Ravina Abdagire

Information Security Analyst(L1)
Accenture, Pune
Email Id- ravinasabdagire@gmail.com
Contact Number- 9359247276
LinkedIn- https://www.linkedin.com/in/ravina-abdagire-652795322

Objective:

An experienced information security professional with strong Cyber Security, management skills & soaring interest in cutting edge security trends that require profound reading and experimentation. Fully committed to understand and re-invent processes to develop innovative approach towards problem solving. Always eager to learn more tricks from all team members adding to holistic knowledge gain in a way that is beneficial to the company while enhancing productivity and reputation.

Skills Highlights:

- Domain: Security Operations & Security Monitoring.
- Understanding of SIEM Network architecture.
- Good knowledge of Reference Set, Active list, Rules & IOCs configuration in SIEM.
- Technical Knowledge: SIEM (Q-Radar, Splunk), EDR (Crowd Strike, Microsoft Defender), Vulnerability Assessment, Suspicious File Analysis, Firewall (Fortinet, SOPHOS & Checkpoint), Antivirus (SOPHOS, Symantec), Proxy (Zscaler), IPS (Fortinet, McAfee, Palo Alto,) Incident Response, Suspicious Email Analysis & Information Security Advisories.

Experience:

- **Information Security Analyst, Accenture Pune. (August 2022 – Present)**
- **Security Operation, Event Detection & Investigation(L1):**
- Q-Radar, Splunk - day to day operations & perform real-time proactive security monitoring detection & response to security events & offence for Enterprise infrastructure. Threat Hunting, Recorded Future, Crowd strike, IPS/IDS, DLP, Incident Handling, Log analysis & Deep investigation, Presentations, Dashboards & Reports.
- Conduct thorough investigation of security events generated by our detection mechanisms such as SIEM, EDR, IDS/IPS, WAF, Firewall, Proxy.
- Incident Handling, Investigate, collaborate and report on root-cause-analysis of malware attacks.
- Investigate a threat and correlate it with multiple implemented security platforms and analyze the historical to current research-based scenario to take appropriate actions.
- Implemented best practices for incident response and investigation, correlation trainings for team to maintain the SLA.

- Conducted sessions & trainings on Use-Case, Playbooks & Cybersecurity related topics. Implemented Play-books for investigation steps & response.

.

Event detection & Investigation (L1):

- Security SIEM Operational task – Log Analysis and Correlation, Filters, Active channels, Security event monitoring and Incident handling, Email Analysis, Domain analysis, Team Lead, Good leadership skills and ability to coordinate and direct teams of SOC analysts calmly and effectively in high-pressure situations.
- Worked in 24x7 operational support, Knowledge of Networking and Information security concepts processes, In depth idea about SIEM architecture (Q-Radar), Good understanding on different types of Cyber-Attacks.
- Real Time Monitoring on SIEM Tool Splunk and Q-Radar.
- Based on network devices, operating systems and platform of client's environment, creating customer specific security reports and monthly dashboard as well as fine-tuning on client requirements. Report Automation on Q-Radar SIEM platform. Actively involved into configuring IOCs of latest security threats on Q-Radar ESM.
- Block IOCs on Security solutions.

Incident Response(L1):

- Investigate of Incidents raised by SOC Team, share incident with stakeholder & provide mitigation.
- Maintain record of reporting & non-reporting devices on daily basis & present these reports in weekly meeting with CISO & respective stakeholders.
- Co-ordinate with SOC Team regarding client queries & provide solution within SLA time.
- Prepare reports & share report observations with respected stake holders.
- Perform use-case review activity on quarterly basis.

Education:

- BE (Electronics & Tele-Communications), Savitribai Phule Pune University in 2020 - 2023

Hobbies:

- I like spending time in learning of new cyber security concepts and share it with my team mates specially for new commers and freshers, Because Freshers are not getting /learning required skills for industry in their college life.
- I usually spend my leisure time in listening music, meditation and exercise.

Ravina Abdagire