Kirubakaran Kamatchi

Information Security & Infrastructure Manager

kkirubakaran@gmail.com • +91 99414-80275 • Chennai, India
linkedin.com/in/kiruba81

Professional Summary

Results-driven Information Security & Infrastructure Manager with 15+ years of progressive IT security experience. Expertise in Identity and Access Management (IAM), Vulnerability Assessment and Penetration Testing (VAPT), and compliance frameworks including ISO 27001, SOC 1/2, HIPAA, and HITRUST. Proven track record of reducing security incidents by 30%, improving compliance scores by 40%, and enhancing operational resilience through strategic security initiatives. Specialized in endpoint security, SIEM implementation, business continuity planning, and insider-threat defense across cloud and on-premises environments.

Professional Experience

IT Security Manager Oct 2023 – Nov 2025
ERP Shipping Company Pvt Ltd *Chennai, India*

- Strengthened IAM governance by implementing Microsoft Entra ID with MFA enforcement and Conditional Access policies, reducing unauthorized access incidents by 30% through quarterly access reviews
- Enhanced endpoint security posture by administering ESET Protect Cloud and Trend Micro Apex One, improving threat remediation speed by 40% through automated response workflows
- Implemented comprehensive insider-threat monitoring using Teramind UBA and DLP solutions, reducing data exfiltration risks by 25% through real-time user behavior analytics
- Performed SIEM-driven threat detection and security analysis via Datadog, lowering false positive alerts by 20% through refined correlation rules and custom dashboards
- Improved audit readiness for SOC 1, SOC 2, and ISO 27001 certifications by closing 15+ compliance gaps and aligning IT processes with Annex A security controls
- Optimized Cloudflare log analytics and threat intelligence dashboards, enhancing detection capabilities and reducing mean time to response (MTTR) by 25%
- Built comprehensive Zabbix monitoring infrastructure with custom dashboards, improving IT service uptime visibility and reducing unplanned downtime by 20%

Manager – Information Security & Infrastructure Sep 2022 – Oct 2023
Veryx Technologies Pvt Ltd *Chennai, India*

- Developed and implemented ISO 27001-aligned security policies and procedures, increasing organizational compliance scores by 40% across all departments
- Directed enterprise infrastructure security strategy covering networks, servers, cloud platforms, and applications with zero security breaches during tenure
- Led Business Continuity Planning (BCP) and Disaster Recovery (DR) initiatives and testing exercises, improving RTO/RPO compliance by 25%
- Conducted SIEM integration and continuous security monitoring programs, reducing incident response times by 30% through automated alerting
- Delivered comprehensive security awareness training programs, raising employee security maturity ratings by 40% and reducing phishing susceptibility

Senior Information Security Auditor Mar 2022 – Sep 2022
Global Healthcare Billing Partners *Chennai, India*

- Led HIPAA and HITRUST compliance audits, reducing open non-compliance items through improved documentation and implementation of security controls
- Developed and executed comprehensive BCP workflows, increasing organizational preparedness and resilience by 30%

- Enhanced security policies and procedures to strengthen healthcare information governance and ensure regulatory compliance
- Conducted gap assessments and provided remediation recommendations for Protected Health Information (PHI) handling processes

Senior Technical Support Engineer Nov 2008 – Mar 2022
Exela Technologies Pvt Ltd *Chennai, India*

- Managed enterprise-wide vulnerability management program, reducing high-severity security issues by 30% through systematic patching and mitigation strategies
- Executed Business Continuity Planning (BCP) and Disaster Recovery (DR) programs across multiple business units, minimizing outage impact and ensuring operational resilience
- Conducted comprehensive risk assessments, internal security audits, and root cause analysis (RCA)-driven incident investigations to strengthen overall security posture
- Delivered Security Operations Center (SOC) escalation support and coordinated with cross-functional teams for timely remediation of critical security incidents
- Provided technical leadership for infrastructure projects including server migrations, network upgrades, and security tool implementations

Technical Support Engineer Oct 2005 – Oct 2008
Quick Heal Technologies Pvt Ltd *Chennai, India*

- Performed malware analysis, endpoint troubleshooting, and comprehensive root cause analysis (RCA) documentation for security incidents
- Trained end-users and technical teams on security best practices, threat prevention controls, and safe computing practices
- Assisted customers via phone, email, and chat channels to deliver prompt and effective technical solutions for antivirus and endpoint security issues

Education

Master of Science in Electronics Jun 2001 – Apr 2003
St. Josephs College Autonomous *Trichy, India*

Bachelor of Science in Electronics Science Jun 1998 – Jun 2001
Sengunthar Arts and Science College *Tiruchengodu, India*

Technical Skills

Security Frameworks & Compliance: ISO 27001, SOC 1/2, HIPAA, HITRUST, NIST Cybersecurity Framework, PCI DSS
Identity & Access Management: Microsoft Entra ID, Azure AD, Active Directory, MFA, Conditional Access, SSO
Vulnerability Management: Tenable, Nessus, Qualys, Veracode, Rapid7, OpenVAS, vulnerability scanning and remediation
SIEM & Monitoring: Datadog, Zabbix, Splunk, log analysis, correlation rules, threat detection, security analytics
Endpoint Security: ESET Protect Cloud, Trend Micro Apex One, Symantec Endpoint Protection, EDR, antivirus
Insider Threat & DLP: Teramind UBA, Data Loss Prevention, user behavior analytics, insider threat detection
Cloud Security: Cloudflare, AWS security, Azure security, cloud infrastructure protection, CDN security
Risk Management: Risk assessments, incident response, root cause analysis, security audits, compliance reporting
Business Continuity: BCP/DR planning, RTO/RPO optimization, disaster recovery testing, resilience strategies

Certifications

- **ISO/IEC 42001:2023 Lead Auditor** – Mastermind Assurance, Valid Feb 2026 to Feb 2029
- **ISO/IEC 27001:2022 Lead Auditor** – Mastermind Assurance, Valid Dec 2025 to Dec 2028
- **Cybersecurity Fundamentals** – IBM, Mar 2022
- **Certificate of Proficiency** – Tenable, Jul 2021
- **Advanced Network Security with Cisco ASA Firewall** – Sans Bound Solutions, Mar 2009
- **Cisco Certified Network Associate (CCNA)** – Sansbound Networking School, Jul 2004

Additional Information

Languages: English (Advanced), Tamil (Fluent)
Key Achievements: Reduced unauthorized access by 30%, improved compliance scores by 40%, enhanced threat remediation speed by 40%, reduced false positive alerts by 20%, improved RTO/RPO compliance by 25%