

MANALI THUBE(DHANAWADE)

CYBER SECURITY PROFESSIONAL

THREAT HUNTING | INCIDENT RESPONSE | DIGITAL FORENSICS
| EDR/SIEM MONITORING



CONTACT

+971 507782109 

thubemanali@gmail.com 

UAE 

linkedin.com/in/manali-
dhanawade 

SKILLS

- Threat Hunting
- Incident Response
- EDR Monitoring
- Computer Forensics
- Email Forensics
- Mobile Forensics
- Log Analysis
- Registry Analysis

SUMMARY

Cybersecurity professional with 8+ years of expertise in Threat Hunting, Digital Forensics, and Incident Response. Skilled in proactive threat detection, forensic investigations, and behavior-based hunting strategies. Proficient in analyzing network traffic, utilizing SIEM and EDR tools, and mitigating advanced cyber threats. Experienced in digital evidence preservation, incident response enhancement, and collaboration with MDR teams.

PROFESSIONAL EXPERIENCE

Accenture Pvt Ltd

Associate Manager | Nov 2024 – Present

- Conduct advanced threat hunting using behavioral analytics to detect and contain complex cyber threats before escalation.
- Conduct proactive threat hunts across member firms using IOCs and TTPs.
- Execute incident response actions including containment, isolation, and remediation guidance.
- Enrich alerts using threat intelligence and MITRE ATT&CK mapping.
- Conduct proactive threat hunting to identify hidden threats and detection gaps.
- Escalate and coordinate with senior SOC/IR teams during major incidents.
- Improve detection use cases and SOC monitoring effectiveness through analytics.
- Deliver concise, data-driven reports highlighting key insights, optimized detection use-cases, and targeted recommendations to enhance threat visibility and response efficiency.

KPMG India

Consultant | Apr 2022 – Nov 2024

- Investigated P1 and P2 high-severity incidents, analyzing device timelines and identifying Indicators of Compromise (IOCs).
- Performed deep-dive analysis and EDR monitoring to detect and contain threats within defined SLAs.
- Monitor and triage complex alerts from SIEM and EDR platforms and validate true security incidents.

TOOLS

- Splunk
 - QRadar
 - Microsoft Defender
 - Sentinel
 - CrowdStrike
 - Tanium
-

CERTIFICATIONS

- MITRE Framework (CTI)
 - CHFI
 - CEH V9
 - Access Data's Certified Investigator
 - Certified Mobilyze Operator
 - Training Certified Computer Forensic
-

- Perform deep-dive investigations across endpoint, network, identity, and cloud environments
- Investigate attacker activity to determine entry point, scope, impact, and timeline
- Execute incident response actions including containment, isolation, and remediation guidance.

Network Intelligence

Senior Cyber Security Analyst | Mar 2021 – Mar 2022

- Conducted forensic and malware investigations including email and endpoint analysis
- Performed email header and malware analysis (static and dynamic)
- Analyzed logs from Windows, Linux, and network devices
- Investigated BEC, phishing, and advanced intrusion cases
- Analyzed digital artifacts including event logs, registry hives, amcache, and user activity data for forensic evidence.
- Investigated malicious activity, ATM hacking (Raspberry Pi), and Linux forensics cases.

Arete IR

IR & F Associate Analyst | Oct 2019 – Mar 2021

- Investigated multiple ransomware incidents, identifying patient zero, compromised accounts, and data exfiltration paths.
- Conducted detailed registry and log analysis to trace attack vectors.
- Analyzed Business Email Compromise (BEC) cases using O365 audit logs, email headers, and phishing evidence.
- Managed end-to-end forensic cases, including data indexing, hosting, review, and reporting.
- Investigated ransomware and major incident cases end-to-end
- Reconstructed incident timelines using registry and log analysis
- Performed mobile and endpoint forensic investigations
- Analyzed phishing evidence and O365 audit logs

Pelorus Technologies

Digital Forensic Analyst | Aug 2018 – Oct 2019

- Assisted cyber labs in digital evidence retrieval and forensic investigations.
- Operated a wide range of standard computer and mobile forensic tools.
- Delivered technical training, tool demonstrations, and installations for law enforcement agencies.
- Supported government tenders by preparing technical specifications and compliance documentation.

EDUCATION

University of Mumbai

- PGDM in Digital Cyber Forensics & Related Law
 - PGDM in Cyber Law & Information Technology
 - B.E. (IT)
-

ACHIEVEMENTS

- Represented India at the National Research University, Moscow, presenting a research paper on “The Growing Threat of Cyber Espionage and Related Law.”
- Published “Social Media Forensics with Mobile Forensics” in the IJRT Journal during the National Conference on Cyber Intelligence & Forensics (CICFI), organized by Maharashtra Cyber, BARC, and ISACA.
- Participated in a Maharashtra State Government project, securing a bid through forensic tool demonstrations.
- Invited speaker at “Cyber Security” workshop hosted by L.J.N.J. Mahila Mahavidyalaya College (S.N.D.T. Vile Parle), 2019.