

# Adaptive Authentication

---

A Risk-based Authentication System

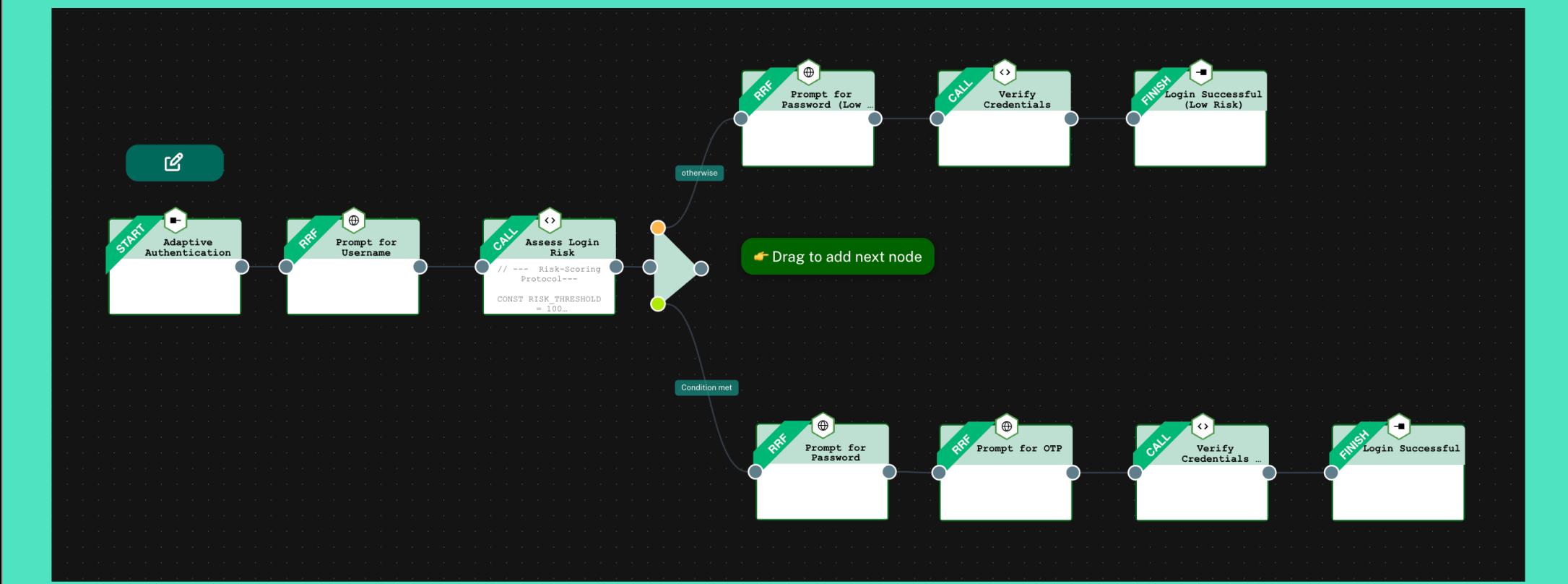
by Ryan Ramirez





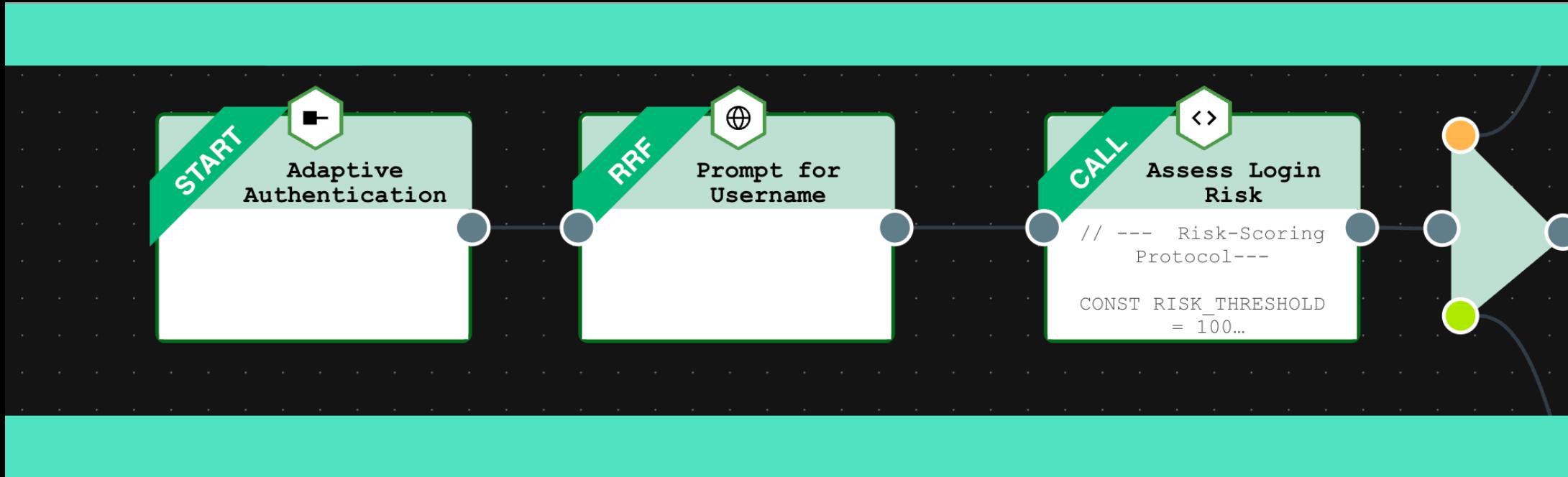
## Objective

- To design a risk-based authentication system that enhances security against high-risk login attempts while preserving a frictionless experience for trusted users.



# Authentication Flow

- This flow is divided into three phases: Identification & Risk Assessment, The Adaptive Decision Path, and Credential Verification.
- Based on the initial risk assessment, the user is directed down one of two paths:
  - Low-Risk: A frictionless, single-factor (password) verification.
  - High-Risk: A Multi-Factor approach to authentication (Password + OTP).



## Phase I: Identification & Risk Assessment

- The flow begins by collecting the user's primary identifier
- A CALL node delegates then executes the risk assessment logic
- The logic for the risk assessment is defined as pseudocode within the node.

# Risk Assessment Logic

- This pseudocode uses a flexible risk-scoring model
- It evaluates multiple risk signals including device IP, New Device, and Impossible Travel
- It then makes a final decision based on the risk scoring threshold.

```
// --- Risk-Scoring Protocol---

CONST RISK_THRESHOLD = 100

FUNCTION analyze(username, request_context):
    risk_score = 0

    // 1. Check IP Reputation (High Impact)

    IF is_ip_blacklisted(request_context.ip_address)
THEN
    risk_score += 90
END IF

    // 2. Check for New Device (High Impact)

    IF is_new_device_for_user(username, request_context.device_fingerprint) THEN
        risk_score += 75
    END IF

    // 3. Check for Impossible Travel (Critical Impact)

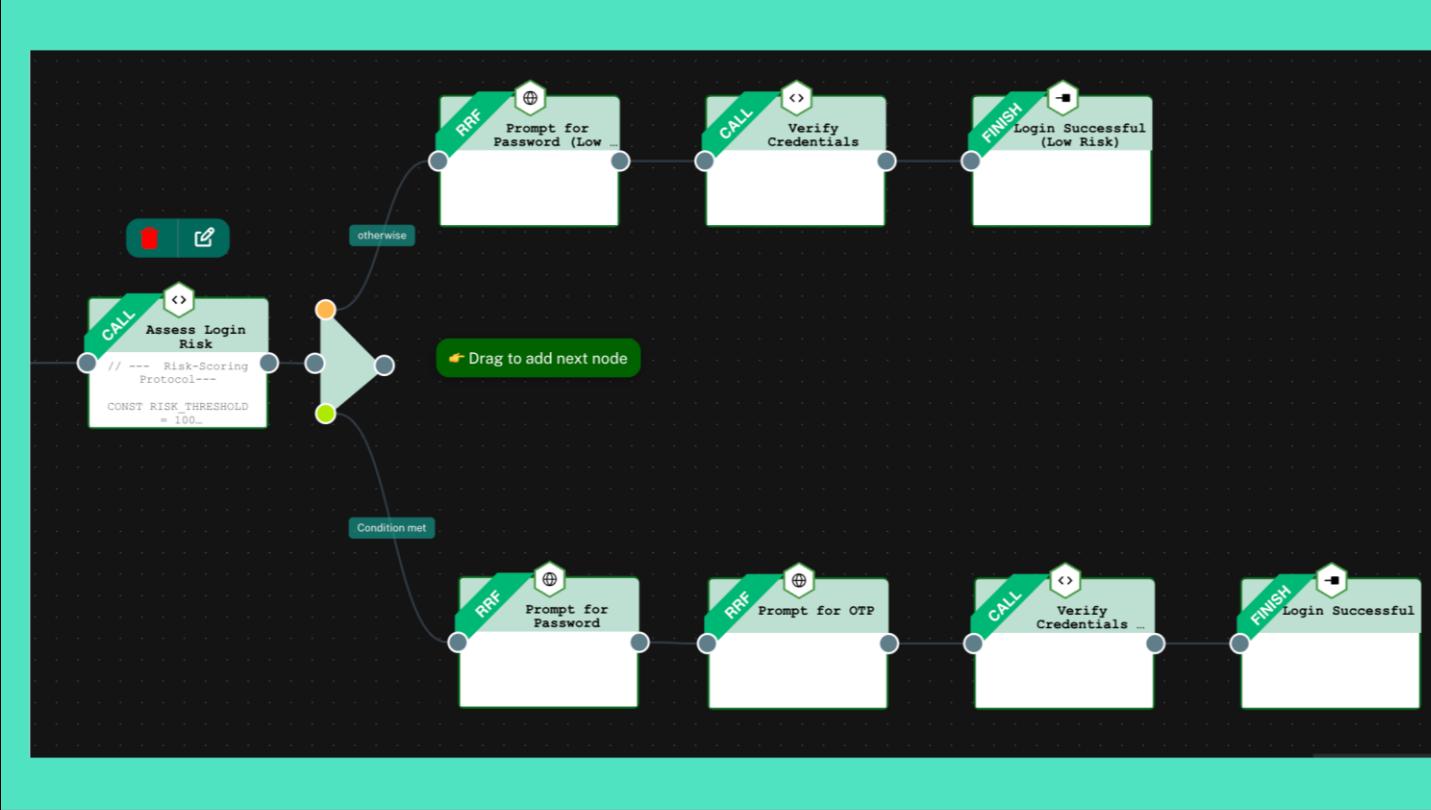
    IF is_impossible_travel(username, request_context.location)
THEN
        risk_score += 150
    END IF

    // 4. Check for Atypical Login Time (Medium Impact)

    IF is_atypical_login_time(username, request_context.timestamp)
THEN
        risk_score += 30
    END IF
    | // 5. Decision

    IF risk_score >= RISK_THRESHOLD
THEN
    RETURN "high"
ELSE
    RETURN "low"
END IF
```

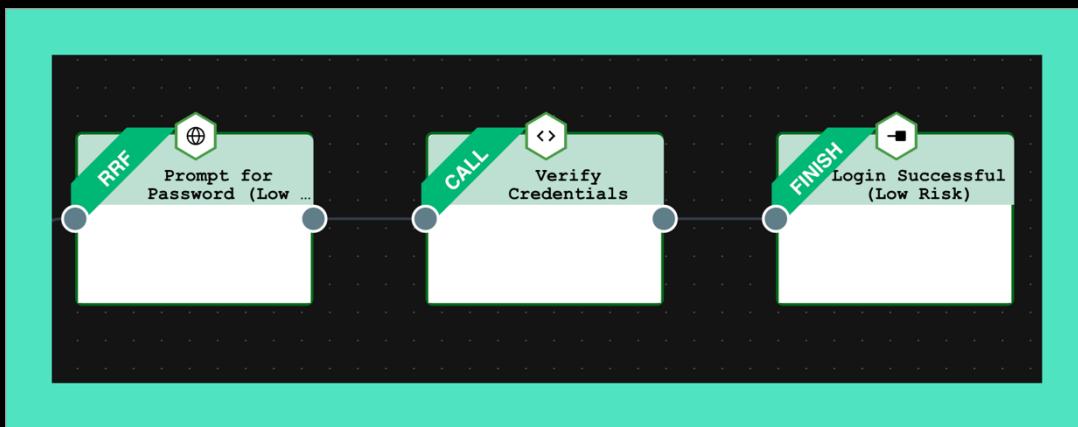
## Phase II: The Adaptive Decision



- The WHEN node acts as the decision point of the flow
- It evaluates the risk level from the risk assessment
- The user is then taken through either the high risk or low risk path.

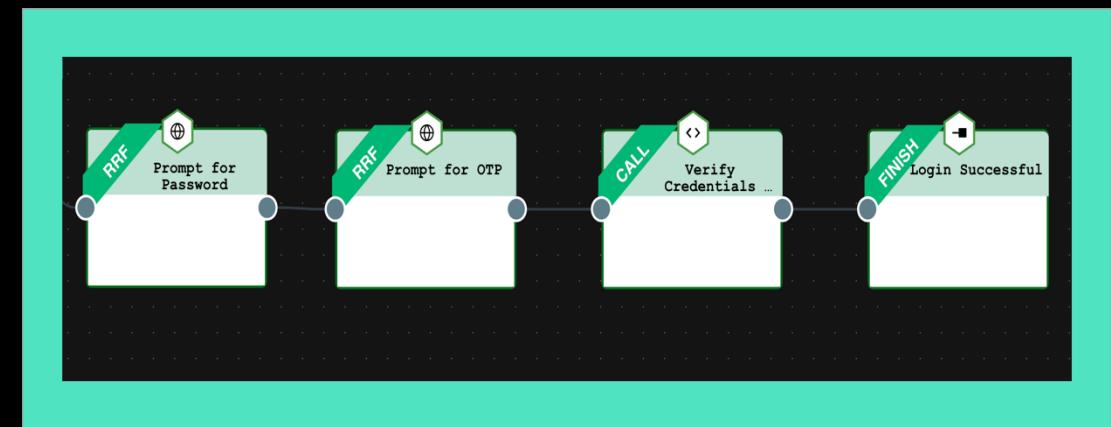
# Phase III: Credential Verification

Low-Risk Path



Password Only

High-Risk Path



Password + OTP