

Vinay Maithani

✉ mvnay08@gmail.com [🌐 linkedin.com/in/vinay-maithani](https://www.linkedin.com/in/vinay-maithani) [📄 credly.com/users/v_cyber_dude](https://www.credly.com/users/v_cyber_dude)

SUMMARY

Information Security Analyst with proficient and thorough experience and a good understanding of information technology. Specialized in proactive network monitoring of SIEM (Azure Sentinel) and relevant Microsoft security tools and solutions. Have a deep knowledge in identifying and analyzing suspicious event. Versatile, bilingual professional and ability to manage sensitive materials. Able to use various security tools to perform logs and packet analysis. Finally, can perform malware root cause analysis with the overall objective to ensure confidentiality, integrity and availability of the systems, networks, and data.

EXPERIENCE

SEQUIRETEK (Associate-Consultant)

April 2022 - Present, Gurugram, Haryana, India · On-site

In my role as an Associate Consultant specializing in SOC and Incident Response, I gained hands-on experience with a range of Microsoft security tools. I also utilized Percept XDR from Sequestek and ArcSight ESM for raw log analysis. Additionally, I leveraged Microsoft Azure Active Directory to correlate user details with alerts and incidents and used MS Sentinel to enhance my analysis and response capabilities.

- Security Operation Center Analyst for a World-renowned confectionery named Perfetti Van Melle.
- CSIR (Incident Responder) for GreyOrange P.

CSIR (Incident Responder)

Client- 02(via Sequestek)

January 2023 - Present, Gurugram, Haryana, India · On-site

Computer Security Incident Responder | Incident Response and Cybersecurity Specialist

Experienced Computer Security Incident Responder with a strong background in incident response and cybersecurity. Expertise in identifying, analyzing, and mitigating security incidents to protect organizations against cyber threats. Skilled in coordinating and leading incident response efforts, developing incident response plans, and implementing effective security controls. Adept at utilizing cutting-edge tools and technologies to investigate and remediate security incidents while maintaining the integrity and confidentiality of sensitive data. Committed to staying up-to-date with the latest cybersecurity trends and best practices to ensure optimal protection for organizations.

Security Operations Center Analyst

Client- 01(via Sequestek)

June 2022 - January 2023, Manesar, Haryana, India · On-site

Security Operations Center (SOC) Analyst at Perfetti Van Melle, appointed by Sequestek IT Solutions, I was responsible for supporting a 24/7 global SOC. My role involved triaging event logs, managing and responding to security incidents, and providing necessary remediations in accordance with SOPs and SOC recommendations. I also generated detailed incident reports and ensured all actions were aligned with company standards. Additionally, I utilized Microsoft technologies, including MS Defender XDR, MS Defender for Cloud, MS Defender for Endpoint, MS Defender for O365, MS Defender for identity, MS Defender for Cloud Apps and Microsoft Azure, along with some usage of MS Sentinel to bolster and maintain the organization's security posture.

Software Quality Assurance Analyst

Acwits Solution LLP

July 2018 - March 2022, Delhi, India

Website and Mobile Application Tester (Android).

As a Website and Mobile Application Tester (Android), I ensured the seamless functionality and security of web and mobile platforms. I tested website features to confirm their flawless operation, identified and tracked bugs using Jira and Zoho, and performed web vulnerability assessments with ZAP Proxy. For

Android applications, I employed Astra Pentest App to detect and address security weaknesses, enhancing app robustness. My role was dedicated to delivering high-quality digital experiences and utilizing advanced testing tools to protect against vulnerabilities.

EDUCATION

Master of Science - MS (I.T), Information Technology

Amity University • 2021 • 83%

Bachelor of Science - BS (I.T), Information Technology

Omkara Nanda Institute of Management & Technology • 2018 • 75%

SKILLS

Industry Knowledge: Malware Analysis, Reconnaissance, Open-Source Intelligence, OSI Model, Data Security, Cyber Threat Intelligence (CTI), Security Information and Event Management (SIEM), DLP, Security Operations, Information Security Management, Cloud Security, Application Security, Microsoft 365 Security Products, Triage, Incident Handling, Incident Analysis, Incident Reporting, Threat Analysis, Threat Detection, Proactive Monitoring

Tools & Technologies: MS Defender XDR, MS Defender for Cloud, MS Defender for Endpoint, MS Defender for O365, MS Defender for identity, MS Defender for Cloud Apps and Microsoft Azure Active Directory, ArcSight Logger, Sequestek Percept XDR, HTML, Cascading Style Sheets (CSS), C, Linux, Java, SQL

Languages: Hindi, English

Certifications

Certificate of Recognition from Gurugram Police for Cyber Security Summer Internship.

Countering Ransomware with MITRE ATT&CK (AttackIQ)

Foundations of Operationalizing

MITRE ATT&CK Certificate (AttackIQ)

Foundations of Purple Teaming Certificate (AttackIQ)

Certificate of Completion for Ethical Hacking training (Internshala)

Cyber Security Foundation – CSFPC from (CertiProf)

Introduction to Ethical Hacking. (Udemy)

Ethical Hacking with Hardware Gadgets. (Udemy)

Stay anonymous with privacy tools. (Udemy)

Organizing a Gaming Competition & Winning the Gaming Competition of CSGO.