

MOISES CEAZAR C. DEL MUNDO CC, CCP

Lipa City, Batangas, Philippines | moisesceazard@gmail.com | Portfolio Website
linkedin.com/in/moises-ceazar-del-mundo-90218a31b | github.com/moisesceazard-creator

SUMMARY

Fourth-year BSIT (Information Security) student and ISC2 CC holder seeking a SOC Analyst / Cybersecurity internship (OJT). Deployed an award-winning Security Onion monitoring platform for a city government (9.7M+ events, 100% detection).

EDUCATION & HONORS

De La Salle Lipa — Lipa City, Batangas

Expected June 2027

BS Information Technology, Major in Information Security | GWA: 3.38 | Dean's Lister, AY 2023–2024

- **1st Place, Best Capstone Project** (InfoSec Track) & **1st Place, Best Group Presentation** — IT Colloquium '26–'27 (Oct 2026)
- **Top Student Awardee** — IT Elective 2 (Information Security), 2026 · **NSTP Lingkod Awardee** — community service, 2024

EXPERIENCE

Security Monitoring Deployment — Tanauan City Hall MIS Office

2025–2026

Capstone Project, De La Salle Lipa | Security Onion, Elastic Stack, Suricata, Zeek, ElastAlert 2, Telegram Bot API

- Deployed the office's first in-house monitoring platform (Suricata and Zeek via SPAN port, Elastic Agent on 5 endpoints), **indexing 9.7M+ events** in four days live.
- Built Kibana host/network dashboards and STRIDE / MITRE ATT&CK-mapped rules for brute force, port scanning, USB exfiltration and C2.
- Achieved **100% detection across 5 simulated attacks**, ~1.5-minute average Telegram alert delivery and ~10% false positives after tuning; tracked incidents in Security Onion Cases.
- Earned **formal endorsement from the MIS Department Head** after UAT; hardened the server (MFA, key-only SSH, secrets migration), raising Lynis from **68 to 83**.

Security Operations Center Lab Mentee — DysrupIT x De La Salle Lipa Partnership

2025–Present

Action1 RMM, Sophos Central, Windows Sysinternals, Nmap, Hydra, Security Onion, T-Pot, Proxmox VE

- Deployed Action1 RMM across lab endpoints for patch management, software deployment and vulnerability remediation.
- Ran controlled Nmap, Hydra and Telnet simulations to evaluate NIDS/HIDS detection; investigated processes, persistence and endpoint alerts with Sysinternals and Sophos Central.
- Triaged phishing via email-header analysis (SPF, DKIM, DMARC) and reviewed attacker logs from T-Pot honeypots.

PROJECTS

- **Wazuh SIEM Detection Lab (2025):** Wazuh agent–manager across Windows and Linux with FIM, active response and custom XML rules for file tampering and privilege escalation.
- **Vulnerability Assessment & Remediation Lab (2025):** Nessus and OpenVAS scans; remediated MS17-010, MS08-067 and PetitPotam; enforced SMB signing via PowerShell and GPOs.
- **SOC Investigation Writeups (LetsDefend):** 11 Tier 1 investigations (e.g. CVE-2024-3400, CVE-2025-53770, Lumma Stealer) with MITRE ATT&CK mapping; 6 SOC badges.

LEADERSHIP & ACTIVITIES

Junior Philippine Computer Society (JPCS) – DLSL Chapter

2025–Present

Project Head, Internal Affairs (IT); previously 3rd Year IT Representative

- Lead committees running IT workshops, seminars and competitions for 200+ students; author concept papers, SWOT analyses and narrative reports for approval.

CERTIFICATIONS & TRAINING

Certifications: ISC2 Certified in Cybersecurity (CC) · Appkademiya CCP · Google Cybersecurity Certificate (in progress)

Training: Fortinet Threat Landscape 3.0 · Cisco Intro to Cybersecurity · LetsDefend SOC badges (6)

TECHNICAL SKILLS

SIEM & Monitoring: Security Onion, Wazuh SIEM/XDR, Elastic Stack (Elasticsearch, Logstash, Kibana), Suricata, Zeek, ElastAlert 2

Endpoint & Vulnerability: Sophos Central, Action1 RMM, Nessus, OpenVAS, Nmap, Hydra, Sysinternals, patch management

Systems & Frameworks: Windows, Linux, Active Directory, PowerShell, Proxmox VE; NIST CSF 2.0, MITRE ATT&CK, STRIDE

Documentation & Support: MS Office, Google Workspace, concept papers, SWOT; hardware & network troubleshooting