Karthik S Arkasali

+917829438119 [karthik.arkasali@gmail.com](mailto:karthik.arkasali@gmail.com) [LinkedIn](https://www.linkedin.com/in/karthik-s-arkasali) [Github](https://karthiksarkasali.github.io/karthik.github.io/)

# OBJECTIVE

Detail-oriented cybersecurity professional with hands-on experience in monitoring and responding to security incidents. Proficient in utilizing SIEM, SOAR tools, and threat intelligence to enhance threat detection and incident response capabilities. Eager to contribute to a dynamic team focused on proactive cybersecurity measures and safeguarding organizational assets.

# EDUCATION

## Bachelor of Engineering (Electronics & Communication)

Sapthagiri College Of Engineering | Bangalore, India

July 2022

# TOOLS & TECHNOLOGIES

**SIEM:** Splunk, Wazuh, Kibana, **Vulnerability Scanning:** Nessus,OpenVAS

**Malware Analysis:** FlareVM, **Programming:** Python, SQL

**SOAR**  **Solution:** Tines, Shuffle **Threat Intelligence:** Honeypot**,** IP Void, IP Abuse

**Ticketing Tool:** Thehive ,osTicket

# TECHNICAL SKILLS

* Hands-on experience with SIEM tools, including Splunk, Wazuh, and Kibana.
* Proficient with network security devices such as firewalls, WAFs, proxies, and IPS/IDS systems.
* Knowledgeable in malware analysis and the OWASP Top 10 vulnerabilities.
* Practical experience with incident management tools and processes.
* Expertise in analysing incidents using the Cyber Kill Chain framework and MITRE ATT&CK methodology.

# PROJECTS

## EDR Project | [Link](https://github.com/KarthikSArkasali/Cybersecurity-SOAR-EDR-Project)

* Created a playbook to automate alerts via Slack and email, enabling user-driven isolation decisions for detected threats.
* Configured LimaCharlie to generate telemetry & tested connectivity with Tines, improving cybersecurity operations.

## SOC Automation Project | [Link](https://github.com/KarthikSArkasali/SOC-Automation-Project)

* Design a logical diagram and set up virtual machines with necessary applications, including TheHive and Wazuh for monitoring and alerting.
* Generate and ingest telemetry into Wazuh, integrate Shuffle (SOAR) for automated alerting to TheHive, and notify SOC analysts via email.

## Active Directory Project | [Link](https://github.com/KarthikSArkasali/Active-Directory-Project)

* **Set up a virtual environment with Windows, Linux, and Splunk for telemetry monitoring and Active Directory.**
* **Perform brute force attacks from Kali Linux, analyse logs in Splunk, and run atomic tests using ART.**

**Threat detection and Incident Response Using ELK |**  [Link](https://github.com/KarthikSArkasali/Threat-Detection-and-Incident-Response-Using-ELK)

* **This project involves configuring the ELK stack for log monitoring and detecting brute force attacks on SSH/RDP servers.**

# CERTIFICATION

* Google Cybersecurity Professional Certificate – Coursera ([Link](https://coursera.org/share/b4590eff7be110b2529d92c0f9d373d1))
* Cybersecurity Virtual Experience Program on Forage – Forage ([Link](https://forage-uploads-prod.s3.amazonaws.com/completion-certificates/mastercard/vcKAB5yYAgvemepGQ_Mastercard_wimRMHkmAA8rCb6tx_1729488972782_completion_certificate.pdf))