Mohamed Amir Trigui

Cybersecurity Engineer

✉ mohamedamir.trigui@esprit.tn
☎ +216 50217626
in Amir Trigui

Passionate Cybersecurity with a strong background in Security Operations Centers (SOC), including SIEM, EDR, and Incident Response. My skills also extend to the field of Penetration Testing, where I actively engage in identifying and exploiting vulnerabilities. I am determined to expand my knowledge and skills in Cloud security. My motivation, discipline, and collaborative mindset enhance security measures and foster innovation.

EDUCATION

Computer Engineering , Cybersecurity 2020 – 2023
Ecole Supérieure Privée d'Ingénierie et de Technologies - ESPRIT

Preparatory cycle (MP) 2018 - 2020

Mathematics Baccalaureate 2018

INTERNSHIP

SOC Analyst , Internship — Jan 2023 – Jul 2023

Centre de Calcul El Khawarizmi (cck), Manouba

Security Orchestration, Automation, and Response (SOAR) deployment for automatically detecting and responding to cyber threats in a production environment using:

- ELK SIEM , Wazuh EDR solution
- TheHive Incident Response , Cortex Automation enrichment
- MISP Threat intelligence , Shuffle Orchestration and Automation
- Velociraptor Digital Forensics
- OSINT frameworks for intelligence gathering and risk assessment

Cybersecurity , Internship — Jul 2022 – Aug 2022

Digitalberry, Lac 2

- Web application Pentesting using Burp suite and Audit management
- Sql injection and XSS on different labs
- Forensics with wireshark and sguil
- Pfsense implementing and Brute force and DDOS detection with Snort
- Establish a local VPN architecture with OpenVpn
- Create a Password policy and Password manager with Bitwarden

Web development , Internship — Jun 2021 – Jul 2021

Orange Tunisie, Charguia

Creation of a web page in PHP, HTML, CSS, JS, and a database using the WAMP server. Implemented authentication functionality and CRUD operations, including a dashboard, a chart, and a datatable.

PROJECTS

Active Directory — Aou 2023 – Sep 2023

- Manage Active Directory by configuring and securing user access and permissions.
- Conduct Penetration Testing and identify vulnerabilities.

DevSecOps — Oct 2022 – Nov 2022

- Continuous integration and automation with Jenkins Pipeline.
- Creating and running unit tests.
- Continuous delivery.
- Enforce Security using SAST and DAST.

Security Operations Center (SOC)Implementation Using SOAR — Jan 2022 – May 2022

- Installing a functional infrastructure design.
- Secure components with pfSense firewall , Snort IDS/IPS and Honeypot.
- Using ELK SIEM, Malware Analysis Cuckoo Sandbox solution.
- TheHive Incident Response , MISP Threat intelligence solution.
- Cortex Automation , Patrowl orchestration solution.

Desktop application for Smart -Farm — Sep 2020 – Dec 2020

I have created a desktop application that automates farming tasks using C, Glade, and GTK for graphical interfaces.

SKILLS

SOC : Splunk , Zabbix , Yara , OpenVAS , Active Directory

Cyber Kill Chain

DevSecOps : Jenkins , Nexus , SonarQube , Gauntlt , Trivy , OWASP -ZAP , Grafana , Ansible , Azure

IAM : Keyclock

Programming : PHP, XML , HTML , CSS , JS , C , C# , JAVA , Java EE , MySQL

Framework : Spring Boot , .Net

Scripting language : Python , Bash

Systems : Working in mixed Windows / Linux , database and virtualized/physical server

COURSES

• Certified Ethical Hacker : CEH v12	2022
• Cloud Security	2022
• ISO 27001	2022
• Palo Alto	2022
• CyberOps Associate 1.0	2021
• CCNA Security 2.01	2021

ACTIVITIES

• CTF player : TryHackMe , HackTheBox et VulnHub	2021 - Présent
• IEEE And Securinets Esprit member	2021 - 2022

LANGUAGES

English	●●●●○
French	●●●○○
Arabic	●●●●○