FortiRecon – User Interview Process (Security Analyst Research)

Goal: Understand how security analysts investigate breach incidents and identify workflow pain points when using FortiRecon.

1. Participant Setup (5 minutes)

Participants: 3 Enterprise Security Analysts, 1 Threat Intelligence Manager, 1 SOC Lead.

Context: Interviews conducted to understand how analysts detect, investigate, and confirm security breaches using multiple modules within FortiRecon.

2. Interview Questions (Real Investigation Context)

- Walk me through the last time you investigated a potential breach.
- Which modules or tools do you usually open first?
- What signals help you confirm whether the breach is real?
- How many screens or modules do you typically navigate during an investigation?
- What information do you wish you could see in one place?

3. Scenario Task (Real Workflow Simulation)

- Imagine FortiRecon alerts you about a suspicious domain related to your company.
- What is the first thing you check?
- How do you verify whether credentials or assets are compromised?
- Which modules do you navigate next?
- What makes this investigation slow or difficult?

4. Key Insights From Interviews

- No single breach timeline exists to see the full attack sequence.
- Analysts must navigate multiple modules to validate a breach.
- Correlating signals across systems requires manual effort.

Example User Quote

"I have to open 4 different modules just to understand if the breach is real." – Enterprise Security Analyst