Security Engineer Security Engineer Security Engineer - Keurig Green Mountain Burlington, MA Expert level understanding of McAfee SIEM Implementation & its Integration with other N/W devices and Applications and the troubleshooting work. Design, develop, recommend, and implement the McAfee technologies. Implementing and supporting McAfee products: ePO, ESM, ELM, DLPe, HIPS Configure and validate secure systems. Experience working with Nexus 7K, 5K, 2K devices. Experience in Implementing & managing Symantec Data Loss Prevention (DLP). Maintaining critical monitoring systems (Splunk - log management systems) measuring system errors logs performance and availability. Evaluation of log management solution Splunk plus open source Linux storage systems. Strong experience working on SIEM tools- HP Arcsight products like Arcsight Express, ESM, Logger, Connector, ArcMC (Arcsight Management Center). Involved in troubleshooting of DNS, DHCP and other IP conflict problems. Experience with various Endpoint tools like McAfee EPO, CarbonBlack, BigFix, Symantec EPO (IDS/IPS). Setting up users with current McAfee software and connecting to ePO, ESM and ELM. System Admin activities related to that, such as some admin of ePO. Experience in working with Cisco Nexus Switches and Virtual Port Channel configuration and Dell SecureWorks Network IPS Experienced with Encryption tools Vormetric and Symantec Endpoint Encryption. Knowledge of implementing and troubleshooting complex layer 2 technologies such as VLAN Trunks, VTP, Ether channel, STP, RSTP and MST. Implementation of HSRP, VRRP for Default Gateway Redundancy. management of network base McAfee DLP 5000 series by deploying at the access layer for monitoring and analyzing data flow of the sensitive content including deployment of McAfee DLP. Experience with Risk assessment using Industry standards like NIST 800-53 Rev3 and Rev4, HIPPA, PCI/DSS and develop Security policy as per these standards. Have experience with Penetration testing tools, vulnerability scanning tools. Strong hands on experience in installing, configuring, and troubleshooting of Cisco 7600, 7200, 3800, 3600, 2800, 2600, 2500, and 1800 series routers, Cisco Catalyst 6500, 4500, 3750, 2950, and series switches. Hands on experience on F5 LTM, GTM series like 6400, 6800, 8800 for the corporate applications and their availability. Experience of Service Now ticketing system. Principal Abilities: Authorized to work in the US for any employer Work Experience

Security Engineer Keurig Green Mountain - Burlington, MA May 2018 to Present Develop and conduct security test and evaluation according to CIS v7 Compliance and PCI-DSS standards. Developed System Security Plan to provide an over life of the system security requirements. Created baseline document to assess the organization based on PCI-DSS standards and CIS v7 Compliance. Auditing Active Directory to check compliance with CIS v7. Develop PowerShell scripts based on the CIS v7 compliance to ensure data integrity. Develop CSRM (Cyber Security Risk Management) standard documents to implement in the organization. Helped in creating ELK Dashboards based on logs captured with Splunk and Rapid 7 Configured Tripwire Tool to meet requirements of PCI-DSS and CIS v7 compliance. Optimized Tripwire tool to ship logs to the ELK server. IT Security Analyst Valeant, NJ January 2018 to April 2018 Worked with endpoint security tools like McAfee EPO and CarbonBlack. Worked with McAfee ESM SIEM tool. Provided real time intrusion detection host-based monitoring services using McAfee EPO and Carbon Black. Developed Guideline document on hardening Cisco Router, Switch and Firewall. Developed Guideline document on Windows server 2008 and later OS versions. Experience with migrating from McAfee EPO to Carbon Black. Good Experience into Handling DLP False positive tickets. Security Analyst Verizon, NJ July 2016 to January 2018 Involved in complete LAN, WAN development (including IP address planning, designing, installation, configuration, testing, maintenance etc.). Implementation of McAfee EPO, ESM, ENS, TIE, MAR, ATD and ELM. Execution of McAfee Policy Orchestrator and McAfee Endpoint Security Protection enterprise suite of software. Assist in the implementation, setup, and management of Symantec DLP (Data Loss Prevention) Provided real time intrusion detection host based monitoring services using Symantec Endpoint, IBM BigFix. Analyze and document client requirements and solution design for how McAfee solutions can meet these requirements now and in the future. Perform upgrades, patching, troubleshooting, threat remediation on McAfee VirusScan Enterprise (VSE), McAfee Host Intrusion Prevention System (HIPS). Experience in deployment of Nexus 7010, 5548, 2148T, 2248 devices Installation and maintenance of Cisco Layer 3 switches 3750, 4500X, 6500 in multi VLAN environment. Encryption - Vormetric Administration; Agent Deployment, Policy Development,

Access control, Guarding Critical Data Elements. Tokenization - Protegrity Administration; managing ESA & DSG appliances, policy/role/data element management. SIEM Tools Metric monitoring and Reporting, Including Ticketing System Remediation Respond to customer requests for assistance on the Dell SecureWorks portal in a timely manner. supporting 90K end user nodes environment utilizing McAfee end point products via ePO server and distributed repositories (DLP, IPS, VS and ePO agents). Design, implementation and Configured and deployed ASA552 and CISCO router for Traffic Signals Group Created and maintained User accounts, Profiles, Security, rights, disk space and process monitoring using Active Directory. Red Hat Linux server testing with various server encryption tools (SafeNet ProtectDB, SafeNet Gemalto and HPE Voltage SecureData appliances.) Deployed Aruba Clearpass 802.1x wireless and Guest Self-Registration for NYSDOT.

Worked on a module for HPE Discover 2017 event to sync the Aruba 8400 Core Switch configuration from git hub using REST endpoints Processes access requests per ticketing system(ServiceNow). Configuring Site to Site IPsec VPN and RA VPN for the Customers' requirements. Deployed Aruba IAP for NYSDOT locations and created 3 SSID for IPods/IPad/DM all on separate VLANS. Security Specialist CCHS, PA April 2015 to June 2016 Experience with migrating from OSPF to BGP WAN Routing protocol. Installation and Configuration of Cisco Catalyst switches 6509, 3750 & 3550 series and configured routing protocol OSPF, EIGRP, BGP with Access Control lists implemented as per Network Design Document and followed the change process as per IT policy. It also includes the configuration of port channel between core switches and server distribution switches Worked on Symantec HIDS/ HIPS CSP solution for FIM (File Integrity Monitoring) and prevention policies including detailed policy creation/ application and Alert configuration Performed System Administration Tasks for Symantec Data Centre Security Prime engineer for the database encryption project using Vormetric Data Security Manager (DSM), Vormetric Application Encryption (VAE) and Vormetric Transparent Encryption (VTE) products. McAfee Engineer on proof of concept / pilot of Device Control in McAfee Data Loss Prevention (DLP), McAfee (IDS/IPS) Responsible for design and deployment of the McAfee Enterprise Security Suite, McAfee ePolicy Orchestrator (ePO), McAfee Enterprise Security Manager (ESM) and

McAfee Enterprise Log Manager (ELM). Network support for Aruba Networks wireless products management console also supporting day to day security operation function by managing Nitro Security (McAfee Acquired) SIEM Experience with setting up MPLS Layer 3 VPN cloud in data center Surveyed Sites and Deployed Aruba Wireless controllers 7010, 7210 and recommended procedures for optimization and improvements in Performance. Create and test Cisco router and switching operations using OSPF routing protocol, ASA Firewalls, and MPLS switching for stable VPNs. Worked with Policy writer and implemented new security policies and controls using NIST framework Performed Penetration Testing on the network to find vulnerabilities. Worked on Windows Admin and created access for creation, updates and terminations of accounts. Wrote programs and implement processes to automate admin tasks (self- initiated), tool used Excel Provide direct day to day support for various technologies such as: WAN technologies (MPLS, Metro Ethernet, etc.), Data Center infrastructure (VLANs, trunks, teaming, L2 & L3, etc.), Campus switching, Load Balancer and Virtualization, Routing protocol support (BGP, IEGRP & OSPF), VPN technology support, VoIP communications and infrastructure, enterprise wireless, RADIUS services, enterprise DNS / DHCP and other various enterprise technologies and services Jr. Network engineer Sparta systems - IN April 2011 to November 2014 India Device integration, custom parser deployment and content development Responsible for mining, framing business rules and policies Install and configure servers, desktops and networking equipment. Managing Layer 2 switches of CISCO, VLAN configuration and assigning ports to specific VLAN as per requirement. Troubleshoot TCP/IP problems, troubleshoot connectivity issues. Handled Tech Support as it relates to LAN & WAN systems. Supporting and performing projects for the client WAN environment at a global level. Worked on installation, maintenance, and troubleshooting of LAN/WAN (ISDN, Frame relay, NAT, DHCP, TCP/IP, SMTP and HTTP). Installed operating systems, applications, service packs etc. Education Master's in Information Security and Intelligence Ferris State University - Grand Rapids, MI January 2015 to December 2016 Master's Skills CISCO (6 years), DHCP (4 years), FRAME RELAY (3 years), HTTP (3 years), ISDN (3 years) Additional Information Operating Systems: Microsoft XP/Vista/7, UNIX, Linux (Redhat, Fedora) Windows

Servers [2008 and 20012] Windows MS-Office. Technical Skills: Operating Systems: Windows (XP- 8.1), Windows Server (2008, 2012), Linux/Unix familiarity (CLI skills) Routers/Switches: Cisco 1600, 1700, 1800, 2500, 2600, 3600, 4000, 6000, 7206 Protocols: OSI, TCP/IP, DHCP, UDP, RIP v1, RIP v2, IGRP, EIGRP, OSPF, BGP, SSH, TFTP, FTP, HTTP, SMTP, NTP, LDAP, Active Directory, L2F, L2TP, PPP, Frame Relay, ATM, Fast/Gig Ethernet, HSRP, ISDN, AAA, DES, 3DES, AES, and MD5, VPN (IPsec and SSL), VRRP, HSRP, DNS, SNMP. SIEM Splunk, Qradar, Nessus Vulnerability scanner DLP Symantec & McAfee

Name: Timothy Lucas

Email: mitchellmatthew@example.org

Phone: 418.437.7112x5501