Aakash Raman

LinkedIn https://aakashraman.github.io/

Email : aakashr93@gmail.com
Mobile : +1-240-921-7770

Education

University of Maryland, College Park — Graduate College
Masters of Engineering in Cybersecurity — *Aug 2022 - May 2024*

VIT University, Vellore — Undergraduate College
BTech CSE with Information Security — *Jul 2017 - Jun 2021*

Experience

Atlas Systems — East Brunswick, NJ
Cybersecurity Analyst - Full Time — *Aug 2024 - 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, enabling clients to assess their security posture.
- 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
Cybersecurity Consultant - Intern — *May 2023 - Aug 2023*

- 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.
- 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 using 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
Cybersecurity Associate - Full Time — *Jan 2021 - May 2022*

- 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 modeling 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
Security Consultant - Intern — *Apr 2020 - May 2020*

- 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.
- 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, 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, OWASP Top 10.
Malware Analysis/Reverse Engineering Tools: Ghidra, IDA Pro, ProcMon, Process Explorer, 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, Cisco Talos Intelligence, Atomic Red Team, OpenCTI, TheHive, Cortex.
Cloud Security Technologies: AWS, Azure, GCP.
Risk & Compliance Frameworks: Threat Modelling, NIST Cybersecurity Framework, Microsoft Office Suite, MITRE ATT&CK Framework, Cyber Kill Chain, ISO 27001, Atomic Red Team, PCI-DSS, HIPAA, Risk Management, BC/DR Planning.
DevSecOps Tools: Jira, Git, Jenkins, Snyk, ServiceNow.
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.

Performing Forensic Analysis on a Suspected Malware Disk Image: Conducted a comprehensive Digital Forensics Investigation using the Autopsy Forensic Suite on a disk image, extracting key data and identifying a malicious executable. Utilized VeraCrypt, Wireshark, and CyberChef to analyze the malware behavior and its characteristics for deeper insights.(GitHub)

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)

Improving Security Posture at Horizon Inc: Enhanced Disaster Recovery, Business Continuity, Threat Intelligence, and Risk Management for Horizon Inc. Implemented “Defense in Depth” using technical/non-technical solutions. Utilized STRIDE and DREAD for threat modeling and conducted cost-benefit analyses. (GitHub)

Home Active Directory Lab: Developed an Active Directory Lab, utilizing tools like Kali Linux, Bloodhound, Mimikatz, and Rubeus to simulate and analyze security threats, enhancing skills in privilege escalation and AD security.

Home Malware Analysis Lab: Built a Malware Analysis Lab using REMnux VM, Cuckoo Sandbox, Wireshark, PE-Bear, Regshot, Volatility, and the SIFT Workstation to dissect malware, understand behavior, and create mitigation strategies.

Home Threat Hunting Lab: Set up an Open Source Threat Hunting Lab with Greylog and Splunk, enabling real-time monitoring, analysis, and response to simulated cyber threats.

Certifications

CompTIA Security+	*March 2022*
CompTIA CySA+	*July 2022*
CompTIA PenTest+	*January 2023*
CompTIA Advanced Security Practitioner (CASP+)	*July 2023*
AWS Solutions Architect Associate (SAA-C03)	*September 2023*
Certified CyberDefender	*January 2024*

Occupational Highlights

CTFs: Achieved 51st rank in UMD CTF’24, 9th rank globally in Level Effect’s Cyber Defense Analyst CTF and 13th rank in Payment Card Hacking CTF at DEFCON32 by solving challenges in Forensics, Web, Privilege Escalation, Cryptography, Log Analysis, Threat Hunting, Incident Response, and OSINT.
Cybersecurity Platforms: Currently in the Top 1% on TryHackMe with 100+ rooms, pursuing Pwning Boxes and Defensive Sherlocks on HackTheBox, and participated in CyberDefenders Blue Team CTFs covering Threat Intelligence, Malware Analysis, Cloud Forensics, and Threat Hunting.
Cybersecurity Blogger: Cybersecurity Blogger on Medium, sharing insights and expertise on various cybersecurity topics.
Volunteering Experience: Volunteered at BSides Charm and DEFCON32, managing CTFs, providing IT support, and overseeing event management.
Future Work: Pursuing the Practical Junior Penetration Tester (PJPT), and Certified Information Security Systems Security Professional (CISSP) certifications.