Mr. Akshay Reddy Kothwal is a Cybersecurity Analyst specializing in Security Operations Center (SOC) operations, Vulnerability Assessment and Penetration Testing (VAPT), and Threat Detection. He holds his M.Tech in Information Security & Cyber Forensics at SRM Institute of Science and Technology. His research and professional interests primarily focus on cybersecurity operations, incident response, cloud security monitoring, digital forensics, and secure authentication mechanisms.

He has actively worked on security monitoring and defense evasion detection, particularly in the domain of SOC log tampering attacks and cloud-based security architectures. His work involves designing detection mechanisms using File Integrity Monitoring (FIM), analyzing security logs, implementing automated alerting systems, and evaluating security controls against real-world attack scenarios.

Primarily, his work revolves around Security Information and Event Management (SIEM), threat detection engineering, vulnerability assessment, penetration testing, and security analytics. His areas of expertise include Security Monitoring, Incident Investigation, Threat Intelligence, Log Analysis, Network Security, Cloud Security Operations, and Authentication Systems. He is also interested in exploring advanced applications of Artificial Intelligence, Physical Layer Security, IoT Security, and Digital Forensics to strengthen modern cybersecurity infrastructures.

Research Interests

- Security Operations Center (SOC) and Security Monitoring
- Threat Detection and Incident Response
- Vulnerability Assessment and Penetration Testing (VAPT)
- SIEM Technologies and Security Analytics
- Cloud Security and Defensive Monitoring
- Digital Forensics and Incident Investigation
- Physical Layer Security for IoT
- Authentication and Access Control Mechanisms
- Threat Intelligence and MITRE ATT&CK Framework
- Cybersecurity Risk Management and Compliance

Professional Highlights

- Worked extensively on SOC Evasion Detection and Log Tampering Analysis using Wazuh and OpenSearch.

- Built a cloud-based SOC environment for monitoring, investigation, and incident response.
- Implemented File Integrity Monitoring (FIM) mechanisms to detect defense evasion techniques.
- Developed automated security alerting and response workflows for real-time threat detection.
- Conducted Vulnerability Assessment and Penetration Testing using industry-standard tools including Burp Suite, Nmap, Nessus, and Metasploit.
- Designed a lightweight authentication protocol using Physical Layer Security (PLS) for secure IoT communications.
- Developed an Adaptive Intrusion Detection System using Danger Theory and Negative Selection Algorithms.
- Experienced in network traffic analysis, log investigation, and security control validation across cloud and enterprise environments.

Vision and Goals

Mr. Akshay Reddy Kothwal aspires to contribute towards advanced research and innovation in Cybersecurity Operations, Threat Detection Engineering, Cloud Security, and Digital Forensics. His vision is to develop intelligent security monitoring systems capable of detecting sophisticated cyber threats while enhancing organizational cyber resilience. He aims to contribute to impactful research in SOC automation, AI-driven cybersecurity, IoT security, and next-generation threat detection frameworks.

Contact Information

Email ID: kothwalakshay10@gmail.com

LinkedIn: https://www.linkedin.com/in/akshay-reddy-kothwal-a75b24280/