SR. PENETRATION TESTER SR. PENETRATION TESTER Sr. Security Operations/Penetration Tester - CON EDISON, INC New York, NY Experienced in Vulnerability management and remediation. Scanning the network and provide the scan reports to operational teams. Mitigate vulnerabilities identified in Security scans. Expert in Identifying and evaluating risks during review and analysis of System Development Life Cycle (SDLC), including design, testing/QA, and implementation of systems and upgrades. Expert in preparing audit scopes, reported findings, and presented recommendations for improving data integrity and operations. Skilled in conducting reviews of data centers, extranets, telecommunications, and intranets to assess controls and ensure availability, accuracy, and security under all conditions. Performed checks to ensure that the audits are performed accurately in allocated time frame. Good understanding of Incident Response and Forensic investigation on volatile memory, hard drives and cloud storage. Understanding of Incident response policies and guidelines, REACT principle, Policy enforcement, Malware analysis and Incident recovery. Skilled in using Access Data FTK software's, volatility and Encase in analysing and presenting it in a proper documentation. Worked on McAfee VSE product for Stop worms, spyware, and viruses, get high-performance security, Lessen damage from outbreaks. Having Strong understanding of DLP Architecture. Experienced in performing automation on AWS and Google Cloud instances of a Three tier structure through Ansible playbooks. Configured a load balancer to divert traffic to different webserver's, and securing Apache and SSH through playbooks. Designed a backup database slave server which saves any data manipulation from the master database via the playbook. Designed IP tables playbook to restrict unknown connection reaching out the webservers. Experience in creating and deploying Docker containers. Manage and perform Nessus and Nmap scans before all production releases and analyse vulnerabilities and report to all stakeholders. Performs vulnerability assessments and penetration testing using automated tools on web applications. Examine assets to determine if vulnerabilities exist and if vulnerabilities are found proposes remediation strategies that can be applied to mitigate them. Implemented security fundamentals like SANS top 25. Perform remediation activities for Applications, OS, Database, Middleware, Digital Certificate, Layer

Products, Java. Identify issues on sessions management, Input validations, output encoding, Logging Exceptions, Cookie attributes, Encryption, Privilege escalations. Proactively identified system vulnerabilities to reduce or eliminate potential exploitation using Nessus Security Center and Passive Vulnerability Scanning. Assist in vulnerability remediation efforts across various projects by proposing remediation strategies and engaging key stakeholders utilizing Plan of Actions and Milestones. Experienced in using Microsoft System Center 2016 Endpoint Protection and System Center Configuration Manager for blocking virus, worms via emails or documents and lessen damage from the outbreaks. Skilled in creating and managing security policies for firewalls, software hardening, policies implementation, prioritization, and deployment. Experience related to advance threat protection, firewall policy administration, network profiling and device health monitoring. Experience with industry recognised SIEM (Security Information and Event Management) solutions such as SNORT, Splunk, Log Rhythm and many other tools. Worked on McAfee HIPS product for Get the broadest IPS coverage, Safeguard against malicious threats, Get automatic security updates, Protection around the clock. Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and prioritising them based on the criticality. Performed Symantec DLP environments management and support configuration as well as data security environments used in testing and configuring client sites prior to installation. Strong knowledge and experience in Symantec DLP workflow & architecture. Good Experience into Handling DLP False positive tickets. Implemented Symantec DATA Loss prevention to secure all end points. Configured and instrumented Symantec management console, Symantec management server and Symantec database on Oracle. Experienced in using Symantec DLP monitored the transmission of confidential data contained in corporate emails that were sent using Microsoft Exchange and downloaded to mobile devices. Assisted in monitoring and setting policies in EPO server, maintain updates on HBSS server, domain servers, and domain workstations, push McAfee policies to required computers, and Symantec to servers. Expert level understanding of ArcSight Implementation & its Integration with other N/W devices and Applications and the troubleshooting work. Expert Understanding to develop the complex Use Cases, Universal device support

Modules on the ArcSight SIEM. Integration of different devices/applications/databases/operating systems with ArcSight SIEM. Performed task related to cleaning up log auto-discovered sources in ArcSight by identifying duplicates, correcting misidentified log sources, and identifying log sources from their logs. Experience in editing building blocks to reduce the number of false positives that are generated by ArcSight and writing co-relation rules. Expert in installing SPLUNK logging application for a distributed environment. Experience in Automated and Manual Penetration Testing, Contractor Assessments, Source Code Review, Controls Assessment. Software Development of Customs Compliance Modules, Attacks, and Exploitation for Nessus and Metasploit. Worked on a multi-vendor platform with the checkpoint, Fortinet and Cisco firewalls requesting net flow for security compliance, coding, and pushing firewall rules after approval and troubleshoot incidents as required. Secure Email Gateway, Web-Marshal proxy gateway and Secure Connect Fortinet Firewalls. Strong understanding of Security Information and Event Management Solutions (SIEM) to analyse and modify the existing SIEM solution and implemented QRadar SIEM. Skilled in Identifying security attacks using IBM QRadar SIEM and by proposing remediation or preventive actions after analysis implemented QRadar in the organisation. Skilled in Monitoring Critical assets like IBM QRadar, PIM, DLP, and DAM analysing them. Expert in Installation of Connectors and Integration of multi-platform devices with IBM QRadar. Experience in Integration of IDS/IPS to IBM QRadar and analyse the logs to filter out False positives and add False negatives into IDS/IPS rule set. Extensive knowledge of security controls (ISO/27002, NIST 800-53) used to implement regulatory compliance (NERC CIP, PCI, SOX, HIPAA) with IBM QRadar products. Review and updating System Security Plan (SSP) based on findings from Assessing controls using NIST SP 800-18 rev1, NIST SP 800-53a rev4, and NIST SP 800-53. Experience with Risk assessment using Industry standards like HIPPA, PCI/DSS and develop Security policy as per these standards. Actively pursued abnormal activity on assets that may be signs of compromise. Experience with industry recognised SIEM (Security Information and Event Management) solutions such as SNORT, Splunk, Log Rhythm and many other tools. Antivirus McAfee Virus Scan Enterprise, Symantec, Endpoint Protection Suite Conducts vulnerability scans

and penetration tests to meet PCI requirements. Solid understanding of RSA authentication and Rapid 7 technologies Perform vulnerability, configuration and compliance scan with Rapid7 to detect deficiencies and validate compliance with information systems configuration with the organisation's policies and standards. Experience in supporting, operation and troubleshooting the problems. Written Nmap scanner and multithreaded python program to brute-force an FTP server using a password file. Authorized to work in the US for any employer Work Experience SR. PENETRATION TESTER CON EDISON, INC - New York, NY September 2018 to Present Responsibilities: Executed daily vulnerability assessments, threat assessment, mitigation and reporting activities to safeguard information assets and ensure protection has been put in place on the systems. Actively monitored and responded to activity impacting various enterprise endpoints facilitating network communication and data handling (McAfee End Point Security, DLP, Splunk). Gather testing tools and methodologies and perform step by step Penetration testing by enumerating information. Good Experience in Metasploit Framework and Social Engineering. Involved in standardising Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms. Conduct Malware analysis and investigate behavioural characteristics of each incident utilising IDS monitoring tools. Experienced with McAfee ePO, Nitro, Web gateway, DLP, Bluecoat Websense, ForcePoint, Proofpoint, Trend Micro, Nexpose (Rapid7) and Splunk Enterprise SIEM security tools to monitor network environment. Monitor and investigate SOC incidents and alerts with McAfee EPO. Good experience in working security management tool McAfee ePolicy Orchestrator (ePO) console and deploying the McAfee agents on the client side. Managing End Point Encryption and Infrastructure using MacAfee EPO. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Performed wireless pen testing using Air cracking and analysed the network using Wireshark. Found network vulnerabilities using Nexpose and analysed web application using HP Fortify. Experience on vulnerability assessment and penetration testing using various tools like BurpSuite, DirBuster, OWASP ZAP Proxy, NMap, Kali Linux, and Metasploit. Experienced in working with Splunk authentication and permissions and having significant experience in supporting large scale Splunk

deployments. Responsibility for policy configuration for all the McAfee components and the same is deployed to the clients. Proficient in Penetration testing based on OWASP Top 10 vulnerabilities like XSS, SQL injection, CSRF, Source code review assessment. Managed security incidents resulting from Splunk and third-party alerts, including investigation and remediation. Administer and maintain corporate DLP environments while structuring and documenting the corporate DLP infrastructure environments. Managed security incidents resulting from Splunk and third-party alerts, including investigation and remediation. Performed Symantec DLP environments management and support configuration as well as data security environments used in testing and configuring client sites prior to installation. Experience on vulnerability assessment and penetration testing using various DAST & SAST tools like BurpSuite, DirBuster, NMap, Nessus, IBM App Scan, Kali Linux. Used McAfee ePolicy Orchestrator to monitor and identify potential intrusions and attacks for the Security Operations Center (SOC). Managed security incidents resulting from Splunk and third-party alerts, including investigation and remediation. Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures. Internal, External, White box, Black box, Grey box penetration testing. CYBER SECURITY ANALYST (INTERN) Marsh - Houston, TX April 2018 to August 2018 Responsibilities: Designing architecture, implementation and Troubleshooting Cyber Security solutions like MacAfee, HP ARC SIGHT SIEM, IBM Q Radar and Splunk Solution. Conducted onsite penetration tests from an insider threat perspective. Migration of Data Center and Perimeter Security technologies to Cloud security Technologies. Designing architecture, implementation and Troubleshooting Vulnerability Assessment and Penetration testing solutions using Nessus, Nmap and Qualys. Performed host, network, and web application penetration tests.

Maintain McAfee ePO environment in optimum performance and compliance standards. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Documentation regarding DLP administration, scanning, reporting, and remediation. Analysis of Offenses created based on vulnerability management tools such as Rapid7 Developed Black Box Security test environments & conducted tests as part of the team for precautionary

measures. Developed approaches for industry-specific threat analyses, application-specific penetration tests and the generation of vulnerability reports. Responsibility for policy configuration for all the McAfee components and the same is deployed to the clients. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Performed risk assessments to ensure corporate compliance. Symantec DLP and RSA DLP architecture and implementation for enterprise level companies. Developed detailed remediation reports and recommendations for compliance and security improvements across industries based on changing threats. Troubleshooting issues related to McAfee ePO servers (5.x), VSE 8.x and HIPS. Performed Vulnerability Assessments and Data Classification and their impacts. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Performed application security and penetration testing using IBM AppScan. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Managing Security tools DLP, SIEM, Vulnerability scanner and Penetrations test. Perform automated and manual security assessments to identify configuration and patch related vulnerabilities using commercial and open source tools. Configuration, troubleshooting, and management of Websense Data Security (DLP). Monitoring McAfee dashboard for updated DAT versions in all the client. IT SECURITY ANALYST RECKISTER INFOTECH - Delhi, Delhi January 2014 to July 2017 Responsibilities: Testing, troubleshooting, level II support, documentation, training and technical expertise are services provided. Risk Assessment using Cyber Security Frameworks like NIST, OCTAVE, GLBA Assisted Lead Auditors in Audit data collection and Documentation. Created checklists and collected audit data for compliance with SOX and PCI certifications Installed, configured, and updated Linux machines, with Red Hat and CentOS. Won two quarterly awards for my willingness and ability to work outside my speciality and assist other departments. Resolved security vulnerabilities by analysing and recommending improvements in communications and network security at the component level Ensured business continuity by designing, implementing and testing disaster recovery systems Created checklists and collected audit data for compliance with SOX and PCI certifications Developed, implemented and verified security policy and access

management compliance Monitored system performance and prevented resource exhaustion using ssh, sar, vmstat, iostat, netstat and nmon. Managed, monitored and tested individual and group user access privileges and security Reviewed LAD configuration and Managed daily activities to include user support and system administration tasks Analyse Pre-Implementation network documents for Firewall requests, SEC- ACLs and AppSense requests. Given Information Security oversight and guidance to businesses needing 3rd party connectivity as it relates to the company's Information Security Standards and IS Policies. Liaise with business and multiple technology teams (i.e. CATE Network Engineering; Proxy OPs and Integration; Perimeter Security Ops; System Based Computing; Remote Access Services and Business Information Security Officers; AppSense Implementers); to facilitate cross-functional solutions as it relates to 3rd party connectivity aligning with Company's Information Security Standards. Investigated alleged non-compliance issues and audited and monitored vital activities. Used Security tool like AlgoSec Firewall Analyzer, NetFlow, IDS, and IPS for analysis. Education Cybersecurity and Forensics Sacred Heart University - Fairfield, CT September 2017 to December 2018 Skills Penetration Testing, Forensic, CEH Additional Information Technical Skills Tools: Kali Linux, Parrot Linux, Tableau, Lotus Notes, ERP - SAP, Visio, QlikView, Oracle, Identity and access management Security Web Applications: TCP/IP OWASP, Nessus, Grabber, Zed Attack, Skipfish Hydra, Firewall, IDS, IPS, Acunetix, Arachni. Languages and Database: SQL, Java, C++, Visual Basic, Javascript, JSON, Python, Bro, ASP.NET MVC, PowerShell, PowerBI, STIX, Bash Scripting Automation: Ansible, Docker and Kubernetes Forensics: FTK Imager, Registry viewer, Volatility, Encase Networking & Frameworks: DNS, DHCP, SSO, SAML, NAT, PCI-DSS Continuous Monitoring: Vulnerability Management, Web Application Scanning, ThreatProtect, Cloud Agents, Asset Management, Sourcefire, Nexpose, Forcepoint, Rapid7, Netparker, OPENVas Event Management: RSA Archer, Blue Coat Proxy, Splunk, NetWitness, LogRhythm, HP ArcSight PenTest Tools: Metasploit, NMAP, Wireshark, Routersploit and Kali Security Software: Nessus, Ethereal, Nmap, Metasploit, PFsense, Snort, RSA Authentication, Frameworks: NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS Other: GitHub, Bitbucket, JIRA.

Name: Kevin Thornton

Email: ruth16@example.net

Phone: 553.345.3399