Vinod More

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

# Summary:
Cybersecurity professional with over 7 years of experience in Security Operations, specializing in roles such as Security Analyst, Threat Hunter, Threat Intelligence Analyst, Incident Responder, and Cloud Security Analyst. Mission is to enhance organizational cyber defence and resilience by implementing a robust security stack, proactively identifying, mitigating, and recovering from advanced cyber threats.

# Cyber Security Skills:
- Cybersecurity Incident response to tirage, investigate, contain, remediate, and recover from cyber security incidents or alerts.
- Skilled in the end-to-end threat hunting lifecycle, including hypothesis generation, advanced query development (using KQL, SPL, CQL, LQL), and executing data-driven hunts across SIEM and EDR platforms. Experienced in both structured (intelligence-led) and unstructured (exploratory) methodologies.
- Hands-on expertise with EDR and XDR solutions such as CrowdStrike Falcon, Sentinel One, and Microsoft Defender for Endpoint.
- Leveraged Threat intelligence, for collection, analysis, and reporting of actionable threat intelligence data. Worked with platforms like MISP, OpenCTI, and FortiRecon to gather critical information on adversary TTPs, active vulnerabilities, attack paths, and potential attack vectors for proactive threat mitigation.
- Knowledge of Cloud Security principles and technologies, with hands-on experience securing infrastructure and workloads on AWS and Microsoft Azure, including identity and access management (IAM), logging and monitoring, cloud-native security controls, and container security.
- Familiar of Red Teaming activity, Breach and Attack Simulation (BAS), and adversarial tactics, techniques, and defence evasion strategies.
- Familiar with malware analysis and reverse engineering using dynamic and static analysis tools and sandbox environments.
- In-depth understanding of the cyber threat landscape, emerging vulnerabilities, and mitigation techniques aligned with industry frameworks and best practices.
- Proficient in automation and scripting using Python and PowerShell to streamline investigation, response, and operational workflows.
- Familiarity with the MITRE ATT&CK and D3FEND frameworks, risk assessment methodologies, impact analysis, mitigation planning, and CVSS-based threat scoring.
- Foundational understanding of API security, including authentication, authorization, rate limiting, and abuse detection.
- Knowledge of IT and security infrastructure Router, Switch, Firewall, NGFW, WAF, Load Balancer, VPN Gateway, Proxy Server, IPS/IDS.

# Cyber Security Experience:
- Edelweiss Financial Services Ltd, Senior Manager (Cyber Defence), From: 3 March 2025 – till date
Lead and execute cybersecurity incident response, threat hunting, and threat detection initiatives across a wide range of tools, technologies, and security platforms, ensuring comprehensive threat coverage and rapid mitigation within complex enterprise environments. Enhance organizational cyber defence and resilience by implementing a robust security stack, proactively identifying, mitigating, and recovering from advanced threats across the enterprise landscape.

- Core IT Services Pvt Ltd, Senior Cyber Security Analyst, (Client: Edelweiss Financial Services Ltd) From: 21 Nov 2022 – 28 Feb 2025
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, From: 07 Jan 2020 – 19 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, From: 16 Jan 2019 – 3 Jan 2020
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, From: 22 Jan 2018 – 11 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 &Trainings:
- 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
- Azure Sentinel Training Course - Cloud Native SIEM in Cloud training and certification from Udemy

# Cloud & Systems Infrastructure 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.
- 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, From: 20 Mar 2017 – 17 Jan 2018
- OS3 Infotech Pvt Ltd as Linux System Analyst, From: 1 Nov 2016 to 28 February 2017
- Trimax IT Infrastructure & Services Limited as Systems Engineer, From: 1 July 2015 – 27 Oct 2016

# 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

#Education Qualification:
- SSC (Mumbai University) passed in March 1995 securing 55%
- Advanced Diploma in Computer Hardware & Networking from Jetking School of Electronic Technology form Aug-1999 to Jan 2001 securing Grade A

# Personal Information:

Date of Birth:	3rd December 1979
Gender:	Male
Marital Status:	Married
Nationality:	Indian
Mobile No:	+91-9892086544
Mail Id:	vinodm41@gmail.com
LinkedIn:	https://www.linkedin.com/in/vinodm41
Twitter:	https://x.com/vinodm41

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

# Website/Portfolio:
https://vinodmore.info