

# FATIMAH ALQARZAI

CYBERSECURITY ANALYTICS PROFESSIONAL, DIGITAL  
FORENSIC ANALYSIS, INCIDENT RESPONSE, SOC ANALYST

## DETAILS

### ADDRESS

Saudi Arabia

### PHONE

+966540889809

### EMAIL

fatimahalqarzai@gmail.com

## SOCIAL LINKS

[LinkedIn](#)

## SKILLS

Detect how and when a breach occurred

● ● ● ● ● ●

Identify compromised and affected systems

● ● ● ● ● ●

Perform damage assessments and determine what was stolen or changed

● ● ● ● ● ●

Contain and remediate incidents

● ● ● ● ● ●

Hunt down additional breaches using knowledge of the adversary

● ● ● ● ● ●

Develop key sources of threat intelligence

● ● ● ● ● ●

Cyber-kill chain strategies.

● ● ● ● ● ●

Rapid and deep-dive timeline creation and analysis.

● ● ● ● ● ●

Discovery of unknown malware on a system.

● ● ● ● ● ●

## PROFILE

I am creative, talented and a hard worker. I have strong technical skills, enabling me to deal with a wide range of tasks. With a clear, logical mind and a practical approach to problem-solving and a drive to see things through to completion. With more than 2 years of self-training and studying. I am eager to learn.

## EDUCATION

### Bachelor's of Computer Science , Alqassim University

Alqassim

Jun 2014 — Dec 2018

### Higher Diploma of Cyber Security, Alqassim University

Alqassim

Sep 2019 — May 2020

Graduated with an "Excellent" grade and a G.P.A (of 5.00/5)

## CERTIFICATIONS

### CompTIA Security+

Feb 2021 — Feb 2027

### CompTIA Cyber Security Analyst (CySA+)

Jan 2022 — Jan 2025

### CompTIA Security Analytics Professional (CSAP)

Jan 2022 — Jan 2025

### SANS Windows Forensics Analysis FOR500

Feb 2022

### SANS Advanced Incident Response, Threat Hunting, and Digital Forensic FOR508

Mar 2022

I am proud to announce that I won 1st place along with my team in the last day challenge.

## COURSES

### CyberPro+ Trainee, National Cybersecurity Authority

Dec 2021 — May 2022

### FOR500 Windows Forensics Analysis, SANS Institute

Examination of digital forensics

● ● ● ● ● ●

Acquire data and memory in an efficient and forensically sound

● ● ● ● ● ●

Analyze, and authenticate forensic data on Windows systems and servers

● ● ● ● ● ●

Track individual user activity on networks

● ● ● ● ● ●

Organize findings for use in incident response, internal investigations

● ● ● ● ● ●

Validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies

● ● ● ● ● ●

Network Monitoring and Analysis using Wireshark , Tcpdump

● ● ● ● ● ●

Analysis network traffic using Arkime

● ● ● ● ● ●

Network Security Monitor using Zeek

● ● ● ● ● ●

Searching, monitoring, and analyzing machine generated data using Splunk

● ● ● ● ● ●

Scripting for log analysis using Petit

● ● ● ● ● ●

## LANGUAGES

---

Arabic

● ● ● ● ● ●

English

● ● ● ● ● ●

**FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensic , SANS institute**

**Splunk Security - From Zero to Hero workshop**

**APT Threat Hunting workshop**

**Security Telemetry Essentials workshop**

**Security Investigations Foundations workshop**

## SOFT SKILLS

---

**Data Anlysis using Sql , Python**

**Data Visualization using Tableau and PowerBi**

**Programmer C++,Java, Python, Html, Css, Javascript, Php**

**Working with Databases using Sql**

## EMPLOYMENT HISTORY

---

**Customers Service (Coop-Training), Bank Albilad**

Alqassim

Feb 2019 — Apr 2019

## VOLUNTEER WORK EXPERIENCE

---

**Programmer**

For two month, i worked with: Html, Javascript, Php, Sql, Bootstrap, Css.