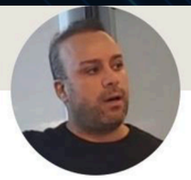
INSIDE TOKEN THEFT

ENTRA ID ATTACK CHAIN

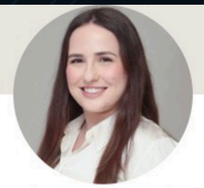
Presented by Liora Itkin & Eli Shlomo

SPEAKERS



Elli Shlomo

Microsoft Security MVP focused on cloud forensics, deep security research, and t...



Liora Itkin

Senior Security Researcher @ CardinalOps

AGENDA

- Authentication token overview
- Tokens in Azure authentication
- Token Tactics
- Attack Demo
- Detection
- Mitigation and conclusion

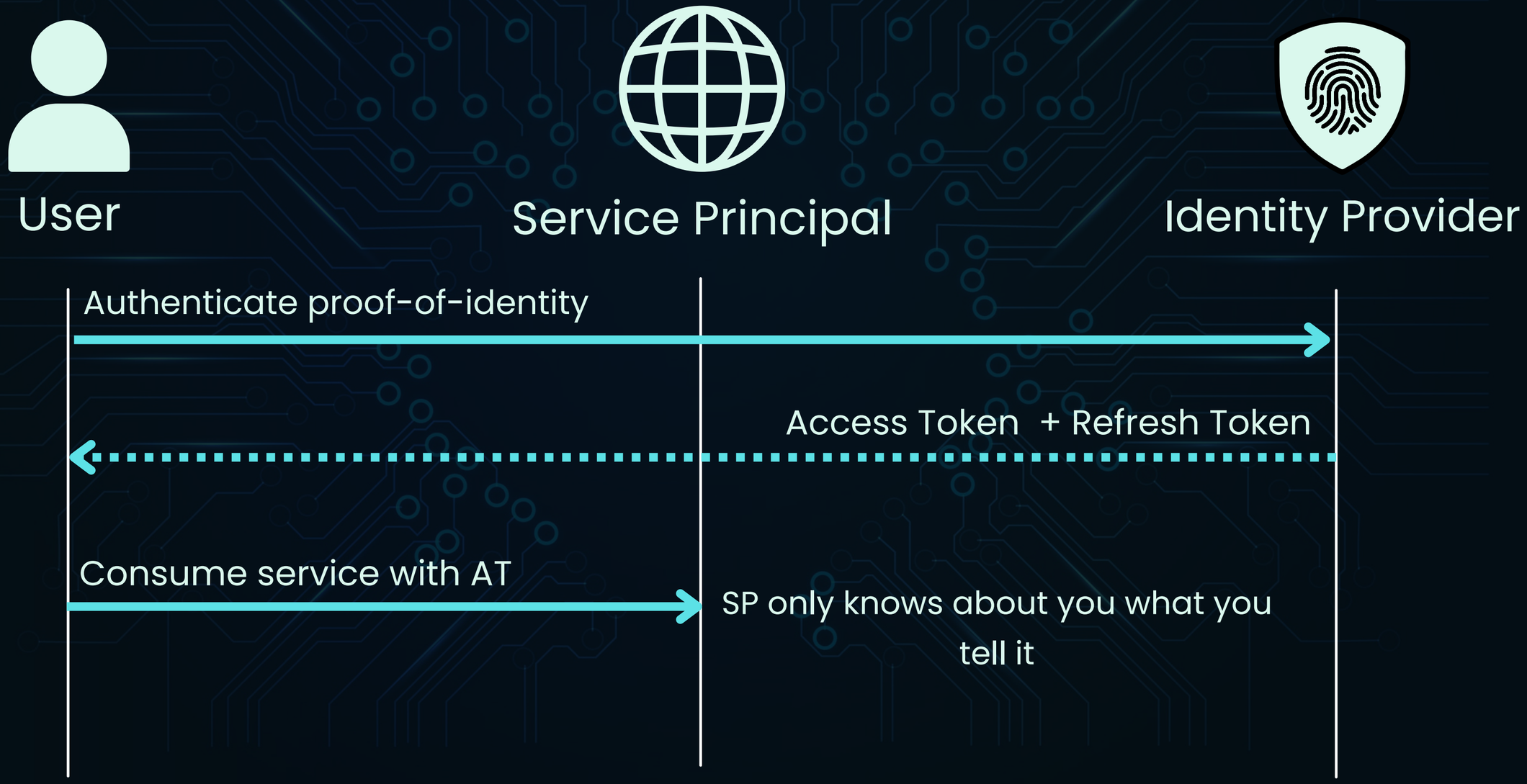
TOKEN OVERVIEW

- Digital proof that a user has been authenticated.
- Issued after login, used instead of a password for later requests.
- Usually contains user info and an expiration time.
- Lets servers verify access without storing session data.
- Common examples: JWTs, OAuth access tokens.

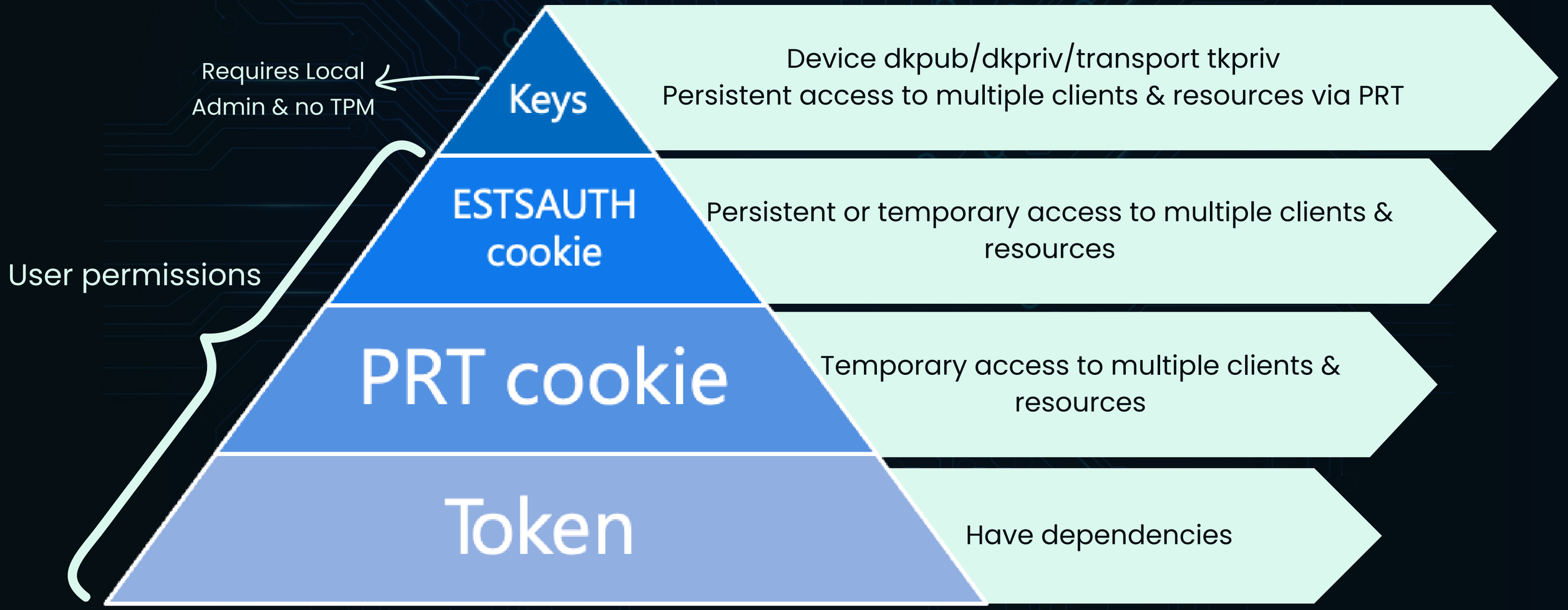
TOKENS IN AZURE

- Used to grant access to resources.
- Issued by Entra ID (Azure AD) after authentication.
- Contain info like user ID, roles, and permissions.
- Used to access M365 & Azure services without sending passwords.
- Common types: ID tokens, access tokens, refresh tokens.

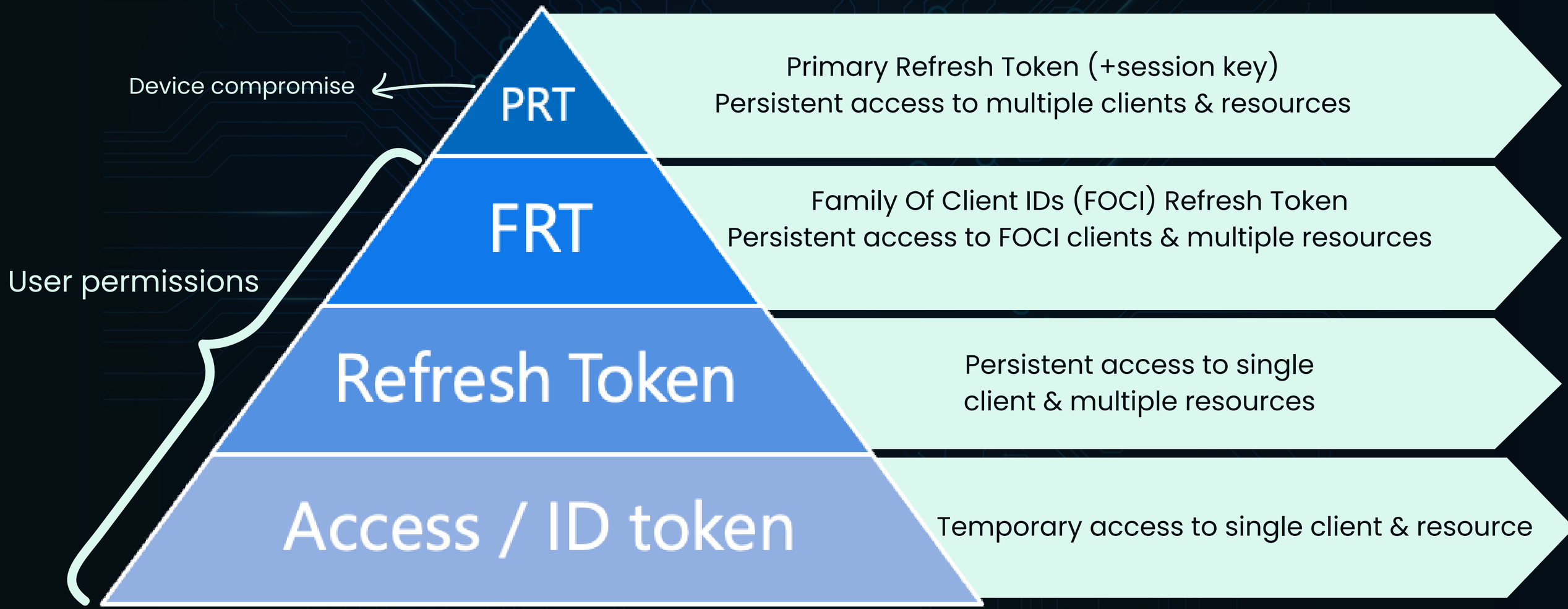
TOKEN-BASED AUTHENTICATION



ENTRA ID TOKEN LADDER



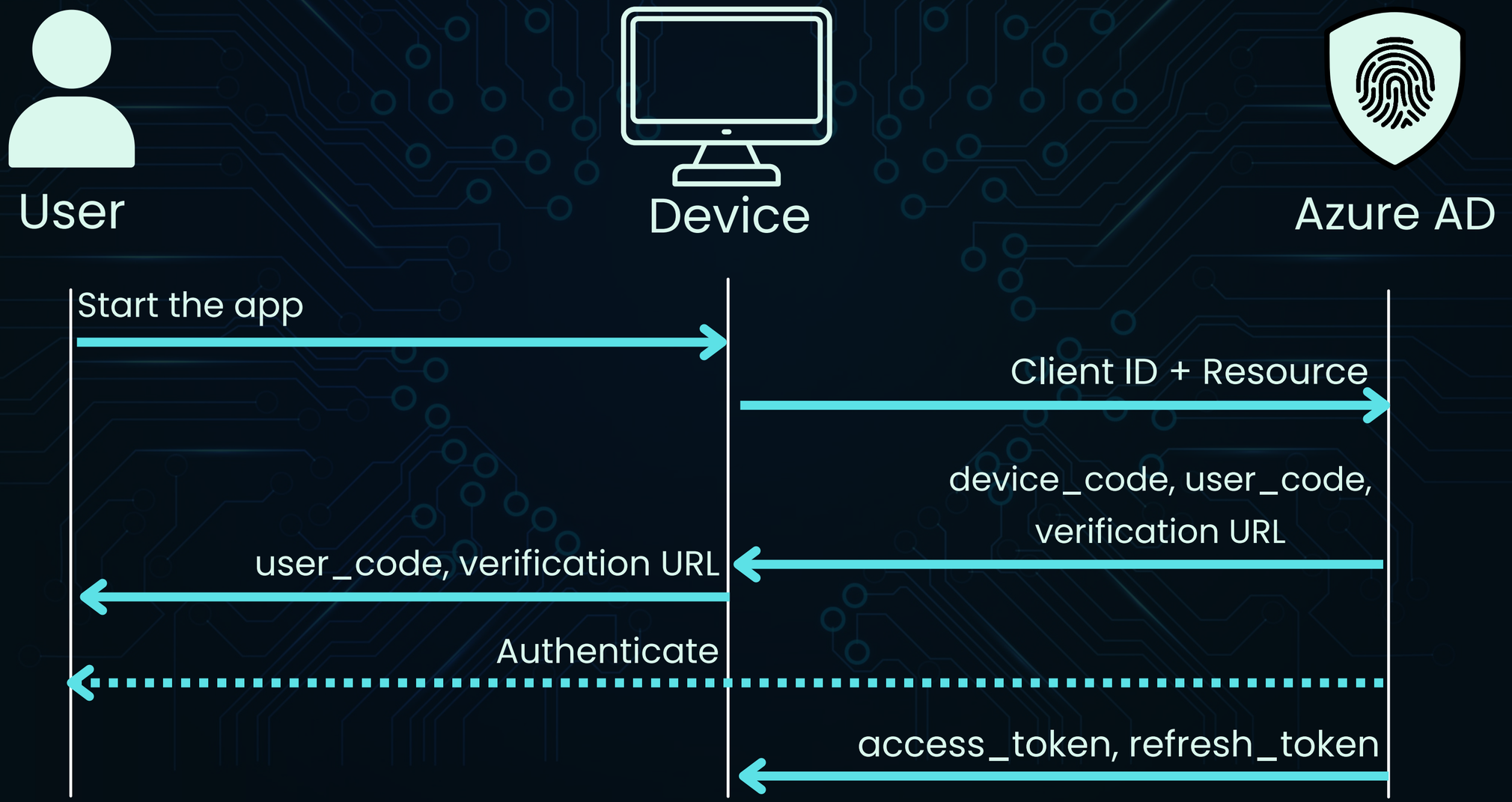
ENTRA ID TOKEN HIERARCHY



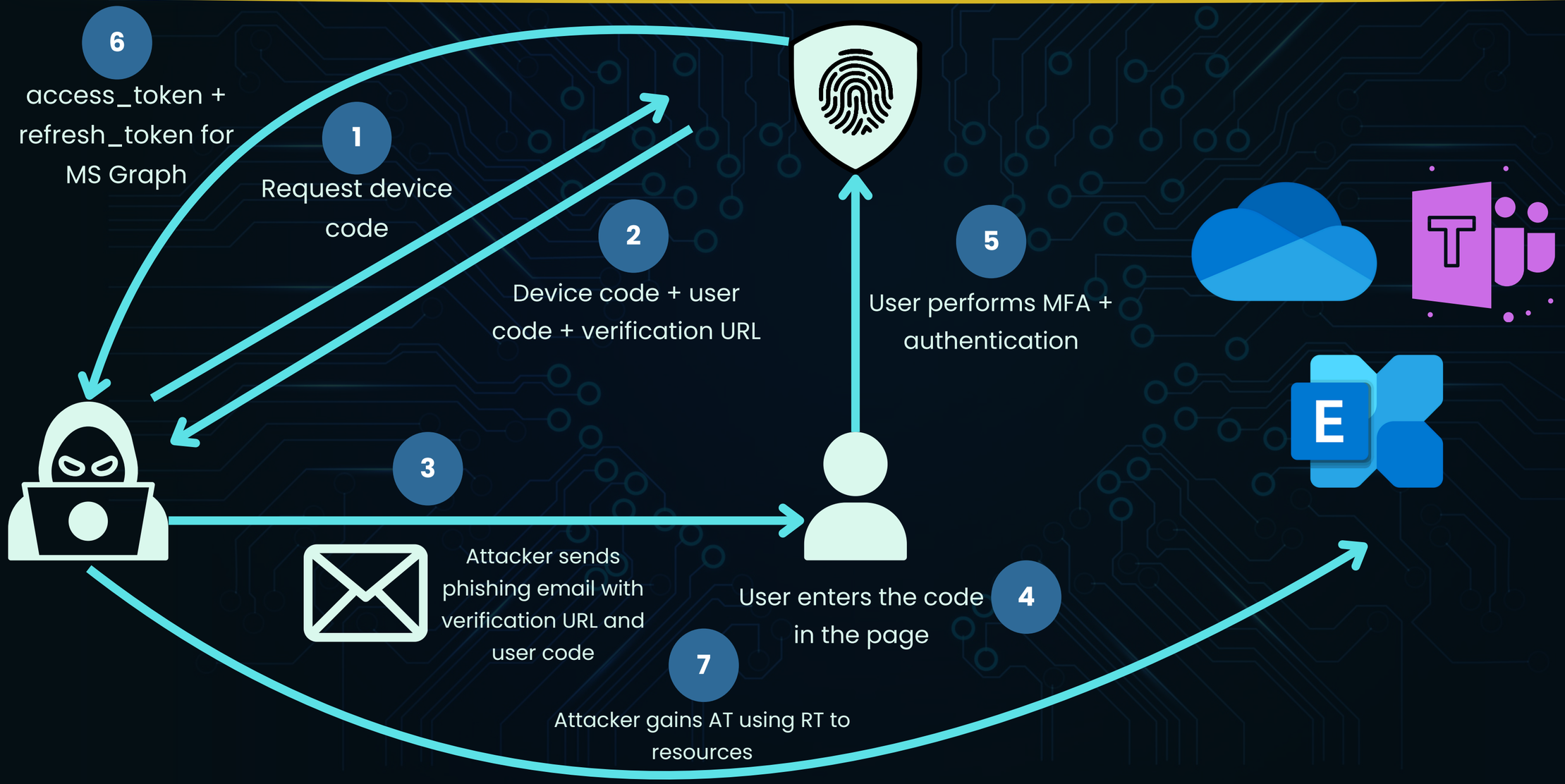
“ BIGGEST PROBLEM WITH BLUE TEAMERS IS, THAT THEY THINK IN LISTS, WHILE ATTACKERS THINK IN GRAPHS. SO, ATTACKERS WILL ALWAYS WIN. “

John Lambert
Corporate Vice President, Security Fellow, Microsoft

DEVICE CODE AUTHENTICATION



TOKEN TACTICS



TOKEN TACTICS DEMO

```
Last login: Wed Dec  3 12:37:00 on ttys004
liora@ip-192-168-64-203 ~ % cd documents
liora@ip-192-168-64-203 documents % cd github
liora@ip-192-168-64-203 github % cd token
cd: no such file or directory: token
liora@ip-192-168-64-203 github % cd TokenTactics
liora@ip-192-168-64-203 TokenTactics % pwsh
PowerShell 7.5.4
PS /Users/liora/Documents/GitHub/TokenTactics>
```

DETECTION

```
SigninLogs
| where AuthenticationProtocol == "deviceCode"
| where ResultType == "0"
| where parse_json(AuthenticationDetails)[0].authenticationStepResultDetail ==
"MFA requirement satisfied by claim in the token"
| where parse_json(AuthenticationDetails)[0].succeeded == true
| where parse_json(AuthenticationDetails)[0].authenticationMethod ==
"Previously satisfied"
| where AppId == "d3590ed6-52b3-4102-aeff-aad2292ab01c" #Microsoft Office -
optional
| where ResourceIdentity == "00000003-0000-0000-c000-000000000000" #MS Graph -
optional
| {{exclusion:AppId}}
| project-reorder UserPrincipalName, UserType, IPAddress, AppDisplayName,
ClientAppUsed, AuthenticationProtocol, ResourceDisplayName, UserAgent
```

THANK YOU FOR ATTENDING!