PRANAV KALIDAS

+91 70395 19926 | kalidas.pranav@gmail.com | my-portfolio | linkedin.com/in/pranav-kalidas

PROFESSIONAL SUMMARY

Security Analyst with 2+ years of SOC experience in monitoring, triaging, and responding to security incidents within Managed Security Service Provider (MSSP) and enterprise environments. Skilled in SIEM monitoring, incident response, phishing analysis, threat hunting, EDR/XDR, log analysis, and playbook automation. Proven ability to investigate and escalate incidents efficiently, reduce false positives, and maintain SLA compliance. Hands-on experience with Defender XDR, Microsoft Sentinel, QRadar, FortiSOAR, and Cisco security tools.

EXPERIENCE

Security Analyst – Tech Mahindra [Bengaluru] **Dec 2023 - Present**

- Working as a SOC Analyst as a Managed Security Service Provider (MSSP) in Detection and Response, supporting **SES Telecom**, a leading European telecom firm with **5000+ employees**.
- Performed triage using KQL with **utmost due diligence** across rotational shifts
- Swiftly initiated playbooks and escalated 20+ alerts daily
- **Seamless collaboration** with L2 and L3 teams to expedite alert resolutions
- Conducted **in-depth analysis** while consistently meeting SLA expectations
- Created detailed incident reports and RCA documents for stakeholders, recommending preventive security measures.
- Communicated directly with end users to validate suspicious activities, gather additional context, and confirm remediation actions.

Software Developer Intern - Netmeds [Chennai] **Oct 2022 - Sep 2023**

- Developed inventory stock management and flow modules (inbound/outbound) in Java, optimizing system workflows.

SECURITY TOOLS AND TECHNOLOGY

- **Microsoft Sentinel & Defender XDR:** Threat hunting using KQL, device timeline analysis, email triage
- **IBM QRadar:** Log correlation, traffic flow analysis, attack context decoding, IoC triaging, threat visualization
- **Cisco Umbrella Proxy:** User browsing behavior analysis, referral page identification beyond SIEM logs
- **Cisco Secure Malware Analytics:** Phishing domain extraction, malware process deconstruction, post-compromise behavior mapping, threat artifact enrichment
- **Fortinet FortiSOAR:** Workflow orchestration, playbook automation for incident response
- **Splunk:** SIEM operations and threat detection

CERTIFICATIONS AND LEARNINGS

Security Operations Analyst Associate (SC-200) ↗	Microsoft**,** July 2025
Certified Ethical Hacker v12 - Practical ↗	EC-Council, April 2025
Certified Ethical Hacker v12 ↗	EC-Council, August 2024
Certified Fundamentals Cybersecurity ↗	Fortinet, October 2024
Ethical Hacking ↗	NPTEL-IIT Kharagpur, November 2023
Actively learner on TryHackMe ↗	Since February 2024

TECHNICAL SKILLS

SIEM, MITRE ATT&CK, Threat Detection, Incident Response, Log Analysis, KQL (Kusto Query Language), EDR (Endpoint Detection and Response), Email Forensics, OSINT Collection, Scripting (Python/Bash, Communication Skills

ACHIEVEMENTS

- Awarded “Pat-On-The-Back” (twice) for exceptional SOC performance.
- Best Final Year Project Award – Bitcoin Price Prediction using Machine Learning.
- Served as College Cultural Team Lead, managing multiple events and teams.

EDUCATION

Bachelor of Engineering in Computer Science, VTU [8.7 CGPA] **Aug 2019 - May 2023**

- Focus: Cryptography, Cybersecurity and Computer Networks