SAI MANIKANTA TEJA PARWATHA

(989) 824-6552 · tejaparwatha@gmail.com ·
linkedin.com/in/tejaparwatha/ · https://tejaparwatha.me · github.com/t3ja-parw4tha

CompTIA Security+ · M.S. Information Systems (Cybersecurity), Central Michigan University

PROFESSIONAL SUMMARY

Security Analyst with 5+ years of experience across SOC operations, cloud security engineering, detection engineering, vulnerability management, and compliance in government, healthcare, and enterprise environments. Deep expertise in Microsoft Sentinel SIEM, Azure (Commercial & Government), Microsoft Defender for Cloud, KQL detection engineering, and HIPAA/NIST 800-53/SOC 2 compliance. Proven ability to reduce risk exposure, operationalize detection at scale, and deliver security-by-design in regulated cloud environments. Builder of KESTREL an open-source AI-assisted SOC triage platform demonstrating end-to-end detection engineering, MITRE ATT&CK integration, and LLM-powered alert analysis.

CORE SKILLS

SOC & SIEM Operations: Microsoft Sentinel, Log Analytics, KQL, Detection Engineering, Threat Hunting, Incident Response, Alert Tuning, MITRE ATT&CK

Cloud & Endpoint Security: Azure Commercial & Government, Microsoft Defender for Cloud/Endpoint/Network, Azure Key Vault, Managed Identities, ADLS Gen2, Intune, Azure Policy, IAM, DLP, WAF

Network & Infrastructure Security: IDS/IPS (Snort, Suricata), Firewalls, VPNs, TCP/IP, DNS Security, Network Segmentation

Vulnerability Management & AppSec: Tenable, Nessus, Qualys, Burp Suite, OWASP ZAP, SAST/DAST, SCA (pip-audit, Snyk), Container Scanning (Trivy), Web & API Security Testing

GRC & Compliance: HIPAA, NIST 800-53, SOC 2, PCI DSS, Risk Registers, System Security Plans (SSPs), Audit Evidence, Control Mapping

Automation & Scripting: Python, Bash, PowerShell, PySpark, FastAPI, SQLAlchemy, Security Automation, Log Parsing, CI/CD (GitHub Actions)

AI & Security Engineering: LLM triage integration (OpenAI, Anthropic Claude), Prompt injection risk, PHI-safe AI patterns, DevSecOps pipeline design

CERTIFICATIONS

- **CompTIA Security+**
- **Microsoft Certified: Security Operations Analyst Associate (SC-200)**

SECURITY ENGINEERING PROJECTS

KESTREL - AI-Assisted SOC Triage & Detection Engineering Platform *(github.com/t3ja-parw4tha/KESTREL)*

Personal Security Engineering Project · FastAPI · React · MITRE ATT&CK · OpenAI/Anthropic · Docker · Prometheus

- Designed and built **KESTREL**, an AI-assisted SOC platform ingesting alerts from 8 security telemetry sources including Sentinel, GuardDuty, Defender, Suricata, Zeek, and Syslog into a normalized alert pipeline.
- Engineered multi-factor risk scoring (0–100) combining alert severity, asset criticality, CVSS scores, threat intelligence (VirusTotal, AbuseIPDB), and historical correlation to automate SOC alert prioritization.
- Implemented automatic MITRE ATT&CK technique mapping on every ingested alert using category, alert type, source signals, and raw field inspection across all 12 ATT&CK tactics, with a real-time detection coverage gap analysis heatmap
- Integrated OpenAI GPT and Anthropic Claude triage layer generating alert summaries, key facts, remediation steps, and recommended next actions per alert with graceful rule-based fallback

- Built alert correlation engine grouping events by shared source IP, username, and asset ID into incident threads with automatic group ID assignment; implemented automated playbooks for brute force, exfiltration, and malware response scenarios
- Architected security-hardened backend: JWT RS256 asymmetric signing, argon2id password hashing, 4-tier RBAC (admin/senior analyst/analyst/viewer), progressive account lockout, per-IP rate limiting, CSP/HSTS headers, and full audit logging
- Implemented end-to-end DevSecOps CI/CD pipeline: SAST (Bandit, Semgrep OWASP Top 10), SCA (pip-audit, npm audit), container CVE scanning (Trivy → SARIF to GitHub Security tab), secret scanning (TruffleHog), and Dependabot automated dependency management
- Deployed observability stack with Prometheus metrics, Grafana SOC dashboard, OpenTelemetry tracing, and structured JSON logging with correlation IDs for full request traceability across the platform

PROFESSIONAL EXPERIENCE

Security Analyst

Nov 2025 – Present

Vanvi Technologies LLC (UnitedHealth Group)

- Designed and implemented HIPAA-aligned security controls for Azure-hosted healthcare platforms handling PHI, enforcing least privilege, auditability, and secure data handling across dev/test/prod environments
- Monitored and investigated security alerts across Microsoft Sentinel SIEM including identity anomalies, suspicious authentication activity, and abnormal PHI data access patterns in Azure-hosted healthcare environments
- Performed threat hunting using KQL queries across Azure logs, Defender telemetry, and identity data to identify lateral movement, privilege escalation, and anomalous account activity
- Tuned SIEM analytics rules and alert thresholds to reduce false positives and improve signal quality for SOC analysts
- Investigated and triaged security incidents involving suspicious login, policy violations, and abnormal storage access within regulated healthcare environments
- Correlated alerts across Microsoft Defender, Azure Activity Logs, and network telemetry to identify potential security incidents and determine root causes
- Supported secure SDLC initiatives by reviewing application deployment configurations, validating security controls, and ensuring adherence to organizational security standards.
- Assisted in security hardening of Azure resources, reviewing storage access policies, encryption configurations, and network security group rules to minimize attack surface.
- Supported vulnerability management by triaging findings from Defender for Cloud and Tenable scans and coordinating remediation with engineering teams
- Assisted compliance and audit teams by maintaining evidence of logging, monitoring, and access controls aligned to HIPAA and NIST 800-53 requirements
- Developed Python and KQL automation scripts to streamline alert enrichment and improve incident triage efficiency within SOC workflows

Associate Security Analyst

Jun 2024 – Oct 2025

RiceFW Technologies Inc. (State of Michigan)

- Designed and maintained Microsoft Sentinel SIEM environments, configuring log ingestion pipelines, KQL-based analytics rules, and alert workflows for SOC operations supporting Michigan government infrastructure
- Engineered KQL detections to identify lateral movement, privilege escalation, and anomalous authentication behavior across cloud and hybrid environments; tuned rules to reduce false positive rates and improve signal fidelity
- Implemented and hardened Microsoft Intune endpoint security and compliance policies, reducing endpoint risk exposure across government-managed device fleet
- Investigated suspicious network activity and security alerts by reviewing firewall logs and network telemetry, identifying potential intrusion attempts and abnormal traffic patterns.
- Deployed Tailscale mesh VPN network to enable encrypted peer-to-peer connectivity between internal systems, improving secure access management and reducing reliance on traditional perimeter VPN infrastructure.
- Supported identity and access management (IAM) security controls through Microsoft Entra ID, enforcing least-privilege access and monitoring privileged account activity.

- Contributed to an AI-assisted internal security portal aggregating logs from cloud, endpoint, network, and IDS/IPS sources (Snort, Suricata) into ticket-driven SOC workflows.
- Integrated Microsoft Defender telemetry with Sentinel SIEM for centralized threat monitoring; applied threat modeling and secure architecture practices to cloud-native logging and telemetry ingestion services
- Conducted vulnerability scanning and penetration testing using Tenable, Nessus, Burp Suite, and OWASP ZAP; validated exploitability and tracked remediation to closure
- Built and maintained enterprise risk registers aligned with NIST 800-53; authored System Security Plans (SSPs) and compliance documentation supporting SOC 2 and government security assessments
- Secured Azure Government and Commercial environments enforcing IAM, logging, encryption, and policy compliance; automated security monitoring and reporting workflows using Python, Bash, and PySpark
- Contributed to employee security awareness initiatives using KnowBe4 to improve phishing awareness and security training participation.

Security Analyst Intern

Jun 2022 – Nov 2022

Genzeon Technologies

- Performed penetration testing and vulnerability assessments for healthcare and dental applications handling ePHI and regulated data under HIPAA and PCI DSS requirements
- Conducted credentialed vulnerability scans using Qualys and Nessus across Windows, Linux, and database systems; identified high-risk issues including weak authentication, insecure session management, misconfigurations, and injection flaws
- Validated remediation effectiveness through repeat testing and exploit validation; produced executive-level security reports translating technical findings into compliance posture and business risk exposure
- Automated security validation and re-testing workflows using Python and Bash, improving assessment efficiency and consistency across engagements

Support Analyst

Apr 2021 – Jun 2022

Amazon Development Center

- Investigated seller account security incidents involving authentication abuse, phishing, and credential stuffing; analyzed login activity and abuse patterns to identify unauthorized access and fraud risk
- Collaborated with risk, fraud, and engineering teams to strengthen seller authentication controls and account protection workflows; authored security-focused process documentation to improve incident handling consistency

EDUCATION

M.S. in Information Systems (Cybersecurity Concentration) 2024

Central Michigan University

Bachelor's in engineering 2020

Kakatiya Institute of Technology and Science

SECURITY RESEARCH & COMMUNITY

Government of India Responsible Disclosure Program – Recognized Contributor

Active on Hack The Box, TryHackMe, Bugcrowd, and HackerOne