Sowmith Reddy **(P): (P): 224-326-0427**

**(E):** [**sowmithreddy.infosec@gmail.com**](mailto:sowmithreddy.infosec@gmail.com)

**Career Objective**

A proven Risk and Security professional with vast experience in delivering quality results in a fast-paced, time-sensitive environment. Experienced and skilled in enhancing, operating and maintaining Information Security, Risk Management and Cyber programs.

**Professional Summary**

* Experienced in Vulnerability management and remediation.
* Scanning the network and provide the scan reports to operational teams.
* Hands on experience with Qualys Guard vulnerability management tool.
* Worked on McAfee VSE product for Stop worms, spyware, and viruses, get high-performance security, Lessen damage from outbreaks.
* Worked on McAfee HIPS product for Get the broadest IPS coverage, Safeguard against malicious threats, Get automatic security updates, Protection around the clock.
* Knowledge of IDS-IPS.
* SIEM monitoring and security event analysis for all critical servers and applications utilizing customized Splunk queries, network traffic analysis, and Symantec End Point Manager.
* Highly skilled in Splunk to build, configure and maintain different environments and in-depth knowledge of log analysis generated by various operating systems.
* Experience in supporting, operation and troubleshooting the problems.
* Diverse background with fast learning skills and creative analytical skills.
* Developed communication interpersonal skills, team coordination and versed with software processes.
* perform basic service request based on standard operating procedures, follow qualitysecurity process defined for the engagement.
* Experienced in Vulnerability management and remediation.
* Scanning the network and providing the scan reports to technical teams.
* Hands on experience with Qualys Guard vulnerability management tool.
* Strong grasp of TCP/IP and common Internet fundamentals such as DNS, DHCP, NTP, SMTP, HTTP, etc.
* Extensive knowledge of information security principles and practices, understanding of security protocols, standards and defense in depth.

**Technical skills**

**Qualys Continuous Monitoring:** Vulnerability Management, Web Application Scanning, ThreatProtect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance.

**Event Management**: RSA Archer, Blue Coat Proxy, Norse, Splunk, NTT Security, LogRhythm.

**PenTest Tools:** Metasploit, NMAP, Wireshark and Kali.

**Security Software:** Nessus, Qualys Guard, NMap, Metasploit, Snort, BASE.

**Frameworks:** NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS.

**Security Technologies:** WhiteHat Web Security, iDefence, NTT Security, LogRhythm., **McAfee** Nitro (SIEM), **McAfeeePO, McAfee Endpoint Protection** Suite

**Switches:** Cisco Catalyst VSS 1440 / 6513 / 6509 / 4900 / 3750-X / 2960.

**Routers:** Cisco Routers ASR 1002 / 7606 / 7304 / 7206 / 3945 / 2951 / 2600.

**Firewalls:** Check Point, ISA 2004/2006, Palo Alto PA 3000/5000.

**Networking: Conversant in LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Fiber, Firewalls/IPS/IDS.**

**Routing:** OSPF, EIGRP, BGP, RIP-2, PBR, Route Filtering, Redistribution, Summarization, Static Routing.

**Switching:** VLAN, VTP, STP, PVST+, RPVST+, Inter VLAN routing & Multi-Layer Switching, Multicast operations, Layer 3 Switches, Ether channels, Transparent Bridging.

**Protocols:** TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS.

**Hardware: Dell, HP, CISCO, IBM, SUN, CheckPoint, SonicWall, Barracuda Appliances, SOPHOS email appliances**

**Nexus:** Nexus 7010 / 5548 UP / 5020 / 2232 PP / 2248 TP / 1000 V.

**UCS:** Fabric Interconnect 6248/6120, IOM 2208/2204/2104, B200 M2, HP VC FLEX-10.

**ANS:** F5 BIG-IP LTM 6900/6400, Array APV 5200/2600/TMX 5000, Cisco CSM, CSS.

**VPN:** ASA 5520, Cisco Concentrator 3030, Nortel Contivity Extranet 1500.

**NMS:** NAM, Sniffer, Solarwinds NPM, Cisco Secure ACS 5.2, CiscoWorks.

**Operating Systems:** Windows, NT, Windows 98/XP/2000/2003/2007/10, MS-DOS, Linux.

**Professional Experience**

**Equifax,Atlanta May-2016 to Present**

**Sr. Information Security Analyst**

* 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.
* jor hands on with Qualys tool to perform regular and ad-hoc scans on servers.
* Analyzes detected vulnerabilities and vendor reported vulnerabilities for applicability, severity, and solutions.
* Design infrastructure and deploy ArcSight SIEM solutions
* Skilled in working with distinct SIEM platforms including ArcSight, Nitro, LogRhythm, QRadar, and Splunk
* Designed & implemented the department SIEM (Arcsight) to monitor the DOT enterprise (over 20,000 assets). Administration of the DOT security infrastructure consisting of IDS/IPS systems (Snort, ISS, IDSM2, IPS, NFR, Checkpoint IPS1), Vulnerability Assessment tools (Foundscan and Nessus).
* Threat Hunting with Splunk, Qradar, Tanium and RSA Security Analytics.
* Application administration for Qradar, Splunk and Tanium.
* Use ArcSight SIEM to perform intrusion detection by creating rules, channels, alerts, and correlations based on daily and recurring security events
* Performed all content creation for Arcsight SIEM tool, both on the analyst and administration side.
* Created Splunk App for Enterprise Security to identify and address emerging security threats using continuous monitoring, alerting and analytics.
* Hands on experience in installing Splunk TASSymantec DLP, Splunk DB connect Splunk App for AWS and more.
* Worked on various projects involving other security systems to bring in security data to the SIEM. Systems such as Splunk, Tanium, various IPS event data sets, Blue Coat, NetWitness to just name a few.
* Worked on various projects involving other security systems to bring in security data to the SIEM. Systems such as Splunk, Tanium, various IPS event data sets, Blue Coat, NetWitness to just name a few.
* Monitor and maintain a global network of 700+ Cisco SourceFire IDS/IPS devices and 100+ HP ArcSight SIEM servers/appliances (connectors/loggers)
* Architecting and scoping and delivering QRadar SIEM implementations.
* Schedule scans by making Asset Groups and Scan Schedule Option in Qualysguard and record issues occurring during scan. Also, schedule ad hoc scans using Option Profile.
* Automated the centralized detection of security vulnerabilities with scripts for Vulnerability assessment tools like Qualys guard and Splunk.
* Working on SIEM, Threat and Vulnerability management.
* As an analyst, Prepared Several Documents for analysis of PAR log volume on weekly basis as well as monthly basis, Performed Quality Check on weekly basis.
* Conduct Malware analysis and investigate behavioral characteristics of each incident utilizing IDS monitoring tools.
* Writing complex tasks such as ETL jobs to integrate RSA Archer with Nessus, Rapid 7 and Qualys Vulnerability Scanners.
* Performed wireless pen testing using Aircrack-ng and analyzed the network using Wireshark. Found network vulnerabilities using Nexpose and analyzed web application using HP Fortify.
* Execute N-map and Qualys Guard Network scanner tools for port Scanning and detecting Bugs.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Running IBM App-scan, HP-Web-Inspect, Qualys Guard Scanner tools on various client supplied applications.
* Done quarterly activity of Penetration Testing of WAS using Qualys Guard.
* Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework.
* 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.
* Vulnerability Reporting and vulnerability scan scheduling using QualysGuard in line with PCI requirements.
* Team is responsible for technical security assessments to identify vulnerabilities, misconfigurations and weaknesses that may lead to unauthorized access of IT systems, applications, the data contained within Accenture network through the Qualys Guard and Nessus scanning tools.
* Administer and maintain the corporate DLP environments while structuring and documenting the corporate DLP infrastructure environments.
* Performing Qualys Vulnerability scans and manage reporting of all infrastructure assets
* Performed Symantec DLP environments management and support configuration as well as data security environments used in testing and configuring client sites prior to installation.
* Chase up, validate and update on status of the security assessment vulnerabilities (identified through Qualys guard) and make sure risk is mitigated.
* Responsibility for policy configuration for all the McAfee components and the same is deployed to the clients.
* 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.
* Design ePO Reports based on customer requirements.
* Troubleshooting issues related to McAfee ePO servers (5.x), VSE 8.x and HIPS.

**CNA Financial,Chicago Dec 2014-Apr 2016**

**Information Security Analyst**

* Analyze new forms of malware and design countermeasures to protect the enterprise from their impact.
* In depth experience with internal, external, network, & application vulnerability assessments utilizing QualysGuard and FireEye.
* Perform daily/weekly/quarterly health checks on Security Information and Event Management (SIEM) systems including ArcSight, Nitro, LogRhythm, QRadar, and Splunk
* Created and managed use cases, analyze correlated traffic, created and monitor channels, create and send reports, collected detailed evidence to support cases with SIEM HP Arcsight Application Worked with SIEM tools such as IBM QRadar to get real-time analysis of security alerts generated by network hardware and applications.
* Responsible for Arcsight ESM(Enterprise Security Manager) Data seed Upgrade testing
* Primary role is to deliver security services around HP Security Suite (ArcSight ESM, Logger, ArcMC, Connector Appliances, HP Smart Connectors, and ArcSight Express Appliances)
* Monitor and maintain a global network of 700+ Cisco SourceFire IDS/IPS devices and 100+ HP ArcSight SIEM servers/appliances (connectors/loggers)
* Architecting and scoping and delivering QRadar SIEM implementations.
* Knowledge on Configuration files in Splunk (props.conf, Transforms.conf, Output.confg)
* Maintained and monitored ArcSight SIEM infrastructure for corporate security.
* Configured and maintained ArcSight Management Console appliances.
* Monitor and analyze network threats through Palo Alto Panorama; run vulnerability assessment on machines with anomalous behavior, monitor firewall for incoming and outgoing threats.
* Provide expertise with incident response, security event monitoring, vulnerability management, asset security compliance and data loss prevention utilizing McAfee Nitro (SIEM), McAfee ePO, McAfee DLP.
* Strong knowledge on Vulnerability Management using QualysGuard and Nexpose .
* Third-party assessment of vendor cyber security, disaster recovery and business continuity controls. Worked with cloud security controls (IaaS, PaaS and SaaS). Assessment included business continuity planning at vendors.
* End to End Vulnerability Management services - Qualys tool.
* Oversee the execution of the Cyber Security Incident Response Playbook by the Security Operations Center and others for minor security incidents.
* Doing Policy compliance using Qualys Guard.
* Analyze new forms of malware and design countermeasures to protect the enterprise from their impact.
* Investigation for false positives for issues with Qualys with the help of support.
* Managing ePO version 5.3 and VSE 8.8 for large enterprise network.
* Handling migration, upgrade and new product roll out.
* Installing and configuring new ePO server.
* Maintain McAfee ePO environment in optimum performance and compliance standards.
* Monitoring McAfee dashboard for updated DAT versions in all the client.
* Monitoring and updating the Stores Closing details in McAfee and Bit9 console.
* Monitor Threats and Security events on McAfee and Bit 9.
* Handled the compatibility issues that arise due to Qualys scans.
* Provide a Weekly report about the number of threats and alerts triggered, ticket created and its status.
* Maintained security software to prevent security threats to the database, examined system access data and monitored access to the database. Corroborated with management and stake holders to revise and maintain security manuals and attend to existing matters.
* Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.
* Responsible for resolve issues of QRADAR.
* Designing and maintaining production-quality Splunk dashboards.
* Vulnerability Assessment and patch validation through Qualys guard express.
* Developed security metrics dashboards to illustrate trends in security events and situational views over time.
* Operations - Security Incidents and Vulnerabilities by OS.

**Infolace System,India May 2012-June 2014**

**Information Security Admin**

* In depth experience with Mobile Cloud and MDM solutions to include Fiberlink MaaS360, Citrix XenMobile, and Airwatch.
* Experience with Check Point R75-40 Smart-Dashboard, Anti-bot/Anti-Virus, IDS/IPS and Threat cloud Managed Security service (SOC) .
* In-depth expertise with McAfee ePO, endpoint protection suite, secure email gateway (SaaS) & DLP.
* Involved in standardizing Splunk forwarder deployment, configuration, and maintenance across UNIX and Windows platforms.
* Experience in Splunk development (creating apps, dashboards, data models, etc.
* Experience on Splunk Enterprise Deployments and enabled continuous integration on as part of configuration management.
* Experience with Splunk Searching and Reporting modules – (Splunk ITSI and Enterprise Security App) Knowledge Objects, Administration, Dashboards, Clustering and Forwarder Management.
* Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls
* Experience in Accelops & ArcSight SIEM solutions (Security Incident Event Management) for analytic driven IT operations management including performance and availability monitoring.
* Excellent understanding of secure data storage and transport implementations (E.g. PGP, SSH, SSL, IPSEC).
* In depth knowledge of TCP/IP, IEEE 802.11, wireless, & routing protocols   
  Experienced in Compliance Standards (SO/IEC 27001, PCI DSS, and SOX.) .
* Strong Windows system administration and security assessment skills including Active Directory.
* Experience analyzing network traffic captures and network mapping using WireShark, Nstat, ZenMap, AirCrack, NetStalker, etc.
* Knowledge of email and web filtering Proofpoint, Websense & McAfee Site Adviser.   
  Strong organizational, problem-solving, written and communication skills.

**Education**

## Master of Science in Computer Science.

**Certification**

* Qualys certified Vulnerability Management Specialist