Cyber Security Operations Analyst (Contractor) Cyber Security Operations Analyst (Contractor) Cyber Security Analyst - Sanofi Bridgewater, NJ Strong solving organization information problems and analyzing issues in some agile methods. Recommending systems controls and protocols to the management. Preparing technical reports by collecting, analyzing, and summarizing information and trends. Investigating any irregularities to determine if the network has been compromised. Adept at interdepartmental coordination to maximize business functionality and efficiency. Solutions-oriented with an aptitude for solving problems and acting on own initiative. Highly motivated with a willingness to learn new technologies and be a hands-on engineer. Effective communicator with a positive and confident attitude. Excellent writing skills with the capability to create well-formatted reports and client-facing documentation. Excellent consultative skills with experience preparing business solution proposals and presenting them to senior executives. Team player with strong collaboration skills and a flexible approach to problem solving. Authorized to work in the US for any employer Work Experience Cyber Security Operations Analyst (Contractor) SANOFI - Bridgewater, NJ April 2019 to Present Leverage cyber Security monitoring systems to hunt, detect and respond to cyber- security threats, risks, and attacks. Participate in incident response processes by taking actions based on work instructions and standard operating procedures to remove threats, block attacks and enhance cyber- security protections. Assist with small security projects to extend security protections and reduce risk. Configure or make recommendations for improving security incident response, and detection capabilities across various security technologies like Firewalls, IPS, EDR and Antivirus. Create basic command prompts to automate detection and incident response processes. Participate in Red and Blue team testing exercises to develop and improve incident response processes. Maintain a current understanding of the cyber threat landscape Cyber Security Operations Analyst Leidos - Roseland, NJ January 2018 to April 2019 Identify information security alerts, threats and prevent outbound data leaks (e.g. Trustwave WAF). Proactively and iteratively search through data-sets to detect and respond to threats and anomalies. Perform cyber threat analysis, correlate actionable security events, and custom sensor output as it pertains to the cyber security of communication networks, and participate in the coordination of resources during

incident response efforts (e.g. McAfee IDS, McAfee ePO, CheckPoint IPS). Coordinate resources during enterprise incident response efforts, driving incidents to timely and complete resolution. Analyze to get real-time detection and understand threat campaign(s) techniques, lateral movements and extract indicators of compromise (IOCs). Identify network, systems and application vulnerabilities and perform security assessments using automated tools (e.g. Carbon Black). Following the Cyber Kill Chain framework to categorize incidents according to its severity level and recommend remediation and recovery strategies, suggest defensive policy enhancements and information technology procedures. Using packet analyzer tool to analyze the packets according to designate source IP and destination IP (e.g. Wireshark). Work with technology support teams and vendors to implement, maintain and optimize Information Security systems that include various endpoint and network logging, monitoring, and prevention systems (e.g. Splunk ES/UBA and Carbon Black). Developing incident response efforts through Symantec Managed Security Services (MSS) and putting all the alerted incidents together by using the ticket systems (e.g. Resilient Systems). Filtering and categorizing web, authenticating users, and preventing data loss with the secure web gateway software. (e.g. Bluecoat Proxy). Perform analytic support and analyzing triages to inspect any threats that are detected at any endpoint (e.g. FireEye EX, NX, HX and Redline). IT Support Engineer I Amazon Fulfillment Services, Inc - Gouldsboro, PA October 2017 to January 2018 Help the operations team in resolving technical problems within the Fulfillment Center that cover a multitude of technical disciplines and using TCP/IP network protocols to troubleshoot Provide second level of support for the operations of the Fulfillment Center and serves as a resource to Technical Support Technicians while also acting as a representative of the IT department to internal customers. Cisco networking with Nexus and iOS switches ? Responsible for pushing out and performing all firmware upgrades via TFTP ? Made necessary port changes for networking in the office ? Set up several switches with VPN connectivity for onsite use Regular activities include network engineering and troubleshooting, project management, mentor-ship of Technical Support Technicians, data cabling, systems administration in a variety of software and hardware environments, root cause analysis in problem solving, and assistance in managing

the daily activities of the department. Managed a Cisco VoIP network consisting of Unified Call Manager and Unity Messaging o User administration consisting of creating user profiles and editing line settings ? Created system wide profiles and templates managing button layouts, basic settings and default images depending on user groups to establish uniformity ? Created policies regarding voicemail forwarding and age retention To install new IT equipment and updating according to the Amazon network. Assigning IP addresses to new and old equipment's by using DNS server and DHCP protocol Provisioning RF Scanners for the end users and assigning/troubleshooting Zebra GX430t Label Printer, Zebra ZT420 Label Printer for end users Responsibilities included: Windows/Mac/Linux OS deployment and support User hardware/software/peripheral support, LAN troubleshooting and support Systems administration, Hardware procurement and asset management, Creating and maintaining documentation, Mentoring and handling technical escalations from junior technicians Data Security Intern Berkshire Hathaway GUARD Insurance - Wilkes-Barre, PA February 2017 to May 2017 Review and update documentation for policies, procedures, standards and guidelines. Research and evaluate applications and services for use by the institution. Provide a matrix when possible, detailing features within each different application or service. Assistance with the deployment and upkeep of the information security department's website content. Provide first level compliance monitoring and investigations. Assist with applications/tools including but not limited to SIEM, IPS, Netflow, e-mail gateway protection, and DLP tools. Record and track IT security incidents, including but not limited to copyright violations, compromised accounts, e-mail threats, and abuse reports from various sources. IT Security Analyst Intern TMG Health, Inc - Jessup, PA August 2015 to December 2015 Performing risk assessments and testing of data processing systems by using Facet software and to forward the processed data to the management. Help and carry out the security implements, business analysis and solving problems as well as using the Active Directory for new user information. User administration through Active Directory including permission changes, password resets and updating user information Generating and formulating data by using SQL server. Generate and maintain documentation of security systems architecture, troubleshooting and support guidelines, system

metrics, project information and plans Participate in development of best practices including security monitoring, capacity planning, network monitoring, configuration, security, historical metrics, recovery strategies, and migration strategies Education Master's in Cyber Security Purdue University - Lafayette, IN December 2018 to December 2019 Bachelor's in Computer Information Systems King's College - Wilkes-Barre, PA August 2013 to May 2017 Skills Splunk (1 year), CheckPoint IPS (1 year), Blue Coat Proxy (1 year), Microsoft Office 365 (5 years), Microsoft Exchange (4 years), Microsoft Outlook (4 years), TCP/IP (4 years), Nmap (3 years), CMD (3 years), SQL (2 years), C# (4 years), Carbon Black (1 year), Trustwave Web Defend (2 years), McAfee IDS (2 years), Resilient Systems (1 year), Managed Security Services (2 years), Wireshark (2 years), Redline (1 year), FireEye EX, NX, HX (2 years), Symantec (1 year), TCP Dump (2 years), Incident Management (2 years), Data Analysis (2 years), Database Management (2 years), Windows 7 (4 years), Windows 8 (3 years), Windows 10 (3 years), Linux (1 year), Cyber Security (2 years), Siem (2 years), Information Assurance (2 years), Nist (1 year), Cyber Kill Chain Framework (2 years), Incident Response (2 years), LAN (3 years), WAN (3 years), Network Access Control (2 years), Windows Server 2008 (3 years), Visual Studio (3 years), Word (7 years), Excel (7 years), Webex (2 years), Powerpoint (6 years), Service Now (1 year), Information Security, Troubleshooting (3 years), AWS (1 year), Azure (1 year), Google Drive (5 years), Dropbox (5 years), One Drive (5 years), Google Docs (5 years), Trustwave WAF (2 years), QRadar (1 year), Security, Active Directory Links https://www.linkedin.com/in/anmol-singh-717349b4/ Additional Information Technical Proficiencies Operating Systems: Windows 7, Windows 8, 8.1, 10, Linux/OS, Windows Server 2008-2012, VMWare Software: Microsoft Office 365, Visual Studio 2013, Office 2016, Microsoft Exchange, Microsoft Visio, Active Directory, Salesforce, MS SharePoint, Microsoft Project, Cisco VPN, MS Exchange, Group Policy, MS Visual Studio, MS SQL, Lotus Notes Hardware: Dell workstations, Dell laptops, HP workstations, HP Laptops, HP Printers, Amazon Kindle, RF Scanners, HP Label Printers, Zebra GX430t Label Printer, Zebra ZT420 Label Printer, Android Devices, Apple Devices (iPads) Networking: TCP/IP, LAN/WAN, DNS, DHCP Development: CMD, SQL, C# Security Protocols: IDS/IPS, Data Loss Prevention, Distributed Denial of Service, Endpoint detection and

response, Security Tools: Splunk, Carbon Black, CheckPoint IPS, Trustwave WebDefend, FireEye EX, HX, NX, McAfee IDS, McAfee EPO, Wireshark, Nmap, Blue Coat Proxy, Resilient Systems, Remedy, Redline, TCPDump

Name: David Dorsey Jr.

Email: rhodescarol@example.org

Phone: (717)305-4305x8245