Pratinav Chandra

Website | Linkedin | Github | +1(240)-927-9770 | pratinav.chandra1997@gmail.com | College Park, Maryland

EDUCATION

Master of Engineering in Cybersecurity, *University of Maryland, College Park* *Aug 2022 - May 2024*
Bachelor of Engineering, Computer Science, *Manipal University, India* *Jul 2015 - Jul 2019*

SKILLS

Domain: Network Security, Security Monitoring, Detection Engineering, Threat Hunting, Digital Forensics and Incident Response, Threat Intelligence, Cloud Security, Automation, Computer Networking, Troubleshooting, Documentation
Infrastructure: Firewalls, Web proxies, VPN, IDS, Routers, Switches, Raspberry Pi, AWS (Amazon Web Services)
Programming Languages: Python, C, Javascript, Java, x86 Assembly
Security Tools: Splunk, CrowdStrike Falcon, CloudFlare WAF, Anvilogic, YARA, Sigma, Snort, Wireshark, Zeek, Arkime, Volatility, Autopsy, Elastic Search, Kibana, Azure Data Explorer, Burp Suite, Nmap, Metasploit, Docker, Canary Tokens
Security Frameworks: MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain, PEAK
CTF Competitions and Platforms: JawnCon '23 CTF (Winner), Huntress CTF, CyberDefenders, TryHackMe, KC7

WORK EXPERIENCE

Security Engineering Intern, Sigma Computing, *San Francisco, CA* *Jun 2023 - Aug 2023*

- Developed and enhanced threat detection rules in diverse security tools, resulting in a 40% increase in threat identification and reduced analyst fatigue.
- Spearheaded the creation of a centralized security data lake, automating ingestion from 80% of data sources, and improving threat hunting, detections, and data correlation.
- Led high-priority security incident investigations and proactive threat hunting to mitigate risks.
- Created custom dashboards for security analysis and cloud vulnerability management using Sigma's platform, contributing to a new product use case and acquiring a major security vendor as a customer.

Senior Cybersecurity Analyst, Dell Technologies, *Bengaluru, India* *Jul 2019 - Jul 2022*

- Contributed to a high-paced global Cyber Defense team, effectively managing high-priority network security incidents and overseeing network security infrastructure with a customer satisfaction rating of 98%.
- Implemented security architectures and deployed and configured network security solutions to segment multiple sites globally, resulting in an 80% reduction in the attack surface.
- Developed monitoring alerts, constructed dashboards, and extracted valuable insights from enterprise network traffic and network security device logs using tools like Splunk and SolarWinds NPM enhancing visibility by 60%.
- Pioneered the creation of automated tools for process and workflow optimization, resulting in a 70% reduction in manual workload for the team within four months.

PROJECTS

Home Cybersecurity Lab, *Independent Project* *Sept 2023*

- Designed a comprehensive home cybersecurity lab from the ground up to evaluate vulnerabilities and utilize open-source tools for security research, encompassing various operating systems.

Rubber Ducky using Raspberry Pi Pico, *Independent Project* *Aug 2023*

- Constructed a custom USB-C device, replicating the functionality of the Hak5 USB Rubber Ducky, using a Raspberry Pi Pico and a 3D-printed exterior. Developed malicious payloads designed to target various operating systems for adversary simulation.

ACHIEVEMENTS

CS Research Mentorship Scholar, Google, *Remote* *Sept 2023 - Present*

- Accepted to a three-month mentorship program to explore industry research in Security, Privacy, and Abuse Prevention under the guidance of a Google researcher and collaborated with the rest of the cohort within the research area.

Technical Content Writer, Infosec Write-ups, *Remote* *Sept 2021 - Present*

- Researched and authored technical write-ups as part of the team at "InfoSec Write-ups", the largest Cybersecurity publication on medium.com with over 29k followers. My write-ups have received recognition from a SANS instructor, who recommended them as essential reading resources, and have been featured as walkthroughs on prominent blue team Capture The Flag (CTF) platforms like CyberDefenders.