Anas TAGUI

Futur Ingénieur Cybersécurité · Analyste SOC · Alternance 12 mois

+33 7 80 83 37 37 | atagui.ir2027@esaip.org | Angers, France | linkedin.com/in/taguianas | github.com/taguianas

PROFIL

Étudiant ingénieur cybersécurité (4e année, ESAIP), certifié CEH & Google Cybersecurity. Tryhackme Top 4%. Spécialisé SOC : détection de menaces, réponse aux incidents, SIEM/SOAR . Auteur de PhishGuard, Admin-Script et Red Team Framework (GitHub).

PROJETS

PhishGuard : Détection Anti-Phishing · Python, VirusTotal API *PhishGuard-AI*

- Outil SOC de scoring et classification d'URLs malveillantes via VirusTotal API (risque faible/suspect/malveillant), avec alertes automatisées et journalisation des IOCs : reproduit un workflow analyste N1.

Admin-Script : Automatisation Sécurité Linux · Bash, PowerShell *admin-script*

- Suite de scripts d'audit système (droits users, intégrité fichiers, rotation logs) sous Linux/Windows Server : réduction du temps d'audit manuel de ~50 % dans le homelab SOC.

Red Team Shell Framework · Bash, Shell *redteam-shell-framework*

- Framework Red Team modulaire (recon, exploitation, post-exploitation) aligné MITRE ATT&CK : réduit de ~40 % le setup d'un test d'intrusion.

SOC Virtuel : Homelab SIEM/SOAR [En cours] · Wazuh, TheHive, Shuffle *soc-home-lab*

- Homelab SOC complet avec scénarios d'attaques contrôlées, playbooks SOAR et corrélation multi-sources : réduction estimée de 60 % du temps de réponse manuelle.

EXPÉRIENCE PROFESSIONNELLE

Technicien Informatique : Stage : **Ministère de l'Equipement, Transport & Logistique** | Maroc *Juin – Sept. 2023*

- Déployé et durci 20+ postes (OS, logiciels, hardening) résolution d'incidents et rédaction de fiches de configuration pour la base de connaissances IT.

FORMATIONS

- **Cycle Ingénieur : Informatique & Réseaux** : ESAIP, Angers, France *2024 – 2027*
- **Échange : Informatique & Sécurité de l'Information** : Politechnika, Varsovie, Pologne *Fév. – Juil. 2025*
- **Échange : Cybersécurité & Réseaux** : La Salle, Barcelone, Espagne *Fév. – Juil. 2026*

COMPÉTENCES TECHNIQUES

SIEM/SOAR/CTI : Wazuh, Splunk, TheHive, Shuffle, MISP, OpenCTI, VirusTotal API, AbuseIPDB
Pentest & Offensif : Metasploit, Burp Suite, Nmap, Nessus, OpenVAS, Netcat, Hydra
Forensique/Malware : Ghidra, x64dbg, Autopsy · Frameworks : MITRE ATT&CK, OWASP Top 10, ISO 27001, NIST
Systèmes & Dev : Linux/Kali, Windows Server, AD, Docker, Kubernetes · Python, Bash, PowerShell, JS, Java
Langues : Arabe (natif) · Français (courant) · Anglais (courant) · Espagnol (intermédiaire)

CERTIFICATIONS

Google Cybersecurity Certificate : Google *2025*
Certified Ethical Hacker (CEH) : EC-Council *2026*
SOC Analyst Path + CTF (TryHackMe) : Hack The Box & TryHackMe *2024 – en cours*

À PROPOS DE MOI

Taekwondo Ceinture Noire · discipline et résilience sous pression **Snooker (Billard)** · stratégie et concentration