

VINCENT JERALD G. MENDOZA

CYBERSECURITY ANALYST



About

With more than three years of experience in Cybersecurity, I have gained comprehensive knowledge across various branches of the field. My expertise spans from Malware Analysis and Email/Web Threats to Network Security, as well as identifying and mitigating both External and Internal threats. Throughout this time, I have honed my skills in proactively safeguarding systems, analyzing potential risks, and responding to security incidents to ensure protection against the evolving cyber risks.

Personal Information

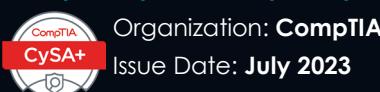
- Gender: **Male**
- Email: **vjgmendoza@gmail.com**

Education

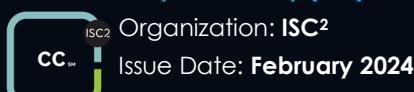


Certifications

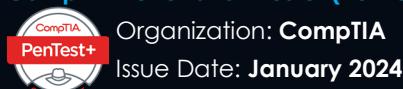
CompTIA Cybersecurity Analyst (CySA+)



Certified in Cybersecurity (CC)



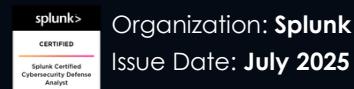
CompTIA Penetration Tester (PenTest+)



Security Analyst Level 1 (SAL1)



Certified Cybersecurity Defense Analyst



Professional Experience

CYBERSECURITY ANALYST – SOC DEPARTMENT



SecureOps Incorporated, Philippines
January 2023–Present

- Monitor several business-critical devices across multiple locations for a variety of clients
- Monitor consoles and dashboards, and investigate security alerts
- Creating tuning recommendations for **IDS/IPS** devices across client infrastructures
- Identify/Investigate** potential **malware infections, intrusions, DoS/ DDOS** attacks on client network space
- Write **analysis notes** and **reports** detailing findings
- Perform **queries** and **research** to complement monitoring

THREAT RESPONSE ENGINEER – CORE TECH DEPARTMENT



Trend Micro Incorporated, Philippines
August 2021 – April 2022

- Analyze and categorize reported **websites** and **emails** to determine whether they are normal, malicious, phishing, spam, or other threat types.
- Perform static and dynamic **malware analysis** to document and report on malware behavior, either partially or in full.
- Develop and document steps to **contain** and **eradicate** the malware, and how to **recover** from **damages**
- Experience in using different types of debuggers and tools

Skills and Tools

Proficient in:

- Log** correlation and analysis, OSINT, Threat Hunting
- Email** and **URL** threat investigation
- IPS/IDS, EDR, firewall** technologies
- SIEM** platforms (Splunk, Google SecOps)
- Windows** and **Mac** Operating Systems
- Citrix** and **Amazon Workspace** Machines

Familiar with:

- Malware** analysis and **debugging** tools
 - (VMware, OllyDbg, IDA Pro, Wireshark, Fiddler)
- Java and Assembly Programming