Seyed Matin Mahmoudi

Threat Hunting | Detection Engineering | Security Research

Email: seyedmatinmahmoudi@gmail.com | **Education:** B.Sc. Computer Engineering
Marital Status: Married | **Military Service Status:** Educational Exemption | LinkedIn Profile

CERTIFICATES

- CompTIA Network+
- CompTIA Security+
- Cisco Certified Network Associate - Routing & Switching
- Microsoft Certified Solutions Expert: Core Infrastructure
- Microsoft Exchange Server 2016
- Microsoft System Center: Operations Manager
- Microsoft System Center: Configuration Manager
- AZ-900: Microsoft Azure Fundamentals
- Mikrotik Certified Network Associate (MTCNA)
- Mikrotik Certified Routing Engineer (MTCRE)
- Mikrotik Certified Wireless Engineer (MTCWE)
- Mikrotik Certified User Management Engineer (MTCUME)
- Certified Linux Administrator (LPIC-1)
- Certified Ethical Hacker (CEH)
- PWK (Penetration Testing with Kali Linux)
- SANS FOR500 - Windows Forensics
- Splunk Fundamentals
- MCSA: Windows Server 2012 - Microsoft (ID: H188-3023)
- MCSA: Windows Server 2016 - Microsoft (ID: H188-3259)
- MCSE: Core Infrastructure - Microsoft (ID: H188-3213)
- Active Directory Red Team (AD-RTS) - Cyber Warfare Labs

SKILLS

Security Operations, Detection Engineering & Threat Monitoring:

Security Monitoring & Alert Triage • SIEM Engineering & Administration (Splunk, Elastic Stack) • Detection Use Case Development & Tuning • MITRE ATT&CK-aligned Detection & Coverage Mapping • Network Security Monitoring (Zeek, Stream, Suricata, Snort, Arkime, Wireshark) • Endpoint Telemetry Analysis (Sysmon, Windows Event Logs, Auditd) • Threat Hunting (THOR, Loki, Chainsaw) • Threat Intelligence Operations (MISP, OpenCTI) • Security Hardening based on CIS Benchmarks

Incident Response & Digital Forensic:

Evidence Acquisition & Preservation • Disk & File System Forensics (FTK Imager, Arsenal Image Mounter) • Memory Forensics (WinPmem, Volatility, KAPE) • Windows Registry Forensics • Email & Phishing Investigations • Network Forensics

Purple Teaming & Adversary Emulation:

Purple Team Operations • Atomic & Scenario-Based Attack Simulation • Adversary Emulation (Atomic Red Team, MITRE CALDERA) • C2 Operations (Cobalt Strike) • Web Application Security Testing (Burp Suite) • Vulnerability Assessment

Security Automation:

SOAR Development & Playbook Engineering (Splunk SOAR) • PowerShell Automation & Tooling • Bash Scripting • Custom Security Utilities & Integrations

Windows Infrastructure & Enterprise Services:

Active Directory Services (AD DS, AD CS, AD LDS) • Group Policy & Security Baselines • DNS, DHCP, IIS, DFS, RRAS, NPS, WSUS, WDS, File & Print Services, FSRM, NLB & Failover Clustering • Microsoft Exchange Administration & Hardening • System Center (SCOM, SCCM/MECM)

Linux Administration:

System Logging & Troubleshooting • Linux Access Control Models (DAC, MAC) • Access Control Lists (ACLs) • SELinux Administration & Policy Concepts • Auditd Configuration & Analysis

Virtualization, Containers & Platform Security:

VMware vSphere • Docker • Kubernetes • Container Runtime Security (Falco)

Networking & Identity Security:

Network Architecture & Segmentation • Routing & Switching (L2/L3) • Network Access Control (Cisco ISE & TrustSec) • Identity & Access Management (IAM) • Privileged Access Management (PAM) • Least-Privilege Access Concepts (RBAC, JIT)

Cloud:

Microsoft Azure Fundamentals • Azure Identity & Access Concepts

WORK EXPERIENCE

SOC Technical Lead *Sadad Informatics Corporation* Oct 2026 – Present | *Full-Time | On-Site*

Network & Cybersecurity Instructor *Douran Academy* Nov 2022 – Present | *Part-Time | Hybrid*

Network & Cybersecurity Instructor *Ravin Academy* Sep 2026 – Present | *Part-Time | Hybrid*

SOC Governance & Operations Specialist *Spara Security Group* Sep 2025 – Sep 2026 | *Full-Time | On-Site*

Microsoft Enterprise Services Consultant *Secure Data Network (SDN)* Feb 2023 – Sep 2025 | *Part-Time | Remote*

Education Director *APK Group (Amn Pardazan Kavir)* May 2024 – Jan 2025 | *Full-Time | On-Site*

Network & Cybersecurity Instructor *Sematec* Sep 2023 – Aug 2024 | *Part-Time | Hybrid*

Network & Cybersecurity Instructor *Cando Academy* Dec 2021 – Nov 2023 | *Part-Time | Hybrid*

IP Backbone Engineer *Respina Networks & Beyond* Nov 2021 – Jan 2023 | *Full-Time | On-Site*

Network Operations Center Specialist *Respina Networks & Beyond* Aug 2020 – Nov 2021 | *Full-Time | On-Site*

Senior SOC Analyst (Tier 2) *APK Group (Amn Pardazan Kavir)* Aug 2021 – Jul 2022 | *Full-Time | On-Site*

Technical Support Specialist *Shatel* Jun 2019 – Aug 2020 | *Full-Time | On-Site*

PROJECTS

National Artificial Intelligence Organization *(Sep 2024)*

Assembled and configured an HPE DL380 G10+ server, Fortigate G-Series firewall, and Cisco Catalyst 9200/9500 switches; organized rack infrastructure and deployed a VMware vSphere environment including vCenter, VCHA and VMCA configuration. Deployed core Active Directory services (AD DS, AD CS), DHCP with policy-based IP assignment, DNS, a file server (DFSR & FSRM), Microsoft LAPS, AD Self-Service and an NTP server. Deployed Splunk as a single-instance log collector, Zabbix for network monitoring, and a hardened Exchange Server 2019 mail platform (DAG configuration, anti-spam tuning, and edge transport/mailbox server hardening covering banner-grabbing protection, autodiscover hardening, ECP restriction, IIS hardening, MSA usage, GAL hardening, connection tuning and fake-mail restriction). Implemented 802.1X network access control via multi-node Cisco ISE with TACACS, identity-based access and posture assessment, plus a UniFi WLAN infrastructure with dynamic VLAN assignment and ISE captive-portal redirection through a DNS sinkhole. Delivered a VoIP infrastructure based on Issabel IP PBX.

Islamic Propagation Organization *(Aug 2024)*

Configured IP SLA-based WAN link redundancy (check gateway, scope and target scope), VRF and policy-based routing via Mangle, and CAPsMAN with access-point meshing. Implemented Zero-Trust network segmentation with isolated camera traffic, DNS filtering with traffic redirected to the organization's name server, traffic shaping with advanced queue configuration, and SwitchOS/RouterOS hardening.

Barez Industrial Group *(Mar 2022)*

Migrated Microsoft Exchange to Exchange Server 2019 with DAG configuration and a proxy server for OWA; tuned the anti-spam module and hardened edge transport and mailbox servers (banner-grabbing protection, autodiscover hardening, ECP restriction, IIS hardening, MSA usage, GAL hardening, connection tuning and fake-mail restriction).

Enjemad System *(May 2021)*

Configured IP SLA-based WAN link redundancy and policy-based routing via Mangle; implemented an SSO-enabled remote access solution and centrally managed site-to-site tunneling; ran dynamic routing for remote network routes; configured DNS filtering with traffic redirected to the organization's name server.

TEACHING EXPERIENCE

CompTIA	Microsoft	Mikrotik	EC-Council	SANS
A+	MCSE Windows Server	MTCNA	CSCU	SEC 301
Network+	Exchange Server	MTCRE	CEH	SEC 401
Security+	SCCM (MECM)	MTCWE		SEC 450
Cloud+	AZ-900	MTCUME		SEC 503
		MTCTCE		SEC 504
				SEC 511
				SEC 555
				FOR 500
				FOR 508

Over 5,000 hours of teaching experience delivered at Cando Academy, Douran Academy, Sematec, RashaTech and Ravin Academy.

Courses Delivered for the Following Organizations:

- The Student Basij Organization
- Shazand Petrochemical Company
- Ports and Maritime Organization of Iran
- National Organization for Civil Registration
- Telecommunication Infrastructure Company
- The Islamic Republic of Iran Customs Administration
- Iran Ministry of Roads & Urban Development
- National Iranian Gas Company
- National Iranian Oil Company
- Yazd Regional Electrical Company
- Iranian National Tax Administration
- Judicial System of the Islamic Republic of Iran
- Iran Khodro Company
- Ministry of Defence and Armed Forces Logistics