MANICHAND GUPTA

Meerut, UP · Open to relocation · Graduating 2027 • +91-7266913997 • manichand.gupta.contact@gmail.com
eclipsemanic.me • github.com/EclipseManic • linkedin.com/in/manichandgupta

PROFESSIONAL SUMMARY

Investigates security alerts end-to-end - log correlation, endpoint triage, and incident documentation - across a self-hosted SOC lab spanning **Wazuh**, **Splunk**, and **Microsoft Sentinel** (SIEM), with **150+ alerts triaged** since February 2026. Independently investigates live fraud and malware campaigns outside the lab - including reverse-engineering an evasive PDF-based infostealer disguised as a fintech internship offer - and builds open-source DFIR tooling to support that work. Ranked **Top 5% on CyberDefenders** and **Top 1% on KC7**.

TECHNICAL SKILLS

Security Tools: Wazuh, Suricata, TheHive, Velociraptor, Splunk, Microsoft Sentinel, Elastic Stack
DFIR & Malware Analysis: Autopsy, KAPE, Volatility, Ghidra, YARA, ANY.RUN, Joe Sandbox, Hybrid Analysis, Tria.ge
Threat Intelligence: VirusTotal, urlscan.io, URLhaus, ThreatFox, Shodan
Network Analysis: Wireshark, tcpdump, Nmap, TCP/IP, DNS, HTTP/S, SSH
Security Operations: SIEM alert triage, log analysis, threat hunting, IOC analysis, event correlation, endpoint investigation
Phishing Analysis: SPF, DKIM, DMARC, ARC, email header analysis, phishing and quishing detection
Infrastructure & Cloud: Docker, WireGuard, Linux, Windows, Windows Server, OVHcloud, DigitalOcean, Azure, AWS
Frameworks & Compliance: MITRE ATT&CK, NIST CSF, NIST SP 800-61, CIS Controls, OWASP Top 10
Programming: Python, Bash, PowerShell, KQL

RELEVANT EXPERIENCE – SELF-DIRECTED

Personal SOC & Incident Response Lab **Feb 2026 – Present**

- Built a hybrid SOC environment across OVHcloud and DigitalOcean, connecting a WireGuard-tunneled multi-VM network with **3 victim endpoints** (Windows Server 2022, Windows 10, Ubuntu) to run controlled, repeatable attack simulations.
- Triaged **150+ alerts** using **Wazuh** and **Suricata**, correlating endpoint and network telemetry to identify suspicious activity and extract IOCs.
- Built a custom Python integration (`Wazuh` → `TheHive`) to replace a broken Shuffle SOAR pipeline, automating alert normalization, severity mapping, and case creation.
- Conducted endpoint investigations with **Velociraptor** to validate detections and trace attacker activity, then documented evidence, IOCs, and response actions in **TheHive**, mapping confirmed activity to **MITRE ATT&CK** (Initial Access, Execution, Discovery, Command and Control).

PROJECTS

Malware Analyzer – Web | github.com/EclipseManic/Malware_Analyzer_Web **Jul 2026**

- Built a malware triage tool that scans PE, ELF, Mach-O, APK, Office, PDF, scripts, and archives, with a Flask/WebSocket dashboard for live analysis.
- Curated 2,778 YARA rules from 40 sources (Elastic, CAPE, APKiD, THOR), combined with static checks for entropy, packers, imports, and macros to flag malicious files.
- Integrated 4 threat-intel APIs (VirusTotal, Hybrid Analysis, Tria.ge, FileScan.io) with live scan progress tracking and persistent scan history.
- Validated scoring accuracy, API integration, and report output with a suite of 75 automated tests.

Phishing Mail Detector | github.com/EclipseManic/Phishing-Mail-Detector-Web **Jul 2026**

- Built a Flask-based email analysis tool that runs SPF, DKIM, DMARC, and ARC checks to detect spoofed and forged senders.
- Built a brand-impersonation detector covering ∼50 commonly faked brands, plus QR-code (quishing) scam detection.
- Designed a risk-scoring model (∼40 signals) to flag dangerous emails, mapping results to MITRE ATT&CK technique T1566 (sub-techniques .001, .002, .003).
- Added VirusTotal and urlscan.io lookups, with live scan progress and saved scan history.

Investigation Portfolio | github.com/EclipseManic/Investigation-Portfolio **Feb 2026 – Present**

- Independently investigated a live internship-fraud campaign (**Zorvyn FinTech**) – OSINT company/domain verification plus sandbox reverse-engineering of an evasive PDF dropper (DPAPI credential access, Windows Credential Vault, DLL-injection staging) – published with full MITRE ATT&CK mapping and IOCs.
- Investigated a live multi-vector job scam impersonating **Naukri.com** (coordinated call, SMS, spoofed email, PII-harvesting attachment); validated detection gaps by running the case through my own Phishing Mail Detector (scored 5/10) and documented specific scoring fixes.
- Completed 5 additional CyberDefenders/HackTheBox case write-ups – RAT analysis, credential-poisoning attacks, cloud breach reconstruction, and web exploitation – each MITRE ATT&CK-mapped, full library at eclipsemanic.me.

EDUCATION

Bachelor of Computer Application – Cloud & Cybersecurity (In Progress) **2024–2027**
IIMT University, Meerut || 7.5 CGPA Upto 4th Sem

CERTIFICATIONS

Google Cybersecurity Professional Certificate — *Coursera* **July 2025**
IBM Cybersecurity Analyst — *Coursera* **July 2025**
Microsoft Azure Cloud Administration — *EICT, IIT Kanpur* **Dec 2025**
Linux Administration with Scripting — *EICT, IIT Kanpur* **July 2025**
AWS Cloud fundamentals — *EICT, IIT Kanpur* **Dec 2024**