Sagar Kishore Kumar

Saarbrücken, Germany | sagarkishore.7@gmail.com | +49 17625005604 | GitHub | LinkedIn

Threat Intelligence • Detection Engineering • Cloud Security • Security Automation

Overview

Cybersecurity engineer with 3 years of experience across threat intelligence, detection engineering, and security automation at production scale. Skilled in OSINT and MITRE ATT&CK-driven CTI, SIEM-based threat hunting and incident triage (Elasticsearch/OpenSearch), and cloud security risk assessment (STRIDE, NIST SP 800-30, ISO 27005). Builds automated, AI-assisted security pipelines in Python across environments handling up to 4 billion emails/week.

Technical Skills

Cloud Security & GRC: GCP security architecture, IAM, Workload Identity Federation, IAP, secrets management, threat modeling (STRIDE), risk assessment (NIST SP 800-30, ISO 27005), CI/CD & supply-chain security, security controls design, SLSA provenance

SIEM & Detection Engineering: Elasticsearch / OpenSearch / Kibana (dashboards, alerting, investigation, rule tuning), threat hunting, incident triage, log & telemetry analysis, detections-as-code, playbook authoring, Prometheus, Grafana

Threat Intelligence & CTI: OSINT collection & enrichment, MITRE ATT&CK mapping (TTPs, tactic heatmaps), IOC analysis (IP, domain, hash, CVE), threat actor attribution, ransomware tracking, Cyber Kill Chain, intelligence reporting

AI & LLM Security: LLM-driven classification & clustering, prompt injection testing (OWASP LLM Top 10), RAG pipelines, NER (BERT, GLiNER), grammar-constrained extraction (GBNF), AI-assisted triage

Automation & Development: Python (FastAPI, Flask, pandas, asyncio, TensorFlow), API integrations, event-driven automation, Bash, SQLite, Postgres, Docker, Git, CI/CD (GitHub Actions, SARIF)

Tooling & Networking: Burp Suite, Nmap, OWASP ZAP, Wireshark, nuclei, subfinder, httpx; TCP/IP, DNS, TLS, Firewalls, IDS/IPS, Linux

Professional Experience

Cyber Threat Intelligence Researcher (Master's Thesis) *Oct 2024 – Oct 2025*
CISPA Helmholtz Center for Information Security, Saarbrücken

- Built a fully automated 16-source OSINT ingestion pipeline (Ransomware.live, CISA, international CERTs) accumulating 4,231 incidents across 53 countries, with fuzzy deduplication and incremental source-state tracking.
- Automated MITRE ATT&CK mapping via semantic RAG (697 techniques embedded, top-5 candidates per article), yielding 512 technique observations across 14 tactics with no manual tagging.
- Designed a 105-field grammar-constrained LLM extraction schema (GBNF) with GLiNER NER pre-pass and Pydantic-validated self-correction; 67% enrichment coverage across 2,847 incidents.
- Built a 14-table intelligence database with an 8-type IOC schema and ∼50 FastAPI endpoints powering an interactive dashboard with tactic heatmaps and sector-targeting matrices.

Email Security Analyst, NGSF Team *Jan 2023 – Aug 2025*
1&1 Mail & Media SE, Karlsruhe

- Built and maintained LLM-driven classification pipelines for spam and phishing detection processing ∼350K emails/day on infrastructure handling ∼4 billion emails/week; tuned detection rules and alert thresholds against evolving campaigns.
- Performed large-scale threat hunting and telemetry analysis in Elasticsearch/OpenSearch; built Python automation for threat enrichment, incident triage, and operational response.
- Engineered a brand-impersonation detection system combining ML models, embeddings (RETVec), and BERT-based NER via OpenSearch pipelines across IONOS, GMX, and WEB.DE user bases.
- Contributed to detections-as-code: automated rule deployment, version-controlled alerting logic, and structured telemetry pipelines across email security infrastructure.

Test Development Engineer *Nov 2020 – Sep 2021*
Wipro Limited, Bangalore

- Built automated test and data-validation frameworks for enterprise cloud applications (.NET/MSSQL), cutting manual QA cycles by 25% and surfacing data-integrity anomalies for triage.
- Documented technical findings and reproduced edge-case failures for cross-functional teams, reducing defect investigation turnaround.

Education

M.Sc. Cybersecurity (Grade: 2.0) *Oct 2021 – Oct 2025*
Universität des Saarlandes, Saarbrücken

- Coursework: Data Networks, Web Application Penetration Testing, Cryptography, IT Forensics, Physical Layer Security, Industrial Control System Security, Security Testing, Automated Debugging

Projects

Cloud Migration Security Assessment – *Self-directed case study* *GCP, STRIDE, NIST*

- Designed an end-to-end security risk assessment for migrating a self-hosted GitLab environment to Google Cloud: STRIDE threat modeling and NIST SP 800-30 / ISO 27005 rating across 18 risk scenarios on a 5x5 likelihood-impact matrix.
- Identified critical risks (access-token and long-lived service-account key exposure) with remediation via short-lived credentials and Workload Identity Federation; produced a five-layer reference architecture (landing zone, identity, secrets, pipeline/supply-chain, detection) with IAP, FIDO2 MFA, and SLSA provenance, and ATT&CK-mapped detections.

EduThreat-CTI – Education Sector Threat Intelligence (GitHub) (Dashboard) *Python, LLMs, FastAPI*

- Built an end-to-end automated OSINT threat-intelligence platform for the education sector: 15-source ingestion distilling 124,676 raw observations into 2,967 verified incidents across 91 countries (2000–2026) via LLM enrichment and deterministic multi-signal canonicalization; served through a 73-endpoint FastAPI REST API and a Next.js analytics dashboard.
- Engineered schema-constrained LLM extraction into a 132-field CTI schema (MITRE ATT&CK, threat actors, ransomware families, supply-chain vendors, impact/disclosure) using Qwen3-Coder (480B) at temperature 0 with GLiNER NER and sentence-transformer ATT&CK retrieval; blind expert validation confirmed 91% accuracy on ransomware-vs-rest classification and 7% median error on affected-record counts.
- Ran a large-scale measurement study identifying ransomware as the dominant threat (∼40% of incidents, peaking at 52% in 2025) and quantifying supply-chain amplification: a single vendor breach (MOVEit) cascaded to 93 institutions, and vendor breaches carried 2.7× the median records, under extreme geographic concentration (Gini 0.85; US 53%).
- Designed a deterministic, auditable campaign-correlation layer and threat knowledge graph linking 213 threat actors, CVEs, and vendors across incidents to surface coordinated campaigns invisible at the single-incident level; findings drove sector-specific detection and disclosure-transparency priorities.

LLMMap – Prompt Injection Testing Framework (GitHub) (Demo) *Python, FastAPI, LLMs*

- Dual-LLM attack-and-judge architecture covering 227 prompt injection techniques across 18 attack families, with SARIF v2.1.0 export for CI/CD security integration.
- Built PromptLab, a companion AI security lab with OWASP LLM Top 10 classification and vulnerable/defended simulation across Ollama, OpenAI, Anthropic, and Google backends.

WRX – Web Recon eXecutive (GitHub) *Python, Automation*

- Security automation orchestrator unifying subfinder, httpx, katana, ffuf, nuclei, and OWASP ZAP; async job monitoring, run diffing, and export connectors for SARIF, GitHub, and Jira aligned with detections-as-code.

Publications

Localization of Eyes using HAAR Cascade Classifiers – TEST Magazine (May 2020) (Paper)

Languages

English (C1) • German (A2)