# Punith B S

• punithbs66@gmail.com • +91 8431411063

## SUMMARY

Hands-on experienced SOC Analyst with expertise in multiple security tools, ranging from SIEM to EDR. Responsible for monitoring, analyzing, and responding to security events and incidents to ensure the organization's IT environment remains secure. Possesses strong skills in identifying potential threats by reviewing security alerts, logs, and incidents using various security monitoring tools.

## TOOLS AND TECHNOLOGIES

- SIEM: Sentinel, Qradar
- IPS/IDS: Symantec
- Email Security: MS O365
- Proxy: Zscaler, Bluecoat
- EDR - Crowdstrike, MS defender
- TI Sites - Any Run, Urlscan, browserling, AbuseIpdb, VirusTotal, CyberChef
- Query Language – SQL
- OS: Windows, Linux

## Hands on Skills

- Strong understanding of typical SOC workflows with a focus on providing security while ensuring the confidentiality, integrity, and availability (CIA) of data and systems.
- Proficient in using frameworks like MITRE ATT&CK and OWASP; solid knowledge of cyberattacks, malware categories, DNS, DHCP, ports, and protocols.
- Detailed phishing email analysis involving malicious URLs, files, and QR codes.
- Skilled in proxy log analysis and investigating suspicious file downloads; educating users about security policies.
- Expertise in identifying and analyzing false positives in security alerts.
- Real-time log monitoring on SIEMs, EDR, proxy, firewall appliances, and IPS/IDS systems.
- Proficient in investigating and analyzing events in Endpoint Detection and Response (EDR) tools, taking required actions, and ensuring tickets are resolved within SLA.
- Experience in malware analysis using both static and dynamic techniques.
- Providing investigation, triage, and mitigation of detected security events to prevent user interaction with malicious content.

## EDUCATION

Bachelor of Engineering (B.E.) in Electronics and Communication Engineering

Dayananda Sagar Academy of Technology and Management, Bangalore

CGPA: 7.10

Graduation Year: 2024

## PROJECTS

**Exploitation of OWASP Juice Shop (E-commerce Website):**

Enhanced web security skills by exploiting multiple vulnerabilities in the OWASP Juice Shop using tools like Burp Suite and ZAP. Analyzed OWASP Top 10 vulnerabilities (SQL Injection, XSS), performing vulnerability analysis and applying mitigation techniques.

## INTERNSHIP EXPERIENCE

**Matex - Bug Bounty Certification Program**

Feb 2024 – June 2024

- Identified and exploited vulnerabilities such as SQL Injection and XSS during security assessments.
- Reported bugs and practiced responsible disclosure, improving system security and reducing vulnerabilities.

## CERTIFICATIONS

- Cybersecurity and Ethical Hacking Internship Program — Edureka
- Bug Bounty Certification — Matex