**Avinash Reddy**

+1(484) 433-2251

[avinashreddy17390@gmail.com](mailto:avinashreddy17390@gmail.com)

**Summary:**

* Over 6 years’ experience in IT Security Operations and implementation, integration & operation of **SIEM Qradar**, **Tripwire** and **Splunk.**
* Experienced with Vulnerability Scanning tools like **Nexpose, Nessus** and **Qualys**
* Implemented and Maintained **SIEM** infrastructure – **Qradar**, **SPLUNK**
* Hands on Experience on vulnerability assessment and penetration testing using various tools like **Burp Suite**, **SQL map**, **HP Web Inspect** and **IBM AppScan**
* Plan, implement and manage vulnerability scanner environment.
* Monitors server and workstation scans from **Rapid 7/Nexpose** for vulnerabilities.
* Responsible for **IBM Qradar SIEM** monitoring and configuration aligned to internal **PCI** and **SOX** controls
* Gathered, evaluated, and reported on multiple data sources, conducted investigations, and made recommendations for critical intelligence, , and security measures.
* Knowledge in Authentication, Endpoint Security, Internet Policy Enforcement, Firewalls, Web Content Filtering, Database Activity Monitoring (**DAM**), Data Loss Prevention **(DLP**) solutions
* Monitor and respond to network intrusions and vulnerability alerts raised by automated detection systems, internal and external reports and manual investigation, using tools such as : McAfee Network Security Manager (**IDS/IPS**), (**SIEM McAfee/Nitro**), and **McAfee ePO**.
* Hands on Experience in **Incidence Response**& Forensics- host-centric tools for **forensic** collection and analysis and host based **detection** and **prevention** suites.
* Experience with **NIST** standard on cyber security and incident handling (**800-53, 800-61**)
* Prepared Security Assessment and Authorization (**SA&A**) packages to ascertain that management, operational and technical security controls adhere to **NIST SP 800-53,37,61** standards
* Experienced with vulnerability assessment tool for monitoring and identifying critical vulnerabilities in network, applying patches, Security compliance scanning and risk management.
* Experienced in creating detailed remediation plans and risk mitigation strategies for vulnerabilities to be incorporated into agency procedures.
* Create documentation on specific remediation steps to close vulnerabilities or mitigate risk to acceptable levels.
* Good knowledge of threats analysis and remediation efforts about Intrusion prevention, Intrusion Detection and penetrations
* Good Understand of **OWASP 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, and Qradar Vulnerability Manager

**SAST/DAST:** App scan, Web inspect, Fortify

**Compliance Requirements:** PCI, NIST SP 800-53, 53A, 61, ISO 27001, HIPAA

**Networking Protocols :** TCP/IP, HTTP/HTTPS, SSH, SSL, DNS, SNMP

**Email Security Tools:** Barracuda-spam firewall, Guava-E-mail Filtering Service

**Threat Management:** Fire eye, MacAfee \_epos & Hips, Websense (URL filtering service)

**Reverse Engineering Tools:** Ollydbg, Immunity Debugger, Ida Pro

**Network Monitoring:** ScienceLogic, Solar winds (NPM, SAM)

**Patch Management:** Lumension-Prism Patch

**Certificate Monitoring:** Digi-cert

**Networking Tools:** Routers, Switches, Load balancers, Cisco VPN, NAC/NAP

**DLP:** Symantec

**DAM:** Guardium, Imperva

**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**
* **CompTIA Security +**
* **CISSP**

**Project Summary**

**Client: Michelin, Greenville, SC Nov 2017 – Till Date**

**Role: Security Analyst/ Engineer**

**Responsibilities:**

* Review, analyze, and correlate global, network/security incidents from multiple systems (i.e. **IBM QRadar, Nessus, Web Inspect**) to identify cyber threats and vulnerabilities
* Manages and conducts annual security assessments in addition to daily, monthly and quarterly requirements
* Monitored the enterprise network for intrusions, malware, and other anomalies. Analyzed log data utilizing several tools including **Firepower (Sourcefire),** and **Symantec Endpoint** Protection.
* Involvement in various web application security testing tools like **Nessus**, **Burp Suite**, **OWASP** and **HP Fortify**
* Develops, implements and maintains security and risk policies and procedures aligned with industry and **PCI** security compliance
* Apply knowledge of technical, analytical skills to ensure the confidentiality, integrity, and availability(**CIA**) of all information systems assets and ensure compliance with company policies, procedures, contractual, and regulatory requirements
* Perform development and maintenance activities for security applications and tools.
* Perform investigative research, analysis and troubleshooting to identify, resolve, and report highly complex security issues. May evaluate and monitor system or tool performance.
* Configure, implement, monitor, and support security software/systems that will help ensure compliance with regulatory, industry, and corporate policies and procedures. This includes but is not limited to **IDS/IPS** (Host/Network/Wireless), secure file transfer, **DLP**, full disk encryption, firewall rule assessments, log management/correlation, secure password storage/retrieval, application whitelisting, vulnerability management, threat hunting, etc.
* Identify and recommend potential areas where existing data security policies and procedures require change, or where a supplement is required to mitigate key security risks.
* Preparing and maintaining technical documentation for information security products and prepares standards and procedures for their administration and use.
* Implementing **Check Point** firewalls, monitoring **VPN** access, and filtering content.
* Troubleshot and resolved client communication problems, and firewall and **Check Point IPS** blocking problems
* Ensures IT disaster recovery plans are appropriately maintained, including investigation, planning, documentation, implementation, and revision of disaster recovery plans.
* Identifying potential intrusions and reporting any violations that occur.
* Monitors multiple logs across diverse platforms to uncover specific activities as they occur from platform to platform. Creates case studies and profiles with log information in support of security monitoring and account/data access
* Ensure remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.; Provide clear updates to management on vulnerabilities; Investigate, document, and report on status and emerging trends
* Maintain current knowledge on information security topics and their applicability program requirements.

**Client: Wells Fargo, San Francisco, CA June 2016 – Oct 2017**

**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 using continuous monitoring, alerting and analytics
* Work with tools like **Burp Suite**,  **Web inspect**, **Nessus**, **IBM AppScan** and **Check Marx** as part of the penetration testing, on daily basis to complete the assessments
* Responsible for **Check Point** and **Cisco** firewall administration across global networks.
* Implemented and maintained **McAfee**Endpoint Encryption system to protect computers.
* Identified new malware infections and removed those remotely using admin tools or by identifying the user and guiding them through a removal process using **SIRT** Procedures
* Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in **SOX** and **PCI** compliance requirements and understanding of **NIST** and **ISO** standards
* Maintain overall program compliance and audit readiness of agency information systems in accordance with PCI DSS,  MARS-E (FISMA) and other applicable regulatory requirements
* Perform Vulnerability assessment and policy compliance and **PCI** compliance using **IBM AppScan**
* Aggregate, correlate, and analyze log data from network devices, security devices and other key assets using **Qradar**
* Manages **PCI**Compliance Program for organization protecting cardholder data and executing the **PCI-DSS** Program Life Cycle.
* Performed day-to-day administration of **McAfee EPO 5.1** for maintenance of system policies, container maintenance, coordination of system maintenance and client upgrades for desktop environment
* Responsible for assisting various sites with troubleshooting and integrating all aspects of the **ePO5.3 suite** to include **HIPS**, Asset Baseline Monitor, AV, Rogue System detection, Policy Auditor.
* Configure and install **McAfee IPS** sensors, and **Cisco ASA** with Firepower Appliances.
* Designed, implemented and maintained wireless IDS/IPS system to monitor and Wireless LAN (WLAN) using **AirTight** Networks **WLAN IDS/IPS** system
* Experience to work with different kind of **F5** Load balancers.
* Performed troubleshooting on**McAfee**,**Cisco**firewalls and **FireEye** devices
* Knowledge and working exp of **LAN/WAN** networking concepts-- **TCP/IP, OSI** layer routing and switching, **OSI** Layer; and scripting languages

**Client: AIG, Camp hill, PA July 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
* Installed, configured and administered **IBM AppScan Enterprise**, including scan agent configuration, scan scheduling, troubleshooting of failed scans, user administration.
* Conduct requirements gathering with Data Security and security controls converting high level requirements into policies using our management tools.
* Responsible for troubleshooting issues in **ePolicy Orchestrator** such as **McAfee** Agent Handler Network issues
* 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.
* Responsible for creating **Qradar POC** and asset groups in Qualys as part of our increased asset visibility initiative
* 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 quarterly penetration test analysis against **Qualys** scan data and extensive vulnerability assessment analysis
* Responsible for configuring and updating **Qradar API** plugins for **Tenable Nessus**&**Qualys** Enterprise
* Responsible for updating SharePoint sites with up to date Line of Business surveys and contact list information
* Used **Cisco IDS/IPS** to correlates both **SIEM** for further scoring, analytics, and protection against internal and internal threats.
* Monitoring of security events in **epos, Tanium, Splunk, SIEM,** as well as other security feeds and handling them as per standard
* 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 2014**

**Role: Security Engineer**

**Responsibilities:**

* Provide information to **HIPAA** security officer/audit department of health care hospital area.
* Create and maintain any **HIPAA** related documentation concerning my area of responsibility and projects.
* **SIEM**: Installs, assets, log activity, network activity, dashboard, patch, upgrade, firmware.
* Monitors the network traffic and maintain the records with the help of **SPLUNK**
* Configuration of the IBM App scan tool to meet individual scanning requirements to test websites for vulnerabilities.
* Assist **HIPAA** Compliance Officer with any new rules and regulations from CMS.
* Reviewed source code and developed security filters within **IBM AppScan** for critical applications.
* Administer, Maintain, and deploy **IPS**&**VPN** systems, and **McAfee** network based Data Loss Prevention (**DLP**) devices.
* Institute and monitor management, operational, and technical controls that meet **HIPAA, SOC2,** and **ISO** standards
* Maintained environment and architected every solution to meet SOC and **HIPAA** compliance.
* With **HIPAA** Application Security Program (HASP), performing risk and compliance assessments for KPIT enterprise controls, application systems and supporting infrastructure components determining their compliance base with requirements specific to **HIPAA**, **SOX**, and **PCI**
* 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** .
* Perform vulnerability scanning and assist with compliance auditing to ensure customer networks conform to all relevant compliance standards, including **PCI-DSS, HIPAA** and **Sarbanes-Oxley**
* Conduct comprehensive Risk Management Framework (**RMF**), **HIPAA**, and **PCI DSS** compliance assessments and security audits.
* 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:**

* Manual Vulnerability Assessment and Penetration Testing on Web Applications, Web APIs and Desktop Applications.
* Identification of web application vulnerabilities using **Black box** and **White box** penetration testing approach,
* Vulnerability assessment using tools like **Burp Suite, Nmap, Wireshark** and **SQL Map**.
* Identification all the vulnerability details, comprehend the severity and its risk, recommendation of the vulnerability and its impact with references, subsequently enlisting them in to the final report.
* Interaction with clients to discuss, guide thoroughly the vulnerability and demonstration of the impact of the vulnerability with proof of concept.
* To find out new type of security bugs and register as vulnerability in the database and compose security research papers on it.
* Research in the area of web application security tools for improvement of the performance of the tools.

**Client: Berry9 IT Solutions-Hyderabad, India June 2010– Mar 2011**

**System Engineer**

**Responsibilities**:

* Worked with Unix/Linux systems to gain expertise and did **LAN/WAN** networking and actively involved in monitoring the server’s health status using different tools.
* Installed and implemented new programs, modules, servers, hardware, network equipment when necessary to upgrade, improve resource or increase compatibility
* Managed and tracked change control process of requirements and design changes. Documented the changes, issues and their impact on the system design and delivery.
* Involved in detail design, development, testing, conversions and modifications of the client as part of implementation.
* Developed, executed and documented test plans and test cases for unit test and end-to-end software integration.
* Designed **ACLs, VLANs**, troubleshooting **IP** addressing issues and taking back up of the configurations on switches and routers.
* Basic understanding of **SDLC** from the requirements phase all the way down the testing and deployment phase