VIT CHENNAI ECDS L&T EduTech

DATAQUEST 2.0

DQCS_2

Insider Threat Detection Using User Behavior Analytics (UBA)

Problem Statement:

Insider threats are difficult to detect as they originate from trusted employees or contractors with legitimate access to systems. The goal is to develop an AI-powered system that continuously monitors user activities, including file access, login times, and application usage, to detect abnormal patterns indicating malicious intent or policy violations, and to alert security teams in real time.

How to Solve:

• Collect endpoint and network logs covering file access, login/logout times, application usage,
and system commands.
• Apply anomaly detection algorithms like Isolation Forest and Autoencoders to identify deviations
from typical behavior.
• Flag activities such as unusual login times, mass data downloads, or privilege escalations.
• Visualize anomalies and alerts on an intuitive dashboard for SOC teams to investigate.

“Wishing you all the very best for the hackathon. May your hard work, creativity, and teamwork lead you to great success.”