**Avinash Reddy**

+1(484) 433-2251

avinashreddy17390@gmail.com

**Summary:**

* 7+ years of experience in the vulnerability management, SIEM and SIRT
* Experienced with Vulnerability Scanning tools like Nexpose, Nessus and Qualys
* Implemented and Maintained SIEM infrastructure – Qradar, SPLUNK
* Experienced and proficient in performing Security Administration, setting up role based security, resource permission for the organization.
* Deployed multiple Threat management, security event and correlation monitoring, IDS and NAC devices for a SOC operation.
* Integrate the DLP solutions with the SIEM by writing dashboard templates, providing issue reports and proposing new features.
* Implemented Security Policies using ACL, Firewall, IPSEC, SSL, VPN, IPS/IDS, AAA (TACACS+ & RADIUS)
* Ensures the integrity through the performance of formal Risk Assessments, Policy and Governance, and internal Threat Analysis in regards to a SOC environment
* Developed and streamlined PKI architecture which included upgrading internal root to remediate vulnerabilities, and select vendor and processes for external SSL certificates.
* Security auditing and assessment using: Kali, Backtrack, Nessus, Metasploit, Nmap, Wireshark, Snort, tcpdump, and various additional security auditing tools
* Responsible for Web Application Vulnerability and Penetration testing activities with outsourced Approved Scanning Vendors (ASV's) to meet PCI DSS compliance requirements
* Expert level knowledge in troubleshooting commands and tools like Ping, Traceroute, Wiresharkand TCP dump
* Experience working with IP networking, networking protocols and understanding of security related technologies including encryption, IPsec, PKI, VPNs, firewalls, proxy services, DNS, electronic mail and access-lists.
* Provide root cause analysis and remediation techniques for management in regards to security incidents and governance documents
* Good knowledge of threats analysis and remediation efforts about Intrusion prevention, Intrusion Detection and penetrations
* Good Understand of OWSAP Top 10 and SANS vulnerabilities
* Knowledge of networking concepts - LAN/WAN, TCP/IP, Routing & Switching and OSI Layers
* Strong troubleshooting, reasoning and problem solving skills

**Skills:**

|  |  |
| --- | --- |
| **SIEM Tools** | QRadar, Splunk, |
| **Security / Vulnerability Tools** | Qualys, Nessus, Nexpose, Qradar Vulnerability Manager |
| **Compliance Requirements** | PCI, NIST SP800-53,53A, ISO 27001, HIPAA |
| **Networking Protocols** | TCP/IP, HTTP/HTTPS, SSH, SSL, DNS, SNMP |
| **Networking Tools** | Routers, Switches, Load balancers, Cisco VPN, NAC/NAP |
| **Ticketing Systems** | Service Now, Remedy, Heat, Clarify |
| **Scripting language** | PowerShell, bash |
| **Operating Systems** | Linux (kali Linux), red hat, Windows |

**Education details**

* Master of Science – Computer and Information systems Security (Wilmington University, DE)
* Bachelor of Technology (India)

**Certifications**

* Qualys Certified – Vulnerability management
* Cybrary CompTIA Security +
* CISSP Cybrary Certified

**Project Summary**

**Client: Wells Fargo, San Francisco, CA June 2016 – Till date**

**Role: Security Engineer/Analyst**

**Responsibilities:**

* Analyze and review data from SIEM - QRadar for suspicious activity and trigger alerts to the concerned teams.
* Created Splunk app for Enterprise Security to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics
* Monitors server and workstation scans from Rapid 7/Nexpose for vulnerabilities.
* Configured internal and external vulnerability assessments for all sites in Rapid7 Nexpose.
* Setup access and reports for multiple teams for their respective assets in Rapid7 Nexpose.
* Rolled back the broken SSL implementation and made recommendations for appropriate implementation
* Collaborates with other teams to troubleshoot and resolve network connectivity issueswith the help of  TCPDUMP and Wireshark to identify root causes of various types of network, systems, and application problems
* Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards
* Involvement in various web application security testing tools likeNexpose, Metasploit, Burp Suite, SQL map, OWASP ZAP Proxy, Acunetix, Nmap and HP Fortify
* Aggregate, correlate, and analyze log data from network devices, security devices and other key assets using Qradar
* Internal & external vulnerability assessments, compliance and best practice gap analysis, penetration testing with a focus on PCI DSS  and risk assessment
* Developing customized Shell scripts in order to install, manage, configure multiple instances of Splunk forwarders, indexers, search heads, deployment servers
* Implemented and maintained McAfee Endpoint Encryption system to protect computers.
* Designed and implement security strategies with CiscoIronPort and Palo Alto firewalls.
* Performs a GAP Analysis to identify organization's current controls, to remediate the missing PCI controls by developing processes, policies, and procedures to mitigate risk
* Involved in writing custom parser using regular expression to identify unknown log events and receded the unwanted noise during anomaly detection.
* Worked with IR team with Log collections, analysis, and forensic activities.

**Client: AIG, Camp hill, PA Aug 2015 - May 2016**

**Rule: Security Analyst**

**Responsibilities:**

* Part of a team managing SIEM and information security infrastructure security.
* Created SIEM dashboard for Qradar and reconciliation with Storage, Database Server, Workstation and Server and Network Devices
* Used Cisco IDS/IPS to correlates both SIEM and DLP for further scoring, analytics, and protection against internal and internal threats.
* Develop policies and procedures adherent to HIPAA,  PCI-DSS and NIST 800 series frameworks
* Created Rapid7 Nexpose monthly scans and reports used for SOX and IT General Controls (ITGCs) compliance.
* Perform vulnerability scans on the Rapid 7, Nexpose scanner for internal scans and remediated vulnerabilities by decommissioning assets and by performing normal Nexpose cleanup.
* Responsible for repository updates and all current daily updates, as well as any patching and upgrades to McAfee and EPO requiring research, testing and implementation.
* Monitored network environment for threats, intrusions, or misuse using Sourcefire/ /LogRhythm. (IDS/IPS/NGIPS/SIEM).
* Administered IDS / IPS to maximize network security, pushing and updating policies, and analyzing traffic
* Monitor and analyze data feeds of events and logs from firewalls, routers, and other network devices or host systems for security violations and identify vulnerabilities.
* Work closely with development teams to remediate application vulnerabilities detected through fortify tool.
* Coordinate with subject matter experts to resolve any security incidents and correlate threat assessment data as needed.
* Support in the detection, understanding and resolving information security incidents affecting information systems & the business.
* Research and recommend corrective actions to ensure information dissemination regarding targeted or potentially targeted attacks.

**Client: United Health Group Hyderabad, India May 2013 – Aug 2015**

**Role: Security Engineer**

**Responsibilities:**

* SIEM: Installs, assets, log activity, network activity, dashboard, patch, upgrade, firmware.
* Monitors the network traffic and maintain the records with the help of SPLUNK
* Administer, Maintain, and deploy IPS & VPN systems, and McAfee network based Data Loss Prevention (DLP) devices
* Managing Corporate and Client facing audit engagement to meet applicable standards and compliance initiatives (e.g. PCI DSS and SOX).
* Manages PCI Compliance Program for organization protecting cardholder data and executing the PCI-DSS Program Life Cycle
* Managed and maintained the IDS and IPS with McAfee and handled the security incidents related to IDS/IPS
* Troubleshot IDS/IPS output, analyzing events and complete tasks in a highly professional manner, monitored outages, security alerts, and network intrusions
* Developed and implemented detection methods using all SIEM resources (rules, reports, dashboards) and custom security events, custom applications, host groups, etc.
* Conducted dynamic and static analysis of web application using IBM AppScan and Web inspect.
* Conducted risk assessments regularly; ensures measures raised in assessments are implemented in accordance with risk profile.
* Performed security testing, analyze test results, document risk and recommends counter measures.
* Analyzed and reported management on current vulnerabilities and provide countermeasure recommendations
* Responsible for performing penetration testing all the way from planning, designing, executing and reporting.
* Used appropriate tools, techniques and conforming to agreed process standards and industry specific regulations.
* Created and maintained test ware (test cases, test scripts, test reports, test plans, etc.) to measure and improve the security of the application being scanned.

**Client: Access IT Solutions, Hyderabad, India Apr 2011 – Apr 2013**

**Role: Security Consultant**

**Responsibilities:**

* Monitor, Analyze and respond to security incidents in the infrastructure.
* Troubleshoot any security issues found in the infrastructure per the security standards and procedures.
* Good knowledge in handling Burp Suite for web application penetration tests.
* Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
* Actively used NMAP for port scanning and made sure only appropriate ports are in use.
* Actively researched on any security gaps that are beyond the ability of detection by any security scanner.
* Responsible for performing periodic Vulnerability assessment (VA) as per the security policy and standards.
* Involved in documenting all web applications and systems, audit data and ensuring compliance with legal and regulatory requirements.
* Conducted application penetration testing of 20+ business applications and compliance audits.

**Client: Berry9 IT Solutions-Hyderabad, India Jan 2010–Mar2011**

**System Engineer**

**Responsibilities**:

* Installation and Configuration of Linux systems like CENT OS, Red Hat and Windows Servers. Also involved in user account management.
* Actively involved in monitoring the server’s health status using different tools.
* Responsible for application support on Red Hat servers which included apache configurations
* Experience in Performance monitoring, usage and load the system.
* Provided port binding, port security and router redundancy through HSRP.
* Designed ACLs, VLANs, troubleshooting IP addressing issues and taking back up of the configurations on switches and routers.
* Created Perl and Shell scripts to automate administration tasks.
* RPM package installation & upgrade released by Red Hat in the repository
* Administration of client machines using SSH and FTP
* Supported for application upgrade and rollback, Start or Stop services in Linux Servers.