Uddip Ranjan Das

New Delhi, India

📞 +91 9311237276

✉️ Email | LinkedIn | Twitter | Blog

Professional Summary

Cybersecurity Specialist with 5+ years of experience across threat intelligence, malware analysis, and SOC operations. Proven success managing security for clients with 2000+ endpoints, reducing response times, and enhancing detection efficiency. Skilled in malware research, APT hunting, and SIEM/SOAR optimization. Published writer and strategic thinker with strong technical and communication skills

Work Experience

Writer & CTI Analyst

The CTI Dispatch | June *2025 Present*

- My own publication of weekly editions of curated CTI news and analysis, along with special bulletins of high impact events.

Senior SOC Analyst & CTI Analyst

Versprite Cybersecurity | *March 2023 – June 2025*

- Led 6+ cyber threat intelligence projects across 8 clients, identifying 20+ critical risks.
- Delivered security for clients with 2000+ endpoints; average investigation time <15 mins, response time <30 secs.
- Managed 3 clients simultaneously, improving SOC workflows by 65% and reducing false positives by 40%.
- Published 4 technical blogs and 25+ weekly threat intel newsletters consumed by marketing team, clients and stakeholders.
- Participated in APT threat hunting, enabling early detection of 7+ threat groups.
- Analyzed 10,000+ security logs/month via Stellar Cyber, D3, Cybereason, SentinelOne, and Rapid7; mitigated 500+ intrusions/vulnerabilities.
- Streamlined IR processes with Blue Teams, enhancing detection precision by 25% and reducing false alerts by 30%.

Senior SOC Analyst

Versprite Cybersecurity | *March 2022 – March 2023*

- Monitored and triaged 3000+ alerts/month for 2 enterprise clients using SentinelOne and Rapid7.
- Tuned SIEM detection rules and developed dashboards, improving signal-to-noise ratio by 35%.
- Conducted malware investigations and supported RCA documentation for weekly incident reports.
- Collaborated with Blue Teams to escalate and resolve P1 incidents within SLA, maintaining 98% on-time resolution.

Security Research Intern

Versprite Cybersecurity | *December 2021 – February 2022*

- Performed malware analysis and system hardening using Windows Internals.
- Conducted OSINT- driven threat hunting for training and internal use cases.

Security Researcher

Ministry of Defence of India | *August 2021 – December 2021*

- Contributed to 5+ cyber defense initiatives, performing malware triage and delivering technical assessments.
- Participated in Blue Team simulations involving nation-state threats; identified 12+ IOCs linked to APT actors.
- Delivered weekly intelligence updates and final reports to defense cybersecurity leadership.

Information Security Analyst

Innefu Labs Pvt. Ltd. | *December 2019 – July 2020*

- Managed endpoint defense and vulnerability scans across 1500+ nodes.
- Generated 20+ risk assessment and vulnerability reports with actionable remediation plans.
- Enhanced detection efficiency in internal Blue Team lab by implementing MITRE ATT&CK-based playbooks.
- Coordinated patching cycles and tracked resolution metrics, achieving >90% patch compliance.

Information Security Trainee

Innobuzz Knowledge Solutions | *July 2018 – July 2019*

- Conducted penetration testing and web application security training for students.

Education

- **Bachelor of Arts**, Subharti University, New Delhi | *2020 – 2023*
- **Senior Secondary (CBSE)**, Indirapuram Public School, Ghaziabad | *2016 – 2017*

Certifications

- Cybereason: Cyber Threat Intelligence Analyst
- Pentester Academy: Certified Red Team Professional
- D3 Security: SOC Analyst
- Innobuzz: Advanced InfoSec Diploma

Skills

- **Threat Intel & OSINT**: APT tracking, geopolitical analysis, Intelx, Maltego
- **SOC & SIEM**: Stellar Cyber, D3, SentinelOne, Cybereason, Rapid7, Qualys

- **Malware Analysis**: Static & dynamic reverse engineering
- **IR & Detection**: Incident response, log analysis, MITRE ATT&CK, IDS tuning
- **Soft Skills**: Technical writing, cross-functional collaboration

---

Trainings & Achievements

- Reverse Engineering by U.S. Department of Homeland Security
- SOC Core Skills by Wild West Hack Fest
- Top 1% on TryHackMe and Hack The Box
- Contributor to PolyX and Operation Chimera
- Intel 471: Intelligence Planning Workshop
- Flare Academy Training-Cybercrime Forums: Investigation and Intelligence Gathering

---

Hobbies & Interests

- Building and experimenting with custom hardware and tech setups.
- Engaging in cybersecurity challenges and Capture the Flag (CTF) events.
- Exploring off-road travel and customizing 4×4 vehicles—hands-on problem-solving in motion.
- Dog lover and advocate for animal welfare.

P.S. When I'm not busy chasing cyber threats or tinkering with technology, you'll find me traveling or trying to solve impossible cybersecurity puzzles. *If you're looking for someone who takes security seriously but brings a touch of creativity and curiosity to the team, let's connect!*