

# Wykiyanos Woldesemayat

Dallas–Fort Worth, TX · Open to remote

wykiyanosa@gmail.com

Portfolio · GitHub

LinkedIn: add link

Entry-level SOC analyst with the **Google Cybersecurity Professional Certificate** and hands-on labs in SIEM alert triage, incident response, network traffic analysis, Linux/SQL, and **Python automation**. Known for clear documentation, fast triage, and customer-centric communication from prior entrepreneurship experience.

SIEM (Microsoft Sentinel, Splunk)

KQL / SPL

Wireshark / PCAP

Linux & Bash

SQL

Nmap

Regex

Python

Git/GitHub

## CERTIFICATIONS

### Google Cybersecurity Professional Certificate — Coursera

Nov 2025

Foundations · Manage Security Risks · Network Security · Linux & SQL · Assets/Threats/Vulnerabilities · Detection & Response ·

Automate Cybersecurity Tasks with Python · Prepare for Jobs

Verify: <https://coursera.org/verify/BQG7YW6GGDH>

## TECHNICAL PROJECTS & PORTFOLIO

### SIEM Alert Triage Lab — Microsoft Sentinel & Splunk

2025

- Investigated >100 practice alerts; used **KQL/SPL** to filter noisy events, validate IOCs (IP, hash, domain), and decide: close, contain, or escalate.
- Documented timelines, evidence (screenshots, PCAP extracts), and next steps in an Incident Handler's journal.

### Network & Log Analysis — Wireshark, Linux, Regex

2025

- Parsed auth.log with Python/Regex to extract failed SSH attempts and top offending IPs; built quick indicators list for blocking.
- Analyzed PCAPs to identify beaconing and suspicious DNS; wrote investigation notes and remediation recommendations.

### Vulnerable System Analysis — Nmap, Hardening

2025

- Enumerated services and misconfigurations on a lab host; prioritized findings using CVSS-style severity and proposed hardening steps.

### SQL Investigation Queries — Incident Reporting

2025

- Wrote reusable SQL to correlate user accounts with failed logins, geo-anomalies, and endpoint alerts; exported CSVs for case notes.

See: Portfolio [oceansrat.github.io/cyber-portfolio](https://oceansrat.github.io/cyber-portfolio) · GitHub journals: thm-journal, incident-handlers-journal, vulnerable-system-analysis, sql-investigation-queries

## CORE SKILLS

- Alert Triage:** SIEM dashboards, IOC validation, false-positive reduction.
- Incident Handling:** scoping, containment suggestions, ticket updates, clean hand-offs.
- Network Analysis:** Wireshark filters, HTTP/DNS review, lateral-movement clues.

- Linux & SQL:** log review, grep/awk/sed, SQL joins/filters for investigations.
- Python:** small automations for log parsing, IOC extraction, CSV reporting.
- Documentation:** reproducible notes, timelines, and evidence attachments.

## PROFESSIONAL EXPERIENCE

### Owner / Operator — Small Business (DFW, TX)

2019–2025

- Led operations, scheduling, and customer communications; maintained records with Google Workspace.
- Developed checklists and SOPs that improved quality and reduced rework; resolved customer issues with clear, calm communication.
- Transferred strong documentation and prioritization habits directly to SOC workflows.

## EDUCATION & TRAINING

- **Merit America — Cybersecurity Track** (2025)
- Google Cybersecurity Professional Certificate (Coursera), 2025

## TOOLS

Microsoft Sentinel

Splunk

Wireshark

Kali / Linux

Windows

Nmap

Python

SQL

Regex

Git/GitHub