

JINSOO YANG

Information Security Engineer | Cloud, Application & Compliance Security

Seoul, South Korea (Remote) | s1ns3nz0@gmail.com | [LinkedIn](#) | [GitHub](#) | [miata.cloud](#)

PROFESSIONAL SUMMARY

Information Security and Infrastructure Engineer with 7 years across IBM, Deloitte, and the Republic of Korea Army.

- **Application & Product Security:** Built a threat modeling and security requirements tool for the SDLC. Delivered product security consulting to strengthen clients' software supply chain security. Maintainer of the Secure Software Supply Chain domain in the SEAL Frameworks.
- **Cloud & Infrastructure Security:** Developed an AWS security maturity assessment tool and methodology. Contributed 28 security checks to Prowler, an open-source CSPM with 15.1k GitHub stars.
- **Detection & Response:** Managed Splunk and QRadar detection rules, proposing new rules and optimizing existing ones, and led detection-tuning meetings with clients. Led first-line incident investigations at an Army Corps CERT, covering evidence collection, timeline reconstruction, and incident reporting.
- **Identity & Secrets:** Led development of a multi-cloud CIEM tool with an IAM policy normalization engine for AWS, Azure, and GCP, and published research on it.
- **Compliance Engineering:** Led compliance readiness consulting for ISO 27001, EU CRA, ISMS-P, and digital signature regulations. Contributed a bug fix and a new GitHub Actions plugin to OSCAL Compass, a CNCF Compliance-as-Code project. Built a personal compliance management dashboard on OSCAL.
- **Vulnerability Analysis:** Identified vulnerabilities in a digital asset issuance platform and a blockchain payment platform, both confirmed by the vendors.

TECHNICAL SKILLS

- **Languages:** Go, Python, Bash
- **Security & Cloud:** AWS, Kubernetes, Terraform, GitHub Actions, Vault, OPA, Kyverno, Trivy, Sigstore, Prowler, Splunk, QRadar
- **Frameworks:** ISO 27001, ISMS-P, NIST CSF, SP 800-53, SSDF, EU CRA, OSCAL

PROFESSIONAL EXPERIENCE

Cybersecurity Consultant

Nov 2024 – Sep 2026

IBM Consulting Korea

Seoul, South Korea

- Built an AWS security posture assessment tool on open-source CSPM (Prowler) and defined a cloud security maturity grading model.
- Designed and recommended automated AWS posture scanning with AWS Batch, which later detected a crypto miner in the client's environment.
- Led product security assessments based on NIST SSDF (SP 800-218) and SP 800-204D to strengthen clients' software supply chain controls and DevSecOps culture.
- Conducted OT risk assessments across 10 plant sites and implemented OT SOC solutions.
- Reviewed and implemented iDMZ architecture across global plants for semiconductor, industrial vehicle, and energy companies.
- Managed OT SOC detection rules with IBM's global SOC, leading weekly tuning meetings to propose new rules and optimize existing ones.

Sr. Security Consultant

Mar 2024 – Nov 2024

Deloitte Consulting Korea

Seoul, South Korea

- Ran an ISO 27001 certification audit for a global IoT service: gap analysis, control-effectiveness testing, and remediation validation, and reported findings to global stakeholders in English.
- Audited digital-signature authentication services covering cryptographic controls, access management, and key lifecycle.
- Reviewed AWS architectures against compliance frameworks and set prioritized remediation.
- Drafted the evaluation criteria in Appendices 2–3 of Korea's Digital Signature Certification Service Evaluation Guide v1.4.0 (published in Korean).

Vulnerability Analysis Track

Jun 2023 – Feb 2024

KITRI Best of the Best (BoB) 12th

Seoul, South Korea

- Selected for a national program with about a 3% acceptance rate. Trained in web and binary exploitation and reverse engineering.
- Led a multi-cloud CIEM platform with an IAM policy normalization engine for AWS, Azure, and GCP. The project was published as research and spun out as a startup.

Signal Officer (Captain), Corps CERT

Dec 2021 – Mar 2023

Republic of Korea Army

South Korea

- Led first-line incident investigations for a command of about 10,000 members, covering triage, evidence collection, timeline reconstruction, and incident reporting.
- Tuned Splunk detection rules and dashboards, reducing false positives. Built an SPL query assistant and a SIEM training platform for new analysts.
- Managed firewall, IDS, and endpoint security policies through security event analysis.
- Audited security configurations of servers, networks, PCs, and military equipment, and built a self-audit script that let users find and fix their own misconfigurations.
- Built control-level audit evidence packages and drove remediation for cybersecurity assessments.
- Selected for the Army's Elite 300 Cyber Warriors. Won the Ground Operations Command incident response CTF. Placed 2nd in a cybersecurity education competition with a web-based security awareness game.

Signal Officer (Lieutenant), Network Platoon Leader

Mar 2018 – Dec 2021

Republic of Korea Army

South Korea

- Led a 25-member signal platoon responsible for military network availability and security. Ranked #1 of 24 signal sites in a corps-level readiness evaluation.
- Designed and tested network failover and disaster recovery procedures.

SELECTED PROJECTS

Compliance Ops Platform (OSCAL) [\[Live\]](#)

- Built a Compliance-as-Code platform that structures controls, policies, owners, and evidence in OSCAL, tracking NIST SP 800-53, NIST SSDF, and a custom key management policy on one dashboard.
- Automated evidence collection through MCP integrations with Slack and Jira for continuous audit readiness.

Compliance-Based Security Requirements AI Plugin [\[GitHub\]](#)

- Built a Claude Code plugin that derives verifiable security requirements from a service's compliance obligations, FIPS 199 impact, the SP 800-53B baseline, and STRIDE threat models.

Ethereum Hoodi Validator (Private EKS, now local Kubernetes) [\[GitHub\]](#)

- Ran an active Hoodi validator on private EKS with key signing isolated in Web3Signer and Vault.
- Secured delivery with 24 CI/CD controls mapped to NIST SSDF and SP 800-204D, including SHA-pinned actions, GitHub OIDC, fail-closed scanner gates, OPA policy, and digest-bound SBOM and provenance.
- Pinned all 84 actions and 39 images, mirrored them to private ECR with KMS encryption, and enforced the baseline at admission with Kyverno.
- Currently operate a Hoodi validator on local Kubernetes (Besu, Teku, Web3Signer), monitored in Grafana.

OPEN SOURCE CONTRIBUTION

34 merged contributions to cloud, compliance, and blockchain security tooling.

- **Prowler:** 28 Azure and GCP security checks, covering AKS, Cosmos DB, Entra ID, Secret Manager, and more.
- **SEAL Frameworks:** Maintainer of the Supply Chain section. Contributed Policy as Code, private registries and mirrors, and an endpoint compromise runbook.
- **LND (Lightning Network):** Co-authored the fix for short reads in the NodeAnnouncement2 address decoders, shipped in v0.22.0.
- **OSCAL Compass:** Fixed a KeyError bug in compliance-trestle.
- **Aperture (L402):** Fixed a flaky L402 test that could fail CI at random.
- **Trail of Bits Gosentry:** Reported a silent fuzzer failure, fixed by the maintainers the same day.

Contributions under review, including x402 payment fixes and L402 security metrics, are documented at miata.cloud.

VULNERABILITY DISCLOSURE

- Identified vulnerabilities in a digital asset issuance platform and a blockchain payment platform. Both were confirmed by the vendors, with fixes scheduled for the next release.

4 additional reports are under review. Details stay private until fixes ship.

EDUCATION

M.S., Cyber Defense — Dakota State University

Aug 2026 – Expected Aug 2028

B.S., Civil Engineering — Korea Military Academy

Feb 2014 – Mar 2018

CERTIFICATIONS & LANGUAGES

AWS Certified Security – Specialty · AWS Certified Solutions Architect – Professional · AWS Certified CloudOps Engineer – Associate · Kubestronaut (CKA, CKAD, CKS, KCNA, KCSA) · Engineer Information Security (Korea, national certification)

Languages: English (Professional Working) · Korean (Native)