THIRUVARASU THIRUGNANAM

Cybersecurity | Network Security | Security Operations
Miami, FL • +1 (312) 868-8532 • mailto:thiruvarasuthirugnanam@outlook.com
www.linkedin.com/in/thiruvarasu • www.thiruvarasuthirugnanam.com

PROFESSIONAL SUMMARY

Cybersecurity and network security professional with an M.S. in Cybersecurity from DePaul University and 2+ years of professional experience securing enterprise networks, systems, and sensitive data across healthcare, finance, and technology environments. Experienced across the full security lifecycle: threat detection and incident response, vulnerability management, firewall and VPN administration, DLP and access control, and compliance alignment to NIST and CIS Controls. Currently the sole security practitioner for a growing technology company, responsible for detection, response, system hardening, and audit support. IEEE-published researcher in applied machine learning.

TECHNICAL SKILLS

Security Operations & Incident Response: SIEM (Splunk), IDS/IPS (Snort, Wazuh), incident response, threat detection, log analysis, MITRE ATT&CK

Vulnerability & Threat Management: Nessus, Nmap, Metasploit, Burp Suite, Hydra, Hashcat; penetration testing, system hardening, patch management

Network & Infrastructure Security: Firewalls, VPNs, ACLs, VLAN segmentation, network segmentation, DLP, UBA, disaster recovery

Digital Forensics: Autopsy, FTK Imager, RegRipper, Wireshark

Systems & Cloud: Windows Server 2019/2022, Active Directory, DNS, NTFS, Linux, Cisco IOS, AWS (EC2, S3, VPC), Docker, VMware

Programming & Automation: Python, PowerShell, Bash, SQL, C++, JavaScript, MATLAB

Governance & Compliance: NIST CSF, CIS Controls, HIPAA, GDPR, SOX, CIS Benchmarks; security documentation, audit support

PROFESSIONAL EXPERIENCE

Device Connect LLC — Doral, FL **Mar 2026 – Present**

Systems and Network Administrator III

- Design, implement, and manage cybersecurity infrastructure including firewalls, IDS/IPS, VPNs, routers, switches, and network segmentation policies protecting internal and customer-facing systems.
- Monitor network traffic for unauthorized access attempts and anomalous activity; lead incident response end to end, spanning containment, eradication, recovery, and post-incident root cause analysis.
- Deploy and administer data loss prevention (DLP) and user behavior analytics (UBA) tooling to detect insider threats and enforce least-privilege access across all systems.
- Conduct vulnerability assessments, penetration testing, and system hardening across servers, workstations, and cloud environments; manage patch cycles to reduce organizational attack surface.
- Administer network servers, cloud systems, backup and disaster recovery, and workstation configuration and inventory; manage cybersecurity tool licensing and third-party vendor renewals.
- Maintain security documentation and support compliance audits, ensuring alignment with NIST and CIS Controls frameworks; serve as escalation point for cybersecurity troubleshooting across the organization.

FTT LLC — Miami, FL **Mar 2025 – Feb 2026**

Systems and Network Administrator

- Administered and monitored Windows Server 2019/2022 environments supporting business-critical infrastructure across 50+ server instances.
- Developed and deployed PowerShell scripts automating server health checks, log collection, and user account audits, substantially reducing manual administrative workload.
- Configured and managed Active Directory, DNS, and NTFS permissions to maintain secure domain operations across the server estate.
- Implemented patch management and endpoint hardening aligned to NIST guidelines, supporting clean results across internal audit cycles.
- Managed workstation inventory, maintenance logs, data archiving, and company-wide software subscription lifecycle; provided frontline technical support across hardware, software, and network issues.

Databels — Tiruchirappalli, India **Mar 2021 – Feb 2022**

Software and Security Engineer

- Supported administration of enterprise firewalls, VPNs, and network security protocols for healthcare and finance sector clients.

- Designed and enforced role-based access control (RBAC) policies for 50+ users, reducing unauthorized access incidents over the following six months.
- Configured Splunk SIEM correlation rules across a 50+ device network, improving threat detection coverage.
- Implemented VLAN segmentation and ACLs to reduce network attack surface; investigated and resolved critical outages through root-cause analysis and preventive remediation.
- Delivered phishing awareness training to 20+ employees, measurably reducing successful phishing attempts.

MAXVY Technologies Pvt Ltd — Bengaluru, India **Sep 2018 – Feb 2019**
Embedded Systems Security Intern

- Implemented AES-256 and RSA encryption across IoT device firmware; developed secure boot protocols to prevent unauthorized firmware modification.
- Identified and patched critical firmware vulnerabilities through systematic testing across deployed devices.

VOLUNTEER EXPERIENCE

Refugee-Immigrant Young-Adult Neighbor (RYAN) **Sep 2024 – Feb 2025**
Cybersecurity Engineer (Volunteer)

- Monitored and triaged security events across organizational systems, containing threats before escalation and documenting findings for compliance records.
- Conducted vulnerability scans and security assessments across network and endpoint environments, producing findings reports that drove security posture improvements.
- Implemented and enforced security policies with cross-functional teams; maintained current documentation for security processes, controls, and access records.

EDUCATION

DePaul University — Chicago, IL **Mar 2022 – Mar 2024**
Master of Science, Cybersecurity — GPA: 3.54 / 4.0

Coursework: Network Security, Enterprise Security Infrastructure, Governance Policies, IT Risk Management, Cyber Law & Ethics, Computer Forensics.

Sri Krishna College of Engineering and Technology (Anna University) — Coimbatore, India **Aug 2017 – Apr 2021**
Bachelor of Engineering, Computer Science and Engineering — CGPA: 7.99 / 10

CERTIFICATIONS

- Google Cybersecurity Professional Certificate — Google
- Cisco Certified: Cybersecurity Essentials | IoT Fundamentals | Packet Tracer | Entrepreneurship
- VMware IT Academy: Network Virtualization Concepts | Software-Defined Storage Concepts
- AWS Cloud Computing (badge)

SECURITY PROJECTS

Enhancing Cybersecurity through Stylometric Analysis — DePaul University **Jan – Mar 2024**
Built an authorship-verification and impersonation-detection system for digital text. Engineered lexical and POS-tag stylometric features, applied Chi-square and ReliefF feature selection, and trained an ensemble bagged-tree classifier achieving 87.5% accuracy, 0.90 precision, and 0.873 F1 on held-out data. Python, NLP, scikit-learn.

Computer Forensics Investigation (Cold Case Lab) — DePaul University **Oct – Nov 2022**
Conducted a full forensic examination of a disk image: recovered deleted files, reconstructed user activity, identified hidden encrypted containers and malware artifacts, and produced a complete timeline analysis and incident report. Autopsy, FTK Imager, RegRipper.

Reversible Data Embedding Using Difference Expansion — Sri Krishna College **2019**
Implemented a high-capacity, low-distortion reversible watermarking scheme using difference expansion on pixel pairs, enabling exact original-image restoration after extraction. Achieved 2–3 dB PSNR improvement over G-LSB and RS methods at equivalent payload. MATLAB, cryptography.

PUBLICATION

Thirugnanam, T., et al. "Scrutinizing Students Performance using Machine Learning." International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2021.