Sanket Taware

SOC Analyst | Security Engineer | Threat Detection

+91 7218099435 | sankettawarework@gmail.com | linkedin.com/in/sanket-taware | github.com/sankettaware16

Summary

Security Engineer with 1+ year of hands-on experience building and operating a live **SIEM** pipeline in a production SOC environment at IIT Bombay. Skilled in **security monitoring**, log analysis, and **detection engineering** using **Apache Kafka**, **ELK Stack**, and **Python**. Experienced in **threat intelligence** integration, **incident response**, and **MITRE ATT&CK** mapping. Familiar with **Splunk**, **Microsoft Sentinel**, and **QRadar** workflows through strong SIEM query and log analysis foundations.

Experience

Security Engineer — Lead SOC Architect Nov 2024 – Present

TrustLab, IIT Bombay *Mumbai, Maharashtra*

- Engineered and deployed a production-grade, agentless **SIEM pipeline** using **Apache Kafka** and the **ELK Stack**, ingesting and processing **1M+ log events per day** from web, mail, and proxy infrastructure across the IIT Bombay CSE Department
- Wrote scalable, YAML-driven **Python parsers** with custom **Regex** patterns to handle complex, non-standard log formats from NGINX, Apache, and Postfix, reducing ingestion errors by **40%** and improving correlation rule accuracy
- Designed and trained **ML-based anomaly detection** models (Isolation Forest) to identify low-and-slow brute force attacks and credential leaks, catching **15+ attack patterns** missed entirely by signature-based tools
- Integrated **MISP** threat intelligence platform with the SIEM to enrich alerts with real-time IOCs, improving alert fidelity and reducing **false positives by 30%** across detection pipelines
- Managed full lifecycle of SOC infrastructure on **Proxmox VE**, deploying, hardening, and maintaining **5+ Ubuntu servers** achieving **99.9% uptime** for all monitoring and detection services
- Built a custom **Python attack simulation framework** to generate DDoS, SQLi, and Brute Force traffic against the SIEM, validating **100% of detection rules** in staging before production deployment
- Developed and mapped **20+ MITRE ATT&CK-aligned** correlation rules in Kibana, reducing mean time to detect (MTTD) for known attack patterns by **50%**
- Led and mentored a team of **7–8 cybersecurity interns**, conducting weekly code reviews for detection logic and overseeing log analysis workflows aligned with SOC objectives
- Selected as co-presenter at **RISC 2025** and **TrustSummit** to demonstrate the custom SOC architecture and ML detection capabilities to industry and academic researchers

Projects

FOSS SOC Engine (TrustLab, IIT Bombay) | *Python, Kafka, Redis, Elasticsearch, YAML, GeoIP* | GitHub2024 – Present

- Designed and built a production **log parsing and normalization engine** that consumes raw logs from **Apache Kafka**, dynamically routes each log to the correct parser, and outputs **ECS-compliant JSON** into Elasticsearch – deployed live at IIT Bombay to process **1M+ log events per day**
- Implemented **4 hybrid parsing strategies** in YAML-driven rules – stateless regex, multi-match, stateful multi-line reassembly (Redis-backed), and JSON field mapping – supporting NGINX, Apache, Postfix, ModSecurity, and Linux auth logs with zero code changes per new source
- Built a **Dead Letter Queue (DLQ)** to capture 100% of unparsed logs for forensic review, and integrated **MaxMind GeoIP enrichment** to annotate every alert with attacker geolocation metadata automatically
- Engine emits real-time health metrics (EPS, error rate, uptime) every 60 seconds, enabling direct ingestion by Filebeat or Wazuh agents into the central **SIEM dashboard** for SOC monitoring

TLSOCDockerDeploy (TrustLab, IIT Bombay) | *Docker Compose, ELK Stack, Kafka, TLS, Shell* | GitHub 2024

- Built a one-command, **TLS-secured SOC deployment stack** (Kafka + Logstash + Elasticsearch + Kibana) using Docker Compose for fresh Ubuntu servers, reducing full SOC stack deployment from days to **under 30 minutes**
- Hardened all internal service communication with **end-to-end TLS encryption** using a locally generated CA, protecting the log pipeline against interception in shared and cloud environments

ML Anomaly Detection Engine (TrustLab, IIT Bombay) | *Python, Scikit-learn, Isolation Forest, ELK Stack* 2024

- Designed and trained a custom **Isolation Forest** model integrated directly into the SIEM log pipeline to detect behavioral anomalies such as low-and-slow brute force attacks and credential stuffing at scale
- Reduced false positive alert rate by **30%** compared to baseline signature rules, directly improving SOC analyst efficiency and decreasing alert fatigue across the IIT Bombay monitoring environment

LLMGuard (Personal) | *JavaScript, Chrome Extension, Regex, Manifest v3* | GitHub 2025

- Built a **browser security extension** that performs real-time scanning of user input on LLM platforms (ChatGPT, Gemini, Claude, Copilot) to detect and block accidental leakage of **30+ secret types** – API keys, AWS credentials, JWTs, private keys, and DB connection strings – before they reach the model
- Implemented **Shadow DOM-isolated blocking modals** with severity badges (Critical/High), a full event log with timestamps, and an analytics dashboard with CSV export – fully local, zero external dependencies, under 50KB

FOSS SOC Blueprint (Personal) | *SOC Architecture, Detection Engineering, ELK, Wazuh, Suricata, Zeek, MISP* | GitHub202

- Authored an open-source **practitioner guide** for building a complete SOC using free tools (ELK Stack, Wazuh, Suricata, Zeek, TheHive, MISP, Osquery), covering architecture design, log normalization, **detection rule engineering**, alert triage, incident response, and FOSS vs. commercial cost comparison

Technical Skills

SIEM & Detection: SIEM Architecture (Design & Build), ELK Stack (Elasticsearch, Logstash, Kibana), Apache Kafka, Wazuh, Splunk (Familiar), Microsoft Sentinel (Familiar), QRadar (Familiar)
Threat Detection: Detection Engineering, MITRE ATT&CK Mapping, Correlation Rule Development, Anomaly Detection (Isolation Forest), Alert Triage, Incident Response (IR), False Positive Reduction
Scripting & Automation: Python (Log Parsing, API Integration, ML), Bash Scripting, YAML, Regex, Grok Patterns
Threat Intelligence: MISP, IOC Enrichment, Threat Hunting, Log Analysis, SOC Operations
Infrastructure & DevOps: Linux (Ubuntu/Debian), Proxmox VE, System Hardening, NGINX, Apache, Docker, Git
Certifications (In Progress): CompTIA Security+ (Planned), Microsoft SC-200 (Planned)

Certifications & Training

Cyber Threat Management | *Cisco Networking Academy* 2023

Introduction to Cybersecurity | *Cisco Networking Academy* 2023

Cybersecurity Virtual Experience Program | *Mastercard — Social Engineering & Phishing Simulation* 2023

Cybersecurity Virtual Experience Program | *Commonwealth Bank — Fraud Detection & Cyber Investigation* 2023

Education

Sinhgad College of Science Pune, Maharashtra
Bachelor of Computer Application — CGPA: 8.26 *2020 – 2023*