# Mohammed Elzanaty

Glendale, CA 91214
818-430-2738 | m8elzanaty@gmail.com
https://www.linkedin.com/in/mohammed-elzanaty

## SUMMARY

Analytical, diligent Cybersecurity Engineer with leadership skills and a passion for cybersecurity. Lifelong learner, experienced collaborator, and innovator. Ability to leverage background in Mathematics Education, critical thinking, and analytical skills to identify system vulnerabilities and mitigate risks to prevent future security breaches.

## CYBERSECURITY CERTIFICATIONS

| | |
|---|---|
| ● CompTIA Security+ | September, 2021 |
| ● Python (part 1) | July, 2021 |
| ● Computer Science Discoveries | June, 2021 |
| ● Real-Time Cyber Threat Detection and Mitigation | April, 2021 |
| ● Cybersecurity in Healthcare (Hospitals & Care Centers) | April, 2021 |
| ● Splunk Infrastructure Overview; Splunk User Behavior Analytics | January, 2021 |
| ● Splunk 7 .x Fundamentals Part1 | January, 2021 |
| ● AWS Security Fundamentals (Second Edition) | January, 2021 |

## CYBERSECURITY TECHNICAL SKILLS

**Tools:** Kali Linux, Metasploit, Hashcat, Wireshark, Nmap, Microsoft Azure, Autopsy, ELK, Kibana, and Splunk
**Cyber:** Linux Administration and Hardening, Windows and Mac OS, Cloud Security and Virtualizations, Forensics

## CYBERSECURITY PROJECTS

**Attack, Defense & Analysis of a Vulnerable Network** January, 2021

Worked as a Cybersecurity Engineer, collaborated with a team of 5, supporting an organization's SOC infrastructure to investigate some discrepancies with alerting in the Kibana system and confirm that newly created alerts are working.

- Completed the project individually but also engaged in troubleshooting meetings with the team for problem-solving.
- Defensive Security: Implemented alerts and thresholds, determined to be effective.
- Offensive Security: Used Penetration testing concepts to assess and attack vulnerable VMs and exploited the vulnerabilities in their network gaining root access to the machines.
- Network Forensics: Verified that Kibana rules worked as expected and used Wireshark to analyze live malicious traffic on the wire.
- Documented and developed reports of the findings and analysis.
- Presented recommendations to the company to improve the security of their data and mitigate risks to prevent future security breaches.
- Kali Linux; Searchsploit; Nmap; nikto; gobuster; netcat; John the Ripper password cracker; Kibana; Wireshark
- https://github.com/zanatooo/Pen-Testing-Defense.git

**Assessment, Analysis, and Hardening of a Vulnerable System** December, 2020

Worked on a Red Team v. Blue Team scenario as both pentester and SOC analyst.

- **Red Team**: Used penetration testing concepts and attacked a vulnerable VM, gaining root access to the machine.
- **Blue Team**: Used Kibana to review logs, extracted hard data and visualizations, then interpreted the log data to suggest mitigation measures for each exploit that was successfully performed.
- Kali Linux; Metasploit (Meterpreter); Nmap; Hydra; CrackStation (hash cracker); Kibana
- https://github.com/zanatooo/Assessment-Hardening.git

**Cloud Security and ELK stack** November, 2020

- Completed the project individually but also collaborated with my team to:
- Deploy containers using Ansible and Docker; Deploying Filebeat using Ansible; Deploying the ELK stack on a server; Diagramming networks and creating a README. Created an ELK monitoring stack to monitor the performance of a Web server that is running DVWA.

- Azure Host; ELK stack; GitHub Repository
- https://github.com/zanatooo/Cloud-Security.git

## EXPERIENCE

**East West Bank** June 2021-July 2021

Information Security Engineer

- Monitored AV/EDR/IDS/IPS solutions for incidents, threat hunt for malicious activity, and triage as needed on a 24x7 basis.
- Monitored enterprise spam and phishing emails and participate in developing social engineering exercises
- Supported incident management and response activities as a member of the bank's incident management team; and assisted in triage, response and mitigation, postmortem analyses, and forensic analysis.
- Assisted in creating correlation rules to enhance detection via SIEM platform
- Assisted in monitoring DLP incidents, investigation, and tuning of DLP solution

**UCLA Cybersecurity Program** 2020 - 2021

Cybersecurity Engineer/Trainee

- Completed an intensive program at UCLA, dedicated to Cybersecurity, which is equivalent to two to three years' work experience. Skills and experience consist of Wireshark, Kali Linux, Metasploit, Burp Suite, and training towards Security+, Network+, CEH, and CISSP.
- Completed projects including Attack, Defense & Analysis of a Vulnerable Network; Assessment, Analysis, and Hardening of a Vulnerable System; and Cloud Security, which are outlined above.

**Glendale Unified School District** 2017 – Present

Mathematics Teacher; Robotics and Coding Teacher; Mathematics Department Chair

- Improved student's performance and math test scores by incorporating new technology/curriculum and innovative teaching and learning, and Led robotics and coding teams to win many awards in the First Lego Robotics League tournament and MESA (Math, Engineering, Science Achievement) competition.
- Awarded Teacher of the Year; Mathematics Department Chair; Lead Math Teacher for the STEM program.

Tech Lead

- Solve tech problems for teachers and students and ensure that tech infrastructure, including teacher and student laptops, Chromebooks, Ipads, Smartboards, projectors, and printers stay up-to-date and in working order for in-person and remote learning.
- Train teachers and other personnel on how to use various teaching apps safely such as Google Suite, Zoom, Nearpod, GoGuardian, Kami, Flipgrid, and Pearson online Textbook.

**Los Angeles Unified School District**

Mathematics Teacher; Robotics and Coding Teacher; Mathematics Department Chair; Soccer Coach

- Improved student's performance and math test scores by incorporating new technology/curriculum and innovative teaching and learning
- Developed the robotics and coding program.

Tech Lead

- Incorporated technology into math classrooms and solved tech problems for teachers and students
- Ensured that tech infrastructure, including teacher and student laptops, Ipads, Smartboards, projectors, and printers stay up-to-date and in working order.

**Key Accomplishments:**

- Completed hands-on projects in the UCLA Cybersecurity program with an overall A+.
- Nominated for the Presidential Awards for Excellence in Mathematics and Science Teaching, Teacher of the year; Mathematics Department Chair; Lead Math Teacher for the STEM program.

## EDUCATION

**Computer Science Discoveries Certificate:** University of Southern California**,** Los Angeles, CA

**Cybersecurity Certificate**: University of California, Los Angeles, CA

An intensive program dedicated to Cybersecurity. Skills learned consist of Wireshark, Kali Linux, Metasploit, and training towards Security+, Network+, CEH, and CISSP.

**Master of Arts in Educational Leadership/Administration**: CSU Northridge, Northridge, CA

**Professional Teaching Credential in Mathematics:** CSU Los Angeles, Los Angeles, CA

**Single Subject Teaching Credential In Mathematics:** CSU Northridge, Northridge, CA

**Bachelor of Science in Tourism and Travel Services Management**: Suez Canal University, Ismailia, Egypt