Anshuman

Pune, Maharashtra
+91-8709934756 anshuman0124@gmail.com anshuman-00020a193

Security consultant with experience in Microsoft Defender 365 and Sentinel. I specialize in endpoint protection, threat detection, and automating security responses. Currently working at CGI, I focus on threat hunting using KQL and enhancing cloud security with Microsoft Defender 365, Intune, and Azure AD, driving proactive solutions and compliance.

WORK EXPERIENCE

CGI Inc] **01 2025 – Present**
Cyber Security Analyst *Pune, Maharashtra*

- Monitoring over 80,000 endpoints using Microsoft Defender for Endpoint (MDE) to detect and respond to threats.
- Performing alert triaging and deep-dive investigations to ensure quick threat containment and minimal business disruption.
- Implementing and managing Defender policies such as Attack Surface Reduction (ASR), Device Control, AppLocker, and antivirus update configurations (platform, engine, and signature).
- Integrated Microsoft Defender for Endpoint with Azure Data Explorer (ADX) using Event Hub for advanced analytics and custom detection.
- Actively working to improve the Microsoft Secure Score by remediating security recommendations across the environment.
- Designing and deploying firewall policies through Group Policy Objects (GPO) to enforce network security.
- Utilizing Azure AD for group creation and management to support RBAC within Microsoft Defender 365.
- Implementing Role-Based Access Control (RBAC) in MDE to manage security operations team access.

LTIMindtree] **07 2022 – 01 2025**
Cyber Security Consultant *Pune, Maharashtra*

- Led the deployment and configuration of Microsoft Defender for Endpoint across client and Customer environments, ensuring endpoint protection, threat detection, and response.
- Monitored and analyzed security incidents using Microsoft Defender 365, responding to malware, phishing, and other threats in real time to minimize business disruption.
- Designed and implemented security policies and procedures in line with Microsoft Defender 365's best practices to enhance the organization's overall security posture.
- Assisted in integrating Microsoft Defender 365 alerts with SIEM tools like Microsoft Sentinel for centralized threat monitoring and incident management.
- Performed in-depth investigation of security incidents using Defender 365 tools, including analysis of attack vectors, root cause identification, and threat intelligence.
- Developed automated response playbooks within Microsoft Defender 365 to streamline responses to common threats and reduce incident response time.
- Utilized Microsoft Sentinel for proactive threat hunting, correlating logs and events from Defender 365, Azure and other services to identify suspicious activities and potential security incidents.
- Designed and maintained custom dashboards and workbooks in Microsoft Sentinel for real-time monitoring of security events and KPIs, providing actionable insights to customers.

Knuckle Head Corporation LLP] **08 2021 – 12 2021**
Data Analyst *Kolkata, West Bengal*

- Analyzed data for 2500 monthly active user and used the output to guide the marketing and product strategies.
- Cut project time for data analysis.
- Done annotation of Image, Text, Videos.

EDUCATION

Asansol Engineering College (MAKAUT) **07 2017 – 06 2021**
B.Tech *Asansol, West Bengal, India*

TECHNICAL SKILLS

Languages: KQL, HTML, CSS, JAVA
Security Platforms & Tools:: Microsoft Defender 365, Microsoft Sentinel, Microsoft Intune, Azure Active Directory (AAD), Microsoft Defender for Cloud, Microsoft Purview (DLP)
Skills: Threat Detection & Incident Response, Cloud Security, Automation & Scripting, Security Compliance & Governance, Networking & Firewalls, MITRE ATTACK

CERTIFICATIONS AND ACHIEVEMENTS

• Microsoft AZ-900 Certified • Data Analytics Essentials certified • Received a spot award for outstanding performance two times • Led a team of 20 security professionals as the Subject Matter Expert (SME) to successfully deliver a critical cybersecurity project for Microsoft.