




UTKARSH TRIPATHI
SOC L1 Cyber Security Analyst

CONTACT INFORMATION

 BTM Layout, Bangalore

 utkarsh.dnt@gmail.com

 +91 8303492128

PROFESSIONAL SUMMARY

Results-driven **SOC L1 Cyber Security Analyst** with expertise in **incident response, threat hunting, and log analysis**. Adept at safeguarding digital assets, monitoring security events, and mitigating risks in dynamic environments. Skilled in **SIEM, security incident management, and forensic analysis** to ensure proactive cyber defense. Having basic knowledge of VAPT also.

PROFESSIONAL EXPERIENCE

Cyber Security Intern

Cyber Sapiens United LLP, Mangalore | Nov 2025 – Present

- Managing **Situations, Alerts, and Cases** related to cybersecurity incidents.
- Analyzing threats using **Raw Log Search** and conducting **situation analysis**.
- Using **SIEM like Splunk and ELK Stack** for Log Analysis, Correlation and Aggregation

Cyber Security Analyst – SOC L1

Netenrich Technologies Pvt Ltd, Hyderabad | Nov 2023 – May 2024

- Managed **Situations, Alerts, and Cases** related to cybersecurity incidents.
- Analyzed threats using **Raw Log Search** and conducted **situation analysis**.
- Worked on **Resolution Intelligence Cloud (RIC)** and provided **MDR (Managed Detection & Response)** support.
- Assisted in **FedRamp security compliance** and **Microsoft MDE** security solutions.

Trainee (Cyber Security & IT Infrastructure)

CDAC – Hyderabad | March 2023 – August 2023

- Completed hands-on training in **cybersecurity, network security, and system security**.
- Gained expertise in **cyber forensics, system administration, and IT infrastructure management**.

Freelancer (Website Design & Development, SEO/SMM) worked for Company called Web Wizard Technologies on freelance basis

2016 – 2023

- Provided web development, SEO, and social media marketing services.

Business Analyst

S.B. Infotech, Indore | 2012 – 2016

- Coordinated with clients and created **SRS, technical reports, RFPs, and RFQs.**
 - Engaged in requirement gathering and documentation.
-

EDUCATION

- **PG Diploma in IT Infrastructure, System, and Security (DITISS) | CDAC Hyderabad | 2023-2023**
 - **Bachelor of Engineering (IT) | Rajiv Gandhi Technical University, Bhopal | 2008 – 2012**
 - **Intermediate & High School | Central Academy, Gorakhpur | 2006 – 2007**
-

TECHNICAL SKILLS

SOC Operations & Threat Hunting

- **SIEM & SOAR** (Security Information and Event Management, Automated Response)
- **Incident Analysis & Case Management**
- **Threat Intelligence & Detection Rules Analysis**
- **Security Event & Incident Management (SEM & SIM)**
- **Endpoint Detection & Response (EDR)**
- **Log Ingestion, Log Analysis, Log Deletion**
- **Google Chronicle & SecOps Operations**

Cybersecurity & Penetration Testing

- **SQL Injection, XSS Attacks, Brute Force, DOS & DDOS Attacks**
- **Website Interception & Session Hijacking**
- **Wireshark Packet Analysis & Network Sniffing**
- **Burp Suite & OWASP ZAP**

Cyber Forensic Tools

- **Autopsy, FTK Imager, WinHex, HashCalc**
- **FRAT, FDAC, WinAudit**

Network & Security Tools

- **Cisco Packet Tracer, Wireshark**
 - **Advanced IP Scanner, Nmap, Metasploit**
 - **Firewall Management & Bastion Host**
-

CYBER SECURITY KNOWLEDGE BASE

- **OWASP Top 10 for Web**
 - **MITRE ATT&CK Techniques, Tactics and Procedure**
 - **Microsoft Defender for Endpoint (MDE) and VIRUS TOTAL/ Abusal IPDB**
 - **Threat Hunting & Incident Response Training**
 - **Cyber Forensic & Malware Analysis Training**
-

STRENGTHS

- ✓ Strong analytical and problem-solving skills
- ✓ Ability to work in high-pressure environments
- ✓ Quick adaptability to new security tools and technologies
- ✓ Strong understanding of compliance frameworks (CSA Star,HIPPA,ISO 27001, NIST, etc.)