# MANJUL VERMA

## Sr. Architect Product Information Security| Head Product Security Engineering

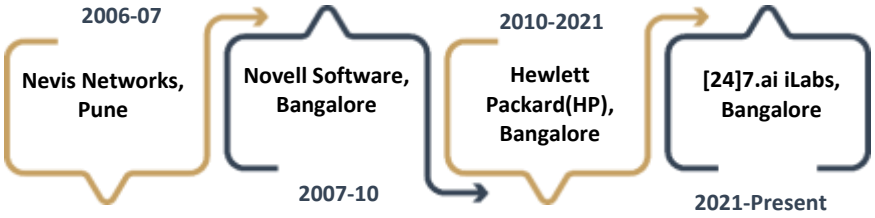
*A versatile & accomplished professional driving innovative security solutions as a seasoned leader in cybersecurity and product security architecture, focusing on enhancing safety and compliance across diverse technological platforms.*

+91 9611131235 | LinkedIn | Medium | verma.infosec@gmail.com

## PROFILE SUMMARY

- **Strategic** professional leveraging **over 2 decades** years of rich experience in **cybersecurity,** with a concentrated focus on **product security architecture and management in the technology industry,** ensuring the delivery of secure solutions.
- Currently, leading as the **Sr. Architect of Product Information Security at [24]7.ai iLabs,** end-to-end security measures for innovative products in a rapidly evolving technological landscape.
- **Expertise in formulating security strategies** and executing secure development practices, ensuring robust protection across all phases of product development.
- **Achieved substantial achievements** in driving security innovations, including the creation of advanced frameworks that enhance organizational security and compliance.
- **Exhibited strong leadership** by fostering collaboration, mentoring junior staff, and promoting a culture of security awareness and proactive risk management.
- **Formulated annual budgets** to optimize fund utilization for corporate goals and led cost estimation for business, regional infrastructure, and application projects.
- In-depth **understanding of regulatory compliance and industry standards**, ensuring seamless integration of security measures aligned with GDPR, NIST, and other key frameworks.
- Proven expertise in **collaborating with clients and top management** to shape strategic vision, drive change, implement emerging technologies, and enhance enterprise system performance and productivity.
- Actively involved in **continuous learning, academic consultancy,** and presenting emerging security trends at industry conferences.

## CAREER TIMELINE (Recent 4)




## WORK EXPERIENCE

**[24]7.ai iLabs, Bangalore | Senior Architect, Product Information Security**
**Head of Product Security for Conversational AI SaaS Platform | May 2021 – Present**

**Key Result Areas:**

- Responsible for end-to-end security in the Product Development Lifecycle of the Conversational AI SaaS platform, integrating advanced AI technologies such as Generative AI, NLP, computer vision, speech recognition, content moderation, AI gateways, and cybersecurity applications.
- Managed deployments across on-premises (data centers and LAN) and multi-cloud environments, including GCP, Azure, and AWS.
- Led the development and launch of "Privacy Analytics," a privacy-centric application that strengthened data protection and compliance, with high adoption among finance and telecom clients.
- Collaborated with cross-functional teams, including R&D Engineering, data analysts, IT, DevOps/SRE, legal, sales, and marketing, to achieve these outcomes.

## CORE COMPETENCIES

- Security Strategy Development & Implementation
- Secure Product Lifecycle Management
- Security Automation & Orchestration
- Shift-Left Expertise: devSecOps, LLMSecOps
- Cloud, Application and Networking Security
- Data Protection and Privacy
- People Management & Thought Leadership
- Compliance & Regulatory Frameworks
- Security Audits & Penetration Testing
- Cross-Functional Collaboration

## CAREER ACCOMPLISHMENTS

- Led security, privacy, and compliance strategy for (Gen)AI, multi-cloud SaaS, and IoT devices (Printers), ensuring robust protection across all platforms.
- Integrated secure SDLC practices and automated security in DevOps (CI/CD) for multi-cloud deployments, leveraging (Gen)AI technologies.
- Enhanced security across applications and infrastructure through collaboration with customers and security experts, staying ahead of emerging threats.
- Defined and implemented secure agile methodologies, applying shift-left practices to optimize development and accelerate time-to-market.
- Fostered a security-first culture by leveraging expertise in evolving threats, emerging regulations (e.g., GDPR, NIST), and industry standards.
- Aligned product security strategy with market trends, launching innovative features that strengthened the company's competitive edge.

**Highlights:**

- **Achieved $13M** in cost savings through optimization of security tools, shift-left automation, SaaS re-architecture in K8s/GKE, and the use of open-source solutions to reduce licensing costs in multi-cloud setups.
- Established the Customer Security Positioning (CSP) program to showcase security controls and gain third-party validation, increasing **NPS by 20 points** and improving customer satisfaction and loyalty.
- Introduced GenAI security innovations like AI Proxy, Content Moderation, Secure Prompting, and AI Ethics Safeguards, **reducing AI implementation costs by 30%** and enhancing security across organizational AI initiatives.
- Directed the agile Secure SDLC process, embedding security requirements, secure-by-design principles, and driving secDevOps and LLMSecOps, **reducing time-to-market by 25%.**
- Ensured compliance with industry standards, including PCIDSS, HiTrust, SOC2, ISO27001, GDPR, OWASP, and NIST, integrating robust security frameworks and **reducing compliance overhead by 15%.**

**Hewlett Packard(HP), Bangalore | Master (Sr.) Security Architect - worked on product security and devSecOps of IoT(Printer) centric cloud (AWS) ecosystem | June 2010 to May 2021**

**Key Result Areas:**

- Directed the security strategy for a Digital Ecosystem platform integrating IoT devices, AWS-based cloud infrastructure, client applications, and big data systems, supporting over 10 million users and 5 million devices.
- Oversaw security competitive intelligence and third-party certifications, positioning the platform as a leader in secure technology.
- Ensured full compliance with international security standards, including NIST, ISO, SOC2, OWASP, and GDPR, embedding security best practices across the Product Development Lifecycle.
- Partnered with diverse teams, including R&D, data analytics, IT, DevOps/SRE, legal, sales, and marketing, to align security initiatives with business objectives and deliver impactful outcomes.

**Highlights:**

- Spearheaded organization-wide security risk assessments using advanced methodologies like STRIDE, SAST, DAST, and VAPT, complemented by launching a bug bounty program. Integrated findings into the Secure SDLC, identifying and mitigating over 500 vulnerabilities, improving incident response efficiency by 25%, and **achieving $5M in cost savings.**
- Pioneered the development of a DevSecOps framework and a Product Security Quality (PSQ) model, reducing security vulnerabilities by 45% and accelerating **secure release cycles by 55%.**
- Innovated real-time threat management capabilities, including advanced Threat Inspection, Protection, and Monitoring systems, leading to **a 40% reduction in false positives** and strengthening customer confidence and trust.
- **Achieved a 7-point increase in NPS**, enhanced customer retention, and unlocked significant revenue opportunities through robust technical and administrative controls.

**Novell Software, Bangalore | Software consultant – worked on end point security solutions | March 2007-June 2010**

**Key Result Areas:**

- Evaluated and implemented safeguard controls, including IAM, Firewall, VPN, and NAT, while simulating adversarial offensive security scenarios and automating security features for Novell's IAM, ZESM, and Border Manager products.
- Oversaw product management, security architecture design, requirement analysis, vulnerability management, incident triaging and response, stakeholder engagement, and team hiring and development.

## TECHNICAL SKILLS

- **(Gen)AI Security**: Conversational AI; NLP; NER; LLMs (Azure OpenAI); LLM gateway/proxy; Guardrails; Prompt injections/hacking
- **Data Security**: Storage; Runtime; Transmission
- **Application Security**: Authentication / Authorization (Vault; SSO; OAuth; SAML; MFA); RBAC/ACLs; Cryptography; PKI & Digital Certificates; Web Application Firewall (WAF); API and web technologies (HTTPS; SOAP; REST; JSON; XML); OWASP Top 10
- **Cloud Security**: Compute (VMs; Containers; K8s/GKE); Storage; Networking/ACLs; Firewall; Key management or Vault
- **Network Security**: Protocols (TCP/IP stack - ARP; ICMP; DHCP; OSPF); Firewall; VPN (IPSec); SSH; SSL/TLS; Kerberos; SFTP/FTP
- **Operating System Security**: RTOS; (SE)Linux; Windows (Kernel & User Mode)
- **Hardware/Firmware Security**: Embedded systems; IoT; Desktop/Server; Secure boot; TPM; FOTA
- **IT Infrastructure Security**: On-premise; Data center (DC); Multi-cloud; Workload migrations & optimizations; Patch & Vulnerability management

## AREAS OF EXPERTISE

- **Trustworthy AI Security:** NIST-500-1, ATLAS, OWASP, Privacy & Traditional Defense-in-Depth
- **Secure SDLC:** OWASP SAMM, OKR, DoR & DoD, Acceptance & Release Criteria
- **Product Management:** Developing end-to-end security requirements of different personas, data sovereignty
- **Security Architecture:** OSA, Secure by Design & Default, Privacy by Design & Default, Threat Modeling (STRIDE)
- **VAPT & Risk Management**: SAST, DAST, SCA, Forensics, GDPR, OWASP, Incident & Threat Management
- **Compliances:** NIST, OWASP, Mitre, PCI DSS, HiTrust, ISO27001x1, SOC2
- **Vendor Risk Management:** Framework Development of 3rd-Party Evaluation, Including QnA, Acceptance Checklist & Criteria

## PREVIOUS WORK EXPERIENCE

**Nevis Networks, Pune | Sr. Software Engineer - Focused on internal (switching) security | Aug 2006 – Mar 2007**

Accountable for test planning, automation, security assessment scripting, and penetration testing of the LANSight Manager product at Nevis.

**Symphony (Kazeon) Services, Bangalore | Technical Lead | Feb 2006 – July 2006**

Worked on data center product security, including writing security assessment scripts and conducting penetration testing on the IS1200 (Information Server) built on NFS, CIFS, ONTAP6.5, and Linux platforms

**Juniper Networks, Bangalore | Member of Technical Staff | May 2004 – Feb 2006**

Developed offensive security assessment frameworks and automated UTM (Unified Threat Management) security products, including ns5gt/xt/204/500, isg2000, IDS/IDP, and NSM, with features such as VRRP/NSRP failover, TCP/IP, routing (Vrouters), OSPF, RIP, log management, and access control.

**Daybegins Engineering Innovations, Bangalore | Software Engineer - Specialized in perimeter security products | Feb 2000 – May 2004**

## EDUCATION

**Masters of Science (MS) in Information Technology,** SM University, (distance mode), Grade - 1st, 2009

**BCA,** MCRP University, Grade – 1st , 2000

## EXTRACURRICULAR ACHIEVEMENTS

**Publications:**

- Published business white papers on security technology, including customer security positioning and AI security design.
- Contributed to various defensive publications related to security technology and methodologies.
- Published research in magazines like "Hakin9".

**Conferences:**

- Frequent speaker at Bangalore Cyber Security Summit (2019/20).
- Mentor and reviewer for conferences (e.g., ICISS2022, Smart India Hackathon, IITs).