Verodin Job Posting – IT/Security Manager

Who We Are

Verodin is reshaping how organizations measure, manage and improve cyber security effectiveness. Evangelizing a technology movement takes more than just a good sales pitch. As a team, we obsess over helping our customers:

- Assess their current state and expose true security gaps
- Establish a means to measure security effectiveness and demonstrate improvement over time
- Realize the maximum potential of existing security investments
- Raise the bar for the entire security organization

If you're passionate about being part of a huge shift in the cyber-security industry, have the core competencies outlined below and are looking to join a team on a mission, Verodin is the place for you.

The Team and The Role

The Operations team supports all aspects of Verodin. All team members must take ownership of their role within the organization, as well as a willingness expand their responsibilities when necessary.

This is a new position within the organization, reporting directly to the Chief Operating Officer, located in Northern Virginia. The IT / Security Manager will work closely with management and the various functional teams to support a fast-paced growing technology company. The ideal candidate is looking for a company to grow with, take on new challenges, and move into leadership. If you are passionate about IT and cyber-security and are constantly looking to take on new challenges, this is the role for you.

Job responsibilities include:

- Procure, configure, operate, and maintain corporate systems, networking and security infrastructure & software

- Manage corporate IT services including email, shared storage, collaboration tools, and other cloud-based services

- Perform availability, performance, and security monitoring on all internally and externally facing corporate systems

- Perform IT on/off-boarding and service-desk support for both local and remote users

- Provision and provide asset, configuration, device management of all IT physical assets (laptops, desktops, mobile devices, servers, printers, etc.)

- Enforce compliance with internal corporate information security policies and procedures, including but not limited to:

    o Change management policies and procedures

    o End-user information risk & security program

    o Security incident response policies and procedures

    o Data privacy policies and procedures

- Act as key member of Business Continuity Plan

Required qualifications include:

- Superior IT learning and problem-solving skills.

- Excellent time management, reporting, and communication skills.

- 3-7 years professional experience working with networks and systems.

- 3+ year professional experience creating technical documentation.

- Prior experience in a technical team leadership role (SME, team lead, manager, etc.)

- Understanding of network & security architecture and implementation is a must; ideal candidate will have worked, hands-on with at least some of the following technologies:

    o Networking: Cisco or Juniper Switches/Routers

    o Network Security: Palo Alto, Fortinet, Cisco or Checkpoint

    o Endpoint Security: McAfee EPO, Symantec SEP, Cylance or Carbon Black

- Experience managing Identity Access Management, Multi-Factor Authentication and/or SSO platforms

- Administrative Experience with Windows, Linux, and OSX, MS Office Suite required

Desired qualifications include:

- Any of the following certifications: CISSP, CCNA, CNSE, MCSE
- Familiar with ITSM and compliance frameworks

To apply for this role, please send your CV/resume and a detailed cover letter describing why you're a fit to careers@verodin.com.

Verodin is an equal-opportunity employer.