Gayathri Penumur

Associate SOC Analyst

Gayathrinaidu1999@gmail.com | (314)-203-3252 | https://www.linkedin.com/in/gayathripenumur/ | **(Open to Relocation)**

SUMMARY

*Passionate and detail-oriented **Associate SOC Analyst** with 2+ years of experience in **security monitoring, alert triage, and incident response** across enterprise environments. Proficient in **SIEM tools (Splunk, Microsoft Sentinel)** and **EDR solutions (Microsoft Defender)** for real-time detection, analysis, and escalation of threats. Skilled in **log analysis, vulnerability management, and basic scripting (Python, PowerShell)** to support automation and process efficiency. Certified in **CompTIA Security+ 701** and **BTL1**, with strong analytical and communication skills and a proven commitment to continuous learning in cybersecurity operations.*

TECHNICAL SKILLS

- **SOC & Monitoring Tools:** Microsoft Sentinel, Splunk SPL, ELK, Wazuh, Microsoft Defender for EDR/XDR, Defender for Office 365, Sysmon
- **Incident Response and Cyber Threat Intelligence:** Incident Scoping, IOC enrichment, Host Isolation, Blocking Indicators, Forensic Imaging, Evidence Handling, False Positive Triage, Containment and Escalations, Alert Triage, Event Correlation, Threat Hunting, VirusTotal, Ticket Lifecycle Tracking, Threat Intelligence Platforms, Security Configurations, MISP.
- **Threat Detection, Network & Forensics Analysis:** Snort (IDS/IPS), Zeek, Suricata, Wireshark (PCAP analysis), Tshark, NetworkMiner, FTK Imager, Volatility, Encase, Autopsy
- **Vulnerability & Pentesting Tools:** Burp Suite, OWASP ZAP, Nessus, Qualys, CVSS scoring, Hydra, Sqlmap, Metasploit, Gophish (Phishing Campaign)
- **Security Frameworks & Concepts:** CIA Triad, MITRE ATT&CK, Cyber Kill Chain, Incident Response Plan, Root Cause Analysis, IOC Analysis, OSI model, TCP/IP Model, OWASP Top 10, System Hardening, Diamond Model, Vulnerability Management, DLP (Microsoft Purview), Antivirus, FIM, MFA, Email security tools, Security Principles, Disaster Recovery Plan.
- **Programming & Query Languages:** C, Java, Python, Linux CLI, PowerShell, KQL, SQL, SPL
- **Compliance & Frameworks:** HIPAA, PCI DSS, SOX, GLBA, SOC2, NIST CSF, NIST 800-61, GDPR, ISO 27001, CIS controls
- **Operating Systems & Cloud**: Windows 10/11, Linux (Ubuntu/Kali/Parrot), MacOS, Azure, AWS (Basic Level), WSL, VMware, VirtualBox
- **Documentation & Reporting:** SOP writing, Incident Playbooks, Executive Summary Reports, Alert Queue Management, Rule/Signature Documentation, Case Documentation, Power BI.

WORK EXPERIENCE

NCyTE Center | Security Analyst Intern | Feb 2025 – May 2025

- Designed and secured segmented LAN architecture using routers, switches, and a pfSense **firewall** with VLAN isolation; validated security controls by simulating cross-zone traffic and analyzing alerts in SOC monitoring tools.
- Configured enterprise network components including Active Directory, DNS, and firewall rules; conducted network assessments using Nmap and Hydra to identify weaknesses, leading to improved access controls and strengthened firewall configurations.
- Deployed a DMZ web application and evaluated WAF effectiveness by simulating OWASP Top 10 attacks (SQLi/XSS), then analyzed pfSense logs to identify detection gaps and recommend improved monitoring rules. Conducted KQL-driven log correlation to identify IOCs and anomalies across endpoints, firewalls, and web proxies, leveraging TTP analysis for threat hunting.
- Conducted end-to-end security assessments following PTES methodology, documenting findings in alignment with **MITRE ATT&CK**, and developed SOC playbooks for multi-layer incident detection and response across network and application layers.

Cognizant Technology Solutions India Pvt Ltd | Programmer Analyst (SOC Analyst) | Aug 2021 – Jul 2023

- Served as the **first line of defense by monitoring and analyzing 200+ daily security logs** and alerts from SIEM, firewalls, proxies, IDS/IPS, Active Directory, and IAM systems; correlated events to detect threats, reduced false positives by 20%, and escalated incidents through **ServiceNow** tickets in accordance with defined **SLAs**, ensuring timely containment and mitigation per established incident response procedures.
- Led incident triage and investigation of malware, phishing, and unauthorized access in a CSOC environment; utilized Microsoft Sentinel and KQL to perform forensic analysis, threat hunting, and IOC correlation. Monitors emails for suspicious links and attachments to identify phishing attempts and provides patching recommendations for zero-day threats.
- Examined malicious files and payloads to determine attack techniques, contributed IOCs to threat intelligence feeds, and **tuned detection rules and security tools to strengthen monitoring** capabilities and reduce alert fatigue. Stayed updated on emerging threats and trends, integrating intelligence into monitoring and SOC processes.
- Conducted proactive threat hunting across endpoints and network systems using internal & external threat intelligence, identifying vulnerabilities, recommending improvements to SOC workflows, playbooks, detection logic, and **automating repetitive tasks such as log analysis, alert correlation, and reporting with KQL** to enhance SOC efficiency and reduce IRT.
- Configured and refined SIEM alerts and dashboards, ensuring log source enrollment, data hygiene, and actionable threat intelligence; enhanced incident response playbooks, SOPs, and documentation while ensuring compliance with CSOC operational standards. Participated in post-incident reviews and lessons learned sessions.
- Participated in on-call rotations, **providing 24x7 escalation support for** high-priority incidents; contributed to **after-action reviews,** gathering information for security reports ensuring accuracy and completeness, and dashboards development to refine response procedures and strengthen organizational security posture.

TECHNICAL PROJECTS

Azure-Based Honeypot and Security Log Analysis with Microsoft Sentinel

- Designed and deployed a Windows 10 honeypot in Azure with intentionally exposed **NSG** rules and a disabled firewall to simulate realistic attacker behavior and gather telemetry.
- Collected and analyzed Windows Security Event Logs in Azure Log Analytics and Microsoft Sentinel, **performed log ingestion, alert tuning, and custom rule creation** to detect brute-force attempts, failed authentications, and anomalous activity.
- Built dynamic attack maps using Sentinel Workbooks and GeoIP data, visualizing geographic patterns of attacks and adversary behavior. Developed and tested custom detection rules in a lab environment to reduce noise and improve alert accuracy, simulating SOC operations.
- Created automated response playbooks via Azure Logic Apps to streamline alert handling and demonstrate SOAR integration benefits.
- Conducted **KQL**-driven log correlation to identify IOCs and investigate anomalies, enabling Tier-2 style threat hunting by mapping attacker TTPs. Configured Azure IAM roles and Purview DLP policies to secure sensitive data at rest and in transit. Simulated enterprise **cloud security operations** and validated protective controls.

Ethical Hacking Blueprint Development & Prototyping

- Designed a comprehensive testing blueprint for Sun-Micro systems, including network configuration setup and phishing simulations with **Gophish** to assess employee susceptibility to social engineering attacks. Participated in **tabletop exercises** and Red/Purple Team simulations to evaluate incident response readiness.
- Conducted real-time security data analysis using Splunk (SPL queries and dashboards) and performed vulnerability scanning with Nmap and Qualys, identifying critical exposures, including an unpatched zero-day in the SMTP service.
- Exploited identified vulnerabilities using **Metasploit** to demonstrate attack paths from initial compromise to privilege escalation, documented findings, recommended prioritized remediation strategies, and delivered executive reports resulting in a 40% reduction in attack surface.

CERTIFICATIONS

- CompTIA Security+ 701(IAT level II) | Issued: March 2025
- Vulnerability Management Detection and Response from Qualys | Issued: June 2025
- Certified Email Authentication Specialist from Proofpoint | Issued: July 2025
- BTL 1| Issued: September 2025
- SC-200| Expected by December 2025

KEY ACHIEVEMENTS, LEADERSHIP EXPERIENCE & ACTIVITIES

- Ranked in the **Top 2.9% (26/8,482)** in the individual game and **Top 21% (113/534)** in the team game at the **NCL 2023 CTF competition**.
- Earned a **Top 5% Global Ranking on TryHackMe**, completing hands-on labs in penetration testing, threat hunting, and SOC analysis.
- Served as **Vice President of the WiCyS SLU Student Chapter**, leading initiatives for women in cybersecurity and organizing professional events.
- Participated in **Capture the Flag (CTF) competitions** and collaborated on cybersecurity challenges as a member of the **Cyber Billiken CTF Club**.

EDUCATION

Saint Louis University — May 2025
MS Cyber Security — **GPA: 3.97/4**
Sri Venkateswara Engineering College for Women — June 2021
Bachelor of Technology in Computer Science and Engineering