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

• **Domains:** Network Security, Security Monitoring, Detection Engineering, Threat Hunting, Digital Forensics and Incident Response, OSINT, Cloud Security, Automation, Computer Networking, Troubleshooting, Documentation
• **Infrastructure:** Firewalls, Web proxies, VPN, IDS, Routers, Switches, Raspberry Pi, AWS (Amazon Web Services)
• **Tools:** Splunk, Wireshark, Burp Suite, MITRE ATT&CK, CrowdStrike Falcon, Solarwinds NPM, Nmap, Metasploit, Yara, Snort, Zeek, Volatility, 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

WORK EXPERIENCE

Sigma Computing – *Security Engineering Intern* — *San Francisco, CA · June 2023 - Present*
• Implemented advanced **threat detection rules across various security tools**, resulting in a **40% increase in identifying potential security threats** and **reduced analyst fatigue** by **fine-tuning false positive alerts**.
• Spearheaded the development of a **centralized security data lake**, **automating data ingestion** covering **80% of available data sources**. This enabled the **correlation of data** to increase visibility and **enhance Sigma's Threat Hunting and Detection Engineering capabilities**.
• Investigated **high-priority security incidents** and actively engaged in **threat hunting activities**, mitigating security risks to the organization.
• Built **dashboards for security analysis, investigations, and cloud vulnerability management** using Sigma's own platform which **helped in defining a new use case for the product** and the **signing of a major security vendor as a customer.**
• Supported the **deployment and validation of data loss prevention policies** from scratch.

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** to segment 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.

PROJECTS

Home Cybersecurity Lab - *Independent Project* — *September 2023*
• Designed a home cybersecurity lab from scratch to **test vulnerabilities and open-source tools for security research across multiple operating systems**.
• Deployed an **isolated malware analysis lab**, configured a Raspberry Pi 4 to run ESXi ARM, and hosted multiple virtual machines to run services and tools **to enhance the lab's security and increase visibility on the network**.
• Established **edge defense** by deploying a Palo Alto Networks **firewall** to analyze and monitor network traffic.

Rubber Ducky using Raspberry Pi Pico - *Independent Project* — *August 2023*
• Built a USB-C DIY version of the Hak5 **USB Rubber Ducky** using a **Raspberry Pi Pico** with a 3D-printed exterior.
• Developed **malware payloads** targeting different operating systems for **adversary simulation**.

Security-Focused Cloud Migration - *University of Maryland* *December 2022*
• **Re-architected a web application** to migrate it to **AWS with a security-first approach** to enhance resiliency, Identity and Access Management (IAM), data protection, compliance, secure system administration, and coding best practices.

pxymon - *Dell Technologies* *April 2022*
• Implemented a **command-line tool for security analysts** to troubleshoot and identify issues related to **web proxy infrastructure** and web-based traffic automatically by **parsing security policies based on keywords** to search through the configuration faster and **deploy changes at scale**.

MISCELLANEOUS

CS Research Mentorship Scholar - *Google* *September 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.

CTF Player - *Independent, University of Maryland* *August 2022 - Present*
• Actively took part in Capture The Flag tournaments with the UMD Cybersecurity Club and Individually.
• Solved challenges on CyberDefenders and TryHackMe to test my skills and learn and explore new tools and security domains.

Technical Content Writer - *InfoSec Write-ups* *September 2021 - Present*
• Researched and published 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 been **recommended as reading resources** by a **SANS** instructor as well as **featured as walkthroughs** at leading blue team **CTF** platforms such as **CyberDefenders**.