Aakash Raman

aakashr93@gmail.com | +1 (240) 921-7770 | LinkedIn| Medium| GitHub | College Park, MD (Willing to Relocate)

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on SOC experience in threat hunting, digital forensics, incident response, and threat intelligence across cloud and on-premises environments. Skilled in optimizing SIEM, automating response workflows, and enhancing threat detection. Proficient in incident triage, investigating anomalous activities, and leading containment efforts. Achieved 1st place at WiCyS Tier 1 Mini SANS BootUp CTF 2024 and 8th place at the Amazon x WiCyS CTF 2024.

WORK EXPERIENCE

Atlas Systems East Brunswick, (NJ, USA)

Cybersecurity Analyst (Incident Response & SOC) Aug '24 - Present

- Managed and **tuned SIEM (ELK, Splunk) queries mapped to the MITRE ATT&CK Framework** for real-time threat detection and response, **reducing incident response time by 30%.**
- Led **Incident Response & Network-based Threat Hunting** activities focussing on OpenCTI Threat Intelligence APTs using Azure Sentinel and Microsoft Defender.
- Conducted proactive threat hunting and security alert monitoring in a **24/7 SOC environment** along with the investigation, containment, and remediation for incidents involving cloud and on-premise environments.
- Triaged and correlated events across multiple networks and host-based log sources, proactively identifying malicious activity and suspicious behavior using OpenCTI Threat Intelligence.
- Conducted cybersecurity awareness sessions for staff, educating teams on best practices for phishing defense, password security, and incident reporting.
- Optimized incident management workflows with ServiceNow, **automating processes to improve support delivery** and reduce incident response times.

IBM (X-Force Incident Response) Austin, (TX, USA)

Cybersecurity Consultant Intern May '23- Aug '23

- Enhanced **incident response by 95% through Purple Teaming bootcamps**, collaborating with Digital Forensic Analysts and Incident Responders, leveraging MITRE ATT&CK Framework and Atomic Red Team.
- Increased **threat detection and response efficiency by 40%** by refining SIEM queries and integrating Threat Intelligence and IOCs in Splunk and IBM QRadar.
- Conducted web application security testing and vulnerability assessments to ensure compliance and reduce risks, collaborating with teams to optimize security rules and alerts.
- Led **phishing campaign identification** and remediation efforts, through proactive threat hunting and analysis using OpenCTI, Cisco Talos, and Yara rules.
- Developed and **implemented insider threat detection playbooks using TheHive and CrowdStrike Falcon**, reducing incident time by **40%**.
- Developed **automation scripts in Bash, PowerShell, and Python** for malware triage and forensic data extraction from Wireshark packet captures.

Hevo Data, Inc Bangalore, India

Cybersecurity Associate Jan '21- May '22

- Reduced **false positives by 30% by optimizing ELK SIEM queries** and creating custom alerts to enhance threat detection.
- Integrated Proofpoint for E-Mail security along with DMARC and DKIM protocols on the organization's domain, **reducing phishing and spam by 60%**.
- Conducted **risk assessments and implemented security controls** aligned with **NIST and ISO 27001 frameworks** to ensure compliance.
- Monitored and analyzed security alerts on **AWS and Azure**, ensuring prompt mitigation of cloud security threats based on **CIS Benchmarks**.

Ramco Cements Ltd Chennai, India

Security Consultant Intern Apr '20 – May '20

- Strengthened **Active Directory infrastructure** by applying Microsoft's best practices, enhancing resilience against insider threats.
- Boosted **insider threat detection by 75%** through digital forensics using tools like KAPE, VeraCrypt, and FTK Imager.
- Managed SMTP E-Mail server and authentication setup (SPF, DKIM, DMARC) for clients in the HR department.

SKILLS SUMMARY

Programming/Scripting Languages: Python, C, JavaScript, Bash, PowerShell, SQL.
Operating System/Virtualization Technologies: Windows, Kali Linux, Ubuntu, Remnux, Flare VM, Docker.
OSINT/Offensive Security Tools: Burp Suite, Nessus, Nikto, Metasploit, Bloodhound, Mimikatz, Qualys.
Malware Analysis/Reverse Engineering Tools: Ghidra, Cuckoo Sandbox, VirusTotal, Any.Run.
Digital Forensics/Incident Response Tools: Elastic SIEM (ELK), Splunk, IBM QRadar, Snort, Yara, Velociraptor, FTK Imager, Autopsy, Volatility, Wireshark, OpenCTI, TheHive, CrowdStrike Falcon EDR, Microsoft Defender.
Cloud Security Technologies: AWS, Azure, GCP.
Risk & Compliance Frameworks: NIST Cybersecurity Framework, MITRE ATT&CK Framework, Cyber Kill Chain, BC/DR Planning, ISO 27001, HITRUST, FEDRAMP.
DevSecOps Tools: Jira, Git, Snyk, Ansible, ServiceNow.
Soft Skills: Incident Communication, Project Management, Problem Solving, Quick Learner, Critical Thinking, Attention to Detail.

PROJECTS

- **Visualizing Lateral Movement with Velociraptor JSON Logs:** Developed "Velocigrapher" using Python's "igraph" library, Velociraptor JSON Logs and Windows Authentication IDs, improving Incident Report Quality by **85%**.
- **Android Malware Analysis Research Paper**: Published in JESTR Journal, covering technical and business impacts of Android malware, their interactions with C2C servers, and mitigation techniques.
- **Penetration Testing and Incident Response for Horizon Inc:** Conducted penetration testing & incident response for a fictional company using MITRE ATT&CK and Cyber Kill Chain, implementing defensive measures by analyzing attacker TTPs. (GitHub)
- **Designing a Secure Cloud Security Architecture for Cobra Kai**: Designed and implemented a secure AWS Cloud architecture, ensuring robust security with EC2, Lambda, and CloudWatch. (GitHub)

CERTIFICATIONS

CompTIA Security+, CySA+, PenTest+, CASP+	(March 2022 - July 2023)
AWS Solutions Architect Associate (AWS SAA)	(September 2023)
Certified CyberDefender	(January 2024)
Pursuing CISSP, GCIH & GCFE	

OCCUPATIONAL HIGHLIGHTS

- **Ranked 1st globally in WiCyS Tier 1 Mini SANS BootUp CTF 2024** & **8th globally** in **Amazon x WiCyS CTF 2024**.
- Staff Member at **BSides Charm and DEFCON32**, managing and testing CTFs, providing IT support, and overseeing event management.
- Presented 'Introduction to Windows Malware Analysis' to ~100 cybersecurity professionals at **OWASP Mumbai**. (GitHub)
- CTF Player at **TryHackMe** (Top 1%), **HackTheBox**, & **CyberDefenders**.

EDUCATION

University of Maryland, College Park College Park, MD, USA

Master of Engineering in Cybersecurity Aug '22 - May '24

Vellore Institute of Technology, Vellore Vellore, TN, INDIA

Bachelor of Technology – Computer Science Engineering with Information Security Jul '17 - Jul '21