

INFORMATION SECURITY ENGINEER INFORMATION SECURITY ENGINEER INFORMATION SECURITY ENGINEER Las Vegas, NV Experienced analyst with over five years experience of working in IT and Cyber Security. Experienced with email protection, SIEM, IDS/IPS, endpoint security protection, network access controls, vulnerability management software, and packet analysis. Education includes an AAS in Telecommunications and an AAS in Network Administration, GSEC, GCIA, GCIH, A+, Network+, Project+, CIW-WSA, Splunk I & II certifications. Other experience includes 10+ years of Management experience, 20+ years of Customer Service/Technical Support experience, and 5+ years of Sales experience. Work Experience

INFORMATION SECURITY ENGINEER UNITED POWER - Las Vegas, NV March 2019 to Present Responsible for the installation, configuration, upgrading, tuning, creating correlation rules and policies for SIEM, IDS/IPS, Vulnerability Management, Network Access Controls, endpoint security solutions, and deception software. Knowledge of packet inspection, IDS/IPS, firewall policies, firewall extended dynamic lists, creation of custom host based and perimeter IDS/IPS signatures, and deception technology. Analyze items escalated by other team members and determine further escalation and/or actions. Assist in creating and maintaining standard operating procedures, policies and playbooks. Mentor and assist other team members. Completed project implementing a NAC solution in multiple locations. Configured fail-over solutions and created policies for NAC. Currently deploying SIEM solution and configuring data inputs and data forwarding. Ensure proper configuration with 3rd party API s. Principal SIEM admin and engineer.

GLOBAL CYBER SECURITY ANALYST I/II LAS VEGAS SANDS CORP July 2016 to March 2019 Experience in a global enterprise environment by monitoring 10 properties in the US, China, and Singapore. Responded to IDS/IPS, SIEM, WAF alerts by obtaining pcaps and using Wireshark for deep packet analysis. Utilized endpoint protection to monitor, encrypt, and complete virus scans for servers and workstations. Created security tickets to assign block requests and to track previous events/incidents. Created a Visual Task Board for triaging, assigning and monitoring open tickets. Generated reports for auditing security tickets and for tracking SLA s. Used open source tools for researching events/incidents. Created and maintained SOP s and playbooks to

ensure consistency in processes. Used multiple tools to correlate alerts between host, proxy, and external traffic. Created SOC Training Playbook for onboarding and training new employees ensuring consistency in the information given and received. Mentored and trained other analysts.

Assisted other team members in any escalations that needed further analysis. Maintained Scheduling for the department to ensure there is no coverage gaps. Compiled and created ticket/repository audits and various other reports for team presentations and upper management.

Assisted with multiple projects as needed. SOLUTIONS MANAGER VERIZON WIRELESS May 2015 to July 2016 Work daily with solutions sales teams to manage customer wait times, resolve customer issues, and assist with customer transactions as needed. Manage store merchandise and layout to align with store merchandising plans. Assess and track team's performance, which includes meeting and exceeding assigned quotas. Provide ongoing development, training, and coaching. Analyze store staffing needs, provide hiring and promoting decisions, reporting financial and sales statuses, managing cash and inventory levels, and ensuring compliance, sales, and retention objectives are met. SOLUTIONS SPECIALIST VERIZON WIRELESS August 2011 to May 2015 Responsible for managing and exceeding sales quota/revenue targets for net activations, accessories, data sales and customer renewals, demonstrating equipment functions and network capability, proposing solutions that best benefit the company and the customer, ensuring customer satisfaction with every sale, retaining customer business, renewing contracts, presenting data solutions, and offering accessories designed to enhance the Verizon Wireless experience. Winner's Circle winner 2012 and 2013. IT Support Specialist Maritime Museum of San Diego - San Diego, CA September 2013 to September 2014 Provided technical support for the museum staff including software and hardware related issues. Managed Windows Exchange Server including creating, modifying and deleting users. Install, troubleshoot and maintain software and hardware including servers, computers, printers, monitors, telephones, video security system, and POS systems making repairs as needed. Proficient in Microsoft products including Windows and Office suite. Provided end user support and education on hardware/software systems. Installed/Repaired CAT5 cable, routers and switches as needed. Installed and maintained anti-virus, malware programs and spam

filters to aid in preventing attacks on computer systems. Maintained Tech Soup account for non-profits to ensure the museum was able to get software products they needed. Maintained Microsoft VLSC account that contained all donated Microsoft software and license keys for the museum. Migrated users from Windows XP Professional to Windows 7 Professional. Implemented the migration of users to Office 365 and other cloud solutions. Created a repair request log to track and prioritize user requests. Education BACHELOR OF SCIENCE in BS, CYBER SECURITY AND INFORMATION ASSURANCE WESTERN GOVERNORS UNIVERSITY March 2017 to Present AAS in INFORMATION SYSTEMS TECHNOLOGY TIDEWATER COMMUNITY COLLEGE 2012 AAS in COMPUTER SCIENCE ECPI COLLEGE OF TECHNOLOGY 2001 Skills Cyber Security, Information Security, Siem, Network Security, Incident Management, McAfee ePO/NSM/SIEM, Rapid7 Nexpose, Office Suite, Attivo, ForeScout, CrowdStrike, FireEye, Palo Alto, Splunk, SOC Operations, Mentoring, ServiceNow, Packet Analysis, Symantec, AlertLogic, Team Leader, Teamwork, Cyber Security Engineering, Wireshark, Network Access Control (NAC), Endpoint Security, Cyber Security Analyst Links <https://www.linkedin.com/in/edna-stephensen-42308a54/> Certifications/Licenses GIAC Security Essentials Certification (GSEC) June 2017 to June 2021 GIAC Security Essentials Certification (GSEC) Issuing authority GIAC Certifications Issued Jun 2017 - Expires Jun 2021 Credential Identifier Credential ID 40916 GIAC Certified Intrusion Analyst (GCIA) June 2018 to June 2022 GIAC Certified Intrusion Analyst (GCIA) Issuing authority GIAC Certifications Issued Jun 2018 - Expires Jun 2022 Credential Identifier Credential ID 12948 GIAC Certified Incident Handler (GCIH) June 2019 to June 2023 GIAC Certified Incident Handler (GCIH) Issuing authority GIAC Certifications Issued Jun 2019 - Expires Jun 2023 Credential Identifier Credential ID 34841 CIW Web Security Associate October 2017 to Present CIW Web Security Associate Issuing authority CIWcertified Issued Oct 2017 - No Expiration Date Credential Identifier Credential ID 791761 See credential Industrial Control Systems 301 - Certificate of Completion May 2018 to Present Industrial Control Systems 301 - Certificate of Completion Issuing authority National Cybersecurity and Communications Integration Center Issued May 2018 - No Expiration Date Splunk Certified User

July 2018 to Present Splunk Certified User Issuing authority Splunk Issued Jul 2018 - No Expiration Date Credential Identifier Credential ID Cert-235127 Splunk Certified Power User
August 2018 to Present Splunk Certified Power User Issuing authority Splunk Issued Aug 2018 - No Expiration Date Credential Identifier Credential ID Cert-253796 AWS Cloud Essentials - Certificate of Completion April 2019 to Present AWS Cloud Essentials - Certificate of Completion Issuing authority Amazon Web Services (AWS) Issued Apr 2019 - No Expiration Date Network+ Certification August 2014 to August 2020 Network+ Issuing authority CompTIA Issued Aug 2014 - Expired Aug 2020 Credential Identifier Credential ID COMP001020612259 A+ Certified A+ Issuing authority CompTIA Issued Aug 2014 - Expired Aug 2020 Credential Identifier Credential ID COMP001020612259 Project+ February 2018 to Present Project+ Issuing authority CompTIA Issued Feb 2018 - No Expiration Date Credential Identifier Credential ID COMP001020612259

Name: Luis Harris

Email: kristymiller@example.com

Phone: 531-623-7818x40242