VICKRAM D

SOC Analyst | IT Infrastructure & Cybersecurity

+91 6380215490 | vickramdurai111@gmail.com | LinkedIn: linkedin.com/in/vickram-d05 | GitHub: github.com/vickram-5

Profile Summary

B.Tech IT graduate with hands-on experience in **IT Infrastructure, Networking, and Cybersecurity Operations**. Skilled in **network configuration, endpoint protection, and security compliance** aligned with **ITIL and ISO 27001** standards. Experienced in **network scanning, vulnerability assessment, and SIEM monitoring** using **Nmap, SpiderFoot, Splunk, and Wazuh**. Strong understanding of **access management, risk assessment, and audit documentation** within **SOC2 and ISO frameworks**. Passionate about **network security, governance, and continuous improvement** in IT operations and InfoSec environments.

Key Projects

1 Network Scanning & Vulnerability Enumeration (Nmap)

Executed subnet scans (192.168.1.0/24) using Nmap to identify live hosts, open ports, and service versions. Performed TCP SYN and OS detection scans to map vulnerabilities and prioritize risk mitigation.
(Key Focus: Networking, Vulnerability Assessment, Incident Response)

2 OSINT-Based System Footprinting (SpiderFoot)

Configured and executed SpiderFoot for OSINT-based reconnaissance. Discovered domain, IP, and host data to assess exposure and correlation with external sources. Visualized network data graphs to enhance asset discovery and risk visibility.
(Key Focus: Network Intelligence, Governance, Risk Identification)

3 Information Security & Compliance Implementation

Built a simulated compliance framework aligned with SOC2, ISO 27001, and NIST standards. Performed user access reviews, vulnerability scans, and patch validation using Nessus and Wazuh. Developed security policies for incident response and audit readiness.
(Key Focus: Risk Assessment, Compliance, Governance)

4 IT Infrastructure & Service Delivery Optimization

Implemented ITIL-based service delivery framework for improved uptime and user experience. Configured Active Directory, Windows Server, and Microsoft 365 Admin for centralized control. Automated patching and backup processes while ensuring VPN-based secure access.
(Key Focus: IT Infrastructure, Service Management, Automation)

5 Splunk SIEM Security Monitoring & Threat Detection

Configured Splunk Enterprise SIEM to monitor logs, detect anomalies, and visualize attack patterns. Built dashboards for privilege escalation, brute-force detection, and MITRE ATT&CK; correlation.
(Key Focus: SIEM, Security Monitoring, Threat Response)

6 Windows Endpoint Hardening & Security Policies

Configured GPOs, BitLocker, and Windows Defender for endpoint protection and data security. Implemented password, audit, and lockout policies to meet ISO 27001 security baselines.
(Key Focus: Endpoint Hardening, Access Control, Compliance Alignment)

Core Competencies

- IT Infrastructure Management (Servers, Networks, Endpoints, Cloud)
- Security Monitoring & Incident Response (SIEM, EDR, DLP)
- Network Configuration, VPN Management & Troubleshooting
- Risk Assessment & SOC2 / ISO 27001 Compliance Support
- Governance, Policy Implementation & Audit Documentation
- Access Control & Privileged Account Management
- Automation, Patch Management & Continuous Improvement

Technical Skills

Networking: TCP/IP, VPN, DHCP, DNS, LAN/WAN, Routing, Switching, Wireshark, pfSense, Snort
Infrastructure & Cloud: Windows Server, Linux (Ubuntu / Kali), Microsoft 365 Admin, Azure
Security Tools: Splunk, Wazuh, ELK Stack, Nessus, SpiderFoot, Security Onion
Governance & Compliance: SOC2, ISO 27001, NIST, GDPR (familiarity)
Endpoint & Patch Management: Group Policy, BitLocker, Windows Defender, Updates
ITSM Tools: ServiceNow, Jira, Freshdesk
Scripting: PowerShell, Command Prompt

Professional Experience

TeamLease Services Pvt. Ltd | Bajaj Finance Ltd — IT Support & CRM Analyst (Mar 2024 – Jul 2025)
• Managed user access, troubleshooting, and patch updates across end-user systems.
• Supported VPN configuration, Active Directory, and license compliance.
• Ensured ITIL-aligned ticketing and incident documentation via ServiceNow.

Cogent E Services Ltd — Customer Care Executive (Sep 2022 – Mar 2024)
• Assisted customers with technical escalations, documenting incidents in ticketing tools.

Bajaj Finance Ltd (RR Financial Services) — Sales Executive (Jun 2018 – Oct 2018)

Education & Certifications

B.Tech in Information Technology — SS International University (2016 – 2020)
Cybersecurity Training & Hands-on Practice — LinkedIn E-Learning (2019 – Present)

Certifications: CompTIA CySA+ (Linkedin Learning), CISM (Linkedin Learning), CEH (Linkedin Learning), Tech Mahindra Cybersecurity Program, Microsoft Azure AI Fundamentals, ITIL Foundation (Planned)