Cyber Security Analyst/Engineer Cyber Security Analyst/Engineer Cyber Security Analyst/Engineer - Zyston Plano, TX Skilled security professional with broad experience specializing in the escalation of threats within network environments. Work Experience Cyber Security Analyst/Engineer Zyston December 2018 to Present Implementation of Alienvault and Qradar AWS based VPN configuration Log/Event analysis using multiple SIEMs and Security Solutions Worked with engineering teams to map out customer network topologies Log/Event correlation pivoting between Cylance, Forti, Checkpoint, and Proofpoint. ESXi management Escalation of Phishing Emails Escalated abnormal traffic events VIA threat hunting within customer environments. Cyber Security Engineer Wipro June 2017 to December 2018 Designed network topology for projects. Configured and administrated ESXi hosts Implemented network hardware SIEM event analysis Installed and configured numerous security solutions. (QRadar, Vectra, Demisto & Intsights) Threat intelligence for vulnerability management Worked in forensic analysis using Autopsy Worked as Vulnerability Management Lead assisting in collating vulnerability data and sending remediation tasks to appropriate teams. IT INTERN SOUTHERN ILLINOIS UNIVERSITY August 2016 to May 2017 Designed Asterisk VOIP Lab Acted as T.A. for undergraduate networking class Wrote and presented lecture on VOIP Tutored Students Configured CMS based ticketing system for networking class IT SUPPORT TECHNICIAN CITY OF MURPHYSBORO IL February 2016 to January 2017 Monitored city-wide support ticket queues Upgraded and expanded network systems and their components Worked extensively with Spiceworks Completed remote maintenance Incorporated feedback and recommendations from other staff members when modifying software configurations Upgraded server systems Extensive work with Windows Server Education BACHELOR OF INFORMATION SYSTEMS TECHNOOLOGY in INFORMATION SYSTEMS TECHNOOLOGY SOUTHERN ILLINOIS UNIVERSITY - Carbondale, IL May 2017 ASSOCIATE OF ARTS JOHN A. LOGAN COLLEGE - Carterville, IL June 2015 Additional Information VMware Vsphere/ESXi Administration QRadar Installation & Log Forwarding Configuration Vulnerability Scanning Tools (Nessus, Rapid 7, Nikto, WPScan) Proofpoint Event Correlation and Escalation (Clicks permitted/Phishing) Splunk Installation & Log Forwarding

Configuration Wifi hacking/WPA2 cracking using tools like Aircrack & Hashcat Secureonix Event Analysis and Escalation AlienVault Installation & Log Forwarding Configuration Fingerprinting using tools like NMAP & Netcat McAfee ESM Event Analysis and Escalation Demisto Installation/ Configuration & Playbook Design Reconnaissance using cached DNS records, Whois, Dmitry, and Web Directory Enumeration Fireye NX Event Analysis and Escalation Vectra Installation & Configuration MITM attacks using tools like Fluxion to create rogue AP's and Fake Portals Qradar Event Analysis and Escalation Soft Firewalls (Untangle, PFSense) Wireshark or TCPDump to grab plain/cleartext credentials Alienvault Event Analysis and Escalation Packet Analysis (Wireshark) Carbon Black Certified

Name: James Rodriguez

Email: cjohnson@example.net

Phone: +1-345-330-2120x316