

# Vijay Bandari

Cyber Security Researcher | Malware Analyst | SOC (L2)

Hyderabad, Telangana

[vijaypbandari@gmail.com](mailto:vijaypbandari@gmail.com)

Phone: 9581519018, 7702543272

LinkedIn: <https://www.linkedin.com/in/vijay-bandari-a65413193/>

## Aspiration

Seeking a dynamic environment that will enhance my expertise in Cybersecurity with 5.3 years of related experience, I am eager to secure a challenging role where I can leverage my skills to achieve and surpass organizational objectives. Envisioning a rewarding position offering continual learning opportunities and challenges, I aim for a role that fosters both personal and professional advancement.

---

## Professional Experience

LTIMindtree, Hyderabad, Telangana, India  
Cyber Consultant

Feb 2023 – Present

Extensively engaged in the identification and comprehension of various malware types and their delivery techniques. Responsibilities include providing investigation, triage, and mitigation for detected security events. Additionally:

- Working on Static and dynamic analysis of PE & Non-PE samples.
- Determining samples and adding detection in AV signature.
- Validation of determination by other researchers from different teams.
- Working on FP and FN alerts for determination and validation.
- Working on samples belonging to different environments such as Windows, Linux, Android, MAC OS, Java.
- Analyzing different scripts such as batch, python, ruby, powershell, JS, XML, HTML, PHP, etc.
- Analysis of Microsoft office related documents (File types such as doc, docx, xls, ppt, etc)
- Writing static/generic signatures for Malware, PUA (Potentially Unwanted Applications), UWS (Widely known as Riskwares) samples.
- Working on different client tasks which includes signature analysis, Signer Hash analysis and specific malware families for better coverage of Automation.
- Working on testing, integration of Copilot with Microsoft Defender.
- Collaborated with a team of Microsoft for development of a tool, used for determination of samples and also enabling researchers in sample analysis by providing scan results of Microsoft as well as third party AVs, vital metadata about sample.
- Conducting sessions on malware campaigns such as Whispergate, Qakbot, etc. for almost 4 teams with 100% capacity.
- Training of new joiners/juniors on file analysis and signature writing.
- Working with packed samples such as UPX, MPress, Themida, Enigma, VMProtect, etc., and AutoIT samples as well.
- Reviewing technical reports of different determination provided by client and performing Vulnerability Assessments on the same.
- Providing Network Security protocols focusing on protecting industrial control systems (ICS) and operational technology (OT) from cyber threats, ensuring the safety and reliability of critical infrastructure like power grids and manufacturing plants.
- Reviewing different Pull request of signatures before publishing and documenting all the reports.

- Served Part of the Security Researcher team as a Microsoft Defender for Endpoint (EDR).
- Analyzing machine event data to identify False Positives (FP) and True Positives (TP), and creating reports based on analysis.
- Writing suppression rules to mitigate False Positives and fine-tuning False Positive detectors.
- Recommending changes to the source code of EDR detectors to address False Positives.
- Creating new EDR detections and triaging False Negatives for undetected suspicious or malicious threat campaigns.
- Testing newly developed detectors across various scenarios and telemetry to assess detection quality before production.
- Actively hunting for advanced targeted attacks using large datasets and Microsoft's Threat Intelligence IOCs.
- Involved in various stages of incident response, including in-depth analysis and Root Cause Analysis (RCA) submission on security incidents.
- Hands-on experience with network management solutions and firmware updates.
- Emulating APT group behaviours and attacks to validate detections and align them with the ATT&CK framework.
- Handling customer and client detection issues, providing prompt and accurate feedback.

## Tollplus India Private Ltd., India

CSA System Analyst

Nov 2019 - Nov 2021

To review the higher-priority security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence tools.

- worked round the clock in a security operations centre.
- Using OSINT tools to investigate harmful phishing emails, domains, and IPs. Then, depending on your findings, suggest appropriate blocking.
- Surfing security blogs to explore emerging and changing threats and vulnerabilities.
- To conduct security testing, use vulnerability assessment tools like Nessus and NMAP.
- Conducting real-time monitoring of URLs and traffic behaviour, making daily adjustments to database records through CRUD operations based on analysis.
- Re-scan systems to prevent new infections. Return systems to the network if there are none.
- Using Splunk for log analysis.
- Performed the high level Gap and Risk assessments in the process.
- Examine DNS, web, email, and firewall logs to find and stop attack attempts.
- Developed and optimized automation rules and playbooks within SIEM, analysing cybersecurity data to identify trends and collaborating with management to develop service improvement strategies.

## Key Skills

- Malware Analysis - Developed and implemented new methods of detecting and analysing malicious activity, leveraging knowledge of malware, network security, reverse engineering, and digital forensics. Writing signatures for intended files.
- Email and URL analysis - Scan suspicious emails for malicious content by isolating and implementing ways to harden frames and reduce their attack surface.
- Vulnerability Assessment - Being adept in discovering vulnerabilities, misconfigurations, and possible attack vectors creating in-depth reports that identify weaknesses in security.

- Incident Response and Digital Forensics – Investigating and analyzing evidence and Classify security events, conduct indepth forensic analysis, and suggest appropriate course of action, and coordinate incident response activities. To ensure efficient incident handling, create and maintain standard operating procedures for the Security Operations Center (SOC).
  - SOC – Well versed in cryptographic techniques, IDS, IPS, Network security, Splunk, Firewall, Arcsight, Incident handling and documentation. Knowledge and experience working with various security tools like SIEM, EDR tool, WAF, Email Protections tools, etc
  - Well versed in Network security concepts.
- 

## Education

- Bachelors in Computer Science (July 2015 - August 2019) Osmania University
  - Board Of Intermediate Education (2013 - 2015) NRI Academy
- 

## Certifications:

Certified Ethical Hacker (CEH)

Secure Delivery for Infrastructure Security

Protecting Cloud Infrastructure

Essential Incident Response

Securing Infrastructure Architecture

---

## Achievements:

- Recognized as a “STAR PERFORMER” during 2023 and 2024 annual awards in LTI Mindtree.
  - I was a recipient of the coveted “TOP PERFORMER” award for efficiently performing QC checks in Mindtree.
  - Worked in CDC (Cyber Defence Centre) in RED team and blue team. Knowledge in OWASP Top10 vulnerabilities.
- 

## Personal Profile:

- Date of Birth : 17th February 1997
- Languages Known : English, Telugu and Hindi

Declaration: I hereby declare that all the information furnished above is true to the best of my belief.

Place: Hyderabad

Bandari Vijay.