AMIRUL AZIM BIN AMRAN

CYBERSECURITY ANALYST | COMPTIA SEC+ | COMPTIA CYSA+

Address: Kuala Lumpur, Malaysia

Email: amirulazimiv@gmail.com

Contact: +60 129691530

LinkedIn: linkedin.com/in/amirul-azim

Website: sovayle.github.io

Driven Cybersecurity Analyst and SOC shift lead with ~2 years of experience across alert triage, deep investigation and incident response. Skilled with SIEM, EDR and SOAR in enterprise environments, including coordinating containment during high-severity incidents. Proficient in Mandarin and progressing toward SOC L2 and Incident Response specialization.

EDUCATION

International Islamic University Malaysia, Gombak, Selangor Oct 2020 - Aug 2024
Bachelor of Computer Science (Network And Security)
CGPA: 3.70

WORK EXPERIENCE

Vigilant Asia Sdn Bhd, Bukit Jelutong, Shah Alam Mar 2025 - Present
Security Analyst - Shift Lead

- Led 12-hour SOC operations, supervising a team of 3-4 analysts to ensure accurate triage, escalations and response across 20+ enterprise clients.
- Directed cross-team response during high-severity incidents, coordinating rapid containment and recovery to restore operations 100% within SLA.
- Conducted 1-3 deep-dive investigations daily into security incidents and ad hoc client requests, delivering detailed analysis and mitigation guidance.
- As shift lead, I proof-read 10-15 escalations daily and providing appropriate commendations in escalations to all clients.
- I have proven to maintain 99% - 100% SLA in all alerts (100-200 daily) by ensuring smooth coordination with my team.
- Enhanced SIEM detection quality by reviewing and optimizing correlation rules for 200+ daily alerts. Documented and reported recurring alarm issues to L2 analysts, which led to fine-tuning that reduced alert noise by 80%.

Security Analyst Sep 2024 - Feb 2025

- Monitored and analyzed over 200+ daily alerts from network traffic, endpoint alerts, and system logs via SIEM, EDR, and SOAR platforms to detect and respond to potential security threats.
- Investigated and validated alerts an average of 30-50 alerts per shift, escalating confirmed incidents to clients with detailed findings and mitigation guidance.
- Managed client communications for incident updates and service requests, maintaining clear audit trails via ticketing systems.
- Collaborated with senior analysts on 1-3 complex investigations daily and client escalations to ensure accurate analysis and timely resolution.

Cybersecurity SOC Analyst Internship Mar 2024 - Aug 2024

- Acquired hands-on SOC experience working 12-hour shifts under senior analysts, reviewing 200+ daily alerts and assisting with 10–15 escalations per day to ensure timely and accurate incident response.
- Generated daily SIEM reports across all platforms for 20+ enterprise clients.
- Drafted a daily average of 10 incident escalation reports and client notifications daily, ensuring clarity accuracy, and 100% SLA compliance.

CERTIFICATIONS

CompTIA Cybersecurity Analyst + (CySA+)	Oct 2025
CompTIA Security +	Oct 2025
LogRhythm Security Analyst (LRSA)	Mar 2025
AWS Certified Cloud Practitioner	Dec 2025
Rocheston Certified Cybersecurity Engineer	Jan 2024
Microsoft SC-900: Security, Compliance, and Identity Fundamentals	Apr 2023

SOFT SKILLS

Effective Communicator

- PIC for monthly reports for an Operational Technology (OT) client, managing monthly reports and ensuring timely response to all requests and incidents.
- Delivered daily shift handovers to team leads and incoming shifts, ensuring knowledge transfer and continuous improvement.

Presenter & Trainer

- Presented for multiple cybersecurity awareness sessions, including a program for a banking client and annual awareness campaigns for internal staff, driving measurable improvements in security posture.

Languages

- Mandarin (Proficient)
- English (Native)
- Malay (Native)

TECHNICAL SKILLS &TOOLS

Cybersecurity

- SIEM (LogRhythm, Level Blue USM Alienvault, ThreatDefence)
- SOAR (Swimlane)
- EDR/XDR (TrendMicro Suites, BitDefender, SentinelOne, Trellix HX)
- Cloud Security Platform Monitoring (Orca AWS)
- Website, breach, mobile monitoring (Site 24x7, Spycloud, Zimperium)
- MITRE ATT&CK
- Linux
- Wireshark
- Sysinternals

LEADERSHIP

Security Analyst - Shift Lead

- Guided Junior Security Analysts by addressing their inquiries, sharing best practices, and ensuring adherence to 100% SLAs.
- Trained interns, resulting in their promotion as permanent employees.

Head of Public Relations (University level)

IIUM Special Interest Group (SIG) Cybersecurity

- Moderated cybersecurity workshops for 50+ students, strengthening their technical skills.
- Designed 5-10 cybersecurity challenges to engage and challenge participants.
- Prepared 3 comprehensive proposals and reports for cybersecurity programs.

REFERENCES

Mr. Murugan Mariappan
Cyber Defense Manager,
Vigilant Asia Sdn Bhd,
murgan11@hotmail.com

Dr. Andi Fitriah Abdul Kadir
CTF Supervisor & Lecturer,
Department of Computer Science,
International Islamic University Malaysia,
andifitriah@iium.edu.my