AAKASH RAMAN

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

EDUCATION

UNIVERSITY OF MARYLAND, COLLEGE PARK — College Park, MD, USA
Master of Engineering in Cybersecurity; CGPA: 3.77 — Aug '22 - May '24

VELLORE INSTITUTE OF TECHNOLOGY — Vellore, TN, INDIA
Bachelor of Technology – Computer Science Engineering with Information Security; CGPA: 3.8 — Jul '17 - Jul '21

EXPERIENCE

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 and Atomic Red Team.
- Improved threat detection and response efficiency by **40%** through optimized detection engineering strategies and refined SIEM queries using Splunk, and IBM QRadar.
- Boosted incident response capabilities by **20%** through visualizing lateral movement with Velociraptor JSON logs, Python and the Splunk SIEM.
- Reduced phishing-related security incidents by **30%** via advanced threat hunting utilizing OpenCTI, Cisco Talos Intelligence, and YARA rules.
- Streamlined incident handling efficiency by developing and implementing playbooks and runbooks for insider threats using TheHive, Cortex, CrowdStrike Falcon and SOAR platforms.
- Achieved a **40%** improvement in threat detection by refining Splunk and IBM QRadar configurations and integrating comprehensive threat intelligence feeds and STIX/TAXII protocols.

HEVO DATA INC — Bangalore, (KA, INDIA)
Cybersecurity Associate — Jan '21- May '22

- Worked with the Data Analysis/InfoSec team to monitor security events and authored technical blogs on security and analytics, increasing online presence by **30%** using WordPress.
- Improved visibility and strategic decisions with the ELK SIEM, reducing false positives by **30%** through optimized queries and custom alerts.
- Reduced risks by **15%** by refining methodologies with NIST Cybersecurity Framework, ISO 27001, and MITRE ATT&CK Framework for threat modelling and compliance auditing.
- Enhanced E-Mail security by integrating DMARC and DKIM protocols on the organization's domain, reducing phishing and spam by **60%**.
- Enhanced endpoint security by administering Linux/Windows systems and implementing best practices using Docker, Git, and Ansible.
- Conducted vulnerability assessments on networks, endpoints, and AWS instances using Nessus; proposed solutions and leveraged analytics to enhance security protocols.

RAMCO CEMENTS LTD — Chennai, (TN, INDIA)
Security Consultant Intern — Apr '20 – May '20

- Reduced the company's downtime by **25%** by enhancing Risk Management and Business Continuity Plans.
- Hardened Active Directory by implementing Microsoft best practices and Role-Based Access Control.
- Boosted insider threat detection and response by **75%** through digital disk forensics using KAPE, Veracrypt, Autopsy, and FTK Imager.
- Enhanced network security by securing network traffic with SonicWall Next-Gen Firewall.

SKILLS SUMMARY

Programming/Scripting Languages: Python, C, C++, Java, HTML, CSS, JavaScript, Bash, PowerShell, SQL.
Operating System/Virtualization Technologies: Windows, Kali Linux, Ubuntu, VMware, Docker, Kubernetes.
OSINT/Offensive Security Tools: Burp Suite, OWASP ZAP, Nessus, Nikto, Nmap, Metasploit, SQLMap, Hydra, John the Ripper, Bloodhound, Gobuster, Responder, Mimikatz, OWASP Top 10.
Malware Analysis/Reverse Engineering Tools: Ghidra, IDA Pro, ProcMon, Process Explorer, Regshot, PE-Bear, Cuckoo Sandbox, VirusTotal.
Digital Forensics/Incident Response Tools: Elastic SIEM (ELK), Splunk, CrowdStrike Falcon EDR, IBM QRadar, Snort, Yara, Velociraptor, FTK Imager, Autopsy, Volatility, Wireshark, E-Mail Security, Microsoft 365 Defender, SonicWall Firewall, Forcepoint DLP, Active Directory, OpenCTI, TheHive.
Cloud Security Technologies: AWS, Azure, GCP, Azure Sentinel.
Risk & Compliance Frameworks: Threat Modelling, NIST Cybersecurity Framework, Microsoft Office Suite, MITRE ATT&CK Framework, Cyber Kill Chain, ISO 27001, PCI-DSS, HIPAA, Risk Management, BC/DR Planning.
DevSecOps Tools: Jira, Git, Jenkins, Synk.
Soft Skills: Ownership, Problem Solving, Quick Learner, Time Management, Critical Thinking, Attention to Detail.

PROJECTS

- **Visualizing Lateral Movement with Velociraptor JSON Logs:** Developed "Velocigrapher" using Python's "igraph" library, 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 testing using MITRE ATT&CK and Cyber Kill Chain, implementing defensive measures with the Diamond Model of Intrusion Analysis. (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 (September 2023)
Certified CyberDefender (January 2024)
Pursuing PJPT & CISSP

HIGHLGHTS

- Ranked 51st in UMD CTF'24 by solving Forensics, Web, Privilege Escalation, Cryptography, Log Analysis, and Threat Hunting challenges.
- Achieved 9th place globally in Level Effect's Cyber Defense Analyst CTF by solving Forensics, Incident Response, and OSINT challenges.
- TryHackMe: Currently in the Top 1% with 100+ rooms & HackTheBox: Currently Pursuing Pwning Boxes and Defensive Sherlocks.
- Participated in CyberDefenders Blue Team CTFs, covering Threat Intelligence, Malware Analysis, Cloud Forensics, Threat Hunting.
- Volunteered at BSides Charm and Defcon32, managing CTFs, providing IT support, and overseeing event management.