IT Cyber Security Analyst II IT Cyber Security Analyst II IT Cyber Security Analyst Little Rock, AR I have been fortunate to have a career in something that I am passionate about and throughly enjoy, it's a privilege to be a Cyber Security Specialist. I have been working in the IT profession for approximately 16 years in multiple industries allowing me to gain progressive experience which has allowed me to hone into my skills and passion; hunter and defender of network security with a mission to thwart off intruders and maintain the integrity of data, network security, and maintain confidential data, and ensure the companies reputation is always protected by any unwanted attacks or the bad publicity that follows that could damage a companies reputation. You can't rely or expect breaches will be caught by passive alerting tools. I feel it is imporant to remain abreast of the threat landscape and continue to utilize all the tools within your organizations arson to block, detect, and log any type of traffic with similar signatures to be reviewed to determine whether it is a positive or false positive threat and continue to remain vigilant and do my best to stay ahead of the attackers. Although there is certainly a tedious and cumbersome task of ensuring that you are maintaining complaince regardless of your industry you have the responsibility to maintain a certain level of regulatory compliance, this isn't always the most exciting part of our jobs but it is definitely a necessary evil. Compliance is the first step and key to securing data and maintaining integrity of your private intellectual data and maintain compliance regardless of the industry. Authorized to work in the US for any employer Work Experience IT Cyber Security Analyst II Arkansas Electric Cooperatives of Arkansas - Little Rock, AR February 2018 to June 2019 As a member of the Security Operations Center team I participated in Incident Response team who were responsible to investigate and minimize the threat of damage resulting from a breach of restricted/confidential or internal data and ensure that the threat is contained and segmented off. As a member of the IT Security Team at the Arkansas Electric Cooperative I was NERC/CIP authorized and our team managed the Security, Vulnerability, and Compliance. Our main priorities have been primarily focused on the new NERC/CIP standards and ensuring our compliance. Key Responsibilities: Administration of LogRhythm SIEM Solution Performing Baseline configuration of assets to ensure no unauthorized changes are being made to assets. Maintained security, integrity, and

documentation of cyber & physical assets to meet corporate standards and/or NERC CIP standards Maintained access authorization to cyber & physical assets to meet corporate standards and/or NERC CIP standards Performing Vulnerability Scanning and Analysis Manage the Vulnerability Working Group to include multiple areas within our ITI and Network Administration teams. Developed Mitigation plans for critical vulnerabilities discovered Developing mitigation plans for vulnerable systems where for instance a critical patch was unable to applied due to the necessity of the availability of the system and it's relia- bility take precedence. Information Security Analyst II FIS GLOBAL September 2013 to November 2017 As a member of the Security Operations Center team I participated in Incident Response team who were re- sponsible to investigate and minimize the threat of damage resulting from a breach of restricted/confidential or internal data and ensure that there was no interruption of the businesses processes or resources. Additionally, I was responsible for maintaining the DAM (Database Access Management) solution that was previously de- ployed and selection of a new DAM solution and initiating the deployment of the new solution. Tasked with determining the in-scope systems based on Risk factors and audit regulations. Responsible for the engineering of the system infrastructure to deploy the DAM solution and build and maintain the security and audit policies of the system to protect the Database systems that had been determined to be in scope. Through a framework that addresses policy, process, operations, people, and technology, DAM protects infrastructure, corporate data, and customer assets, and ensures alignment with applicable regulations and laws. I was also responsible for monitoring, configuration changes, creating roles and accounts, managing log sources, and software updates for the client SIEM solution. Tasked with the responsibility to analyze, troubleshoot, and remediate issues with the SIEM. Responsible for working closely with other teams to ensure that the SIEM is performing to standard with all necessary logging sources. Key Responsibilities: Provide Database ID management support the following types of databases: Oracle, SQL, DB2, Sybase, Informix and Teradata. Provision and de-provision Database requests submitted. Participate in SOX/PCI Compliance and Audit work. Perform periodic review of existing documentation to ensure current understanding of processes and procedures making updates/changes as necessary. Maintaining

ACL's for access to sensitive data Identified Sensitive Data Provide Database Auditing for Privileged Users, Sensitive Tables, and objects Create Reports for monitoring access to sensitive data Integrated DAM solution with LogRhythm and RSA Security Analytics Act as the subject matter expert for the customer's SIEM solution. Maintain SIEM operations and document current environment. Work with external teams to ensure all necessary logging sources are reporting to the SIEM. Creation of technically detailed reports on the status of the SIEM to include metrics on items such as number of logging sources; log collection rate, and server performance. Incorporate change management into all system changes. Troubleshooting and problem solving a wide variety of agent/agentless issues during deployment to physical and virtual servers, Firewalls, IDS/IPS, and Databases. Perform health checks on SIEM platform. Provide engineering support for immediate issues. Develop use case content. Capacity management of event collectors and propose increase in the capacity Additional Key Roles: SME for Akamai- A protective solution for DDOS SME for RSA Security Analytics SIEM SME for IBM Guardium Backup for IDS/IPS PROVENTIA IT MANAGER and Network Analyst The PEABODY LITTLE ROCK - Little Rock, AR November 2007 to May 2013 Advanced to IT Manager from a network analyst role to provide IT leadership for hospitality technology infra- structure. Managed migration projects, system conversion and performance tuning and monitoring of applica- tions/systems. Help set long-range technical direction and capacity plans. Key Results: Led hotel in the upgrade of previously wired guest network for HSIA to implementation of all wireless system in all 418 guest rooms and public spaces.

In a joint effort with corporate office identified processes, applications, and systems which were not PCI compliant and led initiative to identify PCI-DSS data and implement system controls and and procedures to ensure PCI compliance Managed the transition to PCI compliance and Coordinated and launched "pre-load" training clinics, op- timized training documentation prior to go-live date of system and applications to ensure a smooth tran- sition for operations areas Implemented system to track and control Property Management schedules, cleaning of facility, and guest requests that streamlined procedures which decreased labor time and eliminated redundancies. Allowed ability to customize or utilize canned reports reflecting accurate labor to help

trim labor cost when possi- ble. Migrated from Novell NetWare to Active Directory Domain Managed, developed, and maintained digital media and website content. Managed hardware and software systems for server, POS and desktop environments. Provided end-user support Lead and Managed IT initiatives for the hotel based on industry best practices Managed Database for Property Management System and created customized reports Maintained Inventory of all computer hardware and software Built and Maintained relationships with external vendors Reviewed License Agreements and Contracts for new and existing software and services. Gathered and assessed needs from internal business units; created custom solutions to resolve issues (e.g., system slowdowns, virus outbreaks and process bottlenecks); and developed functional specifica- tions which assisted in the planning and design of enhancement or upgrade/replacement/installation Automated previously manual, time-consuming processes to drive gains in Senior Systems/ Security Analyst & Webmaster ARKANSAS BLUE CROSS AND BLUE SHIELD March 2000 to November 2006 Provided object-oriented analysis/design, coding and testing of company's proprietary self service customer claims and benefits portal, management software application. Defined, wrote and managed requirements for a major application that is the cornerstone of companies business communication; the email encryption applica- tion is designed to quickly process all outbound communications to determine if the message meets the criteria of containing personally identifiable information as outlined in HIPAA regulations. Key Results: Implemented email encryption system in response to HIPAA mandate. Member of pilot launch team for deployment of legacy systems on Citrix platform which resulted in suc- cessful virtualization of platform systems Became a part of the companies first Information Technology Departments internal audit team to review systems, processes, and services to ensure integrity and security for systems, data, and intellectual prop- erty. Performed penetration testing of DMZ systems through automated security testing tools to determine ex- ploitable vulnerable systems in order to mitigate Reviewed audit findings with appropriate committee's and management to determine appropriate action- able items and create plans of action Lead appropriate divisions and teams toward mitigating or resolving Vulnerabilities in systems, applica- tions, and databases to ensure

organization complied with all state and federal regulatory governances and mandates Managed and monitored IDS/IPS systems to ensure network security to further strengthen the privacy and identity protection of all group and individual policy holders. Managed servers in a DMZ environment Managed External DNS for company websites Handled escalated senior level issues and requests received by Help Desk Monitored and managed Internet traffic and enforced categorized blocking based on Internet Usage pol- icy and best practices. Education A.S. in Applied Computer Information Systems in Applied Computer Information Systems U OF A AT PULASKI TECHNICAL COLLEGE - North Little Rock, AR 2011 Certifications/Licenses CISSP May 2013 to November 2020

Name: Colleen Holloway

Email: kristin54@example.org

Phone: (991)883-8471x3656