Muhammad Falah Aufa Anggara

082322047740 | mfaufalaha@gmail.com | LinkedIn | GitHub | aufa.me

Sleman, Yogyakarta, Indonesia

Information Technology student at Universitas Gadjah Mada focused on blue team and SOC operations. Hands-on practice through SIEM home labs (Wazuh, Elastic Stack, Splunk): attack simulation, alert triage and validation, detection rules, and incident response playbooks. Seeking a cybersecurity internship.

Education

Universitas Gadjah Mada Aug 2024 – Present

Bachelor of Engineering, Information Technology · Yogyakarta, Indonesia

Skills

SIEM & Monitoring: Wazuh, Elastic, Splunk, Suricata, Log Analysis, Alert Triage, Detection Rules

Security Concepts: Incident Response, Playbooks, MITRE ATT&CK, Network Security, Linux Hardening

Tools & Scripting: Python, Bash, Linux, Wireshark, Nmap, Hydra, Git

Projects

Wazuh Home Lab · *Wazuh 4.14.6, Hydra, VirtualBox* · GitHub Jul 2026 – Aug 2026

- Built a Wazuh SIEM lab and simulated SSH brute force from Kali (Hydra and a sequential script); wrote custom correlation rule 100002 (5 failures vs. default 8) for earlier detection.
- Validated alerts in stages (wazuh-logtest, Dashboard, alert count vs. attempts) and automated containment with Active Response firewall-drop.

Elastic Stack Home Lab · *Elasticsearch 9.5.5, Kibana, Fleet* · GitHub Sep 2026 – Oct 2026

- Deployed Elasticsearch, Kibana, and Fleet with Linux and Windows agents; investigated SSH and RDP brute force with KQL, cross-checking raw logs (auth.log, Event IDs 4625/4624) after finding parsed fields unreliable.
- Built two detection rules (custom query, threshold) mapped to MITRE ATT&CK T1110.001, plus a dashboard per endpoint.

Incident Response Playbooks · *Wazuh, Suricata, Kali Linux, DVWA* · GitHub Oct 2026 – Present

- Responded to two simulated attacks (SSH brute force; SQL injection and web shell upload with RCE), documented as incident reports with YAML playbooks.
- Used Suricata as a network sensor feeding Wazuh and wrote a custom rule for web shell activity after finding a missing signature; root-caused a broken monitoring pipeline that had stopped Active Response.

Linux Hardening & Audit · *Ubuntu Server 24.04, Bash, CIS Benchmark* · GitHub Jul 2026 – Present

- Hardening Ubuntu Server 24.04 against the CIS Benchmark by hand (custom 6-partition layout, noexec/nosuid/nodev on /tmp) with a 96-item checklist and a baseline snapshot.
- Analyzed auth.log from simulated failed SSH logins and found a single grep pattern misses “Invalid user” events; Bash audit script in progress.

Certifications & Training

Google Cybersecurity Certificate Coursera · 2026

Foundations of Cybersecurity (Jul 2026) · Play It Safe: Manage Security Risks (Oct 2026) · Connect and Protect: Networks and Network Security (Oct 2026)

TryHackMe 2026

Cyber Security 101 (Jul 2026) · Pre Security (May 2026)

Cisco Networking Academy 2025 – 2026

Introduction to Networks (Jun 2026) · Introduction to Cybersecurity & Python Essentials (Oct 2025)

Experience

Gadjah Mada Robotic Team Oct 2024 – Sep 2025

Motion Programmer · Universitas Gadjah Mada

- Programmed motion control for autonomous robots and maintained the team’s legacy codebase.
- Tuned control parameters through iterative testing and calibration to improve movement stability.