Executive Summary

We are pleased to present the executive summary of the cybersecurity assessment conducted for Artemis Gas, Inc. This summary provides a concise overview of the key findings and recommendations resulting from the assessment, focusing on the business risks and necessary actions to fortify the organization's security posture.

Our assessment revealed critical vulnerabilities within Artemis Gas, Inc.'s network infrastructure and web applications that require immediate attention. These vulnerabilities expose the organization to significant risks, including unauthorized access, data breaches, and potential financial and reputational damage.

Network Infrastructure Vulnerabilities
We identified several high-risk vulnerabilities within the network infrastructure that demand urgent mitigation measures. These vulnerabilities pose a high risk to the organization's security posture. The risk ratings and corresponding vulnerabilities are as follows:

- High Risk: Unpatched Remote Desktop Protocol (RDP) exposed to the internet: This vulnerability poses a high risk of unauthorized access to critical systems and potential data breaches. Immediate patching is recommended to eliminate this high risk vulnerability.
- High Risk: Default passwords on the Cisco admin portal: The utilization of default passwords increases the likelihood of unauthorized access to network devices, compromising the integrity and confidentiality of Artemis Gas, Inc.'s infrastructure. We recommend enforcing strong password policies and mandating regular password changes to address this high risk vulnerability.
- High Risk: Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions): Misconfigurations in cloud storage settings expose sensitive data to unauthorized access. Implementing proper access controls and reviewing and updating security configurations will effectively mitigate this high risk vulnerability.

Web Application Vulnerabilities
We identified medium risk vulnerabilities in the web applications used by Artemis Gas, Inc., which require attention to minimize potential risks. The risk ratings and corresponding vulnerabilities are as follows:

- Medium Risk: Vulnerability to SQL Injection: The web applications are susceptible to SQL injection attacks, which can result in unauthorized access to databases and potential data leakage. Implementing secure coding practices, regular patching, and updates will significantly reduce the risk associated with this medium risk vulnerability.
- Medium Risk: Broken access control: Insufficient access controls within the web applications increase the risk of unauthorized access and privilege escalation. We recommend implementing robust access control mechanisms and conducting thorough testing and reviews of the access management process to address this medium risk vulnerability.
- The graphic below explains the color coded risk severity (as written above), and its corresponding risk score.

CVE SCORE V3.1

Severity	Base Score
No Risk	0
Low Risk	0.1–3.9
Medium Risk	4.0–6.9
High Risk	7.0–8.9
Critical Risk	9.0–10.0

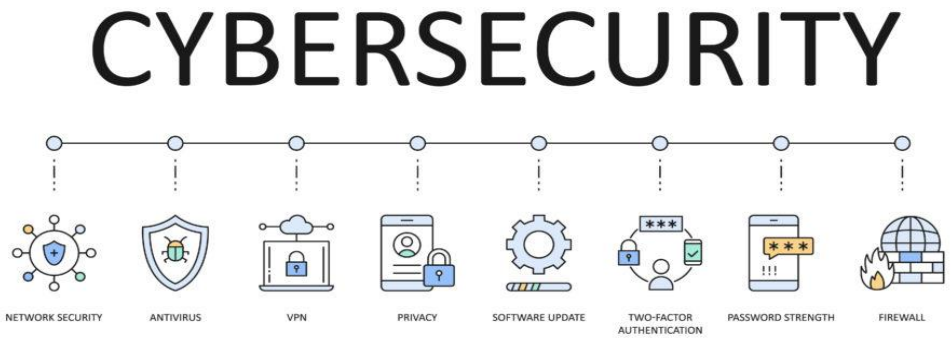
Threat Analysis

Based on the identified vulnerabilities and the current threat landscape, Artemis Gas, Inc. faces significant risks, including unauthorized access to critical systems, potential data breaches, service disruptions, and potential financial and reputational damage. It is crucial to prioritize and address these risks promptly to protect the organization's assets and maintain business continuity.

Recommendations

To enhance the security posture of Artemis Gas, Inc., we recommend the following actions:

- Patch Management: Establish a rigorous patch management process to ensure timely application of security updates and patches across all systems and applications.
- Password Management: Enforce strong password policies, including regular password changes, and educate employees on the importance of creating unique and complex passwords.
- Secure Configuration: Regularly review and update security configurations for network devices, cloud storage, and web applications to ensure they align with industry best practices.
- Web Application Security: Implement secure coding practices, perform regular vulnerability assessments, and conduct thorough penetration testing to identify and address vulnerabilities in web applications.
- Access Control: Strengthen access controls across all systems and applications, implementing least privilege principles and regular access reviews.
- The graphic below displays the industry standard for the best practices of Cyber Security that are necessary to mitigate threats.



Conclusion

The cybersecurity assessment has identified critical vulnerabilities within Artemis Gas, Inc.'s network infrastructure and web applications. Addressing these vulnerabilities promptly and implementing the recommended measures will significantly reduce the organization's exposure to potential risks and bolster its overall security posture. We recommend prioritizing these actions to ensure the protection of sensitive data, maintain operational continuity, and safeguard the company's reputation. We remain committed to supporting Artemis Gas, Inc. in their journey towards improved cybersecurity and are available to provide further guidance and assistance as needed.

Sincerely,

Asad Patel
Cyber Security Consultant