MADHU BALAKRISHNAN BASHYAM

Dublin, Ireland | Open to Relocation
madhubb1905@gmail.com | +353 89 472 0296
LinkedIn: linkedin.com/in/madhubalakrishnanbashyam | Portfolio: madhubashyam.net

SUMMARY

Cybersecurity professional with 2+ years of experience in security monitoring, incident response, threat hunting, phishing and malware analysis, vulnerability management, and SIEM operations. Experienced in investigating security incidents, performing alert triage, endpoint investigations, and vulnerability remediation using Microsoft Sentinel, CrowdStrike Falcon, and Qualys. MSc in Cybersecurity with Certified Ethical Hacker (CEH) and CompTIA Security+ certifications. Currently a Trust and Safety Analyst at Accenture, Dublin, seeking a SOC Analyst role where I can apply and further develop my cybersecurity expertise.

TECHNICAL SKILLS

- **Security Operations:** Security Monitoring, Alert Triage, Incident Investigation, Incident Response, Threat Detection, Threat Hunting, Containment and Remediation, Detection Tuning and Correlation Rules, Log Analysis, Security Reporting.
- **SIEM and EDR:** Microsoft Sentinel (KQL), Splunk, CrowdStrike Falcon (EDR), Microsoft Defender, Endpoint Security, IDS/IPS and AV Log Analysis.
- **Vulnerability Management, Email Security and Networking:** Vulnerability Management and Remediation (Qualys, Nessus), Email Security and Phishing Analysis (Microsoft EOP), Network Traffic Analysis (Wireshark), TCP/IP, DNS, Firewall Concepts, Windows and Linux.
- **Threat Intelligence and Analysis:** Threat Intelligence and Enrichment (VirusTotal, AbuseIPDB, Any.Run), IOC Analysis, Phishing and Malware Analysis, Host and Network Forensics.
- **Scripting and Frameworks:** Python, PowerShell, Bash, SQL; NIST Incident Response Lifecycle, Cyber Kill Chain; Jira, ServiceNow (Ticketing and ITSM).

PROFESSIONAL EXPERIENCE

Trust and Safety Analyst | Accenture, Dublin, Ireland **March 2026 - Present**

- Performed risk-based investigations into high-risk user behaviour and policy violations, identifying suspicious activity and escalating cases according to security procedures.
- Triaged and escalated complex abuse cases to Security and Legal teams based on risk severity and established escalation frameworks.
- Conducted root cause analysis on recurring violation patterns to identify control gaps and support policy improvements.
- Identified and flagged emerging abuse trends, contributing to proactive detection improvements across the team.
- Collaborated cross-functionally with Legal, Policy, and Security stakeholders to resolve high-priority investigations.
- Maintained thorough case documentation in line with compliance and audit requirements.

SOC Analyst | Hackup Technology, Coimbatore, India **July 2022 - July 2024**

- Monitored and investigated security alerts using Microsoft Sentinel and KQL, identifying and escalating confirmed security incidents.
- Conducted endpoint investigations using CrowdStrike Falcon, containing threats and supporting timely remediation.
- Investigated phishing emails, validated IOCs, and enriched investigations using Microsoft EOP, VirusTotal, Any.Run, and AbuseIPDB.
- Performed vulnerability assessments using Qualys, validated remediation activities, and analysed suspicious network traffic using Wireshark.
- Developed KQL queries and automated repetitive SOC tasks using PowerShell, Python, and Bash to improve operational efficiency.
- Documented investigation findings, managed incidents in Jira and ServiceNow, and collaborated with IT teams to resolve security issues.

EDUCATION

MSc in Cybersecurity — First Class Honours **September 2024 - October 2025**

Dublin Business School, Ireland

Focus: SOC Operations, Incident Response/DFIR, Threat Detection and Hunting, Vulnerability Management

Bachelor of Computer Applications **July 2020 - June 2023**

VIT (Vellore Institute of Technology), India

Focus: Programming, DBMS, Computer Networks, Operating Systems, Web/Application Development

---

PROJECTS

SeCPoD — AI-Powered Insider Threat Detection & Investigation Platform

- Built an end to end SOC platform that detects insider threats through machine learning behavioural analytics and guides analysts from alert to investigation, featuring MITRE ATT&CK mapping, adaptive risk scoring, and VirusTotal/Talos threat intel enrichment, using Python, FastAPI, SQLAlchemy, scikit-learn, and Streamlit.

Advanced USB Security Control (HID Attack Prevention)

- Developed a Python-based solution to detect and block malicious USB/HID devices (BadUSB and keystroke injection) to strengthen endpoint security using Python, Windows API, and PowerShell.

Python Vulnerability Scanner

- Developed a Python tool to automate vulnerability scanning, identify common misconfigurations, and generate remediation reports based on CVSS severity using Python and REST APIs.

CERTIFICATIONS

- CompTIA Security+ (SY0-701)
- Certified Ethical Hacker (CEH) — EC-Council