Following are several test scenarios that can be used to manipulate the behavior of different predictors and generate diverse risk scores. These scenarios focus on the factors that influence the predictors. By testing these scenarios, we can evaluate how the various predictors contribute to the overall risk score.

**1. GeoVelocity Anomaly**

* **Objective**: Test for LOW, MEDIUM, and HIGH values.
* **Scenarios**:
  + **LOW**: Log in from the same location or within a short travel distance.
  + **MEDIUM**: Log in from a different location within the same country or nearby countries (e.g., neighboring states).
  + **HIGH**: Simulate logins from two geographically distant locations within an implausible time frame (e.g., log in from the US and then quickly from Europe).

**2. User Location Anomaly**

* **Objective**: Test known, new, and unexpected locations.
* **Scenarios**:
  + **LOW**: Log in from a frequently used or previously seen location.
  + **MEDIUM**: Log in from a new but plausible location (e.g., a different city within the same country).
  + **HIGH**: Log in from an unexpected or high-risk location (e.g., a country with restricted or suspicious activity).

**3. Anonymous Network Detection**

* **Objective**: Detect anonymous or public networks.
* **Scenarios**:
  + **LOW**: Log in from a regular ISP or private network.
  + **HIGH**: Use a VPN, proxy, or TOR browser to simulate anonymous network activity.

**4. IP Reputation**

* **Objective**: Test IP addresses with different reputations.
* **Scenarios**:
  + **LOW**: Use an IP address from a trusted ISP or a static IP with no malicious history.
  + **MEDIUM**: Use a dynamic IP that has a neutral or moderately suspicious history.
  + **HIGH**: Use a public, blacklisted, or known proxy IP to simulate malicious activity.

**5. IP Velocity**

* **Objective**: Test velocity of activity from the same IP.
* **Scenarios**:
  + **LOW**: Log in a few times from the same IP within a reasonable time frame.
  + **MEDIUM**: Simulate moderate activity by multiple users sharing the same IP.
  + **HIGH**: Simulate high activity (e.g., automation or bots) using multiple concurrent logins from the same IP.

**6. New Device**

* **Objective**: Test known and unknown devices.
* **Scenarios**:
  + **LOW**: Log in from a recognized device (same browser and OS).
  + **HIGH**: Use a completely new device or clear browser cookies and cache to simulate an unknown device.

**7. User Velocity**

* **Objective**: Test user activity levels from multiple IPs.
* **Scenarios**:
  + **LOW**: Log in a few times within a short period from the same IP.
  + **MEDIUM**: Use 2–3 different IPs to log in within the evaluation period.
  + **HIGH**: Log in from multiple distinct IPs within a short time, simulating suspicious velocity.

**8. User-Based Risk Behavior**

* **Objective**: Test behavioral patterns for anomalies.
* **Scenarios**:
  + **LOW**: Perform regular login behavior (e.g., consistent device, location, and login frequency).
  + **MEDIUM**: Simulate slightly unusual behavior (e.g., log in at an odd time or from a less common device).
  + **HIGH**: Perform highly irregular actions, such as multiple failed login attempts, rapid session switches, or erratic device changes.

**9. Country Filter**

* **Objective**: Test country-specific restrictions.
* **Scenarios**:
  + **LOW**: Log in from an allowed country.
  + **HIGH**: Log in from a restricted or high-risk country based on policy settings.

**10. Impossible Travel**

* **Objective**: Test impossible travel scenarios.
* **Scenarios**:
  + **LOW**: Log in sequentially from locations within a plausible travel range.
  + **HIGH**: Log in sequentially from distant locations within a short period (e.g., log in from the US and immediately from Asia).

**11. User Velocity by IP**

* **Objective**: Test activity levels per user for a single IP.
* **Scenarios**:
  + **LOW**: Log in a few times from the same IP.
  + **MEDIUM**: Log in with moderate frequency from the same IP within the time frame.
  + **HIGH**: Simulate high-frequency activity from a single IP.

**12. IP Velocity by User**

* **Objective**: Test activity levels per user across multiple IPs.
* **Scenarios**:
  + **LOW**: Use 1–2 IPs for logins in a short time frame.
  + **MEDIUM**: Use 3–5 IPs for logins in the evaluation period.
  + **HIGH**: Use 6+ IPs for logins within a short time, suggesting shared credentials.

**13. Risk Combination Testing**

* **Objective**: Test cumulative risk scores.
* **Scenarios**:
  + Simulate a combination of HIGH GeoVelocity, HIGH Anonymous Network, and LOW User-Based Behavior to observe how scores aggregate.
  + Test with combinations of MEDIUM scores across multiple predictors to observe cumulative impact.

**14. Previous Transaction Details**

* **Objective**: Test scenarios involving historical data.
* **Scenarios**:
  + Use a new device from a previously unseen IP.
  + Use an old device but log in from a previously successful transaction IP.

**15. Browser and OS Testing**

* **Objective**: Test device fingerprinting capabilities.
* **Scenarios**:
  + Log in from commonly used browsers like Chrome or Safari.
  + Log in from lesser-known browsers to see if they are flagged.

**16. Device Attributes**

* **Objective**: Test new and known device scenarios.
* **Scenarios**:
  + Log in with a recognized device ID.
  + Change the browser, OS, or device to simulate an unknown or unrecognized device.

**17. Proxy Detection**

* **Objective**: Test proxy-related scenarios.
* **Scenarios**:
  + Use a regular connection with no proxy.
  + Enable a proxy or VPN to simulate anonymous behavior.

**18. High-Volume Testing**

* **Objective**: Test predictors under heavy traffic conditions.
* **Scenarios**:
  + Simulate multiple users logging in from the same IP.
  + Use multiple IPs for the same user to test velocity predictors.