

# ULLAS T L

Cyber Security Analyst | SOC Analyst | Incident Response

Phone: +91 9353701019 | Email: ullasraju5@gmail.com | Location: Bengaluru, India

## PROFESSIONAL SUMMARY

Detail-oriented Cyber Security Analyst with hands-on experience in SOC operations, real-time security monitoring, incident triage, and threat analysis using SIEM and EDR tools. Skilled in identifying true positives, investigating phishing and malware incidents, and escalating incidents for remediation. Strong knowledge of MITRE ATT&CK incident lifecycle, threat intelligence, and networking fundamentals.

## CORE SKILLS

- SIEM: Splunk, IBM QRadar
- EDR: CrowdStrike Falcon
- Open-Source Tools - Virus Total, IP-Void, Mx Toolbox, Cisco Talos.
- Incident Response & SOC Operations (L1)
- Log Analysis: Firewall, Proxy, IDS/IPS, Antivirus, Windows Event Logs
- Threat Intelligence, Threat Hunting, IOC/IOA Analysis
- Email Security: Phishing Analysis, Header Analysis, URL & Attachment Sandboxing
- MITRE ATT&CK Cyber Kill Chain, Incident Lifecycle
- Networking: TCP/IP, OSI Model, DNS, DHCP, NAT, Ports & CIA
- Ticketing & Reporting: ServiceNow, Dashboards & Reports

## PROFESSIONAL EXPERIENCE

### Cyber Security Analyst – Incident Response

UnitedLex, Bengaluru | Nov 2025 – Present

- Monitor and analyze security events using IBM QRadar SIEM in a 24x7 SOC environment.
- Perform incident triage, prioritization, and classification based on severity and business impact.
- Map alerts and incidents to MITRE ATT&CK techniques and tactics.
- Analyze real-time alerts and determine true positives and false positives.
- Investigate phishing emails using header analysis, URL sandboxing, message tracing, and domain reputation checks.
- Escalate confirmed incidents to respective teams and track remediation through ServiceNow.
- Maintain awareness of latest TTPs, IOC feeds, and emerging cyber threats.

### Trainee – Security Analyst Tier 1

WAS Techno Developers | Oct 2024 – Oct 2025 (1 year)

- Monitored and reviewed security alerts and events from SIEM and other security tools to detect suspicious activity.
- Performed initial triage of security incidents, validated alerts and determined if further investigation was required.
- Conducted basic analysis of logs and system data to identify potential threats and categorize incidents accurately.
- Escalated confirmed or high-risk incidents to senior (L2/L3) analysts following SOC processes and SLAs.
- Documented incident findings, generated incident tickets and reports for audit and follow-up.
- Assisted in 24x7 real-time security monitoring operations, ensuring broad coverage across shifts.

### Security Analyst (Internship)

WorldSec Technologies LLP | Feb 2024 – Sep 2024 (8 months)

- Monitored and analyzed security events using Splunk SIEM.
- Worked as L1 SOC analyst handling alerts and security incidents.
- Performed real-time monitoring and identified true positive and false positive alerts.
- Investigate malicious phishing emails, domains, and IPs using Open-Source tool sand recommend proper blocking based on analysis.
- Assisted in investigation, reporting, and escalation of security incidents.

## **EDR & THREAT INTELLIGENCE EXPERIENCE**

SIEM Expert – Certified SOC analyst

- Hands-on experience with CrowdStrike Falcon EDR for detection, triage, and response.
- Performed malware analysis including dynamic analysis and sandboxing.
- Handled fileless malware and ransomware incidents using EDR containment techniques.
- Used RTR for containment, remediation, and host investigation.
- Good at understanding Sandboxing reports & Good at performing the EDR host and user management
- Excellent in handling the malware and performing the Static Analysis & Dynamic analysis.
- Knowledge on Ryuk ransomware
- Conducted daily threat hunting using open-source threat intelligence feeds.
- Developed and validated IOCs/IOAs and supported use-case creation.
- Analyze EDR alerts from CrowdStrike Falcon and perform response actions including host isolation.

## **CERTIFICATIONS**

- SIEM Xpert – Certified SOC Analyst
- Cisco – Introduction to Cyber Security
- Great Learning Academy – Cyber Security Threats
- Udemy – SOC Analyst Strong Foundation

## **EDUCATION**

Bachelor of Engineering (Mechanical Engineering)  
BNM Institute of Technology, Bengaluru – 2024

## **LANGUAGES**

English | Kanada | Hindi

## **DECLARATION**

I hereby declare that the above-mentioned information is true to the best of my knowledge.

Place: Bengaluru

Ullas T L