IT Security Operations Analyst IT Security Operations Analyst IT Security Operations Analyst - Nike, Inc Washington, DC Versatile, achievement based professional with over 4 years of experience in Intrusion Detection, Vulnerability Management, Security Operations and Cloud Security using tools like Splunk, Demisto, Nessus, Splunk and DivvyCloud. Critical problem solving and analytical skills, a fast learning curve and the ability to quickly adapt to a fast paced and evolving environment. Dedicated professional with the skills sets and personality to excel both in a team and individually. Authorized to work in the US for any employer Work Experience IT Security Operations Analyst Nike, Inc - Beaverton, OR July 2018 to Present Achieved 90% compliance on remediation of vulnerabilities on external facing data center assets within 3 weeks by initiating and maintaining proper professional communication with various stake holders to ensure remediation was completed within policy defined timeframes. Ensure security of cloud resources like EC2, S3 and RDS and enforced cloud security standards by creating NACLs, Route Tables, Security Groups and WAF. Perform scheduled and non-scheduled vulnerability scans using Nessus and Nexpose to achieve greater visibility on the vulnerability posture of the environment and reports to appropriate parties with remediation recommendations. Coordinate with Pentest Team for the validation and remediation of web application vulnerabilities like XSS and SQL injection to ensure security of consumer data. Cyber Security Incident Handler InfoPro Solutions LLC - Lanham, MD September 2016 to July 2018 Managed security awareness program focused on phishing that led to over 35% drop in security incidents whereby users were educated on how to identify a suspicious email and how to respond. Monitor and manage the flow of network traffic with the use of protocol analyzers like Wireshark, Firewalls like Palo Alto, Checkpoint and Intrusion Detection with Snort to identify anomalies, ensuring proper network performance and maintaining SLAs. Support 24x7 MSSP SOC using Demisto, CrowdStrike, VirusTotal, Splunk in performing log analysis to investigate security incidents and ensure the enforcement of security policies. Lab Manager Sacred Heart Computer Lab September 2014 to March 2016 Troubleshooting, configuring of desktop components and assisting installation of hardware and software. Ensure efficiency and availability of network by troubleshooting routers, switches and other network devices. Certifications/Licenses

CompTIA Network+ CompTIA Security+ AWS Certified Developer Associate EC- Council Certified Incident Handler Additional Information CORE COMPETENCIES Tools: FireEye, Nessus, Burp Suite, ServiceNow, SolarWinds, Snort, Nexpose, Splunk, Privacy Guard. Skills: Cloud Security, Vulnerability Management, Intrusion Detection, Risk Management, SIEM. Concepts: TCP/IP, Firewall, OSI Model, OWASP, SSO, NACs, TLS, Router, Switches. Cloud: VPC, CloudTrail, Route 53, EC2, S3, Aurora, DynamoDB, Lambda, CloudFront. Platforms: AWS, Ubuntu, Kali Linux, Red Hat, CentOS, Windows Servers, Oracle and SQL databases.

Name: Albert Fernandez

Email: rfox@example.net

Phone: 2254630883