AAYUSH PANDEY

+1(716)-939-6832 | aayushcybersec@gmail.com | LinkedIn | GitHub | Coursera | USA

SUMMARY

Cybersecurity Engineer with hands-on experience securing microservices in Cisco's enterprise systems—reduced production vulnerabilities by 25% via SDLC hardening, IAM design, and CI/CD controls. Specialized in cloud and on-prem security, red/blue team synergy, and ISO/NIST-aligned compliance. Proven ability to translate technical risk into action, automate enforcement, and drive measurable improvements across high-scale infrastructures.

WORK EXPERIENCE

TECHNICAL PROGRAM MANAGER | SECURITY ENGINEER - HOLIDAY WORLD, CO, USA **03/2025 – PRESENT**

- Building Holiday Channel's security program from the ground up—developing **ISO/NIST**-aligned policies, enforcing **RBAC** and leading **DevSecOps** using **GitHub Actions, Docker, and Terraform** across **Node.js/MongoDB** microservices, reducing exploit risk **by 40%.**
- Managing **AI**, **SEO**, and **DevOps** onboarding across **3 product lines** while Overseeing secure releases on **Cloudflare**, **Render** & **AWS** with token lifecycle controls.
- Performing penetration testing with **Burp Suite and Nmap**, and driving **GDPR/CCPA** compliance using **Cookiebot**, **asset monitoring**, and sandboxing.

AI SECURITY INTERN, ZUMMIT AFRICA, DELAWARE, USA **06/ 2024 – 08/ 2024**

- Performed end-to-end testing on **Zummit's GenAI-integrated web platform**—identified **10+ critical flaws** including **SQL** injection and access control bypass, cutting **risk exposure by 35%.**
- Tuned SIEM rules in Wazuh for false positive reduction &Researched AI product architecture and **designed IAM** and data control strategies to secure GenAI usage in production.

SENIOR SYSTEMS ENGINEER, CISCO, BENGALURU **03/ 2021 – 07/2023**

- Secured **Cisco's Order Processing microservices** (**Java SpringBoot**) handling **100K+ subscriptions/month** by integrating SonarQube into Jenkins pipelines via Bitbucket, reducing production vulnerabilities by 25%.
- Conducted unit and fuzz testing to harden code across **Duo's** secure **SDLC**. Built **IAM** policies on **Azure AD** with **OAuth**, **SAML**, and **Zero Trust models**.
- Optimized **CI/CD** pipeline security using **Terraform**, **Ansible**, and **PowerShell**, reducing **misconfigurations by 40%.**
- Delivered **monthly bug-fix reports** using **PowerBI** tracking **critical vs. low-priority** issues to guide engineering roadmap decisions.

EDUCATION

STATE UNIVERSITY OF NEW YORK AT BUFFALO, USA - *MS*, Cybersecurity **01/2025**

- *Internal Lockdown V4 2nd Place | UBNetDef Red Team Coordinator*

ITM UNIVERSITY, INDIA- *B.Tech*, Computer Science and Engineering (Cybersecurity and **Digital Forensics)** **12/2020**

- ***Cyber Forensics TA**: Conducted Classes alongside professor and team of four for junior students on Cyber-awareness, Information Security, Cyber Laws, and Data Recovery | Vice-President, **Technical Head** at ITM University's Fest (2018-20)*

PROJECTS

- **PhishGuard - *Phishing Scanner* :** Enhanced phishing detection rates by 40% through the implementation of honeypots and adaptive filtering algorithms, incorporating real-time monitoring with **Splunk** for actionable threat analysis ; Contributed to the development of incident response playbooks to standardize mitigation processes.
- **Cloud Security Compliance Automation** : Developed Infrastructure as Code scripts using **Terraform** to automate cloud security policy enforcement, ensuring continuous compliance with NIST 800-53.

SKILLS

Python, Java | **SQL** | **SIEM Tools** (Splunk, Datadog, Wazuh) | **IAM** | **Active Directory** | **Cloud Security | Firewall Configuration | Compliance** | **Networking** (OSI Model, TCP/IP, DNS, VPN, SSL/TLS) | **Encryption** | **Scripting** (PowerShell, Python) | **Virtualization & Containers | Penetration Testing** | **Data Protection Automation** (Terraform, Ansible, APIs) | Threat Hunting FW (OSINT, MITRE ATT&CK) | **Data Analysis & Query Optimization** (Log Parsing, Vulnerability Reporting)

CERTIFICATES

- **Security** : CompTIA Security+ 701 | **Cloud :** AWS Cloud Practitioner | **ONGOING –** CompTIA **CYSA**
- **Specializations** - IBM and ISC2 Cybersecurity Specialist | IBM Cybersecurity Analyst | IBM Security Analyst Fundamentals | Cisco Cybersecurity Operations Fundamentals | Palo Alto Networks Cybersecurity | Splunk Search Expert | Google IT Support | Google Cybersecurity | Google IT Automation with Python | Infosec Cyber Incident Response | IBM Gen AI for Cybersecurity Professional