Trishul singh *Deputy Manager*

trishulsingh01@gmail.com
+91-9140275880
Bengaluru, Karnataka
www.LinkedIn.com/in/trishulsingh

Profile

- Cybersecurity professional with 6+ years of experience specializing in Malware Analysis, Threat Research, and Incident Response across MDR domains. Expertise in reverse engineering, static/dynamic malware analysis, and developing custom detection mechanisms to counter advanced cyber threats.
- Played a key role in advanced threat detection, response, and mitigation strategies. Strong background in Root Cause Analysis (RCA), impact assessments, and proactive defense strategies to enhance organizational security.
- Expert in Microsoft XDR, SIEM, EDR, and malware research, with hands-on experience in exploit analysis, building automated security tools, and fine-tuning preventive security rules. Developed malware playbooks, automated detection mechanisms, and security frameworks to strengthen cybersecurity resilience.
- Recognized for problem-solving skills, leading malware research, developing custom security tools, and uncovering novel attack techniques. Adept at working in fast-paced security environments, collaborating with cross-functional teams, and delivering actionable insights to mitigate sophisticated cyber threats.

Professional Experience

Deloitte India

Deputy manager 2024/07 – present | Bengaluru, India

- Pioneered the MDR practice, collaborating with leadership to establish advanced threat detection and response capabilities.
- Investigated complex malware threats using XDR, ensuring 100% RCA and impact assessment coverage by leveraging all available logs and telemetry.
- Developed and fine-tuned preventive security rules to enhance detection, response, and mitigation strategies.
- Led in-depth analysis of threat patterns and vulnerabilities, providing actionable insights to strengthen cybersecurity resilience.

Assistant Manager 2023/11 – 2024/06 | Bengaluru, India

- Developed a comprehensive malware playbook, outlining protocols and procedures for efficient response to malware incidents.
- Utilized diverse methods to validate SIEM signatures, ensuring accurate detection of malicious activities.
- Created and managed a dynamic malware analysis lab with Windows 10 and REMnux Linux VMs, equipped with tools like Radare2, IDA Pro, etc., for static and dynamic analysis within a secure virtual private network environment.
- Investigated complex malware threats using XDR, ensuring 100% RCA and impact assessment coverage by leveraging all available logs and telemetry.

IBM India, *Security Analyst* 2021/11 – 2023/11 | Bengaluru, India

- Conducted comprehensive malware analysis: Identified, analyzed, and mitigated complex malware threats targeting client systems.
- Led malware incident response efforts: Oversaw malware-related incidents, coordinated investigations, and provided timely recommendations for containment and remediation.
- Created custom tools for malware analysis: Developed Python-based tools such as an IOC scanner and PE analyzer, streamlining the malware analysis process and enhancing detection capabilities.
- Collaborated with cross-functional teams: Worked closely with network security, threat intelligence, and forensic analysts to gather intelligence, share findings, and develop comprehensive incident response strategies.
- Documented findings and provided actionable insights: Prepared detailed reports on malware analysis results, documented indicators of compromise (IOCs), and malware behavior, and recommended mitigation measures to assist clients in fortifying their security posture.

Globals India pvt ltd, *Malware Analyst* 2020/10 – 2021/11 | Bengaluru, India

- Conducted rigorous testing of antivirus software against the latest bypass techniques using self-made payloads.
- Identified vulnerabilities and provided recommendations for improving software efficacy.
- Developed web automation solutions using Python, streamlining processes and improving efficiency.
- Created custom tools and scripts to automate repetitive tasks, reducing manual effort.

ACSG Corp

Team lead - Information Security 2019/08 – 2020/10 | Delhi, India

- Extensive experience in cyber threat analysis, malware identification, evidence handling, and debugging malicious binaries.
- Proficient in reverse engineering various PE formats such as EXE, ELF, and DLL, as well as non-PE file types such as JavaScript, VBS, and Microsoft file formats like RTF, CFBF, and OOXML.
- Collected, extracted, and analyzed over 1,500 malicious samples per month from more than 25 sources.
- Developed four new security products in FY19-20, leading to a 25% increase in delivery and a 20% improvement in results compared to the previous year.

Executive Analyst - Information security 2018/08 – 2019/08 | Delhi, India

- Analyzed and implemented various security vulnerabilities in Windows and Android OS.
- Examined security vulnerabilities in Microsoft products such as Word, Excel, PowerPoint, and various other software.
- Detected flaws in antivirus software using SCANTIME and RUNTIME FUD techniques, including various cloud-based detection methods.

Education

IERT, *Bachelor of technology* 2014/08 – 2018/06 | Prayagraj, India

DAV PUBLIC SCHOOL, *12th , SSSC* 2013 | Bilaspur, India

Skills

Malware Analysis
Static and dynamic malware analysis

Reverse engineering
Reverse Engineering malware using debuggers & Disassemblers

Python programming language
Developing tools like scanners and analyser for malware analysis

MS-XDR
Microsoft Defender suite

Languages

- English
- Hindi