Mohammad Hossein Sokhanfar

Senior Security & Networl Engineer
B.Eng. (Information Techonolgy)
Iran, Tehran
Male, 28, single
Mobile: +98-938-9899755
Email: mhusokhanfar@gmail.com

Education

Computer Systems Information Techonolgy (B.Sc.)
Karaj Branch of Azad University, 2015 - 2019

About

I have an information technology engineer degree with 3 years of official work experience and 5 years of project-oriented experience (totally 7 years of experience) in the field of design implementation, and security based on established standards and project implementation.

I have computer network management and relevant qualifications.

Management of the SOC department, I have relevant international qualifications and I am currently working in this Field.

In general, I consider myself a researcher, flexible, dynamic, hardworking and looking for effective and committed ways

Career History

Details	Organization	Position
Teaching more than 500 hours of Cisco, Microsoft and security courses	CanDo training center	Teacher
• Management of the distribution layer and configuration of Cisco devices • Implementation of SPAN (Port Monitoring) for monitoring • Optimization Layer 2 and Switch Block • BGP & DMVPN Implementation Working with HP ProLiant server and setting up required services • Solving network and server problems • Microsoft Network Support • Virtualization Base on VMware solutions • Management of the technical team (Helpdesk) to handle user tickets and solve problems	Namvaran Consulting Engineers Managers	Administration & Helpdesk Supervisor

• Microsoft Network Support • Virtualization Base on VMware solutions • Fortinet FortiGate :70F,100D,30F • PALO ALTO: PA-5060 • bandwidth management solutions • ORACLE AVDF (Database FW) • Redesign Network Infrastructures & Tuning for Clients Project manager and security consultant • Iranian Privatization Organization • Prisons and Security and Corrective Measures Organization • Asiatech	REMIS	Senior Network Engineer, Senior Security Engineer
• Redesign Network Infrastructures Base on latest Technology • Implementing Security Services Like (Zeek, snort, Splunk, Sysmon, …) • Implementing APN • Infrastructures And Security Appliance Automation • Tunning Security Appliances • Automation Incident Management (AIM) • System Hardening and Availability • Network Request Automation • Design UPD Flood Attack Detection • MPLS & VPN Infrastructure • SOC VA/Forensic • F5 ASM&LTM&DNS admin T-shoot	Behsazan Mellat	Senior Network Engineer, Senior Security Engineer

Teaching records	
Course	**Institute/ Organization**
CCNA 200-301 MCSE CSCU	CanDo Training Center
SANS Sec 504 SANS Sec 511	State Welfare Organization of Iran
Security+ SANS Sec 401 SANS Sec 504	Administrative and employment organization of the country

Certificates	No.
CCIE Enterprise Infrastructure	1
CCNA Routing & Switching / CCNA 200-301	2
CCNP ENCOR 350-401	3
CCNP ENARSI 300-410	4
CCNA Security	5
Kerio	6
Fortinet NSE 4,5,6,7	7
MCSE	8
CEH & PWK V12	9
VMWare ICM&OMPIMIZE, VDI	10
VoIP (Elastix – Issabel)	11
MTCNA	12
MTCTCE	13
MTCRE	14
MTCWE	15
MTCUME	16
MTCSE	17
MTCEWE	18
GIAC Certified incident handler (SANS Sec504)	19
SANS 450	20
SANS 503	21
SANS 511	22
GIAC Certified Detection Analyst (SANS Sec555)	23
GIAC Certified Forensic Analyst (SANS For508)	23
GIAC Certified Forensic Examiner (SANS For500)	24
GIAC Network Forensic Analyst (SANS For572)	25
GIAC Exploit Researcher and Advanced Penetration Tester (SANS Sec660)	26
PEN 100	27
PEN 200	28
WEB 100	29
SPLUNK	30
LPIC 1 & LPIC 2	31
HPE ATP Hybrid Solutions Certified	32
Zabbix	33
Try To Hack Me SOC 1 & 2 Certificated	34
Python Scripting	35
Automation	36

Network Skills	No.
Mastery of layer 2 mechanisms: Ether Channel, HSRP, MST, Private VLAN, VlANing, inter VLAN Routing, STP. RSTP. PVST	1
Mastery of layer 3 mechanisms: RIP, OSPF, EIGRP, Route Map, BGP, Route summarization, OSPF Route, Redistribution Policy Based Routing – IS-IS	2
Implementation of Cisco technologies: Aggregating switch links, STP securing and configuration, multilayer switching, enterprise campus network design, VXLAN, L3 HA(HSRP,VRRP,GLBP), IP telephony, integrating wireless LAN's, securing switch access, NAT, EIGRP, OSPF, IGP, policy base routing, IP service level agreement, BGP, branch office networking, ACL, AAA, CME, CUCM, IOS firewall security, IPSEC tunneling, QOS, Route map, Route summarization, Route redistribution, WCCP, CEF, MST, SPAN, port security, IPV4, IPV6, Multicasting…	3
Mastery of network security solutions: Layer 2 Security (Port Security, Dot1x, VLAN Access map), Layer 3 Security (IP ACL, Context-based Access Control), VPN (IPSec, Site to site VPN) Device Hardening	4
Familiarity with network firewalls such as Fortigate ،Cisco ،Juniper, Sophos	6
Advice on cases: Network security, network platform implementation, VOIP implementation, design and implementation of server room and data center	7
Familiar with data center concepts such as VXLAN, LISP	10
Familiar with MPLS protocol	11
Experience working with Cisco switching equipment, for example 4500, 6500, 9200, 9300, 9400, 3850 and 3650, 3750, 2960 and 2950Nexus Switches	13
Experience working with Cisco Routing equipment, for example Cisco 7600 Series and ASR 1000 Series	14
Proficient in IPv6 topics	18
Proficient in Mikrotik and setting up routing services	19
Proficient ITIL	20
Virtualization VMware, VDI	21
Implementation and management of network antiviruses	22
Implementation of various services under Windows Server AD, DNS, DHCP, IIS, FTP, NAT, VPN, WSUS, WDS, HYPER-V, IPSEC	23
Familiar with HP servers	24
Implementation all Type of VPN types	25
Linux Administration	26
PAM WALLIX	27
F5 LTM & ASM	30

Security Skills	No.
Penetration Testing & Vulnerability Management: • Advanced penetration testing and ethical hacking using tools like Kali Linux, Metasploit, Burp Suite • Vulnerability assessment and risk remediation aligned with ISO 27001, NIST, SOC 2, and GDPR standards	1
Incident Response & Digital Forensics: Experience with SIEM tool (Splunk) and digital forensic techniques	2
Identity & Access Management (IAM): Expertise in SSO, MFA, Active Directory security	3
Threat Intelligence & Malware Analysis: Competent in threat hunting, OSINT, and using YARA rules for malware analysis	4
Secure Coding & Application Security: Familiar with OWASP standards, secure development practices, SAST/DAST	6
Cryptography & Encryption: Knowledge of TLS/SSL, PKI, and encryption algorithms	7
SIEM & Log Analysis: Skilled in analyzing logs with Splunk	8
Risk Management & Compliance: Understanding of ISO 27001, NIST frameworks, SOC 2, and GDPR requirements	9
Soft Skills: Critical thinking, problem solving, effective communication, and team	10
Leadership, Strategic Consulting & Continuous Improvement • **SOC & Incident Command Leadership:** Management of SOC operations, cross-functional team coordination during security incidents, and leadership in forensic investigations • **Risk Management & Compliance:** • Strategic risk assessment, policy development, and implementation of compliance frameworks • **Effective Communication & Mentorship:** • Proven ability to translate complex technical concepts to both technical and non-technical stakeholders • Experience in training and mentoring teams to foster continuous improvement and innovation	11

Languages

- Persian (First language)
- English (Professional Working)

I invite you to visit my Website
Please open the link below

WEBSITE