Pravin Kumar Kumaravel Ananthi

Email: pravink8122@gmail.com
Phone: +1 (365) 883-3237
Linkedin: linkedin.com/in/pravinkumar8122
Portfolio: www.pravinkumar.site
Address: 1673 Clearbrook Drive Oshawa, ON L1K 0V9

SUMMARY

- Entry-level cybersecurity professional with three years of experience in technical support, system administration, and IT security.
- Hands-on experience in monitoring and triaging security incidents using tools like Wazuh, Crowdstrike EDR, and Bitdefender EDR.
- Skilled in cloud security with practical experience in AWS and GCP, focusing on IaaS security and compliance best practices.
- Proficient in endpoint protection tools, SIEM solutions, and vulnerability assessment techniques.
- Familiar with cybersecurity frameworks including MITRE ATT&CK, NIST CSF, and CIS Benchmarks, applied in academic and lab environments to identify and mitigate threats.
- Strong scripting skills in PowerShell and Bash for automation of administrative and security tasks.
- Competitive CTF participant with a passion for continuous learning through home labs and cybersecurity challenges.

WORK EXPERIENCE

Helpdesk Technical Support Specialist - June 2021 - August 2023

Trimble Inc.

- Delivered Tier-2 IT support for Windows, Mac, and Linux environments, resolving escalated technical issues with a 30% improvement in ticket resolution speed.
- Conducted incident triage and analysis using tools like CrowdStrike EDR and Bitdefender EDR, ensuring a 40% reduction in endpoint security incidents.
- Documented troubleshooting processes, creating resources used by 20+ team members to ensure consistent resolution strategies.
- Led system imaging and deployment projects for enterprise environments, diagnosing and addressing post-deployment issues.
- Oversaw asset management and secure disposal of decommissioned devices in alignment with data security policies.
- Enhanced collaboration with cross-functional teams, improving service delivery and communication.

Associate Systems Engineer - June 2020 - April 2021

Technosprint Info Solutions

- Provided Tier-1 technical support, achieving a 95% ticket resolution rate by troubleshooting hardware, software, and network issues.
- Supported user account management and configuration for Google Workspace and O365, optimizing access

control and workflow.

- Conducted diagnostics and audits remotely, improving system uptime by addressing critical technical issues promptly.
- Collaborated with senior engineers to identify and resolve complex technical problems, reducing average resolution time by 20%.
- Managed multi-channel support requests, enhancing end-user satisfaction and improving SLA adherence.

SKILLS AND TOOLS

- **Languages:** Python, Bash, PowerShell
- **Operating Systems:** Linux, Windows, MacOS, Remnux, Kali, FlareVM, Windows Server 2022.
- **Tools:** Wazuh, Wireshark, Nmap, Burp Suite, Recon-ng, Aircrack-ng, Nikto, Autopsy, IDA PRO, VMware, Active Directory, Crowdstrike EDR, Bitdefender EDR, Splunk, CISCO Firewalls, Remote Desktop, ServiceNow, JIRA, O365, GSuite, AWS, GCP, Security Onion.
- **Concepts:** Networking protocols, routing and switching, Incident Response, Vulnerability Management, Active and Passive Reconnaissance, Digital Forensics, Network Security, Cloud Security, EDR, IDS/IPS, WAN Technologies, Cryptography, Perimeter Control, Phishing Campaign, Compliance Auditing, MITRE ATT&CK Framework and NIST Cybersecurity Framework.

PROJECTS AND ACTIVITIES

- **SEIM Homelab with Wazuh:** Designed and configured a SIEM homelab with Wazuh to simulate log collection and evidence archiving, supporting mock compliance audits such as SOC 2 and NIST CSF.
- **High-Availability VPN Between AWS and GCP:** Designed and implemented a high-availability VPN connection to ensure secure and seamless data communication between two cloud platforms.
- **Private Cloud Infrastructure Deployment:** Deployed a private cloud infrastructure using OpenNebula and VMware, optimizing resource allocation and ensuring robust security configurations.
- **Network Security Design and Simulation with Cisco Packet Tracer:** Configured and simulated a secure enterprise network using Cisco Packet Tracer, implementing firewalls, VLANs, and IDS to monitor and mitigate potential threats.

EDUCATION

Postgraduate Certificate in Cybersecurity - Durham College (September 2024 – April 2025)

Postgraduate Certificate in Virtualization and Cloud Computing - Conestoga College (September 2023 – April 2024)

Bachelor of Technology in Information Technology - Agni College of Technology (August 2016 – July 2020)