


Jeevanantham Kumarasamy

Erode,Tamilnadu,India | jeevakumar712@gmail.com | +971-504908187

 <https://www.linkedin.com/in/jeevanantham-kumarasamy/>

Professional Summary

As an experienced Security Analyst, I bring extensive expertise in rapid incident response, malware analysis, and proactive threat hunting. I specialize in advanced DFIR techniques, conducting precise root cause analyses, and leveraging frameworks like the Cyber Kill Chain, MITRE ATT&CK, and APT knowledge to enhance system and network security through strategic mitigation. My work includes rule creation and fine-tuning in OpenSearch, monitoring in Kibana, and vulnerability management using tools such as FireEye-HX, Trellix, and McAfee.

I am proficient in USB, Registry, Memory, Mobile, and Cloud forensics (AWS, Azure) and dedicated to continuous learning to stay abreast of industry advancements. This ensures a comprehensive understanding of emerging threats and the implementation of effective, preemptive security measures to safeguard organizational assets.

Skills

DFIR | Endpoint & Network Logs Analysis | Memory forensics | Vulnerability Assessment and Pentesting | Disk Forensics | Phishing Expert | File carving | USB forensics | Threat Hunting | Malware Analysis | Mobile forensics

Tools Experience

SIEM & EDR - Sentinel, Splunk,Elasticsearch,Cyberreason, Symantec, Wazuh, Opensearch, Kibana, FlreEye, Trellix

Live Forensics - Win-event logs, Hayabusa, Kuiper, Cylr, Chainsaw, Deepbluecli

Disk,RAM acquisition and Analysis - FTK Imager, Magnet RAM capture, Belkasoft X, Autopsy, Volatility, Redline

File carving - Photorec, HxD64, foremost, Magnet axiom, Scalpel, Recoverjpeg, Bulk extractor, AccessData, FTKImager, QphotoRec

Email Forensics - Oletools, Exiftool, Email Header Analysis(EHA), Strings

USB & Registry Forensics - Regshot, Registry Explorer, USBDViewer, Amcache, KAPE, Autopsy

Professional Experience

CSIRT

Coordinated Technology | Dubai,UAE

OCT 2023 - Present

Dedicated IT professional specializing in cybersecurity, excelling in incident response, threat monitoring, and malware analysis. Skilled in SIEM tools for security event monitoring and detailed incident reporting. Proficient in vulnerability management, prioritizing remediation based on severity. Experienced in DFIR analysis using FireEye tools to address emerging threats. Collaborative and detail-oriented, committed to enhancing security posture through continuous learning and proactive defense strategies.

Security Analyst

CyberProof | Chennai,India

JAN 2022 - OCT 2023

- Conducted proactive monitoring, investigation, and mitigation of security incidents in a 24x7 Security Operations Center.
- Analyzed security event data from the network using IDS, SIEM, and conducted log analysis using Splunk.
- Investigated malicious phishing emails, domains, and IPs using Open Source tools to recommend proper blocking based on analysis.

Junior Security Analyst

UST Global

Aug 2021 - Jan 2022

Proactively oversee and resolve security incidents, analyzing network event data through IDS and SIEM. Conduct thorough malware analysis on isolated virtual servers, detecting intrusion attempts via detailed event assessment. Enforce policies, protect systems, and stay informed on emerging threats through ongoing research. Collaborate within a 24/7 SOC, continuously monitoring, analyzing, and mitigating security events, utilizing Open Source tools for investigating malicious elements.

Education

Bachelor in IT ,Coimbatore,Tamilnadu, India

Aug 2017 - May 2021

Certification:

- Certified AppSec Practitioner (CAP) by SecOps
- Maximizing DFIR Results with YARA, Sigma, and Belkasoft X
- Blackperl Certified Advanced Defender (BCAD)
- Blue Team Level 1 (BTL1)