MANISH BAJAJ

Security Operations Team Lead **|** Azure Sentinel **|** Microsoft Certified (SC-200, SC-300, SC-400, BTL1)
Ahmedabad, Gujarat, India | +91-9468076875 | manishbajaj1998@gmail.com | linkedin.com/in/manish-bajajb48ab9223

PROFESSIONAL SUMMARY

Security Operations Team Lead with 4.5+ years of cybersecurity experience specializing in Microsoft cloud security, incident response, and threat detection. Microsoft Certified (SC-200, SC-300, SC-400) and Security Blue Team Level 1 (BTL1) professional with expertise in Azure Sentinel SIEM, threat hunting, and vulnerability management. Proven ability to lead SOC teams, mentor analysts, and drive scalable security operations in MSSP environments.

CORE COMPETENCIES

Microsoft Security Suite: Azure Sentinel, Microsoft Defender, Defender for Cloud, Defender for Identity, Defender for Office 365, Information Protection, SC-200, SC-300, SC-400 **|** SIEM & Monitoring: Splunk Enterprise **|** Incident Response: Alert Analysis, Triage, Investigation, Remediation **|** Threat Intelligence: Threat Hunting, IOC Analysis, Vulnerability Management **|** Security Tools: Nessus, VirusTotal, IBM X-Force **|** Compliance: MITRE ATT&CK;, OWASP **|** Additional: Phishing Analysis, ServiceNow, Firewalls, IPS, Email Gateway, WAF

PROFESSIONAL EXPERIENCE

Security Services Team Lead | Atech Cloud
December 2024 - Present | Ahmedabad, Gujarat

- Lead SOC operations team, mentoring analysts on Azure Sentinel SIEM management, incident response, and threat analysis
- Design and optimize Azure Sentinel detection rules to identify security threats and anomalous activities
- Oversee incident response lifecycle from alert triage through investigation, documentation, and engineering team coordination
- Manage threat intelligence programs including IOC analysis, vulnerability management, and threat hunting
- Lead phishing awareness campaigns and security testing initiatives with cross-functional engineering teams
- Generate executive-level security reports demonstrating SOC metrics and organizational security posture

L-2 Cyber Security Analyst | Atech Cloud
November 2023 - December 2024 | Ahmedabad, Gujarat

- Conducted advanced SIEM alert analysis using Azure Sentinel with high accuracy incident escalation
- Performed threat intelligence research and vulnerability assessments for engineering teams
- Managed incident response workflows including ticket creation, documentation, and remediation tracking
- Supported phishing campaign development and security awareness initiatives

Cyber Security Analyst | Wipro
May 2022 - November 2023 | Gurugram, Haryana

- Monitored and analyzed security alerts using Splunk Enterprise SIEM with deep-dive investigation
- Triaged alerts, identified false positives, and escalated validated incidents to response teams
- Created threat intelligence reports and dashboards for senior management decision-making
- Participated in phishing awareness campaign development

Advisor 1 | Concentrix
December 2020 - May 2022 | Chandigarh, India

- Resolved average of 50 customer inquiries daily through phone, email, and chat support with 90% satisfaction rating
- Demonstrated exceptional problem-solving by effectively troubleshooting and resolving complex customer issues
- Achieved 20% decrease in unresolved cases in first quarter through process improvements

CERTIFICATIONS & CREDENTIALS

- Security Blue Team Level 1 (BTL1)
- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- Microsoft Certified: Identity and Access Administrator Associate (SC-300)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-400)
- Microsoft Administering Information Protection and Compliance
- Splunk Fundamentals Certified
- Cortex XSOAR Analyst Training (Palo Alto)
- Microsoft Applied Skills: Create Agents in Microsoft Copilot Studio
- Fortinet NSE 1 and NSE 2

EDUCATION

Master of Business Administration (MBA) | Human Resources Management **|** Chandigarh University (2021-2023)

Bachelor of Science (Honours) in Chemistry | Kirori Mal College, University of Delhi (2016-2019)