SHUBHAM MANE

Cybersecurity & AI Engineer · Senior Security Operations

Chicago, IL • shubhammane56@gmail.com • +1 315-539-9755 • linkedin.com/in/shubhm-mane • github.com/Shubhmane9503

PROFESSIONAL SUMMARY

Senior security engineer with **7+ years** defending enterprise environments and acting as the primary technical escalation point for complex incidents. Specializes in advanced threat detection & response, proactive threat hunting with the MITRE ATT&CK framework, and deep-dive digital forensics — backed by mastery of SIEM / EDR / XDR platforms, custom detection engineering, and automated SOAR playbooks. Also builds production AI & automation systems (Python, n8n, browser automation, LLM APIs) that ship real workflows end to end.

TECHNICAL SKILLS

Detection & Response	Splunk Enterprise Security, Microsoft Sentinel (KQL/SPL), CrowdStrike Falcon, SIEM/EDR/XDR, SOAR (Phantom, Demisto), MITRE ATT&CK
Threat Hunting / DFIR	Hypothesis-based hunting, Volatility, Rekall, FTK Imager, memory analysis, incident response (NIST 800-61), threat intel & IOC enrichment
Assessment	Nmap, Nessus, Metasploit, Burp Suite, OWASP ZAP, Qualys, purple teaming, vulnerability management
Cloud & Identity	Azure (Sentinel, Key Vault, Defender for Cloud), AWS, Active Directory / Entra ID, IAM & access control, OAuth2
AI & Automation	Python, n8n (self-hosted), Playwright, Anthropic Claude API, Google Gemini, Telegram bots, ffmpeg / edge-tts, Railway, SQL, PowerShell

PROFESSIONAL EXPERIENCE

Senior Information Security & Risk Analyst — Rigelsky, Inc.

Sep 2021 – Present

- Architected an enterprise SIEM correlation framework (Splunk ES) across five data centers processing **15TB of daily logs**, reducing MTTR **45%** and preventing an estimated **$2.3M** in annual incident losses.
- Served as primary technical escalation point for advanced persistent threats targeting **Azure & AWS** cloud infrastructure; led 15+ critical incident responses annually, cutting average containment from 8h to **1.5h** and preventing ~$1.5M in revenue loss.
- Developed **40+ custom Splunk correlation searches** and high-fidelity Microsoft Sentinel KQL detections mapping 15 TTPs across 2M daily events — increasing detection rate **60%** while reducing false positives **35%**.
- Built a proactive threat-hunting program (20+ hypothesis-based hunts/quarter using CrowdStrike Falcon + MITRE ATT&CK), identifying five adversary techniques that bypassed automated detection.
- Automated triage & containment with Python and SOAR playbooks, saving the Tier-1 team **200+ hours/month** and improving SLA adherence 40%.
- Managed EDR policy lifecycle across **5,000+ endpoints** (CrowdStrike Falcon) at 99.9% coverage, and led detection-engineering CI/CD that improved time-to-detection for zero-days **70%**.

Information Security Engineer — Infosys Ltd.

Jun 2018 – Aug 2021

- Deployed Network Detection & Response (NDR) sensors and integrated flow data into Sentinel for lateral-movement detection, protecting **$10M** of critical infrastructure.
- Hardened privileged Active Directory / Entra ID accounts with custom alerting, reducing credential-theft exposure from 24h to **30 minutes**.
- Led integration of a Threat Intelligence Platform that enriched **100%** of incoming events with IOC context; authored monthly threat-landscape reporting that influenced executive resource allocation.
- Developed PowerShell detection logic for registry tampering and process-injection, improving early detection of fileless malware.

SELECTED PROJECTS

IntelliApply — Resume & Job-Search SaaS
Automated resume generation and job-application assistance built on n8n, Playwright, and the Anthropic API.

AI Content Automation Pipeline — Multi-Platform, Zero-Touch
Fully autonomous content engine publishing to YouTube, Instagram, TikTok & Threads — generation, voiceover, edit and publish, orchestrated via n8n and controlled from Telegram (Grok, edge-tts, ffmpeg, CapCut).

n8n Automation Suite — Internal Tooling & Bots
Production automations including a Teams–Jira integration bot (OAuth, SQL state, Azure Key Vault, Gemini NLP) and a Railway-hosted Telegram/Gmail job-alert bot.

CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- AWS Certified Solutions Architect – Associate
- CompTIA Security+

EDUCATION

M.S. Cyber Security
DePaul University · 2021

B.E. Computer Science
D.Y. Patil Institute of Technology · 2017