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 Aug ‘22 - May ‘24

VELLORE INSTITUTE OF TECHNOLOGY Vellore, TN, INDIA
Bachelor of Technology – Computer Science Engineering with Information Security Jul ‘17 - Jul ‘21

EXPERIENCE

ATLAS SYSTEMS East Brunswick, (NJ, USA)
Cybersecurity Analyst Aug ’24 - Current

- Enhanced cloud security by **70%** by developing Azure Cloud Security Baselines for migrating from Rackspace Cloud to Azure Cloud, adhering to Microsoft CIS v1.3 and MCSB v1 benchmarks across database, network, VM, and storage configurations.
- Increased report generation efficiency by **40%** through the development of a Python script, converting CSV vulnerability scan data into customizable PDF templates.
- Supported the development of the SOC and Managed Security Services, improving vulnerability remediation by **30%** through vulnerability assessments using Nessus, Burp Suite, and Qualys.
- Performed Azure Cloud security assessments, identifying and mitigating **25%** of security gaps through Azure-native vulnerability scans, compliance checks, and remediation strategies.
- Enhanced incident management workflows using ServiceNow to automate ticket creation and resolution tracking, boosting team efficiency.

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.
- Improved threat detection and response efficiency by **40%** through optimized detection engineering strategies and refined SIEM queries using Splunk, and 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

- Collaborated with the Data Analysis/Information Security team to scrutinize security events and authored technical blog posts on security trends and analytical methods, boosting our digital footprint by **30%** through strategic content deployment on 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 and MITRE ATT&CK Framework for threat modelling and 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.
- Executed comprehensive vulnerability scans on network architectures, endpoint devices, and AWS environments utilizing Nessus.

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

- Decreased organizational downtime by **25%** through the strategic enhancement of Risk Management frameworks and Business Continuity Plans.
- Fortified Active Directory infrastructure by adopting Microsoft’s best practices and configuring Role-Based Access Control.
- Boosted insider threat detection and response by **75%** through digital disk forensics using KAPE, Veracrypt, Autopsy, and FTK Imager.
- Streamlined IT service operations by integrating ServiceNow with existing systems.
- Boosted network security by configuring SonicWall Next-Gen Firewalls and implementing advanced iptables rules for traffic management.

SKILLS SUMMARY

Programming/Scripting Languages: Python, C, C++, Java, JavaScript, Bash, PowerShell, SQL.
Operating System/Virtualization Technologies: Windows, Kali Linux, Ubuntu, VMware, Docker, Kubernetes.
OSINT/Offensive Security Tools: Burp Suite, Nessus, Qualys, Nikto, Nmap, Metasploit, SQLMap, Hydra, John the Ripper, Bloodhound, Gobuster, Responder, Mimikatz.
Malware Analysis/Reverse Engineering Tools: Ghidra, IDA Pro, ProcMon, Process Explorer, Regshot, PE-Bear, Cuckoo Sandbox, VirusTotal, Tor, Dark-Web Monitoring.
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, Snyk, Ansible.
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, 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 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 CISSP & PJPT	

HIGHLGHTS

- Ranked 1st globally in WiCyS Tier 1 Mini SANS BootUp CTF 2024 & 9th globally in Level Effect’s Cyber Defense Analyst CTF.
- Staff Member at BSides Charm and DEFCON32, managing and testing CTFs, providing IT support, and overseeing event management.
- CTF Player at TryHackMe (Top 1%), HackTheBox & CyberDefenders.