

# Sudhir Dubey

📞 1234567890 | 📧 Email | 💬 LinkedIn | 🐾 GitHub | 🌐 Blog

Security Engineer with 4+ years securing 5,000+ devices across ISO 27001 and PCI DSS environments. Expert in Skybox, AlgoSec, and auditing firewalls and network devices. Reduced manual configuration effort by 40% through strategic automation and vulnerability management.

## EXPERIENCE

### Senior Information Security Engineer @ISG

Infosys Ltd.

July 2023 — Present

Mumbai, Maharashtra

- Evaluated security compliance across **5,000+ network devices**, identifying critical vulnerabilities and executing remediation plans to harden infrastructure.
- Led **secure configuration management** for ISO 27001 and PCI DSS adherence, successfully securing and maintaining certification through rigorous audit preparation.
- Reduced manual effort for security configuration tasks by **40%** through process automation, documentation updates, and standardization, significantly accelerating task completion while ensuring comprehensive scope coverage.
- Designed and enforced **standardized security baselines** for heterogeneous network assets (Firewalls, Switches, Routers, NIPS) to ensure enterprise-wide policy consistency.
- Optimized Skybox Security Suite to **automate compliance auditing** and vulnerability reporting, significantly increasing validation efficiency.
- Spearheaded a **Proof of Concept (POC)** for AlgoSec to evaluate and deploy network compliance automation capabilities.

### Information Security Engineer @ISG

Infosys Ltd.

Oct 2021 — June 2023

Mumbai, Maharashtra

- Executed Network device assessments** against network security policies, identifying vulnerabilities and reporting non-compliance for immediate mitigation.
- Validated security configurations** across firewalls (Palo Alto, FTD, Check Point) and routing infrastructure (Cisco IOS and Nexus, Mellanox, Cumulus) to ensure defense-in-depth.
- Managed L1 security operations**, including metric collection, configuration preparation, and tracking the remediation lifecycle of reported vulnerabilities.

### Cyber Security Practice Intern

Gurugram Police

Jun 2021 — July 2021

Gurugram, Haryana

- Analyzed potentially compromised systems and network traffic using forensic tools like FTK Imager, Wireshark, and Burp Suite during cybercrime investigations. Also analyzed case studies of various cybercrimes.

## SKILLS

- Core Competencies:** Configuration Hardening & Auditing, Risk-Based Vulnerability Management (RBVM), Continuous Compliance, Network Auditing
- Network Technologies:** Palo Alto, Check Point (Cloud & On-Prem), Cisco (ASA, FTD, Nexus), Mellanox, Cumulus, NIPS
- Security Tools:** NSPM (Skybox, AlgoSec), Qualys, CyberArk, Cortex XSIAM
- Frameworks & Standards:** ISO 27001, PCI DSS, RSA Archer, ServiceNow

## CERTIFICATIONS

- Skybox Security Certified Vulnerability Control Expert (SCVCE)** – Skybox Security
- Skybox Security Certified Assurance Expert (SCAE)** – Skybox Security
- Infosys Certified Network Security Associate** – Infosys
- Python and Big Data Certificate** – CDAC
- Publication: Drug Safety Report Generator – IJSRCSEIT

## EDUCATION

### Sandip University, Maharashtra

B.Tech in Cloud Tech and Information Security - 8.7/10

Maharashtra, India

July 2017 — Sept 2021