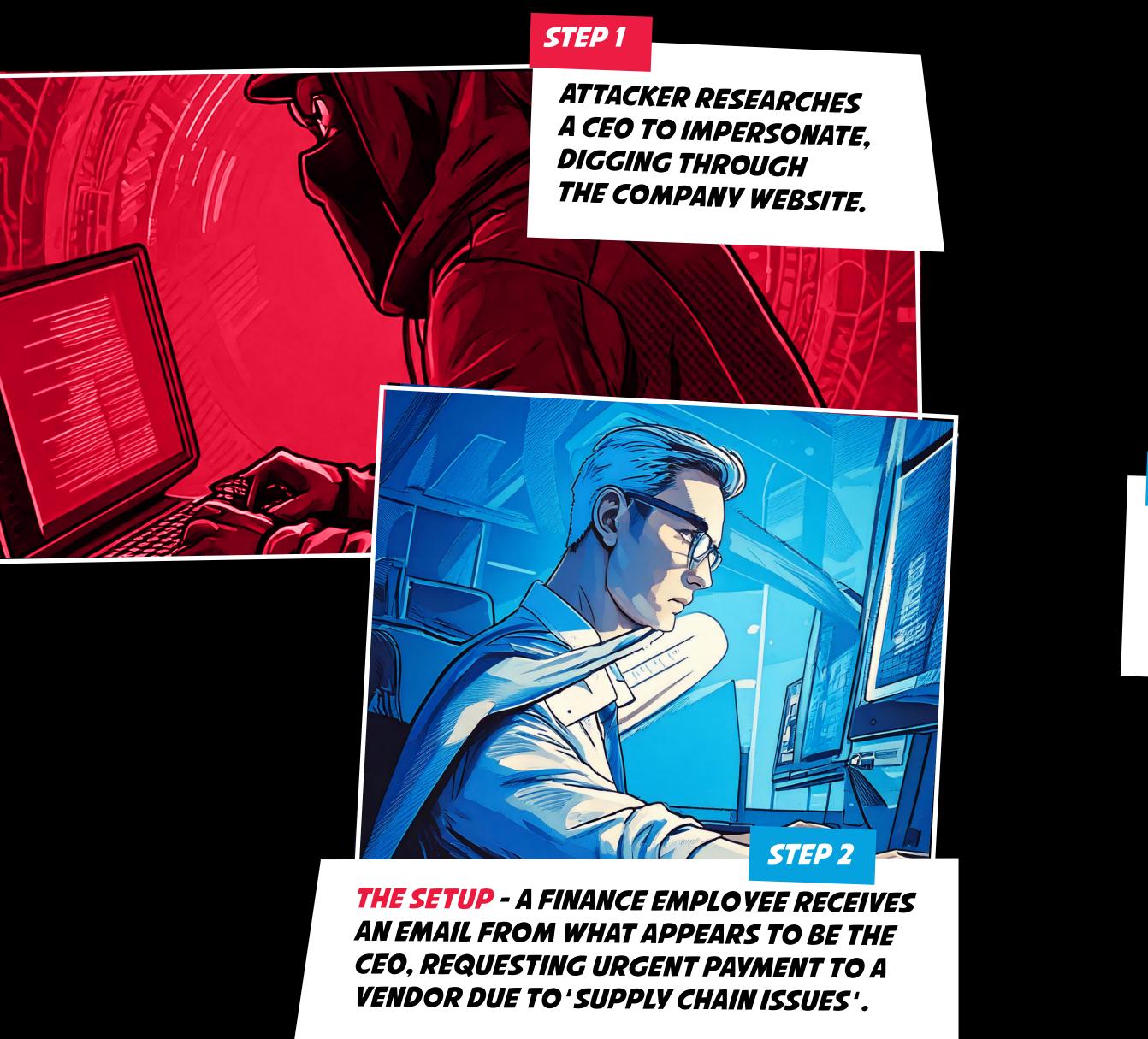
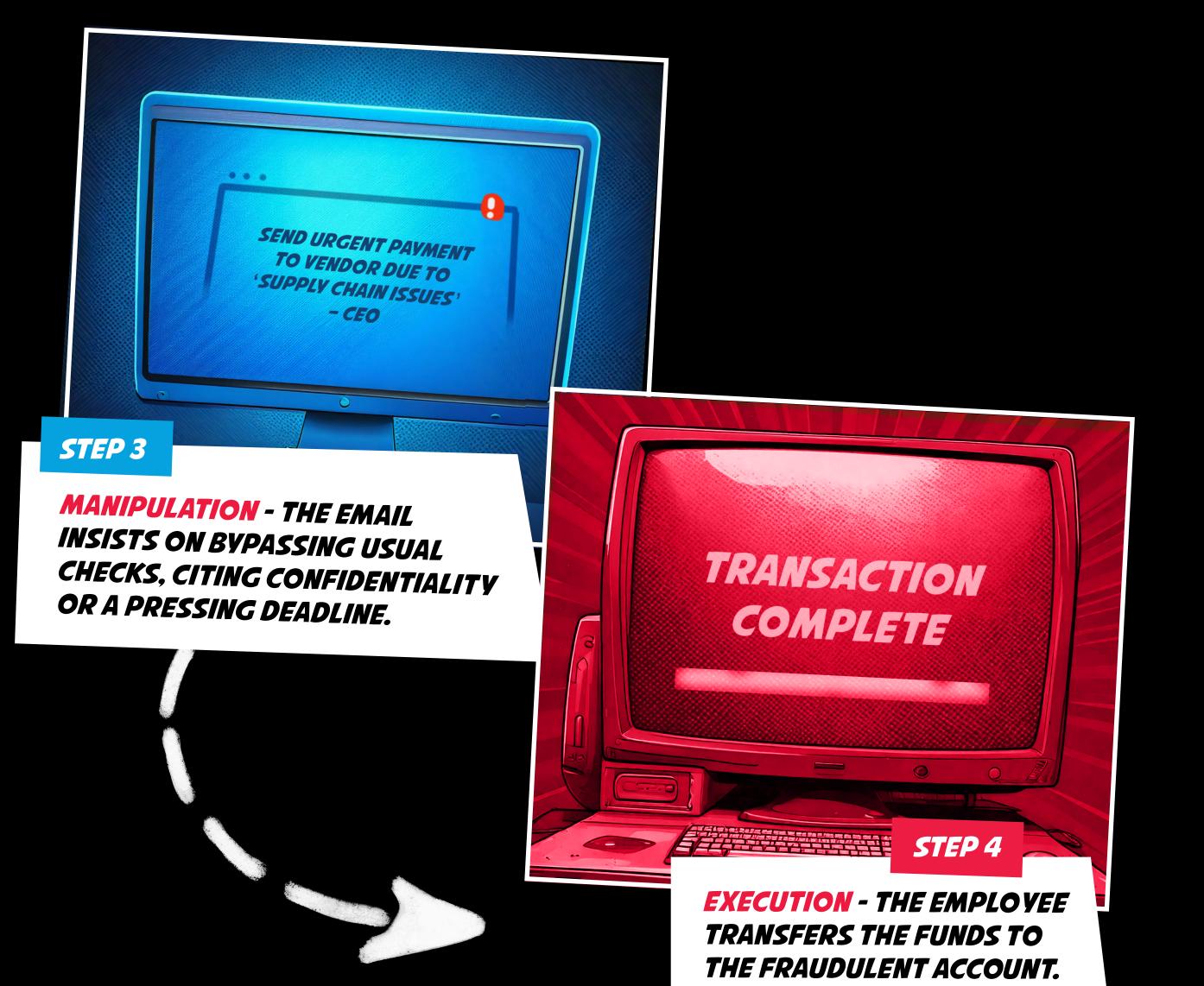
### binalyze

Business Email Compromise (BEC):

A Growing Threat to Organizations Worldwide

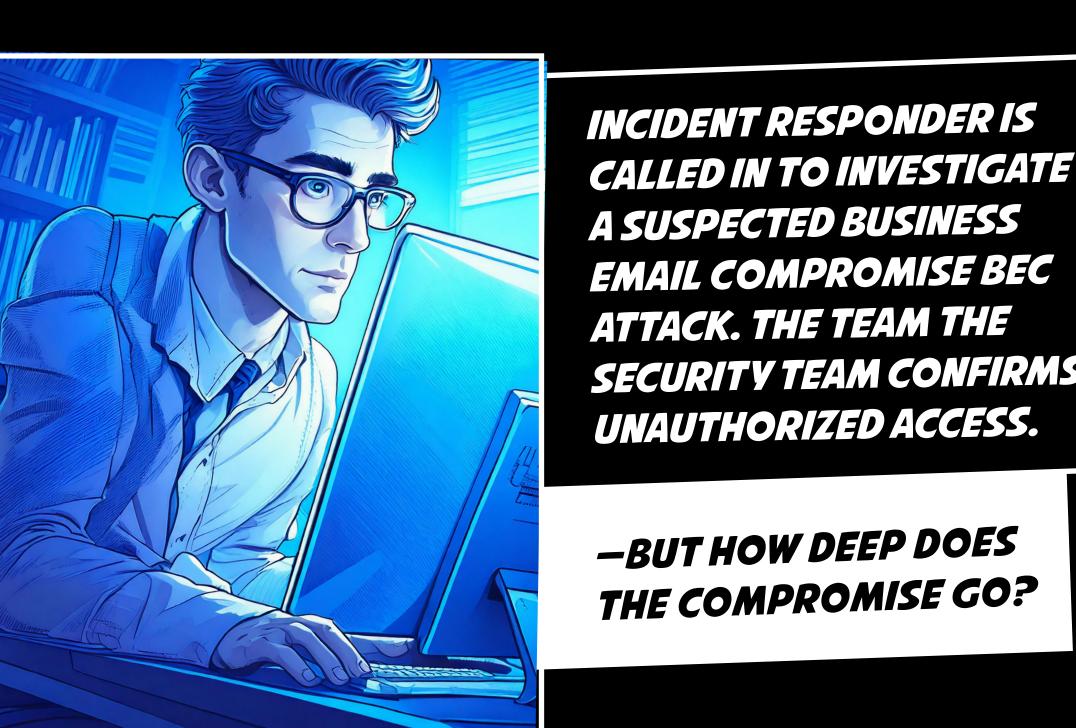
REAL WORLD EXAMPLE







### REAL WORLD EXAMPLE THE INVESTIGATION



INCIDENT RESPONDER IS CALLED IN TO INVESTIGATE A SUSPECTED BUSINESS EMAIL COMPROMISE BEC ATTACK. THE TEAM THE SECURITY TEAM CONFIRMS

**—BUT HOW DEEP DOES** 

#### THE RESPONDER HAS TO ANSWER CRITICAL INVESTIGATIVE QUESTIONS:

HOW DID THE ATTACKER GAIN ACCESS?

DID THEY SET UP FORWARDING RULES TO MAINTAIN CONTROL?

ARE THERE OTHER COMPROMISED ACCOUNTS?

DID THEY ACCESS SENSITIVE FILES OR MOVE LATERALLY?



# THE CHALLENGE BEGINS - STARTING WITH GAINING ACCESS TO EVIDENCE AND VISIBILITY NEEDED IN CLOUD ACCOUNTS:



EVERY MINUTE WASTED INCREASES RISK —
ATTACKERS CAN WIPE LOGS, ESCALATE ACCESS,
OR MOVE TO ANOTHER ACCOUNT.

## THE FASTER WAY TO COLLECT CLOUD EVIDENCE

A FAST, USER-FRIENDLY TOOL FOR INSTANT CLOUD EVIDENCE COLLECTION—EMAIL RECORDS, USER LOGS, AND ADMIN ACTIONS IN MINUTES.



### binalyze!

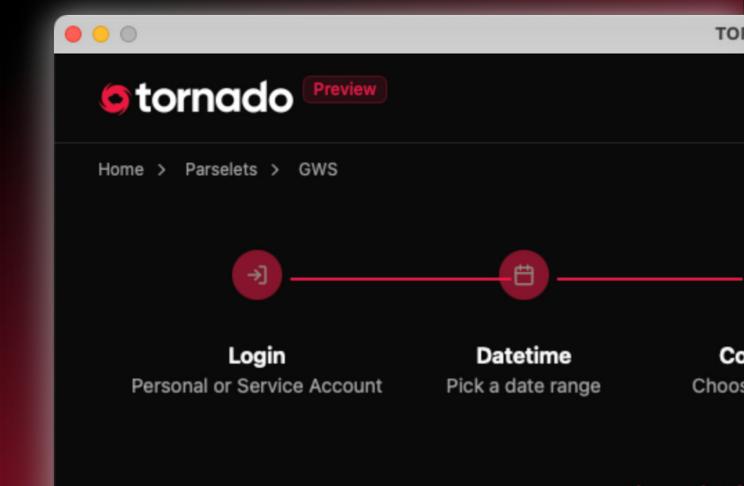


#### Preview Binalyze Tornado

- Collect critical artifacts like email records, user access logs, and admin actions in minutes.
- Support for Microsoft 365 & Google Workspace.
- Export to SQLite for further analysis.

Get access as soon as it's available – for free!

Join the waitlist



binalyze.com