

Position Summary

Avum, Inc. is seeking an IT Operations Specialist to help keep daily IT work organized, responsive, and well documented. This role supports technical documentation, vulnerability follow-up, ticket coordination, employee support, and recurring IT processes.

The IT Operations Specialist will work across technical teams to resolve routine issues, track work through completion, and make sure issues requiring specialized support reach the right people with the information they need. This is an individual contributor role reporting to the IT Manager.

Key Responsibilities

- Create and maintain technical procedures, runbooks, troubleshooting guides, and knowledge base articles in collaboration with technical teams.
- Review documentation for accuracy and identify processes that need to be documented or updated.
- Monitor CVE alerts, vendor advisories, and other vulnerability notifications. Conduct an initial review to identify potentially affected systems and the appropriate technical owners.
- Create and track vulnerability remediation tickets, maintain accurate status records, and escalate significant or overdue items according to established procedures.
- Coordinate vulnerability follow-up with system owners and security teams. Technical remediation and risk decisions remain with the appropriate owners.
- Review incoming IT and support tickets for completeness, priority, and appropriate routing.
- Gather diagnostic information before escalating issues, follow up on open work, and identify recurring problems.
- Provide Level 1 and appropriate Level 2 support for common workstation, application, account, authentication, VPN, and connectivity issues.
- Assist with employee onboarding and offboarding, account provisioning, access changes, and routine identity management tasks.
- Maintain IT inventories, service records, operational checklists, and other administrative information.
- Coordinate recurring IT activities and follow-up when work involves multiple teams.
- Recommend improvements to documentation, support processes, and recurring operational tasks.

Compensation

The salary range for this position is \$55,000 to \$70,000, with a target of \$60,000 to \$65,000. Actual compensation will be determined based on experience, qualifications, certifications, and geographic location. Avum offers a comprehensive benefits package including medical (Cigna), dental and vision (Principal), 401(k), PTO, education reimbursement, and certification reimbursement.

Work Environment & Requirements

- Hybrid/remote work environment with potential on-site requirements based on contract needs
- U.S. citizenship required
- Security clearance may be required based on contract assignment

Equal Employment Opportunity

Avum, Inc. is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, veteran status, or any other protected class under federal, state, or local law. Avum is committed to compliance with Section 503 of the Rehabilitation Act and VEVRAA, and maintains an active Affirmative Action Plan.

Required Qualifications

- Five or more years of experience in IT operations, technical support, systems administration, infrastructure support, cybersecurity operations, or a related technical field.
- Experience troubleshooting common operating system, application, account access, and connectivity issues.
- Experience using an IT ticketing or service management system to document, route, and follow up on work.
- Ability to write clear technical procedures and troubleshooting documentation.
- Working knowledge of operating systems, networking fundamentals, identity and access management, and common enterprise applications.
- Familiarity with CVEs, vendor security advisories, vulnerability severity, and remediation tracking.
- Ability to manage multiple issues independently and recognize when an issue requires escalation.
- Strong communication, organization, prioritization, and follow-through.

Preferred Qualifications

- Experience coordinating vulnerability remediation or using vulnerability scanning and security management platforms.
- Familiarity with CVSS, patch management, remediation timelines, and compensating controls.
- Experience supporting Windows, macOS, and Linux environments.
- Familiarity with AWS, identity providers, single sign-on, and multifactor authentication.
- Experience in a regulated environment or supporting infrastructure, security, or DevOps teams.
- Experience improving IT service processes, documentation standards, or recurring workflows.
- Relevant CompTIA, ITIL, AWS, Microsoft, or similar certifications. Certifications are valued but not required when equivalent experience is demonstrated.