JEEVANANTHAM KUMARASAMY

Senior Security Analyst

+971 504908187
jeevakumar712@gmail.com
LinkedIn
Netlify

JOB OBJECTIVE

Dynamic professional cultivated a proactive approach in the cybersecurity field, emphasizing security operations and incident response while effectively addressing threat detection and mitigation challenges within various enterprise settings. Targeting to leverage extensive experience in advanced digital forensics and security analysis.

EDUCATION

B.Tech. in Information Technology,
Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India, CGPA-8.02, 2021

CORE COMPETENCIES

Cybersecurity Operations

Incident Response Management

Threat Detection and Mitigation

Vulnerability Assessment Strategies

Security Information and Event Management (SIEM)

Firewall Management

Data Loss Prevention (DLP)

Root Cause Analysis (RCA)

Security Monitoring Frameworks

Risk Assessment and Management

Security Policy Development

Compliance and Regulatory Standards

Security Awareness Training

PROFILE SUMMARY

- Results-driven professional offering **nearly 4 years** of expertise in the cybersecurity sector, particularly in **Security Operations Centers (SOC),** showcasing a profound grasp of incident response, threat detection, and the management of security operations.
- Leading the role of **Senior Security Analyst at Coordinated Technology FZE**, overseeing the monitoring of security events, executing incident investigations, and devising impactful strategies for threat mitigation.
- Skilled in employing a **diverse array of cybersecurity tools and technologies**, such as SIEM solutions, EDR platforms, and vulnerability management systems, to guarantee thorough security coverage.
- Developed a strong foundation in cybersecurity through various roles, acquiring expertise in **log analysis, SIEM management, and advanced digital forensics**, while continuously enhancing skills in vulnerability management and threat hunting.
- Realized a notable **decrease in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)** by creating and executing cutting-edge detection use cases, reflecting a dedication to enhancing the overall security posture.
- Expertise in security frameworks like MITRE ATT&CK and Cyber Kill Chain, facilitating strategic planning and the implementation of security measures to combat emerging cyber threats.
- Proficient in leveraging advanced cybersecurity methodologies and tools, including **SIEM, EDR, and threat intelligence platforms**, to enhance organizational security posture and ensure rapid incident response.
- Showcased **outstanding analytical and problem-solving capabilities**, effectively guiding investigations into intricate security incidents while delivering actionable insights for effective threat mitigation.

WORK EXPERIENCE

Oct'2023 to Present: Senior Security Analyst at Coordinated Technology FZE, Dubai, UAE

Role:

- Spearheading the monitoring of security events and alerts, utilizing advanced SIEM tools to ensure comprehensive oversight of potential threats and vulnerabilities across the organization.
- Executing detailed incident response investigations, employing tools such as FireEye HX & memory analysis software to effectively contain & remediate security incidents.
- Conducting thorough vulnerability assessments on a diverse range of endpoints and servers, ensuring timely tracking and resolution of identified vulnerabilities while maintaining compliance with service level agreements (SLAs).
- Analyzing extensive logs from various sources to identify indicators of compromise (IOCs), facilitating early detection of potential security breaches and lateral movement within the network.
- Collaborating with cross-functional teams to develop and refine detection use cases, significantly enhancing the SOC's ability to respond to emerging threats.

Achievements:

- Analyzed over **5,000+ security events and alerts** related to malware, phishing, and network intrusions, ensuring timely threat detection and response.
- Monitored and triaged 100+ daily alerts using SIEM platforms like Splunk and ELK, and successfully reduced false positives by 20% by optimizing detection rules and enhancing log enrichment strategies.
- Executed vulnerability assessments across 50+ endpoints and servers, achieving 100% SLA compliance by effectively prioritizing risk and driving timely remediation in coordination with infrastructure teams.
- Led 20+ incident investigations utilizing tools such as FireEye HX and memory forensic utilities, which helped reduce threat containment time by 30%, enhancing overall SOC efficiency.

TECHNICAL SKILLS

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

- Designed and deployed custom detection use cases, contributing to a 35% improvement in Mean Time to Detect (MTTD) and a 25% reduction in Mean Time to Respond (MTTR), strengthening organizational cyber resilience.

Jan'2022 to Oct'2023: Security Analyst at Cyberproof, Chennai, Tamil Nadu, India

Role:

- Executed real-time assessment and classification of over 50 daily security alerts in a 24x7 SOC setup, ensuring swift incident escalation and containment in alignment with SLA timelines.
- Dissected log data from IDS, firewalls, and endpoint protection tools to uncover hidden patterns indicating lateral movement and unauthorized privilege elevation.
- Partnered with senior threat analysts and cyber intel units to investigate critical threats, enriching incident context and streamlining containment and reporting efforts.
- Ensured continuous operational integrity by conducting routine health checks across EDR agents, threat feeds, and log pipelines, maintaining high availability and data fidelity.

Achievements:

- Neutralized phishing threats by scrutinizing suspicious emails, domains, and URLs via tools such as VirusTotal, AbuseIPDB, and URLscan, resulting in a **40% uplift in detection precision.**
- Refined and optimized SIEM alert rules and detection logic, which led to **a 30% reduction in analyst alert fatigue** and increased actionable insights.

Aug 2021 - Jan 2022: Junior Security Analyst at Ust Global, Kochi, Kerala, India

Role:

- Analyzed and triaged 30+ daily security events using SIEM platforms such as Splunk and ELK, effectively filtering false positives and escalating genuine threats to L2 teams for rapid containment.
- Supported continuous SOC operations as part of a 24x7 coverage model, ensuring seamless shift transitions and sustained incident response readiness.
- Tracked and analyzed emerging threat trends and attacker TTPs, mapping external threat intelligence to internal telemetry to enhance detection precision.
- Documented incident response actions meticulously in case management platforms, ensuring transparency, traceability, and compliance with audit standards.

Achievements:

- Conducted initial malware assessments in isolated VM environments, uncovering indicators of compromise (IOCs) and sharing intelligence with incident response teams, **leading to a 25% reduction in recurring alerts.**
- Leveraged open-source analysis tools like Wireshark, CyberChef, and VirusTotal to investigate suspicious files, IP addresses, and URLs, **cutting average investigation time by 30%.**

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