pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Sr. Cybersecurity Application Support Engineer

Job Description	Perform testing of infrastructure changes in lab environment to simulate effects on production systems, prepare test plans, and properly document test results. Proactively monitor system performance and improve system architecture to maximize performance and eliminate potential problems. Plan, monitor, and implement backup and recovery of Windows and UNIX/Linux OS's. Troubleshoot and/or provide technical support in the event of an issue. Work closely with vendors, team lead, technical lead, database architects/administrators, other systems engineers, project/program managers, and government customers to develop, implement, maintain and upgrade IT infrastructure. Publish standards, policies, and procedures, and work with development staff to standardize environment and improve efficiency. Other support includes licensing administration, troubleshooting system issues and errors, reviewing vendor provided support materials and monitoring system performance and data recoverability in accordance with customer Information Technology policies and procedures. Responsible for leading a test team or supporting a test team lead. Provide briefs to government staff on ongoing activities
Daily Responsibilities	• Support industry-specific security application, lead deployments and installations, configuration management and troubleshooting. • Support mission-focused infrastructure to ensure performance and availability of system and environment • Schedule and coordinate system maintenance activities to reduce impact to production environment • Support customer Windows servers (e.g. installations, configuration management, patching, vulnerability remediation, compliance checking, performance analysis and troubleshooting. • Support industry-specific security application backend servers (e.g. installations, configuration management, patching, performance analysis and troubleshooting. • Test changes in development environment before application in production environment. • Core work hours are 9:00am – 3:00pm (8.5 work day), Rosslyn, VA
Required: Basic Requirements	****Top Secret Clearance Required to Start (Must be able to obtain SCI)**** 10+ years of experience in the information security field Bachelor's Degree Required • CompTIA Security+ • Applied security application engineering experience • Applied Windows systems engineering experience • Experience applying baseline security configuration controls to servers running Windows OS (e.g. DISA STIGS) • Enterprise support and deployment of multiple operating systems (e.g. Windows 2008, 2012, Linux) • Experience in configuring and troubleshooting Windows and Linux servers • Experience with storage area networks (SANs) • Experience with Virtualization (e.g. VMWare)
Desired: Skills: Preferred but not required	Certifications: • Linux (e.g. Red Hat Certified System Administrator) • Oracle (e.g. Oracle Linux Certified Administrator) • Cisco (e.g. CCNA) • Microsoft (e.g. MCSE) • Experience with integration of multiple types of data sources. Experience with hardware and input/output evaluation and optimization. • Experience and deep familiarity with Dell hardware including, RAID configuration, Direct Attached Storage, SANs, and Hyper-converged solutions. • Familiarity with Dell servers, Direct Attached Storage and RAID • Working knowledge of information security and IT standards like ISO27002, NIST, ITIL, etc.

Sr. Cybersecurity Application Support Engineer

Desired: Skills: Preferred but not required	• Understanding of data privacy principles and regulations (breach notification, etc.) • Advanced written and verbal communication skills • Excellent leadership and teaming skills • Demonstrated integrity within a professional environment • Be able to assess complex IT environments and map the data flow of the through systems/applications and organizational functions • Develop data protection program and help architect technology solutions to fit client's IT environment and the culture of the organization • Support data loss prevention and data storage security technology solutions, including the design of the solution, configuration of agents or network appliances and data policies/rules. • Analyze data usage patterns, detect usage anomalies, and tune policies, procedures, or product configurations for improve performance and efficacy