umamaheswaripm10@gmail.com
+91 93445 65122
linkedin.com/in/uma-maheswari-p-m-87655b213
umamaheswari.pm
Chennai, India

Uma Maheswari P M

Senior Cyber Security Consultant · SOC Operations · DLP · Incident Response

PROFILE

Senior Cyber Security Consultant with hands-on SOC experience monitoring and investigating security alerts, performing incident response and alert triage across multi-client environments using leading SIEM and EDR platforms. Strong command of SOC processes and the MITRE ATT&CK framework — focused on precise threat analysis, false-positive reduction, cross-team coordination and SLA-compliant incident documentation.

EXPERIENCE

Senior Cyber Security Consultant

2023 – Present

LTIMindTree (LTM) · Chennai, India

SOC Monitoring & Incident Response

- Performed 24×7 SOC monitoring, alert triage and investigation across multiple client environments using Devo SIEM, Microsoft Sentinel and Rapid7 InsightIDR.
- Investigated and responded to brute-force attempts, malware detections, excessive object deletions, suspicious outbound connections, authentication failures and abnormal user behaviour.
- Developed and maintained SOPs ensuring accurate incident handling, consistent documentation and strict SLA adherence across all client accounts.
- Collaborated with end users, clients and internal teams to investigate alerts and drive timely, structured incident resolution.

Email Security — Microsoft Defender for Office 365

- Triaged email security incidents — performing phishing analysis, quarantined email review and legitimacy-based remediation actions using Microsoft Defender for O365.

Endpoint Security — Microsoft Defender for Endpoint

- Handled endpoint security alerts and blocked malicious IOCs including IPs, URLs and file hashes to contain threats and prevent further compromise across client environments.

SOAR & Automation

- Built and maintained SOAR playbooks integrating threat intelligence feeds — automating alert enrichment for faster and more consistent incident response workflows.

DLP — Monitoring & Incident Investigation

- Monitored and investigated DLP alerts, performed root cause analysis and coordinated with stakeholders for remediation and user awareness.
- Investigated DLP incidents using Microsoft Purview and Google Chronicle — conducting root cause analysis to assess breach scope and identify contributing factors.
- Worked closely with SOC and IT teams to fine-tune policy thresholds, reduce false positives and improve detection accuracy.
- Maintained clear communication with affected users and their managers throughout the incident lifecycle.

DLP — Process Improvement & Automation

- Automated escalation workflows using macros to improve response time and reduce manual effort.
- Regularly reviewed and improved incident response procedures to enhance speed, accuracy and overall effectiveness.
- Created and maintained SOPs, incident response guides and training materials to support ongoing DLP operations and vendor onboarding.

DLP — Knowledge Transfer & Vendor Enablement

- Delivered Knowledge Transfer (KT) sessions to third-party vendors during transition phases — covering DLP architecture, incident workflows and escalation procedures.

SKILLS

- Alert Triage & Incident Handling
- SIEM / SOAR Operations
- Endpoint Detection & Response
- Security Log Analysis
- Email Security & Phishing IR
- Threat Intelligence Integration
- Data Loss Prevention (DLP)
- SLA Adherence & Documentation
- MITRE ATT&CK Framework

TOOLS

SIEM / SOAR

Devo SIEM · Devo SOAR · MS Sentinel · Rapid7 IDR · G. Chronicle · MS Purview

ENDPOINT

MDE · MDO / O365 · CrowdStrike · Panda AD360

FRAMEWORKS

- MITRE ATT&CK
- NIST (Foundational)
- Cyber Kill Chain

CERTIFICATIONS

AZ-500
Azure Security Engineer Associate
Microsoft Certified

SC-900
Security, Compliance & Identity Fundamentals
Microsoft Certified

EDUCATION

Master of Computer Applications
Bharathiar University
2024 – 2026 · Pursuing

B.Sc. Computer Science
(Cognitive Systems)
Thiagarajar College
2020 – 2023 · CGPA 8.87

STRENGTHS

- Detail-oriented alert investigation
- Professional incident documentation
- Clear stakeholder communication
- Fast & accurate threat analysis