|  |  |
| --- | --- |
| SivaRamaRaju Uddaraju **Cybersecurity Analyst/consultant**  Herndon, Virginia, United States | +1([571)-464-4474](tel:5714644474)  [siva.cybsec@gmail.com](mailto:siva.cybsec@gmail.com) |

|  |
| --- |
| Professional summary Cybersecurity Analyst/Consultant with 12+ years of extensive expertise in vulnerability management and executive reporting. Demonstrates proficiency in cross-functional collaboration, knowledge sharing, and continuous improvement. Proven track record in enhancing security posture through effective patch management and automated reporting processes.  **Key Domain and Technical Knowledge**  • Domain: Infrastructure Vulnerability Management and Networking  • Operating Systems: Windows, Mac OSX, Linux  • Firewalls Used: Juniper SRX, Watchguard  • Vulnerability management: Qualys, InsightVM & Nexpose, Tenable.io, Kenna Securities  • Network Packet Analyzing using NMAP, ADVANCE IP SCANNER, WIRESHARK, PACKETIZER, TCP DUMP  • Data Reporting Tools: ServiceNow, Tableau, Ivanti.  **Certifications / Professional Awards:**  • Microsoft certified professional  • Microsoft certified systems administrator  • Cisco certified network associate  • Certified Ethical Hacker (CEHv9)  • QualysGuard Certified Specialist in Vulnerability Management  • Rapid7 InsightVM Certified Administrator  • Rapid7 Nexpose Advance certified Employment historyCyber Security Senior Consultant Feb 2024 - PresentNIH (National Institute of Health) Bethesda, Maryland, United States  * Analyze vulnerability findings, report impacts, and propose solutions to stakeholders, ensuring risk prioritization. * Deliver vulnerability executive summaries and key risk indicator reports to security leadership. * Coordinate and support Vulnerability Management processes, including patch and remediation management. * Manage tracking and remediation of vulnerabilities, facilitating meetings to address high-severity issues. * Automated task processes with VBA scripts, improving efficiency in reporting vulnerabilities. * Conduct thorough vulnerability assessments, prioritize risks, and deliver actionable reports to stakeholders, enhancing overall security posture. * Streamline Vulnerability Management processes, leading to improved patch management and faster remediation of high-severity vulnerabilities within SLAs. * Develop VBA scripts to automate excel file splitting and email reporting, significantly boosting efficiency in vulnerability communication. * Facilitate cross-functional meetings to address remediation challenges, fostering a culture of proactive security across business groups. * Drive continuous improvement in scan coverage and authentication, contributing to a more robust and comprehensive security infrastructure. * Lead vulnerability assessments, prioritizing risks and delivering actionable reports to enhance organizational security posture at NIH.  Cyber Security Senior Consultant May 2022 - Oct 2023Backcountry Park City, Utah, United States  * Responsible for analyzing the vulnerability findings and its impact and report them to stakeholders with feasible solutions and risk prioritization. * Provided vulnerability executive summary related to VM metrics, key risk indicators, trending, and exploitable vulnerability reports to Security leadership and management. Point of contact for status updates regarding vulnerabilities across multiple platforms and multiple business groups. * Refined the Vulnerability Management (VM) process, coordinate, monitor and support activities in the areas of the VM program, security patch and remediation management. And provide inputs, solutions and update VM roadmap, develop, maintain and publish process and operation schedules for maximum coverage. * Managed tracking and remediation of vulnerabilities by leveraging and facilitating meetings with various remediation stakeholders to identify the challenges and plan of action for fixing the high severity vulnerabilities within defined SLA. * Proposed feasible ideas for reducing the overall risk such as hardening golden images and grouping of vulnerabilities with common solution. * Participated in knowledge-sharing and write technical articles based on investigative analysis performed for internal knowledge bases.Led vulnerability assessments, prioritizing risks and presenting actionable solutions to stakeholders. Refined VM processes and coordinated remediation efforts across platforms. * Spearheaded executive reporting on VM metrics and trends, driving informed decision-making. Facilitated cross-functional meetings to address high-severity vulnerabilities within SLAs. * Proposed novel risk reduction strategies, including hardening golden images and grouping vulnerabilities with common solutions. Contributed to knowledge bases with technical articles. * Served as primary point of contact for vulnerability status updates across multiple business groups. Coordinated with diverse stakeholders to optimize patch management and remediation. * Contributed to VM roadmap development, enhancing operational schedules for maximum coverage. Championed knowledge-sharing initiatives to bolster team expertise and efficiency. * Led vulnerability assessments, prioritizing risks and presenting actionable solutions. Refined VM processes, coordinated remediation efforts across platforms.  Cyber Security Consultant May 2019 - May 2022LittelFuse Chicago, Illinois, United States  * Had created High level Architecture Diagrams, Deployed and maintained the Tool from scratch. * Used Nexpose tool extensively and effectively in this project for evaluating security risk of the Client’s environment. * Responsible for analyzing the vulnerability findings and its impact and report them to stakeholders with feasible solutions and risk prioritization. * Utilized the ServiceNow incident management service for raising the Vulnerability incident ticket to the concern team and tracking them till they are remediated. * Provide vulnerability executive summary related to VM metrics, key risk indicators, trending, and exploitable vulnerability reports to Security leadership and management. Point of contact for status updates regarding vulnerabilities across multiple platforms and multiple business groups. * Refining the Vulnerability Management (VM) process, coordinate, monitor and support activities in the areas of the VM program, security patch and remediation management. And provide inputs, solutions and update VM roadmap, develop, maintain and publish process and operation schedules for maximum coverage. * Manage tracking and remediation of vulnerabilities by leveraging and facilitating meetings with various remediation stakeholders to identify the challenges and plan of action for fixing the high severity vulnerabilities within defined SLA. * Proposing feasible ideas for reducing the overall risk such as hardening golden images and grouping of vulnerabilities with common solution. * Strive towards complete scan coverage and authenticated scans as applicable. * Participate in knowledge-sharing and write technical articles based on investigative analysis performed for internal knowledge bases.Spearheaded vulnerability management, analyzing findings, prioritizing risks, and presenting actionable solutions to stakeholders for enhanced security posture. * Streamlined incident management using ServiceNow, efficiently tracking and resolving vulnerability tickets to meet defined SLAs and reduce overall risk exposure. * Facilitated cross-functional meetings to address high-severity vulnerabilities, fostering teamwork to overcome challenges and implement timely remediation strategies. * Proposed and implemented novel risk reduction strategies, including hardening golden images and grouping vulnerabilities with common solutions for efficient remediation. * Refined Vulnerability Management processes, developed roadmaps, and drove initiatives for comprehensive scan coverage, elevating organizational cybersecurity standards. * Led vulnerability management initiatives, analyzing findings and prioritizing risks to enhance security posture. Presented actionable solutions to stakeholders.  Cyber Security – Process Lead June 2014 – April 2019Ryna Technologies Pvt Ltd Hyderabad, India  * To Identify and communicate the technical requirements to the client for assessments. * To Identify vulnerability points of the client organizations in public and private network to undergo the proposed cyber security assessments. * To analyze using various scanning tools and foot printing techniques including google search strings to identify the exposure and to design the network and system data flow. * To create and formalize the pre-assessment documentation with milestones to accomplish the task. * Instrumental to drive the process of cyber security assessments spear heading the team involved. * Coordination and to communicate with clients on the requirements to take up the assessment tasks. * To prepare the findings report in network, System and Data auditing. * To prepare the complete assessment documentation for task specific or periodical jobs as per the client contract. * Correlation of analysis report on the anomalies and malwares as per the findings with impact level. * Maintaining the internal CVE and IOC database and correlation of vulnerabilities, findings, impacts and remediation processes. * Working on project planning and constraints based on the client requirement. * Communication of any identified project risks and issues to the delivery/project along with delivery dates.Led cyber security assessments, identifying vulnerabilities in client networks and systems. Developed comprehensive reports and remediation strategies. * Coordinated with clients to define assessment requirements, communicated technical needs, and managed project timelines for successful security audits. * Utilized advanced scanning tools and footprinting techniques to uncover exposure points. Created and maintained internal CVE and IOC databases. * Spearheaded assessment teams, driving process improvements and ensuring timely delivery of findings reports and documentation to clients. * Analyzed anomalies and malware, correlating vulnerabilities with impact levels. Prepared thorough pre-assessment documentation with clear milestones. * Led cyber security assessments, identifying critical vulnerabilities and developing comprehensive remediation strategies for client networks and systems.  System and Networking administrator June 2011 – May 2014VEGA Entertainment Pvt Ltd Hyderabad, India  * Configuration and management of network devices including watch guard firewall. * Configuration of VPN connectivity. * Configuration of firewall rules and modification of the rules time to time. * Configuration of REDIS server for CMS integration. * Administration of Ubuntu 16.10 and Centos 7 servers. * Event log capturing and monitoring to ensure the server and process uptime. * Management of CMS platform form on you tube and compiling the insights report. * Management of Facebook postings of the new releases and celebrity pages. * Ensuring the connectivity of servers to the remote OTT and DTH platforms for content Streaming. * Periodic backups to the cloud related to management file server and accounting platform. * Managing the software and hardware inventory of the organization. * Administration of antivirus and patch management across the physical and cloud platforms. * Configuration of new VM instances on the cloud. * Designed, deployed and implemented organization’s own apache cloud stack platform. * Documentation of configurations and performance reports time to time. * Involved in deployment of automation in users environment. * Repetitive task analyzing and understanding the process. * E-books and apps publication on Samsung mobile platform. * Client interactions on issues and reports * Converting physical books to Digital books through OCR conversions * Deploying the books in digital platforms like Web, mobiles, note pads in Epub, Pdf formats. * Applying Html coding and CSS styles Converting PDF/InDesign Document into Word/XMLo Re- flowable & Fixed layout Epub & Mobi format. * Verification of Created Comics and Designing of the page layouts, book cover page, index (total designing and layout of books).Managed network infrastructure, including firewall configuration and VPN setup, ensuring robust security and seamless connectivity for the organization. * Spearheaded implementation of Apache cloud stack platform, optimizing resource utilization and enhancing scalability of IT operations. * Administered Ubuntu and CentOS servers, meticulously monitoring event logs and conducting regular backups to maintain system integrity and uptime. * Streamlined content management processes for OTT and DTH platforms, significantly improving content delivery efficiency and user experience. * Facilitated digital transformation by converting physical books to e-books, enhancing accessibility across web and mobile platforms. * Pioneered deployment of automation in user environments, analyzing processes to streamline repetitive tasks. Transformed physical books into digital formats for multi-platform distribution.  EducationJNTU - Hyderabad, Hyderābād, India | Bachelor of Technology Oct 2007 - May 2011 |