PRASHANT AJAGEKAR

MUMBAI
prashanataja08@gmail.com | +91- 9049126848
LinkedIn: linkedin.com/in/yourprofile
Portfolio: yourwebsite.com

PROFESSIONAL SUMMARY

Detail-oriented **SOC Analyst with 2 years of experience** in 24×7 security operations, SIEM monitoring, alert triage, incident escalation, and daily health-check reporting. Hands-on experience with **SIEM tools, malware analysis using VirusTotal, log analysis, and basic SOAR workflows**. Strong understanding of networking and security fundamentals with the ability to work effectively in rotational shifts.

PROFESSIONAL EXPERIENCE

L&T Finance |April 2024 – Present

- Worked in a 24x7 shift environment to ensure continuous security monitoring and incident response.
- Performed **incident response activities for client environments**, including identification, analysis, containment, and escalation as per defined playbooks.
- Acted as **first point of contact for client-side incident response** during security events in rotational shifts.
- Conducted **alert triage**, validated true positives vs false positives, and prioritized incidents based on severity and business impact.
- Performed **malware and IOC analysis using Virus Total** (hashes, IPs, URLs, domains).
- Escalated confirmed incidents to **L2 teams with detailed analysis, logs, and investigation notes**.
- Worked on **Tenable vulnerability scanning** to identify security weaknesses across client assets.
- Assis ted in **vulnerability assessment (VA) reporting**, including risk classification, remediation recommendations, and report validation.
- Reviewed and tracked vulnerabilities based on **severity (CVSS scores)** and supported remediation follow-ups with stakeholders.
- Created and maintained **daily SOC health check, incident summary, and morning reports**.
- Analyzed logs from firewalls, servers, endpoints, and network devices to support investigations.
- Worked in a 24x7 shift environment to ensure continuous security monitoring and incident response.
- Monitored real-time security events within the SOC environment to identify suspicious activities and potential threats.
- Hands-on experience in monitoring logs and security events using IBM QRadar SIEM and Sentinel one EDR
- Prepared weekly and monthly security reports as per client requirements.
- Conducted SIEM servers (Windows & Linux) health checks to ensure optimal performance and log ingestion.

- Reviewed and approved requests for Zscaler Private Access (ZPA after validating identity and access requirements
- Validated and approved user requests for external URL access based on security policies.
- Involved in integration of log sources such as DLP, NAC, and DAM into the SIEM environment.
- Involved in Phishing email analysis and malware analysis.
- Conducted threat hunting activities to proactively identify potential security risks,
- Participated in Weekly VOD (Video on Demand) activities related to security reviews.
- Hands-on experience on Microsoft AD, Netskope (Proxy & DLP), Kaspersky AV, Zscaler VPN and Firewall (FortiGate, Palo alto and checkpoint)
- Performed continuous monitoring of GSuite and Google Cloud Platform (GCP) logs to support use case development and finetuning.
- Developed and enhanced SIEM use cases mapped to the MITRE ATT&CK Framework to improve detection of advanced threats. 15. Closely working with the governance team on audit activities to ensure compliance

EDUCATION

Bachlores of Science
Shivaji university, Kolhapur | 2022