Vinod More

Mumbai, Maharashtra | vinodm41@gmail.com | +91-9892086544 | Linkedin.com/in/vinodm41 | https://vinodmore.info

Profile Summary:
Cyber Security professional with 7+ years skilled in Incident Response, Threat Hunting, Security Operations, Security Engineering and Red Teaming.

Cyber Security Skills:
- Experienced in handling the full lifecycle of incident response, including triage, investigation, containment, remediation, and recovery from cybersecurity incidents.
- Threat hunting leveraging EDR, XDR, Proxy, SIEM, and other open source and commercial tools.
- Create threat hunting queries, hypothesis driven threat hunts and Structured and Unstructured hunting.
- Hands on EDR tools, Crowd Strike Falcon, Trend Micro Deep Security, and Windows Defender Advanced Threat Protection.
- Understanding of Red Teaming and Breach Attack Simulation, Adversarial Tactics, Techniques and Defence Evasion.
- Understanding of Malware analysis and reverse engineering with tools and sandbox.
- Holistic understanding of the cyber threat landscape, vulnerabilities, and mitigation strategies, aligned with industry best practices.
- Knowledge of Pentest and Offensive tools like Reconnaissance and OSINT, Vulnerability Scanning, Exploitation Frameworks, Web Application Testing, Password Cracking, Wireless Testing, Network Scanning and Enumeration, Post-Exploitation, Social Engineering, Container and Cloud Security, Reverse Engineering, Phishing and Credential Harvesting, Malware Analysis and Evasion.
- Automation, scripting (Python & PowerShell), and leverage tools and technologies to improve efficiency.
- Knowledge of Cloud Security and Cloud infrastructure on AWS and Azure cloud platform.
- Understanding of Mitre ATT&CK and D3FEND frameworks, risk, impact, mitigation, threat & CVSS scoring system.
- Knowledge of Firewalls, UTMs, WAF, Routers, Switches, Network infrastructure and Cloud infrastructure.

Cyber Security Experience:
- Core IT Services, Senior Cyber Security Analyst, Duration: Nov 2022 – till date

Respond to Cyber Security Incidents to tirage, investigate, contain, remediate, and recover from cyber security incidents.
Threat hunt for security threats by leveraging EDR, XDR, SIEM, and other security platforms and commercial tools.
Sandboxing of software and tools. Static Malware analysis and simulation

- Mphasis Limited, Security Engineer, Duration: Jan 2020 – Nov 2022

Incident response to triage the incident and mitigate it. Create proactive cyber defence with threat hunting and threat analysis to identify and patch vulnerabilities in the infrastructure, prevent data and security breaches.

- Qualys Security Tech Services Pvt Ltd, Security Analyst, Duration: Jan 2019 – Dec 2019

Create security controls for secure configuration of Operating Systems, Databases, Applications, Services, Network Services, and Network devices based on CIS & DISA or vendor-described secure configuration guidelines for Qualys Guard Policy compliance module.

- Sequretek IT Solutions Pvt Ltd, Security Analyst, Duration: Jan 2018 – Jan 2019

Security monitoring of Servers, Networks, and Services to mitigate any security incident. Monitoring, reporting, hardening, security audit, vulnerability assessment, and penetration testing of systems Linux, Windows systems, and Network infrastructure.

Cyber Security Certifications/Training:
- Certified Cyber Threat Intelligence Analyst (CTIA), certification from EC-Council (ECC7950346821)
- Certified Ethical Hacker version 9 (CEH), certification from EC-Council (ECC74143996924)
- Red Teaming, training and certification from TryHackMe (THM-92AIYYGM42)
- CompTIA Certified Penetration Tester (PenTest+), training and certification from LinkedIn Learning
- CompTIA Cybersecurity Analyst (CySA+), training and certification from LinkedIn Learning
- Learning Cyber Incident Response and Digital Forensics - training and certification from LinkedIn Learning
- Azure Sentinel Training Course - Cloud Native SIEM in Cloud training and certification from Udemy

Cloud, System and Network Skills:

- Hands-on in installation, configuration, troubleshooting, maintenance, and hardening of Linux-based server systems
- Administration of Windows environment services like Active Directory Domain, Group Policies, DNS Management, DHCP Scope, Web Services, and Remote Desktop
- Administering Azure & AWS cloud infrastructure and services.
- Working knowledge of Docker and container management technologies
- Network packet analysis with packet analysis tools like Wireshark, Tshark, and TCPDump.
- Understanding of Bash scripts, PowerShell scripts, and Python scripts.
- Knowledge of protocols like TCP, UDP, DNS, DHCP, FTP, SNMP, SMTP, SSH, SSL, RDP, and HTTP working and features.
- Installation and configuration of services SSH, LDAP, DNS, DHCP, NFS, Samba, HTTP, Proxy, FTP server.
- Knowledge of IPsec, NAT, PAT, VPN, IPS/IDS, Proxy, Load Balancers, VLAN,
- Basic scripting knowledge in Linus bash, shell scripting, and PowerShell command line and modules
- Understanding of Switches/Firewalls/UTM/Routers configuration and settings

Systems Administration Experience:

- Lyra Network Private Ltd as Linux System Analyst, Duration: Mar 2017 – Jan 2018
- Trimax IT Infrastructure & Services Limited as Systems Engineer, Duration: July 2015 – Oct 2016
- Taj Television India Pvt Ltd as Systems Administrator, Duration: Oct 2007 – Aug 2014
- Orient Technologies Pvt Ltd, Technical Support Engineer, Duration: Nov 2004 – Oct 2007
- Allied Digital Services Pvt Ltd, Technical Support Engineer, Duration: Feb 2002 – Nov 2004

Cloud and Systems Certifications/Trainings:

- Microsoft Azure Fundamentals Certification AZ-900, from LinkedIn Learning
- Microsoft Azure Administrator Associate AZ-104, from LinkedIn Learning
- Microsoft Azure Security Engineer Associate AZ-500, from LinkedIn Learning
- AWS Certified Solutions Architect - Associate 2019, from Udemy
- Completed Red Hat Enterprise Linux 7 RHCE, RHCSA training.
- Advanced Diploma in Computer Hardware & Networking from Jetking School of Electronic Technology

---

Personal Information:

Date of Birth:	3rd December 1979
Gender:	Male
Marital Status:	Married
Nationality:	Indian
Mobile No:	+91-9892086544
Mail Id:	vinodm41@gmail.com
Passport No:	W8335414, Expiry 16/12/2032
PAN:	APPPM9280E
LinkedIn:	https://www.linkedin.com/in/vinodm41/
Github:	https://github.com/vinodm41

Certifications/Trainings:
https://vinodmore.info/certs.htm

Website/Portfolio:
https://vinodmore.info