Chaitanya Vilas Garware

Cybersecurity Analyst • SOC Analyst • SIEM & Threat Detection
Birmingham, AL • +1-205-747-6214 • chaitanyagarware7@gmail.com • LinkedIn • GitHub

Summary

Cybersecurity Analyst with hands-on SOC, SIEM, and AI security experience, including building and publishing OpenSOC-AI, a fine-tuned LLM for automated MITRE ATT&CK threat classification (arXiv: 2604.26217). Internship experience at Palo Alto Networks and AWS. TryHackMe Top 1% globally. Skilled in Splunk, QRadar, Snort, Suricata, Python, MITRE ATT&CK, NIST, ISO 27001, HIPAA, and SOC 2.

Work Experience

University of Alabama at Birmingham — Birmingham, AL
Graduate Teaching Assistant, Computer Networks (CS 334/534) — *Jan 2026 – May 2026*

- Led hands-on network security labs for 80+ students by teaching TCP/IP, Linux administration, packet analysis, network configuration, and troubleshooting workflows.
- Improved student lab performance by 27% by coaching Python scripting, secure Linux configuration, Wireshark analysis, and network diagnostics during lab sessions.

Medlaunch Concepts – Healthcare IT Security Startup — Florida, FL
Cybersecurity Specialist — *Sep 2025 – Dec 2025*

- Reduced mean time to detect threats by 45% by designing real-time SIEM dashboards and alerting workflows in Splunk and QRadar across healthcare security environments.
- Supported remediation of 30+ critical vulnerabilities by executing ISO 27001 and HITRUST security assessments, identifying control gaps, and validating security fixes.
- Improved audit readiness by maintaining 100% control mapping against documented compliance requirements and prioritizing risk-based vulnerability remediation.

Palo Alto Networks – AICTE — Pune, India
Cybersecurity Intern — *May 2023 – Jul 2023*

- Increased IDS detection coverage by 70% and reduced false positives by 20% by deploying and tuning Snort and Suricata rules across live network environments.
- Validated remediation for 15+ critical vulnerabilities by performing 5+ vulnerability assessments and penetration tests using Kali Linux and Nmap.
- Improved alert fidelity and incident triage workflows by analyzing packet captures, network traffic, and attack patterns to refine detection logic.

AWS Academy – AICTE — Pune, India
Data Analytics Intern — *Dec 2022 – Feb 2023*

- Improved cloud security visibility across access patterns and compliance gaps by analyzing 47+ GB of security logs using AWS Athena and Amazon Redshift.
- Accelerated security event monitoring by developing Amazon QuickSight dashboards, increasing the detection rate of critical operational risk indicators by 25%.
- Reduced security log analysis runtime by 40% by streamlining processing and reporting workflows using Python and Bash automation.

Projects

OpenSOC-AI | *AI-Powered SOC Automation* | *arXiv* | *TinyLlama-1.1B, QLoRA, Splunk SIEM, MITRE ATT&CK*

- Reduced manual SOC log triage by converting raw security logs into MITRE ATT&CK mappings, severity labels, threat categories, and analyst-ready summaries.
- Generated structured threat intelligence in under 2 seconds per log across 10 MITRE ATT&CK categories by fine-tuning TinyLlama-1.1B with QLoRA and Splunk SIEM integration.
- Achieved 68% classification accuracy and 0.68 F1-score on a 50-sample evaluation set, a 68-point F1 improvement over the zero-shot baseline, published on arXiv (2604.26217).

Quantum-Safe Password Manager | *Kyber Encryption, Secure Authentication, Encrypted Credential Storage*

- Eliminated classical encryption exposure by building and deploying a post-quantum password manager using Kyber encryption, risk-based authentication, and NIST/ISO 27001-aligned safeguards.

Skills

Security Operations: SOC Operations, Security Monitoring, Alert Triage, Log Analysis, Incident Response, Incident Handling
SOC Automation: SOAR, Security Orchestration, Playbooks, Incident Response Automation, Automation Frameworks, Threat Intelligence, Threat Hunting
SIEM & Detection: Splunk, QRadar, ELK, IDS/IPS, Snort, Suricata, Detection Rules, Alert Tuning, Use Case Development, Risk Management
Vulnerability Management: Vulnerability Assessment, Vulnerability Scanning, Penetration Testing, Kali Linux, Nmap, Risk Assessment, Remediation Validation
Cloud & Endpoint: AWS Athena, Amazon Redshift, Amazon QuickSight, EDR, XDR, CrowdStrike, SentinelOne
Scripting & Frameworks: Python, Bash, PowerShell, Linux, Networking, MITRE ATT&CK, NIST, ISO 27001, HIPAA, SOC 2

Certifications & Achievements

CompTIA Security+ • Certified SOC Analyst • ISO/IEC 27001 Information Security Associate • TryHackMe Top 1% Globally • Southeast Cybersecurity Summit CTF: 2nd Place Team, Top Individual Contributor

Education

University of Alabama at Birmingham, Birmingham, AL — Aug 2024 – May 2026
Master of Science in Cybersecurity, GPA: 4.0/4.0

AISSMS Institute of Information Technology, Pune, India — Aug 2020 – May 2024
Bachelor of Engineering in Computer Engineering, GPA: 4.0/4.0