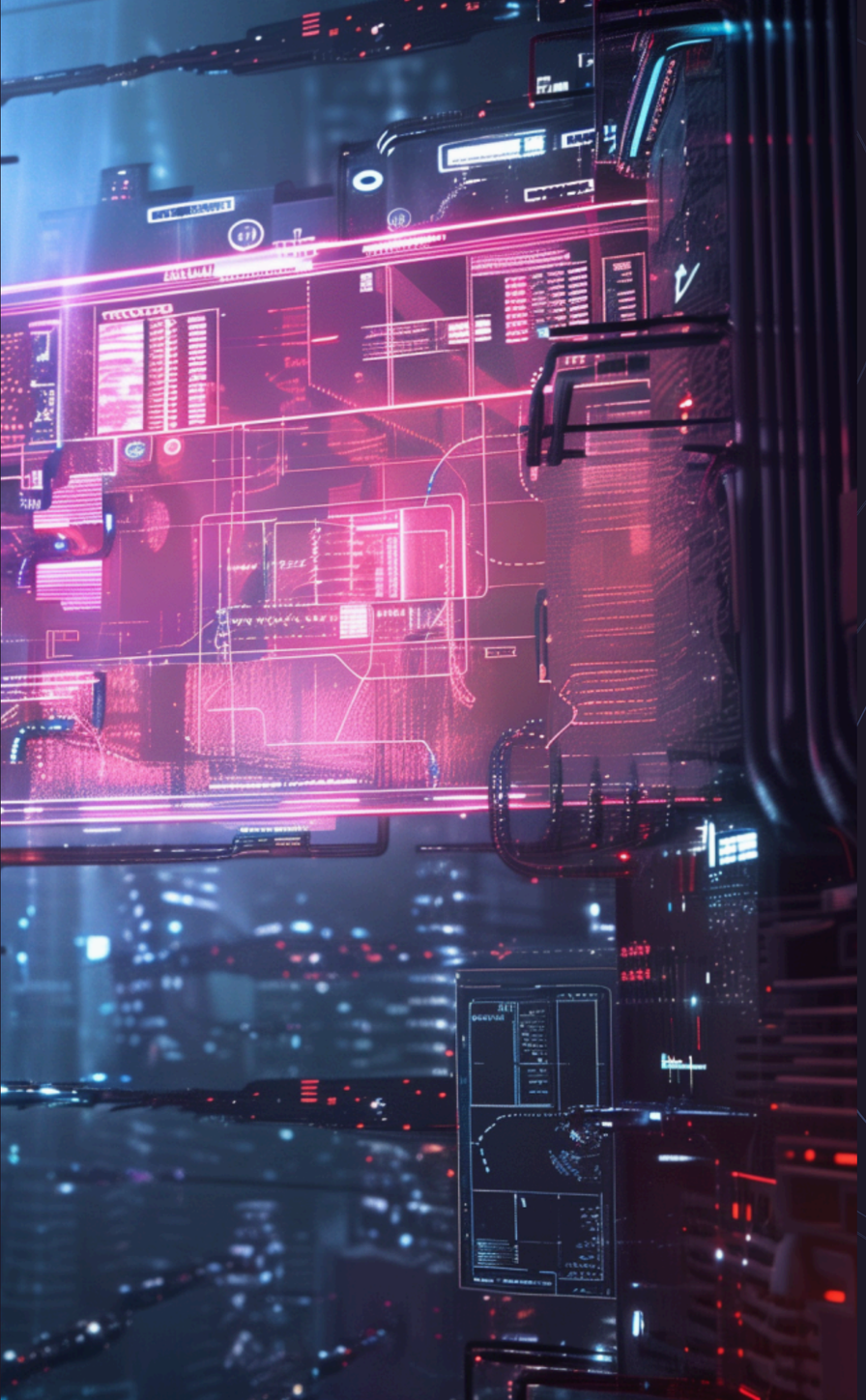

2025
PORTFOLIO
CYBERSECURITY JOURNEY'S
MARLLINE CALLISTA



MARLLINE CALLISTA

Introduction

– Aspiring Junior SOC Analyst

Lulusan IT yang berfokus pada transisi karier ke bidang keamanan siber, khususnya peran SOC Analyst. Memiliki fondasi yang kuat dalam konsep keamanan jaringan, insiden triage, dan analisis dasar malware melalui platform latihan praktis seperti TryHackMe. Berorientasi pada pembelajaran cepat, teliti dalam investigasi, serta memiliki minat besar terhadap deteksi ancaman dan perlindungan infrastruktur organisasi

31marll.chen@gmail.com

https://marllc31.github.io/portfolio/

www.linkedin.com/in/marllc

Tangerang, Indonesia

CYBERSECURITY SKILLSET

NETWORK & SECURITY
| WIRESHARK, ZEEK, NMAP, TCP/IP BASICS |

SCRIPTING
| PYTHON, COMMAND LINE (LINUX & WINDOWS) |

SIEM & MONITORING
| SPLUNK (BASIC), ALERT TRIAGE, LOG ANALYSIS |

INCIDENT RESPONSE
| EMAIL PHISHING TRIAGE, INCIDENT RESPONSE WORKFLOW, INCIDENT REPORT |

PLATFORM & LAB
| TRYHACKME, DICODING, IDCAMP |

LAB SHOWCASE 1

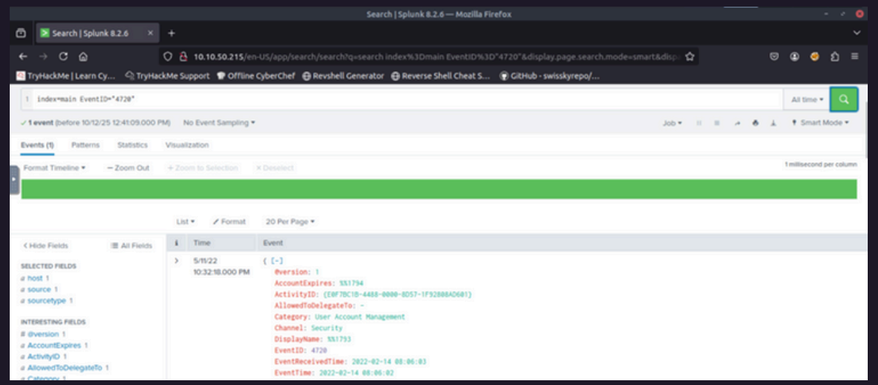
PLATFORM : TRYHACKME | KATEGORI : SIEM & INCIDENT INVESTIGATION
DATE : AUG '25

🧠 Ringkasan Investigasi

Simulasi investigasi compromised web server menggunakan Splunk SIEM dengan menganalisis log Windows (Sysmon, PowerShell, Event Logs) untuk mengidentifikasi indikator kompromi (IOCs).

- Melakukan pencarian awal (initial hunting) untuk mendeteksi aktivitas abnormal dari akun tertentu.
- Menemukan akun backdoor dan modifikasi registry untuk persistence.
- Menganalisis akun yang ditiru serta perintah berbahaya yang digunakan.
- Mengorelasikan IP, host, dan event untuk mengonfirmasi kompromi.

Tools yang digunakan: Splunk, Cyberchef, Mozilla Firefox



Screenshot of Splunk Dashboard
Src: TryHackMe Challenge

📝 Hasil & Deliverable

- Teridentifikasi akun backdoor dan aktivitas persistence pada server Windows.
- IOCs terkonfirmasi melalui korelasi log lintas sumber.
- Memperkuat keterampilan deteksi ancaman dan analisis log SIEM.

🧰 Keterampilan: *Splunk query* · Windows log analysis · Log correlation · SOC investigation workflow

LAB SHOWCASE 2

PLATFORM : TRYHACKME | KATEGORI : ALERT TRIAGE & PHISHING DETECTION

DATE : AUG '25

🧠 Ringkasan Investigasi

Simulasi investigasi phishing pertama menggunakan SOC Simulator. Fokus utama adalah mengidentifikasi apakah alert yang muncul merupakan True Positive atau False Positive.

Langkah-langkah:

- Menganalisis alert firewall terkait akses ke URL yang diblokir.
- Mengecek IP, domain, dan URL terhadap threat intelligence feed.
- Mengonfirmasi bahwa alert adalah True Positive (URL & IP malicious, domain lookalike).
- Menyimpulkan bahwa firewall berhasil mencegah koneksi sehingga tidak ada kompromi nyata dan tidak memerlukan eskalasi.

Screenshot of Alert
Src: TryHackMe Challenge

📝 Hasil & Deliverable

- Teridentifikasi alert phishing valid (True Positive) tanpa eskalasi.
- IOC (IP, URL, domain) terdokumentasi untuk threat intel feed.
- User yang menjadi target (HR Dept.) perlu edukasi dan reset password jika sempat submit kredensial.
- Menyusun incident report berdasarkan hasil investigasi.
- Memahami alur kerja dasar triage alert dalam SOC Simulator.

🧰 Keterampilan: *Alert triage* · IOC validation · Threat intelligence check · SOC workflow fundamentals · Incident reporting

LAB SHOWCASE 3

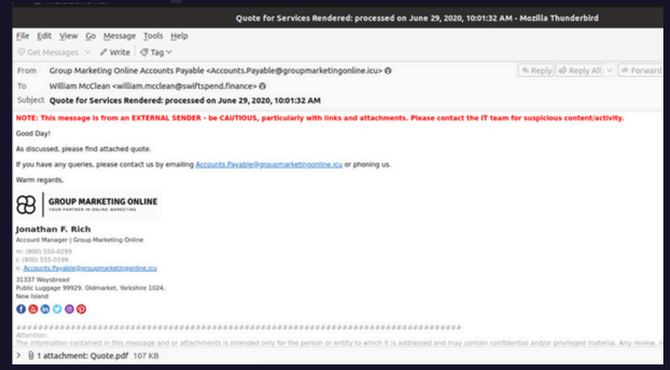
PLATFORM : TRYHACKME | KATEGORI : PHISHING & INCIDENT RESPONSE
DATE : SEPT '25

🧠 Ringkasan Investigasi

Simulasi investigasi phishing dengan langkah-langkah:

- Menganalisis header email menggunakan Thunderbird untuk mengidentifikasi pengirim asli dan domain spoofing.
- Menelusuri URL phishing menggunakan Firefox dan mengambil kit phishing melalui command line.
- Menggunakan Cyberchef & VirusTotal untuk korelasi CTI dan identifikasi infrastruktur berbahaya.
- Mengumpulkan informasi lanjutan dari kit phishing untuk profiling penyerang.

Tools yang digunakan: Thunderbird, Cyberchef, VirusTotal, Command Line, Mozilla Firefox



Screenshot of Email Header
Src: TryHackMe Challenge

📝 Hasil & Deliverable

- Mengidentifikasi sumber phishing dan memastikan tidak ada akun pengguna yang terkompromi.
- Memperkuat keterampilan triage alert dan investigasi email — kompetensi inti seorang SOC Analyst.

🧰 Keterampilan: *Email header analysis* · URL investigation · CTI correlation · Alert triage

CAREER TIMELINE

IT GRADUATE	ADMIN PAJAK	BELAJAR CYBERSECURITY	SERTIFIKASI + TRYHACKME	FOKUS SOC ANALYST
2022	2022-2024	2024-2025	2025	2025

CERTIFICATIONS & COURSES

- TRYHACKME SOC LEVEL 1 — 2025
- CISCO JUNIOR CYBERSECURITY ANALYST CAREER PATH — 2024
- COURSE-NET INDONESIA NETWORK ADMIN, IT SUPPORT & ETHICAL HACKING — 2024
- EC-COUNCIL DIGITAL FORENSICS ESSENTIALS — 2022

🌑SILENT BUT SCANNING 🐾
NEWBIE IN THE TERMINAL, VETERAN IN CURIOSITY.
WALKING THROUGH WALLS, ONE MODULE AT A TIME.
CURRENTLY HACKING MY OWN LIMITS. 🌱

“PORTFOLIO PREPARED BY MARLLINE. C — 2025”