Logesh Chandrasekar

+91 6382339981 | logeshchandrasekar5@gmail.com | www.linkedin.com/in/logeshchandrasekar5

PROFESSIONAL SUMMARY

Senior Information Security Analyst with 3+ years of experience in threat detection, incident response and security operations. Passionate about maintaining robust security frameworks and ensuring adherence to industry best practices. Proficient in vulnerability assessments, penetration testing, identifying and fine-tuning EDR/EPP solutions to improve detection accuracy. Skilled in endpoint, network and cloud security, with hands-on experience managing firewalls, endpoint protection, and identity security. Adept at log analysis, threat hunting and automation using PowerShell and Python, driving proactive security improvements and reducing incident response time.

TECHNICAL SKILLS

- **Operating System:** Windows (10, 11, Server 2016, 2019), Linux (Ubuntu, Kali, Parrot), macOS (Ventura 13, Sonoma 14, Sequoia 15)
- **Networking:** TCP/IP, DHCP, DNS, VPN, Firewalls, SSL/TLS, SSH, IDS, IPS
- **Standards and Methodologies:** Threat Modeling (STRIDE), OWASP Top 10, Threat Intelligence Lifecycle
- **Framework:** ISO/IEC 27001:2022, GDPR, CIS Controls, NIST (RMF, CSF), PCI DSS, SOC2, MITRE ATT&CK
- **Security & Analysis Tools:** Wireshark, Nmap, Zen Map, Tenable Nessus, Metasploit, Yersinia
- **Log Analysis & SIEM Correlation:** Microsoft Sentinel, Wazuh
- **Extended Detection & Response (XDR) Tuning:** Microsoft Defender, Microsoft Purview
- **Endpoint Protection & DLP Monitoring:** Trend Micro, Sophos (EPP), Qualys (Patch management & VMDR)
- **Phishing Analysis:** Email Header Analysis, SPF/DKIM/DMARC, GoPhish
- **Compliance:** Compliance management, Incident response, Data Privacy, Risk Mitigation, Audit Support, BCP, DR, ISMS Implementation
- **Language:** SQL, KQL, PowerShell, Python

CERTIFICATIONS

- **Qualys Certified Specialist – Web Application Scanning** (Mar 2024 – Mar 2026)
- **CompTIA Security+ ce Certification, CompTIA** (Sep 2023 – Sep 2026)
  Certification Number: YZ049185F2R410C0
- **ISO 9001:2015 Quality Management System** (July 2023)
  Certification Number: QHSE-QMS-IAC01609
- **ISO/IEC 27001:2022 Information Security Management System** (July 2023)
  Certification Number: QHSE-ISMS-IAC01633
- **AWS Certified Cloud Practitioner** (Feb 2022 – Feb 2025)
  Validation Number 9SVTQ08DGMV1Q35P
- **ITIL V4 Foundation** (Feb 2021)
  Certification Number: GR671234899LC
- **MCSE: Microsoft Certified Solutions Expert: Core Infrastructure** (Jan 2021)
  Certification Number: H627-9090
- **MCSA: Microsoft Certified Solutions Associate: Windows Server 2016** (Dec 2020)
  Certification Number: H619-1955
- **CCNA: Cisco Certified Network Associate** (Feb 2020 – Feb 2023)
  Certification Number: ME8V0QQLWPF41MKD

EDUCATION

Fanshawe College - **Canada** (Sep 2017 – Apr 2019)
Ontario College Diploma - Internet Applications and Web Development

Dr. NGP Arts and Science College - **India** (Jun 2013 – Apr 2016)
Bachelor of Science – Computer Technology

WORK EXPERIENCE

Senior Information Security Analyst (April 2025 to Present)
Verticurl Marketing Pvt.ltd

- Executed comprehensive ISO 27001:2022 internal audits of production and support teams to assess ISMS effectiveness and ensure alignment with organizational security policies
- Played a key role in achieving successful ISO 27001 audit outcomes by proactively preparing documentation, gathering evidence, and coordinating with stakeholders to ensure a smooth and efficient audit process
- Proactively managed client security questionnaires, providing clear, evidence-based responses and collaborating with stakeholders to remediate control gaps, ensuring comprehensive compliance and client satisfaction
- Proficient in developing, maintaining, and updating security incident response procedures and playbooks, incorporating industry best practices and lessons learned from past incidents
- Proficient in risk management framework enhancement, risk assessment, security auditing, and penetration testing
- Collaborated with business units to define security requirements for new implementations and resolved security related inquiries
- Developed and delivered comprehensive security awareness training and user education programs to specific departments and new hires

IT Security Analyst (July 2023 to March 2025)
Verticurl Marketing Pvt.ltd

- Successfully implemented Sophos XDR, WithSecure MDR and MDE-EDR to analyze security incidents, implemented containment measures and developed preventive strategies
- Designed, documented and deployed effective SOC and SOP procedures to ensure consistent security practices and recommended remediation actions
- Performed in-depth incident response activities, including evidence collection and preservation to support security incident investigations
- Identified, collected and analyzed digital evidence related to security breaches, system anomalies and data integrity issues
- Actively contributed to incident response activities by following standardized incident management procedures and collaborated with security teams to effectively manage security incidents from inception to resolution
- Served as the primary point of contact for client security inquiries, providing clear, concise, and accurate information regarding security policies and procedures details
- Efficiently scheduled patch deployment jobs tailored to specific asset types and swiftly deployed emergency patches as needed through Qualys

Associate Specialist - IT (Oct 2022 to June 2023)
Verticurl Marketing Pvt.ltd

- Provided IT support for new hires, including system and access provisioning, workstation setup and software installation
- Effectively managed IT incident resolution and service request fulfillment, ensuring timely response and closure within defined SLAs
- Accurately tested, installed, troubleshot, identified, repaired, setup, resolved, maintained and documented end user endpoint system technical issues regarding laptop/desktop support, network drop and other IT related technology issues
- Efficiently categorized and prioritized end-user and IT service requests based on urgency and offered comprehensive first-line support, ensuring timely communication, taking ownership of issues and escalating appropriately