Ankur Singh

Cyber Security Consultant

My Contact

Gorakhpur, Uttar Pradesh
+918504899838
singh999ankur@gmail.com
Ankur-Singh2698
Portfolio
Ankur982

Technical Skills

- Incident response & event management
- Vulnerability management
- Azure Sentinel
- Microsoft Defender for Endpoint & Cloud
- Malware analysis & threat detection
- Threat hunting (MITRE ATT&CK)
- Cyber threat intelligence (CTI & IOCs)
- InfoSec standards (ISO 27001)
- Data Analysis with KQL, SQL & Python
- Data Encryption and Decryption
- Full Stack Development (MERN Stack)
- Role-Based Access Control and APIs
- Web Application Security & Secure APIs
- Basic Linux & Windows CLI

Certifications & Trainings

ISO 42001:2023 LI
Issued by: BSCIC Pvt. Ltd. , July 2024

ISO 27001:2022 LA
Issued by: BSCIC Pvt. Ltd. , July 2023

ISO 27701:2019 LI
Issued by: Intertek Pvt. Ltd. , June 2023

ISO 27001 LI
Issued by: Intertek Pvt. Ltd. , Sept 2023

AUTOCAD
Issued by: Ielogix training centre, June 2021

Soft Skills

- Problem-Solving & Time Management
- Teamwork & Collaboration
- Initiative & Proactiveness
- Continuous Learning & Multitasking

Summary

Cybersecurity Analyst with hands-on experience in incident response, threat hunting, and security operations using Microsoft Sentinel and XDR. Proven track record of enhancing detection accuracy, automating workflows, and delivering strategic insights for proactive defense. Adept in cloud security, MITRE ATT&CK framework, and full-stack development, bridging security operations with application security expertise.

Work Experience

PwC India (March 2023 – Current)

Areas of responsibility:

- Managed incident response and threat investigation using Microsoft Sentinel and Microsoft XDR tools, including Defender for Endpoint (EDR), MDATP, Defender for Identity (MDI), Microsoft Cloud App Security (MCAS), and Microsoft Defender for Cloud.
- Fine-tuned Sentinel use cases by analyzing client-specific risks, improving detection accuracy, and operational efficiency.
- Utilized KQL for log analysis, threat hunting, root cause analysis (RCA), report generation, and dashboard creation to provide stakeholders with clear visibility into cyber threats and risks.
- Performed regular assessments and optimization of Microsoft Defender for Cloud configurations to enhance threat detection and security posture.
- Automated incident response workflows using Logic Apps, reducing manual effort to improve response time.
- Worked cross-functionally to develop remediation plans for audit findings, leading to improved risk management and reduced vulnerabilities.
- Delivered detailed reports and executive presentations outlining key findings and actionable recommendations, helping clients strengthen their security frameworks and resilience against threats.

Production Engineer at DBG India Pvt. Ltd.

April 2021 – October 2021 (6 Months)

Areas of responsibility:

- Optimized production setups to boost efficiency and output.
- Enhanced product quality and minimized operational downtime.

Education Details

Executive PG Certification in Cyber Security & EH
iHUB DivyaSampark IIT Roorkee **(June 2025 – Current)**

Full Stack Web Development
Masai School, Bangalore **(April 2022 – March 2023)**

B.Tech in Mechanical Engineering
Galgotias University, Greater Noida **(Aug 2016 – June 2020)**