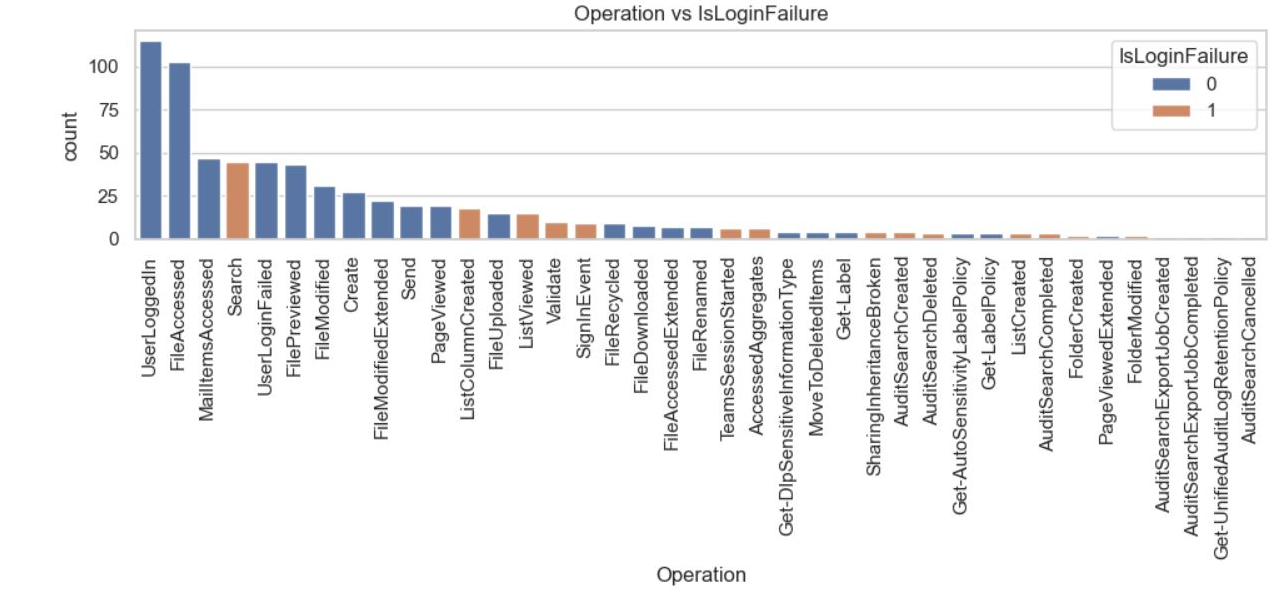
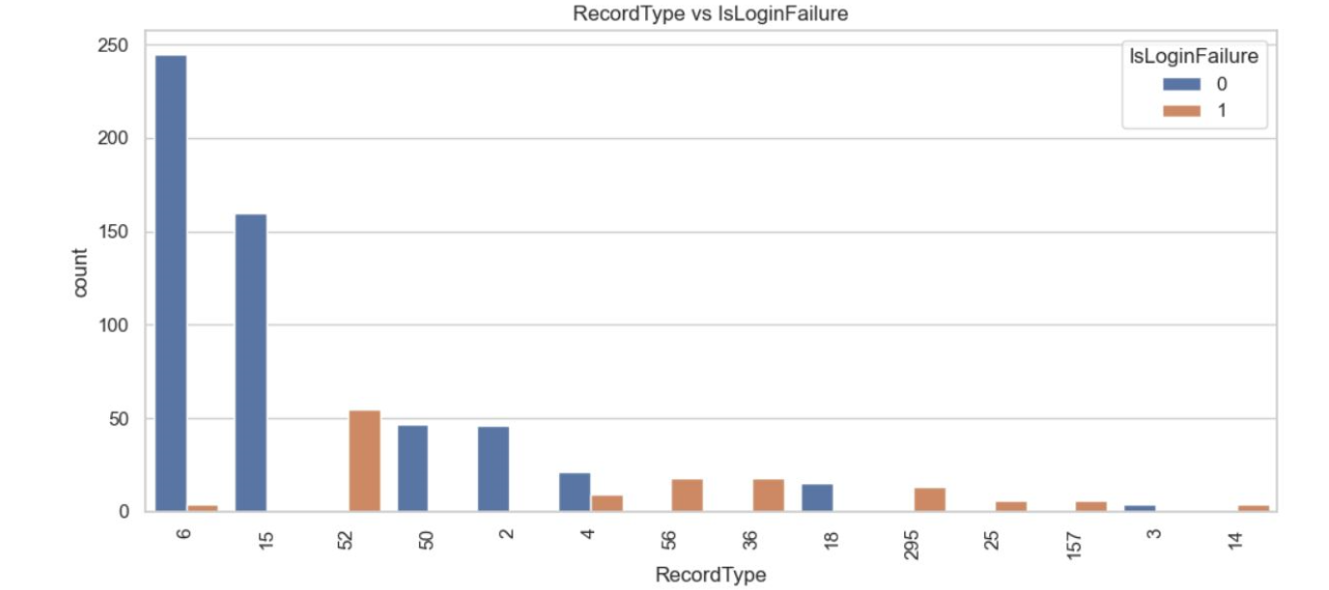
**Bivariate Analysis Report** based on the bar charts, focusing on categorical columns from dataset:

1. **Operation vs IsLoginFailure**



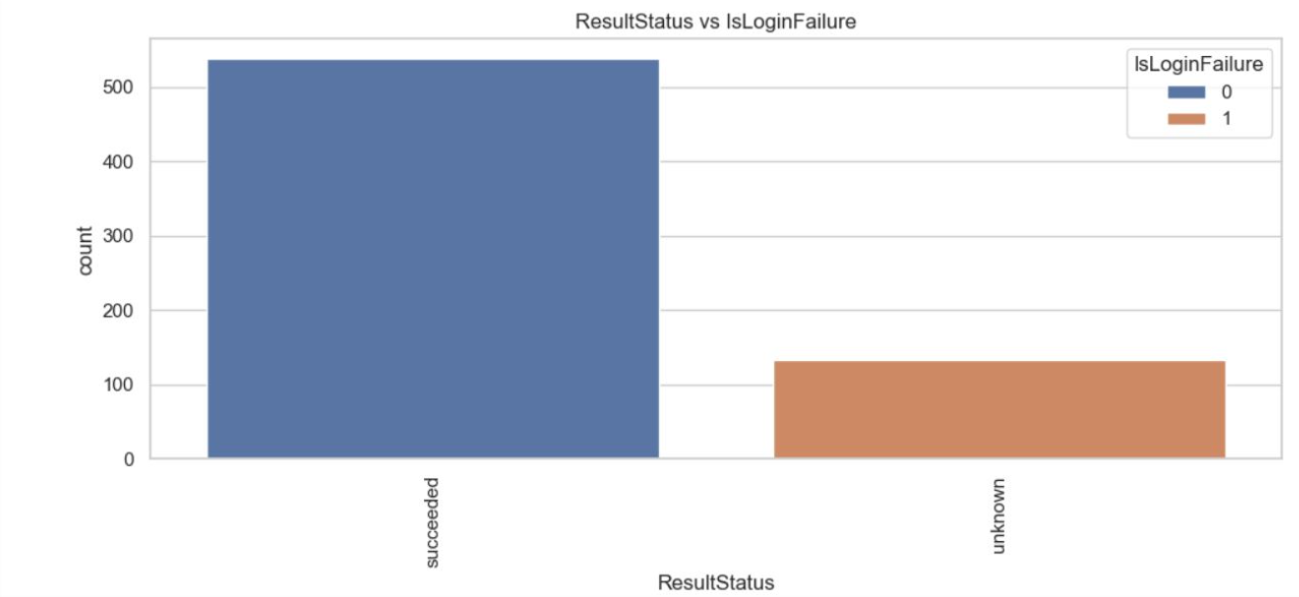
* **Key Insight**:
  + UserLoggedIn and FileAccessed are the most frequent operations.
  + The majority of operations are successful (IsLoginFailure = 0).
  + UserLoginFailed, MailItemsAccessed, and Search have significant IsLoginFailure = 1 values.
* **Conclusion**:
  + Login failure is more associated with UserLoginFailed, which is expected.
  + Other suspicious activities like Search and MailItemsAccessed with login failures might indicate malicious intent.

**2. RecordType vs IsLoginFailure**



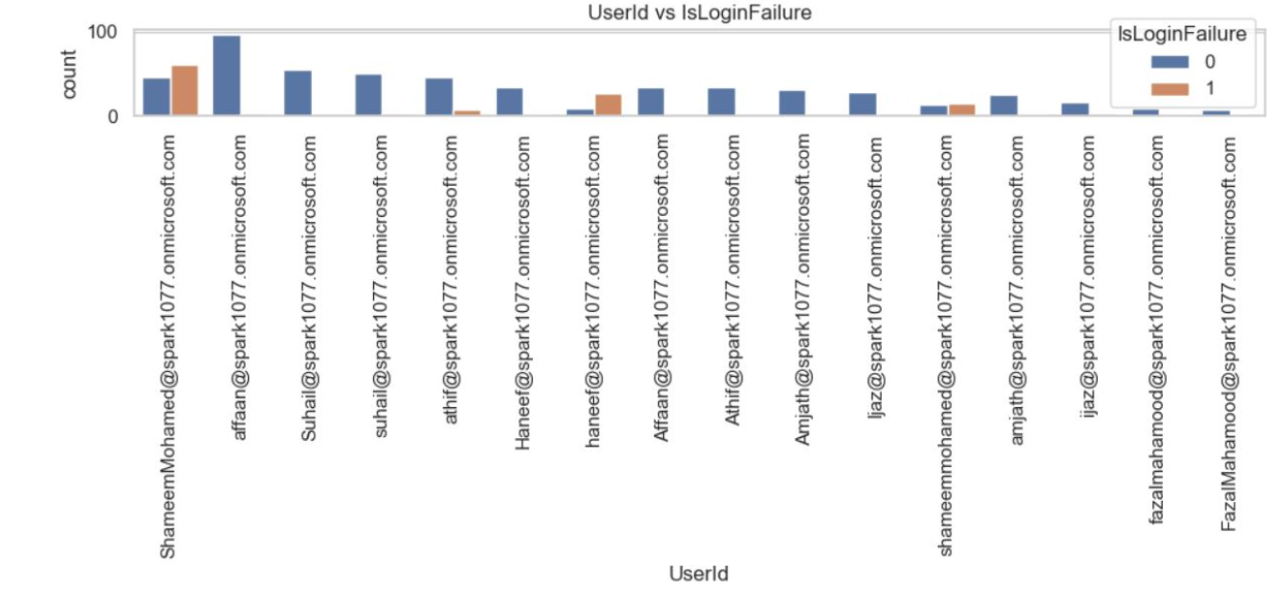
* **Key Insight**:
  + RecordType 6 and 15 are mostly successful.
  + RecordType 52 and 56 have more login failures.
* **Conclusion**:
  + RecordType 52 and 56 may require investigation or alerts, as they show a higher ratio of failed login attempts.
  + RecordType 6 is most common and mostly safe.

**3. ResultStatus vs IsLoginFailure**



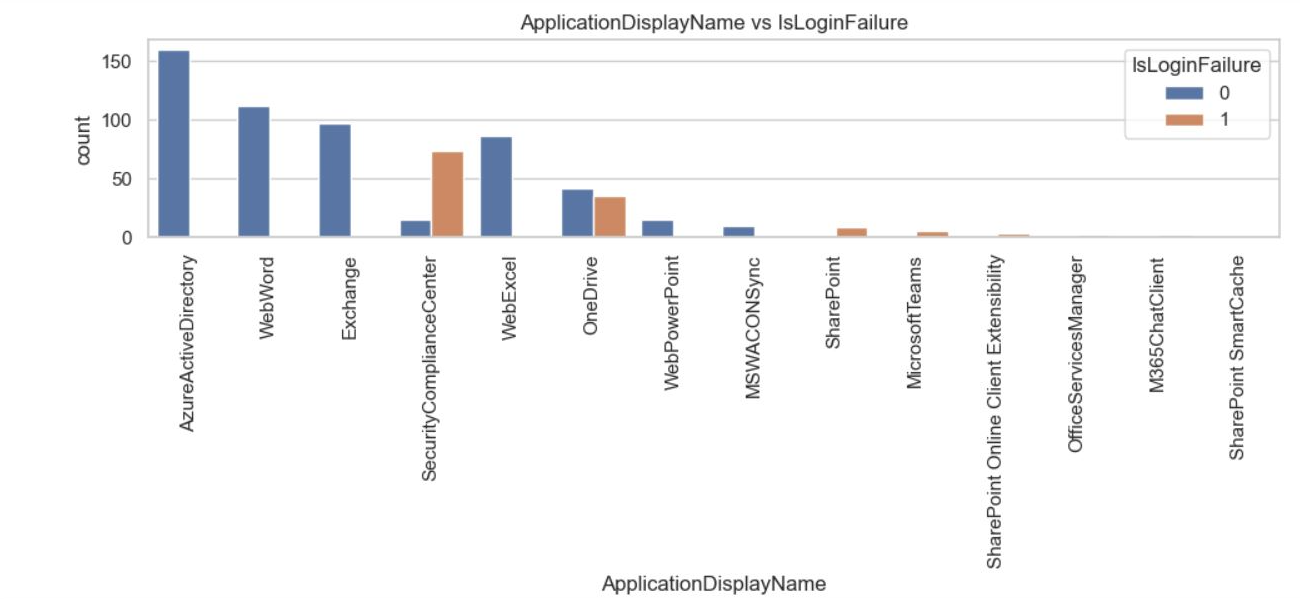
* **Key Insight**:
  + succeeded status is fully associated with IsLoginFailure = 0.
  + unknown status appears **only** with IsLoginFailure = 1.
* **Conclusion**:
  + All login failures are marked with ResultStatus = unknown, which could be used as a strong indicator of failed/malicious attempts.

**4. UserId vs IsLoginFailure**



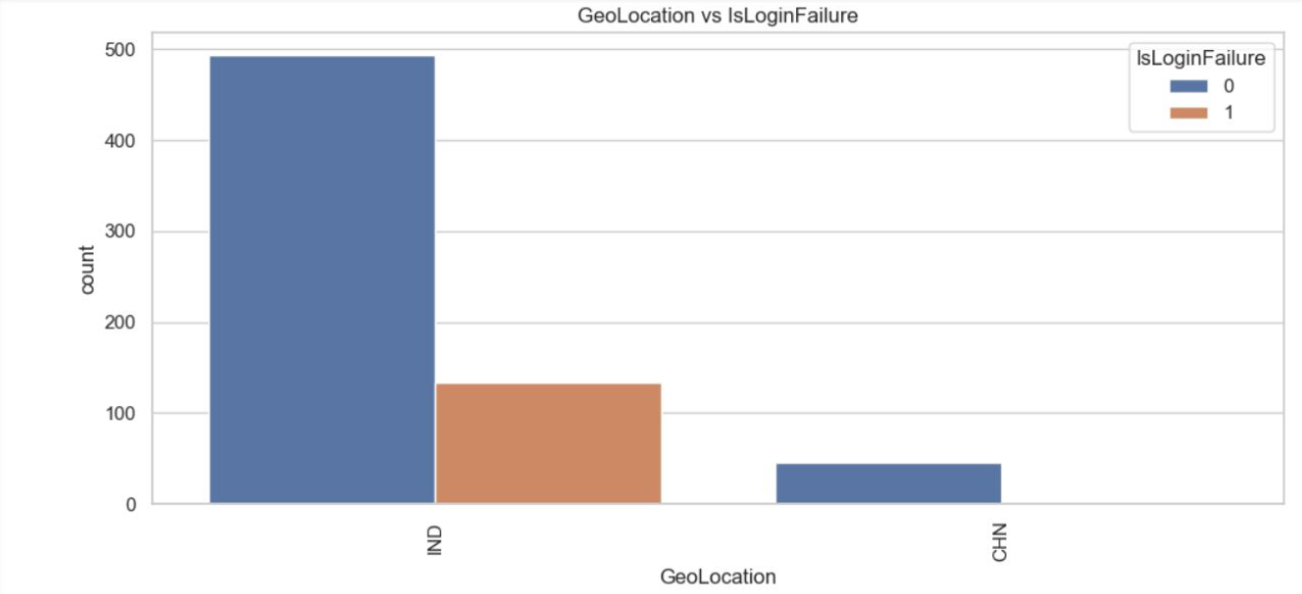
* **Key Insight**:
  + Most users have more successful than failed logins.
  + Few users (e.g., ShameemMohamed, Haneef) show failed login attempts.
* **Conclusion**:
  + Failed login attempts are not widespread, but a few specific users may be experiencing issues or could be targets of brute-force attempts.

**1. ApplicationDisplayName vs IsLoginFailure**



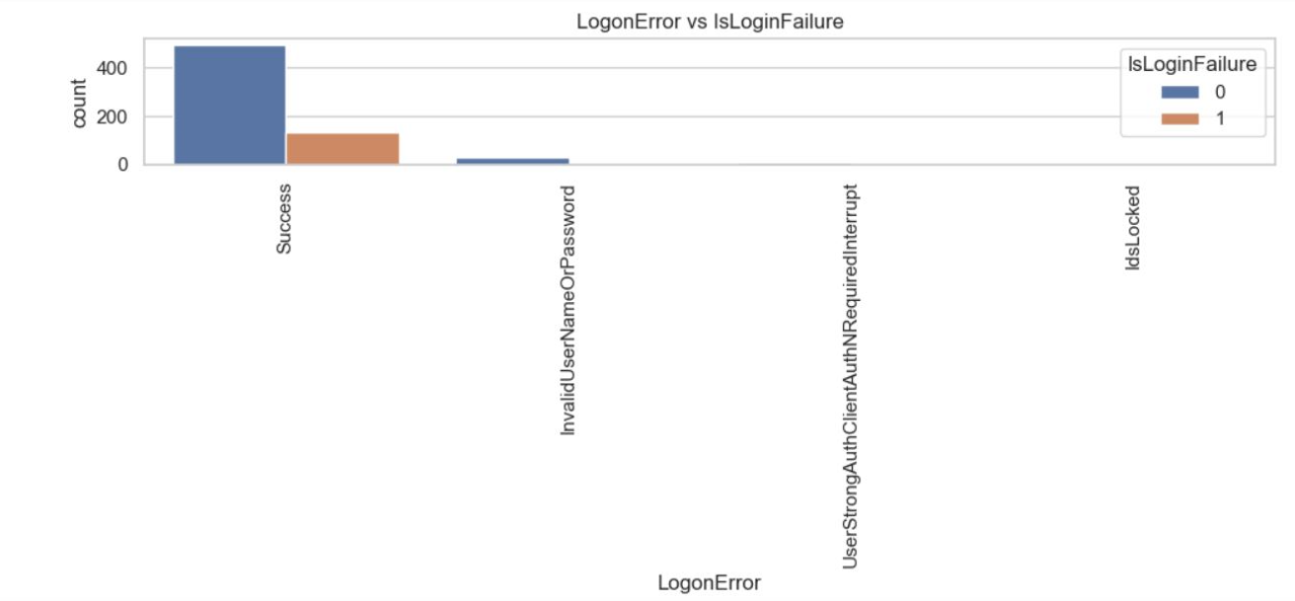
* **Key Insights**:
  + Most successful logins (IsLoginFailure = 0) are from AzureActiveDirectory, WebWord, and Exchange.
  + High login failures (IsLoginFailure = 1) are observed in SecurityComplianceCenter, followed by WebExcel and OneDrive.
* **Conclusion**:
  + SecurityComplianceCenter is a notable risk point due to its high login failure count, suggesting it should be monitored for unauthorized access attempts.

**2. GeoLocation vs IsLoginFailure**



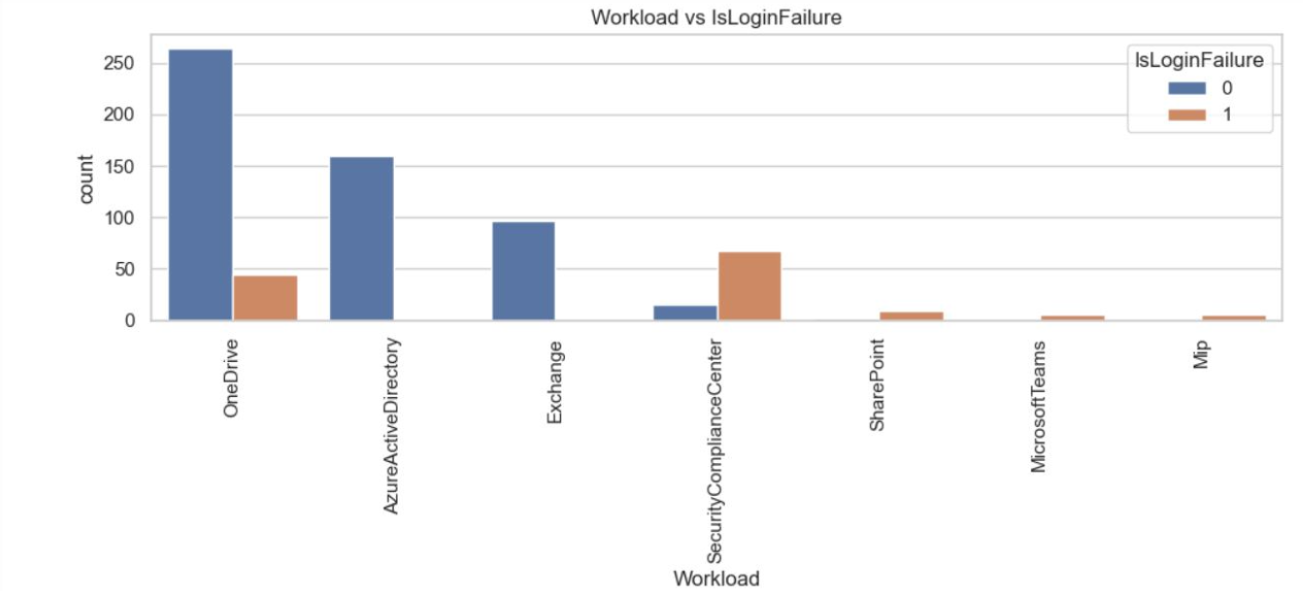
* **Key Insights**:
  + The majority of activity (both successful and failed) is from **India (IND)**.
  + All activities from **China (CHN)** are successful.
  + A substantial number of login failures are observed from **India**.
* **Conclusion**:
  + Login failures are mostly domestic (IND). Geo-based anomaly detection can be helpful, but location alone isn’t a clear threat indicator here.

**3. LogonError vs IsLoginFailure**



* **Key Insights**:
  + Most Success logons are marked as IsLoginFailure = 0, which is expected.
  + However, **some logons with Success still have IsLoginFailure = 1**, which is unusual and may point to data quality issues or inconsistent labeling.
  + Errors like InvalidUserNameOrPassword, UserStrongAuthClientAuthNRequiredInterrupt, and IdsLocked are purely associated with IsLoginFailure = 1.
* **Conclusion**:
  + Errors such as InvalidUserNameOrPassword are strong indicators of failed login attempts.
  + Any mismatch between LogonError = Success and IsLoginFailure = 1 needs investigation or data cleanup.

**4. Workload vs IsLoginFailure**



* **Key Insights**:
  + Most successful logins come from OneDrive and AzureActiveDirectory.
  + The highest failure count is in SecurityComplianceCenter, just like in the previous chart.
  + Minor login failures observed in SharePoint, MicrosoftTeams, and Mip.
* **Conclusion**:
  + SecurityComplianceCenter again emerges as a high-risk workload with elevated login failures.
  + OneDrive is frequently used, with relatively low failure rates—likely a common trusted service.