Bishal

7009828997|bishalsapkota0001@gmail.com|

Professional Summary

Experienced SOC Analyst with over **3 years** of expertise in security incident response, **vulnerability management**, and **compliance monitoring**. Skilled in **Microsoft Defender, Intune, Microsoft Sentinel**, and collaboration policy enforcement, with a proven track record of safeguarding critical data and ensuring regulatory **compliance**.

Skills

- **Security Monitoring:** Experience with SIEM tools **Microsoft defender**, **Microsoft sentinel** and log analysis for threat detection.
- **Incident Response:** Basic skills in triaging and escalating security incidents.
- **Endpoint & Network Security:** Knowledge of endpoint protection, network protocols, and IDS/IPS.
- **Vulnerability & Email Security:** Basic vulnerability assessment and email threat monitoring.
- **Technical Skills:** Basic scripting with PowerShell for automation and analysis.
- **Communication & Compliance:** Effective documentation, team collaboration, and understanding of compliance frameworks.
- **Implemented NIST 800-53 Controls:** Conducted compliance assessments and ensured alignment with NIST 800-53 standards, enhancing organizational cybersecurity posture.
- **Data loss prevention:** Prevent from stealing data, Protect from unauthorized person.

Work Experience:

SOC Analyst

De Facto Infotech 11/2021 - Present

Responsibilities:

- **Monitor and respond to security incidents** using **Microsoft Defender**, managing **alerts**, **incidents**, and **vulnerability assessments**.
- **Handle email monitoring**, **indicators management**, and **endpoint management** to ensure a **secure enterprise environment**.
- **Manage and configure Microsoft Intune** for **mobile device management**, **compliance policies**, and **security baselines**.
- **Implement security and compliance policies** using **Microsoft Compliance Manager**, including creating **Information Barriers**.
- **Maintain security monitoring and incident response** for **Azure services**, ensuring effective **monitoring** and **remediation** across **cloud infrastructure**.
- **Execute vulnerability management**, identifying, assessing, and **mitigating risks** across the organization.
- **Microsoft Sentinel:** Security monitoring, **playbook** automation, data connector configuration, incident management.

Projects:

Experience with Azure Cloud and Microsoft Defender:

- **Virtual Machine (VM) Deployment**: Created and configured **Virtual Machines (VMs)** in the **Azure Portal**, including **OS**, **disk**, and **networking** configuration.
- **Security Integration**: Onboarded **Azure VMs** into **Microsoft Defender** for **cloud security monitoring**, enabling **threat protection**, **vulnerability management**, and **endpoint security**.
- **User Management**: Managed **user accounts** assigned **roles** and configured **security policies** for **VM** access and **compliance**.

Automated Security Tasks:

- Developed and deployed **PowerShell scripts** to automate **security operations**, including **log aggregation**, **alert management**, and **report generation**.
- Utilized **Windows PowerShell** and **Task Scheduler** to enhance **operational efficiency** and **incident response capabilities**.

Experience with Microsoft Intune:

- **Windows Updates Deployment** Managed and deployed **Windows updates** across devices using **Microsoft Intune**, ensuring system security and compliance.
- **Policy Management** Created and enforced **security policies**, including **device configuration, update schedules**, and **compliance policies** to manage **Windows endpoints** efficiently.
- **Device Management** Used **Intune** for **device monitoring**, managing **updates** and ensuring devices met **compliance** standards.

Education

Bachelor’s degree in computer science
Doaba Group of colleges 2019-2021

Certification

- **Microsoft Certified: Azure Security Engineer Associate (AZ-500)**

Language : English **,** Hindi