JAYASHRI DESHMUKH

• +91 8421208036 • boradejaya1@gmail.com

SUMMARY

Results-oriented SOC Analyst with over 4 years of hands-on experience in monitoring, triage, analysis, and swift response to security incidents. Proficient in leveraging industry-leading tools like SIEM, IDS/IPS, Firewall, AV/EDR, Email Gateway, and Web Proxy for effective cyber threat detection and mitigation. Notable expertise in conducting in-depth investigations, implementing robust security measures, and collaborating with cross-functional teams to fortify organizational defenses

PROFESSIONAL EXPERIENCE

SOC Analyst, Aarna Technologies Pvt Ltd **Oct 2021 - Present**

- Conduct proactive monitoring and efficient triage of security events.
- Investigate all security alerts, to determine whether the event is a false positive or a security incident.
- Monitor diverse security events and logs (Proxy, IPS/IDS, Firewall, Email, AV, EDR, and WAF).
- Investigate reported emails, categorize them, & respond to users with findings & recommendations.
- Monitor the health of security sensors & SIEM infrastructure. Fine-tune SIEM rules to minimize false positives. Develop SOC monitoring use cases to proactively detect emerging threats.
- Identify, ingest, and manage IOCs in applicable security controls.
- Update incident response playbook for security readiness. Deliver concise SOC reports to stakeholders.

SKILLS

- SIEM-Splunk
- EDR- Crowdstrike
- Firewall- Palo alto
- Email Gateway- Proofpoint
- Web Proxy- Zscaler
- Application Firewall- Imperva
- Anti-Malware - Symantec Endpoint,
- IDS/IPS- McAfee
- Ticketing Tools- ServiceNow
- Malware Analysis-Wireshark, McAfee ATD, Anyrun, Hybrid Analysis
- Threat intelligence-Recorded Future, Anomali
- Vulnerability Management-Qualys

KEY HIGHLIGHTS

- Proactively detected threats through continuous event monitoring and Triage.
- Investigated and classified security alerts for rapid response.
- Mitigated intrusion attempts, ensuring a secure environment.
- Responded swiftly to suspicious emails, enhancing security measures.
- Collected and reviewed threat intelligence for proactive defense.
- Optimized SIEM rules for accurate threat identification

EDUCATION

Nutan Mahavidyalaya Sailu
Bsc

Dr Babasaheb Ambedkar Marathwada University Aurangabad
Msc

CERTIFICATIONS

- **EC-Council-Network Defense Essentials**
- **Identifying Web Attacks Through Logs**
- **Executive Vulnerability Management**
- **Incident Response Lifecycle**
- **Enterprise Security Leadership: Creating World Class Security Operations Center (SOC)**