VARGHESE ANIL

Leadership Role: Information Security Management | Cyber Security

+91 9323739259 / +9122 25793425

iamanil@gmail.com

VP - Cyber Investigation and Response Team (CIRT) / Lead Investigator, with **nearly 21** years of experience in Enterprise Information Security, Cyber & Security Operations, Network Administration, and Infrastructure Management; accomplishing the business objectives by leveraging broad range of technical insight against the unique challenges of complex business processes and requirements

PROFILE SUMMARY

- Technocrat with specialization in end-to-end **IT Security and Infrastructure Consulting, Management, Enterprise Integration Strategy, Enterprise Architecture and Consultancy Projects on IT systems**; directed the business operations through executive level planning and analyzed delivery issues in a timely fashion
- **Proven success in leading enterprise Information Security**, Cyber Security, Risk and Compliance vertical for large organizations
- Investigated information security incidents (legacy included) including backdoor, unauthorized access, network intrusion, malware infection, policy violation, data leakage, and so on
- Pivotal member of Cyber Investigation and Response Team (CIRT) investigations for the ASPAC region
- Successfully managed, conducted, and coordinated investigations utilizing Citi Security and Investigative Services (CSIS), Security Operation Centre (SOC) and other resources
- Exhibited leadership skills while leading 3 teams across Mumbai, Gurgaon, and Hyderabad with ~ 42 members
- Rich experience in managing **business continuity plan, disaster recovery plans,** process reengineering, continuous process improvement, and implementing best practices across the organisation

CORE COMPETENCIES

- Information Security (IS) Architecture, Planning & Consulting
- Business Continuity Planning & Implementation Roadmap
- Policy Design & Administration
- GRC (Governance Risk Management and Compliance)
- Change Management / Trend Analysis
- Cyber Security Framework / Vulnerability Management
- Systems Auditing / Incident Investigation / Problem Management
- IT Security Risk Assessment / IT Facilities Management
- Service Delivery
- Project/ Program Management
- Vendor Management
- People Leadership

CAREER TIMELINE

- **2002-2003** — Team Computers (P) Ltd., Mumbai
- **2003-2004** — GajShield InfoTech (I) Pvt. Ltd., Mumbai
- **2005-2005** — 4004 Incorporated, Mumbai
- **2005-2006** — Pidilite Industries Ltd., Mumbai
- **2006-2013** — BA Continuum India Pvt. Ltd., Mumbai
- **2013-2023** — Citibank NA, Mumbai

WORK EXPERIENCE

03 Jun'13 - 13 Sep'23: Citibank NA, Mumbai as VP - Cyber Investigation and Response Team (CIRT) / Lead Investigator

Key Result Areas:

- Spearheading strategic and operational initiatives for information and cyber security program
- Instituting IS Governance, Technology & Operational Risk, Incident Management practice within the organization
- Devising organizational Cyber Security Strategy by defining vision, mission and roadmap in quantitative manner with timelines
- Steering Incident Investigation to address security concerns utilizing IN-office resources to contain/remediate the incident
- Convening the Cyber Investigation and Response Team (CIRT) in addressing and investigating security incidents that arise

Highlights:

- Contributed towards:
  - Collection and preservation of digital evidence and coordinate required forensic examinations
  - Fraud Management program
  - Master Control Assessment (MCA) for Vigilance & Security functions @India

- Manage, conduct and coordinate investigations utilizing Security and Investigative Services (CSIS), Security Operation Centre (SOC) and other resources
- Timely escalation and notification to Senior Management on any incident investigation
- Timely incident updates in case management system
- Ensure local regulatory and data privacy issues are escalated and addressed as required

PREVIOUS EXPERIENCE

12 Jul'06 - 26 May'13: BA Continuum India Pvt. Ltd., Mumbai as Manager – Global Information Security

Highlights:
- Led GB project to reduce the time and risk involved with respect to Security events and their responses. (GB - Analyze phase)
- Directed administration of operations constantly for Security Operations Centre (SOC) and Insider Threat Controls as well as 24/7 Information Control Hotline to report information incidents and phishing
- Pivotal members of pilot project; guided a team for extension of control exceptions
- Facilitated the Inclusion of Information Control SMEs on new projects and expansions to reduce risk quotient of any project
- Organized trainings for the vertical - sync in coordination with the learning team to arrange Technical/ Domain/ Behavioral sessions
- Attained Onshore recognitions for supporting other critical processes attain 24/7 operations (DLP exceptions, DIM incidents, Urgent departures, etc.)

09 May'05 - 01 Jul'06: Pidilite Industries Ltd., Mumbai as Executive IT- Infrastructure & Networking

Highlights:
- Log monitoring and analysis of Checkpoint Firewall & IDS, manage Symantec proxy server and resolve Internet access issues
- Co-ordination with Helpdesk for closure of day-to-day network issues. Vendor co-ordination and follow up
- IT inventory maintenance and planning, assist in IT procurement – preparation of RFQ's, techno-commercial comparison
- Expense monitoring and maintaining reports
- Ensure timely payment of PSTN/ISDN/DSL/Leased line bills in co-ordination with accounts and branches

21 Feb'05 - 03 May'05: 4004 Incorporated, Mumbai as Network Engineer

Highlights:
- Deploying and configuration of Cisco VOIP phones, maintaining Cisco Call Manager and Cisco Unity Servers & formulation of rules on Cisco PIX
- Maintaining the network of 300+ users spread across two location and maintain least downtime

01 Dec'03 - 06 Nov'04: GajShield InfoTech (I) Pvt. Ltd., Mumbai as Support Executive

Highlights:
- Testing, installation and configuration of GajShield security appliances including formulation of security policies
- Technical support for products viz, Firewalls, IDS, Proxy with Content filter, VPN, mail server, G/W level Anti-Virus and scheduled backup of all appliances

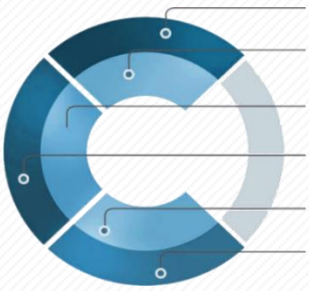
15 Jul'02 - 25 Nov'03: Team Computers (P) Ltd., Mumbai as Customer Support Engineer

Highlights:
- Deputed at Transasia Bio-Medicals Ltd. for handling administration of 120 workstations

TRAININGS

- CISSP Training from Infosec Train – Jan 2023
- Encase Computer Forensics – Feb 2017
- 1 week Training on SANS Security 504 – Hacker Techniques, Exploits, and Incident Handling – Mar 2014
- Cisco PIX Training from KARrox Technologies – Jun 2004
- One month Training on Networking and Systems at HCL Info Systems Ltd., NOIDA – Jun 2002
- 12 weeks' Training on Advanced System & Linux Administration at Linux Technologies Pvt. Ltd., Mumbai – Nov 2000

SOFT SKILLS



Collaborator

Communicator

Leader

Motivator

Planner

Negotiator

EDUCATION

- Bachelor of Computer Engineering from University of Pune, Loni (Dist. - Ahmednagar) in 2002
- Diploma in Public Speaking from Success Speakers Academy, Mumbai in 1992

CERTIFICATIONS

- GIAC Certified Forensic Analyst (GCFA) - SANS – 2020
- GIAC Certified Forensic Examiner (GCFE) - SANS – 2019
- Microsoft Certified Professional (MCP) - KARrox Technologies – 2004
- Cisco Certified Network Associate (CCNA) – KARrox Technologies – 2003

PERSONAL DETAILS

Date of Birth: 7th May 1978 **| Languages Known:** English, Hindi, Marathi, and Malayalam
Address: Flat #804, Nirvana C.H.S Ltd., Nehru Nagar, Kanjur-Marg (E), Mumbai – 400042