Aditya Jain

Cybersecurity Engineer | SecOps · Purple Team · Threat Hunting

India (Open to U.S. Relocation / H-1B Sponsorship) | +91 740 058 8896 | adityasec32@gmail.com

linkedin.com/in/ajainx1 | github.com/ajainx1 | adityasec32.systems

Professional Summary

Versatile **Cybersecurity Engineer** with **4+ years of enterprise experience** in Security Operations, Threat Hunting, and Vulnerability Management across India's national government IT infrastructure. Deployed EDR/SIEM solutions across **750+ government offices**, automated compliance workflows reducing audit effort by **60%**, and led incident response to CERT-In (India's CISA equivalent) advisories. Skilled in bridging offensive and defensive disciplines — Active Directory attacks, sandbox malware analysis, and IDS signature development. Pursuing eJPT, CEH v13, and CompTIA Security+ (2026); CISSP and OSCP on structured roadmap. Targeting U.S. roles in **SOC Analysis, Detection Engineering, or Threat Hunting**.

Technical Skills

SIEM / EDR	Wazuh, Blu Sapphire SIEM, SentinelOne, Trend Micro Deep Security, Kaspersky EDR, Microsoft Sentinel (familiar), Splunk (familiar)
Offensive Security	Metasploit, Nmap, Burp Suite Pro, BloodHound, Impacket, Mimikatz, Kerberoasting, Pass-the-Hash, DCSync, Kerberos Delegation Abuse
Network Security	Check Point NGFW, Fortinet FortiGate, Sophos, Cisco AnyConnect, OSPF, TACACS+/RADIUS, Wireshark, PCAP Analysis
Scripting	Python, PowerShell, Bash, Git
Compliance / IR	NIST CSF, OWASP Top 10, CISA Guidelines (CERT-In equiv.), RAM Dump Analysis, PoC Validation, Snort/Wazuh IDS
Endpoint / Infra	KACE UEM (750+ nodes), USB Policy Enforcement, Linux Server Admin, DHCP/PXE, Patch Management

Professional Experience

Ebix Technologies — Patna, Bihar, India

Security Administrator — *Feb 2024 – Present*

Contracted to National Informatics Centre (NIC) — India's federal government IT and e-governance agency, equivalent to the U.S. General Services Administration (GSA) IT arm, managing national network infrastructure across 750+ regional offices.

- **Enterprise EDR Deployment:** Architected and managed SentinelOne and Trend Micro Deep Security across **750+ regional government offices**; monitored threat telemetry and tuned detection policies to neutralize emerging attack vectors.
- **Incident Response & Forensics:** Primary responder to CERT-In (India's CISA equivalent) advisories; performed host forensics including RAM dump analysis and IP reputation triage; authored PoC exploits to validate successful vulnerability closure.
- **Compliance Automation:** Built PowerShell and Python frameworks executing **120+ automated compliance checks** (NIST/ISO 27001-aligned) across 750+ endpoints — cutting audit effort by **60%** and eliminating manual reporting error.
- **Vulnerability Management:** Led coordinated disclosure and patching workflows with government application teams to remediate OWASP Top 10 flaws, including Open Redirect vulnerabilities across government-facing platforms.
- **Endpoint & Network Hardening:** Enforced default-deny policies on Check Point NGFW, deployed USB block via EPS, configured Linux rack servers, and conducted public IP exposure audits across the state-level network.
- **Security Awareness Training:** Designed and delivered technical training on Check Point operations, SentinelOne IR workflows, and CERT-In compliance procedures for **20+ district-level IT teams**.

RRG Engineering Technologies — Kota, Rajasthan, India

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

Contracted to Nuclear Fuel Complex (NFC) — a Critical National Infrastructure (CNI) facility under India's Department of Atomic Energy, equivalent in sensitivity to U.S. Department of Energy (DOE) nuclear facilities.

- **CNI SOC Operations:** Threat hunting and incident response SME in a **24×7 nuclear-sector SOC** (DOE-equivalent CNI), monitoring enterprise telemetry via Blu Sapphire SIEM.
- **Payload & Sandbox Analysis:** Reproduced adversary exploit signatures in isolated sandboxes; performed behavioral malware analysis with Kaspersky EDR to reverse-engineer TTPs and update detection signatures.
- **Detection Engineering:** Tuned SIEM correlation rules and EDR behavioral policies, achieving a **35% improvement in true-positive detection rates** while reducing alert fatigue.
- **Threat Intelligence:** Authored actionable IOC and TTP intelligence reports distributed to cross-functional IR and infrastructure teams to drive hardening decisions.

E2E Networks Limited — Vellore, Tamil Nadu, India
SOC Analyst — IDS & Signature Development — *Aug 2022 – Oct 2022*

- **IDS Engineering:** Authored and deployed custom Snort and Wazuh IDS signatures in a 24×7 SOC, improving detection coverage against novel attack patterns.
- **Threat Intelligence Integration:** Automated AbuseIPDB threat feed ingestion to enforce real-time perimeter IP blocklisting, reducing inbound malicious traffic.
- **Telemetry Analysis:** Analyzed bandwidth and network telemetry to identify routing anomalies, packet drops, and traffic spikes indicative of active compromise.

Teleperformance — Jaipur, Rajasthan, India
Technical Support Executive — *Dec 2021 – May 2022*

- Delivered Tier-2 Microsoft enterprise product support via Rave ticketing platform; maintained SLA compliance and contributed to knowledge base documentation.

Key Security Projects

- **CDAC/CERT-In Compliance Automation Engine** — *NIC Production (Classified)*
  PowerShell + Python framework executing **120+ automated compliance checks** (NIST-equivalent standards) across **750+ government endpoints** via KACE UEM — reducing audit cycles by **60%**. `PowerShell · Python · KACE UEM`
- **Government NOC Admin Portal** — *Live Deployment — NIC Bihar State Centre*
  Network Operations Center dashboard monitoring 38 district-level nodes with live device status, traceroute diagnostics, and a voice-enabled RAG chatbot (Ollama LLM). `JavaScript · PHP · Ollama LLM`
- **Real-Time Network Alert Dashboard** — *Live Deployment*
  Ping-monitoring and traceroute diagnostic dashboard for government core routers and floor switches, with mute controls and automated outage alerting. `JavaScript · CSS Grid · Fetch API`

Education

Chitkara University — Rajpura, Punjab, India
MBA in Cybersecurity (in progress) — *Expected Jul 2027*

Manipal University Jaipur — Jaipur, Rajasthan, India
B.Tech — Computer Science & Engineering — *2019 – 2022*

Certifications & Professional Development

Completed

- Fortinet Certified Associate in Cybersec. (FCAC) — Jan 2026
- Red Hat Certified System Admin. (RHCSA) — 2018–2021
- In the Trenches: SOC — EC-Council
- Autopsy Basics (Digital Forensics) — BasisTech
- Fundamental AI Concepts — Microsoft
- TCM Security Live Training & Certifications

In Progress / Targeted

- eJPT — eLearnSecurity *(Target: Q4 2026)*
- CEH v13 / CompTIA Security+ *(Target: 2026)*
- CISSP — ISC2 *(Target: Q3 2027)*
- OSCP / PEN-200 *(Planned: Post-CISSP)*

Offensive Security Labs: Hack The Box (Active — AD exploitation, privilege escalation, network pentesting) · Vulnlab (Active — multi-forest AD chains, Domain Controller compromise) · INE/eLearnSecurity (eJPT in preparation)

Work Authorization

Currently based in India. Seeking U.S. employer **H-1B sponsorship** or **remote/contract** engagements. Open to relocating to **Washington D.C. Metro / Northern Virginia (NOVA)**, **Austin, TX**, **Dallas, TX**, or **Chicago, IL**.