EWALDO SIMON HIRAS

aldo@aldosimon.com | linkedin.com/in/aldosimon | aldosimon.com

PROFESSIONAL EXPERIENCE

PHILIP MORRIS INTERNATIONAL

Senior Infosec Incident Response Engineer 2022 - Present

- Triaged and responded to various incidents across enterprise infrastructure of over 50.000 endpoints (AD, AAD, OT)
- Planned, managed, and reported company's quarterly threat hunts
- Developed and implemented incident response tooling and scripts enhancing in-house SOAR collection capabilities
- Developed and improved L1 and L2 detection and analysis playbooks
- Provided technical advice to regional information security officers, L1-L2 analyst, and quarterly tabletop exercise
- Awarded "Above and Beyond Call of Duty 2023 award" for contribution in SOC migration from inhouse to third party SOC

DIRECTORATE GENERAL OF TAXES

Digital Forensic Lead 2013 - 2022

- Supervised a team of 9 digital forensic investigators, ensuring timely delivery of high quality digital forensic services
- Conducted information system assessment, host based forensic analysis, presenting analysis result to support over 150 investigations
- Interviewed and delivered testimony as expert witness in various cases focusing in digital forensics and digital evidence handling
- Developed and improved digital forensic procedures to better suit NIST SP 800-86, ISO 27037, ISO 27042, and ISO 17025
- Coordinated and taught in various digital forensic themed training courses

EDUCATION

UNIVERSITY COLLEGE DUBLIN – Dublin, Ireland

Master's in digital forensic

- First class honour/ GPA 3,91
- Awarded full tuition from Indonesia Endowment Fund for Education Scholarship
- Final project Metasploit exploitation from a forensic perspective
- Tutor for 121 IT for adult course

UNIVERSITY OF INDONESIA – Jakarta, Indonesia

Bachelor's in accounting

PROJECTS AND VOLUNTEER EXPERIENCE

- Indonesia Forensic Digital Association Research Team.
- Writer for Indonesia cyber defense community (cdef.id). Topics includes MITRE, windows core process, and honeypot.
- Reviewer for e-Magazine article on Indonesia cyber defense community (cdef.id)
- Configuring & running ELK stack to process suricata & syslog from a personal server
- Configuring & running ELK stack and tableau to process cowrie log from a personal honeypot
- Digital forensic team for investigative forensic audit project (undisclosed company)
- Present in OWASP ID-Virtual Appsec 2020 on honeypot use case
- Present in Indonesia security summit 2018, 2020 on digital forensic topics
- Mentor in 121digital.ie on IT for adult program
- Lecturer in Indonesia Ministry of Education Program on network forensic subject
- Mentor in Dealls Mentoring program (data and engineering category)
- Instructor in digital forensic class for audit in various platform

SKILLS

- **Frameworks:** DFIR framework (ISO 27037, ISO 27042, NIST SP 800-86, NIST SP 800-61); NIST cyber security framework and NIST security controls (NIST SP 800-53), NIST risk management framework (NIST SP 800-37), and MITRE ATT&CK framework
- **Security Operation Tools:** SIEM/SOAR (ELK Stack, Azure Sentinel, MDE, Splunk, Phantom), DFIR (KAPE, FTK, Encase, Autopsy, UFED Cellebrite, Oxygen Forensic), IDS/IPS (Suricata), vulnerability management tools (Brinqa, OpenVAS, Nessus, Openscap), threat intelligence platform (Shodan, GiB portal), CMDB (SOFY, LeanIX)
- **Languages:** bash, python
- **Supporting tools:** Confluence, JIRA, SNOW

CERTIFICATION

- Tryhackme cyber defence learning path certificate (tryhackme.com/ 2022)
- Certified Hacking Forensic Investigator/ CHFI (EC-Council/ 2021)
- Access Data Certified Investigator (Access Data/ 2020)
- XRY Certification (MSAB/ 2020)
- Cisco Certified CyberOps Associate (Cisco/ 2019)
- Oxygen Forensic Certified Examiner (Oxygen Forensic/2016)