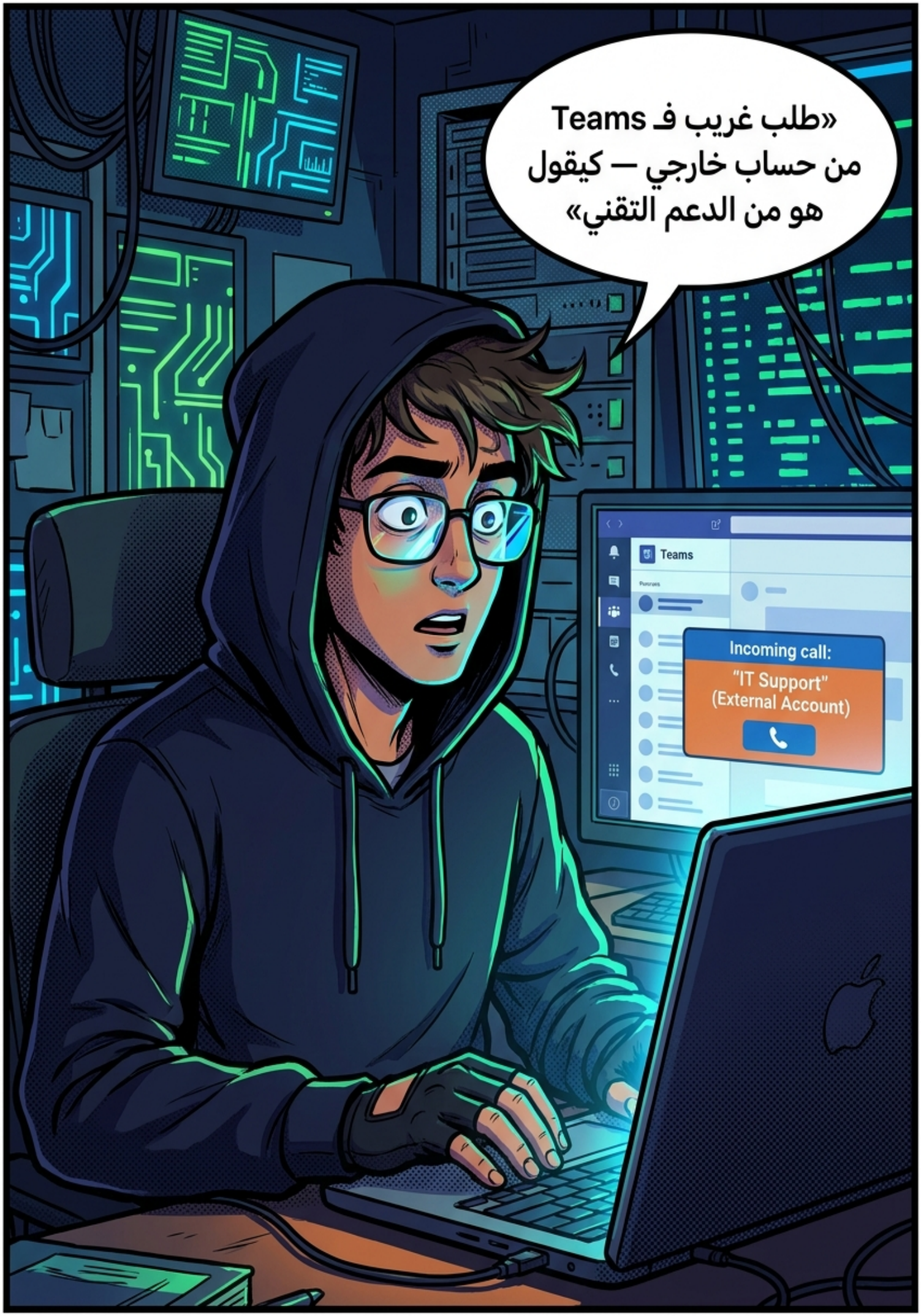
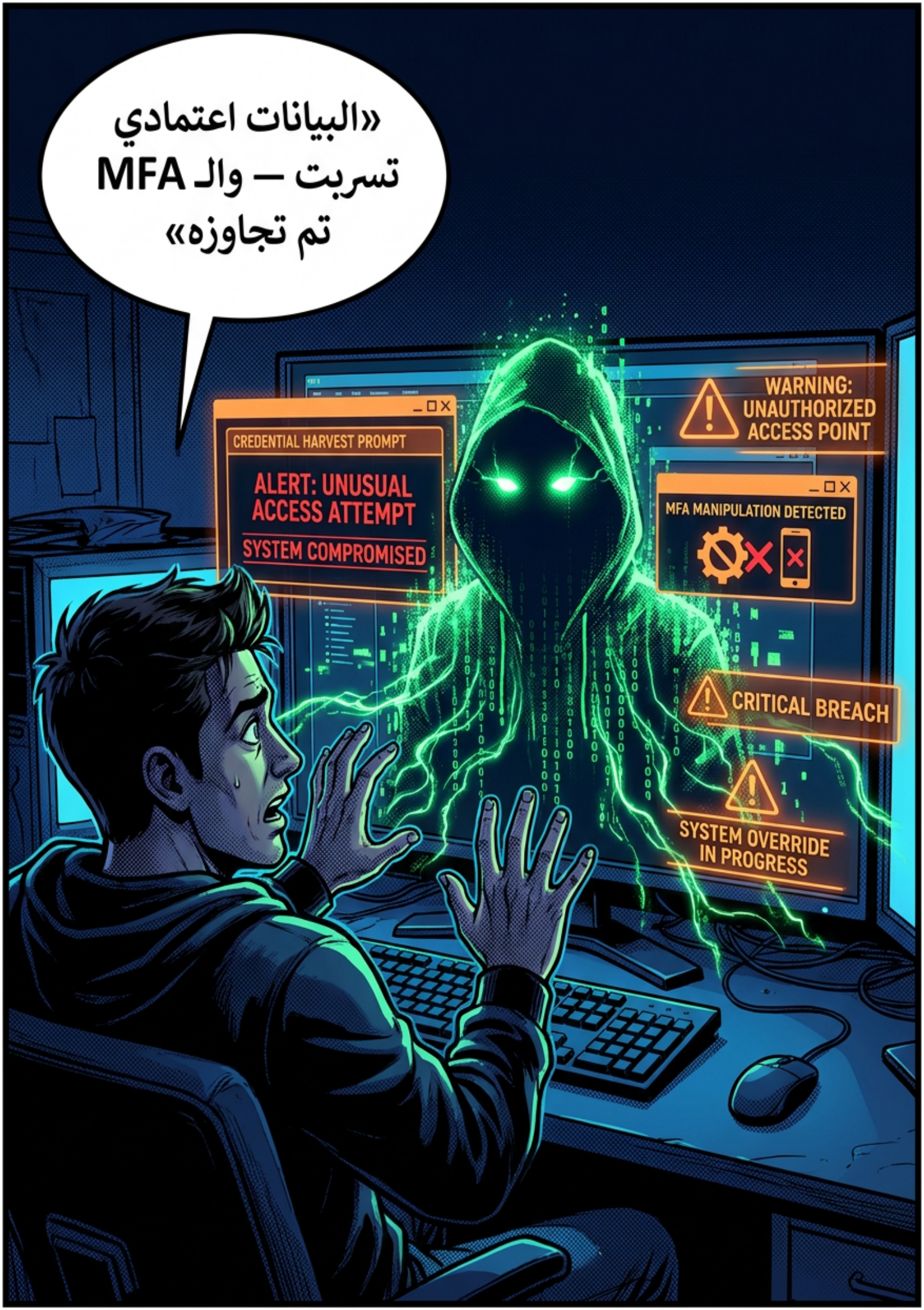
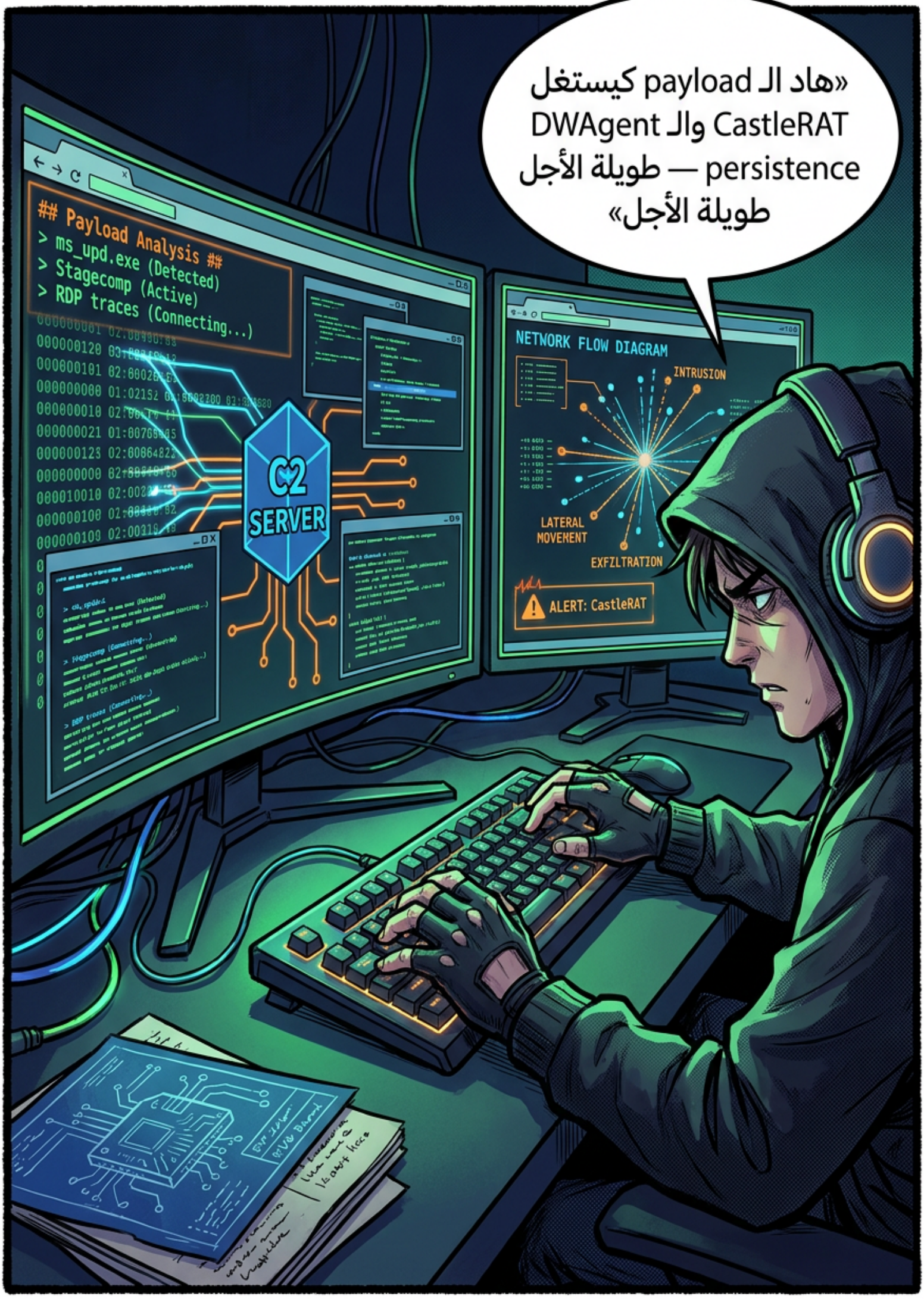
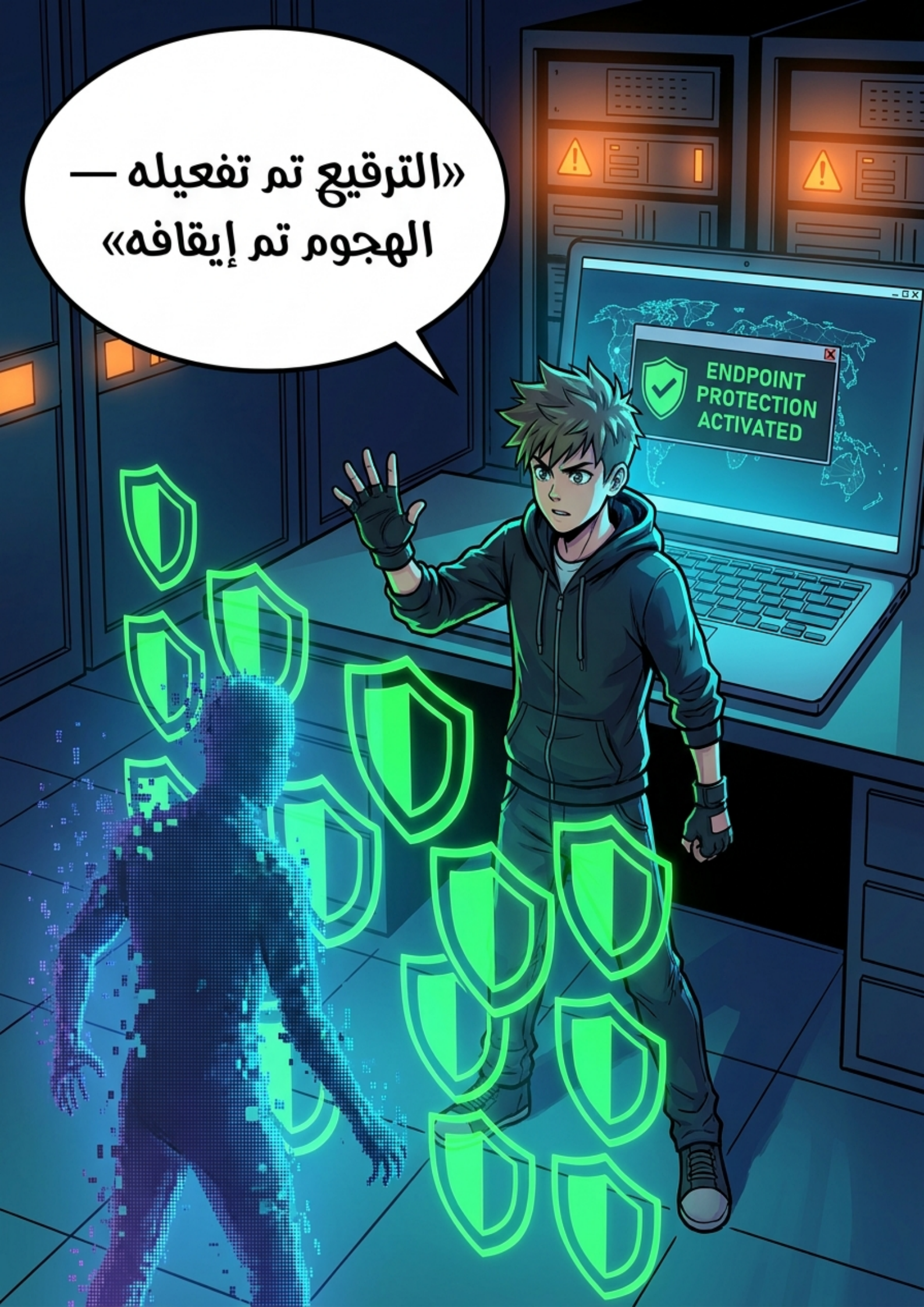

«طلب غريب فـ Teams
من حساب خارجي — كيقول
هو من الدعم التقني»
Teams
Incoming call:
"IT Support"
(External Account)


«البيانات اعتمادي
تسربت – والـ MFA
تم تجاوزه»
CREDENTIAL HARVEST PROMPT
ALERT: UNUSUAL ACCESS ATTEMPT
SYSTEM COMPROMISED
WARNING: UNAUTHORIZED ACCESS POINT
MFA MANIPULATION DETECTED
CRITICAL BREACH
SYSTEM OVERRIDE IN PROGRESS


«هاد الـ payload كيستغل
CastleRAT والـ DWAgent
persistence — طويلة الأجل
طويلة الأجل»
Payload Analysis
> ms_upd.exe (Detected)
> Stagecomp (Active)
> RDP traces (Connecting...)
C2
SERVER
NETWORK FLOW DIAGRAM
INTRUSION
LATERAL
MOVEMENT
EXFILTRATION
ALERT: CastleRAT


«الترقيع تم تفعيله —
الهجوم تم إيقافه»
ENDPOINT
PROTECTION
ACTIVATED