Senior Tier 2 - Security Incident Handler / Digital Forensics Investigator Senior Tier 2 - Security Incident Handler / Digital Forensics Investigator Senior Tier 2 - Security Incident Handler Winder, GA I have vast knowledge and understanding of security tools and work independently as well as with a team in a Security Operations Center environment to handle all security incidents for a global financial company. I stay knowledgeable on current attacks and methods to be better prepared for possible attacks to our environment and how to prevent them. As the senior Tier 2 analyst I am responsible for handling high priority incidents, threat hunts, creation of new processes/rules/alerts, creating training material and process guides, as well as training new Tier 1 and Tier 2 analyst. Authorized to work in the US for any employer Work Experience Senior Tier 2 - Security Incident Handler / Digital Forensics Investigator First Data - Marietta, GA January 2017 to Present Researched common and current attack vectors and penetration techniques in the First Data environment for vulnerabilities and possible breaches - Effectively worked independently and with team members in a SOC environment to triage, contain, report, resolve or escalate security incidents based on company protocol - Strong analytical, technical, and problem-solving skills with vast working knowledge of security tools such as Splunk, Threat Stream, Fireeye, Netwitness, Security Analytics, Bluecoat Malware Analysis, Scout Vision, Reverse Labs and Tanium. - Weigh business needs against security concerns and articulated issues to management providing detailed documentation of possible resolutions - Demonstrated leadership qualities and skills as the senior incident handler, including independent decision making on incidents, mentoring of junior analysts, creation of process guides and training documents in Confluence, and providing feedback of process improvements - Attend FS-ISAC weekly calls on current events seen in the security environment and created knowledge documents to share with other analysts Digital Forensics Investigator - Investigate escalated Data Loss Protection incidents by utilizing the programs Risk Fabric, Symantec DLP, EnCase, and Palantir to gather information about a user's email history, computer usage, and their activities - Further investigated cases using Splunk to monitor and analyze email and browsing history as well as computer logs and USB usage - Participated in the notification and interview of both management and offending associates, providing detailed

supporting documentation of our findings - Identified, summarized, and escalated cases if an Acceptable Use Policy was broken as well as engaging Legal and HR in a timely manner - Conducted Case Trend Analysis to identify bad business processes and provided solutions to decrease First Data's DLP risks - Thoroughly trained other technicians and created process and mitigation guides on the DLP process - Consistently works with the Digital Investigations Team on internal investigations involving cyber espionage, workplace harassment, policy violations, and monitoring for suspicious behavior involving trade secrets IT SYSTEMS SUPPORT SPECIALIST USAR February 2010 to Present - Reviewed and monitored database access - Educated, enforced, and implemented all security procedures - Trained multiple technicians on how to identify and prevent security attacks - Directed management on security updates that needed to be implemented or prevented - Researched and Identified possible database security threats - Implemented system recovery procedures regularly - Prepared weekly and monthly security reports - Develop system documentation, standards, and operating procedures for the Civil Information Management team on specialized IT equipment - Develop oral and written communication support to the Civil Military Operations Chief on mission policy changes in support of Civil Affairs Operations. - Researched and analyzed Civil Information data to prepare information analysis on areas of interest. - Responsible for management and maintenance of SQL database for a 200 person Civil Affairs organization. - Strong experience with Windows 7, Microsoft Office, software support, and data management. - Organizational expert in satellite and radio communications. - Responsible for the maintenance, troubleshooting and repair of more than $1 Million in US Army Communications Equipment. - Managed a five person communications team including setting work objectives, managing all personnel records through US Army Automated Systems, responding to pay inquiries, and resolving administrative issues. - Managed the entire communications inventory for a 1,000 person Military Intelligence organization. - Responsible for customer service on 75 Government Information Systems, including desktop support, networking, maintenance, and repair. - Maintained the training calendar and scheduling of official and unofficial duties of the organization's communications department. FIELD OPERATIONS SUPPORT ANALYST TENNESSEE VALLEY

AUTHORITY September 2013 to October 2016 - Identify potential security risks in software and hardware - Strong understanding of security software applications and response methods - Developed how to better prepare users for possible security attacks with management - Educated internal and external users on how to better identify cyber security attacks - Informed internal users on the proper procedures and protocols when concerning any streaming, social media, or external site - Recommend software updates needed for specialized applications - Ensure internal and external email standards were upheld - Monitored and responded to the use of all unapproved external devices - Investigated and resolved possible security threats - Ensured encrypted backup and recovery for internal users - Field support analyst for more than 3,000 personnel, including maintaining support records for all trouble tickets - Maintained a professional appearance and attitude when interacting with users, management, and other technicians - Conducted myself according to TVA's safety procedures when operating in an industrial environment - Worked cohesively on/with support teams of up to 15 personal - Used Bomgar remote access software daily for customer service and troubleshooting. - Frequently troubleshooted desktop and server errors on a variety of Windows operating systems - Responsible for the support and maintenance on a variety of specialized software, hardware, and unique Windows installations - Provided support and maintenance to voice, data, and telecommunication networks - Responded to five or more short deadline trouble tickets per week - Develop analysis on desktop support issues to Management on the efficient deployment of Windows 7 and unresolved desktop support tickets - Organization and retirement of end user devices - Managed an eight-person migration team in the transition from Windows XP to Windows 7 on 500 information systems per week for a period of nine months - Plan work objectives and assigned schedules, work hours, and team duties for an eight-person Information Technology Team Education B.S. in NETWORK SECURITY & FORENSICS FOUNTAINHEAD COLLEGE OF TECHNOLOGY - Knoxville, TN April 2017

Name: David Rasmussen

Email: christine00@example.net

Phone: 337.616.2807x15342