KOUSHIK KUILA

L1 Security Analyst, currently in Kolkata and working in UCO Bank Datacentre in SOC L1 profile for SIEM Tools

+91-8016250389

koushikkuila8016@gmail.com

CARRIER OBJECTIVE:

To be the part of an Enthusiastic Work Environment, where I can use my technical skills to accomplish my Dreams.

Company 1: CMS IT

Client: UCO Bank

Duration: June 2024 to Jan 2025

Profile: L1 Security Analyst

Tool: ArcSight, WAF, DLP, NAC

Summary:

➢ Incident assigning & alert investigation.

➢ Prepared weekly, monthly, quarterly, half and yearly reports.

➢ Investigate and solves security breaches and other cyber security incidents and provide incident response.

➢ Results-oriented professional experience on ArcSight.

➢ On-Call Support function (responding to incidents off regular working hours and weekends/holidays)

➢ Malware analysis, log analysis, SIEM log analysis utilizing Enterprise Products

➢ Preparing roaster and providing assurance of availability of analyst 24*7 without any fail.

➢ Understanding of SIEM component which collect, process, model, prioritize, correlate, monitor, and

➢ Navigate the SIEM console to effectively correlate, investigate, analysis and remediate both exposed and

obscure vulnerabilities to give situational awareness and real time incident response.

➢ Generation of report on daily basis.

➢ Document and report security breaches and assess the damage they cause.

➢ Analysing the security breaches for determining their root cause for resolving the same.

➢ Analysing network traffic through a SIEM tool.

➢ Dynamic access control over super users creates an added security layer. Protects against critical error

statements which can lead to significant down time, thus loss of business.

➢ Provides security arc over all IT Assets in the organization through RDP connection.

➢ Enhances security posture from internal threats and makes it impregnable for cyber attackers.

Company 2: Hitachi System

Client: UCO Bank

Duration: Feb 2025 to Till Now

Profile: L1 Security Analyst

Tool: DAM(Imperva)

Summary:

□ **Monitor Database Activity:**

- Track database user logins, logoffs, and activity sessions.
- Review and report on database queries and transactions executed.

□ **Review Alerts:**

- Respond to and escalate alerts related to unusual activity, failed login attempts, or database errors.
- Ensure alerts from database monitoring tools (such as IDS/IPS systems) are reviewed and followed up on.

□ **User Activity Tracking:**

- Monitor user permissions and database access controls.
- Review and report on user activity, ensuring it aligns with policies and access requirements.

□ **Audit Log Management:**

- Monitor database logs for security and compliance purposes.
- Ensure audit logs are correctly configured and securely stored.

□ **Compliance Checks:**

- Verify compliance with security policies, industry standards (e.g., GDPR, HIPAA), and regulations.
- Ensure that all necessary monitoring and auditing configurations are in place to meet these requirements.

□ **Basic Troubleshooting:**

- Troubleshoot basic database performance issues, such as query slowdowns or deadlock situations.
- Escalate more complex database issues to higher-level support (L2/L3).

□ **Generate Reports:**

- Prepare and review activity reports for security or compliance audits.
- Create regular reports summarizing database usage patterns, suspicious activity, or policy violations.

□ **Access Control Review:**

- Assist in reviewing and managing user roles, permissions, and access controls.
- Help ensure that only authorized users have access to sensitive data.

□ **Assist with Incident Response:**

- Support database security teams in investigating security incidents or breaches.
- Provide logs, access details, or other monitoring data to help diagnose issues.

□ **Routine Database Monitoring Tasks:**

- Conduct scheduled checks of database monitoring systems for normal operations.
- Ensure that monitoring tools are functioning properly and collecting the necessary data.

EDUCATIONAL QUALIFICATION:

COURSE	BOARD	COLLEGE/SCHOOL	YEAR	SCORE
Bachelor of Technology (Electrical Engineering)	MAKAUT	OmDayal Group of Institutions	2021-2024	8.01CP
Diploma In Electrical Engineering	W.B.S.C.T.E.	Contai Polytechnic	2018-2021	8.4 CP
Senior Secondary Education	W.B.C.H.S.E.	Panskura Bradley Birt High School	2018	69.60%
Secondary Education	W.B.B.S.E.	Panskura Bradley Birt High School	2016	72.42%

TECHNICAL SKILLS:

Microsoft Applications	Excel, Power Point, Word, Office etc.
Operating System	Windows XP/7/8/10.
Database	Basic of SQL.
Web Technology	HTML, CSS.

STRENGTH:

Quick Learner, Self Confidence, Communication Skills, Positive Attitude.

HOBBIES:

Bike Ride & Travelling New Adventure Places about Ancient Indian History and Facts.

DECLARATION:

I hereby declare that the above-mentioned particulars are true to be the best of my knowledge and belief.