Senior Advisor, IT Security Senior Advisor, IT Security Senior Advisor, IT Security Springdale, AR To obtain a position where proven technical skills would be utilized. Specializing in Cloud Security with a strong understanding of compliance and regulations in cyber security. Over 10 years of IT experience Authorized to work in the US for any employer Work Experience Senior Advisor, IT Security Virtustream - Remote June 2017 to Present Oversee development, implementation and execution of security projects and assignments. Prioritize project work while mentoring junior staff and handling escalations when necessary. Provide consultation from architectural, engineering, and support for Information Security requests. Review security policy clarifications and exception requests Lead Security projects Triage general security questions from other internal teams. Tune, monitor, and analyze network traffic and respond to IDS alerts Analyze network and host-based security logs to identify potential security threats. Create and review documentation for Security Operations and procedures Collaborate with GRC team to develop policies, standards, and procedures related to Security Management - including compliances/regulatories: PCI-DSS, FISMA, HIPAA, SSAE-16, CSA Star Program Architect and design security as a service with associated virtualized tools such as Nexpose, Splunk, Fortinet, Palo Alto, and F5 Consultant Wells Fargo - Remote December 2017 to May 2018 Consult with senior manager and security engineers to develop a hierarchy model for Palo Alto s firewall policy management Collaborate with application owners to retrieve technical specs to apply appropriate layer 7 application ID on Panorama s policy. Assist application owners by developing a visio diagram of their applications on a network topology level Acquire appropriate ports and collaborate with Palo Alto to develop custom application ID s Create API script for automated configuration on the Panorama device Ensure proper communication in place as well as maturing the change request process for any new firewall rule request to the Panorama/Palo Alto devices. Senior IT Security Engineer Tyson Foods Incorporated - Springdale, AR October 2015 to June 2017 SSL-VPN/Juniper Pulse Secure Configuration | Entrust IDG | QRadar Configure SSLVPN profiles to allow 3rd party remote Troubleshoot any Pulse Secure VPN connection issues on client-end Manage ACL for any new or old external/3rd party devices on the network Utilize IBM Qradar SIEM for any log entry payloads

for connection troubleshooting Rely on IBM Qradar SIEM for log traffic based from Palo Alto & Fireeye Security Awareness Create content based on main topics related to security awareness. Phishing Confidential Handling Passwords Social Engineering Collaborate with Champion to setup and establish classes for malware awareness related topics such as scareware, ransomware Provide qualitative metrics based upon client survey and responses. Nexpose Vulnerability Management & Metasploit Framework/Pro Create a liaison for all of Tyson s IT to service for remediation of existing vulnerabilities Perform scannings (including authentication scans) on sites based on assets/operating system Assist with scanner-rights given users to manage their own vulnerability remediations Collaborate with Rapid7 for any false positives debugging process Arrange scheduled dates of scan engine initiations. Create reports based on Nexposes reporting templates and distribute for remediation Create documentation guidelines and auditing purpose Maintain and manage account settings (Global administrators, scanners, user's privileges) Perform Metasploit exploitations/pen-testing if exception is provided (both framework & pro version) MPCS certified Palo Alto Engineer | Firemon Security Manager | F5 - Big IP | Dell SonicWall Monitor any threats and abnormal traffic activities. Utilize Panorama as management console for over 500 PA devices Configure site-to-site setups utilizing IKE phases Manage and create firewall rules and utilizing change request methods (BMC Remedy) Install and configure Palo Alto devices (PA-200, PA-500, PA-4020, PA-7050) Troubleshoot traffic activity for firewall configurations Utilize Palo Alto s APIs to perform automation tasks using Python or Powershell Collaborate with Palo Alto s support team for any troubleshooting. Convert Cisco ASA and SonicWall devices to Palo Alto. Conversion includes: Firewall Administration IPSec Tunnels Manage the Firemon security module to monitor any firewall devices on Palo Alto Configure Firemon to send reports for any anomalies with Palo Alto s devices. Configure F5 virtual pools for web applications. Setup web application firewall within F5. Configure F5 manually for any RMA purpose IT Support Analyst & Malware Response Team ARUP - Manhattan, NY March 2015 to September 2015 Responsibilities Responsible for IT Supporting in all of Americas Region Perform software installation via SCCM and configure Cisco IP Phones/Communicator Monitor daily activities for malware/viruses Managing and maintaining

anti-malware solutions within Americas region Utilize Symantec Endpoint Protection through SEPM Management Console Identifying and reporting on malware related activities through log analysis Perform research and development, identifying best practices for handling malware outbreaks and infections Raising security awareness with end-users Utilize Cisco Ironport to filter malicious attachments and phishing emails. Troubleshoot network application inbound/outbound connectivity utilizing Cisco WSA proxies and wireshark. Vulnerability Management Specialist & Policy Compliance Novartis - East Hanover, NJ April 2012 to March 2015 Responsible for the delivery of service for global vulnerability scanning and reporting on all Novartis network devices Migrated IBM Tivoli tool to QualysGuard for Policy Compliance Created controls based on ISO27001/2 and NIST framework Utilize QualysGuard as primary tool to perform policy scanning (involves authentication scanning) Implemented controls on various OS: Windows 2003/2008/2012, AIX 6/7/8, SQL 2012, Red Hat Enterprise, VMWare ESXI Perform penetration testing utilizing Metasploit Framework version Provide assistance in remediation of vulnerabilities to customers. Assist with documentation for guideline procedures Education AVTech Institute of Technology 2008 Skills IT Security (10+ years), Firewalls (5 years), Network Security (5 years), IT Management, Information Security, Siem, Nist, Cyber Security, Linux Links https://www.linkedin.com/pub/steven-atoche/48/57/176 Certifications/Licenses MPCS Present Metasploit Professional Certified Specialist CompTia Security+ July 2015 to July 2018 Certified Information Systems Security Professional (CISSP) February 2017 to January 2020 CCSK Present Certificate of Cloud Security Knowledge A valid IT Specialist certification CCSP

Name: Andrew Lamb

Email: michelefleming@example.org

Phone: +1-744-211-7754x073