RAJA M

9176220725 | raja.madhavann@gmail.com | Chennai, India | rajam.vercel.app | Raja M | Cyberblogz

SUMMARY

Security professional transitioning into Cybersecurity Analysis and Security Operations, with a solid foundation in SRE and mainframe infrastructure from Kyndryl. Experienced in reducing manual workloads through Python, Bash, and PowerShell automation, and supporting incident handling and system stability across critical environments. Skilled in vulnerability assessment, cloud security automation, and leveraging the MITRE ATT&CK framework for threat analysis. Seeking SecOps roles where deep infrastructure knowledge can enhance monitoring, threat detection, and proactive defense.

TECHNICAL SKILLS

- **Security & Monitoring :** Security monitoring (ServiceNow/BMC), basic log analysis ,endpoint security basics, learning SIEM (Wazuh/ELK) & IDS/IPS fundamentals.
- **Offensive Security :** Nmap, Burp Suite, OWASP ZAP, Metasploit, SQLMap, MITRE ATT&CK mapping.
- **Scripting & Automation :** Python, Bash, PowerShell.
- **Networking & OS :** foundational firewall/VPN concepts , Firewalls , Windows, Linux (Kali/Ubuntu)
- **Cloud & Infrastructure :** AWS (IAM, S3, CloudWatch), AWS security automation , Active Directory basics.
- **Tools & Security Standards :** ServiceNow, BMC, Control-M, GitLab CI , NIST CSF, ISO 27001 (foundational), SOC 2 (basic understanding) , OWASP Top 10 .

WORK EXPERIENCE

Associate Technical Engineer | Kyndryl (IBM Spin-off) **Aug 2023 –Jun 2025**

- Drove operational efficiency by automating job scheduling workflows (Control-M, Tivoli OPC), achieving a 30% reduction in manual tasks and improving operational precision.
- Managed and maintained secure configurations for mission-critical IBM Mainframe batch processing environments, consistently ensuring 100% SLA compliance.
- Reduced recurring incidents by 20% through detailed Root Cause Analysis (RCA) and the implementation of preventive measures across high-impact systems.
- Utilized BMC and ServiceNow for continuous monitoring and rapid incident resolution, proactively eliminating performance bottlenecks before user impact.
- Collaborated with internal Security teams to ensure secure batch processing workflows, maintaining data integrity and alignment with organizational compliance standards checks.

EDUCATION

Bachelor's in Computer Application | SRM Institute of Science and Technology **Aug2020 – May2023**

- Academic Achievement: Maintained a strong CGPA of 8.71 / 10.0.
- Relevant Coursework & Technical Foundation: Cybersecurity fundamentals, Computer Networks, Cloud Computing, AI concepts, Python programming, Web Technologies, and Database Management Systems (DBMS).

PROJECTS

Security Operations Incident Detection and Investigation

- Analyzed Windows authentication and system logs to identify suspicious login behavior and potential brute-force patterns using SIEM concepts and structured log analysis.
- Investigated security events by building a timeline of activity, validating indicators, and mapping findings to incident response steps including containment and remediation.
- Documented investigation outcomes, response actions, and detection improvement recommendations to demonstrate practical security operations workflows.

Cloud Security Misconfiguration Detection and Response

- Identified common cloud security misconfigurations such as public storage access and over-permissive IAM policies within an AWS environment.
- Analyzed cloud activity and access patterns using logging and monitoring concepts with AWS CloudTrail and CloudWatch to support detection and investigation.
- Documented security risks, recommended remediation actions, and proposed monitoring strategies aligned with cloud security and SecOps best practices.

CERTIFICATIONS

- AWS Certified Cloud Practitioner **– Amazon**
- Offensive Pentesting **– TryHackMe**
- Cybersecurity & Ethical Hacking (Advanced) **– Guvi**
- Scripting & Programming Fundamentals (Bash, PowerShell, Python) – **Cybrary**
- Automation & Workflow Optimization **– Kyndryl**

VOLUNTEERING

Cybersecurity Community Member – EC-Council

- Actively engage with global cybersecurity professionals through the EC-Council Cybersecurity Community.
- Contribute to discussions on ethical hacking, cloud security, detection techniques, and emerging threats.
- Participate in community initiatives focused on OWASP Top 10, MITRE ATT&CK, and defensive security practices.
- Support knowledge sharing by helping beginners understand security labs, web vulnerabilities, and Linux basics.
- Committed to continuous learning and advancing cybersecurity awareness within the community.

ACHIEVEMENTS

- Contributed to workflow automation initiatives at Kyndryl that resulted in a 30% reduction in manual effort across batch operations.
- Reduced recurring incidents by 20% by supporting RCA activities and implementing recommended preventive measures.
- Successfully contributed to data center migration, ensuring smooth transition of critical batch workflows and systems.