Cybersecurity Intern

Position Summary

Join our team to help protect the organization from cybersecurity threats. In this role, you will manage system patching, review vulnerabilities, and support secure application deployments. You will investigate security alerts, assist with compliance efforts, and help improve cloud security. Additionally, you will contribute to our security awareness program and promote a culture of security.
This position is intended for McCownGordon's Kansas City office.

Primary Responsibilities

Patching and Vulnerability Management

- Mitigate cybersecurity risks by deploying software and operating system patches.
- Review patching automation and ensure compliance with documented patching standards.
- Analyze logs to determine the root cause of patching noncompliance.
- Analyze vulnerabilities, provide recommendations for mitigation, and document mitigation efforts.

Application Deployment

- Analyze new applications for security concerns.
- Learn how to deploy applications silently across Windows and Mac operating systems.

Security Analysis

- Investigate and validate security alerts from various sources, including network, endpoint, identity, email, and more.
- Work with end users and internal IT to triage and mitigate security alerts.
- Make recommendations for preventative measures to improve the security posture.

Governance

- Learn about Governance, Risk, and Compliance frameworks, including ISO 27001, NIST CSF, and NIST 800-53/171.
- Help review and document cybersecurity risks and mitigation strategies to ensure compliance.

Cloud Security

- Learn to identify cybersecurity risks within a cloud environment.
- Work with internal teams to mitigate misconfigurations and improve the security posture.

Security Awareness

- Operate a security awareness program, including uploading content to a Learning Management System (LMS).
- Help write internal cybersecurity newsletters to foster a culture of security.

Knowledge, Skills, and Abilities

(Attributes necessary for success in this role)

- Exhibits the company's core values of Integrity, Performance, and Relationships.
- Demonstrates a team-oriented approach and attitude.
- Ability to work independently.
- Strong interpersonal skills.
- Eagerness to learn and improve.
- Thorough knowledge of Microsoft operating systems.
- Thorough understanding of cybersecurity fundamentals.

- Proficiency in scripting languages such as PowerShell, CMD, Bash, etc.
- Proficiency in query languages such as SQL, KQL, etc.
- General knowledge of networking fundamentals and architecture.

Minimum Qualifications

- Completion of the sophomore year in a bachelor's degree program in Cybersecurity, Computer Science, Computer Engineering, or a related field, or an equivalent combination of education, training, and experience.
- Proficiency in computer applications.

Working Conditions

- The position requires work in an office environment.

Note: This job description reflects a summary of the job and does not prescribe or restrict the responsibilities that may be assigned. The job description is subject to change at any time.