Muhammad Abdullah

Security Operations Analyst · Islamabad, PK

muhammaddabddullah@outlook.com | linkedin.com/in/mabddullah | github.com/muhammad1502 | mabddullah.vercel.app

SUMMARY

Security operations analyst with two years of SOC, incident response and IT operations work for North American enterprise clients. Investigates 100+ alerts a week in Elastic SIEM and Microsoft 365 Defender and supported the response to an active, threat actor-led ransomware attack. Also designs and builds accessible websites using AI-assisted development.

WORK EXPERIENCE

Security Operations Analyst, Ninpo Inc. · Ottawa, Canada · Remote — Oct 2024 to present

SOC analyst for a Canadian cybersecurity firm. I handle threat detection, incident response and IT operations across several North American enterprise client environments.

- **Incident response:** Supported the response to an active, **threat actor-led** ransomware attack by isolating compromised domain controllers and ESXi hosts before large-scale encryption.
- **Threat hunting and triage:** Investigate **100+** alerts a week in Elastic SIEM and classify phishing in Perception Point with **95%+** accuracy. Findings have ranged from compromised VPN credentials to unauthorized RDP lateral movement.
- **Detection engineering:** Worked with engineering to tune SIEM detection rules, cutting false positives by **20%** through baseline behavior analysis and log correlation.
- **Endpoint hardening:** Audited Elastic EDR health across hybrid environments and fixed hosts where anti-tampering protection had been turned off, reaching **100%** telemetry coverage.
- **IT operations and Microsoft 365:** Administer Microsoft 365 tenants through Pax8, configure VPNs and firewall updates, resolve client support tickets and provision endpoints for new hires.
- **Reporting:** Built incident metrics mapped to MITRE ATT&CK, giving leadership clear data on adversary tactics, techniques and procedures (TTPs).

Product Growth & Strategy, AfterDesk · Independent Product · Remote — Jul 2026 to Aug 2026

Built the product and growth groundwork for AfterDesk, an after-sales case manager for small online sellers that keeps the evidence with every case.

- **Product strategy:** Defined the core case workflow: the customer report, evidence, deadlines, resolution, third-party recovery and the final financial outcome.
- **Acquisition and activation:** Built a public site with transparent pilot pricing, an interactive product demo and a protected pilot workspace, so prospects can go from first visit to trying the product.
- **Trust and readiness:** Wrote **37** linked notes on product, architecture, security, API and ethics, and documented the privacy policy and terms, evidence-security boundaries and pilot release risks.

Product Growth Auditor, FitSmart AI · Project Contribution · Remote — Jul 2026

Ran an evidence-based UX and growth review of an AI fitness and nutrition app, then turned the risks I found into a remediation plan the team could implement.

- **Growth and monetization:** Audited nine product areas and designed clearer quota visibility, plan-aware paywalls, pricing guardrails and retention flows, plus a measured path toward token or credit pricing.
- **Conversion and trust:** Gave upgrade prompts more context, made payments safer and removed misleading "unlimited" language. Users who hit a limit keep what they were doing, and product claims now match how the system actually behaves.
- **Product quality:** Specified and validated fixes for accessibility, data integrity, AI routing and usage observability, covering **37** audited icon controls with **18/18** Worker tests passing.

PROJECTS

GitLab Triage Accelerator · Browser extension: Quick actions and hotkeys that speed up high-volume GitLab security triage for L1 and L2 analysts.

VT Extension · Browser extension: Right-click a selected IP, URL, hash or domain to check it on VirusTotal (Manifest V3).

VT Checker for Android · Android app: Adds "Check on VirusTotal" to the text-selection menu in any Android app.

SKILLS

Security operations: Elastic Security (SIEM), Incident response, Alert triage, Phishing analysis with Perception Point, IOC hunting, OSINT

Threat detection: MITRE ATT&CK mapping, TTP analysis, Sysmon, Osquery, Anomaly detection, Cyber Kill Chain

Infrastructure and admin: Microsoft 365 Defender and Admin via Pax8, SonicWall and WatchGuard firewall & VPN, RDP/SSH forensics, VMware ESXi, Windows and Linux

Data and programming: Python (Pandas, NumPy, OOP), Bash scripting, SQL, Regex, Jupyter, Matplotlib

Web design and development: Responsive and accessible web design (WCAG 2.2), AI-assisted development (React, TypeScript), UX and growth audits, Landing pages and interactive product demos

CERTIFICATIONS AND TRAINING

Google Cybersecurity Professional Certificate · Professional certificate

CompTIA Security+ · Certification exam · In progress

Blue Team Junior Analyst (BTJA), Security Blue Team · Training pathway certificate

Introduction to Cybersecurity Essentials, IBM · Course certificate

Identity Security Sales Certification, WatchGuard · Sales certification · Valid through Sep 2027