ADITYA JAIN

Cybersecurity Engineer & Subject Matter Expert (SME) | EDR/SIEM Architecture & Threat Emulation

India • Open to Relocation / Remote • **Phone:** +91 9897577007 • **Email:** aavkjain@hotmail.com •

linkedin.com/in/ajainx1 • ajainx1.github.io

PROFESSIONAL SUMMARY

Distinguished Cybersecurity Engineer and Subject Matter Expert (SME) with extensive enterprise experience orchestrating Security Operations (SecOps), threat hunting methodologies, and network security architectures. Proven track record deploying and managing endpoint detection and response (EDR) agents across government-scale infrastructure (750+ state offices) and designing custom automated compliance auditing platforms. Expert in leveraging generative AI automation and advanced scripting to rapidly construct custom network tools, secure communication bots, and local repository platforms. Active practitioner of offensive security and Active Directory chain exploitation, combining deep defensive insights with red team methodologies (Purple Teaming) to systematically fortify enterprise defenses.

CORE TECHNICAL SKILLS

Offensive Security & Red Teaming: Active Directory Exploitation (Kerberoasting, Pass-the-Hash, DCSync, Kerberos Delegation), Network Pivoting, OWASP Top 10 validation, Burp Suite Pro, Metasploit, Nmap, BloodHound, Impacket, Mimikatz.

Detection & Security Analytics: Wazuh SIEM, Blu Sapphire SIEM, SentinelOne EDR, Deep Seek EDR for servers, Kaspersky EDR, Event Viewer, Wireshark, PCAP analysis, Packet Drop Triage.

Network Security & VPNs: Cisco AnyConnect VPN, Tailscale VPN, Check Point NGFW, Fortigate NGFW, Sophos / WiJungle Firewalls, OSPF routing protocol, AAA (TACACS+/RADIUS), MTU optimization.

Scripting & AI Automation: PowerShell scripting, Bash, Python, Git, generative AI pair programming (AI-assisted development).

Compliance & Endpoint Management: CDAC Standards, CERT-In Guidelines, Security Policy Tuning, KACE UEM.

Vulnerability Research: CVE Analysis, Exploit Replication, Lab Emulation, Service Misconfigurations.

PROFESSIONAL EXPERIENCE

Security Administrator **Feb 2024 – Present**

Ebix Technologies / National Informatics Centre (NIC) *Noida, India*

- **Enterprise Architecture:** Direct security compliance audits and network security gateway policies across NIC's multi-state government network.
- **EDR & Telemetry SME:** Architected and managed the enterprise deployment of SentinelOne EDR and Deep Seek EDR for servers across 750+ regional offices, monitoring threat telemetry and tuning detection rules.
- **Audit Automation:** Developed custom PowerShell and Python auditing frameworks to automate 120+ regulatory compliance checks (CDAC/CERT-In), reducing local audit cycles by 60%.

- **AI & Telemetry Training:** Conduct weekly (Friday) training seminars for security teams and admins on leveraging Generative AI to automate network telemetry analysis, bandwidth monitoring, and anomaly detection.
- **Vulnerability Remediation:** Coordinated with CERT-In and developer groups to identify, replicate (via exploit proofs), and patch web/server vulnerabilities mapped to OWASP Top 10.
- **Endpoint Compliance:** Supervised KACE UEM across 400+ critical nodes to streamline patch management and maintain unified security baselines.
- **Network Gateway Control:** Implemented secure AAA controls (TACACS+/RADIUS), resolved complex packet drop incidents using Wireshark, and optimized OSPF routing and MTU sizes.

SOC Analyst — Threat Hunter **Dec 2022 – Jul 2023**

RRG Engineering Technologies / Nuclear Fuel Complex (NFC) *Rajasthan, India*

- **Incident Scoping:** Acted as SME for threat hunting and incident response, monitoring real-time enterprise telemetry via Blu Sapphire SIEM.
- **Threat Simulation:** Recreated emerging exploit signatures in sandbox environments and analyzed malicious payloads using Kaspersky EDR to reverse-engineer threat actor behavior.
- **EDR Optimization:** Tuned SIEM detection rules and EDR policies, boosting defensive detection rates by 35% and reducing false positives.
- **Intelligence Reporting:** Authored comprehensive reports on threat actor TTPs, scoping indicators of compromise (IOCs) to support incident response workflows.

SOC Analyst — IDS & Signature Development **Aug 2022 – Oct 2022**

E2E Networks Limited *Tamil Nadu, India*

- **IDS Engineering:** Managed security event triage via Wazuh SIEM in a 24x7 SOC environment and authored custom Snort/Wazuh IDS signatures.
- **Telemetry Analytics:** Analyzed bandwidth telemetry and node logs to identify routing loops, packet drops, and anomalous spikes.
- **Defensive Hardening:** Integrated AbuseIPDB feeds to automatically identify and block malicious IP blocks, hardening perimeter firewalls.

Technical Support Executive **Dec 2021 – May 2022**

Teleperformance *Hybrid*

- **Escalation Management:** Directed tier-2 escalation support for enterprise Microsoft suite services via the Rave ticketing platform, optimizing incident resolution SLAs.

KEY TECHNICAL PROJECTS (AI-ASSISTED DEVELOPMENT)

Enterprise LAN Asset Management Portal & Network Deployer

- **LAN Portal Development:** Designed and deployed a responsive, locally hosted web portal for secure utility and software download management within an internal LAN environment using AI-assisted development workflows.
- **Core Functions:** Built a secure local chatbot, professional file upload/download management modules, and a centralized software repository.
- **Network Boot Services:** Configured and segmented LAN services (DHCP/PXE), enabling automated network-based OS installations across target machines.

Automated MetaTrader 5 (MT5) Algorithmic Trading Bot

- **System Design:** Engineered a Python-based automated trading system implementing multi-indicator strategies (EMA, MACD, RSI, Supertrend).
- **Risk & Notification Engine:** Integrated position sizing risk-management logic, order execution via MT5 API, exit parameters, and real-time Telegram alert integration.

Custom WhatsApp Communication & Alert Bot

- **Bot Automation:** Created an automated WhatsApp chatbot to interface with local systems, support file distribution, and broadcast system status alerts.

Terminal-Themed Portfolio Web Portal (ajainx1.github.io)

- **Dynamic Portfolio:** Built and deployed a custom terminal-themed developer portfolio page.
- **Integrations:** Integrated real-time APIs (including live Spotify current playing status tracking) and showcased proprietary trading bot distributions.

EDUCATION

MBA in Cybersecurity — Chitkara University (Expected Jul 2027)

B.Tech in Computer Science & Engineering — Manipal University Jaipur (2019 – 2022)

Diploma in Computer Science — Hindu College of Engineering (2013 – 2018)

CERTIFICATIONS

- Fortinet Certified Associate in Cybersecurity (FCAC) – Jan 2026
- Introduction to Network Security – University of London (May 2026)
- Mathematical Foundations for Cryptography – University of Colorado (May 2026)
- Security Management and Governance – Royal Holloway, Univ. of London (May 2026)
- Red Hat Certified System Administrator (RHCSA) – (2018 - 2021)
- Ethical Hacking Expert – Star Certification (2019 - 2022)
- In the Trenches: Security Operations Center – EC-Council
- Autopsy Basics and Hands On (Digital Forensics) – BasisTech
- CISSP Exam Prep Pathway – CyberFrat (Mar 2025)
- Fundamental AI Concepts – Microsoft (Mar 2025)

OFFENSIVE SECURITY TRAINING & LABS

Hack The Box: Active Directory exploitation, privilege escalation, standalone boxes (Rank: Pro Hacker).

Vulnlab: Multi-forest Active Directory exploitation, network pivoting, and Domain Controller compromise.

OSCP (PEN-200): Preparing for exam (Target Q4 2026).

CEH (v13): Core methodologies and scanning tools (Target Q3 2026).

CISSP: Target completion Q1 2027.

Hobbies & Interests: Tech Blogging, Yoga & Mindfulness, Traveling.