Soc Analyst, NPAC Soc Analyst, NPAC Soc Analyst, NPAC Philadelphia, PA Authorized to work in the US for any employer Work Experience Soc Analyst, NPAC IConectiv - Bridgewater, NJ February 2018 to May 2019 Monitor and resolve suspicious and potentially malicious network activity with the use of SIEM solutions Splunk, MacAfee Security Center & Zenoss. I use these tools to monitor network activity as well as checking logs on an as needed basis and correlate logs between the systems Part of the Number Portability Administration Center (NPAC) team, supporting the implementation of local number portability (LNP) for all telecom service providers in the United States. As part of the Security Operations team we are responsible for the confidentiality and integrity of proprietary data from thousands of telecommunications service providers. Correlate suspicious activity seen in the SIEM to activity seen on our WAFs Responsible for using Linux jump boxes to transfer and/or add & delete data files across servers, as well as investigating suspicious activity and correlating it to activity seen in the SIEM Responsible for running vulnerability scans using Nessus on the appropriate asset groups and our satellite server rooms. Also responsible for the helping in the creation and distribution of Vulnerability Reports Information Security Analyst WILLIS TOWERS WATSON - Philadelphia, PA August 2015 to December 2017 Monitor and resolve suspicious and potentially malicious network activity with the use of SIEM solutions Splunk & Qradar. I use these tools to monitor network activity as well as checking logs on an as needed basis Investigate malicious activity on end user machines with the use of FireEye as well as eliminating the threat while keeping the user updated on the progress Monitor the sending of PII information through our Data Loss Prevention (DLP) tool. Make sure any unencrypted PII information has not been sent to any parties who are not meant to receive it while educating users who violate this policy on how to properly encrypt PII information Responsible for making sure DLP was configured based on client requirements and was responsible for making sure our DLP systems were used in accordance with those requirements Involved in multiple audits for DLP showing that the systems were being monitored, investigated, and followed client requirements as well as regulatory requirements. Responsible for running vulnerability scans on all assets being accounted for in out data centers. Responsible for mapping assets as well as adding/removing any

assets from the monthly list. Responsible for creating vulnerability reports on a monthly basis as well as detailing potential solutions for the vulnerabilities with the highest amount of instances Investigate suspicious emails to determine if the email is malicious as well as analyzing suspicious attachments through the use of a sandbox environment IT Security Specialist SMART SOURCE TECHNOLOGIES - North Brunswick, NJ October 2014 to August 2015 Ensuring all company hardware and software meets minimum security baseline. This includes making sure all hardware and software is up to date on configurations and security patches. Developed Smart Source's security plan pertaining to their internal network. Bitdefender Internet Security 2015 was used. Ensuring sensitive company files have the proper security configuration and can only be accessed by the appropriate individuals. Ensuring all devices connected to the company network matches an authorized security profile. Ensuring any unauthorized access of the company network and its files is documented and logged to determine the severity and risk associated with the access attempt. Running anti-malware and virus programs on all company hardware and software to ensure there are no breaches of security. Created regular backups of all files on company machine to improve the safety of sensitive information. Conducted vulnerability scans of our machines and servers using Advanced IP scanner and was in charge of restoring machines in the event of a network compromise. Trained Smart Source employees in what to look for regarding suspicious activity that may occur on the network. Data Standardization, Team Lead NEW YORK STATE DEPARTMENT OF HEALTH - Albany, NY October 2014 to August 2015 In charge of a data standardization team consisting of five individuals. Responsible for screening, hiring training and daily oversight of the team on the use of NYEHMS, a data repository tool developed for New York Department of Health to standardize hundreds of thousands of physician records. Coordinated with the database administrator with respect to both quality and quantity of data standardization efforts. Education Bachelor of Science in Information Technology in Information Technology Rutgers University - New Brunswick, NJ May 2015 Skills Dlp, Qualys, Splunk, Security, Scanning Additional Information 2+ years experience with Splunk 1+ Year Experience with Qradar 2+ Years experience with Fire Eye 2+ Years Experience with Qualys Vulnerability

Scanning Tool 2+ Years' Experience with DLP Experience with MacAfee Security Center Experience with Zenoss

Name: David Williams

Email: nramirez@example.com

Phone: 564.342.4388x2989