400 3600 604800 3600\n;ADDITIONAL"
}
--
sample2/sample2_dns_dig_email.json:
{
  "text": "id 47123\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\ngasinc.
net. IN ANY\n;ANSWER\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmaster.gasinc.ne
t. 2025101402 14400 3600 604800 3600\ngasinc.net. 3600 IN NS dns1.gasinc.net.\ngasin
c.net. 3600 IN NS dns2.gasinc.net.\ngasinc.net. 3600 IN A 104.28.1.189\ngasinc.net.
3600 IN MX 10 mx.mailhostbox.com.\ngasinc.net. 3600 IN MX 20 mx2.mailhostbox.com.\ng
asinc.net. 3600 IN TXT \"v=spf1 include:spf.mailhostbox.com ~all\""
}
--
sample2/sample2_port_scan_external_ip.json:
{
  "text": "---------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:16:11.890123\n-------------------------
-------------------------\nPort 21 is open\nPort 22 is open\nPort 25 is open\nPort 8
0 is open\nPort 110 is open\nPort 443 is open\nPort 3389 is open"
}
--
sample2/sample2_port_scan_web.json:
{
  "text": "---------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:15:30.456789\n-------------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
```

--

==========

In [7]:
```
# === SAMPLE 1 ===

# LaTeX input, LaTeX output
response = proModel.generate_content(contents=[prompt_text, context1_text + "\n" +
print(response.text)
```

```
\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 Apex Innovations}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report provides a cybersecurity readiness assessment for Apex Innovations, base
d on a combination of a self-reported security questionnaire and external technical
scans. The analysis reveals that Apex Innovations has implemented strong internal se
curity controls, particularly regarding user authentication and email security. Howe
ver, the organization's network architecture presents a potential risk by exposing i
ts public-facing website on the same IP address as its primary external network inte
rface.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Apex Innovations
    \item \textbf{Email Domain}: apexinnovations.com
    \item \textbf{Website Domain}: \url{www.apexinnovations.com}
    \item \textbf{External IP (Firewall \& Website)}: 72.21.196.160
    \item \textbf{Email Provider}: Microsoft 365 (inferred from SPF record)
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
```

```
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: Apex Innovations reports a strong commitment to security policies and user access controls. The universal requirement for Multi-Factor Authentication (MFA) and consistent security awareness training significantly reduces risks associated with phishing and unauthorized access.

\section{DNS \& Email Security}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The organization's SPF record points to Microsoft's protection services: \seqsplit{\texttt{v=spf1 include:spf.protection.outlook.com -all}}.
    \item The hard fail flag (\texttt{-all}) is a security best practice that helps prevent email spoofing.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item An excellent DMARC record is in place with a \textbf{reject policy}: \seqsplit{\texttt{v=DMARC1; p=reject; rua=mailto:dmarc\_reports@apexinnovations.com; fo=1}}.
    \item The \texttt{p=reject} policy provides the strongest level of protection against domain spoofing and phishing attacks by instructing recipient servers to reject unauthenticated emails.
\end{itemize}

\noindent \textbf{Conclusion}: Email security is robustly configured. The combination of SPF and a restrictive DMARC policy demonstrates a mature approach to preventing email-based threats.

\section{Port Scanning Results}

\subsection*{External Firewall / Website (72.21.196.160)}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
\noindent The scans confirm that the external IP address provided, which represents the organization's network perimeter, is also hosting the public website. Only standard web ports are open, which limits the attack surface. However, co-locating a public web server on the primary firewall IP is not a recommended practice, as a compromise of the web server could potentially expose the internal network.

\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 & Strong & Comprehensive MFA implementation reported. \\
Email Security & Strong & SPF and DMARC with "reject" policy in place. \\
Network Exposure & Moderate Risk & Web server is exposed on the primary firewall IP.
\\
Policy \& Training & Comprehensive & Strong policies and regular employee training.
\\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
While Apex Innovations has a solid security foundation, the following actions are re
commended to further enhance its posture:
\begin{enumerate}
    \item \textbf{Network Segregation}: Isolate the public-facing web server from th
e primary corporate network. This can be achieved by moving the website to a separat
e, dedicated IP address, placing it in a Demilitarized Zone (DMZ), or migrating to a
third-party web hosting provider.
    \item \textbf{Verify DKIM Implementation}: While SPF and DMARC are correctly con
figured, ensure that DKIM (DomainKeys Identified Mail) is also enabled and aligned f
or all outgoing email. DKIM is a critical component of the DMARC framework.
    \item \textbf{Web Application Security}: Conduct regular vulnerability scans and
penetration tests on the web server (\url{www.apexinnovations.com}) to identify and
remediate potential application-level security flaws.
    \item \textbf{Develop an Incident Response Plan}: If not already in place, creat
e and regularly test a formal incident response plan to ensure the organization can
respond effectively to a security breach.
\end{enumerate}

\section{Conclusion}
Apex Innovations demonstrates a strong and mature cybersecurity posture in its inter
nal policies, user authentication, and email security. The organization has successf
ully implemented key controls to mitigate common cyber threats. The primary area for
improvement lies in the network architecture. By segregating the public web server f
rom the main network perimeter, Apex Innovations can significantly reduce its attack
surface and further strengthen its overall security readiness.

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

\end{document}
```

In [44]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "pro_sample1_latex_latex.html")
```

✅ Successfully exported HTML: pro_sample1_latex_latex.html

In [13]:
```
response = flashModel.generate_content(contents=[prompt_text, context1_text + "\n"
print(response.text)
```

```
\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 Apex Innovations}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report evaluates the cybersecurity posture of Apex Innovations based on technic
al scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire.
The findings indicate a strong commitment to foundational cybersecurity practices, p
articularly in user access, email protection, and staff awareness, with a well-secur
ed external network presence.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Apex Innovations
    \item \textbf{Email Domain}: \url{apexinnovations.com}
    \item \textbf{Website Domain}: \url{www.apexinnovations.com}
    \item \textbf{External IP}: \seqsplit{72.21.196.160}
    \item \textbf{DNS Hosting}: Self-hosted (ns1.apexinnovations.com, ns2.apexinnova
tions.com)
    \item \textbf{Email Provider}: Microsoft 365 (based on SPF records)
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
```

```
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: Apex Innovations reports full implementation of crucial cyber hygiene practices, including Multi-Factor Authentication (MFA) across key acce ss points and comprehensive security awareness training programs. This demonstrates a proactive and policy-driven approach to mitigating common user-centric risks.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS is self-hosted with authoritative nameservers \seqsplit{\texttt{\url{n s1.apexinnovations.com}}} and \seqsplit{\texttt{\url{ns2.apexinnovations.com}}}. Thi s implies direct control over DNS management.
    \item The A record for \url{apexinnovations.com} points to \seqsplit{72.21.196.1 60}, which is the organization's external IP address.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item MX records point to \seqsplit{\texttt{\url{mx1.apexinnovations.com}}} and \seqsplit{\texttt{\url{mx2.apexinnovations.com}}}. Combined with the SPF record, thi s indicates the use of Microsoft 365 (Exchange Online) for email services, where the se hostnames typically resolve to Microsoft's mail servers.
    \item \textbf{SPF record} is correctly configured: \seqsplit{\texttt{v=spf1 incl ude:\url{spf.protection.outlook.com -all}}}. This record effectively defines authori zed mail servers, significantly reducing email spoofing attempts.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A valid DMARC record is present with a strong \textbf{reject policy}: \seq split{\texttt{v=DMARC1; p=reject; rua=\url{mailto:dmarc_reports@apexinnovations.co m}; fo=1}}.
    \item The `p=reject` policy instructs receiving mail servers to reject unauthent icated emails that fail SPF or DKIM checks, offering robust protection against phish ing and email impersonation. Reporting is also configured.
\end{itemize}

\noindent \textbf{Conclusion}: Apex Innovations has implemented robust DNS and email security measures, adhering to best practices with strong SPF and DMARC policies.

\section{Port Scanning Results}

\subsection*{External IP / Website (72.21.196.160)}
The port scans of the external IP address \seqsplit{72.21.196.160}, which also hosts the website, revealed the following open ports:
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
These ports are standard for a public-facing web server. The fact that only these es
```

```
sential web service ports are open indicates good perimeter hardening for the expose
d IP address, minimizing the attack surface. There were no other unexpected or high-
risk ports found to be open.

\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 & Strong & MFA is required across key systems \\
Email Security & Strong & SPF and DMARC with "reject" policy in place; Microsoft 365
used \\
Network Exposure & Secure & Only essential web ports (80, 443) open on external IP
\\
Policy \& Training & Comprehensive & Acceptable use policies and regular training in
place \\
DNS Management & Good & Self-managed DNS, but configuration follows best practices
\\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
While Apex Innovations demonstrates a strong cybersecurity posture, continuous impro
vement is vital in the evolving threat landscape. We recommend the following:
\begin{enumerate}
    \item \textbf{DKIM Verification}: Confirm that DomainKeys Identified Mail (DKIM)
is fully configured and active for all outbound emails sent via Microsoft 365. While
SPF and DMARC are strong, DKIM adds another layer of authentication.
    \item \textbf{DNS Security Best Practices}: Given self-hosted DNS, ensure DNS se
rvers are regularly patched, securely configured (e.g., DNSSEC implementation, rate
limiting), and protected against DDoS attacks.
    \item \textbf{Web Application Security}: Implement regular web application vulne
rability scanning and penetration testing for the website hosted on ports 80/443 to
identify and remediate potential vulnerabilities within the application itself.
    \item \textbf{Incident Response Plan}: Develop, document, and regularly test a c
omprehensive cybersecurity incident response and disaster recovery plan to ensure pr
eparedness for potential breaches.
    \item \textbf{Cloud Security Monitoring}: For Microsoft 365, leverage advanced s
ecurity features such as Advanced Threat Protection (ATP), Cloud App Security (MCA
S), and regular audit log reviews to monitor for suspicious activities.
\end{enumerate}

\section{Conclusion}
Apex Innovations exhibits a commendable cybersecurity readiness, characterized by st
rong authentication protocols, robust email security, a well-hardened external netwo
rk perimeter, and a strong commitment to employee training and policy enforcement. B
y addressing the recommendations for further enhancements, the organization can cont
inue to strengthen its defenses against emerging cyber threats.

\vspace{1cm}
\noindent Prepared by: \\
```

```
Cybersecurity Assessment Team\\
Date: October 14, 2025

\end{document}
```

In [49]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_sample1_latex_latex.html")
```

✅ Successfully exported HTML: flash_sample1_latex_latex.html

In [15]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context1_text + "
print(response.text)
```

```
\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 Apex Innovations}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report assesses the cybersecurity readiness of Apex Innovations based on provid
ed DNS records, port scan results for their external IP and website, and responses t
o a security questionnaire. The analysis indicates a good foundational security post
ure, with particular strengths in user authentication and email protection.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Apex Innovations
    \item \textbf{Email Domain}: \url{apexinnovations.com}
    \item \textbf{Website Domain}: \url{www.apexinnovations.com}
    \item \textbf{External IP (Firewall)}: \seqsplit{72.21.196.160}
    \item \textbf{Website Hosting IPs}: \seqsplit{72.21.196.160}
    \item \textbf{DNS Hosting}: Managed by Apex Innovations (ns1.apexinnovations.co
m, ns2.apexinnovations.com)
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
MFA for Sensitive Data Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
New Employee Security Awareness Training & \ding{51} Yes \\
```

```
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: Apex Innovations reports robust implementation of key se
curity controls, including mandatory Multi-Factor Authentication (MFA) across critic
al access points and comprehensive security awareness training for all employees. Th
is demonstrates a strong commitment to reducing human-factor risks and securing user
credentials.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item The organization manages its own DNS zones (\url{ns1.apexinnovations.com},
\url{ns2.apexinnovations.com}).
    \item The main domain (\url{apexinnovations.com}) resolves to the provided exter
nal IP (\seqsplit{72.21.196.160}).
    \item MX records point to \url{mx1.apexinnovations.com} and \url{mx2.apexinnovat
ions.com}, indicating internal or dedicated mail servers.
    \item The SPF record is configured as \seqsplit{\texttt{v=spf1 include:spf.prote
ction.outlook.com -all}}, suggesting the use of Microsoft 365 for email services.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A DMARC record is present for \url{_dmarc.apexinnovations.com} with a \tex
tbf{reject policy}: \seqsplit{\texttt{v=DMARC1; p=reject; rua=mailto:dmarc_reports@a
pexinnovations.com; fo=1}}.
    \item This policy, combined with the SPF record, provides strong protection agai
nst email spoofing and phishing attempts by instructing receiving servers to reject
unauthorized emails. The inclusion of \texttt{fo=1} means failure in SPF or DKIM wil
l trigger reporting.
\end{itemize}

\noindent \textbf{Conclusion}: DNS and email security measures, including SPF and a
strict DMARC reject policy, are well-implemented, indicating a proactive stance agai
nst email-based threats.

\section{Port Scanning Results}

\subsection*{Website Hosting (\seqsplit{72.21.196.160})}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
These ports are standard for web servers and are expected to be open for a publicly
accessible website. This suggests the website is configured for secure (HTTPS) and s
tandard (HTTP) access.

\subsection*{Firewall / External IP (\seqsplit{72.21.196.160})}
\begin{itemize}
    \item The port scan of the external IP (\seqsplit{72.21.196.160}) reported \text
bf{only ports 80 and 443 as open}.
\end{itemize}
```

```
\noindent \textbf{Analysis}: This indicates that while the website is accessible, th
e firewall is effectively blocking all other inbound traffic to the external IP addr
ess. This is a positive sign of perimeter security, minimizing the attack surface to
only necessary services.

\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 & Strong & MFA implemented for email, computers, and sensiti
ve data. \\
Email Security & Strong & SPF and DMARC with "reject" policy in place; likely using
Microsoft 365. \\
Network Exposure & Secure & Firewall restricts access to only necessary web ports (8
0, 443). \\
Web Hosting & Standard & Standard web ports are open as expected. \\
Policy \& Training & Comprehensive & Acceptable use policy and regular security awar
eness training are in place. \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
Apex Innovations has a solid cybersecurity foundation. To further enhance readiness,
consider the following:
\begin{enumerate}
    \item \textbf{DKIM Implementation}: While SPF and DMARC are in place, ensure Dom
ainKeys Identified Mail (DKIM) is also configured and aligned for comprehensive emai
l authentication. This is crucial for a strict "reject" policy to be fully effectiv
e.
    \item \textbf{Regular Vulnerability Scanning}: Implement routine internal and ex
ternal vulnerability scans to proactively identify and remediate potential weaknesse
s in the network infrastructure and web applications.
    \item \textbf{Incident Response Plan}: Develop or refine an incident response pl
an, including regular testing and tabletop exercises, to ensure preparedness for sec
urity incidents.
    \item \textbf{Asset Management}: Maintain a detailed and up-to-date inventory of
all IT assets to ensure proper security configurations and monitoring.
    \item \textbf{Review Port 80 Security}: While port 80 is standard, ensure that a
ll traffic is redirected to HTTPS (port 443) and that any HTTP-specific vulnerabilit
ies are addressed.
\end{enumerate}

\section{Conclusion}
Apex Innovations demonstrates a commendable level of cybersecurity readiness. The or
ganization has invested in critical security measures such as multi-factor authentic
ation, robust email protection policies, and a well-configured network perimeter. By
addressing the recommended enhancements, Apex Innovations can further strengthen its
security posture against evolving cyber threats.

\vspace{1cm}
```

```
\noindent Prepared by: \\
Cybersecurity Assessment Team\\
Date: October 14, 2025

\end{document}
```

In [45]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_lite_sample1_latex_latex.html")
```

✅ Successfully exported HTML: flash_lite_sample1_latex_latex.html

In [17]:
```
# === SAMPLE 2 ===

# LaTeX input, LaTeX output
response = proModel.generate_content(contents=[prompt_text, context2_text + "\n" +
print(response.text)
```

```
\documentclass[12pt]{article}
\usepackage[letterpaper, margin=1in]{geometry}
\usepackage{amsmath, amssymb}
\usepackage{pifont} % For the checkmark and x-mark symbols
\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
\usepackage{xcolor} % For colors

\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 readiness assessment for G.A.S. Inc., based on
publicly available technical data and a self-reported security questionnaire. The fi
ndings reveal critical vulnerabilities in network perimeter security, email authenti
cation, and internal security policies. The organization's current posture presents
a high risk of unauthorized access, data breach, and email-based attacks such as phi
shing and spoofing. Immediate remediation is strongly advised.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: G.A.S. Inc.
    \item \textbf{Email Domain}: gasinc.net
    \item \textbf{Website Domain}: \url{www.gasinc.net}
    \item \textbf{External / Website IP}: 104.28.1.189
    \item \textbf{Email Hosting}: MailHostBox (\url{mx.mailhostbox.com})
\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 & \textcolor{red}{\ding{55}} No \\
MFA for Computer Login & \textcolor{red}{\ding{55}} No \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \textcolor{red}{\ding{55}} No \\
```

```
New Employee Security Awareness Training & \textcolor{red}{\ding{55}} No \\
Annual All-Employee Security Training & \textcolor{red}{\ding{55}} No \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: The organization lacks fundamental security controls. Th
e absence of Multi-Factor Authentication (MFA) for email and computer access creates
a significant risk of account compromise. Furthermore, the lack of an acceptable use
policy and any form of security awareness training indicates a deficient security cu
lture, leaving the organization vulnerable to human error and social engineering att
acks.

\section{DNS \& Email Security}

\subsection*{SPF Record}
\begin{itemize}
    \item The organization has an SPF record: \seqsplit{\texttt{v=spf1 include:spf.m
ailhostbox.com ~all}}.
    \item The \texttt{~all} (SoftFail) mechanism instructs receiving servers to acce
pt and mark, but not reject, emails from unauthorized sources. This significantly we
akens its effectiveness against domain spoofing.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A DNS query for the DMARC record (\seqsplit{\texttt{\_dmarc.gasinc.net}})
returned \texttt{NXDOMAIN}, confirming that \textbf{no DMARC record exists}.
    \item This is a critical security gap, as it leaves the domain highly susceptibl
e to being impersonated in phishing and spoofing attacks. There is no policy to inst
ruct receiving mail servers on how to handle unauthenticated email.
\end{itemize}

\noindent \textbf{Conclusion}: Email security is poor. The weak SPF policy and compl
ete absence of DMARC provide inadequate protection against email-based threats.

\section{Port Scanning Results}

\subsection*{Firewall / External IP (104.28.1.189)}
A port scan of the primary external IP address revealed numerous open ports, indicat
ing a severely misconfigured and insecure network perimeter.
\begin{itemize}
    \item \textbf{Port 21 (FTP)}: \textbf{Open}. FTP is an unencrypted protocol. Exp
osing it to the internet risks credential theft and unauthorized file access.
    \item \textbf{Port 22 (SSH)}: \textbf{Open}. While secure, exposing SSH directly
to the internet makes it a target for brute-force attacks.
    \item \textbf{Port 25 (SMTP)}: \textbf{Open}. This is unexpected, as the organiz
ation's email is hosted externally. This could be an open mail relay, a serious secu
rity risk.
    \item \textbf{Port 80 (HTTP) \& 443 (HTTPS)}: \textbf{Open}. These are expected
for hosting a public website.
    \item \textbf{Port 110 (POP3)}: \textbf{Open}. POP3 is an unencrypted email prot
ocol, posing a risk of password interception.
    \item \textbf{Port 3389 (RDP)}: \textbf{Open}. Exposing Remote Desktop Protocol
directly to the internet is extremely dangerous and a primary vector for ransomware
attacks.
```

```
\end{itemize}
\noindent \textbf{Conclusion}: The network perimeter is critically exposed. The pres
ence of multiple open ports for unencrypted and high-risk services creates a large a
nd easily exploitable attack surface.

\section{Risk Assessment \& Readiness Summary}
\begin{table}[h!]
\centering
\caption{Readiness Summary}
\label{tab:readiness_summary}
\begin{tabular}{l l l}
\toprule
\textbf{Category} & \textbf{Status} & \textbf{Notes} \\
\midrule
Authentication Security & Weak & No MFA for email or computers. \\
Email Security & Weak & No DMARC and a weak SPF "SoftFail" policy. \\
Network Exposure & \textbf{Critical Risk} & RDP, FTP, and other insecure ports are e
xposed. \\
Web Hosting & High Risk & Hosted on a server with many vulnerable services. \\
Policy \& Training & Non-Existent & No AUP or security awareness training reported.
\\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
The following actions are recommended to address the identified critical risks. Item
s are listed in order of priority.

\begin{enumerate}
    \item \textbf{Secure the Network Perimeter (Immediate Priority)}:
        \begin{itemize}
            \item Close all unnecessary ports on the firewall, especially \textbf{21
(FTP)}, \textbf{110 (POP3)}, and \textbf{3389 (RDP)}.
            \item If remote access is required, implement a Virtual Private Network
(VPN) and close ports 22 (SSH) and 3389 (RDP) to the public internet.
            \item Disable and replace unencrypted protocols like FTP and POP3 with s
ecure alternatives (e.g., SFTP, IMAPS).
        \end{itemize}
    \item \textbf{Implement Multi-Factor Authentication (MFA)}:
        \begin{itemize}
            \item Immediately enforce MFA for all user accounts, starting with emai
l, remote access (VPN), and administrative accounts.
        \end{itemize}
    \item \textbf{Strengthen Email Security}:
        \begin{itemize}
            \item Implement a DMARC record, starting with a monitoring policy (\text
tt{p=none}) and progressing to a quarantine or reject policy (\texttt{p=reject}).
            \item Modify the SPF record to use a "HardFail" mechanism (\texttt{-al
l}) instead of "SoftFail" (\texttt{~all}).
        \end{itemize}
    \item \textbf{Establish Security Policies and Training}:
        \begin{itemize}
            \item Develop and enforce an employee Acceptable Use Policy (AUP).
            \item Implement a mandatory security awareness training program for all
employees upon hiring and at least annually thereafter.
```

```
        \end{itemize}
\end{enumerate}

\section{Conclusion}
G.A.S. Inc. currently has a very low level of cybersecurity readiness. The combinati
on of an exposed network perimeter, weak authentication controls, and inadequate ema
il security places the organization at an extremely high risk of a significant cyber
attack. The lack of security policies and training further exacerbates this risk. Th
e recommendations outlined in this report should be implemented with urgency to miti
gate these critical vulnerabilities and establish a basic security foundation.

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

\end{document}
```

In [46]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "pro_sample2_latex_latex.html")
```

✅ Successfully exported HTML: pro_sample2_latex_latex.html

In [19]:
```
response = flashModel.generate_content(contents=[prompt_text, context2_text + "\n"
print(response.text)
```

```
\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 assesses the cybersecurity posture of G.A.S. Inc. based on an analysis o
f DNS records, email security configurations (SPF, DMARC), external port scans, and
a self-reported security questionnaire. The findings reveal significant vulnerabilit
ies across network perimeter security, email protection, user authentication, and or
ganizational policies and training, indicating a low level of cybersecurity readines
s.

\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}: \seqsplit{104.28.1.189}
    \item \textbf{DNS Hosting}: Self-hosted (\url{dns1.gasinc.net}, \url{dns2.gasin
c.net}), resolving to the organization's external IP.
\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 & \ding{55} No \\
MFA for Computer Login & \ding{55} No \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{55} No \\
```

```
New Employee Security Awareness Training & \ding{55} No \\
Annual All-Employee Security Training & \ding{55} No \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: G.A.S. Inc. exhibits significant gaps in fundamental sec
urity practices. Multi-Factor Authentication (MFA) is largely absent for common acce
ss points like email and computer logins, which are prime targets for attackers. The
complete lack of an Acceptable Use Policy and any form of security awareness trainin
g leaves the organization highly vulnerable to social engineering and internal threa
ts.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS for \url{gasinc.net} is self-hosted on \url{dns1.gasinc.net} and \url
{dns2.gasinc.net}, both of which resolve to the organization's primary external IP
(\seqsplit{104.28.1.189}). This single point of failure configuration for DNS, along
side other services, increases risk.
    \item The A record for \url{gasinc.net} points to \seqsplit{104.28.1.189}.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item Email services are hosted externally by Mailhostbox (\seqsplit{\texttt{\ur
l{mx.mailhostbox.com}}}).
    \item \textbf{SPF record} is present: \seqsplit{\texttt{v=spf1 include:\url{spf.
mailhostbox.com} ~all}}. While present, the `~all` mechanism indicates a "SoftFail"
policy, which is less secure than a "Fail" (`-all`) policy for preventing email spoo
fing.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A DMARC record for \url{_dmarc.gasinc.net} was \textbf{not found} (NXDOMAI
N).
\end{itemize}

\noindent \textbf{Conclusion}: The absence of a DMARC record is a critical vulnerabi
lity. Without DMARC, G.A.S. Inc.'s email domain is highly susceptible to spoofing at
tacks, which can be used for phishing against employees, customers, or partners. The
"SoftFail" SPF policy further weakens email-based defenses.

\section{Port Scanning Results}

\subsection*{External IP / Firewall (\seqsplit{104.28.1.189})}
This single external IP appears to serve as the organization's primary internet gate
way, firewall, and host for various critical services.
\begin{itemize}
    \item \textbf{Port 21 (FTP)}: Open (\faExclamationTriangle) --- FTP is an insecu
re protocol that transmits credentials and data in plain text. Its exposure is a hig
h-risk vulnerability.
    \item \textbf{Port 22 (SSH)}: Open (\faExclamationTriangle) --- SSH provides sec
ure remote access but requires stringent security measures (e.g., strong, key-based
```

```
authentication, IP whitelisting, MFA) to prevent unauthorized access.
    \item \textbf{Port 25 (SMTP)}: Open (\faExclamationTriangle) --- While essential for mail servers, its presence on the organization's primary IP suggests an internal mail relay or outgoing SMTP server. Given external MX records, its direct exposure warrants careful review to prevent abuse.
    \item \textbf{Port 80 (HTTP)}: Open (\faCheck) --- Expected for web services.
    \item \textbf{Port 110 (POP3)}: Open (\faExclamationTriangle) --- POP3 is an insecure protocol that transmits credentials in plain text. Its exposure is a high-risk vulnerability. Secure alternatives like POP3S or IMAPS should be used.
    \item \textbf{Port 443 (HTTPS)}: Open (\faCheck) --- Expected for secure web services.
    \item \textbf{Port 3389 (RDP)}: Open (\faSkullCrossbones) --- Direct exposure of Remote Desktop Protocol (RDP) to the internet is a \textbf{critical security risk}. RDP is frequently targeted by attackers for initial access and ransomware deployment. This must be secured immediately, ideally placed behind a VPN with MFA or restricted by IP.
\end{itemize}

\noindent \textbf{Conclusion}: The organization's external IP presents a dangerously wide attack surface. Critical, high-risk services like FTP, POP3, and especially RDP are directly exposed to the internet. This configuration makes G.A.S. Inc. extremely vulnerable to brute-force attacks, credential theft, and exploitation of service 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 & \faExclamationTriangle\ Weak & Significant gaps in MFA for email and computers. \\
Email Security & \faSkullCrossbones\ Critical & Missing DMARC, 'SoftFail' SPF; high spoofing risk. \\
Network Exposure & \faSkullCrossbones\ Critical & Multiple high-risk ports (RDP, FTP, POP3) directly exposed. \\
Web Hosting & \faExclamationTriangle\ Moderate & Standard ports, but hosted on the main external IP alongside other services. \\
Policy \& Training & \faSkullCrossbones\ Critical & Complete absence of AUP and security training. \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
G.A.S. Inc. requires immediate and comprehensive cybersecurity improvements across multiple domains.

\subsection*{Immediate Action (Critical Risks)}
\begin{enumerate}
    \item \textbf{Secure RDP (Port 3389)}: Immediately close or restrict direct internet access to Port 3389 (RDP). Implement a secure remote access solution, such as a VPN gateway with Multi-Factor Authentication (MFA), through which all RDP connection
```

```
s must be made.
    \item \textbf{Close Insecure Ports}: Close Port 21 (FTP) and Port 110 (POP3). If file transfer is needed, implement SFTP/FTPS with strong authentication. For email access, enforce the use of secure protocols like IMAPS (Port 993) or POP3S (Port 995).
    \item \textbf{Implement DMARC}: Deploy a DMARC record for \url{gasinc.net} with at least a `p=quarantine` policy. Monitor DMARC reports to identify legitimate sending sources and eventually transition to a `p=reject` policy to prevent email spoofing effectively.
\end{enumerate}

\subsection*{User Access & Authentication}
\begin{enumerate}
    \item \textbf{MFA for Email}: Implement mandatory MFA for all email accounts to prevent unauthorized access even if passwords are compromised.
    \item \textbf{MFA for Computer Logins}: Introduce MFA for user and administrator logins to company computers and servers.
    \item \textbf{Strengthen SSH Security}: For Port 22 (SSH), implement strong, key-based authentication, disable password authentication, enforce IP whitelisting, and consider rate-limiting failed login attempts.
\end{enumerate}

\subsection*{Email Security Enhancements}
\begin{enumerate}
    \item \textbf{Strengthen SPF}: Change the SPF record from `~all` (SoftFail) to `-all` (Fail) once confident that all legitimate sending sources are included, providing stronger protection against spoofing.
    \item \textbf{Implement DKIM}: Ensure DomainKeys Identified Mail (DKIM) is properly configured for all outbound email to further enhance email authenticity.
\end{enumerate}

\subsection*{Policies & Training}
\begin{enumerate}
    \item \textbf{Acceptable Use Policy (AUP)}: Develop and enforce a clear AUP that outlines acceptable and unacceptable use of company IT resources.
    \item \textbf{Security Awareness Training}:
        \begin{itemize}
            \item Implement mandatory security awareness training for all new employees during onboarding.
            \item Conduct annual mandatory security awareness training for all employees, covering topics such as phishing, password hygiene, social engineering, and incident reporting.
        \end{itemize}
\end{enumerate}

\subsection*{Infrastructure & General Security}
\begin{enumerate}
    \item \textbf{DNS Review}: Evaluate migrating DNS services to a dedicated, resilient, and professionally managed external provider to enhance availability and security, separating it from the primary external IP.
    \item \textbf{Firewall Audit}: Conduct a comprehensive audit of firewall rules and network configurations to ensure only essential services are exposed and proper segmentation is in place.
    \item \textbf{Patch Management}: Implement a robust patch management program for all operating systems, applications, and network devices, especially those exposed to the internet.
```

```
    \item \textbf{Incident Response Plan}: Develop, document, and regularly test a c
ybersecurity incident response and disaster recovery plan.
    \item \textbf{Strong Password Policy}: Enforce a strong password policy requirin
g complexity, length, and regular changes, complementing MFA.
\end{enumerate}

\section{Conclusion}
G.A.S. Inc. currently faces a high level of cybersecurity risk due to critical vulne
rabilities in network exposure, email security, user authentication, and a complete
lack of foundational security policies and training. Addressing the critical risks,
particularly the exposed RDP port and missing DMARC, should be the immediate priorit
y. A systematic implementation of the recommended security controls and practices is
essential to significantly improve the organization's cybersecurity readiness and pr
otect against potential breaches.

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

\end{document}
```

In [47]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_sample2_latex_latex.html")
```

✅ Successfully exported HTML: flash_sample2_latex_latex.html

In [21]:
```
response = flashLiteModel.generate_content(contents=[prompt_text, context2_text + "
print(response.text)
```

```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 assesses the cybersecurity readiness of G.A.S. Inc. based on technical s
cans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The
findings highlight areas of strength and significant opportunities for improvement,
particularly in user security practices and policy implementation.

\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 (Firewall)}: \seqsplit{104.28.1.189}
\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 & \ding{55} No \\
MFA for Computer Login & \ding{55} No \\
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{55} No \\
New Employee Security Awareness Training & \ding{55} No \\
Annual All-Employee Security Training & \ding{55} No \\
\bottomrule
```

```
\end{tabular}
\end{table}

\noindent \textbf{Summary}: The responses indicate significant gaps in foundational cybersecurity practices. The absence of Multi-Factor Authentication (MFA) for email and computer logins, coupled with no acceptable use policy and a lack of security aw areness training for any employees, presents substantial risks. While MFA is used fo r sensitive data systems, the overall user access security is weak.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item The organization's domain (\url{gasinc.net}) has A records pointing to \se qsplit{104.28.1.189}, which is also identified as the external IP.
    \item Mail is handled by \texttt{mailhostbox.com} services, indicated by MX reco rds.
    \item \textbf{SPF record} is configured as \seqsplit{\texttt{"v=spf1 include:sp f.mailhostbox.com ~all"}} . This is a positive step to help prevent email spoofing.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A DMARC lookup for \url{_dmarc.gasinc.net} returned \texttt{NXDOMAIN}. Thi s means no DMARC record is published.
\end{itemize}

\noindent \textbf{Conclusion}: While basic SPF is in place for email authentication, the absence of a DMARC record leaves the email domain vulnerable to spoofing and phi shing attacks. This is a critical gap in email security.

\section{Port Scanning Results}

\subsection*{Website Hosting (\url{www.gasinc.net} / \seqsplit{104.28.1.189})}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
These ports are standard for a web server and are expected to be open for a publicly accessible website.

\subsection*{External IP / Firewall (\seqsplit{104.28.1.189})}
\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}

\noindent \textbf{Analysis}: The extensive list of open ports on the external IP add ress (which appears to be the firewall or a directly exposed server) is a significan t security concern. Services like FTP, SSH, SMTP, POP3, and RDP are often targets fo r attackers. Without proper access controls, monitoring, and security hardening on t
```

```
hese services, they represent a broad attack surface.

\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/computers; no AUP. \\
Email Security & Moderate & SPF present, but DMARC missing. \\
Network Exposure & High Risk & Numerous open ports on external IP. \\
Policy \& Training & Non-existent & No AUP, no security training. \\
Sensitive Data Access & Moderate & MFA for sensitive systems is good, but user accou
nts are not secured. \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
Based on the assessment, G.A.S. Inc. has significant cybersecurity vulnerabilities t
hat require immediate attention. The following recommendations are prioritized:

\begin{enumerate}
    \item \textbf{Implement MFA Everywhere}: Mandate MFA for all access to email, co
mputer logins, and any other applicable systems. This is the single most effective c
ontrol against account compromise.
    \item \textbf{Establish Security Policies}: Develop and implement an Acceptable
Use Policy (AUP) that clearly outlines user responsibilities regarding IT system usa
ge and data security.
    \item \textbf{Conduct Security Awareness Training}: Implement mandatory security
awareness training for all employees, both for new hires and annually. This should c
over common threats like phishing, social engineering, and password security.
    \item \textbf{Secure External Services}:
    \begin{itemize}
        \item \textbf{Firewall Configuration Review}: Conduct a thorough review of t
he firewall configuration. Close all unnecessary open ports. Only allow access to es
sential services and restrict access to trusted IP addresses where possible.
        \item \textbf{Service Hardening}: Ensure all open services (FTP, SSH, SMTP,
POP3, RDP) are hardened according to best practices. This includes strong password p
olicies, disabling anonymous access, and secure configuration. Consider disabling se
rvices like FTP and POP3 if not strictly required.
        \item \textbf{RDP Access}: If RDP is required, ensure it is not directly exp
osed to the internet. Use a VPN or a secure gateway.
    \end{itemize}
    \item \textbf{Implement DMARC}: Publish a DMARC record for \url{gasinc.net} with
a protective policy (e.g., \texttt{p=quarantine} or \texttt{p=reject}) to further en
hance email security and protect against spoofing.
    \item \textbf{Regular Vulnerability Scanning}: Implement regular internal and ex
ternal vulnerability scans to identify and address potential weaknesses proactively.
    \item \textbf{Logging and Monitoring}: Enable comprehensive logging for all crit
ical systems and the firewall, and establish a process for regular review and incide
nt detection.
\end{enumerate}
```

```
\section{Conclusion}
G.A.S. Inc. is currently in a low state of cybersecurity readiness, with critical ga
ps in user authentication, policy, training, and external network security. The nume
rous open ports on the external IP represent a high-risk exposure. Addressing these
recommendations, especially the implementation of MFA and securing external service
s, is crucial to mitigate significant cybersecurity threats.

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

\end{document}
```

In [48]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_lite_sample2_latex_latex.html")
```

✅ Successfully exported HTML: flash_lite_sample2_latex_latex.html

Summary

Qualitative Analysis: Score 1-3 from least to greatest.

Input	Output	2.5 Pro	2.5 Flash	2.5 Flash Lite
Markdown	Markdown	1	1	2
Markdown	JSON	3	3	1
PDF	Markdown	2	2	1
PDF	JSON	3	3	2
PDF	LaTeX	3	1	1
LaTeX	LaTeX	3	3	3

Notes:

Markdown/Markdown:

- Pro Markdown Markdown: Sample 1 did not generate the cybersecurity team at the end. Headers were not easy to read as the font size was similar to the other paragraph text. Sample 2 had some text not indented into separate newlines.
- Flash Markdown Markdown: Sample 1 had more text not properly moved into separate newlines. Headers were also not easy to read. Table text was center aligned and harder to read at a glance. Sample 2 had similar issues.
- Flash Lite Markdown Markdown: Sample 1 had text not properly moved into separate newlines and bullet-pointed lists not rendering due to the newline issue. Though, the

tables wer left-aligned and easier to understand than the Flash model's output. Sample 2 in particular had better results than the Flash and maybe even the Pro model.
- Overall, did not perform as consistent as I would have liked. Markdown being used as both the input and output lead to inconsistencies in the styling.

Markdown/JSON:

- Pro Markdown JSON: For the bare bone minimum text per header, JSON works quite effectively. The Pro model in particular was able to hit home all of the points. It would only lose points on styling, as with this method, the styling would be handed over to frontend rather than being handled by the backend (which, if communicated effectively, would not be an issue).
- Flash Markdown JSON: Similar to the Pro model, the JSON output works effectively to generate only the headers of information we provide.
- Flash Lite Markdown JSON: For some reason, Sample 1 was able to generate the emojis. However, it also generated some of the Markdown text which was not expected. Lost points on mixing up the output formatting.
- Overall, performed as consistent as I expected- the Pro and Flash models in particular. If we choose to have the frontend capture most of the formatting of the PDF, then we will be able to use the JSON output.

PDF/Markdown:

- Pro PDF Markdown: Sample 1 was not able to move some of the text properly into separate newlines, leading to breaks in the bullet-pointed formatting. Similarly, Sample 2 had breaks in the numbered list for Recommendations. However, it was able to come up with creative emokis and formatted the tables in a way that was easy to understand at a glance.
- Flash PDF Markdown: Sample 1 also had some breaks in the bullet-pointed format. Sample 2 however, had more tables and was easy-to-read at a glance. Both had emojis like the Pro model's output but limited to checks and x's.
- Flash Lite PDF Markdown: Sample 1 did not have a proper header for the report and most of the paragraphs were not indented correctly into new, bullet-pointed lines. Sample 2 however, was able to generate successfully without any errors in the response. The only potential issue was lack of emoji's to simplify information and have it easier to see at a glance.
- Overall, the PDF input was able to get more context to the model as compared to the Markdown/Markdown reports, but the Markdown output was still leading to inconsistencies in the styling.

PDF/JSON:

- Pro PDF JSON: Best of the three models due to it's extensive information, even putting the potential risk for Sample 1. Sample 2 had capital letters with URGENT on the recommendations which was extremely helpful.

- Flash PDF JSON: Included strange spacing in the beginning for a couple of the string values trying to mimic the bullet-pointed format. Not sure if we like those.
- Flash Lite PDF JSON: Not the best but still performed well compared to other input/output tests.
- Overall, the PDF input and JSON output performed the highest compared to all other report types. The PDF input provided enough context to the model and JSON has the most consistent output. Similar with the other JSON output, if we choose to have the JSON output we have to have frontend capture most if not all of the formatting for the PDF. We will go with the Flash as the free tier rate limits are much lower and easier to manage than the Pro.

PDF/LaTeX

- Pro PDF LaTeX: Really good. Pretty much exactly what we want aside from the repeat/broken LaTeX at the bottom.
- Flash PDF LaTeX: The LaTeX broke, probably due to PDF input or something. In Sample 2 it looks like half Tex and half Markdown.
- Flash Lite LaTeX: Didn't generate as well as I hoped.
- Overall, the LaTeX output has potential to be the best option. It is able to still generate the emojis while having a structure, unline Markdown and JSON. Perhaps changing the input type also to LaTeX and having a template will have the best results.

LaTeX/LaTeX

- Pro LaTeX LaTeX: Has all the information and generated pretty well. A couple things were in-line tex and inline doesn't allow for spaces so it looks a little weird.
- Flash LaTeX LaTeX: Also has all the information.
- Flash Lite LaTeX LaTeX: Some of the text was short and minimal.
- Overall, the processing from LaTeX to HTML to view it was the hardest part. Pretty much all the information was there and very consistent between generations. Best way thus far for getting consistent results.

Prompt Engineering

Previous research has proven that the LaTeX input and LaTeX output had the most potential for consistent results. Now we will finesse the process with prompt engineering to further ensure the LaTeX report generates as consistent as possible.

We will only be using the Pro and Flash models, as the Flash Lite did not perform as well.

In [50]:
```
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')
```

In [51]:
```
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 [52]:
```
proModel = genai.GenerativeModel('gemini-2.5-pro')
flashModel = genai.GenerativeModel('gemini-2.5-flash')
```

In [53]:
```
import pypandoc


def _extract_latex_content(text_content: str) -> str | None:
    """
    Internal helper to extract LaTeX content from raw text or a JSON block.
    """
    latex_content = ""
    try:
        # Check for code-fenced JSON structure first
        json_match = re.search(r'```json\s*(.*?)\s*```', text_content, re.DOTALL)
        if json_match:
            json_string = json_match.group(1).strip()
            try:
                data = json.loads(json_string)
                latex_content = data.get("text", "")
            except json.JSONDecodeError:
                print("Warning: JSON inside the code block is not valid. Treating e
                latex_content = text_content
        else:
            # Try to load the entire content as plain JSON
            try:
                data = json.loads(text_content)
                latex_content = data.get("text", "")
            except json.JSONDecodeError:
                # If neither works, treat the entire input as LaTeX text
                latex_content = text_content

        if not isinstance(latex_content, str):
```

```
            print(f"Error: LaTeX content is not a string, it's a {type(latex_conten
            return None

        return latex_content

    except Exception as e:
        print(f"An unexpected error occurred during content extraction: {e}")
        return None


def _wrap_html_shell(body_content: str, title: str = "LaTeX Export") -> str:
    """
    Internal helper to wrap HTML body content in a full document
    with KaTeX for math rendering.
    """
    return f"""
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>{title}</title>

    <!-- KaTeX CSS -->
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/kat

    <!-- KaTeX JS -->
    <script src="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/katex.min.js" xinte

    <!-- KaTeX Auto-render extension -->
    <script src="https://cdn.jsdelivr.net/npm/katex@0.16.9/dist/contrib/auto-render

    <style>
        /* Base styles */
        body {{
            font-family: 'Noto Sans', 'Arial', sans-serif;
            line-height: 1.6;
            color: #333;
            max-width: 800px;
            margin: 2rem auto;
            padding: 0 1rem;
        }}
        h1, h2, h3, h4, h5, h6 {{
            color: #1a1a1a;
            margin-top: 1.5em;
            margin-bottom: 0.5em;
        }}
        p {{
            margin-bottom: 1em;
        }}
        pre {{
            background-color: #f4f4f4;
            padding: 1rem;
            border-radius: 4px;
            overflow-x: auto;
            border: 1px solid #ddd;
```

```
            font-family: monospace;
        }}
        code {{
            font-family: monospace;
            background-color: #f0f0f0;
            padding: 2px 4px;
            border-radius: 3px;
        }}
        ul, ol {{
            padding-left: 2em;
            margin-bottom: 1em;
        }}
        li {{
            margin-bottom: 0.5em;
        }}

        /* KaTeX specific styling for display math */
        .katex-display {{
            overflow-x: auto;
            overflow-y: hidden;
            padding: 0.5em 0;
        }}

        /* Custom LaTeX styles */
        .table-wrapper {{
            margin: 1.5em 0;
            overflow-x: auto;
        }}
        table {{
            border-collapse: collapse;
            width: 100%;
            margin-bottom: 1.5rem;
        }}
        caption {{
            font-weight: bold;
            font-size: 1.1em;
            margin-bottom: 0.5em;
            text-align: left;
        }}
        th, td {{
            border: 1px solid #ddd;
            padding: 10px;
            text-align: left;
            vertical-align: top;
        }}
        th {{
            background-color: #e9ecef;
            font-weight: bold;
        }}
        .latex-url, .seqsplit {{
            word-break: break-all;
        }}
    </style>
</head>
<body>
{body_content}
```

```
<!-- KaTeX auto-render script -->
<script>
    document.addEventListener("DOMContentLoaded", function() {{
        renderMathInElement(document.body, {{
            delimiters: [
                {{left: "$$", right: "$$", display: true}},
                {{left: "$", right: "$", display: false}},
                {{left: "\\(", right: "\\)", display: false}},
                {{left: "\\[", right: "\\]", display: true}}
            ],
            throwOnError : false
        }});
    }});
</script>
</body>
</html>
"""

def generate_html_from_latex(text_content: str) -> str | None:
    """
    Extracts LaTeX content and converts it into a full, styled HTML string
    using pypandoc.

    This is the most robust method but requires:
    1. `pip install pypandoc`
    2. The Pandoc binary to be installed on the system:
       https://pandoc.org/installing.html

    Args:
        text_content (str): The raw text content (LaTeX or JSON-wrapped).

    Returns:
        str or None: The complete HTML string, or None if conversion fails.
    """

    latex_content = _extract_latex_content(text_content)
    if latex_content is None:
        return None

    if pypandoc is None:
        print("Error: pypandoc library is not imported. Cannot convert.")
        return None

    try:
        # Extract content only between \begin{document} and \end{document}
        # Pandoc is smart enough to handle the full document, but this
        # ensures we only get the body content if needed.
        body_match = re.search(r'\\begin\{document\}(.*?)\\end\{document\}', latex_
        if body_match:
            content_to_convert = body_match.group(1).strip()
        else:
            content_to_convert = latex_content

        # Use pandoc to convert.
        # --katex tells pandoc to format math for KaTeX.
```

```
        # --standalone would wrap it in a full HTML doc, but we want
        # to use our own shell to control the CSS and JS.
        html_output = pypandoc.convert_text(
            content_to_convert,
            'html',
            format='latex',
            extra_args=['--katex']
        )

        # Pandoc will correctly handle \ding and other symbols.
        return _wrap_html_shell(html_output, "Pandoc LaTeX Export")

    except FileNotFoundError:
        print("="*50)
        print("ERROR: Pandoc executable not found.")
        print("Please install Pandoc from https://pandoc.org/installing.html")
        print("="*50)
        return None
    except Exception as e:
        print(f"An unexpected error occurred during Pandoc conversion: {e}")
        return None
```

In [ ]:

```
import textwrap

prompt_text = textwrap.dedent(r'''You are an expert-level Cybersecurity Analyst and
Your task is to receive a list of JSON objects containing raw technical data (dig o
You must analyze, correlate, and synthesize this data into a single, complete, and

Core Instructions:
1. Parse & Correlate: You must parse all JSON inputs. The data is fragmented, so yo
    - The structured JSON (questionnaire) provides the "Organization Name," "Email
    - The dig output for the domain (e.g., valier.k12.mt.us) provides the A records
    - The dig output for _dmarc provides the DMARC policy.
    - The port scan results must be matched to their respective IPs (the "External

2. Analyze & Synthesize: Do not just list the data. You must analyze it.
    - Synthesize the questionnaire answers (e.g., all "Yes" answers) into a summary
    - Analyze the technical records. For example, identify that p=reject is a stron
    - Extract the date from the port scan logs (e.t., 2025-07-18) and use it as the

3. Generate New Content: The report must include analytical sections that are not d
    - An "Overview" section.
    - A "Risk Assessment & Readiness Summary" table.
    - A "Recommendations" section (e.g., verify DKIM, create an incident response p
    - A "Conclusion" section.

4. Strict LaTeX Formatting:
    - The output MUST be a single, complete LaTeX document.
    - It must start with \documentclass[12pt]{article} and end with \end{document}.
    - It MUST include the following packages in the preamble: geometry, pifont, boo
    - Use booktabs (\toprule, \midrule, \bottomrule) for all tables.
    - Use \ding{51} Yes for "Yes" answers in the questionnaire table.
    - Use \seqsplit{\texttt{...}} for long technical strings (IP lists, DMARC/SPF r
    - Use \url{...} for all domains and email addresses.
''')
```

```
context1_text = 'Context:\n'
context2_text = 'Context:\n'
example_text = 'Example Task:\nFollow the structure, formatting, and analytical sty

filepaths = ["report_template/test_questionnaire.json", "report_template/test_port_
latex_file_path = "report_template/test_report.tex"

sample1_filepaths = ["report_sample1/sample1_questionnaire.json", "report_sample1/s
sample2_filepaths = ["report_sample2/sample2_questionnaire.json", "report_sample2/s

for file in filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            example_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

with open(latex_file_path, 'r') as file:
    latex_content = file.read()
    example_text += latex_content

print("=======  Example ==========")
print(example_text)
print("==========================")

for file in sample1_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context1_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 1 =========")
print(prompt_text)
print(context1_text)
print("==========================")

for file in sample2_filepaths:
    try:
        with open(file, 'r', encoding='utf-8') as f:
            data = json.load(f)
            context2_text += f"{file}:\n{json.dumps(data,indent=2)}\n--\n"

    except FileNotFoundError:
```

```
        f"[ERROR] File not found at path: {file}"
    except json.JSONDecodeError:
        f"[ERROR] Failed to decode JSON from file: {file}. Please check the file's
    except Exception as e:
        f"[ERROR] An unexpected error occurred: {e}"

print("======== Sample 2 =========")
print(prompt_text)
print(context2_text)
print("==========================")
```

======= Example ==========
Example Task:
Follow the structure, formatting, and analytical style of this example precisely.tem
plate/test_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Valier School District",
    "Email Domain": "valier.k12.mt.us",
    "Website Domain": "www.valier.k12.mt.us",
    "External IP": "216.220.16.170",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
```

--
template/test_port_scan_external_ip.json:

```
{
  "text": "-------------------------------------------------\nScanning Target: 216.
220.16.170\nScanning started at:2025-07-18 22:12:17.055226\n-----------------------
-------------------------\nno ports open\n"
}
```

--
template/test_port_scan_web.json:

```
{
  "text": "-------------------------------------------------\nScanning Target: 216.
239.32.21\nScanning started at:2025-07-18 22:09:34.408091\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open\n"
}
```

--
template/test_dns_dig_email.json:

```
{
  "text": "id 49113\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\nvalier.
k12.mt.us. IN ANY\n;ANSWER\nvalier.k12.mt.us. 3600 IN SOA cudess1.umt.edu. dns-reque
st.umt.edu. 2024030501 21600 900 1209600 86400\nvalier.k12.mt.us. 3600 IN NS ens-o1.
umt.edu.\nvalier.k12.mt.us. 3600 IN NS cudess2.umt.edu.\nvalier.k12.mt.us. 3600 IN N
S cudess1.umt.edu.\nvalier.k12.mt.us. 3600 IN A 216.239.38.21\nvalier.k12.mt.us. 360
0 IN A 216.239.32.21\nvalier.k12.mt.us. 3600 IN A 216.239.34.21\nvalier.k12.mt.us. 3
600 IN A 216.239.36.21\nvalier.k12.mt.us. 3600 IN MX 1 aspmx.l.google.com.\nvalier.k
12.mt.us. 3600 IN MX 10 aspmx2.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 10 aspm
x3.googlemail.com.\nvalier.k12.mt.us. 3600 IN MX 5 alt1.aspmx.l.google.com.\nvalier.
k12.mt.us. 3600 IN MX 5 alt2.aspmx.l.google.com.\nvalier.k12.mt.us. 3600 IN TXT \"v=
spf1 include:_spf.google.com include:mg.infinitecampus.org -all\"\n;AUTHORITY\n;ADDI
TIONAL\n"
}
```

--
template/test_dns_dig_email_dmarc.json:

```
{
  "text": "id 45565\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
valier.k12.mt.us. IN ANY\n;ANSWER\n_dmarc.valier.k12.mt.us. 3600 IN TXT \"v=DMARC1;
p=reject; rua=mailto:dmarc@valier.k12.mt.us\"\n;AUTHORITY\n;ADDITIONAL\n"
```

```
}
--
\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 Valier School District}}
\author{Date: July 18, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report evaluates the cybersecurity posture of Valier School District based on t
echnical scans (DNS, DMARC, and port scanning) and a self-reported security question
naire. The findings reflect a strong commitment to foundational cybersecurity practi
ces across user access, email protection, network exposure, and staff awareness.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Valier School District
    \item \textbf{Email Domain}: valier.k12.mt.us
    \item \textbf{Website Domain}: \url{www.valier.k12.mt.us}
    \item \textbf{External IP (Firewall)}: 216.220.16.170
    \item \textbf{Website Hosting IPs}: \seqsplit{216.239.32.21, 216.239.34.21, 216.
239.36.21, 216.239.38.21}
    \item \textbf{DNS Hosting}: Managed by University of Montana (umt.edu nameserver
s)
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
```

```
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: The district reports complete implementation of basic cy
ber hygiene practices, especially user authentication (Multi-Factor Authentication)
and routine training. This indicates a proactive and policy-driven approach to risk
mitigation.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS is managed by the University of Montana (\url{cudess1.umt.edu}, \url{c
udess2.umt.edu}), suggesting centralized and professionally administered DNS.
    \item A records point to IPs within Google's network (likely Google Sites hostin
g for web content).
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The district uses Google Workspace (Gmail) for email, as shown by multiple
\seqsplit{\texttt{\url{aspmx.l.google.com}}} MX records.
    \item \textbf{SPF record} is correctly configured: \seqsplit{\texttt{v=spf1 incl
ude:\url{spf.google.com} include:\url{mg.infinitecampus.org -all}}}. This helps miti
gate spoofing by defining authorized mail senders.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A valid DMARC record exists with a \textbf{reject policy}: \seqsplit{\text
tt{v=DMARC1; p=reject; rua=\url{mailto:dmarc@valier.k12.mt.us}}}.
    \item This instructs receiving servers to reject unauthenticated mail, providing
strong protection against phishing.
\end{itemize}

\noindent \textbf{Conclusion}: DNS and email protections (SPF, DMARC, and hosting se
curity) are configured correctly and follow best practices.

\section{Port Scanning Results}

\subsection*{Website Hosting (Google IP: 216.239.32.21)}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
These ports are expected for a publicly accessible website and are typical for Googl
e-hosted services.

\subsection*{Firewall / External IP (216.220.16.170)}
\begin{itemize}
    \item All scanned ports are \textbf{closed}.
```

```
\end{itemize}
This is a strong sign of network perimeter hardening and good firewall configuratio
n. No externally exposed services were found on the organization's primary IP.

\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 & Strong & MFA is required across key systems \\
Email Security & Strong & SPF and DMARC with "reject" policy in place \\
Network Exposure & Secure & No exposed services on the external firewall IP \\
Web Hosting & Secure & Google-hosted; limited attack surface \\
Policy \& Training & Comprehensive & Acceptable use policies and regular training in
place \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
Although the cybersecurity readiness is solid, continuous improvement is essential.
We recommend the following:
\begin{enumerate}
    \item \textbf{Verify DKIM}: While SPF and DMARC are configured, ensure DKIM is a
lso active for all sending domains.
    \item \textbf{Vulnerability Scanning}: Consider regular internal and external vu
lnerability assessments of network devices and servers.
    \item \textbf{Incident Response Plan}: Document and regularly test a cybersecuri
ty incident response and disaster recovery plan.
    \item \textbf{Asset Inventory}: Maintain a regularly updated inventory of hardwa
re/software assets and monitor for unauthorized changes.
    \item \textbf{Third-party Risk}: Evaluate vendors (e.g., Infinite Campus) for th
eir security posture, especially since they're included in SPF.
\end{enumerate}

\section{Conclusion}
Valier School District demonstrates a strong cybersecurity foundation, particularly
in authentication, email protection, staff training, and perimeter security. Continu
ed vigilance and regular audits will help maintain and improve this strong security
posture.

\vspace{1cm}
\noindent Prepared by: \\
Cybersecurity Assessment Team\\
Date: July 18, 2025

\end{document}
==========
======== Sample 1 =========
You are an expert-level Cybersecurity Analyst and LaTeX Report Generator.
Your task is to receive a list of JSON objects containing raw technical data (dig ou
tputs, port scans) and a questionnaire.
```

You must analyze, correlate, and synthesize this data into a single, complete, and p
rofessional LaTeX report.

Core Instructions:
1. Parse & Correlate: You must parse all JSON inputs. The data is fragmented, so you
must correlate it:
    - The structured JSON (questionnaire) provides the "Organization Name," "Email D
omain," and primary "External IP."
    - The dig output for the domain (e.g., valier.k12.mt.us) provides the A records
(Website Hosting IPs), NS records (DNS Hoster), MX records (Email Provider), and TXT
record (SPF).
    - The dig output for _dmarc provides the DMARC policy.
    - The port scan results must be matched to their respective IPs (the "External I
P" from the questionnaire vs. the "Website Hosting IPs" from the A records).

2. Analyze & Synthesize: Do not just list the data. You must analyze it.
    - Synthesize the questionnaire answers (e.g., all "Yes" answers) into a summary
table and a brief analytical text.
    - Analyze the technical records. For example, identify that p=reject is a strong
DMARC policy, that aspmx.l.google.com means Google Workspace is the email provider,
and that "no ports open" on the firewall is a secure configuration.
    - Extract the date from the port scan logs (e.t., 2025-07-18) and use it as the
report date.

3. Generate New Content: The report must include analytical sections that are not di
rectly in the JSON. You will generate these based on your analysis of the data and c
ybersecurity best practices:
    - An "Overview" section.
    - A "Risk Assessment & Readiness Summary" table.
    - A "Recommendations" section (e.g., verify DKIM, create an incident response pl
an).
    - A "Conclusion" section.

4. Strict LaTeX Formatting:
    - The output MUST be a single, complete LaTeX document.
    - It must start with \documentclass[12pt]{article} and end with \end{document}.
    - It MUST include the following packages in the preamble: geometry, pifont, book
tabs, hyperref, url, and seqsplit.
    - Use booktabs (\toprule, \midrule, \bottomrule) for all tables.
    - Use \ding{51} Yes for "Yes" answers in the questionnaire table.
    - Use \seqsplit{\texttt{...}} for long technical strings (IP lists, DMARC/SPF re
cords, MX records) to ensure they wrap correctly.
    - Use \url{...} for all domains and email addresses.

Context:
sample1/sample1_questionnaire.json:

```
{
  "text": {
    "Organization Name": "Apex Innovations",
    "Email Domain": "apexinnovations.com",
    "Website Domain": "www.apexinnovations.com",
    "External IP": "72.21.196.160",
    "Do you require MFA to access email?": "Yes",
    "Do you require MFA to log into computers?": "Yes",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "Yes",
```

```
    "Does your organization do security awareness training for new employees?": "Ye
s",
    "Does your organization do security awareness training for all employees at leas
t once per year?": "Yes"
  }
}
--
sample1/sample1_dns_dig_email_dmarc.json:
{
  "text": "id 31890\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\n_dmarc.
apexinnovations.com. IN ANY\n;ANSWER\n_dmarc.apexinnovations.com. 3600 IN TXT \"v=DM
ARC1; p=reject; rua=mailto:dmarc_reports@apexinnovations.com; fo=1\""
}
--
sample1/sample1_dns_dig_email.json:
{
  "text": "id 52417\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\napexinn
ovations.com. IN ANY\n;ANSWER\napexinnovations.com. 3600 IN SOA ns1.apexinnovations.
com. hostmaster.apexinnovations.com. 2025101401 21600 3600 604800 3600\napexinnovati
ons.com. 3600 IN NS ns1.apexinnovations.com.\napexinnovations.com. 3600 IN NS ns2.ap
exinnovations.com.\napexinnovations.com. 3600 IN A 72.21.196.160\napexinnovations.co
m. 3600 IN MX 10 mx1.apexinnovations.com.\napexinnovations.com. 3600 IN MX 20 mx2.ap
exinnovations.com.\napexinnovations.com. 3600 IN TXT \"v=spf1 include:spf.protectio
n.outlook.com -all\""
}
--
sample1/sample1_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:09:42.589112\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--
sample1/sample1_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 72.2
1.196.160\nScanning started at: 2025-10-14 14:08:15.223456\n-----------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
======== Sample 2 =========
You are an expert-level Cybersecurity Analyst and LaTeX Report Generator.
Your task is to receive a list of JSON objects containing raw technical data (dig ou
tputs, port scans) and a questionnaire.
You must analyze, correlate, and synthesize this data into a single, complete, and p
rofessional LaTeX report.

Core Instructions:
1. Parse & Correlate: You must parse all JSON inputs. The data is fragmented, so you
must correlate it:
    - The structured JSON (questionnaire) provides the "Organization Name," "Email D
omain," and primary "External IP."
    - The dig output for the domain (e.g., valier.k12.mt.us) provides the A records
(Website Hosting IPs), NS records (DNS Hoster), MX records (Email Provider), and TXT
```

record (SPF).
    - The dig output for _dmarc provides the DMARC policy.
    - The port scan results must be matched to their respective IPs (the "External IP" from the questionnaire vs. the "Website Hosting IPs" from the A records).

2. Analyze & Synthesize: Do not just list the data. You must analyze it.
    - Synthesize the questionnaire answers (e.g., all "Yes" answers) into a summary table and a brief analytical text.
    - Analyze the technical records. For example, identify that p=reject is a strong DMARC policy, that aspmx.l.google.com means Google Workspace is the email provider, and that "no ports open" on the firewall is a secure configuration.
    - Extract the date from the port scan logs (e.t., 2025-07-18) and use it as the report date.

3. Generate New Content: The report must include analytical sections that are not directly in the JSON. You will generate these based on your analysis of the data and cybersecurity best practices:
    - An "Overview" section.
    - A "Risk Assessment & Readiness Summary" table.
    - A "Recommendations" section (e.g., verify DKIM, create an incident response plan).
    - A "Conclusion" section.

4. Strict LaTeX Formatting:
    - The output MUST be a single, complete LaTeX document.
    - It must start with \documentclass[12pt]{article} and end with \end{document}.
    - It MUST include the following packages in the preamble: geometry, pifont, booktabs, hyperref, url, and seqsplit.
    - Use booktabs (\toprule, \midrule, \bottomrule) for all tables.
    - Use \ding{51} Yes for "Yes" answers in the questionnaire table.
    - Use \seqsplit{\texttt{...}} for long technical strings (IP lists, DMARC/SPF records, MX records) to ensure they wrap correctly.
    - Use \url{...} for all domains and email addresses.

Context:
sample2/sample2_questionnaire.json:

```
{
  "text": {
    "Organization Name": "G.A.S. Inc.",
    "Email Domain": "gasinc.net",
    "Website Domain": "www.gasinc.net",
    "External IP": "104.28.1.189",
    "Do you require MFA to access email?": "No",
    "Do you require MFA to log into computers?": "No",
    "Do you require MFA to access sensitive data systems?": "Yes",
    "Does your organization have an employee acceptable use policy?": "No",
    "Does your organization do security awareness training for new employees?": "No",
    "Does your organization do security awareness training for all employees at least once per year?": "No"
  }
}
```

--
sample2/sample2_dns_dig_email_dmarc.json:

```
{
  "text": "id 28911\nopcode QUERY\nrcode NXDOMAIN\nflags QR AA RD RA\n;QUESTION\n_dm
```

```
arc.gasinc.net. IN ANY\n;AUTHORITY\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmas
ter.gasinc.net. 2025101402 14400 3600 604800 3600\n;ADDITIONAL"
}
--
sample2/sample2_dns_dig_email.json:
{
  "text": "id 47123\nopcode QUERY\nrcode NOERROR\nflags QR RD RA\n;QUESTION\ngasinc.
net. IN ANY\n;ANSWER\ngasinc.net. 3600 IN SOA dns1.gasinc.net. hostmaster.gasinc.ne
t. 2025101402 14400 3600 604800 3600\ngasinc.net. 3600 IN NS dns1.gasinc.net.\ngasin
c.net. 3600 IN NS dns2.gasinc.net.\ngasinc.net. 3600 IN A 104.28.1.189\ngasinc.net.
3600 IN MX 10 mx.mailhostbox.com.\ngasinc.net. 3600 IN MX 20 mx2.mailhostbox.com.\ng
asinc.net. 3600 IN TXT \"v=spf1 include:spf.mailhostbox.com ~all\""
}
--
sample2/sample2_port_scan_external_ip.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:16:11.890123\n-------------------------
-------------------------\nPort 21 is open\nPort 22 is open\nPort 25 is open\nPort 8
0 is open\nPort 110 is open\nPort 443 is open\nPort 3389 is open"
}
--
sample2/sample2_port_scan_web.json:
{
  "text": "-------------------------------------------------\nScanning Target: 104.
28.1.189\nScanning started at: 2025-10-14 14:15:30.456789\n-------------------------
-------------------------\nPort 80 is open\nPort 443 is open"
}
--

============================
```


In [58]:

```python
# === SAMPLE 1 ===

# LaTeX input, LaTeX output
response = proModel.generate_content(contents=[prompt_text, context1_text + "\n" +
print(response.text)
```

```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 Apex Innovations}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report provides a cybersecurity assessment for Apex Innovations, based on a com
bination of self-reported information from a security questionnaire and external tec
hnical reconnaissance, including DNS record analysis and network port scanning. The
analysis indicates strong internal policies and user access controls, coupled with r
obust email security configurations. However, the external network perimeter shows e
xposed web services on the primary IP address, presenting a notable attack surface.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Apex Innovations
    \item \textbf{Email Domain}: \url{apexinnovations.com}
    \item \textbf{Website Domain}: \url{www.apexinnovations.com}
    \item \textbf{External IP (Firewall \& Web Host)}: 72.21.196.160
    \item \textbf{Website Hosting IP}: 72.21.196.160
    \item \textbf{DNS Hosting}: Self-hosted (\url{ns1.apexinnovations.com}, \url{ns
2.apexinnovations.com})
\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 & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
```

```
MFA for Sensitive Systems & \ding{51} Yes \\
Acceptable Use Policy & \ding{51} Yes \\
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: Apex Innovations reports a comprehensive implementation of foundational cybersecurity controls. The consistent enforcement of Multi-Factor Authentication (MFA) across critical systems and a commitment to regular security awareness training demonstrate a mature approach to mitigating user-based risks like phishing and credential theft.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS appears to be self-hosted, as indicated by the nameserver records (\url{ns1.apexinnovations.com}).
    \item The A record for the primary domain points directly to the organization's main external IP address.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The organization's MX records (\seqsplit{\texttt{\url{mx1.apexinnovations.com}}}, \seqsplit{\texttt{\url{mx2.apexinnovations.com}}}) suggest a self-hosted or on-premise email server infrastructure.
    \item \textbf{SPF record} is configured to authorize Microsoft 365 as a sender: \seqsplit{\texttt{v=spf1 include:\url{spf.protection.outlook.com} -all}}. The `-all` mechanism enforces a hard fail for unauthorized senders, which is a security best practice. The use of Microsoft 365 for sending, while MX records point elsewhere, suggests a hybrid setup or a potential configuration remnant that warrants review.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A strong DMARC record is in place with a \textbf{reject policy}: \seqsplit{\texttt{v=DMARC1; p=reject; rua=\url{mailto:dmarc_reports@apexinnovations.com}; fo=1}}.
    \item This configuration provides the highest level of protection against domain spoofing and phishing by instructing recipient servers to reject emails that fail DMARC authentication checks.
\end{itemize}

\section{Port Scanning Results}

\subsection*{External IP / Web Host (72.21.196.160)}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
\noindent \textbf{Analysis}: The primary external IP address for Apex Innovations is also serving as the public web host. While these ports are necessary for web traffic, their presence on the main organizational firewall IP increases the network's dir
```

ect exposure to web-based attacks. This configuration differs from a best-practice a
rchitecture where web services are isolated from the primary corporate network perim
eter.

\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 & Strong & MFA is mandated across all key systems. \\
Email Security & Strong & SPF and a strict DMARC "reject" policy are in place. \\
Network Exposure & Review Required & Web services (HTTP/HTTPS) are exposed on the pr
imary IP. \\
Web Hosting & Exposed & The web server is co-located on the main network perimeter.
\\
Policy \& Training & Comprehensive & Strong policies and regular employee training a
re reported. \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
While Apex Innovations has many strong security controls, the following actions are
recommended to further enhance their cyber resilience:
\begin{enumerate}
    \item \textbf{Review Email Infrastructure}: Clarify the discrepancy between self
-hosted MX records and the Microsoft 365 SPF record to ensure the email architecture
is configured as intended and that no legacy systems pose a risk.
    \item \textbf{Implement Web Application Firewall (WAF)}: Since web services are
publicly exposed, deploying a WAF can provide critical protection against common web
application attacks, such as SQL injection and cross-site scripting.
    \item \textbf{Network Segmentation}: Consider isolating the web server from the
primary corporate network. Moving it to a separate, dedicated IP or a demilitarized
zone (DMZ) would reduce the risk of a web server compromise affecting internal syste
ms.
    \item \textbf{Verify DKIM Implementation}: Although SPF and DMARC are correctly
configured, ensure that DomainKeys Identified Mail (DKIM) is also enabled and aligne
d to provide an additional layer of email authentication.
    \item \textbf{Develop and Test an Incident Response Plan}: Formalize a plan that
outlines procedures for detecting, responding to, and recovering from a cybersecurit
y incident. This plan should be tested regularly through tabletop exercises.
\end{enumerate}

\section{Conclusion}
Apex Innovations has established an excellent foundation in cybersecurity through ro
bust user authentication policies, security training, and advanced email protection
mechanisms like DMARC. The primary area for improvement lies in hardening the networ
k perimeter by segmenting public-facing web services from the main corporate networ
k. Addressing the recommendations in this report will significantly reduce the organ
ization's attack surface and strengthen its overall security posture.

\vspace{1cm}

```
\noindent Prepared by: \\
Cybersecurity Assessment Team\\
Date: October 14, 2025

\end{document}
```

In [59]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "pro_sample1_latex_latex_prompt_engineered_tes
```

✅ Successfully exported HTML: pro_sample1_latex_latex_prompt_engineered_test.html

In [60]:
```
response = flashModel.generate_content(contents=[prompt_text, context1_text + "\n"
print(response.text)
```

```
\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 Apex Innovations}}
\author{Date: October 14, 2025}
\date{}

\begin{document}
\maketitle
\onehalfspacing

\section{Overview}
This report provides an assessment of Apex Innovations' cybersecurity posture, deriv
ed from a combination of technical data (DNS records, DMARC policy, and port scans)
and self-reported information from a security questionnaire. The analysis highlights
the current security standing across key areas, identifying strengths and areas for
potential enhancement to ensure robust cyber resilience.

\section{Organizational Information}
\begin{itemize}
    \item \textbf{Organization Name}: Apex Innovations
    \item \textbf{Email Domain}: \url{apexinnovations.com}
    \item \textbf{Website Domain}: \url{www.apexinnovations.com}
    \item \textbf{External IP (Website/Firewall)}: 72.21.196.160
    \item \textbf{Website Hosting IPs}: \seqsplit{72.21.196.160}
    \item \textbf{DNS Hosting}: The organization appears to manage its own DNS, or i
t is managed by its web hosting provider, as indicated by \seqsplit{\texttt{ns1.apex
innovations.com}} and \seqsplit{\texttt{ns2.apexinnovations.com}} nameservers.
\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 Access & \ding{51} Yes \\
MFA for Computer Login & \ding{51} Yes \\
MFA for Sensitive Data Systems & \ding{51} Yes \\
```

```
Employee Acceptable Use Policy & \ding{51} Yes \\
New Employee Security Awareness Training & \ding{51} Yes \\
Annual All-Employee Security Training & \ding{51} Yes \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Summary}: Apex Innovations demonstrates a strong commitment to fun
damental cybersecurity practices, with all reported controls indicating full impleme
ntation. This includes comprehensive Multi-Factor Authentication (MFA) across critic
al access points and a robust security awareness training program for all employees.
This proactive stance significantly enhances the organization's defense against comm
on cyber threats.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item \textbf{Nameservers (NS)}: Apex Innovations utilizes its own nameservers
(\seqsplit{\texttt{\url{ns1.apexinnovations.com}}} and \seqsplit{\texttt{\url{ns2.ap
exinnovations.com}}}). This implies direct control over DNS management, which requir
es careful security configuration.
    \item \textbf{A Record}: The domain \url{apexinnovations.com} resolves to \seqsp
lit{\texttt{72.21.196.160}}, which is also identified as the organization's external
IP address. This indicates that their primary website is hosted at this IP.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item The Mail Exchange (MX) records point to \seqsplit{\texttt{mx1.apexinnovati
ons.com}} and \seqsplit{\texttt{mx2.apexinnovations.com}}. Further analysis of the S
PF record indicates the use of Microsoft Exchange Online (Outlook.com) for email ser
vices.
    \item \textbf{SPF Record}: A valid SPF record is configured: \seqsplit{\texttt{v
=spf1 include:\url{spf.protection.outlook.com -all}}}. The `include:spf.protection.o
utlook.com` correctly authorizes Microsoft's mail servers, and the `-all` mechanism
ensures that mail from unauthorized senders is rejected, providing strong protection
against email spoofing.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A robust DMARC record is in place: \seqsplit{\texttt{v=DMARC1; p=reject; r
ua=\url{mailto:dmarc_reports@apexinnovations.com}; fo=1}}.
    \item The `p=reject` policy is a strong defense, instructing receiving mail serv
ers to outright reject emails that fail DMARC authentication. This significantly mit
igates the risk of phishing and impersonation attempts. The `rua` tag ensures aggreg
ate reports are sent to the specified email address, allowing for monitoring and ana
lysis of email authentication failures.
\end{itemize}

\noindent \textbf{Conclusion}: Apex Innovations has implemented robust email securit
y protocols, including SPF and a strong DMARC "reject" policy, which are crucial for
preventing email spoofing and phishing attacks.

\section{Port Scanning Results}
```

```
\subsection*{External IP (72.21.196.160)}
\begin{itemize}
    \item \textbf{Port 80 (HTTP)}: Open
    \item \textbf{Port 443 (HTTPS)}: Open
\end{itemize}
The port scans targeting \seqsplit{\texttt{72.21.196.160}} (identified as the extern
al IP and website hosting IP) reveal that ports 80 (HTTP) and 443 (HTTPS) are open.
These ports are standard and expected for a public-facing web server, indicating the
presence of a website. It is critical to ensure that all web traffic defaults to HTT
PS and that robust web application security measures are in place.

\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 & Strong & MFA required across email, computer, and sensitiv
e systems \\
Email Security & Strong & SPF and DMARC with "reject" policy in place, utilizing Out
look.com \\
Network Exposure & Moderate & Web server exposed (expected); regular hardening is ke
y \\
Web Hosting Security & Good & Standard web ports open; depends on web server hardeni
ng \\
Policy \& Training & Comprehensive & Acceptable use policies and regular training es
tablished \\
\bottomrule
\end{tabular}
\end{table}

\section{Recommendations}
While Apex Innovations demonstrates a commendable security posture, continuous impro
vement is vital in the evolving threat landscape. The following recommendations are
provided to further enhance cybersecurity readiness:

\begin{enumerate}
    \item \textbf{Implement DKIM}: Although SPF and DMARC are robust, ensure DomainK
eys Identified Mail (DKIM) is also fully configured and validated for all sending do
mains. DKIM provides an additional layer of email authentication, cryptographically
signing outgoing emails.
    \item \textbf{Regular Vulnerability Scanning \& Penetration Testing}: Conduct re
gular vulnerability assessments and periodic penetration tests on the external IP
(\seqsplit{\texttt{72.21.196.160}}) and internal network. This proactive approach he
lps identify and remediate weaknesses before they can be exploited.
    \item \textbf{Web Application Firewall (WAF)}: Given that the website is externa
lly accessible, consider deploying a Web Application Firewall (WAF) to protect again
st common web-based attacks (e.g., SQL injection, XSS) and to provide an additional
layer of security for the web server.
    \item \textbf{Incident Response Plan (IRP)}: Develop, document, and regularly te
st a comprehensive Incident Response Plan. This plan should detail procedures for id
entifying, containing, eradicating, recovering from, and learning from cybersecurity
```

```
incidents.
    \item \textbf{SSL/TLS Best Practices}: Ensure that the web server enforces stron
g SSL/TLS configurations, including the use of modern cipher suites, HSTS (HTTP Stri
ct Transport Security), and regular certificate renewals to protect data in transit.
    \item \textbf{DNS Security (DNSSEC)}: Consider implementing DNSSEC (Domain Name
System Security Extensions) to protect the organization's DNS records from spoofing
and manipulation, enhancing the integrity of domain lookups.
\end{enumerate}

\section{Conclusion}
Apex Innovations has established a strong foundation in cybersecurity, evidenced by
its comprehensive MFA implementation, robust email authentication policies (SPF and
DMARC with `p=reject`), and commitment to employee training. The organization's exte
rnal network exposure is limited to essential web services, which is a positive indi
cator. By implementing the recommended enhancements, particularly in areas of web ap
plication security, continuous testing, and incident preparedness, Apex Innovations
can further fortify its defenses and maintain a proactive stance against emerging cy
ber threats.

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

\end{document}
```

In [61]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_sample1_latex_latex_prompt_engineered_t
```

✅ Successfully exported HTML: flash_sample1_latex_latex_prompt_engineered_test.htm
l

In [62]:
```
# === SAMPLE 2 ===

# LaTeX input, LaTeX output
response = proModel.generate_content(contents=[prompt_text, context2_text + "\n" +
print(response.text)
```

```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 combinat
ion of a self-reported questionnaire and external technical scans. The analysis reve
als critical vulnerabilities in network perimeter security, email authentication, an
d internal security policies. The findings indicate a high-risk posture that require
s immediate attention to mitigate significant threats such as unauthorized access, d
ata 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.n
et}, \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 surface 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 SSH 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} domain, starting with a monitoring policy (\texttt{p=none}) and progressing to a quarantine or reject policy (\texttt{p=reject}) to prevent domain spoofing.
    \item \textbf{Strengthen SPF Record}: Update the SPF record to use a hardfail mechanism (`-all`) instead of a softfail (`~all`) to instruct receiving mail servers to reject messages from unauthorized senders.
    \item \textbf{Enforce Multi-Factor Authentication (MFA)}: Mandate MFA for all users for email access, remote access (VPN), and computer logins to protect against credential theft.
    \item \textbf{Develop and Implement Security Policies}: Establish a formal Acceptable Use Policy (AUP) and create a mandatory security awareness training program for 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 fundamental security policies and user training. The combination of these weaknesses creates a high probability of a successful cyberattack. The recommendations outlined in this report are critical and should be implemented without delay to build a foundational security program and protect the organization's assets and reputation.
```

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

\end{document}
```

In [63]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "pro_sample2_latex_latex_prompt_engineered_tes
```

✅ Successfully exported HTML: pro_sample2_latex_latex_prompt_engineered_test.html

In [64]:
```
response = flashModel.generate_content(contents=[prompt_text, context2_text + "\n"
print(response.text)
```

```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 posture assessment for G.A.S. Inc., based on an analysis of technical data including DNS records (A, MX, TXT, DMARC) and port scanning results, combined with responses from a self-reported security questionnaire. The findings indicate several critical areas of concern, particularly related to network exposure, email security hardening, and foundational internal security controls and policies.

\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 / Website Hosting IP}: \seqsplit{104.28.1.189}
    \item \textbf{DNS Hosting}: Self-hosted or Registrar-managed (\url{dns1.gasinc.net}, \url{dns2.gasinc.net})
    \item \textbf{Email Provider}: Mailhostbox (\url{mx.mailhostbox.com})
\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 questionnaire responses highlight significant gaps i
n foundational security practices. Multi-Factor Authentication (MFA) is only reporte
d for sensitive data systems, leaving email and computer logins vulnerable to creden
tial compromise. Furthermore, the absence of an acceptable use policy and any form o
f security awareness training indicates a lack of a formalized security culture and
processes, increasing human-factor risk.

\section{DNS \& Email Security}

\subsection*{DNS Records}
\begin{itemize}
    \item DNS for \url{gasinc.net} appears to be managed via nameservers hosted unde
r the same domain (\seqsplit{\texttt{\url{dns1.gasinc.net}, \url{dns2.gasinc.ne
t}}}). This configuration suggests either self-hosting of DNS or a default setup by
a registrar.
    \item The A record for \url{gasinc.net} is \seqsplit{104.28.1.189}, indicating t
hat the primary server hosts the website and other services.
\end{itemize}

\subsection*{MX Records (Email)}
\begin{itemize}
    \item Email services for \url{gasinc.net} are hosted by Mailhostbox, as indicate
d by the MX records pointing to \seqsplit{\texttt{\url{mx.mailhostbox.com}}} and \se
qsplit{\texttt{\url{mx2.mailhostbox.com}}}.
    \item \textbf{SPF Record}: An SPF record is present: \seqsplit{\texttt{v=spf1 in
clude:\url{spf.mailhostbox.com} ~all}}. While the record exists, the `~all` (softfai
l) mechanism is less secure than `-all` (hardfail). A softfail allows emails from un
authorized senders to be delivered (though marked), potentially leading to successfu
l phishing or spoofing attacks.
\end{itemize}

\subsection*{DMARC Record}
\begin{itemize}
    \item A query for \seqsplit{\texttt{\_dmarc.gasinc.net}} returned an \textbf{NXD
OMAIN} response, indicating that \textbf{no DMARC record is published} for the domai
n.
    \item \textbf{Analysis}: The absence of a DMARC record is a critical security vu
lnerability. Without DMARC, G.A.S. Inc.'s email domain is highly susceptible to emai
l spoofing, making it easier for attackers to send malicious emails impersonating th
e organization to employees, customers, or partners. This significantly increases th
e risk of phishing, business email compromise (BEC), and brand reputation damage.
\end{itemize}

\noindent \textbf{Conclusion}: While SPF is configured, its `~all` policy weakens it
s effectiveness, and the complete absence of a DMARC record leaves the organization
highly vulnerable to email-based attacks.

\section{Port Scanning Results}
```

```
\subsection*{External / Website Hosting IP (\seqsplit{104.28.1.189})}
Port scans conducted on \seqsplit{104.28.1.189} revealed multiple open ports, indica
ting significant exposure of services to the public internet.
\begin{itemize}
    \item \textbf{Port 21 (FTP)}: Open. File Transfer Protocol (FTP) is an insecure
protocol that transmits credentials and data in plaintext, making it vulnerable to e
avesdropping and credential theft.
    \item \textbf{Port 22 (SSH)}: Open. Secure Shell (SSH) is used for secure remote
access. While encrypted, if not properly secured with strong authentication (e.g., k
ey-based, MFA) and restricted access, it can be a target for brute-force attacks.
    \item \textbf{Port 25 (SMTP)}: Open. Simple Mail Transfer Protocol (SMTP) is use
d for sending email. If not properly configured or secured, it can be abused for spa
m relay or targeted attacks.
    \item \textbf{Port 80 (HTTP)}: Open. Hypertext Transfer Protocol (HTTP) is used
for web traffic. This is expected for a website, but traffic is unencrypted, making
it susceptible to eavesdropping and data tampering.
    \item \textbf{Port 110 (POP3)}: Open. Post Office Protocol version 3 (POP3) is u
sed for retrieving email. Like FTP, POP3 often transmits credentials in plaintext, p
osing a significant security risk.
    \item \textbf{Port 443 (HTTPS)}: Open. Hypertext Transfer Protocol Secure (HTTP
S) is used for encrypted web traffic. This is expected and desirable for secure webs
ite access.
    \item \textbf{Port 3389 (RDP)}: Open. Remote Desktop Protocol (RDP) allows remot
e graphical access to a server. Exposing RDP directly to the internet is extremely r
isky, as it is a frequent target for brute-force attacks and ransomware deployments.
\end{itemize}

\noindent \textbf{Conclusion}: The presence of numerous open and critical service po
rts (FTP, SSH, SMTP, POP3, RDP) on the external IP represents a severe security ris
k. Each of these ports serves as a potential entry point for attackers, increasing t
he attack surface significantly. Unnecessary services should be closed, and necessar
y services should be tightly restricted and secured.

\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 & MFA primarily missing for email/computers \\
Email Security & Critical Gap & No DMARC, SPF is softfail; high spoofing risk \\
Network Exposure & High Risk & Multiple critical services exposed directly \\
Web Hosting & Moderate Risk & HTTP (80) open, but HTTPS (443) also available \\
Policy \& Training & Weak & No AUP, no new/annual security training \\
\bottomrule
\end{tabular}
\end{table}

\noindent \textbf{Analysis}: G.A.S. Inc.'s current cybersecurity posture indicates a
significant level of risk across multiple domains. The lack of comprehensive MFA, ab
sence of DMARC, and extensive network exposure are immediate concerns that require u
rgent attention. Furthermore, the lack of internal security policies and training su
```

```
ggests a reactive, rather than proactive, approach to cybersecurity, increasing the likelihood of successful social engineering and insider threats.

\section{Recommendations}
Addressing the identified vulnerabilities and gaps is crucial to improving G.A.S. Inc.'s cybersecurity posture. The following recommendations are prioritized based on their potential impact:

\begin{enumerate}
    \item \textbf{Implement DMARC with a `p=reject` Policy}: Urgently publish a DMARC record for \url{gasinc.net} with a `p=reject` policy. This will provide strong protection against email spoofing and phishing attacks. Start with `p=quarantine` and transition to `p=reject` after monitoring DMARC reports.
    \item \textbf{Strengthen SPF Policy}: Change the SPF record from `~all` (softfail) to `-all` (hardfail) after ensuring all legitimate sending sources are included. This will instruct receiving servers to reject emails from unauthorized sources.
    \item \textbf{Close Unnecessary Open Ports}: Immediately review and close all unnecessary open ports on \seqsplit{104.28.1.189}. Specifically, FTP (21), POP3 (110), and RDP (3389) should almost certainly be closed to the internet. SSH (22) and SMTP (25) should be restricted to trusted source IPs or replaced with more secure alternatives where possible.
    \item \textbf{Implement Multi-Factor Authentication (MFA) Broadly}: Deploy and enforce MFA for all employee email accounts and computer logins. This significantly reduces the risk of account takeover, even if passwords are stolen.
    \item \textbf{Develop and Enforce Security Policies}: Create and implement essential cybersecurity policies, including an Acceptable Use Policy (AUP) for all employees.
    \item \textbf{Initiate Security Awareness Training}: Establish mandatory security awareness training for all new employees and annual refresher training for all staff. Training should cover topics such as phishing detection, password hygiene, and social engineering.
    \item \textbf{Secure Remote Access}: If RDP (3389) is required, place it behind a VPN or a strong firewall with IP whitelisting. Consider alternative, more secure remote access solutions.
    \item \textbf{Regular Vulnerability Scanning and Penetration Testing}: Conduct regular vulnerability scans of external and internal systems, followed by penetration tests, to proactively identify and address weaknesses.
\end{enumerate}

\section{Conclusion}
G.A.S. Inc. currently faces substantial cybersecurity risks due to multiple exposed services, critical email security vulnerabilities, and a lack of fundamental internal controls and training. Addressing the recommendations outlined in this report is paramount to mitigating these risks, protecting sensitive data, and safeguarding the organization's reputation. A proactive and systematic approach to cybersecurity improvement is strongly advised.

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

\end{document}
```

In [65]:
```
generated_html = generate_html_from_latex(response.text)
export_html_to_files(generated_html, "flash_sample2_latex_latex_prompt_engineered_t
```

```
✅ Successfully exported HTML: flash_sample2_latex_latex_prompt_engineered_test.htm
l
```

Summary

The results were more consistent, with some of the inline tex that was in the other outputs no longer appearing and the information properly formatted in every section.