Information Systems Security Engineer Information Systems Security Engineer Information Systems Security Engineer - Dole Packaged Foods LLC Sylmar, CA Work Experience Information Systems Security Engineer Dole Packaged Foods LLC May 2018 to Present Technical Responsibilities ? Sr. Investigator on multiple Incident Response and Digital Forensic engagements. ? Responsible for building Incident Response and Digital Forensics capabilities and processes for entire organization by deploying forensic tools in the environment. ? Deploying and managing Cisco AMP. ? Development of penetration testing procedures. ? Configure and manage Office 365 Security, policies, Alerts and Reporting (ATP Safe links, DLP, Anti-Phishing, Impersonation). ? Responsible for managing and maintaining OS and application vulnerabilities for entire organization. ? Design, configure and administer WAF in Azure. ? Implement and administer SIEM- AlienVault. ? Lead security investigator tasked with investigation of security alerts. Serves as escalation point for other team members. Conducts in depth analysis to determine scope and impact. ? Routinely analyze firewall to check indicators of compromise. ? Manage and run vulnerability scans to check for active vulnerabilities in the organization Management ? Responsible for maintaining risk registrar for entire organization and hold regular meetings with managers and directors of various departments to mitigate risk within the SLA. ? Provide guidance and training to junior team members. ? Senior member of Risk Management team who serves as point of contact for any escalation regarding system security. ? Responsible for creating mitigation plans for existing vulnerabilities to help other teams in remediation process. ? Responsible for providing regular security briefings to Vice President of infrastructure and security. ? Responsible for creating and maintaining technical SOP's. ? Responsible for interviewing and hiring new employees. Network Security Analyst Pancreatic Cancer Action Network June 2017 to May 2018 Security Process and management ? Manage and conduct security testing including, penetration tests, application assessments and general risk and vulnerability assessments. ? Continuously working to remediate known vulnerabilities and eliminate false positives. ? Research and understand Microsoft KB articles and other CVE articles and remediation. ? Stay up-to-date on security trends and threat information ? Review and analyze organizational needs and make recommendations regarding security and compliance requirements for future IT Projects. ? Being part of IT projects, Monitoring and communicating with various level of management. ? Security Patching ? Security auditing and frameworks knowledge (PCI, ISO, HIPAA) ? Train staff on network and information security procedures and practices. ? Create, implement and test network disaster recovery plans ? Vender renewals and management. Technical ? Evault data backup appliance and disaster recovery vendor solution Management. ? Configured Cisco Firepower management policies for web traffic filtering and IDS/IPS protection. ? Managing and configuring VLAN on Cisco switches via Putty. ? Cisco Meraki wireless network, Cisco Switching, Cisco UCS Support ? Manage Network Infrastructure comprised of Cisco ASA 5525-X firewalls and Catalyst 3650 switches ? Administered 20+ primarily windows virtual machines through VSphere. ? Configuring and Managing DMZs ? Configuring ACLs ? Perform troubleshooting and root cause analysis regarding network, server or associated system Problems and document resolution for future reference ? Responsible for preparing incident response documentation. ? Office 365 administration via the exchange and SharePoint admin centers. ? Configuring Advance Threat Protection via Office 365. ? Managing DLP in office 365 for OneDrive, SharePoint and Exchange. ? Managing telecom infrastructure through Cisco unified cell manager and Cisco unity connection. ? Air Watch Mobile Device Management to manage mobile devices. ? Solar Winds log management to monitor network, server and firewall alerts for possible security Challenges. IT System analyst The Children's Clinic - Long Beach, CA June 2012 to January 2017 Security Measures and Investigation ? Develop strategies, tactics, and contingency plans to effectively target Vulnerability Threats using Barracuda. ? Analyzing, deployment and maintenance of Barracuda Web Application Firewall. ? Deployment and maintaining of Proofpoint email protection system. ? Defining rules and thresh holds in Proofpoint. ? Securing Laptops and a USB using Symantec endpoint encryption. ? Contribute in planning and deployment of IT security policies and procedure under HIPAA security Rule (e-PHI). ? Participating in testing and implementation of new security technology ? Penetration testing of network using various tools and technologies. ? Structuring methodologies to adhere to company security policies guidelines. ? Planning, maintaining and managing backup and recovery of servers using Symantec Exec 2014 and 2016 System Administration ? Build, deploy and maintain Physical & VM Servers using MS 2008/2012 R2, as well as Windows 7, 8 workstations. ? Upgrading Windows Server and Exchange server. ? Updating servers using WSUS. ? Managing and deployment of computers using WDS server. ? User management in AD. ? Help desk support and reporting using ManageEngine. ? Cisco Voice/ Phone / Voicemail setup using Cisco Unified Communication manager and Cisco Unity Connection. ? Troubleshooting Epic- a Citrix based EMR System. Report Management ? Dashboard management for Proofpoint and Barracuda. ? Incident report ? ManageEngine Report o DLP Incident Report o Vulnerability report Other ? Part of disaster recovery and incident handling team. Participated in constructing the procedure in case of natural disaster and emergency situations. Anaheim QA Intern Extron Electronics March 2013 to April 2013 Following Hardware test procedures. Analyzing test results and preparing the final report. Education Bachelor of Science in Computer Engineering California State University 2009 to 2013 Skills Active directory, Cisco, Dns, Exchange, Networking, Information Security, Siem, Network Security

Name: Elizabeth Wiggins

Email: garykerr@example.com

Phone: +1-557-755-8507x5879