

INTERESTS

I am a penetration tester at SOT Global and a first-year student in the dual M.S. program of Dakota State University (Cyber Operations) and Seoul Media Institute of Technology (Cybersecurity). Over nearly six years in industry, I have worked across IT infrastructure, managed security monitoring, security consulting, and building an in-house security program as a company's sole security engineer, often filling the blind spots of off-the-shelf solutions with tools of my own. My interests lie in *offensive security*, *operational security* (OPSEC), *zero trust*, and *payload concealment*, such as hiding data from deep packet inspection (DPI). In graduate school, I aim to ground this hands-on experience in rigorous research.

EDUCATION

- Dakota State University, Madison, SD** Aug 2026 – Present
- M.S. in Cyber Operations (dual degree with Seoul Media Institute of Technology)
- Seoul Media Institute of Technology, Seoul, Korea** Aug 2026 – Present
- M.S. in Cybersecurity (dual degree with Dakota State University)
- Hallym University, Chuncheon, Korea** Mar 2013 – Aug 2021
- B.S. in Computer Science & Engineering
 - Member of HUS (Hallym University Security), an academic club studying system and infrastructure security, 2013 – 2014

WORK EXPERIENCE

- SOT Global** Seoul, Korea Oct 2026 – Present
- Penetration Tester*
- Conduct penetration tests across infrastructure, web, mobile, and IoT targets.
- AI Spera** Seoul, Korea Nov 2025 – Jul 2026
- Cyber Security Engineer, Information Security Team*
- Served as the sole technical engineer of a two-person security team formed ahead of IPO; centralized firewall ACLs (FortiGate, pfSense), VPN access, and Cloudflare under the team and set up an M365 Defender (EDR) response process.
 - Built a Cloudflare log pipeline on the GraphQL Analytics API in place of Logpush, feeding ELK, Splunk, and Wazuh with Slack alerts; used Ray ID cross-analysis to separate network- from application-layer DoS and deployed blocking rules.
 - Wrote KISA-guideline vulnerability assessment scripts light enough for 1 vCPU / 1 GB hosts, automated with Ansible and quarterly OpenVAS scans; shipped targeted checks for zero-days such as the Axios supply-chain compromise and React2Shell.
 - Led the technical side of the PCI-DSS assessment and a SOC 2 readiness review; established the company's first bug bounty policy, reproducing reported PoCs and guiding remediation.
 - Rebuilt Wi-Fi security with zero-trust device allowlisting and physical network separation; developed *mr.robot*, an internal tool for FortiGate debugging, AD lookups, and malware sandboxing.
- A3Security** Seoul, Korea Feb 2022 – Nov 2025
- Security Engineer, Managed Security Services (Remote SOC)*
- Monitored universities and financial institutions across SIEM (ArcSight, Elastic, QRadar), SOAR,

NGFW, IPS, and WAF platforms, and onboarded new customers with on-site firewall installations and tailored SIEM ingestion (direct, IPsec VPN, RDP).

- Rewrote the monitoring methodology, deployed Zabbix, and trained analysts on FortiGate and Zabbix; earned Fortinet NSE 4 to serve as the company's registered FortiGate engineer.
- Built automation toolkits (*Abuse_autopilot*, *WorkTools*, *VTZero*) in Python, TypeScript, Next.js, and Supabase, cutting repetitive analyst work.

Security Consultant, KISA SME Information Security Consulting Program

- Served as the sole consultant for the Honam and Gyeongsang regions, assessing SMEs across administrative, technical, and physical security with availability-safe custom scripts.
- Gave budget-aware advice, e.g., prioritizing NAS-based backups for business continuity at a ransomware-affected manufacturer before costly defenses.

Strategic Planning (concurrent role)

Jun 2023 – Oct 2024

- Researched security market trends, co-planned the WDR managed security service, and designed a site rotation program for dispatched SOC staff.

P.A.T (Sebang Group) Seoul, Korea

Dec 2020 – Dec 2021

IT Maintenance Engineer

- Supported endpoints, networks, VPN, and servers across Sebang Group affiliates, including end-to-end onboarding of new hires (PC provisioning, Microsoft 365, security policies).

S-1 Corporation Seoul, Korea · *Research Assistant, AI & Cloud Solution Lab*

Apr 2020 – Jul 2020

Sion Information System Tokyo, Japan · *Web Developer Intern*

Dec 2018 – Feb 2019

PROJECTS

Lacrymaria Cyber Threat Intelligence Service (discontinued)

2025 – 2026

Founder & sole operator

- Built and operated a CTI web service shaped by real support requests from previous employers, from infrastructure (Proxmox, Cloudflare Tunnel) to application development.

Open-Source Security Tools

github.com/sqzer-x

- **USFX**: Python CLI that discovers internal subdomains with twelve offline techniques.
- **UDFX**: PowerShell tool that extracts AD-integrated DNS via LDAP on air-gapped networks.
- **UAF**: Linux Wi-Fi scanner for PCI-DSS audits that flags open APs and maps their networks.
- **transtation**: self-hosted VLESS + REALITY proxy with WARP egress and a fail-closed killswitch.

CERTIFICATIONS & AWARDS

Fortinet NSE 4 – Network Security Professional, Fortinet

Sep 2023

Cisco Certified Network Associate (CCNA), Cisco

Sep 2023

AWS Certified Solutions Architect – Associate, Amazon Web Services

Nov 2023

Basic Host-based Penetration Testing (BHPT), Inlearn course

Sep 2024

Grand Prize, ChatGPT Utilization Contest, A3Security

Aug 2023

TECHNICAL SKILLS

Languages: Python, Rust, C++, TypeScript, PowerShell, Shell

Security: ArcSight, QRadar, Splunk, Elastic Stack, Wazuh, SOAR, M365 Defender, OpenVAS, OpenCTI; FortiGate, pfSense, WINS Sniper, Penta WAPPLES, Cloudflare; PCI-DSS, SOC 2

Infrastructure: Linux, Windows / Microsoft 365, AWS, Proxmox, ESXi, VMware, Docker, Kubernetes, Ansible, Zabbix, Grafana; Cisco, Ubiquiti, IPsec VPN