**Clarence Claude Cristobal | CC | Security+**

306 Manggahan, Santa Maria, Bulacan, Philippines
■ claudecloud9@gmail.com **|** ■ +63 928 532 7549
■ claudecode.netlify.app **|** LinkedIn: **Clarence Claude Cristobal**

## Professional Summary

Dedicated SOC Analyst with hands-on experience in incident response, threat analysis, and secure system design. Proficient in monitoring, triaging, and escalating alerts in a fast-paced SOC environment. Committed to continuous upskilling and backed by a growing portfolio of industry-recognized certifications. Consistently ranked in the Top **6** in LetsDefend players in the Philippines, showcasing hands-on proficiency in real-world SOC scenarios. Actively participated in Hack The Box (HTB) challenges and authored detailed write-ups to share solutions and methodologies, contributing to the cybersecurity community.

## Professional Experience

### SOC Analyst Level 1

Microgenesis Business Systems — Feb 2025 – Present

- Monitors security events using the Stellar Cyber platform and performs initial triage on alerts.
- Investigates incidents using OSINT tools and enriches data for better context.
- Creates custom alert filters and manages lookup tables within Stellar Cyber to reduce false positives and improve detection accuracy.
- Creates and manages Case Tickets and Threat Hunting Tickets for alerts identified as true positives or malicious,ensuring thorough documentation and timely escalation.
- Writes and maintains investigation playbooks to standardize L1 response procedures and enhance team efficiency.
- Handles case documentation, prepares daily reports, and escalates issues to L2/L3 analysts when necessary.
- Conducts routine sensor monitoring and supports continuous operational visibility.
- Actively participates in upskilling programs and platform-specific training to enhance threat detection and response capabilities.

### Web Designer/Developer

NevMet Philippines, Inc. — Jul 2024 – Nov 2024

- Designed and implemented secure, responsive websites using Figma and front-end technologies.
- Applied best practices in web accessibility, secure code design, and UX alignment with client goals.
- Collaborated cross-functionally with clients and internal teams for design feedback and iteration.
- Interpreted metrics and user feedback to optimize design elements and site performance.

### Intern Desktop Support Engineer

Teleperformance — Feb 2024 – May 2024

- Provided desktop-level support and resolved hardware, software, and network issues.
- Conducted secure troubleshooting and basic network diagnostics using packet tracing.
- Communicated technical issues effectively to non-technical users and identified recurring problems.

## Key Incidents & Task Handled

- Top **6** in **LetsDefend Philippines**
  Consistently ranked among the top players in the Philippines, demonstrating hands-on proficiency in real-world SOC scenarios and a commitment to continuous learning.

- **HTB Challenges and Write-ups**
  Actively participated in Hack the Box (HTB) challenges, solving complex cybersecurity problems. Authored detailed write-ups to share solutions and methodologies, contributing to the cybersecurity community.

- **Handled high and critical alerts with tight SLA**

  I usually take around 100–200 alerts per shift including false positives, and for anything high or critical, I make sure to act fast — either escalate or resolve it within 30 minutes to 1 hour as required. Staying within SLA is always a top priority.

- **Efficient triage process**

  When I pick up an alert, I assign it to myself and mark it as 'In Progress' before digging in. For most alerts, I can complete the initial investigation within 5 to 10 minutes, especially if the needed logs or data are available in our XDR platform.

## Core Skills

### Cybersecurity

- Incident Response & Triage: Alert handling, escalation workflows, playbook execution
- Network Security: IDS/IPS, firewall log monitoring and analysis **(Palo Alto, SonicWall, Fortigate, Sophos)**, packet analysis (Wireshark)
- Threat Intelligence: MITRE ATT&CK, vulnerability management, **OSINT** investigations using **VirusTotal, AbuseIPDB, Shodan, VPNAPI.io, WhatIsMyIPAddress, HaveIBeenPwned, urlscan.io, Browserling, Tria.ge, MHA, BrightCloud, OTX AlienVault, Cisco Talos, ANY.RUN, IP2Location**
- Endpoint Security: AV/EDR systems, vulnerability detection & mitigation
- Sensor Monitoring: Stellar Cyber platform, daily visibility reporting

### Technical

- Programming & Markup: Powershell, HTML, CSS, JavaScript, React JS, Python, Java, Git, REST APIs
- Databases: MySQL, SQL
- Tools & Platforms: Stellar Cyber, Splunk, Nmap, PowerShell, Wireshark, Figma, FileZilla, Microsoft Defender, Sophos Central
- OS Environments: Windows, Linux, Kali Linux

### Interpersonal

- Strong problem-solving and analytical thinking
- Clear communicator in diverse technical teams
- Adaptable and collaborative in fast-paced environments

### Certifications

Core Certifications

- **CompTIA Security+ (SY0-701)** — *Dec 2025 – Dec 2028*
- **ISC2 Certified in Cybersecurity (CC)** — *Jul 2025 – Jul 2028*

- **Fortinet Certified Fundamentals in Cybersecurity** — *Apr 2025 – Apr 2027*

Stellar Cyber

- **SOC Analyst Associate** — *Feb 2025*
- **Essentials Associate** — *Feb 2025*

Security Blue Team

- **Blue Team Junior Analyst (BTJA)** — *Jan 2025*
- **Introduction to PowerShell** — *Dec 2024*

LetsDefend (Learning Paths & Skill Programs)

- **CompTIA Security+ Preparation Path** — *Sep 2025*
- **SIEM Engineer Career Path** — *Sep 2025*
- **Programming for Cybersecurity** — *Jul 2025*
- **Detection Engineering Learning Path** — *Jul 2025*
- **SOC Analyst Learning Path** — *Apr 2025*
- **Malware Analysis Skill Path** — *Apr 2025*

Threat Intelligence

- **CTI 101: Foundation Level Threat Intelligence Analyst** — *Mar 2025*

Other Training

- **Cybersecurity Bootcamp Webinar** — *Jul 2024*

## Education

Bachelor of Science in Information Technology – Major in Service Management
Bulacan State University – Bustos Campus | 2020 – 2024

Senior High School Diploma in IT – Mobile App and Web Development
STI College Sta. Maria | 2018 – 2020