HRIDYESH

☎ +91-8860594679

✉ mr.hridyesh@gmail.com

✉ LinkedIn - Profile

SKILLS

- OSINT Framework Development & Automation
- Data Science & Analytics: ETL pipelines, Pandas, NumPy, NLTK, Matplotlib
- Big Data Tools: Dask, PySpark, MongoDB
- Web & Backend Development: Flask, Node.js, EJS
- CI/CD Fundamentals (GitHub Actions, GitLab CI)
- Basic Pipeline Automation
- Penetration Testing: Web, Mobile, Cloud, Network, Thick Client, Bank ATM Pentesting
- Cloud Security Testing: AWS, Azure environments
- Vulnerability Assessment & Management
- Automated Code Review
- Risk Management & IT Auditing – ITGC/ITAC
- Security Policy Design & Compliance Mapping (NIST, ISO 27001, GDPR)
- SOC & Infrastructure Security: SIEM, IDS/IPS, Firewall Configuration
- Scripting & Automation: Python, Bash
- Socket Programming (Python)
- Malware Analysis Fundamentals & Reverse Engineering
- Threat Modeling
- Regulatory Compliance

EDUCATION

- Bachelor of Technology (B.Tech) in Information Technology - RKGIT, Ghaziabad (Affiliated to Uttar Pradesh Technical University – UPTU), completed in 2015.
- Higher Secondary (12th) - R.L.B. Memorial School, Lucknow, completed in 2011.
- High School (10th) - St. James School, Hardoi, completed in 2009.

CERTIFICATIONS

C|EH Certified Ethical Hacker

C|TIA Certified Threat Intelligence Analyst

aws certified Security SPECIALTY

RSA

Microsoft CERTIFIED Professional
Microsoft Certified Professional

ECSA EC-Council Certified Security Analyst

CISA

CISM

CRISC

ISO 27001:2013 Certified LEAD AUDITOR

CAREER OBJECTIVE

Cybersecurity professional with ~10 years of experience in AI/ML security assessments, penetration testing (web, mobile, API, cloud, network), and threat and risk management. Proven in leading offensive security operations, managing SOC functions (SIEM, IAM, MFA, SOAR), and aligning controls with global standards like NIST, ISO 27001, PCI DSS, and GDPR. Adept at bridging technical execution with strategic business objectives to deliver scalable, risk-informed security solutions.

Currently seeking a leadership role to apply my technical expertise, strategic insight, and cross-functional experience in building resilient, business-aligned security programs.

EXPERIENCE - 9.11 YEARS

- **Amazon India @Bengaluru, India** (August 2023 – Till Date): Third Party Security Specialist
- **BMC Software @Pune**, **India** (April 2021-July 2023): Consultant – Threat management
- **SecureLayer7 @Pune, India** (April 2019 –April 2021): Consultant – Cyber Security
- **Tata Consultancy Services @Kolkata**, **India** (January 2018 – March 28, 2019): System Engineer – Cyber Security Practice
- **Gridinfocom Pvt. Ltd. @Gurugram, India** (September 2015-December 2017): Consultant - Information Security
- Multiple Internships before 2015 for CCNA, Freelance web development, Security Trainer etc.

TECHNOLOGIES & PRODUCTS

1. **AI/LLM Security assessment -** Performed security assessments of AI/LLM systems to identify vulnerabilities and mitigate prompt-based risks.
2. **TPRM:** Third Party Risk Management, Perform Risk Assessment and conduct on demand Security Audit
3. **Threat Management:** Threat Hunting, TI Feeds, MISP, OSINT, SafeBreach, Scorecard, MITRE Framework, Red Teaming, lolbins, gtfobins, Crisis Call Management etc., Cybersecurity development, automation etc.
4. **Malware Analysis:** Static Analysis, Dynamic- Behavior Analysis
5. **Vulnerability Assessment:** Nessus; Qualys VM; OpenVAS; Netcat; nmap; GHDB; etc.
6. **Penetration Testing:** Metasploit; Core-Impact; ptf, se-toolkit; w3af; zAnti, spf; sqlmap etc.
7. **Identity & Access Management:** RSA SecurId (for 2FA) and CA IAM i.e. SSO, IM & PIM
8. **Security Information and Event Management:** RSA SA and Alient Vault
9. Apart from RSA SA, I'm also familiar with the architecture and working process of other products like **ARCHER, DLP**
10. "Occasionally undertake freelance web development and automation projects, including implementing SEO for personal and professional sites."

ROLES AND RESPONSIBILITIES

Outlined below are the various responsibilities I have held across multiple organizations, reflecting the technical, operational, and managerial aspects of my career.

- Studying for ISACA AAIA to deepen AI/LLM security expertise, leveraging prior experience in targeted AI/LLM security assessments
- Developing custom ML models designed to scale and integrate with Transformer architectures for advanced NLP tasks
- Performed security assessments on LLM playgrounds and locally deployed models to identify vulnerabilities such as prompt injection, data poisoning, information disclosure, data leakage, and resource abuse (DoS).
- Created a general chatbot and product recommendation engine, with ongoing efforts to scale similar models for AI/LLM integration in cybersecurity use cases.
- Performed and managed third-party security risk assessments along with policy-based security reviews for multiple vendors
- Developed custom frameworks using Python and/or NodeJS to fetch data from multiple sources based on keywords and save it to CSV files or databases
- Designed and developed visual analytics and charts using Pandas, Dask, NumPy, Matplotlib, and Python Flask for threat analysis and statistical reporting
- Identified emerging threats through operations like data count calculation and percentage analysis of critical/high alerts
- Set up, tuned, and reviewed threat intelligence feeds from vendors and open-source sources to ensure relevance and reduce false positives
- Conducted adversarial emulation and mapped findings to the MITRE ATT&CK Framework
- Automated attacker simulations to and from corporate endpoints using SafeBreach
- Generated technical and management-level reports for strategic decision-making
- Reviewed partner and vendor security posture using corporate intelligence tools and frameworks
- Created Python/Bash-based custom frameworks for OSINT and vulnerability detection across Windows and Linux environments
- Acquired, managed, and integrated a variety of intelligence feeds with diverse datasets
- Collaborated with SOC and other technical teams to assist in remediation of threats and vulnerabilities
- Responded to crisis situations and security incidents, providing immediate analysis and support
- Managed client relationships and developed documentation such as Security Assessment Plans, Reports, Questionnaires, Rules of Engagement, Kick-off Briefs, and Exit Briefs
- Effectively communicated complex technical concepts to both technical and non-technical stakeholders
- Performed penetration testing across multiple layers — host, network, web applications, APIs, mobile apps, and cloud environments

As a COE/SME, performed the following specialized activities during my tenure at few organizations:

- Created and reviewed security policies, standards, and procedures
- Proposed and supported remediation strategies for identified vulnerabilities
- Conducted technical reviews and testing of new enterprise-level security technologies
- Advised on secure data deletion, system decommissioning, and equipment reuse practices in high-security environments
- Prepared and conducted audits and risk assessments to support regulatory and internal compliance
- Monitored security events across organization-wide networks and applications
- Conducted onsite and insider threat perspective penetration tests
- Performed security testing on air-gapped and cloud networks, including Azure and AWS
- Conducted wireless and Bluetooth penetration tests in a variety of operational environments
- Developed secure virtual labs for exploit creation, malware analysis, and product testing
- Authored advisories on 0-day exploits, CVE vulnerabilities, and other critical network threats
- Executed social engineering engagements as part of red team operations
- Identified common web vulnerabilities (XSS, CSRF, SQL injection, etc.) across platforms in a non-destructive manner
- Analyzed PCAP files, IDS logs, and honeypot data to identify potential attack vectors and vulnerabilities
- Directed research into evolving threats, tools, and techniques to improve security postures
- Performed de-compilation and reverse engineering of mobile, desktop, and binary applications using standard methodologies and best practices

---End of Resume---