

IT Security Specialist - Security Operations IT Security Specialist - Security Operations IT Security Specialist - Security Operations - Arris Buford, GA Authorized to work in the US for any employer

Work Experience IT Security Specialist - Security Operations Arris - Suwanee, GA September 2016 to Present Monitor and investigate network and security events to protect the environment from internal and external information theft, leakage, and misuse using StealthWatch, Kaspersky, LogRhythm, and BigFix. Conduct forensic analysis using FTK. Work with a 24/7 vendor to ensure they have needed network visibility for monitoring our network. Rule and report creation within LogRhythm, this includes from scratch creation of rule criteria to alert on events we view as important or of interest and tuning of rules and reports to reflect what we are looking for. Working knowledge of Linux, Mac, and Windows Operating systems. I am also tasked with back end administration of our SIEM, StealthWatch, and FTK tools which includes troubleshooting log flow, rule correlation, data collection, host onboarding, agent deployment, and patching of the host servers. Create Incident Response documentation in accordance with laws and regulations from multiple countries.

Network Security Associate Computer Services Inc - Fort Collins, CO May 2015 to August 2016 Make configuration changes to network, system and security devices to ensure that clients are protected from emerging threats. This includes identifying and mitigating security vulnerabilities through patch management as well as applying general and custom IPS and Sourcefire signatures along with other IPS and signature tuning. I also have a very good working knowledge of Cisco, PaloAlto, and Sonic Wall firewalls including blocking malicious IP's and setting up and configuring syslog information to be sent to SIEM solutions along with general day to day administration and troubleshooting of security and network devices. Working knowledge of Linux, Mac, and Windows Operating systems. I am also tasked with back end administration of our SIEM solution which includes troubleshooting log flow, rule correlation, and patching of the host servers.

Network Analyst Intern City of Boise - Boise, ID January 2014 to May 2015 Configure and Install Routers, Switches, Wireless Access Points as well as day to day trouble shooting. I took lead on the purchase, installation and configuration of SPLUNK and was responsible for configuring and scheduling detailed daily, weekly, and monthly reports as well as incident request reports. Work with

senior network engineers on firewall rules and troubleshooting issues. I am CJIS certified and gained a beginner's knowledge of PCI-DSS compliance. Education Associate of Applied Science in Information Security & Digital Forensics College of Western Idaho - Boise, ID January 2013 to May 2015 Skills Cisco (4 years), Security (3 years), SIEM (3 years), solutions (1 year), SPLUNK (2 years), Logrhythm (1 year), Forensic Tools (FTK) (2 years), StealthWatch (1 year) Certifications/Licenses CEH February 2015 to February 2018 CHFI March 2015 to March 2018 Security+ May 2015 to May 2018 CCNA Routing and Switching July 2016 to July 2019 Additional Information TECHNICAL SKILLS I have a working knowledge of setting up and configuring Cisco routers and switches, and Window 7 systems. I can grasp onto concepts quickly and have a good understanding of cabling. I possess excellent communication, writing, computing, and organizational skills. I am highly skilled in working with teams and am proficient in Microsoft Excel, PowerPoint, and Word programs. I have completed the Windows Server 2008 Administration and Active Directory Administration training, as well as Windows Server 2012 Administration and Security+. I have received training for Splunk, BlackStratus, and LogRhythm SIEM solutions and am currently part of a 2 person team tasked with the administration and troubleshooting of a very large multitenant environment.

Name: Erin Hoffman

Email: jacqueline98@example.org

Phone: (848)774-6066x7556