MOKILI SARAVANAN

LinkedIn: https://www.linkedin.com/in/mokili-cyber
Email: infosec.moli@gmail.com
Mobile: +353 89 251 4375
Location: Dublin, Ireland

PROFILE

- Security Operations Analyst with strong hands-on experience in SIEM monitoring, incident triage, threat detection, and log analysis.
- Experienced in Splunk and Linux/Windows event monitoring, with practical exposure to MITRE ATT&CK, EDR tools, and vulnerability assessment in a fully built home SOC lab.
- Skilled in analysing alerts, identifying false positives, investigating anomalies, and escalating incidents using structured runbooks. Highly dedicated to blue-team defence and continuously expanding technical capability across cloud security, detection engineering, and endpoint protection.
- Currently on the Irish Stamp 1G Graduate Visa fully available for full-time roles.

KEY SKILLS

- **SIEM:** Splunk, Microsoft Sentinel (familiarity)
- **EDR & Endpoint Security:** Defender for Endpoint, Linux/Windows event monitoring
- **Vulnerability Management:** Scanning, assessment, prioritisation
- **Security Frameworks:** ISO 27001, NIST CSF, GDPR awareness
- **Cloud Security:** Azure & AWS fundamentals
- **Scripting:** Python (automation), Bash

EXPERIENCE

September 2024 – Present | Home SOC Lab | Ireland

- Built a full detection and monitoring environment using Windows + Kali + Splunk Universal Forwarder.
- Created alerts and dashboards for failed logins, brute-force attempts, Sysmon-based process monitoring, and suspicious network behaviour.
- Performed incident triage and escalation simulation aligned with MITRE ATT&CK techniques (TA0001–TA0009).
- Analysed Windows Event Logs (Security, System, Application) and Sysmon telemetry to detect process injection, persistence, and privilege escalation patterns.
- Conducted investigations on sample phishing emails, malicious documents, and suspicious binaries.
- Performed vulnerability scanning and basic hardening on Linux and Windows machines.
- Documented incidents and created SOC runbooks for repeated detection workflows.

July 2023 – April 2024 | Java Intern | Besoins Technology, India

- Contributed to backend development using Java, APIs, and SQL integration.
- Improved application performance through optimisation and bug fixing.
- Worked with cross-functional teams to deliver stable software releases.
- Strengthened analytical and debugging skills valuable for security monitoring.

PROJECTS

Zero-Day Attack Detection & Response (Practicum Project, 2025)

- Developed a log-based anomaly detection system using Splunk correlation searches.
- Designed detection logic for suspicious IP behaviour, repeated authentication failures, and privilege misuse.
- Built custom dashboards, alerts, and email notifications simulating SOC workflows.
- Reduced false positives through dataset-based tuning and batch testing.
- Documented full architecture, data flow, and IR runbook.

Web Application Security (OWASP)

- Designed and implemented a secure web application, focusing on SQL injection prevention.

- Tools like DB browser, OWASP and GitHub were used to implement parameterized queries to mitigate SQL injection risk.
- Enforced Input validation and web application firewall for additional security layers and integrated logging and monitoring mechanism for detecting SQL injection attempts.

AWS Security Hardening

- Deployed WordPress on AWS EC2 and implemented IAM policies, security groups, and monitoring.
- Tools like CloudWatch, IAM Policies, Security groups were used to harden infrastructure level security and Third-party tools like Plugins and Data dogs were used to secure application level.
- Performed both infrastructure and application-level hardening.
- Deployed WordPress website was tested using Nmap, Nessus, Wireshark and Kali Linux.

EDUCATION

2024 – 2025 | MSc in Cybersecurity | National College of Ireland, Dublin, Ireland.

Modules: Secure web development, secure application development, Network security and Penetration testing, Security Fundamentals, Data governance, Cloud architecture and security, Cryptography, AI/ ML in cybersecurity.

CERTIFICATION

- Google Cybersecurity Professional Certificate
- CompTIA Security+ - Ongoing