

Jyoti Singh *Cyber Security Engineer*

✉ Ec.jyoti29@gmail.com

☎ +91 9738532332

📍 Mumbai, India

🌐 www.linkedin.com/in/jyoti-s-55557010a

Profile

Results-driven Cyber Security Engineer with over 8 years of experience in Threat Hunting, Detection Engineering, SIEM, log Analysis, Incident Response, Digital Forensics and managing security solutions to protect organizational assets and data.

Professional Experience

Working Period	Designation	Organization
From 4th Nov,2016 to 25th Feb 2019	Senior Analyst	Capgemini India Pvt Ltd, Bangalore
From 13th March, 2019 to 30th Apr, 2020	System Engineer	TCS
From 8th May, 2020 till present	Technical Consultant	IBM

Certifications

IBM Certified Analyst	Security QRadar SIEM V7.5
SC-200	MICROSOFT CERTIFIED: Security Operations Analyst Associate

Professional Experience

SIEM:

- Deployed and configured IBM QRadar SIEM, integrating log sources from firewalls, endpoint solutions, cloud platforms, and applications.
- Developed and fine-tuned custom correlation rules, searches, and dashboards to detect and mitigate specific threats.
- Monitored and analyzed logs from SIEM platforms, identifying and escalating potential threats.
- Conducted security event analysis, investigating anomalies, and escalating incidents to the SOC or Incident Response teams.
- Performed regular health checks and maintenance of QRadar infrastructure, ensuring optimal performance and data accuracy.
- Assisted in the deployment of IBM QRadar SIEM, configuring data pipelines and mapping event fields for custom use cases.
- Worked with cross-functional teams to remediate vulnerabilities and implement preventive measures.

EDR:

- Conducted endpoint threat hunting to identify suspicious activities, such as anomalous process behavior and unauthorized access attempts.
- Investigated and remediated malware infections by analyzing indicators of compromise (IoCs) and behavioral patterns.
- Conduct proactive threat hunts using EDR tool.
- Develop and implement custom detection rules to identify anomalies and threats.
- Analyze endpoint logs, alerts, and telemetry for indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).
- Collaborate with the incident response team to resolve and mitigate identified threats.
- Perform root cause analysis for security incidents and create actionable recommendations.
- Designed and implemented a DESTRA (Data Egress Security Threat Response Analysis) Rule to detect and mitigate potential data exfiltration events.
- Monitored outbound network traffic to identify anomalies indicative of insider threats or compromised accounts.
- Integrated the DESTRA Rule into the organizations and fine-tuned detection thresholds, reducing false positives.

Additional Responsibility

- Mentor junior analysts by sharing best practices in threat detection, log analysis, and incident response.
- Create and distribute weekly or monthly threat bulletins highlighting emerging vulnerabilities, malware campaigns, and threat actor activities.
- Preparing monthly and weekly incidents reports to share with clients and team.

Skills

Threat Hunting | Incident Response | Threat Intelligence (MITRE ATT&CK) | Data Analytics | Vulnerability Assessment | Malware Analysis | SIEM | IOT | Endpoint Security | Log analysis | Ethical Hacking | Information Security | Risk management | Digital Forensics | cloud security | DDOS Analysis | Email header analysis | Playbook Development

Technology & Tools

Security Information and Event Management (SIEM) Tools:Qradar, Splunk | Endpoint Detection and Response (EDR) Platforms | Vulnerability Management: Qualys Guard | Email Gateway: Mimecast | Threat Hunting and Behavioral Analysis | Threat Detection and Incident Response | Malware Analysis and Reverse Engineering | Firewall: PaloAlto,Forcepoint DLP | Ticketing tools: BMC Remedy, Snow.

Education

2012/07 – 2016/07 Bangalore	Bachelor of Technology in Electronics and communication Sambhram Institute of Technology Percentage: 73%
2011/03 – 2012/03 Bangalore	HIGHER SECONDARY (12th) -CBSE Kendriya Vidyalaya No-2 Percentage: 67.4%
2009/03 – 2010/03 Bangalore	SECONDARY (10th) -CBSE Kendriya Vidyalaya No-2 Percentage: 82%

Key-strengths

Team Player | Eager to Learn | Self Motivator | Honest | Composed