VINCENT JERALD G. MENDOZA

CYBERSECURITY ANALYST

About

Hi! I'm Vincent, a dedicated and motivated engineering graduate that loves everything about computers. Motivated, eager, and constantly maintains a high level of energy in learning and developing things that makes life comfortable, better, and secure. Handles the task with a clear vision of the goal and always finds a possible way to a more simple, efficient, secure, and effective method. A fast learner, a critical thinker, and an effective team player.

Personal Information

- Gender: **Male**
- Phone: **+639264000089**
- Email: **vjgmendoza@gmail.com**
- City: **Baguio City, Benguet**

Education

B.S. in Computer Engineering
University of Baguio, Philippines
Class Year 2020

Certifications

Certified in Cybersecurity (CC)
Organization: **ISC²**
Issue Date: **February 2024**

Certified Cybersecurity Analyst
Organization: **CompTIA**
Issue Date: **July 2023**

Certified Penetration Tester (PenTest+)
Organization: **CompTIA**
Issue Date: **January 2024**

Certified in Cyber Threat Management
Organization: **CISCO**
Issue Date: **February 2024**

Professional Experience

CYBERSECURITY ANALYST — SOC ENVIRONMENT

SecureOps Incorporated, Philippines
January 2023—Present

- Monitor several business-critical devices across multiple locations for a variety of clients
- Monitor **Splunk** 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
- Perform threat hunting and analysis on User Entity and Behavior Analytics, and Data Loss Prevention

THREAT RESPONSE ENGINEER — CORE TECH DEPARTMENT

Trend Micro Incorporated, Philippines
August 2021 - April 2022

- **WIN32 API Assembly Language Programming**, **File Operations and Windows Internals** (Kernel, Boot-up, Registries, File systems, Processes and Threads, Windows Message, DLL, etc.)
- **Experience in using different types of debuggers and tools** (OllyDbg, IDAPro, Wireshark, Fiddler, etc.)
- **Analyze and Categorize reported websites as normal, malicious, etc.**
- **Analyze and Categorize reported emails as normal, phishing, spam, etc.**
- **Conduct a Black Box analysis** to different types of malwares and create a partial or complete malware report
- **Conduct detailed analysis** and develop documentation on the behavior of the malware
- **Develop and document steps to contain and eradicate the malware,** and how to recover from damages

Skills

Basic skills in **Linux**, **SQL**, **JavaScript**, **JQuery**, **NodeJS**, **ExpressJS**, **GIT**

Average skills in the following:

- **HTML, CSS, Bootstrap**
- **Cisco** Device Configuration
- **Java, Assembly** Programming
- **Malware Analysis and Debugging Tools** e.g. (VMWare, OllyDBG, IDAPro, Wireshark, Fiddler, etc.)

Proficient in the following:

- **Log Correlation and Analysis, OSINT, Threat Hunting**
- **Email/URL Threat Analysis**
- **IPS/IDS and SIEM**(Splunk) Tools
- **Windows and Mac Operating** Systems
- **Citrix and Amazon Workspace** Machines

- Nothing Follows -