Alireza Rahmani

Tehran • Iran

EDUCATION

BS Computer Software Engineering
IAU-Tehran North Branch
Ms in IT
IAU-Pardis Branch

Summary

Cyber Security Operation Center :

- Centralized log management and analysis using Both Open Sourceand Commercial solutions, High scale Log collection methods using Message TransportProtocols.
- Incident Handling, Incident response platforms, automatingevidence analysis, SOC incident handling Workflow…
- Network Forensics systems (full packet capture).
- Intrusion detection/Prevention systems, vulnerability managementsystems, host integrity monitoring.
- Windows system activity monitoring.
- Flow Monitoring systems.
- Attack Techniques, Tactics and Procedures.
- Network Traffic Analysis.Cyber Security Concepts:Familiar with Information security Concepts
- Network security

Specialties

Network Security skills:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography
- Cisco Firewall and intrusion detection systems (FWSM, IDSM-2, IPS)
- Juniper networks security appliances (SRX Branch/Service Gateway series, IDP series).JUNOS operating system.
- Layer 3 security (IP ACL, RPF Checks, TCP Intercept, Context-based Access Control,…)

- OSPF,EIGRP,BGP,IS-IS, VPLS,MPLS,EIGRP-OTP
- IoT,Clouds
- 6+ years of extensive knowledge working with major firewalls including Juniper,Cisco and fortigate.

Familiar with Network security Design and implementation:

- Security Operation Center Design.
- Server and Device Hardening.
- Layer 2 Security (Port Security, Dynamic ARP Inspection, DHCP Snooping, IP source Guard,Dot1x,Storm Control)
- Linux system security.
- Lawful interception on IP traffic.
- Windows Security: Securing Active Directory and DNS, PKI, EFS , IPSec, NPS, VPN, IIS.
- Network Intrusion detection & Prevention services (Snort, Suricata, Bro,...).
- Host Intrusion Detection Systems.
- Security Event and Information managements.
- Network traffic analysis and forensics.

EXPERIENCE

Current:

President office Network Security Engineer & SOC Staff (Since 1394)

Past:

Parsonline NOC (1392-1392)

Fanavacard Network specialist (1392-1394)

Cloud computing bootcamp Instructor

TEM,MFT Branch