

DARRSHAN ERETTAI MUNIANDY

Bandar Putera, Klang, Selangor • +60 13-976 0509 • darrshan2003@gmail.com • [Website](#)

SUMMARY

Cybersecurity Analyst with operational experience in SIEM monitoring, DDoS mitigation, and incident triage within a high-availability environment. Proven ability to manage offense queues, validate security alerts, and adhere to strict Service Level Agreements (SLAs) for timely customer notifications. Combines a Bachelor's in Computer Science with a strong technical foundation in network security protocols (CCNA curriculum) and full-stack development to support critical infrastructure and defensive operations.

WORK EXPERIENCE

TimedotCom

Aug 2025 - Nov 2025

Cybersecurity Analyst, Intern

- SIEM Monitoring & Incident Triage:* Monitored SIEM alerts to detect potential threats, creating tickets for all offenses and escalating validated incidents to L2 analysts or customers for verification.
- DDoS Response & Communication:* Managed DDoS incident protocols by issuing timely notifications to customers via email or phone based on attack duration (≥ 10 mins) and Service Level Agreements (SLAs), ensuring every alert was documented in the ticketing system.
- Operational Support & Reporting:* Assisted in the preparation of monthly security reports and maintained accurate operational data using Excel.
- Platform Proficiency:* Gained hands-on training in Stellar Cyber Open XDR and PRE Security AI SOC to support offense management and analysis.

Mr Digital

Dec 2023 - Aug 2025

Website Developer, Freelance

- Full-Stack Development:* Developed custom, responsive websites from concept to deployment, handling both front-end interfaces and back-end functionality.
- Client Management:* Collaborated directly with clients to translate their specific requirements into functional digital solutions.

EDUCATION

Swinburne University of Technology, Australia

Feb 2023 - Dec 2025

Bachelor of Computer Science major in Cybersecurity

CGPA 3.5 MY | 2.75 AUS

Subang | Australia

INTI International College, Subang

Jan 2022 - Dec 2022

Foundation in IT

CGPA 3.3

Subang

CERTIFICATION & LICENSES

- Certified Cybersecurity Technician, EC-Council, Jan 2026
- Certified in Cybersecurity, ISC2, Dec 2025
- Cybersecurity Awareness: Cybersecurity Terminology, LinkedIn, Nov 2025
- Stellar Cyber SOC Analyst Associate, Stellar Cyber, Nov 2025
- Microsoft Security Essentials Professional Certificate, Microsoft, Oct 2025
- Microsoft Security Essentials: Concepts, Solutions, and AI-Powered Protection, LinkedIn, Oct 2025
- SIEM: Event Management with Splunk Security, LinkedIn, Oct 2025
- AWS x INTI Ideathon, AWS, May 2025
- Fortinet FortiGate 7.4 Operator, Fortinet, Apr 2025
- Fortinet Certified Associate in Cybersecurity, Fortinet, Apr 2025
- Network Security, Cisco, Jan 2025
- ISC2 Candidate, ISC2, Dec 2024

CERTIFICATION & LICENSES

- Linux Unhatched, Cisco, Dec 2024
- CCNA: Enterprise Networking, Security, and Automation, Cisco, Aug 2024
- CCNAv7: Switching, Routing, and Wireless Essentials, Cisco, Aug 2024
- CCNA: Introduction to Networks, Cisco, Jan 2024

SKILLS

Security Tools & Platforms: IBM QRadar, Wazuh, Arbor DDoS, Stellar Cyber Open XDR, Cisco ASA Firewalls, PRE Security AI SecOPS, Fortigate, Cacti, Autopsy, Nmap, Kali Linux, Parrot OS

Security Operations & Analysis: SIEM, Extended Detection & Response (XDR), Incident Response, Log Analysis, Digital Forensics & Evidence Handling, Mitre ATT&CK TTPs, Offense Management & Escalations, Email Quarantine Analysis, Phishing, Brute Force

Networking & Infrastructure: Routing & Switching, Cisco Switches, Network Administration, IPsec VPN, Site-to-site VPN, NAT & PAT, AWS EC2, Windows Server, Active Directory (AD), Docker

Programming & Development: Python, C++, C#, Ruby, HTML, CSS, JavaScript, SQL, PHP, Flask, Data Structures & Algorithms, Object-Oriented Programming (OOP)

Databases & Platforms: PostgreSQL, MySQL, Supabase, Thingsboard, WordPress, Wix

Productivity & Software: Microsoft Word, Excel, PowerPoint, Access, Data Visualization, Generative AI, Web Development, Ticketing System

Professional Skills: Report Writing, Social Engineering, Communication, Teamwork

PROJECTS

Web Exploitation & Penetration Testing Lab | Self-Directed Jan 2026 – Present (In Progress)

- Lab Configuration:* Configured a virtualized testing environment using Kali Linux to simulate real-world web application vulnerabilities.
- Attack Simulation:* Utilizing WebSploit and other penetration testing tools to execute Man-in-the-Middle (MITM) attacks, directory scanning, and credential harvesting in a controlled environment.
- Defensive Analysis:* Analyzing the attack traffic and logs generated during simulations to identify detection patterns and improve threat hunting capabilities.

Go-HIDS: Real-Time Host Intrusion Detection Agent | Jan 2026 - Present (In Progress)

- Developed a real-time security agent in Go, utilizing Goroutines for concurrent log processing without blocking system resources.*
- Engineered a Regex-based detection engine to identify Indicators of Compromise (IOCs) like SSH Brute Force (MITRE T1110) and privilege escalation.*
- Built an automated alerting pipeline that parses raw logs into structured JSON and triggers instant webhook notifications for analysts.*

Mathology In-house Management System (Final Year Project) | July 2025

- Designed and developed a web-based system for class scheduling, attendance tracking, and payment management.*
- Implemented front-end using HTML, CSS, JavaScript and back-end with PHP & SQL.*
- Enhanced operational efficiency by automating manual tasks for a math learning center.*
- Applied secure coding practices to protect student and financial data.*

IoT Obstacle Avoidance Car | April 2025

- Built an autonomous car capable of detecting and avoiding obstacles in real time.*
- Programmed microcontrollers using Arduino and integrated Raspberry Pi for processing.*
- Utilized Python for sensor data handling and motion control.*
- Applied IoT concepts and hardware-software integration for practical robotics.*