

VALDEZ BENTIRAZ

Informatics Graduate (S.Kom.) — Aspiring SOC Analyst

bentirazv@gmail.com | [linkedin.com/in/valdez-bentiraz](https://www.linkedin.com/in/valdez-bentiraz) | github.com/Raiquia245

Location: Bandung, Indonesia

Informatics graduate (S.Kom., GPA 3.94/4.00) from Telkom University focused on blue-team security. Hands-on experience setting up a Wazuh SIEM lab, validating Windows endpoint telemetry, and analyzing alerts, alongside web vulnerability assessment, digital forensics coursework, and applied cryptography. Two-time GEMASTIK CTF representative and ADIKARA 2024 finalist; paper accepted for presentation at IEEE NetCrypt 2026.

SECURITY EXPERIENCE

Vulnerability Researcher — Coordinated Disclosure Program

Public-sector system · Sep–Oct 2026 · Under confidentiality agreement

agreement

- Participated in a coordinated vulnerability disclosure (CVD) program for a public-sector electronic system, under an agreed scope, rules of engagement, and confidentiality agreement.
- Identified and independently verified a high-severity web vulnerability affecting destructive document actions, with a reproducible proof-of-concept; submitted through the official program platform.
- Verified application controls against common web vulnerability classes and produced clear, reproducible finding reports.

Security Manpower Training (SMT) Program Indonesia 2026

Online Training · KISIA & NSHC · Aug–Sep 2026

- Completed the online cybersecurity training curriculum covering OS, web, network, and malware security, cryptography, forensics, VAPT methodology, OSINT, AI security, and ICS/OT and IoT security.
- Performed an authorized grey-box VAPT engagement under strict rules of engagement, delivering a professional English report with findings, proof-of-concept, and remediation.
- Produced a bilingual (English/Indonesian) sales kit for an industry security product.

Participant — Information Security Audit Class

Cisometric Academy · Bandung · Feb–Jun 2025

- Trained in auditing management systems under ISO 19011:2018 guidelines and conducting audits aligned with ISO/IEC 27001:2022 information security standards.
- Practiced audit planning, evidence gathering, and non-conformity reporting for information security management systems (ISMS).

Research Member — Digital Forensics

Forensic & Security Laboratory · Bandung · Oct 2023–Dec 2024

- Researched anti-anti-digital-forensic techniques — studying methods used to evade forensic investigation and how investigators detect and counter them.
- Explored artifact recovery, data-hiding detection, and forensic soundness in evidence handling.

CTF Competitor — GEMASTIK & ADIKARA

GEMASTIK 2023–2024 · ADIKARA 2024

- Represented Telkom University at the national GEMASTIK CTF (2023 & 2024).
- Finalist of ADIKARA CTF 2024 (internal Telkom competition); competed across web exploitation, forensics, and cryptography.

OTHER EXPERIENCE

Software Developer Intern

PT Sarana Multi Infrastruktur (Persero) · Jakarta · Jun–Aug 2025

- Built end-to-end modules with Laravel (backend) and React + TypeScript (frontend), collaborating with the Product Manager and senior engineers on features, bug fixes, and enhancements.
- Participated in requirements gathering, analysis, and sprint reviews, gaining hands-on Agile experience — directly relevant to secure SDLC understanding.

Member — Mobile Development Division

GDGoC Telkom University · Bandung · Dec 2024–Jun 2025

- Built mobile apps with Flutter & Dart; hands-on with UI design, Git collaboration, and Firebase backend integration.

Teaching Assistant — Programming Algorithms

Universitas Telkom · Bandung · Jan–Jun 2024

- Assisted students with algorithmic problem solving and programming fundamentals.

EDUCATION

Telkom University — S1 Informatics (S.Kom.)

Bandung · Aug 2022 – Sep 2026

- GPA: 3.94 / 4.00
- Relevant coursework: Cryptography, Information Security, Computer Networks, Operating Systems, Algorithms & Data Structures.

PUBLICATIONS

“Performance Analysis of ASCON and ACORN Lightweight Cryptography on ESP32 with MQTT Protocol” — Undergraduate thesis benchmarking lightweight AEAD ciphers (ASCON-128, ASCON-AEAD 128, ACORN-128) on real ESP32 hardware over the MQTT protocol for resource-constrained IoT devices. Paper accepted for presentation at IEEE NetCrypt 2026 (4th International Conference on Networks and Cryptology, Jawaharlal Nehru University, New Delhi); to be indexed in IEEE Xplore.

PROJECTS

- **Home Lab SIEM & SOC — Wazuh (Personal Lab, Oct 2026)** — Set up a single-node Wazuh 4.14.9 stack (manager, indexer, dashboard) with Docker on WSL2 and onboarded a Windows 11 endpoint with Sysmon and the Wazuh agent. Validated telemetry for failed logon (4625), process creation (4688 / Sysmon ID 1), PowerShell script block (4104), and file integrity monitoring (rule 550). Analyzed ~2,400 alerts, investigated a level-15 false positive, and documented a triage workflow; attack simulation is planned next.
- **Polyglot DevSecOps CVE Scanner** — Python security tool that scans Python (PyPI) and Node.js (npm) dependencies for known vulnerabilities via the OSV.dev API, classifies CVSS severity, auto-patches to safe versions, and pushes real-time HIGH/CRITICAL alerts to Discord (ChatOps). Includes a live file-watcher mode.
- **Insider Data-Breach Forensic Investigation** (Coursework) — Forensic analysis of a simulated insider data-breach case: examined a full USB disk image acquired with FTK Imager, verified evidence integrity using SHA-256 hashing, and reconstructed the incident timeline from chat-log evidence and transferred design files.
- **Vulnerable Web Application Exploitation Lab** (Coursework) — Exploited SQL injection and path traversal in deliberately vulnerable Flask/PHP/SQLite applications, and compared insecure (string-concatenated queries) against secure (parameterized queries, output encoding) implementations.
- **ADIKARA CTF Writeups** — Public writeups documenting solved challenges across cryptography (RSA factoring), binary exploitation (stack buffer overflow), digital forensics (Morse audio, HAR and Git-history analysis), polyglot files, and OSINT, covering the ADIKARA 2024 qualifiers and finals.
- **Korean Novel OCR + Translator** — Desktop reading aid (Python) that captures an on-screen region, runs Korean OCR (EasyOCR or Tesseract), and translates it to English via Google Translate, Gemini, or an OpenAI-compatible API in an always-on-top overlay.

SKILLS

- **Security Operations:** Wazuh SIEM lab (Windows Event Log, Sysmon, file integrity monitoring), alert triage and false-positive analysis; MITRE ATT&CK mapping practice.
- **Security Assessment & Forensics:** Web vulnerability assessment (OWASP Top 10, grey-box testing) and CVSS 3.1 scoring with reproducible PoCs; digital forensics coursework (FTK Imager disk imaging, SHA-256 integrity verification, timeline reconstruction); information security audit coursework (ISO/IEC 27001:2022, ISO 19011:2018).
- **Cryptography & IoT:** Lightweight/applied cryptography (ASCON, ACORN), embedded security on ESP32, MQTT protocol, performance benchmarking.
- **Programming:** Python, Dart, SQL (Java and C++ from coursework).
- **Frameworks & Tools:** Wazuh, Sysmon, Docker/WSL2, Flutter, Laravel, React + TypeScript, Git, Firebase, MySQL, PostgreSQL.

CERTIFICATIONS

- **SOC Analyst Learning Path** — LetsDefend, 2026: SOC fundamentals, alert triage, MITRE ATT&CK, and phishing analysis
- **Pre Security Certificate** — TryHackMe, 2026 (ID: THM-ODPETU6MFM)
- **Introduction to Cybersecurity** — Cisco, 2025
- **Introduction to Information Security** — Cyber Academy Indonesia, 2023 (ID: PKMI1107231216)
- **Cybersecurity Training (Phase 1–2)** — Elitery & Elite Academy (Diskominfo Jawa Barat), 2026
- **Microsoft Certified: Azure AI Fundamentals** — Microsoft, 2025
- **Belajar Dasar Data Science · Dasar AI · Dasar SQL** — Dicoding Indonesia, 2023–2024

LANGUAGES

- Bahasa Indonesia — Native | English — Professional working proficiency (CEFR B2; Telkom University EPrT 570, 2026)