Pratinav Chandra

pratinav.chandra1997@gmail.com | 240-927-9770 | College Park, MD
· pratinavchandra.github.io · inf0spec.medium.com · linkedin/in/pratinav-chandra · github.com/pratinavchandra ·

EDUCATION

University of Maryland | A. James Clark School of Engineering — **College Park, MD**
Master of Engineering - Cybersecurity — *Aug 2022 - May 2024 (Expected)*

Manipal University — **Jaipur, India**
Bachelor of Technology - Computer Science & Engineering — *July 2015 - June 2019*

SKILLS

• **Domain:** Network Security, Security Monitoring, Digital Forensics and Incident Response, OSINT, Penetration Testing, Cloud Security, Automation, Packet & Log Analysis, Computer Networking, Virtualization, Troubleshooting, Documentation
• **Infrastructure:** Firewalls, Web proxies, VPN, IDS, Routers, Switches, Raspberry Pi, AWS (Amazon Web Services)
• **Tools:** Splunk, Wireshark, tcpdump, Burp Suite, Postman, MITRE ATT&CK, Solarwinds NPM, Nmap, Metasploit, Yara, Snort, Zeek, Volatility, Prometheus, Docker, Canary Tokens, Visio, ServiceNow, MS Office (Word, Excel, PowerPoint) etc.
• **Programming and Scripting Languages:** Python, Bash, C, Java, HTML, CSS, JavaScript
• **Operating Systems:** Windows, Linux (Debian, Ubuntu), macOS
• **Courses & Certifications:** Practical Malware Analysis and Triage by TCM Security Academy (November 2022), Cyber Defense Path by TryHackMe (July 2022), Palo Alto Networks Certified Network Security Administrator by Palo Alto Networks (February 2021), Splunk Fundamentals (August 2019)

WORK EXPERIENCE

Dell Technologies – *Senior Cybersecurity Analyst* — *Bengaluru, India · July 2019 - July 2022*
• Served as part of a fast-paced global Cyber Defense team handling **high-priority network security incidents** and managed network security infrastructure with a **98% customer satisfaction rating**.
• Implemented security architectures and deployed and **configured network security solutions** for the segmentation of multiple sites globally, **reducing the attack surface by 80%.**
• Created monitoring alerts, built dashboards, and **extracted insights from enterprise network traffic** and network security device logs using Splunk, Solarwinds, and Firemon, **increasing visibility by 60%.**
• Spearheaded the development of tools for the **automation** of processes and workflows and **reduced the manual workload on the team by 70%** within four months.

Tecelec Engineers – *Software Development Intern* — *Vadodara, India · Jan 2019 - April 2019*
• Developed web applications to automate earthing and cable sizing calculations using React JS, Node JS, and MongoDB Atlas Database.
• Modelled innovative Python tools for the automation of technical processes that **reduced workload** on teams from days to seconds and also **decreased the cost of resources by 50%.**

PROJECTS

Cloud Migration Strategies - *University of Maryland* — *December 2022*
• Re-architected a web application to migrate it to the cloud with a security-first approach to enhance resiliency, Identity and Access Management (IAM), data protection, compliance, secure system administration and coding best practices.
Technologies used: Amazon Web Services

Home Cybersecurity Lab - *Independent Project* — *April 2022*
• Designed a home cybersecurity lab from scratch to **test vulnerabilities and open-source tools**.
• Deployed an **isolated malware analysis lab**, configured a Raspberry Pi 4 to run ESXi ARM and host multiple virtual machines to run services and tools **to enhance the security of the lab and increase visibility on the network**.
• Established **edge defense** by deploying a Palo Alto Networks **firewall** to analyze and monitor network traffic.
Technologies used: Python, Linux, Prometheus, Grafana, ESXi, Raspberry Pi, FlareVM, REMnux, PANW Firewall

Technical Content Writer - *InfoSec Write-ups* — *September 2021 - Present*
• Researched and published technical write-ups as part of the team at "InfoSec Write-ups", which is the largest Cybersecurity publication on medium.com with over **23k followers**. My write-ups have been **recommended as reading resources** by a SANS instructor as well as **featured as walkthroughs** at leading blue team CTF platforms.

IoC Miner - *Independent Project* — *April 2021*
• Crafted a tool that **analyzes a supplied packet capture file** and **finds and documents indicators of compromise** in the network traffic automatically.
Technologies used: Python, Scapy, Wireshark, VirusTotal, URLVoid