

# Pratyush Srivastava

+91-8318877305 pratyushsrivastava2121@gmail.com LinkedIn GitHub

Prayagraj, Uttar Pradesh -211004, India

## PROFESSIONAL PROFILE

Motivated cybersecurity enthusiast with hands-on experience in SOC monitoring, malware analysis, and security operations. Skilled in using tools like Splunk, Wireshark, Burp Suite, and Nmap for threat detection and incident response. Built and managed automated SOC lab environments using Wazuh, TheHive, and Shuffle. Strong foundation in SIEM, network security, and cyber threat intelligence, with practical exposure through platforms like LetsDefend and TryHackMe. Familiar with industry frameworks such as MITRE ATT&CK and NIST CSF.

## EDUCATION

**Dr. A.P.J. Abdul Kalam Technical University, Kanpur**

*Bachelor of Technology - Information Technology*

August 2022 – Present

Kanpur, India:

**RN Public School, Prayagraj, UP**

*Senior Secondary (Class XII)*

January 2021 – April 2022

Prayagraj, India:

## RELEVANT EXPERIENCE

**SOC Monitoring Experience – LetsDefend Platform**

April 2025 - Present

- Developed practical skills in SOC monitoring with hands-on experience on LetsDefend analyzing and addressing simulated cyber threats.
- Gained hands-on experience in SOC monitoring through LetsDefend platform by investigating 40+ real-world simulated alerts, including phishing, brute force, malware, and unauthorized access attempts.
- Improved response time and accuracy by consistently achieving up to 80 percent alert classification accuracy across multiple incident simulations on the LetsDefend SOC platform.

## PROJECTS

**SOC Automation Lab Project**

July 2025

- Built a fully automated Security Operations Center (SOC) lab using Wazuh, Shuffle, and TheHive for real-time threat detection and response, gaining hands-on experience with open-source SIEM, SOAR, and case management tools.
- Monitored and analyzed events from a Windows 10 client using Sysmon, integrated with VirusTotal to enrich threat intelligence, improving detection and investigation efficiency.
- Designed a scalable SOC architecture with documented workflows and a network diagram, demonstrating practical understanding of end-to-end alert lifecycle and security operations processes.

**Malware Analysis Lab Project** [\(GitHub Link\)](#)

September 2024

- Conducted static and dynamic analysis of disguised pdf.exe malware samples within an isolated FLARE VM environment to ensure safe examination and threat containment.
- Utilized PESTudio, x64dbg, Wireshark, and Process Monitor to investigate obfuscation techniques, anti-analysis behavior, and payload delivery methods used by the Zeus banking trojan.
- Documented attack chains and behavioral patterns, enhancing detection workflows and strengthening skills in identifying indicators of compromise, persistence mechanisms, and malware capabilities.

## KEY SKILLS

**Cybersecurity Skills:** Incident Response, Security Information and Event Management(SIEM), Security Operations Center(SOC), Log Analysis, Malware Analysis, Cyber Threat Intelligence, Network Security, Vulnerability Management, Security Monitoring, Governance, Regulatory Frameworks (ISO, GDPR), Risk Management

**Security Tools:** Splunk, Wireshark, Burp Suite, Nmap, Qualys

**Operating Systems:** Windows, Linux (Kali)

**Virtualization & Environments:** VMware, VirtualBox, FLARE VM

**Frameworks & Standards:** MITRE ATT&CK, Cyber Kill Chain, NIST CSF

**Platforms Practiced On:** TryHackMe, LetsDefend

## CERTIFICATIONS

- **Google Cybersecurity Certificate** – Foundations of Cybersecurity
- **Google Cybersecurity Certificate** – Play It Safe: Manage Security Risks
- **Google Cybersecurity Certificate** – Connect and Protect: Network Security
- **Simplilearn** – Introduction to Cyber Security Security