Hemanth Kori

RSOC Operator · Detection Engineer · Dublin, Ireland

hemanthkori007@gmail.com · https://www.linkedin.com/in/hemanthkori · https://github.com/hemanthkori · https://medium.com/@hemanthkori

Summary

RSOC Operator at Synopsys covering the EMEA region — triaging 800+ alerts a shift across SIEM, CCTV/VMS and access control, and building the detections, dashboards and pipelines that explain them. Published time-series researcher. CompTIA Security+ (in progress).

Skills

SIEM Triage (Splunk / Sentinel)	92%
Incident Response	90%
MITRE ATT&CK Mapping	88%
Detection Engineering (KQL)	85%
Threat Hunting	82%
CCTV / VMS / Access Control	80%
Log Analysis & Correlation	86%
Python / SQL Pipelines	84%
Power BI / Tableau	83%
OWASP / Vuln Assessment	74%

Detection Engineering

• Brute-Force Authentication (T1110) — live: 11,970 failed logons against a single account on one host within minutes.

• Impossible Travel (T1078) — live: Same account signs in from Dublin then Lagos 35 minutes later — implied 9,051 km/h.

• Privileged Activity — Out of Hours (T1078.003) — tuning: Time-based rule returned zero rows — collector was stamping ingest time, not event time.

• Phishing Email Triage Scorer (T1566) — blueprint: CLI that scores auth, sender identity, payload and language on a suspicious .eml and shows its reasoning.

• DMARC Policy Drift Watch (T1595) — blueprint: Incident root cause was a parked p=none DMARC policy letting failed-SPF mail through.

Selected Work

• Microsoft Sentinel Detection Lab — Detection Engineering. Three KQL analytics rules mapped to MITRE ATT&CK with false-positive tuning notes and investigation runbooks.

• Phishing Incident Response Write-up — IR Case Study. End-to-end build of a click-to-C2 scenario: timeline, execution chain, IOCs, ATT&CK mapping and containment actions.

• Beacon Hunter — Threat Hunting. Tooling to surface C2 beaconing behaviour from network logs using jitter and periodicity analysis.

• Sigma Forge — Detection-as-Code. A pipeline that converts hunting hypotheses into Sigma rules and ships them to a SIEM-backed lab.

• CO, Time-Series Forecasting— Research. SARIMA model for atmospheric CO, concentration forecasting. MAE < 1 ppm. Published on Zenodo with DOI.

• VPN Anomaly Detection — ML Security. Anomaly detection on VPN connection telemetry to flag impossible travel and credential abuse patterns.

Experience

• 2025— — RSOC Operator · Synopsys: 24/7 Regional SOC covering EMEA — SIEM, CCTV/VMS (Genetec/Milestone), access control (C•CURE 9000), ServiceNow, Everbridge.

• 2024 — Operations Manager · Appache Food & Health: Led a 10+ team; cut waste 15% and lifted efficiency 20% with Excel/SQL + Power BI dashboards.

• 2023 — Data Research Analyst · upGrad: ARIMA/SARIMA forecasting, credit-risk and ride-share demand models; published CO, research (DOI).

• 2022 — SOC Analyst Intern · Targe Cyberspace: SIEM monitoring, phishing/malware analysis, vulnerability assessment aligned to OWASP.

• 2021 — VAPT Trainee: Specialised training in vulnerability assessment, penetration testing and OWASP Top 10.