Sina Ebrahimi

SOC Analyst

(+98) 9902616166
xsinaebrahimi@gmail.com linkedin.com/in/Sina-Ebrahimi github.com/sinae99

INTRO

Junior SOC Analyst with 1.5+ years of experience

EDUCATION

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

CERTS And COURSERS

Basic Knowledge: Network+, Cisco – "Networking Basics", Security+, THM – "Pre-Security"
Linux: LPIC 1, LPIC2 (in progress)
SANS: 401, 450, 504
SOC Related and Blue Teaming: Nooranet – "SOC 1", THM – "SOC Level 1"
Splunk: Splunk Fundamentals
Red Teaming: Nooranet – "CEH"
Certificates

EXPERIENCE

Company: Central Securities Depository of Iran www.csdiran.ir Apr 2023 - Present
Title: Security Operations Analyst (Tier 1)

- 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 (alongside university) 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 (alongside university)

- 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

SKILLS AND TECHNOLOGIES

Familiar with Microsoft Office, Ticketing System, Splunk, Virtual Machines, Windows, Ubuntu
Mini experience (AP course Level) in Python and CPP and bash
Familiar with Phishing e-mail Investigation, Analyzing Network Traffic and Sysmon Investigation
Understanding of core concepts in MITRE, CKC and basics of TI

ABOUT ME

Interested in finding anomalies, misconfiguration and suspicious behaviors in systems
I enjoy implementing security and hardening protocols to gain maximum protection
Simple & Fast Learner (ready to stand next to the pro people and "**learn**")

HALA MADRID