Sina Ebrahimi

IT Professional | Linux Enthusiast

(+98) 9902616166
xsinaebrahimi@gmail.com
More detailed cv in my github page
sinae99.github.io
linkedin.com/in/Sina-Ebrahimii

INTRO

IT professional with 2.5 years of SOC experience.
Skilled in monitoring, investigating incidents, and resolving system and network issues.
Now focusing on Linux administration and DevOps basics.
Interested in finding anomalies, misconfiguration and suspicious behaviors in systems.

EDUCATION

Bachelor of Computer Science	Amirkabir University of Technology (Tehran Polytechnic)	2018 - 2024
High School, Math and Physics	Allameh Tabatabaei High School	2014 – 2018

EXPERIENCE

Company: Central Securities Depository of Iran www.csdiran.ir Apr 2023 - Present
Title: Security Analyst

- Creating Splunk dashboards (routines) from scratch to monitor company assets and important network metrics
- Identifying security threats and abnormal activities and escalating incidents to the L2
- Analyzing SIEM alerts and identifying false positives
- Monitoring critical company services for availability
- Creating report and documentation for each shift and any related InfoSec

Company: Saba System Sadra www.ssystems.ir Dec 2022 – Apr 2023
Title: SOC Analyst Intern

- Learning security concepts and developing skills with the company's guidance

Company: DigiAhan www.digiahan.com 2022
Title: Office Manager & Salesman

- Managing sales and head of customer service section
- Inputting data into the company website, including daily prices and information about the products
- Cooperate with design team to increase the website performance

CERTS And COURSERS

Basics: "Network+", "Cisco – Networking Basics", "Security+", "CEH"
Linux: LPIC1, LPIC2, Networking with linux
DevOps: Docker (in progress)
SANS: 401, 450, 504
SOC Related and Blue Teaming: "THM – SOC Level 1", SOC-1
Splunk: Splunk Fundamentals 1, Splunk Using ES

SKILLS AND TECHNOLOGIES

Operating Systems: Windows, Ubuntu
Linux Administration: service management, permissions, user & group management, basic automation with Ansible
Networking & Services: DNS, FTP, web servers configuration and troubleshooting
Scripting and Programming: Bash, Python, C++ (basic)
Security & Monitoring: Splunk, Log analysis, Network traffic analysis, Sysmon investigation, MITRE ATT&CK mapping
Tools: Microsoft Office, ticketing Systems, virtual machines