Security Analyst, Tier II Security Analyst, Tier II Security Analyst, Tier II - Southern New Hampshire University Manchester, NH Executed network penetration tests using various tools within Kali Linux (Hydra-THC, Social Engineering Toolkit, Metasploit, Nmap NSE's, etc) to find vulnerabilities in our network and offer guidance for remediation. Assumed responsibility for the security infrastructure of our networks and internal private cloud, including MikroTek switches, Sonicwall NSA firewalls, and AV Recovered failed devices using DFIR methodology and tools (SANS SIFT, Katana Toolkit, EaseUS Data Recovery) Work Experience Security Analyst, Tier II Southern New Hampshire University June 2019 to Present Proactively maintain the integrity of the SNHU corporate infrastructure for staff and students as a key member of the Security Operations Center at a time where processes were definingly reactive. ? Performed log analysis within Splunk Enterprise as our centralized log system, pooling in logs through various products, including; Cisco FirePower IDS, Tenable.io, Windows Defender, Symantec EP, among others for identification and remediation. ? Using Splunk, I was able to speed up our Identification process by an average of 2 hours through specific queries, customizable alerts, and unique dashboards. ? I work with the Security Director and Security Operations Manager to build the SOC from the ground up through our roadmap to increase our overall security posture. ? Performed incident analysis using network analysis tools such as Wireshark and Fiddler for root cause analysis, as well as internal system logs for forensic analysis. ? Cross-trained with our Security Engineering team to work on more complex issues involving Pentesting and DFIR. ? Executed both Network & Application Penetration Tests using various tools within Kali Linux (Hydra-THC, Social Engineering Toolkit, the Metasploit Framework, Nmap NSE's, etc) to find vulnerabilities in our network and offer guidance for remediation. ? Configured and managed internal infrastructure (e.g., DNS, routing, VLANs, DHCP, VOIP) ? Troubleshooted network configuration issues using packet capture and scanning tools, such as Wireshark, Nmap, and Fiddler ? Proactively sought out network and infrastructure "weak points" to harden defenses. Security Administrator C Squared Systems March 2019 to June 2019 Maintained Microsoft Windows domain and Linux (Ubuntu / CentOS) Linux Environment ? Created and updated Windows Group Policies with a security-focused perspective. ? Executed both Network &

Application Penetration Tests using various tools within Kali Linux (Hydra-THC, Social Engineering Toolkit, the Metasploit Framework, Nmap NSE's, etc) to find vulnerabilities in our network and offer guidance for remediation. ? Recovered failed devices using DFIR methodology and tools (SANS SIFT, Katana Toolkit, EaseUS Data Recovery, and FTK Imager). ? Built and was the principal Security Admin of our AlienVault OSSIM setup for Vulnerability Assessments and Check_MK for monitoring the infrastructure. ? Maintaining Microsoft SQL development and production environments. ? Updated and maintained the Company Private Cloud infrastructure and the VPN servers ? Worked with various Virtualization technologies such as HA Virtualization clusters and virtual machines (VMWare). ? Configured and managed internal infrastructure (e.g., DNS, routing, VLANs, DHCP, VOIP) ? Managed Microsoft Exchange Hybrid deployment (Microsoft Exchange server 2013 and Office 365/Exchange Online). ? Deployment and Automation (Scripting and Powershell) ? Troubleshooted network configuration issues using packet capture and scanning tools, such as Wireshark, Nmap, and Fiddler ? Proactively sought out network and infrastructure "weak points" to harden defenses. ? Assumed responsibility for the security infrastructure of our networks and internal private cloud, including MikroTek & Ubiquiti EdgeRouters and switches, Sonicwall NSA firewalls, and AV Desktop Engineer / Security Consultant Scribe Software / TIBCO Software November 2016 to March 2019 With a focus on Security, I've made numerous suggestions in my time here to help us gear toward SOC II compliance, such as creating and managing a Phishing email box associated with Linux + Windows Security Lab VM's for testing of phishing emails and malware entering our system. Created and conducted Security Awareness Training to assist with SOC II requirements. Performed as the primary contact for Security-related incidents within the company. ? Implemented various security fixes for the infrastructure, such as Mimecast for O365, Webroot SecureAnywhere, Incident Reporting, ManageEngine EventLog Analyzer, among multiple hardening fixes for Linux-based, Windows-based environments, Digital Forensics when needed, and other applications. ? Worked with the Security Operations Center and managed and maintained vulnerability scans with Tenable.io Nessus Security Center against multiple environments supporting Windows, macOS, and Linux. ? Provided direction and assisted with the

construction of IT Security Policy, and Disaster Recovery Plan. ? Proficient with the use of various utilities along with PowerShell, and some Python scripts to assist End Users with all varieties of tickets ranging from hardware and software to the network. ? Kept an intuitive mind by seeking out information about the systems and documenting their purpose within a Visio diagram. ? Achieved an automated deployment setup using a mix of PDQ Deploy and a robust Windows Deployment Service environment for the deployment of Windows-based Operating Systems (Win10, Server 2012 and Server 2016), as well as an Automated In-Place Upgrade task through Microsoft Deployment Toolkit to update any non-Windows 10 system to the latest version of Windows 10 Pro for Microsoft compliance. ? Volunteered to assist with issues pertaining to our OpenMind Ruby-On-Rails Web Application, adjusting the forms and scripting of individual (.RHMTL) and (.rb) files. Additionally, assisted with Apache powered redirects for our scribesoft.com sub-domains. ? Office 365 management, involving Exchange, Skype for Business, SharePoint, Local and Azure Active Directory integration, and the Security Center. ? Maintained the CardAccess 3000 Badge System by learning the product and keeping it functional. System Administrator / Security Consultant Alexander Technology Group August 2016 to October 2016 I filled a multitude of roles at Scribe Software, varying from Jr Systems Administrator, Network Administrator, Security Consultant, and deployment. I managed the company's assets and implementing new ideas for standardizing technologies used within the organization, ranging from (Network, Asset Management, and Help Desk Systems). ? Filled network gaps through security assessments and gap analysis. ? Assisted End Users with all varieties of instances ranging from hardware and software to the network. ? Created Windows 10 Deployment package using PDQ Deploy with step-by-step instructions during the install for additional software to be installed after the deployment. ? Provided consulting for cable management in the server room based on best practices. ? I wrote up a plan to standardize the equipment used by each of the teams through the business, based on job function and performance needs. ? After our DNS provider suffered a DDoS attack, I provided an immediate remedy to our Business Continuity plan on backup solutions and failover solutions that should be in place. ? Implemented Microsoft MDM as its Administrator. Configured the policies for several

managed devices (smartphones, tablets, PC's) ? Office 365 management, involving Exchange, Skype for Business, SharePoint, Active Directory integration, and the Security Center. Setup SharePoint sites and configured Jr. Systems Administrator TEKSystems - Stonyfield December 2015 to July 2016 Maintained Business and End Users with tickets ranging from Multi-Server maintenance, Network, Lotus Notes, Cisco IP phones, to various applications including MS Office 2010/2013, as well as hardware replacement and virus removal. ? Managed the setup of new employees through imaging systems with WinPXE, account setup in ADDS, pushing of Group Policy updates, and new software remotely or at the workstation through Symantec Altiris Console. ? Maintained Servers and Network, troubleshooting DHCP and DNS related issues, along with TCP/IP. Provided high-efficiency practices for server room layout and patch cable management. ? Utilized knowledge of various Cisco ASA switches and firewalls, along with servicing phone systems through Cisco CM and Unity. ? Performed Network monitoring tests using SolarWinds, cable testing, as well as VLAN and Port configuration. Provided Security solutions and updates to policies, while monitoring Security trends through US-CERT and ICS-CERT. ? Worked overflow for the Information Security team as an interim Security Analyst, resolving tickets ranging from malware, ACL's, security groups, data recovery, and CERT/CIRT. Systems Administrator RobertHalf Technology - Jabra September 2015 to November 2015 Utilized knowledge of various management systems, such as VMware, Active Directory (start/stop users, password, policies, permissions); MS Lync Server (Assigning phone numbers and policies to accounts); Citrix XenApp Services (setting up mobile devices with access to Exchange email servers). Additional proficiencies with supporting IIS and SCCM. ? Assisted End Users with day-to-day issues involving PC, Server, Network, Malware/AV, and Printer issues. (Tier II/Tier III) ? Managed relationship with our external vendors around product needs and licensing. ? Took a leadership role as the Senior member of the US IT office, managing tasks, and asset inventory. ? Wrote a batch script that performed ICMP requests to our iPad displays for connectivity, which increased productivity for all 3 IT location by maximizing desk time. ? Performed on-call duties such as server maintenance, disaster recovery as part of CERT/CIRT. Help Desk Coordinator PIF Technologies Inc April 2015 to August 2015 Providing

exceptional Technical Support with great product knowledge of PIF Technologies / docSTAR SaaS systems, Cloudberry online backup solutions, and Sugar CRM. Configured ODBC connections, Named Pipes and Aliases to ensure connections with SQLEXPRESS server. ? Ensured proper DocSTAR setup, and DocSTAR Eclipse online setup. ? Assisted with Workflow setup ? Utilized high-end Troubleshooting for printers, scanners, and Network concepts (Windows Firewall, DNS, Advanced Sharing, Permissions), while supporting IIS, Windows 7/8, Server 2008/2012 both remote and on-site. SaaS Support Rep Constant Contact September 2014 to April 2015 Proactively took to learning programming (Ruby, and Ruby on Rails), and Networking concepts (TCP/IP, OSI, Firewall, Remote Assistance, Security) to assist Tier 2 during overflow. ? Became proficient in the Constant Contact platform, assisting clients via phone support with HTML and CSS related scripting issues for their marketing material. Advised on best practices, and provided guidance Education Bachelor's in Science in Cyber Security and Information Assurance Western Governor's University 2020 Skills Dns, Iis, Security, Web server, Web services, Cisco, Exchange, Incident response, Nagios, Nas, Network administration, Network security, Networking, Server administration, System administration, Tcp/ip, Virtualization, Amazon web services, Python, Ruby Additional Information Core Competencies IT Security System Administration Data Recovery Network Security Network Administration Incident Response Cybersecurity Network Pentesting Security Awareness Technical Skills Applications Microsoft Office 365 Suite Cloud Platforms Amazon Web Services, S3, Microsoft Azure Communications Microsoft Lync 2010, Skype for Business, Cisco Jabber, Zoom, Slack Databases Oracle 11g/12c, MySQL, SQL Server 2000/2016/Express, MariaDB Email Systems Microsoft Exchange 2010/2016, G Suite, Lotus Notes Hardware Linksys, Cisco, MikroTek, Meraki, Dell, Lenovo, HP, Microsoft Methodologies/Frameworks NIST 800-53/800-115/CSF, PTES, MITRE ATT&CK Mobile Android, iOS, Microsoft ActiveSync Monitoring CheckMK, Nagios, Wireshark, Nmap, Fiddler, AlienVault OSSIM Networking Cisco IOS, DHCP, DNS, TCP/IP, BGP Operating Systems Windows 95/98/XP/7/8/10, macOS/OS X, Kali Linux/Ubuntu Programming Languages Python 3, Ruby, Bash, Powershell, SQL Remote Access RDP, TeamViewer, ScreenConnect, LogMeIn Security DBAN, Helix, Kali, DirBuster, Hydra-THC, Katana 4.0, NirSoft,

Nessus, Snort, Tenable.io, Metasploit, POSHC2, Empire. Burp Suite, Testssl.sh, SQLMap Server Administration Windows Server 2000-2016 (AD, GPO, RDS, WSUS), CentOS Server Hardware HP Proliant, Dell Server Storage NAS, SAN System Backup and Restore Veem Virtualization VMware, Hyper-V, Norton Ghost, System Imaging, Disk2Vhd Web Server IIS, Apache

Name: David Krause

Email: beckystafford@example.net

Phone: 8253696186