Jeevanantham Kumarasamy

Dubai, Dubai, United Arab Emirates jeevakumar712@gmail.com +971504908187 in/jeevanantham-kumarasamy
jeevanantham-kumarasamy.netlify.app

SUMMARY

Highly skilled and detail-oriented Senior SOC Analyst with deep expertise in security operations, incident response, and threat detection. Proven track record in analyzing complex security incidents, conducting advanced digital forensics, and proactively hunting threats across enterprise environments. Adept in log analysis, SIEM management (Splunk, Sentinel, Elastic), and EDR solutions (Trellix, Cyberreason, Symantec). Experienced in malware analysis, memory and disk forensics, email and registry investigations, and leveraging tools like Volatility, FTK Imager, Magnet RAM Capture, and KAPE. Strong command of frameworks such as MITRE ATT&CK and Cyber Kill Chain, enabling strategic threat mitigation and root cause analysis. Demonstrates leadership in rule creation, alert fine-tuning, and vulnerability management, with a commitment to continuous improvement and staying ahead of evolving cyber threats.

EXPERIENCE

Senior Security Analyst

Coordinated Technology FZE **October 2023 - Present, Dubai, UAE**

- Cybersecurity-focused IT professional with 2+ years in **SOC environments**, having analyzed over **5,00+ security events** and alerts related to malware, phishing, and network intrusions.
- Proficient in **SIEM tools** such as Splunk and ELK, having monitored **100+ daily alerts** and reduced false positives by **20%** through rule refinement and enrichment.
- Conducted vulnerability assessments across **50+ endpoints and servers**, prioritizing and tracking remediation efforts with a **100% SLA compliance rate**.
- Performed **20+ incident response investigations** using FireEye HX and memory analysis tools, accelerating threat containment time by **30%**.
- Developed and implemented detection use cases that contributed to a **35% reduction in Mean Time to Detect (MTTD)** and **25% in Mean Time to Respond (MTTR)**.
- Analyzed **thousands of host and network logs** to identify indicators of compromise (IOCs), enabling early detection of lateral movement and privilege escalation attempts.

Security Analyst

Cyberproof **January 2022 - October 2023, Chennai, Tamilnadu, India**

- **Monitored and triaged 50+ daily security alerts** in a 24x7 SOC environment, identifying and escalating incidents per defined SLAs to ensure rapid containment and response.
- Performed **log analysis across IDS, firewalls, and endpoint tools**, contributing to the detection of lateral movement and privilege escalation attempts in multiple real-world incidents.
- Investigated and responded to **phishing attacks**, analyzing suspicious emails, domains, and URLs using open-source intelligence tools (VirusTotal, AbuseIPDB, URLscan), leading to a **40% increase in phishing detection accuracy**.
- Maintained and updated SIEM alerting logic and watchlists to improve detection fidelity, helping **reduce alert fatigue** for the SOC team by **30%**.
- Collaborated with senior analysts and threat intelligence teams to escalate **high-severity incidents** and provide enriched contextual data for response and reporting.
- Supported **daily health checks of security infrastructure** (EDR agents, log ingestion pipelines, threat feeds), ensuring system uptime and data integrity.

Junior Security Analyst

Ust Global **August 2021 - January 2022, Kochi, Kerala. India**

- **Monitored and analyzed** 30+ daily security events using SIEM tools like Splunk and ELK, identifying false positives and escalating true incidents to L2 analysts.
- Performed **basic malware analysis** on isolated virtual machines, identifying IOCs and sharing findings with incident response teams, reducing repeat alerts by 25%.
- Contributed to **24/7 SOC coverage**, collaborating across shifts to maintain security visibility and incident response readiness.
- Utilized open-source tools (e.g., Wireshark, CyberChef, VirusTotal) to assist in the investigation of suspicious URLs, IPs, and files, reducing analysis time by 30%.
- Maintained up-to-date knowledge of **emerging threats and TTPs**, correlating threat intel feeds with internal telemetry to enhance detection accuracy.
- Logged and documented incident handling steps in case management systems, ensuring clarity for audits and compliance.

EDUCATION

B.Tech

Minor in Information Technology • Sri Krishna College of Technology • Coimbatore, Tamilnadu, India • 2021 • 8.02

- Developed a strong interest in **Cybersecurity**, with a focus on **penetration testing**, **IoT security**, and **threat analysis** during academic studies.
- Completed a key project titled **"Intelligent Analysis for Drowsiness Alert"**, leveraging **Convolutional Neural Networks (CNNs)** to detect fatigue and trigger real-time alerts — blending AI, safety, and real-world application.
- Engaged in self-driven learning around **ethical hacking**, **network defense**, and **incident response fundamentals**, laying a solid foundation for a SOC Analyst career.

CERTIFICATIONS

Security Analyst (SAL1) Certificate

TryHackMe • 2025

Blue Team Level 1 (BTL1)

Security Blue Team • 2024

Certified AppSec Practitioner (CAP)

The SecOps Group • 2023

BlackPerl Certified Advanced Defender (BCAD)

BlackPerl DFIR • 2023

Malware Analyst & Incident Response

LetsDefend • 2023

SKILLS

Sentinel, Splunk,Elasticsearch,Cyberreason, Symantec, Wazuh, Opensearch, Kibana, FIreEye, Trellix, Win-event logs, Hayabusa, Kuiper, Cylr, Chainsaw, Deepbluecli, FTK Imager, Magnet RAM capture, Belkasoft X, Autopsy, Volatility, Redline, Photorec, HxD64, foremost, Magnet axiom, Scalpel, Recoverjpeg, Bulk extractor, AccessData, FTKImager, QphotoRec, Oletools, Exiftool, Email Header Analysis(EHA), Strings, Regshot, Registry Explorer, USBDViewer, Amcache, KAPE, Autopsy