Mohammad Ghanbari
SOC and SPLUNK Architecture and Mentor

Tehran, Iran mghanbari777@gmail.com in/mghanbari7/

https://blog.soclib.net https://splunk-sizing.soclib.net English,Persion

SUMMARY

Over the years, I have built up a diverse set of skills, qualities, and experiences. I have experience designing, implementing, and managing SOC and Splunk, managing many varied tasks, working with security solutions and devices, collaborating with others as part of a team, and communicating positively with customers and clients. First, I was a programmer for four years; after that, I studied network and security and started working in the security field. I have been working and studying in SOC and Splunk for about eight years. I am cheerful and passionate and often make people around me happy. In my spare time, I like to engage in sports and video games, mainly soccer. **Currently, I am present as a Splunk consultant and instructor in various organizations and advise several different teams regarding the implementation, development, troubleshooting, and improvement of various Splunk tools such as ES, SOAR, and UBA.**

EXPERIENCE

Splunk SOAR Consultant
Dotis Arian Qeshm Co. (Dotin). April 2025 – Present
- Designed, implemented, and optimized Splunk SOAR playbooks
- Integrated multiple security tools
- Provided training and knowledge transfer sessions for SOC teams on SOAR playbooks, best practices, and troubleshooting

Splunk SOAR Consultant
Golgohar Sirjan Mining and Industrial Company May 2025 - Present
- Develop and Implement Specific Playbooks as service

Splunk lecture and Instructor
Noavaran Douran Institute 2020 - Present
- Instructing Splunk Courses: Fundamentals 1,2, System & Data Admin, Using and Admin Splunk ES, SOAR and UBA

SOC Consultant
TaraCell . Jan 2025 - Present

SOC and SPLUNK Consultant
ASA Co. June 2021 - Present
- Redesigning and Improving SOC Function and Capability according to SANS, NIST.
- Coaching and Mentoring Splunk administrator for maintaining troubleshooting, and redesigning architecture.
- Designing and implementing Incident Management Plans and Tools.
- Writing and Implementing security policy according to SANS, NIST, and CIS.
- Implementing and tuning Splunk ES (SIEM) and Phantom.
- Designing a New data model for implementing a new use case.
- Providing SOC KPI with executive reporting and dashboards.
- SOC planning, Hiring, and Training.
- Conducting Threat Modeling, use case life cycle, and Framework.
- Instructing Splunk Enterprise Courses such as Data and Sys Admin, ES Admin, and Using.

SOC Consultant
Ministry of Economic Affairs and Finance . September 2023 - Dec 2024

SPLUNK UBA Consultant
SITS Co (Mellat Bank) . September 2023 – Dec 2024
- Writing and developing technical design documentation for Implementing UBA
- Implemented Splunk UBA cluster
- Instructing Splunk UBA Course for two different teams
- Support and advise the team regarding management, troubleshooting and development

SPLUNK ES, UBA and SOAR Consultant and Mentor
Bandar Imam Petrochemical Company. September 2023 –March 2025

SOC and SPLUNK Consultant
AccTech Technology Kish. September 2022 – Apr 2024

• Assessing SOC maturity
• Develop SOC RoadMap
• Create SOC functions
• Designing, Implementing, tuning, and supporting Splunk as distributed with professional apps such as ES.
• Coaching and Mentoring Splunk administrator for maintaining troubleshooting, and redesigning architecture.

SOC and SPLUNK Consultant and Mentor
SAMAN Bank. **September 2021 - 2023**
• Designing, Implementing, Tunning, and supporting Splunk as distributed with professional apps such as ES, UBA, and Phantom,
• Coaching and Mentoring Splunk administrator for maintaining troubleshooting, and redesigning architecture.
• Instructing Splunk Enterprise Courses such as Data and Sys Admin, ES Admin, and Using
• Design Incident Management and SOC Framework

SOC Consultant
MELLAT Bank **April 2022 - October 2022**

SOC and SPLUNK Consultant and Mentor
SAVOLA(Behshahr) Group Co. **September 2021 - 2023**
• Designing, Implementing, Tunning, and supporting Splunk as distributed with professional apps such as ES, UBA, and Phantom,
• Coaching and Mentoring Splunk administrator for maintaining, troubleshooting, and redesigning architect.
• Teaching Splunk Enterprise Courses such as Data and Sys Admin, ES Admin, and Using
• Design Incident Management and SOC Framework
• Develop custom Reports and Use cases

Senior Security Engineer
SITS co (Mellat Bank) **June 2016 - April 2021**
• Assisting the Director with the design and implementation of the SOC program.
• Creating and tracking SOC metrics to continuously improve SOC efficiencies, processes, and procedures.
• Developing Content for SIEM such as Rules, Dashboards, Guide.
• Implementing SOC Maturity Model.
• Optimizing detection and response capabilities as a result of attack simulations and red teaming exercises.
• Proposing and conducting Cisco Firepower, SELKS, Suricata, Bro IDS, Osquery, and Sysmon Solutions to detect and prevent Cyberattacks.
• Updating, customizing, and optimizing over 300 SIEM's built-in use cases based on conditions and results.

Security Engineer
Pajand Electronics **March 2014 - June 2016**
• Configured and supported monitoring software including Zabbix, SolarWinds, Manage Engine, SCOM and SCCM
• Implementing VMware with FT, HA, and Clustering capabilities
• Planned network solutions based on Cisco safe
• Conducting and configure different types of Security Appliances such as FortiGate and Cisco ASA firewalls of over 20 appliances

PROJECTS

Published SOAR Fundamentals Podcast
https://www.youtube.com/m.ghanbari

SOC Lib
January 2021 – Present

• https://splunk-sizing.soclib.net/ (Splunk Sizing Tool)
• https://blog.soclib.net/
• https://www.soclib.ir

YouTube and Aparat:
https://www.youtube.com/m.ghanbari
https://www.aparat.com/m.ghanbari7

Published Threat Hunting book
August 2018 - June 2019

• https://mftbook.ir/product/476924

GitHub Threat Hunting Page
January 2020 - June 2021

• https://github.com/threat-hunting/awesome_Threat-Hunting

Published Article "Reducing Power Consumption based on load balancing in cloud networks using meta-heuristic algorithms."
January 2016 - January 2018

• https://civilica.com/doc/849061

LinkedIn Threat Hunting Page
January 2021 - Present

• https://www.linkedin.com/company/threathunting

EDUCATION

Master of Information Technology (Computer Networking)
Azad University • Garmsar • 2018

Bachelor of Computer Software Engineering.
Azad University • Tehran • 2014

CERTIFICATIONS

IELTS – Academic – 7.5
British Council • 2023 – ID: T54516958
Splunk Enterprise Security Certified Admin
Splunk • 2023
Credential: https://www.credly.com/badges/3126e252-010e-4e90-ada0-a04b9f16a5c2
Splunk Core Certified Power User
Splunk • 2022
Credential: https://www.credly.com/badges/676bd84e-210b-47d6-b5a8-5f6067b8f958
CTIA
EC-Council • 2019
Credential: https://aspen.eccouncil.org/VerifyBadge?type=training&a=lfWbK7Tunjmimux2u5qlQg==
MCITP
Microsoft • 2013
Credential: https://www.credly.com/badges/6106f6de-b21a-43e4-97a7-02bb1ec96f5d
Autopsy
Basis Technology • 2019
Cyber Threat Hunting and Active Defense & Cyber Deception
Active Countermeasures • 2019
NSE 1 and 2 Network Security Associate
Fortinet • 2020
SANS SEC 503 and SEC 511
Carrier Digit (Iranian's security education institute) • 2018
CEH and SANS SEC 504
Carrier Digit (Iranian's security education institute) • 2017
LPIC1 and LPIC2
Laitec (Iranian's IT education institute) • 2016

COURSEWORK

SANS SEC 450 and SEC 551
Self-Study • 2022
Splunk Cluster Administration and Architecting Splunk Enterprise Deployments
Self-Study • 2022
Splunk Phantom Administration and UBA Implementation
Self-Study • 2021
Using and Administering Splunk Enterprise Security
Self-Study • 2020
Splunk Fund 1, Fund 2, System and Data admin
Self-Study • 2018
SANS SEC 560 and SEC 542
Self-Study • 2017
SANS SEC 503 and SEC 511
Self-Study • 2017

SKILLS

Leadership, Team Management, Team working, Timely Communication, Presentation, Creativity, Decision makingSOC Architecture, SIEM Engineering (content development, data, and system tuning), SPLUNK Architecture (ES, phantom), Security Incident Response, Firewall/IDS/IPS Skills, NSM and CSM, Python, Docker