


Jeevanantham Kumarasamy

Erode,Tamilnadu,India | jeevakumar712@gmail | +91-9566614314

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

Professional Summary

Possessing extensive expertise as a seasoned security analyst, I am deeply focused on rapid incident response, thorough malware analysis, and proactive threat hunting. Employing advanced DFIR techniques, I skillfully conduct precise root cause analyses, while proficiently applying the cyber kill chain, MITRE ATT&CK, and APT knowledge to fortify the security of intricate systems and networks through strategic mitigation approaches. Actively immersed in refining proficiencies spanning USB, Registry, Memory, Mobile, and Cloud forensics (AWS, Azure), my commitment to continuous learning drives me to stay updated with industry advancements, ensuring a comprehensive understanding of emerging threats and the effective implementation of preemptive security measures.

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 - Azure sentinel, Splunk, Elasticsearch, Cyberreason, Symantec, Wazuh

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

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

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

As a dedicated and detail-oriented IT professional, I excel in various aspects of cybersecurity, including incident response, threat monitoring, and analysis. My responsibilities encompass resolving escalated security incidents within SLAs, actively monitoring security events using SIEM tools, and conducting thorough incident analysis to generate detailed reports. I specialize in malware analysis, scrutinizing suspicious files and proposing effective remediation strategies. In vulnerability management, I assist with scanning processes and prioritize remediation efforts based on the severity of identified vulnerabilities. I maintain meticulous incident documentation and produce regular reports to ensure transparency and accountability. Collaboration is integral to my role, as I engage with various teams to coordinate incident response efforts and share critical findings, while also ensuring seamless transitions during shift handovers by documenting and communicating incident statuses. Committed to continuous improvement, I stay updated on the latest security threats, contribute to enhancing our security posture, and conduct digital forensics and incident response (DFIR) triage and analysis using FireEye tools, thereby bolstering our organization's defenses against emerging threats.

Senior Security Analyst

- Incident Response: Resolve escalated security incidents within SLAs.
- Threat Monitoring: Monitor security events using SIEM tools.
- Incident Analysis: Analyze security incidents, provide detailed reports.
- Malware Analysis: Analyze suspicious files, propose remediation.
- Vulnerability Management: Assist with scanning, prioritize remediation.
- Documentation and Reporting: Maintain incident documentation, generate reports.
- Collaboration and Communication: Work with teams for incident response, share findings.
- Shift Handover: Document and communicate incident status.
- Continuous Improvement: Stay updated on security threats, contribute to improvement.
- Mentoring and Knowledge Sharing: Guide and train junior analysts, share knowledge.

Related Projects:

Successfully built a Project on top of Elastic with MISP, TheHive, Cortex and full case Management using DFIR-IRIS.

Threat Hunting: -

"Engaging in hypothesis-driven threat hunting using MITRE ATT&CK TTPs and threat intel, followed by DFIR for improved security. Utilizing SIEM, EDR tools, sigma, Yara, YarGEN, and LOKI for TTP-based threat hunting from reputable sources like NCA and SAMA. Developed and executed a DARK PINK APT hunting project in a simulated Splunk setup, ready for presentation."

Security Analyst

UST Global

Aug 2021 - Jan 2022

Roles & Responsibilities

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:

Foundations of Operationalizing MITRE ATT&CK
Autopsy Basics and Hands On (8-Hours)
Intro to DFIR: The Divide and Conquer Process (3 hours)
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) - In-progress