1) As described here, we need to create the token by by concatenating the Client ID, a single colon (:) character, and the Client Secret. The result is then enconded using base64, sending a post request to https://api.incognia.com/api/v2/token

Request:
curl --location --request POST 'https://api.incognia.com/api/v2/token' \
--header 'Content-type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic
UFFpX0p6M0ZKdUR0dVd4dFhyYWlPNGE5bnF4LVQwU2w6YlgzYl8wTnBsUmJxWEZyZUN2d
UI3OFE2a0JUOTQ0RWwtaHZaSzZWMFVreDQ0VEVzc3VicWVqTERRY0J1TnYxbA=='

Response:


{
"access_token":
"eyJ4NXQjUzI1NiI6IlphSFQxaUtGcFZoejIyd3ItWEk4V3kyal9mZlBOdmZXUDVHU1FPdzRuT3M
…",
"expires_in": "900",
"token_type": "Bearer"
}


2) To get the login risk assessment, we need to POST to https://api.incognia.com/api/v2/authentication/transactions using the previously generated token

Request:

curl --location 'https://api.incognia.com/api/v2/authentication/transactions' \
--header 'Authorization: Bearer
eyJ4NXQjUzI1NiI6IlphSFQxaUtGcFZoejIyd3ItWEk4V3kyal9mZlBOdmZXUDVHU1FPdzRuT3Mi
…' \
--header 'Content-Type: application/json' \
--data '{
"account_id": "cd4bd11df4d860313bb1cf2c270e9d35db85d17b5602efb8c6f1ef10b69186e1",
"installation_id":
"YFYS-27UdNRtgeYXh3iIZxQy6cT3hqUXnDaQ2WP1-mptPSm6ZFx0qNw6Xj8-EXixUFFJ-uXS
F6bEG6Pjs8yfX4Qt_ScsufINEigMgAaF4kPjTflG7FYWAdVyw6oXP3JR0PX3lanDkS7gfFv73wz2
bw",
"type": "login"
}'

Response:

```
{
  "id": "df1f61ad-77a3-46a5-b33f-93a020582ae4",
  "policy_id": "bf4da756-7490-48db-bf59-f5f2efcdd0b5",
  "risk_assessment": "unknown_risk",
  "reasons": [
    {
      "code": "device_integrity",
      "source": "local"
    }
  ],
  "evidence": {
    "device_model": "sdk_gphone64_x86_64",
    "known_account": true,
    "location_services": {
      "location_permission_enabled": true,
      "location_sensors_enabled": true
    },
    "device_integrity": {
      "probable_root": false,
      "emulator": true,
      "gps_spoofing": true,
      "app_tampering": true,
      "installation_source": "not_available",
      "first_detected_timestamp": "2024-05-24T17:14:55.883Z"
    },
    "device_fraud_reputation": "unknown",
    "device_behavior_reputation": "unknown",
    "account_integrity": {
      "recent_high_risk_assessment": false
    },
    "location_events_quantity": 0,
    "accessed_accounts": 5,
    "accessed_accounts_by_device_total_60d": 5,
    "app_reinstallations": 0,
    "active_installations": 1,
    "first_device_login_at": "2024-05-24T17:50:23.597Z",
    "first_device_login": false,
    "app_tampering": {
      "result": "detected",
      "app_debugging": "detected",
      "code_injection": "not_detected",
      "package_mismatch": "not_available",
      "signature_mismatch": "not_available",
      "properties_mismatch": "not_available",
```

```
            "first_detected_timestamp": "2024-05-24T17:14:55.883Z"
        },
        "remote_access": {
            "result": "not_available",
            "suspect_accessibility_services_running": "not_available"
        },
        "accounts_by_device_total_3d": 5,
        "accounts_by_device_total_10d": 5
    },
    "installation_id":
"YFYS-27UdNRtgeYXh3iIZxQy6cT3hqUXnDaQ2WP1-mptPSm6ZFx0qNw6Xj8-EXixUFFJ-uXS
F6bEG6Pjs8yfX4Qt_ScsufINEigMgAaF4kPjTflG7FYWAdVyw6oXP3JR0PX3lanDkS7gfFv73wz2
bw",
    "device_id":
"XxIIfOjaBwPLcgHFUBPsKxucxTgHsp7HjncK5-hRTIXwt8IEUFI7l2yvrtXVRoRBKrJWWm2IEKAi
VAa9IjlGKg"
}
```