Anup Tiwari

in linkedin.com/in/tiwarianup547   ▢ +1-6822796147   ✉ tiwarianup547@gmail.com   ◈ Portfolio

EDUCATION

The University Of Texas At Arlington <div align="right">Arlington, Texas</div>
Bachelor of Science in Information Systems <div align="right">May 2023</div>

TECHNICAL EXPERTISE

Programming Languages: Python, Java, C
Tools: Splunk, Nessus, Wireshark, OpenVAS, Anyrun, Cisco Talos, VirusTotal, PhishTool
Skills: Active Directory, Vulnerability Management, Incident Detection and Response, Endpoint and network security, SIEM, Firewall, Access controls and Identity Management
Cloud technology: Microsoft Azure
Operating Systems: Windows, MacOS, Linux, iOS, Android

EXPERIENCE

CyberSecurity Analyst <div align="right">Jan 2023 - Present</div>
Costco IT <div align="right">Arlington, Texas</div>

- Committed to obtaining Splunk Core Certified User certification by completing a series of hands-on labs to develop practical skills in utilizing Splunk for data analysis and visualization.
- Demonstrated a proactive approach to learning and professional development by shadowing other teams, including SOC, Incident Response, and Endpoint Security, to gain a deeper understanding of their roles and responsibilities.
- Demonstrated initiative and leadership by creating an internal Google intranet site providing comprehensive Splunk documentation and useful resources for the Logging and Detection Engineering team and other cybersecurity teams, helping them improve their understanding and utilization of Splunk for security purposes.
- Developed a flowchart to visualize the process of how endpoint logs are filtered in Log Analytics workspace and sent to EventHub and Splunk for further analysis.

Information Technology Assistant <div align="right">Jan 2022 - Jan 2023</div>
Human Resources - University of Texas at Arlington <div align="right">Arlington, Texas</div>

- Provided technical support to non-technical personnel, conducting computer diagnostics to troubleshoot and resolve issues, and expedited service by 50 percent.
- Enrolled university-owned devices in Microsoft Intune for best security management through cloud.
- Ensured data security and privacy by performing data sanitization techniques, such as degaussing and data wiping, on retired hardware.
- Maintained detailed logs of incidents and status of devices in Service-Now Management System, ensuring accurate data entry and efficient workflow management.

Consulting Engineering Associate <div align="right">May 2022 - Aug 2022</div>
Heartland Business systems <div align="right">Pewaukee, Wisconsin</div>

- Gained insights into the workings of IT consulting business and the importance of effective communication with clients to understand their needs and deliver tailored solutions.
- Deployed Microsoft Defender for Endpoint reducing the attack surface and improving malware detection.
- Managed users, computer accounts and licenses in Azure and On-Premises Active Directory.

Peer Academic Leader <div align="right">Aug 2021 - Jan 2022</div>
New Students Courses - University of Texas at Arlington <div align="right">Arlington, Texas</div>

- Mentored a group of three freshmen to ensure a smooth transition from high school to college.
- Collaborated with professors to develop and execute effective lesson plans, including the creation of study groups to enhance the students' learning experience.

PROJECTS

Honeypot and Azure Sentinel(SIEM | ◈ | *Azure, Virtual Machine, PowerShell, Event Viewer, Ip-geolocation API, Azure Sentinel*
- Designed and implemented a honeypot in Azure with virtual machines that were exposed to attack, and utilized PowerShell to extract metadata from Windows Event Viewer, which twas forwarded to a third-party API to derive geolocation data. Configured Azure Sentinel to ingest custom logs containing geographic information and display global RDP brute force attack in a map.

CERTIFICATIONS

- **CompTIA Security+** Passed in Aug 2022
- **CompTIA CySA+** Expected Apr 2023