Cybersecurity Engineer

About the Role

Rubix Foods is seeking a skilled and motivated Cybersecurity Engineer to protect the company's systems, networks, applications, cloud services, and data. This is a mid-level, hands-on role responsible for cybersecurity monitoring, vulnerability management, incident response, security engineering, and the continued development of the company's security program.

This position also has meaningful responsibility for network infrastructure. The successful candidate must have a strong networking background and be comfortable configuring, securing, monitoring, and troubleshooting firewalls, switches, wireless networks, VPNs, network segmentation, routing, and related technologies. The role reports to the Chief Information Officer and works closely with the Technology team, business leaders, and third-party security partners.

Key Responsibilities

- Monitor security platforms, endpoints, systems, networks, and cloud environments for suspicious activity, vulnerabilities, policy violations, and potential security incidents.
- Investigate security alerts and incidents; determine scope, severity, business impact, containment steps, remediation, and required documentation.
- Configure, administer, and maintain cybersecurity tools, including endpoint detection and response, antivirus, email security, web filtering, vulnerability management, identity protection, and security monitoring platforms.
- Perform vulnerability assessments, prioritize findings, and coordinate remediation with internal teams and third-party providers.
- Assist with penetration testing, security assessments, cyber-insurance requirements, audits, and remediation activities.
- Develop and maintain security standards, procedures, incident-response playbooks, technical documentation, and system-security requirements.
- Identify weaknesses in systems, applications, cloud services, and network architecture and recommend practical risk-reduction measures.
- Support identity and access management, multifactor authentication, conditional-access policies, privileged access, service-account governance, and least-privilege practices.
- Secure and monitor Microsoft 365, Microsoft Entra ID, Azure services, Windows systems, virtualization platforms, endpoints, and other business applications.
- Support endpoint compliance, software controls, encryption, patching, system hardening, and secure configuration practices.

13203 Flagler Center Blvd.
Jacksonville, FL 32258
904.268.8999

- Configure, maintain, secure, and troubleshoot firewalls, switches, wireless networks, VPNs, internet connections, VLANs, routing, DNS, DHCP, and network access controls.
- Monitor network availability, performance, traffic, and security events; investigate connectivity and performance issues.
- Maintain network segmentation, firewall rules, secure remote access, network diagrams, configuration records, IP-address documentation, and equipment inventories.
- Support network upgrades, equipment replacements, new-site deployments, and secure connectivity between company locations, cloud services, remote users, vendors, and business partners.
- Evaluate the security impact of new technologies, applications, vendors, and business initiatives.
- Educate employees on cybersecurity risks and information-security best practices.
- Participate in after-hours maintenance and incident-response activities when necessary.

Required Qualifications

- Five or more years of experience in information technology, cybersecurity, network engineering, systems administration, or a related technical role.
- At least two years of direct, hands-on cybersecurity experience.
- Strong knowledge of TCP/IP, DNS, DHCP, VLANs, routing, switching, VPNs, wireless networking, network segmentation, and firewall administration.
- Demonstrated experience securing and troubleshooting enterprise network environments.
- Experience with security monitoring, endpoint protection, vulnerability management, incident response, and security investigations.
- Working knowledge of identity and access management, multifactor authentication, privileged access, least privilege, and authentication technologies.
- Experience supporting Microsoft 365, Microsoft Entra ID, Windows systems, and cloud-based services.
- Knowledge of common threats, attack techniques, vulnerabilities, malware, social engineering, and advanced persistent threats.
- Understanding of operating-system security, encryption, patch management, system hardening, and secure configuration practices.
- Experience with firewalls, intrusion detection or prevention, endpoint-security platforms, email security, web filtering, and network-monitoring tools.
- Ability to interpret technical logs, alerts, network traffic, and system activity during troubleshooting and investigations.

13203 Flagler Center Blvd.
Jacksonville, FL 32258
904.268.8999

- Strong critical-thinking, troubleshooting, documentation, and problem-solving skills.
- Ability to communicate security risks and technical issues clearly to technical and nontechnical audiences.
- Ability to work independently, manage competing priorities, and collaborate effectively with internal teams and external partners.
- Based in Jacksonville, Florida; this is an onsite position.

Preferred Qualifications

- Bachelor's degree in cybersecurity, information technology, computer science, network engineering, or a related field. Equivalent professional experience may be considered.
- Experience in a manufacturing, food-production, distribution, or operational-technology environment.
- Experience with Microsoft Intune, Microsoft Defender, Microsoft Sentinel, Azure, virtualization platforms, vulnerability scanners, penetration-testing tools, or SIEM platforms.
- Knowledge of cybersecurity frameworks and standards such as the NIST Cybersecurity Framework, CIS Controls, or ISO 27001.
- Familiarity with backup security, disaster recovery, business continuity, and ransomware-resilience practices.
- Relevant certifications such as Security+, CySA+, Network+, Microsoft Security, CCNA, CCNP, GIAC, SSCP, CISSP, or comparable credentials.

Core Competencies

- Security-first mindset and sound technical judgment.
- Strong investigative ability, initiative, accountability, and attention to detail.
- Clear written and verbal communication.
- Commitment to continuous learning and professional development.

Compensation / Benefits

- Salary commensurate with experience
- Annual bonus potential
- Generous PTO plan
- Retirement / 401(k) plan
- Health coverage

13203 Flagler Center Blvd.
Jacksonville, FL 32258
904.268.8999

- Professional-development and career-growth opportunities

About Rubix Foods

Rubix Foods is a full-service product development house with end- to-end manufacturing capabilities. We blend culinary creativity, food science, and consumer intelligence to fuel innovation for the industry's most exciting, high-momentum brands. From concept to commercialization, we streamline and accelerate the entire product development journey – delivering white-glove service, disciplined execution, and consistent results that raise the bar every time.

Our Vision: To be the food industry's first call – known for our speed, trusted for our quality, and chosen for our reliability.

Our Mission: To solve the food industry's toughest problems – creatively, collaboratively, and with unrivaled speed and execution.

Qualified candidates may submit their resume and salary requirements to Jason Bell at jbell@rubixfoods.com with "Cybersecurity Engineer" in the subject line.

13203 Flagler Center Blvd.
Jacksonville, FL 32258
904.268.8999