PAVAN SREEVATSAV AKULA

pavansrivatsav.akula@gmail.com • 4903 Southland Ave, Alexandria, VA • (585) 553-0212

Experience

Sr Threat Detection and Response Analyst, Amtrak — Washington, D.C 09/2023 - Present

- Led triage and response for 50+ declared cybersecurity incidents as the primary TDR analyst; authored cyber incident after action reports (CIAAR) and managed high-severity bridge calls with cross-functional digital technology teams.
- Served as secondary team lead, driving SOP standardization, TDR process alignment, and contributing to Incident Response Framework development initiatives.
- Submitted 60+ enhancement requests including alert tuning, log source integrations, and automation improvements; developed 15 custom detection rules using threat intelligence and log hunting techniques.
- Classified and responded to 500+ phishing reports, created Azure Sentinel phishing workbooks, and implemented automated Teams SLA notifications and user response workflows.
- Contributed to development of IOIs, SOPs, and IR playbooks; built Sentinel workbooks to enable 360-degree incident reviews and improve visibility for the SOC team.
- Participated in adversary-driven threat hunting based on MITRE TTPs provided by the Threat Intel team, and supported enterprise-wide cyber hygiene initiatives.
- Represented the TDR team in 4 tabletop exercises (TTXs) and contributed to planning and execution as part of the TTX hosting team.

Cybersecurity Intern, Amtrak — Washington, D.C 09/2022 - 08/2023

- Rotated across GRC, Cyber Engineering, and Cyber Architecture teams, gaining hands-on experience in security governance, cloud security engineering, and architectural design of secure systems.
- Led a major project integrating VirusTotal threat intelligence with Azure Sentinel SIEM and automating security alert workflows through Microsoft Teams to enhance threat detection and incident response.

Web Application Security Teaching Assistant, RIT — Rochester, New York 01/2022 - 08/2023

- Managed 35 undergrad students with teaching, grading, and providing feedback on the assignments.
- Facilitated students with strong foundational skills in computing and networking such as OWASP Top 10, Cryptography, and basic web development.

Cybersecurity Analyst/SOC Analyst, WIPRO LTD — Bangalore, India 06/2019 - 07/2021

- Monitored and analyzed the events or alerts by detecting, prioritizing,Triaging, mitigating, and remediation.
- Investigated 1000's of alerts and classified to true incidents or false positive on both SIEM and EDR tools.

Fine-tuned alerts in SIEM tools and reduced alert count from about 1500 to 300.

- Performed 4 data breach AD-HOC activities and reported the finding in a timely manner to CISO's.
- Collaborated with the content team and created 11 automated IR playbooks to reduce security alert volume by 90%.
- Scheduled standup meetings, assigned tasks, and assisted with critical incidents by leading a 15 member security Level 1 team for five months.

Software Engineering Intern, OPENTEXT — Hyderabad, India 04/2019 - 06/2019

- Guided peer interns with design, testing, production deployment, and stabilization of solutions for OpenText Managed Services.
- Implemented UI tests for the content management system and automated 25 test cases.

Education

Master of Science in Cybersecurity, Rochester Institute of Technology 08/2021 - 08/2023

GPA: 3.79/4.0

Relevant Coursework: Introduction to Computing Security, Adv Malware forensics, Information Risk Management, Computing system security, Cryptography Authentication, Trusted Computing.

Bachelor of Science in Computer Science, B V Raju Institute of Technology 08/2015 - 04/2019

GPA: 3.75/4.0

Relevant Coursework: Information Security, Network Programming, Ethical Hacking, C, C++ Programming, Java, Python.

Skills

Security & Monitoring Tools:

IBM QRadar, Azure Sentinel, CrowdStrike, FireEye, McAfee, Zscaler, XSOAR (Demisto), Swimlane, SailPoint, Binalyze, Absolute

Threat & Vulnerability Management:

Incident Response, EDR, Digital Forensics, Malware Analysis, Threat Hunting, Log Analysis, Vulnerability Assessment, MITRE ATT&CK, Email Security, Tenable, ThreatStream, ZeroFox, Feedly

Networking & Infrastructure:

TCP/IP, DNS, Routing, OSI Model, IDS/IPS, Palo Alto, Check Point, Fortinet, F5 Networks, AWS Security

Languages & Platforms:

Python, PowerShell, Bash, Java, C, C++, JavaScript, Ruby on Rails, SQL, Linux, Windows

Projects

Streamlined SOC Operations with Threat Intel and Incident Response Automation 05/2023 - 08/2023
Integrated VirusTotal and custom threat intelligence into Azure Sentinel using Logic Apps to enrich alerts. Built automation for incident escalation and Teams-based SOC notifications using Azure Sentinel and Microsoft Defender. Streamlined response to policy violations and high-severity threats.

Digital Forensics And Trusted Computing 01/2022 - 05/2022
In this literature survey, researched different ways of achieving the trustworthiness of evidence data from 15 paper publications, which will help digital forensics investigators perform the root cause analysis using TPM, Intel SGX, TSS.

Addressing Visibility Issues Present In TLS 1.3 08/2021 - 12/2021
Addressed the TLS 1.3 visibility issues to make the investigation of encrypted network traffic easy. Implemented an existing proposed solution using the OpenSSL library written in C, crypto algorithms and achieved the 90% efficiency in decryption of data.

Certifications

GIAC Certified Incident Handler (GCIH), Analyst Number - 50881 02/2025 - 02/2029

EC-Council Certified Incident Handler, ECC1873290564 01/2023 - 01/2026

SANS SEC504: Hacker Tools, Techniques, and Incident Handling, CPE 38 Credits

SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics, CPE 36 Credits