Yu-Jung Chou

LinkedIn: yj-chou Github: LilChou https://yujungchou.me

Phone: +1(765)701-8927

Email: pcsvl97249@gmail.com

INTRO

Hello, I am currently making a transition from a Software Engineer into the Cybersecurity field with a passion for penetration testing, app security, and cloud security. Currently building ethical hacker skills through preparing for the certificates, projects/lab, and CTFs. Thank you for reviewing my resume!

Awards & Certificates

- **Security Certificates**: CompTIA Security+
- **Post Graduate Program in Cyber Security**: Certificate courses: CompTIA Security+, CISSP, EC-council: CEH
- **Information Security Computational Profession**: 7/120 applicants were chosen to be the 2017 program candidates.
- **2015 Capture The Flag Competition**: Rank Top 3 in Taiwan, the top 10% among competitors all over the world.

Education

- **Post Graduate Program on Simplilearn** — Simplilearn Online Platform
  Post Graduate Program in Cyber Security — *June 2023 - Nov 2023*
- **Purdue University** — West Lafayette, IN
  Master of Science in Computer Science — *Aug. 2017 – Dec. 2018*
- **National Tsing Hua University** — Hsinchu, Taiwan
  Bachelor of Science in Computer Science — *Sep. 2012 – Jun. 2016*

Technical Skills

- **Programming Languages**: Python(preference), Java, javascript, bash/shell scripts, SQL
- **Security**: NMAP, BurpSuite, Metasploit, Wireshark, Splunk, Nessus
- **AWS (Amazon Web Service)**: Lambda, SQS, SNS, DynamoDB, IAM, S3, CloudWatch, CDK, CloudFormation, ECS, EC2, Athena, Glue, API Gateway
- **Azure**: Azure Sentinel, Log Analytics Workspace, Virtual Machines, Microsoft Defender for the Cloud
- **Other Experiences**: Git, Gitlab, Linux system, REST API development, Docker, Relational Databases, Bamboo, Jenkins, Jira, Quip, Checkmarx security scanning, Serverless Web Framework

Cybersecurity Projects & labs

- **TryHackMe**: 11/2021 - present
  - **Complete Beginner**: Network Exploitation Basics. Web Hacking Fundamentals. Cryptography. Windows Exploitation Basics. Shells and Privilege Escalation. Basic Computer Exploitation.
  - **PRE Security**: Network Fundamentals. How Web Works. Linux Fundamentals. Windows Fundamentals.
- **Active Directory Home Lab Setup**: 05/2024 - Ongoing!
  - Use Virtualbox to launch virtual machines to host Windows Server 2019 and Windows 10
- **Cybersecurity Detection & Monitoring Lab**: 04/2024
  - Setup a honeypot virtual machine with Azure; used custom Powershell script to extract RDP brute force attack metadata from Windows Event Viewer; call third-party API to retrieve geo-location of the attacker's IP addresses; connects the log with Azure Log Analytics Workspace; uses Azure Sentinel (SIEM) to visualize the log on a world map to show where the attacks originated.

Experience

- **Salesforce.com, Inc.** Seattle, WA, USA
  Software Engineering MTS *5/2021 - present*

  Business Technology - Salesforce - Lotus Products and Approvals team:

  - Built the Approval solution in Lotus project. Integrate the Advanced Approvals package to the Quote system and design the customization to fulfill the customer requests.
  - Coaching and supporting the engineers new to the team and project.

  Business Technology - Salesforce - Complex Deals team: building SELA (Salesforce Enterprise License Agreement) deal management service for multi-year, multi-product agreements for account groups.

  - **Scrum lead**: Managed the team projects, prioritized and planned team objectives with scopes from quarter to sprint. Following best practices and standards for the development life cycles.
  - Established the unit test best practices and playbook for new repositories and became the code coverage pioneer of the organization.
  - Designed and restructured the cart architecture from proposal to practical.
  - **CI/CD champion**: Utilized Jenkins to manage the deployment pipelines and nightly run.
  - **Security Champion**: Initialized the security assessment, integrated the Checkmarx security scanning, and mitigated the reported vulnerabilities.

  Business Technology - Tableau - SPOPs team:

  - Built the CloudServiceProvider(CSP) in microservice architecture on top of existing Tableau architecture for Salesforce to interact with quoting service in Tableau. Designed the structure using AWS services from API Gateway to AWS Lambda, adopted Python REST API framework Flask
  - Applying AWS Cloudwatch and SNS to build up the monitoring dashboard to alarm system for CSP.
  - Automated the code health monitor using the Gitlab pipeline. Integrated with Checkmarx scanning and achieved 100% code coverage.
  - **Security champion**: Initialized the Security Assessment for the new service. Assessed the workflow with security boundaries in a diagram; provided the solution for handling sensitive data at rest and in transit; performed threat assessment and mitigation strategy.

- **Amazon.com, Inc.** Seattle, WA, USA
  Software Development Engineer *4/2019 - 4/2021*

  Builder Tools - Quilt team: provides comprehensive OS patching solutions to keep every single host secure with security patches while maintaining the health of applications and reducing operational burden.

  - Designed front-end data provisioning architecture for new patching services to make real-time data provisioned with low latency and avoid throttling.
  - Proposed solutions for the new patching service to support restricted cases. For example, target hosts in the isolated EC2 substrate network.
  - Established the integration process between the new and legacy patching services while maintaining backward compatibility.
  - Implemented the integration tests for our new patching service. Applied Cucumber (Behaviour-Driven Development) to write human-readable test scenarios to improve test readiness and set up the integration test template.

  Prime Air - Panda team: builds up and operates the underlying infrastructure to store and analyze Prime Air's data. Panda team's data platform takes raw data, cleans and reshapes it, and puts it into the database.

  - Designed zero downtime data migration mechanism, reducing the service downtime from 2 days to none.

- Optimized operation APIs to batch operations and accelerated the process 60 times faster.
- Optimized the error handling for schema violation and data processing.
- Introduced Cloudwatch alarms and integrated the Chime (messaging app) notification via Lambda.
- Discovered the vulnerability of unsanitized input and added the input validation according to the input fields.
- Restructured the service architecture and removed the unnecessary layers to optimize the runtime to 20% faster.