+1 7058175542
Mississauga, Canada
parthkdave05@gmail.com

Parth Dave

github.com/parth050501
linkedin.com/in/parth05dave

Aspiring cyber security professional with a strong foundation in network security and programming. Committed to contributing to an organization's success through a strong work ethic, adaptability, and a passion for learning.

Technical Experience

Network Techlab Pvt Ltd **India**

SME SOC **June 2021 – Present**

- Built 15 to 20 sophisticated incident response campaigns, executed forensic analysis and informed root cause to contain security breaches, minimized outages while cutting off further exploitation.
- Proactively identified the presence of advanced threats within client environments using MISP,ELK,Snort,Splunk.
- Ensured the deployment and management of SIEM (Security Information Event Management) systems across massive corporate footprints, thus enabling real-time monitoring and a rapid response to organizational security events.
- Conducted security assessments and tabletop exercises, providing clients with actionable recommendations to strengthen their security posture across cloud, network, and application layers.
- Built and refined Security Operations Centre (SOC) workflows to work with industry standards, and mitigation capabilities, resulting in better detection, response times and threat reduction efficiency.
- Collaborated effectively with a team of business executives and stakeholders on complicated cybersecurity incidents to help align technical security controls and organizational goals.

Network Engineer (Intern) **October 2019 – May 2021**

- Designed and deployed secure network architectures, including routers, switches, firewalls, and VPNs, improving connectivity, network security and remote access for enterprise environments.
- Notified Clients of True positive signal alerts, through templates & informed high priority views by phone
- Maintenance of firewall rules with source, destination IPs, ports and transport protocols for improved network security.
- Led the upgrade and migration of network systems, ensuring minimal downtime and seamless integration with existing infrastructure.
- Created with the support of OEM Technical Assistance Centres (TAC) to client specific issues basic to intermediate customer support tickets and requests, assisting clients via email and phone when necessary.

CERTIFICATIONS

CCNA

Credential ID CSCO14543114 **Jan 2024-Jan 2027**

Education

Post-Graduation Artifical Intelligence with Machine Learning **Jan 2024-Present**
Humber College

Post-Graduation Big Data Analytics **May 2023-Dec 2023**
Georgian College

Skills

- Cybersecurity Tools: Wireshark, Nmap, Metasploit, Antivirus, WebSec, FIM, OpenVPN, MISP, ELK
- Programming: Python, C/C++, Bash
- Network Security: Firewall config, IDS/IPS, VPNs
- Vulnerability Assessment: Nessus, OpenVAS, ELK
- OS: Windows, Linux (Kali, Ubuntu, CentOS)
- Incident Response: SIEM, Forensics, Threat Analysis, SOC, Risk Mitigation, Incident Management
- Cloud: AWS, Virtualization, Networking, Security, Containers, Serverless