IT Security Analyst IT Security Analyst IT Security Analyst Atlanta, GA A CompTia SEC+ Certified Security Engineer with 4+ years of experience in vulnerability assessment, security event handling and security management strategies. Experience includes: Security orchestration and automation with McAfee EPO and Symantec in managing ENS/VSE SEP policies, DLP and Drive encryption standards. Endpoint Management Team managing software deployment using 2008/2012 Active Directory, Microsoft WSUS patching, anti-virus and endpoint protection using McAfee ePO and SCCM Creation and management of PC Build Images Win7 and application for PCI security policies. Used McAfee soft ware for protecting data, database security, emails and web security, endpoint protection, network security, and security management and event management (SIEM). Also, deployment of endpoint protection and managing email gateway policy security in maintaining malware, viruses and collected malware samples for the further analysis. Experienced in Installation and configuration of Splunk product upgrading version and Testing in different environments. Installation of Enterprise, Splunk forwarder, Splunk Indexer, Apps in multiple servers (Windows and Linux) with automation. Knowledge in designing AWS Cloud Formation templates to create custom sized VPC, subnets, NAT to ensure successful deployment of Web applications. Configured and prioritized policies of Palo Alto, Cisco ASA firewalls, McAfee ePO server and McAfee IPS/IDS. Developed low level design documentation (LLD) and network implementation documentation for clients. Configured and maintained proxy server policies with Websense V10000, V5000 (Forcepoint) such as URL Filtering, App ID filtering etc. Experienced in handling Windows (2003, 2008, 2012, 2016) and Linux servers vulnerabilities. Enforced web PKI infrastructure requirements by regular monitoring for certificate expirations and assisted concern SME in installing the latest certificates in regard to TLS/SSL protocol requirements thereby maintained users trust. Knowledge and experience in standard security policy development and regulatory frameworks including ISO 27001/31000, NIST 800-71, SANS, HIPPA and PCI DSS. Supported and helped mature the security risk management program. Familiar with general Governance, Risk and Compliance (GRC) programs with specific knowledge of vendor risk and policy management. Experienced with GRC tool in automating the PCI compliance process.

Experience in Security Information and Event Management Tools like Splunk, Logrthym and RSA. Work Experience IT Security Analyst Atlanta International Airport - Department of Aviation - Atlanta, GA July 2017 to May 2018 Manage McAfee ePO 5.9.1 and 5.3.1 A/V environment, using ePO console to pull reports to validate security protection compliance via DAT file updates and take appropriate action to correct issues found within the ePO environment. Handled out side by side migration of ENS/VSE and EPO 5.3.1 to EPO 5.9.1 and developed an architectural plan to deploy DLP and Drive Encryption products. Managed a Vulnerability Remediation Team (VRT) for reporting all the scan reports and guided them to fix the vulnerabilities and patches using the QID's, Bugtraq ID's and CVE ID's from knowledge base from vendors. Deployed and configured DLP policies for critical customer DB server, backup servers (Data-at-rest), imported dictionaries to enforce Data leakage throught the environment using Symantec DLP and enforced drive encryption rules wherever necessary using McAfee drive encryption. Responsible for working with Endpoint Management team to manage software deployment to PCs using 2008/2012 Active Directory, Microsoft WSUS patching, anti-virus and endpoint protection using McAfee ePO and SCCM Creation and management of PC Build Images Win7 and application for PCI security policies. Expertise in Installation, Configuration, Migration, Trouble-Shooting and Maintenance of Splunk, WebLogic Server [ ] Apache Web Server on different UNIX flavors like Linux and Solaris. Experience on Splunk Enterprise Deployments and enabled continuous integration on as part of configuration management. Experience with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management.

Handled out migration of application from WebLogic 7.x/8.x/9.x to successive Created and Managed splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Monitored Database Connection Health by using Splunk DB connect health dashboards. Used EPO to deploy Minerva, a 3rd party security application and can integrate ePO with any module or 3rd party compatible applications. Used ANSA patch manager for EPO to maintain patch management process of application updates such as Java updates, Wireshark, web browsers. Expertise in deployment and troubleshooting of Windows 2008 and 2012 R2 Domain

Controllers in Active Directory. Worked on Active Directory design and support (GPO s, AD Schema, OUs, LDAP, Sites Replication, etc.) and managing users, objects using identity manager. Manage enterprise security systems, identifying key security risks, reporting risks to management with recommendations for corrective action utilizing NIST frameworks. Worked on McAfee IPS (NS9300) in analyzing attack logs, new signature sets in designing the policies for antimalware and matched anomalies. Configured NTBA ports for active packet capturing and fed that back to McAfee IPS. Proofpoint server WGW / Email Gateway - Managed proxy health and deployment of white/black lists. Created and customized several rules settings for DLP policy, created a security admin group and notified the alerts. Implemented the encryption standards for PCI, HIPAA sensitive data while outbound emails using Proofpoint. Support Aviation Information System and Network and maintained HIPPA Confidentiality, Integrity via vulnerability scanning and testing for OWASP Top Ten Application/Infrastructure Security vulnerabilities. Managed to secure the devices across entire network by using the Threat Protect Module from Rapid7. Measured the level of Severity of devices to fix the issues arising from them by providing solutions. Configured policies in Cisco ISE for different nodes based on our organizational rules including BYOD devices and implemented posture compliance component to check for AV and its Latest DAT policies. Provided necessary designs and implemented security solutions for egress/ingress points using the McAfee IPS/IDSNS sensors across the networks to provide better incident handling and event monitoring Network Security Engineer 3D Infovision Inc - Charlotte, NC September 2016 to June 2017 McAfee EPO 5.1 deployment of endpoint protection and managed email gateway policies security in maintaining malware, viruses and collected malware samples for the further analysis. Attended McAfee monthly SAM meeting reviewing tickets and discussing upgrades of McAfee products. Configured application, content filtering for restricting sites based on organizational policies using PA3060 firewall. Built Site to Site IPsec based VPN Tunnels between various client and business partner sites using Palo Alto firewalls. Experienced in McAfee Nitro SIEM in analyzing the internal alerts and configured SNMP traps to collect Syslog Opened, assigned and closed security tickets assigned in SOC Security Management Console towards Qualys for various

Remediation Process and Patch Management Process. Conducted Assessment and Authorization (A&A), Certification and Accreditation (C&A) IT Security Compliance using GRC tool for clients. Developed low level design documentation (LLD) & network implementation documentation for clients. Experienced in content-based Web Filtering Applications, HTTPS inspection and threat analyzation using Cisco IPS. Experienced configuring AAA using RADIUS, TACACS+ and Active directory protocols for distinct requirements. Performed patch management audit of over 1000+ devices. Network Engineer Jet Broadband Internet Providers Pvt ltd January 2013 to December 2014 Configured Cisco routers for provisioning E1/E3 links. Deployed Inter VLAN routing, SSL, IPSEC VPN, HSRP/VRRP on Cisco routers and switches. Established routing protocol such as BGP, EIGRP, OSPF, RIP on CISCO (1800, 2800, 3500 and 3850 series) and redistributed over different networks. Monitoring, and optimizing, problem resolution, root cause analysis, and managing all aspects of access to specified systems. Managed Active Directories Domain Controllers, DNS and DHCP Servers and Group policy for User Drive Mappings. Used McAfee soft wares for protecting data, database security, emails and web security, endpoint protection, network security, and also security management and event management (SIEM). Designed and Implemented Overlay Network Management Network to manage all our Production Devices with Syslog, Cisco Secure ACS, TACACS+ and SolarWinds NPM. Leads the resolution process for complex problems where analysis of situations or data requires an in-depth evaluation of various factors. Exercises judgment within broadly defined practices and policies in selecting methods, techniques, and evaluation criterion for obtaining results Education Master's in Electrical Engineering University of South Florida - Tampa, FL December 2016 Bachelors in Electronics & Communication Engineering Anna University - Chennai, Tamil Nadu Skills It Security, Cyber Security, Information Security, SEC

Name: Gary Perkins

Email: ann31@example.net

Phone: 001-332-644-9913x1465