DTB

DIAMOND
TRUST
BANK

1. JOB TITLE: Identity Access Management (IAM) Officer

Job Purpose

The Identity and Access Management (IAM) work unit is responsible for how users within the Bank are given an identify and how is protected, including saving critical applications, data and systems from unauthorized access while managing the identities and access rights of people both inside and outside the organization.

Key Responsibilities:

- Administer user accounts and access privileges in the Bank’s identity management system.
- Work closely with the teams to ensure that the right people have access to the right resources.
- Responsible for the day-to-day administration of the IAM system.
- Involved in troubleshooting and resolving IAM issues.
- Participate in IAM projects and initiatives.
- Work with internal customers, business analysts, and application teams to understand access requirements.
- Maintain documentation for the IAM program.
- Participate in IAM audits and review access control reports to identify potential risks.
- Provide training to new users on the IAM system.
- Update and maintain the IAM system according to changes in the Bank’s business needs.
- Managing user accounts and permissions in the identity and access management system.
- Granting or denying access to the Banks' resources based on user role and privileges.
- Creating and managing user groups in the identity and access management system.
- Enforcing company policies and procedures related to identity and access management.
- Monitoring user activity in the identity and access management system.

- Reporting on identity and access management system activity.
- Identifying and addressing identity and access management issues.
- Working with the teams to resolve identity and access management problems.
- Maintaining up-to-date knowledge of identity and access management best practices.
- Documenting IAM processes and procedures.
- Any other Cybersecurity tasks given by the line manager.

Qualifications

- University degree Computer Science and other ICT related courses.

Work Experience

- At least 3 years working experience in Business/IT Applications Support.
- Familiarity with service delivery culture and support function.

Personal Attributes

- A structured approach to dealing with complex and variable work environments in an independent manner.
- Ability to balance opposing business requirements.
- Ability to balance long term and short-term requirements independently.
- Strong evaluation, communication and reporting skills
- Able to provide advice and cause/effect evaluation to support business decision making.
- Independent and logical thinker, yet an achiever and implementer.
- Strong ethic
- Lead by example
- Good at managing large volumes of information and can add value through management reporting.
- Builds relationships and networks easily.

Key Performance Indicators

- Alignment of staff responsibilities versus system access rights.
- Alignment of Privileged access rights versus access required by relevant DTB Staff.
- Regular reviews of system access rights.
- Reporting of the various activities undertaken and as directed by the IAM team lead from time to time.

Performance Evaluation

June & December.

2. JOB TITLE: Security Operations Centre (SOC) Analyst

Job Purpose

The main purpose of the SOC Analyst L2 is to deal with the security incidents which are detected and to lead in-depth analysis on these incidents.

Key Responsibilities:

- Investigates deeper on the detected behaviors when an incident is escalated by the SOC level 1 analyst.
- Add context to the incident to understand the behavior, analyzing data from multiple tools and data sources.
- Participates to the crisis management by providing support to the incident handler and the SOC Level 3 analysts.
- Create reports and visualizations of security attacks.
- Works on the decrease of false positives.
- Maintain the detection rules database.
- Vulnerability Assessment and Penetration testing.
- Threat Hunting and Threat Intelligence.
- Any other Cybersecurity tasks given by the line manager.

Qualifications

- University degree Computer Science and other ICT related courses.

Work Experience

- At least 3 years working experience in SOC/Cybersecurity.
- Proficient in Incident Management and Response.
- In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management etc.
- Able to work in a 24x7 Security Operation center (SOC) environment.

Personal Attributes

- Strong Data Analysis Skills.

- Solid Sense of Logic.
- Ingenuity
- Skilled Problem Solver
- Orientation to Detail
- Independent and critical thinker, yet an achiever and implementer.
- Strong ethic
- Lead by example

Key Performance Indicators

- Number of Total Alerts: How many alerts have been received.
- Number of Reported Incidents: How many incidents are reported within a certain timeline.
- Number of Open Alerts Escalated: How many open alerts were escalated further.
- Number of devices being monitored: How many devices are being monitored.
- Number of events per analyst: How many events were addressed by an analyst.
- Number of false positives alerts: How many false positive alerts did SOC encounter in a week/month.
- Mean Time to Detect (MTTD): How long it takes to become aware of a potential security incident.
- Mean Time to Respond (MTTR): How long is it taking to resolve an actual security incident.
- Mean Time for Investigation: How long is it taking to complete an investigation process.

Performance Evaluation

June & December.

Applications should be submitted to

recruitment2023@diamondtrust.co.tz

DTB is an equal opportunity employer.