Ankit Sharma

SOAR and SIEM Engineer

4 Years 0 Month

(+91) 9882719062

ankitsharma201297@gmail.com

Key skills

- SIEM & Threat Detection: Microsoft Sentinel (Rule Tuning Custom Detection Use Case Development)
- Endpoint Security: Microsoft Defender for Endpoint (MDE) Defender for Cloud Apps (MDCA) Defender for Identity
- Detection Engineering: Kusto Query Language (KQL) for custom analytical rules
- Incident Response & Investigation: Malware Analysis Phishing Mitigation Threat Intelligence
- Cloud Security & Compliance: NIST CSF MITRE ATT&CK ISO 27001
- Security Automation & Integration: SOAR Playbooks Microsoft Sentinel-ServiceNow Integration
- Vulnerability Management: Nessus Qualys Trellix (McAfee) EPO
- Reporting & Risk Analysis: Security Reports KPI & KRI Dashboards
- Phishing Simulation & User Awareness: CybSafe and Microsoft Defender
- Soar Automation

Personal Information

City	**Greater Noida**
Country	**INDIA**

Languages

- English
- Hindi

Social links

https://www.linkedin.com/in/ankit-sharma-429047190/

Profile Summary

Results-driven Information Security Analyst with 4 years of experience in SIEM, SOAR automation, threat detection, and incident response. Specialized in Microsoft Sentinel and Defender XDR for custom detection rules, alert enrichment, fine-tuning analytical rules, and automated response workflows. Proficient in integrating security tools (SIEM, EDR, ITSM) and developing SOAR playbooks using KQL. Strong background in threat detection, workflow orchestration, and reducing manual workload through automation.

Education

B.Tech/B.E., 2020

Atal Bihari Vagpayee Government Institute Of Engineering And Technology Shimla

Work Experience

Nov 2021 - Present

SOAR and SIEM Engineer

Coforge

- Developed and fine-tuned custom analytics rules in Microsoft Sentinel to detect threats such as brute-force attacks, suspicious login patterns, and Phishing Emails.
- Developed and deployed automated phishing response playbooks in Microsoft Sentinel, integrating Defender for Office 365 and ServiceNow to quarantine emails, notify users, and generate incident tickets.
- Used KQL to enrich alerts and automate containment actions.
- Automated investigation of suspicious login activities using Sentinel analytics rules and Azure AD data, triggering MFA challenges and account lockdowns for high-risk events.
- Integrated Microsoft Sentinel with ServiceNow to auto-create and update incident tickets based on alert severity, reducing manual workload and improving SOC efficiency.
- Designed advanced KQL-based Custom detection rules for Microsoft Defender XDR (MDE, MDCA) to identify phishing URL clicks.
- Reduced false positives by refining detection logic based on feedback from SOC analysts and incident response teams.
- Managed the Microsoft Defender suite, achieving 99 % endpoint protection coverage across the organization.
- Conducted vulnerability assessments using Nessus & Qualys, prioritizing remediation for high-risk CVEs and misconfigurations.
- Created Security reports to provide insights into threat trends, incident volumes, and response effectiveness.
- Enhanced SIEM efficiency through content enrichment and detection logic improvements, improving alert fidelity and analyst productivity.
- Administered Microsoft Defender for Endpoint, managing security

policies and configurations.

- Implemented targeted use cases, including Web Content Filtering to block access to non-compliant or malicious websites. Network Protection to prevent outbound traffic to known malicious IPs/domains. Email Scanning to detect phishing and malware in inbound communications. SmartScreen for Microsoft Edge protects users from unsafe downloads and URLs.

Certification

- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Vulnerability Management, Detection, and Response (VMDR
- Cyber Security Solutions and Microsoft Defender