Yash Chandna

+1 (929) 533-6593 yashchandna@gmail.com

PROFILE

Cybersecurity engineer with 4+ years across detection engineering, incident response, and red teaming. Most recently on Coinbase's CSIRT, where I rebuilt the detection pipelines, cut false-positive alert volume by roughly 82%, and led crossfunctional response on a Sev1 incident spanning 4+ teams.

EDUCATION

Masters in Cybersecurity — Sep 2026 – Present
New York University — New York, USA

Bachelor of Technology - Computer Science Engineering - Cyber Security Specialization, — Aug 2018 – Jun 2022
The NorthCap University — Gurgaon, India
CGPA- 8.94/10

All India Senior School Certificate Examination (AISSCE), *Salwan Public School, CBSE* — 2018
Percentage- 90.8% — Gurgaon, India

WORK EXPERIENCE

Coinbase, *Security Engineer, CSIRT* — Oct 2024 – Aug 2026

- Built 4+ threat detections from scratch and tuned 20+ existing ones cutting false-positive alert volume by ~82%.
- Designed and shipped an internal enrichment tool that eliminated a recurring manual bottleneck across detection workflows leading to ~70% reduction in false positives.
- Led cross-functional response during a Sev1 incident, coordinating 4+ teams to resolution
- Co-architected Watson, an AI-powered investigation agent built for security operations
- Built Anubis, an AI agent for blockchain security triage, and presented it at an internal AI hackathon

KPMG, *Analyst - Cyber Defense and Incident Response* — Jul 2022 – Sep 2024

- Designed and implemented security protocols that **reduced incident response time by 60%.**
- **Led a team of 10 security analysts** in proactive threat hunting, enhancing the overall security posture of client networks.
- Collaborated with cross-functional teams to integrate security measures into new product developments, **ensuring compliance with industry standards** to improve efficiency by 75%.
- Conducted **comprehensive security assessments and penetration tests**, identifying and addressing vulnerabilities in client systems.
- Managed security awareness programs for clients, **resulting in a 25% reduction in phishing attack success rates.**

SKILLS

Technical Skills: SIEM, Detection Engineering, Threat Hunting, Threat Intelligence, Incident Response, Alert Triage, Security Enrichment Workflows, AI Agent Development, LLM-powered Security Tools, Python, Bash Scripting, VAPT, Red Teaming, Penetration Testing, Burp Suite, Metasploit, OWASP Top 10

Soft Skills: *Leadership, Time Management, Presentation Skills, Public Speaking*

CERTIFICATIONS AND COURSES

SEC598
SANS

OffSec Certificatied Professional (OSCP)
OffSec

Certified Red Team Professional (CRTP)
Altered Security

Certified Ethical Hacker (CEH) Master
EC-Council

PROJECTS

Cyber Threat Intelligence Platform, *KPMG India* — Apr 2023 – Sep 2023

- **Engineered and implemented the Cyber Threat Intelligence Platform** at KPMG, showcasing advanced proficiency in Linux and expertise in proactive threat hunting.
- Led integration of **MISP (Malware Information Sharing Platform) and ELK (Elasticsearch, Logstash, Kibana) stack**.
- Enhanced organization's **threat intelligence** capabilities and streamlined **threat detection and analysis** processes.

KICon CTF 2022, *KPMG India* — Oct 2022

- Designed and developed challenges for KPMG India's hiring **Capture The Flag (CTF)** competition.
- Set up the necessary infrastructure for the event

Config Bot, *KPMG India* — Feb 2022 – Jul 2022
Developed a bot and its web interface with a dashboard to provide instant configuration review for devices by CISCO running on IOS 15.x to 17.x and ASA 9.x

Sacramentum CTF — Oct 2021

- Organized a free for all **CTF for beginners** to help hone their skills in Cyber Security.
- **Developed challenges** for participants to test their skills on.