

Paul Jang

(443) 603-8247 | pjang2003@gmail.com | github.com/pjang123 | pjang.dev

EDUCATION

University of Maryland, Baltimore County (UMBC)

Bachelor of Science (B.S.) in Computer Science

Baltimore, MD

May 2025

CERTIFICATIONS

CompTIA Security+ (SY0-701)

January 2025

TECHNICAL SKILLS

Languages & Scripting: Java, PowerShell

Security & Networking: pfSense, WireGuard, Tailscale, Snort (IDS), VLAN Segmentation, DNS Filtering, SSH Hardening, Firewall & VPN Administration

Cloud & Virtualization: Amazon Web Services (AWS), Prowler, Docker, Proxmox VE, VMware, LXC Containers

Monitoring & Observability: Wazuh (SIEM), Prometheus, Grafana, Zabbix

Operating Systems: Windows, Windows Server 2025, Linux, OpenWrt, macOS

Directory & Data Services: Active Directory, Group Policy (GPO), LDAP, Redis, Git/GitHub

TECHNICAL PROJECTS

Wazuh SIEM Lab | *Wazuh, VirtualBox, Ubuntu, SSH*

August 2026

- Deployed a self-hosted Wazuh SIEM with a full manager-agent architecture, simulating SSH brute-force, privilege escalation, and account-creation attacks against a monitored endpoint.
- Validated detection coverage by mapping 28 generated alerts to MITRE ATT&CK across 6 tactics, including a correlated Level 10 brute-force alert triggered by attack frequency, not isolated events.
- Conducted a vulnerability assessment identifying 67 critical and 457 high-severity CVEs, prioritized remediation by affected package, and authored a formal incident report with findings and recommendations.

Cloud Security Audit | *AWS, Prowler, IAM, S3, EC2, CloudTrail*

August 2026

- Deployed a deliberately misconfigured AWS environment and audited it with Prowler against the CIS AWS Foundations Benchmark, surfacing 242 failed controls including 5 critical findings such as public S3 exposure, over-permissioned IAM roles, and unrestricted network ingress.
- Remediated critical and high-severity findings following least-privilege and defense-in-depth principles, verifying every fix via re-scan and eliminating the account's critical public-data exposure.
- Identified a scanner coverage gap on an unattached internet-facing security group, confirmed the exposure through manual CLI verification, and documented findings in a formal audit report.

Home Network Security Stack | *OpenWrt, WireGuard, Tailscale, Docker, Prometheus, Grafana*

July 2026

- Engineered a production-grade network security stack on a Raspberry Pi 4 (OpenWrt) with full WAN/LAN segmentation, blocking 251,000+ malicious and ad-serving domains at the DNS layer.
- Deployed a self-hosted WireGuard VPN server with public-key cryptography and DNS filtering enforced on all connected clients; integrated Tailscale as an independent, redundant remote-access layer.
- Hardened the system with SSH key-only authentication and forced DNS redirection, and provisioned a containerized Prometheus/Grafana stack for real-time network telemetry.

Enterprise Active Directory Deployment | *Windows Server 2025, PowerShell, VMware*

February 2025

- Deployed a Windows Server 2025 Domain Controller and Windows 11 client via VMware, standing up a new Active Directory forest and domain (pjang.local) from scratch.
- Automated user account and security group provisioning with custom PowerShell scripts, reducing manual setup time by 60%.
- Enforced Group Policy Objects (GPOs) for password, account lockout, and desktop security policies, and configured Windows Server Backup for disaster recovery.

LEADERSHIP & ACTIVITIES

Korean Student Association (KSA), UMBC

Baltimore, MD

Vice President (Sep 2023 – Jun 2024); Secretary (Sep 2022 – Jun 2023)

- Spearheaded outreach to external corporations and campus organizations, securing partnerships for large-scale fundraisers and cultural events.
- Directed executive board meetings and operational decision-making, serving as the primary liaison between the organization, sponsors, and university administration.
- Launched targeted newsletters and promotional campaigns that sustained a 90% event attendance rate across recurring cultural events.