# **Arun Kumar| Sr. IT Security Engineer**

**Kmrarn777@gmail.com**

**9378154902**

**Professional Summary:**

* Overall 6+ years of experience as Security Engineer and Vulnerability Management Engineer.
* Have good experience in Vulnerability Scanners i.e., Tenable Nessus, Qualys, Rapid 7 Nexpose and InsightVM
* Utliized Forescout to identify and track endpoints on a granular level, providing many means for locating virtual and physical devices, including authorized devices.
* Responsible for managing all aspects of the Vulnerability Risk Management Program including vulnerability identification, analysis, remediation coordination and reporting.
* Experience with Risk Assessment on systems, applications and Active Directory.
* Experience with Network, Windows/Linux OS, Database Policy Compliance and configuration with CIS benchmarks
* Strong experience of Vulnerability Management and Assessment Process with NESSUS and Qualys. Used NESSUS and Qualys for scanning network & host, writing Policies, generating, and analyzing report.
* Experience in conducting IT Security Risk Assessments in accordance to NIST and FFIEC framework
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice,
* Regulatory requirements and ISO 27001
* Good understanding of PCI DSS compliance, PKI and Cryptographic Protocols.
* Experience in Qualys Modelling, VMDR, PC, RTI, WAS, MD during Requirement gathering and Design phases.
* Used Splunk & IBM QRadar Security Manager, Event processor, Flow Processor to identify threats and assigned category.
* Have good experience on Log management, log integration, use-case creation, correlational rule creations, report generations and creating custom dashboards.
* Monitored and researched Cyber Threats with a direct & indirect impact to the organization internally.
* Experience with IT - Governance (GRC) risk tool Digital Manager 360 (Modulo) and reporting tool Nexpose and Qualys.
* Progressive experience in Enterprise Vulnerability Management, Risk Assessment, penetration testing, generating reports, SQL Injection XSS and major hacking protection techniques.
* Experience in testing using various tools like Burp Suite, DirBuster, Nmap, OpenVAS, Nexpose, Qualys, Nessus, HP Fortify, HP Web inspect, Confidential Appscan enterprise, Kali Linux, Metasploit
* Good knowledge on OWASP Top 10 based Vulnerability assessment of web applications.
* Involved in Security Development Life Cycle (SDLC) to ensure security controls are in place.
* Having good experience SAST and DAST applications using different tools HP Fortify and Confidential Appscan.
* Knowledge in detecting vulnerabilities over authentication, authorization, input validation, session management, security misconfiguration, insecure direct object reference, sensitive data exposure, Functional level access control and Invalidated redirects.
* Accomplished history with working with various private businesses and IT organizations to facilitate security architecture in order to further enhance the security stance of the company.
* Coordinate with dev team to report vulnerabilities by explaining the exploitation and the impact of the issue
* Reporting the identified issues in the industry standard framework.
* Experience with Security Risk Management with TCP-based networking.
* Exhibited problem solving when analyzing system designs to identify potential information security risks.
* Experience with threat and vulnerability management tools that include and commercial and open source.

**Technical Skills:**

* SIEM/SOAR, Vulnerability Management, Firewalls, Baseline Hardening, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management, Security Audits and Compliance.
* **CYBER SECURITY SOLUTION**: FireEye CMS, NX, EX, HX, IA, PX, Sourcefire IPS, Wildfire IPS
* **E-MAIL SECURITY:** FireEye email security (EX series), Proofpoint, O365, Cisco Iron Port
* **SECURITY TOOLS:** ZAP, Nikto, Metasploit, Burpsuite, IBM Appscan, Veracode, HP Foritfy
* **NETWORK PROXY:** Websense & Zscaler
* **EVENT MANAGEMENT**: Sumologic, Forescout, RSA Archer, ArcSight, Splunk, QRadar, Log Rythm
* **SECURITY AUDITS AND FRAMEWORKS:** HITRUST CSF, NIST SP 800 - 30/800-53ISO-27001, PCI - DSS
* **PROTOCOLS:** TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS
* **Networking:** NetFlow integrator, Wireshark, SolarWinds, TCP-Dump, LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Firewalls/IPS/IDS

**Professional Experience:**

**MIW/ATT Redmond, WA**

**Sr. IT Security Analyst**  **Jan 2022 - till date**

* Analyze Vulnerabilities reports from various scans and assessments by acting on high risk / critical Vulnerabilities to other Vulnerabilities by using Tenable Nessus, Tenable IO.
* Management of system security and file system security policies and analyzing systems to determine ways of improving performance
* Conducting routine checks, warranty claims, hardware failure, replacement, software up-gradation, download patches and hotfixes.
* Coordinate and manage team activities during assessment engagements
* Establish schedules and deadlines for assessment activities
* Monitor controls post authorization to ensure continuous compliance with the security requirements
* Update the controls changes from NIST-800 53 rev 3 to NIST-800 53 rev 4 and control assessment changes from NIST-800 53A to NIST 53A rev4
* Configuring rules and Maintaining Palo Alto Firewalls & Analysis of firewall logs using various tools.
* Palo Alto installation, configuration, administration, monitoring and implementing the policies.
* Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering).
* Design and Implementation of Bluecoat Proxy Infrastructure. Upgrading Radware Appwall WAF (Web application firewall) and fixing hot fixes and patches.
* Prioritize vulnerabilities/assets from Tenable Nessus and Tenable IO that should be patched during maintenance cycles
* Used automated Vulnerability assessment tools such as Nessus and Tenable IO.
* Monitoring and remediating daily security alerts generated by end users with the tools like Intel/McAfee SIEM, Force Points Websense, and Intel/McAfee EPO and also responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Working on SIEM, Threat and Vulnerability management
* Performing vulnerability assessment using Nessus and Tenable IO
* Experience analyzing Symantec DLP events and reports.
* Experience with Red hat Linux Server, macOS Server, Microsoft Windows Server, MS Active Directory, Azure AD, Configure and manage AWS/Azure Cloud Infrastructure, Virtualization (VMware NSX, Hyper-V).
* Extensive experience hands-on Azure IaaS / PaaS. Experience designing and building Azure solutions. PowerShell experience as it relates to Azure, AD, and Office 365.
* Assist management in authorizing the IT Systems for operation on the and basis of whether the residual risk is at an acceptable level or whether additional compensating controls should be implemented.
* Used ForeScout to create lists of devices imported from a thirdparty source, such as LDAP server to determine which authorized devices are disconnected from the network at given time.
* plans, training and testing were executed appropriately and discuss lessons learnt.
* Coordinate with system owners and ISSOs across the organization to ensure timely compliance.
* Creating the reports based on operating systems and vulnerabilities provide the reports to concern technical team.
* Performs Tenable IO and Nessus scans of new and existing servers and PC’s to determine what vulnerabilities present a threat to the network and require remediation.
* Ensured system vulnerabilities were corrected, patched, and updated.
* Involved and responsible for deep packet inspection with experience of Wireshark, SolarWinds and Tcpdump.
* Comprehensive knowledge in ITSM ticketing tools such as ServiceNow and JIRA Service Desk.
* Maintaining network security, firewalls, kemp, DMZ and blocking internal/externals risks using Symantec Endpoint Protection Manager.
* Maintaining inventory of Disaster Recovery Data Tapes sent to offsite storage.
* Conduct and perform passive application assessments and maintain assessment platforms.
* Window Server, Active Directory, Microsoft Exchange, Rapid and Lotus Notes admin.
* Improving Services - Incident management, change and problem management.

**Cisco Systems, Inc. Raleigh, NC**

**Senior Security Engineer Mar 2021 – Dec 2021**

* Used automated Vulnerability assessment tools such as Qualys Guard and Tenable IO.
* Installed and integrated cloud agents to sync with cloud portals for real time visibility of vulnerabilities and installed programs and processes
* Prioritize vulnerabilities/assets from Qualys Guard and Tenable IO that should be patched during maintenance cycles
* Ensure vulnerabilities are identified as early as possible and mitigated, execute, troubleshoot, and diagnose patching efforts.
* Using Tenable IO to perform Policy hardening scans on Network /Servers /endpoints /database /webservers using CIS benchmarks, and maintained regular cadence in running scans and publishing reports to leadership
* Utilizing Qualys WAS module to perform multiple Web application scans against OWASP Top10 vulnerabilities and working with dev teams in driving remediations.
* Reviewing & monitoring on daily basis and remediating daily security alerts in SIEM generated by end users with the tools like endpoints, servers, Firewalls Forcepoint Websense, and Intel/McAfee EPO and also responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Working on SIEM, Threat Intel (TAXII & STIX feed), Usecases, log integrations from various remote collectors/devices.
* Worked on replacing Checkpoint VPN and Bluecoat Proxy with ZScaler.
* Provided support for Zscaler Web Security Service.
* Worked on troubleshooting firewall rules in Cisco ASA, Checkpoint and Zscaler.
* Responded to Health Care Client Security questionnaires, assessments, collected documents and data for request for information (RFI)
* Executed Security risk assessments on Providers, Partners, and Vendors including a reviewing their Security questionnaire responses.
* Design and Implementation of Websense Proxy Infrastructure. Upgrading Cloudflare WAF (Web application firewall) and fixing hot fixes and patches.
* Provide technical and non-technical audits, risk analyses, and document compliance and/or noncompliance based on findings.
* Worked with Websense Proxy to safeguard network resources, define rules for custom filters and provide real time security updates.
* Experience with Websense filtering service for selectively filtering unwanted internet requests traffic
* Oversees, evaluates and matures the intelligence of data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within the IBM environments (on-premise and cloud) for the purposes of mitigating threats.
* Supported company business objectives to implement HITRUST CSF as a single benchmark to facilitate internal and external security controls measurements that meet requirements of NIST, ISO, PCI, HIPAA, HITECH and COBIT.
* Deploy, manage and effectively maintain security systems and their corresponding or associated software, including firewalls, checkpoint firewall, squid firewall, blue coat proxy and routers, IDS, IPS, cryptography systems, Encryption (RSA, AES), Tokenization (OpenNMT), and anti-virus software.
* Performed HITRUST CSF self-risk assessment and scoring of organizations Policies, Procedures, Implementation and in-scope systems in preparation for HITRUST CSF readiness validated assessment.
* Managed HITRUST CSF technical implementation of Confidential Security Policies, Procedures, and Implementation with multiple departments to correct GAPs identified during HITRUST CSF advisory assessment.
* Followed Security Incident Handling Policy and Procedures for conducting security incident investigations to collect details, document who, what, where, when, how and why, validate collected details, containment to stop or limit impact, restore and/or recover data/services/assets, and remediate to prevent recurrences.
* Web Application Penetration Testing, targeting applications to detect and exploit common vulnerabilities such as the OWASP top 10.
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools, SSL/TLS, SOAP/XML, TCP/IP, HTTP and expertise in open SSL. Moreover, Experience in deploying and administering Dynatrace, APM Tools like Synthetic, DCRUM, UEM, & AppMon.
* Perform Manual Vulnerability testing and static code analysis.

**ODOT Salem, OR**

**Security Engineer Mar 2019 – Feb 2021**

* Opened, Assigned and closed the tickets assigned in SOC Security Management Console towards Qualys for various Remediation Process and Patch Management Process.
* Experience on Network scanning and penetration testing using various web application security tools like Metasploit, OWASP ZAP Proxy, Nmap, Nessus.
* Knowledge of OWASP top 10 vulnerabilities, network and internet architecture, IDS-IPS.
* Deployed Cisco Fire Sight/Firepower appliance and Cisco ASA Firepower inline.
* Identifying OWASP Top 10 Issues identifications like SQL Injection, CSRF, Insecure Cryptographic Storage, XSS and Invalidated redirects and forwards etc.
* Prepared AD Splunk environment by Verifying that all of the domain controllers and DNS servers in the environment have the latest service packs and hot fixes installed
* Networked and hosted DLP monitoring and logging and created regex-based parser to parser logs and configuring different connectors
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools, SSL/TLS, SOAP/XML, TCP/IP, HTTP and expertise in open SSL. Moreover, Experience in deploying and administering Dynatrace, APM Tools like Synthetic, DCRUM, UEM, & AppMon.
* Troubleshoot escalated proxy issues to include Bluecoat and Zscaler.
* Worked on Zscaler Proxy and Content filtering and worked on enforcing security policies using Cisco ISE/NAC for Centralized Policy, Posture Assessment, Guest Access Services and Device Profiling.
* In-depth study and investigation of Governance Risk and Compliance including a deep dive into the NIST Risk Management Framework, FISMA, FedRAMP, GDPR and CCPA, ISO-PCI DSS, GDPR, UCF CCH, Cloud Security Alliance CCM, SOX, ISO 27001, Microsoft SDL, CIS 20 Controls and other legal aspects associated with GRC
* Configuration of SPLUNK data inputs by understanding various parsing parameters like Index, source, source typing, queue sizes, index sizes, index locations, read/write timeout values, line breaks, event breaks and time formats during index-time.
* Migration of Splunk clusters in various AWS accounts to single AWS account rehydration of Splunk cluster on AWS environment.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Worked on Splunk ES to build the correlation searches, alerts, reports and dashboards to get specific monitoring.
* Integrated the data from SAP to ServiceNow by using API, Web services and captured that data in Service Now by creating a table.
* Used automated Vulnerability assessment tools such as Nessus, Nexpose.
* Implementation of name resolution using WINS & DNS in TCP/IP environment
* Worked using Perl CGI, python, Java Script, jQuery, Ajax and automating the test cases using python framework
* Actively used Splunk Phantom SOAR technology for searching and monitoring real time events for network security and compliance.
* Designed, developed, and implemented Maxim's Vulnerability Management Program which included the deployment and management of the Beyond Security Advanced Vulnerability Detection System AVDS .
* Performed vulnerability assessments, penetration tests, and security audits, produced reports of findings, and worked cooperatively with engineers to implement remedial measures.
* Participated in the creation of IT security policies, procedures, guidelines, baselines, and standards.
* Recommended security solutions and processes to improve overall company security.
* Central Point of Contact for the configuration, integration, and deploymentof all new or improved security solutions and processes in accordance with standard best practices and the company's security policies.
* Maxim contact for responding to customer and other third-party inquiries regarding the company's security posture.
* Responsible for maintaining up-to-date baselines for the secure configuration and operation of all existing devices, both under direct control e.g. security tools or under Operations control e.g. workstations, servers, and network devices.
* Administrative expertise with Windows Server 2012/2016 and RedHat Linux 7 environments.
* Track and provide metrics on vulnerabilities and remediation.
* Patch Linux systems (e.g. Ubuntu, Oracle Linux, RHEL, SuSE, Debian) within on-prem and cloud environments. Patch Windows systems within on-prem and cloud environments.
* Understanding of VMware Infrastructure and Patch Management of ESX/i hosts.
* Experience patching Window systems using SCCM and 3rd party patching tools.
* Responsible for the planning, building, testing and deploying the patches to all the non-production and work with asset owners for production systems.
* Help members on the team through patching lifecycle.
* Provide technical assistance to owners of the impacted systems and applications to remediate and mitigate vulnerabilities.

**Centene St. Louis, MO**

**Security Engineer Oct 2016 – May 2019**

* Regularly maintain systems and procedures and effectively assess the information risk.
* Support customer business partners to understand IT security risks, standards, and best practices.
* Provide engineering support for Raytheon Technologies Managed SOC Services infrastructure and client tools focused on integration of RSA Archer Suite integrated risk platform
* Administrative expertise with Windows Server 2012/2016 and RedHat Linux 7 environments.
* Track and provide metrics on vulnerabilities and remediation.
* Patch Linux systems (e.g. Ubuntu, Oracle Linux, RHEL, SuSE, Debian) within on-prem and cloud environments. Patch Windows systems within on-prem and cloud environments.
* Understanding of VMware Infrastructure and Patch Management of ESX/i hosts.
* Experience patching Window systems using SCCM and 3rd party patching tools.
* Mitigating issues related to spam and relaying in Exchange server
* Analyze disclosed vulnerabilities, threat scenarios, and mitigating controls.
* Research and evaluate threats and vulnerabilities to assist in prioritization of remediation actions.
* Review and validate vulnerabilities using available data sources, tools and identifying new data sources as needed.
* Advise stakeholders on appropriate remediation & mitigation solutions.
* Leverage creativity and influence to enhance the Vulnerability & Exposure Analysis program.
* Conduct Vulnerability Assessments using tools such as Nessus.
* Developed a correlated picture of what was occurring right now in an enterprise through integration of information from a variety of devices with QRadar SIEM tool, then normalizing and correlating the information to develop modules that provided real-time (or near real-time) reporting in SOC
* Responsible for notifying systems owners of potential events and remediation. Responsible for drafting and conducting daily briefings to customers
* Assisted in the redesign and implementation of the McAfee ePO for the production environment
* Security Audit, Budget Violation, Operational Violation, Best practice check in client AWS environment
* Writing automation scripts in python and bash
* Achieve security architecture compliance on requirements, including Sarbanes-Oxley, HIPAA/HITECH, global data privacy requirements, as well as state and federal regulations and Serve as SME, trusted advisor; provide advisory and consulting services as needed
* Responsible for the planning, building, testing and deploying the patches to all the non-production and work with asset owners for production systems.
* Help members on the team through patching lifecycle.
* Provide technical assistance to owners of the impacted systems and applications to remediate and mitigate vulnerabilities.
* Web Application Penetration Testing, targeting applications to detect and exploit common vulnerabilities such as the OWASP top 10
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools, SSL/TLS, SOAP/XML, TCP/IP, HTTP and expertise in open SSL. Moreover, Experience in deploying and administering Dynatrace, APM Tools like Synthetic, DCRUM, UEM, & AppMon.
* Perform Manual Vulnerability testing and static code analysis.

Education:

Masters in Computer Science Governor’s State University-2016