Tushar Jain

SOC Analyst | Cyber Security Professional

Contact

+918439028860

tusharmanoj2002@gmail.com

Linkedin

Education

GICSEH, Noida

Diploma in Cyber Security & Ethical Hacking
2024-2025

CCS University, Meerut

Bachelors of Computer Applications
2021-2024

Skills

- **SIEM Platforms** - Wazuh, ManageEngine Log360
- **SOAR & Automation** - Shuffle SOAR, Workflow Automation, Incident Response Playbooks, API Integrations, pfSense Firewall Integration
- **Security Monitoring** - Threat Detection, Log Analysis, Event Correlation, Alert Triage, Detection Rule Creation, IOC Analysis, MITRE ATT&CK Framework
- **Log Management** - Windows Event Logs, Syslog, JSON Log Parsing, Centralized Log Collection, Security Event Correlation
- **Network Security** - Firewalls, VLAN Fundamentals, Network Switching, Access Points, VPN Technologies, IDS/IPS Concepts, TCP/IP Fundamentals
- **Operating Systems** - Windows, Linux (Ubuntu, Kali Linux), macOS
- **Virtualization** - Proxmox VE, Citrix XenServer, Virtual Machine Management, Virtual Infrastructure Administration
- **Cloud Security** - Amazon Web Services (AWS), IAM Basics, Security Best Practices
- **Vulnerability Assessment & Penetration Testing** - Advanced VAPT, Burp Suite, Metasploit, Nessus, Nmap, OWASP Top 10, Web Application Security Testing
- **Security Tools** - Wazuh, ManageEngine Log360, Shuffle SOAR, Wireshark, Nmap, Burp Suite, Nessus, Metasploit, Snort
- **Programming & Scripting** - Python (Basic), SQL (Basic), C Language

Summary

SOC Analyst with 1 year of hands-on experience in Security Operations, SIEM monitoring, threat detection, incident response, and security automation. Experienced in Wazuh, ManageEngine Log360, Shuffle SOAR, log management, and MITRE ATT&CK-based attack simulation. Skilled in developing automated response workflows, integrating security solutions, and validating detection capabilities through adversary emulation. CEH Master certified with strong knowledge of cybersecurity operations, network security, VAPT, virtualization, and AWS cloud technologies.

Work Experience

Red Team Adversary Simulator (POC Project) *Nov 2025 to Present*

Quisitive Businesses LLP

- Participated in a 20-day Proof of Concept (POC) project for an AI-driven SOC/NOC security platform focused on threat detection, incident response, and automated ticketing.
- Executed Atomic Red Team attack simulations from Kali Linux to emulate real-world cyber threats and validate security monitoring capabilities.
- Performed MITRE ATT&CK-mapped adversary emulation to test detection rules, threat hunting workflows, alert generation, and incident response mechanisms.
- Collaborated with SOC and development teams to identify detection gaps, improve threat visibility, and validate AI-driven security analytics aimed at reducing MTTD and MTTR.

Projects

Quisitive Businesses LLP

SIEM Deployment & Security Monitoring Architecture

- Implemented enterprise-grade SIEM monitoring using Wazuh and ManageEngine Log360.
- Integrated Windows endpoints, Linux systems, firewalls, and Syslog-enabled devices.
- Developed custom detection rules and alerting mechanisms.
- Implemented secure log collection architecture for distributed environments.
- Performed log normalization and JSON field parsing for enhanced visibility.

SOAR-Based Automated Incident Response

- Designed and implemented automated brute-force attack response workflows using Shuffle SOAR.
- Integrated pfSense Firewall APIs for automatic malicious IP blocking.
- Automated alert validation, response actions, and security notifications.
- Reduced incident response time through workflow automation.

Advanced Web Application Security Assessment

- Conducted manual and tool-assisted penetration testing against OWASP Top 10 vulnerabilities.
- Identified SQL Injection, XSS, Authentication Bypass, Security Misconfigurations, and Access Control weaknesses.
- Produced professional vulnerability assessment reports with remediation recommendations.

CERTIFICATIONS

- Certified Ethical Hacker (CEH Master) – **EC-Council**
- Learn Ethical Hacking From A to Z – **Udemy**
- Network Ethical Hacking For Beginners – **Udemy**
- Programming in C Language – **Aptech**

ACHIEVEMENTS

- Ranked among the Top 1% on TryHackMe.
- Hands-on experience with SIEM, SOAR, Incident Response, and Threat Detection.
- Built automated security workflows integrating SIEM, SOAR, and Firewall technologies.
- Strong practical understanding of SOC operations, detection engineering, and security monitoring.