

Systems Administrator – Columbia, MD

Vulnerability Research Labs has spent more than a decade becoming the most respected source on cyber threat intelligence while maintaining the culture and feel of a start-up. We are the best in the field because we believe in our mission – to deliver unparalleled capabilities that alleviate the risk posed by today's cyber threats. We offer the opportunity to work on diverse technologies with the best developers in an exciting company with a flat organizational structure. Helping us address the newest cyber threats is where you come in!

We're currently seeking a Systems Administrator for our office in Columbia, MD. You will work closely with the VRL senior systems engineer in our Reston, VA office to manage our full set of IT capabilities. This includes Linux (namely Debian and Ubuntu) servers; Windows, Linux, and Mac desktops, network security hardware and software, backup systems, virtual environments. The SA will also be the company's ISSM/ISSO, working closely with our Security Officer to ensure all systems remain compliant and to implement a new secure network in our Maryland office.

We are looking for:

A systems administrator that is motivated, has a desire to learn new technology, and who is able to:

- Perform all Systems Administrator duties for the Columbia office with oversight and support from the Reston Systems Engineer
- Configure and maintain physical and virtual servers
- Configure and maintain routers, firewalls, and switches
- Detect, diagnose, and report server and desktop software and hardware related problems
- Install new software releases, system upgrades, and evaluate and install patches to resolve software related problems for both servers and workstations, eliminate software bugs and security vulnerabilities, and maintain technology currency of systems and applications
- Perform system backup and recovery of network servers and end user data
- Ensure the backups are running correctly; verify recovery of backups on a regular basis
- Monitor, test, troubleshoot and provide end user support for all LAN/WAN-based applications
- Troubleshoot server based applications and IT infrastructure components
- Perform occasional after-hours tasks including, but not limited to, restarting systems, application upgrades, hardware maintenance, etc.
- Identify, report, and resolve security vulnerabilities to ensure LAN/WAN resources are protected against unauthorized access, modification or destruction
- Perform performance monitoring and provide documentation of issues and recommendations to upper management
- Provide wireless network hardware and software troubleshooting and end user support
- Hands on monitoring of Internet security, VPN access, email server, spam filtering, system/application logs, virus, malware, and botnet protection for servers and workstations
- Add, support and maintain user accounts and information to include application accesses, distribution lists, security and system groups
- Configure and administer DHCP, DNS, Terminal Services, VPN and client desktop devices

- Configure and maintain the VoIP telephone system
- Work with the VRL Security Manager to perform ISSM/ISSO duties for the entire organization, including:
 - Serving as the principal advisor on all matters, technical and otherwise, involving the security of ISs
 - Conducting periodic reviews and technical inspections to identify and mitigate potential security weaknesses, and ensuring all IS security policies are implemented and functional.
 - Maintaining a working knowledge of system functions, policies, technical security safeguards and operational security measures.
 - Producing, developing and updating security documentation to maintain compliance with regulations and program requirements.

Our day-to-day at Vulnerability Research Labs:

- Work closely with highly technical staff to solve complex and interesting problems and provide assistance when needed to non-technical staff
- Provide IT and security support
- Be the go to person and jack-of-all-trades for everything IT
- Automate and discover new ways to make the workplace more efficient and reliable
- Work with cutting edge hardware and software to support production and testing environments
- Evaluate new software and hardware from the open source community

Skills you will need and we will enhance:

- At least 3 years of experience with the administration of the following:
 - Microsoft technologies, including:
 - Microsoft Windows Server
 - DNS
 - File sharing services (SAMBA, SCP, NFS)
 - Backups
 - Microsoft Office suite
 - Linux operating systems including Debian and Ubuntu
 - Host based anti-virus and firewall software
 - VMware ESXi virtualization
 - Fortinet NGFW
 - Dell and Cisco switch configuration (IOS preferred)
- Experience with the following: Linux, Apache, NGINX, MySQL, IPtables, DNS, SSL, LDAP, managed (L2/L3) switches, firewalls (both Linux and COTS based), IDS sensors (snort), TCP/IP, SSL, PostgreSQL, LDAP, Perl, Python, BASH, DNS, DHCP, IPSEC and SSL based VPNs, Asterisk, VoIP, SIP, IAX, OSI layers 1 through 7, Spanning Tree, VLANS, RADIUS, SMB, SVN, GIT, iSCSI, NFS, SMTP(S), POP3(S), IMAP(S), NTP, SSH, Wifi, Fortinet NGFW, Squid, Nagios, Observium, PGP
- At least 3 years of system integration experience, including hardware, software, networks, and databases
- Knowledgeable of system security, operation, performance, and effectiveness

- Ability to troubleshoot and resolve technical issues independently and with minimal supervision
- Professional attitude, appearance, and possess excellent interpersonal and written communication skills
- Strong analytical and decision-making skills

Things we like best about Vulnerability Research Labs:

- Minimal time in meetings
- The ability to go to conferences and training
- Real offices with doors and desks
- Good fresh brewed coffee
- A well-stocked pantry with food and beverages
- Loads of administration tools at your disposal
- Most of all: interesting and challenging work and a great team work with!

VRL is proud to be an Equal Employment Opportunity employer and does not discriminate on the basis of race, religion, gender, national origin, color, age, military service eligibility or veteran status, disability, sexual orientation, marital status or any other protected class. We encourage and support workplace diversity.

Qualified candidates should send their resumes to: info@vrlsec.com.

We are unable to hire non-US citizens. Please, no third party firms.