Security Engineer Security Engineer Security Engineer - ReliaQuest Tampa, FL I am currently a Security Engineer with ReliaQuest and I have 6 years of experience in the IT industry supporting both Linux and Windows environments as well as various SIEM technologies. I have set up, configured and managed Windows Server Update Services (WSUS), FOG imaging server and OpenVAS, and has utilized system management tools e.g. AD, Group Policy, and scripting to effectively monitor and maintain users and group permissions. I have been working as both a Support Engineer and Security Engineer working closely with multiple SIEM technologies as well as IDS and IPS systems. I have set up and maintained a help desk ticket and inventory portal, configured VPN's, and have managed Polycom VoIP phone systems. I am currently working on my Masters degree in Information System Management and have completed my Network Security certification from the Cisco Network Academy as well as my Bachelor's of Science degree in Information Technology from Colorado State University. Authorized to work in the US for any employer Work Experience Security Engineer ReliaQuest - Tampa, FL 2017 to Present Create and present annual health checks for LogRhythm, Qradar and AlienVault customers ? Provide support, health monitoring and expertise for SIEM technologies ? Provide 24/7 expertise for EDR technologies (Carbon Black) ? Provide remote and onsite services including new deployments, re-architecture and best practice solutions for customers ? Work closely with Analyst and Content teams to create new alarms and custom parsers within the SIEM environment ? Work daily on CentOS and RedHat backend issues that arise from SIEM and EDR software issues ? Ensure performance of all custom rules and DSM's within SIEM environments and work closely with IBM and LogRhythm support to identify new bugs ? Create custom parsers for new and existing log sources using RegEx ? Create custom API calls for multiple cloud based applications ? Find creative solutions to bring in unsupported vendor log sources ? Carefully plan and implement both major and minor upgrades ? Demonstrate both LogRhythm and Qradar SIEM's to customers looking to purchase or change SIEM technology ? Identify and address environmental security gaps within the customer environment Projects ? Built out internal and customer facing LogRhythm training labs and guides ? Provide onsite training to Security Engineer Associates in both

LogRhythm and Qradar technologies ? Created custom DSM/Log Source Policies and parsing for highly custom endpoints including Boeing black box endpoints Tier II Advanced Support Service Engineer LogRhythm - Boulder, CO 2016 to 2017 Inspect, detect and report on log data coming in from various hardware and applications ? Work with Security Analysts to setup and fix LogRhythm enterprise SIEM ? Issues include: SQL Database errors, port binding issues, network firewall/IDS issues, log collection failure ? Work in both Windows Server and Linux environments ? Use various network tools to detect problems in client's environment and in our software ? Manage and troubleshoot SQL and Elasticsearch databases ? Assist in maintaining security compliance across various security standards ? Troubleshoot logging systems (i.e., Syslog, Windows Event Log, Flat File collection) ? Install and work with Windows Server operating system ? Troubleshoot Windows AD Domain security and audit policies ? Troubleshoot TCP/IP protocols and routing ? Troubleshoot routers, switches, firewall devices ? Troubleshoot Blue Coat Proxy, CheckPoint Firewall, Nessus Scanner, Wireshark ? Train and assist in deploying LogRhythm and log collection as well as implementing custom MPE rules using regex. ? Create custom alarms and AIE rules to meet the customers security needs. System Administrator The Joshua School - Englewood, CO 2015 to 2016 Managed a mixed Windows and Mac environment across three campuses ? Managed Polycom VoIP phone system ? Managed and ensuring uptime in a primarily wireless network ? Maintained FERPA and HIPAA compliance ? Managed an IT internship program ? Researched and purchased new technologies for staff to help teach special needs students Projects ? Re-cabled the network, replacing Category 3 cables the previous admin installed with Category 6 cables ? Set up Apple Remote Desktop and Administration on all machines MacBook ? Set up and maintained a help desk ticket and inventory portal ? Set up and configured a VPN ? Set up two new campus locations Database Specialist/Help Desk Technician Bridgehealth Medical - Denver, CO 2014 to 2015 Troubleshot software and hardware problems for both remote and in-house users ? Placed PC and hardware/software orders for users ? Added and maintained database entries ? Ensured HIPAA compliance and infrastructure uptime ? Created and managed new and existing GPOs as needed ? Created PowerShell scripts for various maintenance tasks that could be automated Projects ?

Set up, configured and managed Spiceworks inventory system ? Set up, configure and managed OpenVAS vulnerability scanner ? Set up, configured and managed a dataloss prevention service/server ? Set up, configured and managed FOG imaging server ? Set up, configured and managed Windows Server Update Services (WSUS) Computer Technician/Help Desk South Central Library System - Madison, WI 2012 to 2014 Hardware repairs ? Printer troubleshooting ? Created and applied images on PCs for libraries ? Installed and maintained various software for library use ? Tested Access Control configurations ? Cabled and managing switches and routers ? Created spreadsheet Education Master of Science in Information Technology Management Colorado State University 2017 to Present Bachelor of Science in Information Technology in Information Technology Colorado State University 2014 to 2016 IT- Networking and IT- Security Madison Technical College (Cisco Network Academy) 2012 to 2014 Skills Active directory (Less than 1 year), assembly (Less than 1 year), Cisco (Less than 1 year), Dhcp (Less than 1 year), Dns (Less than 1 year), Elasticsearch (1 year), firewalls (Less than 1 year), Hyper-v (Less than 1 year), Intrusion (Less than 1 year), Linux (1 year), Mac (1 year), Mac os (Less than 1 year), Polycom (1 year), Security (5 years), Siem (3 years), Sql (1 year), Tcp (1 year), Tcp/ip (1 year), Voip (1 year), Wireshark (1 year), Information Security, Cyber Security, Splunk, Network Security

Name: Laurie Sanders

Email: ingramdonald@example.net

Phone: 984.262.2225x669