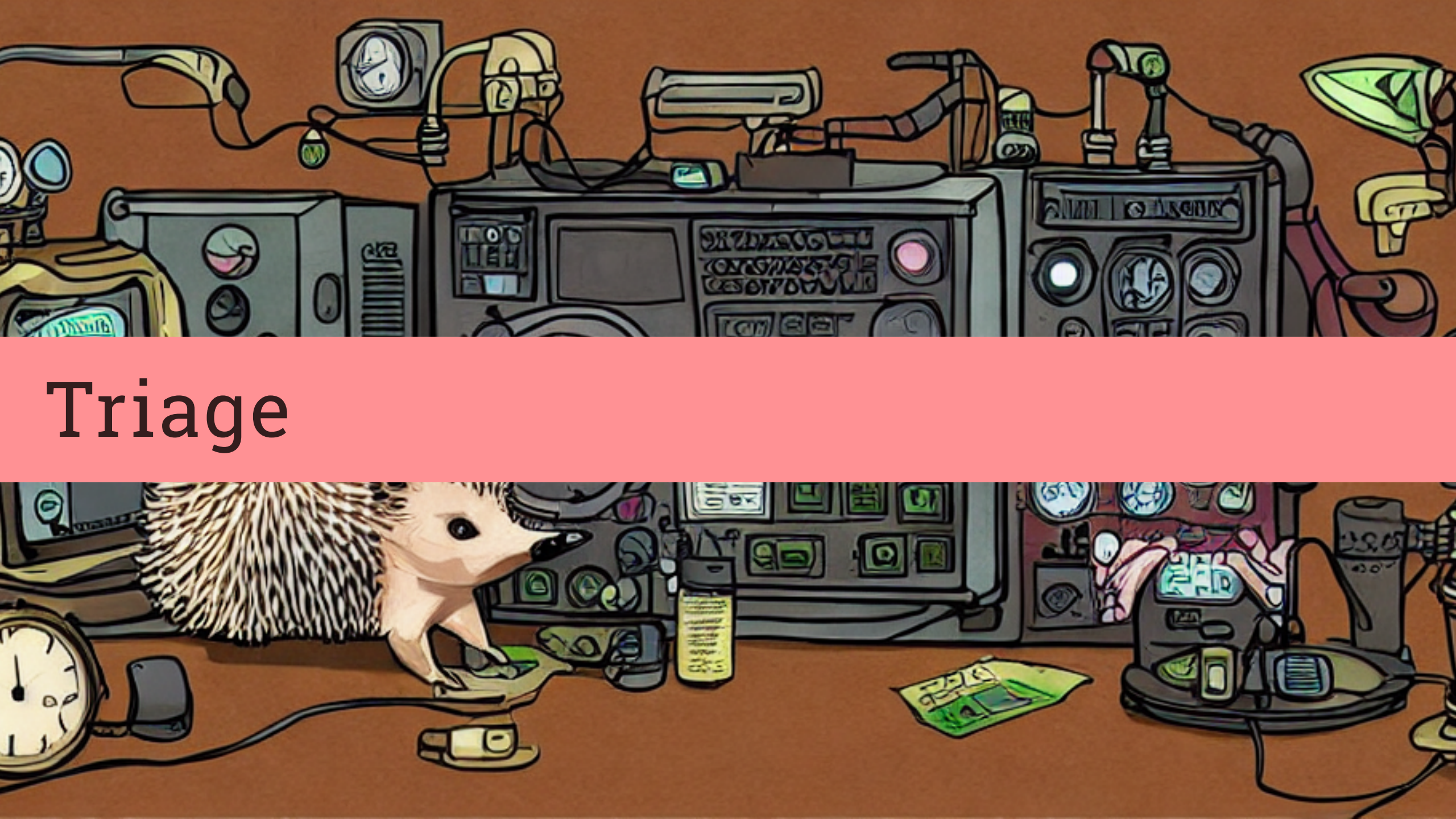
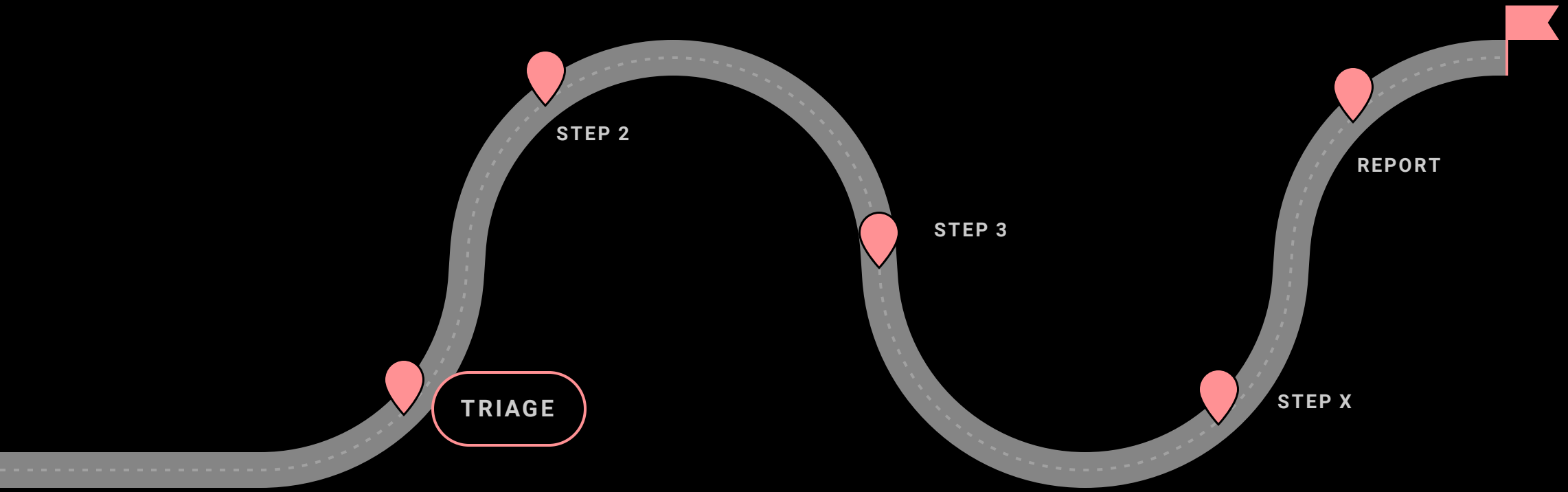
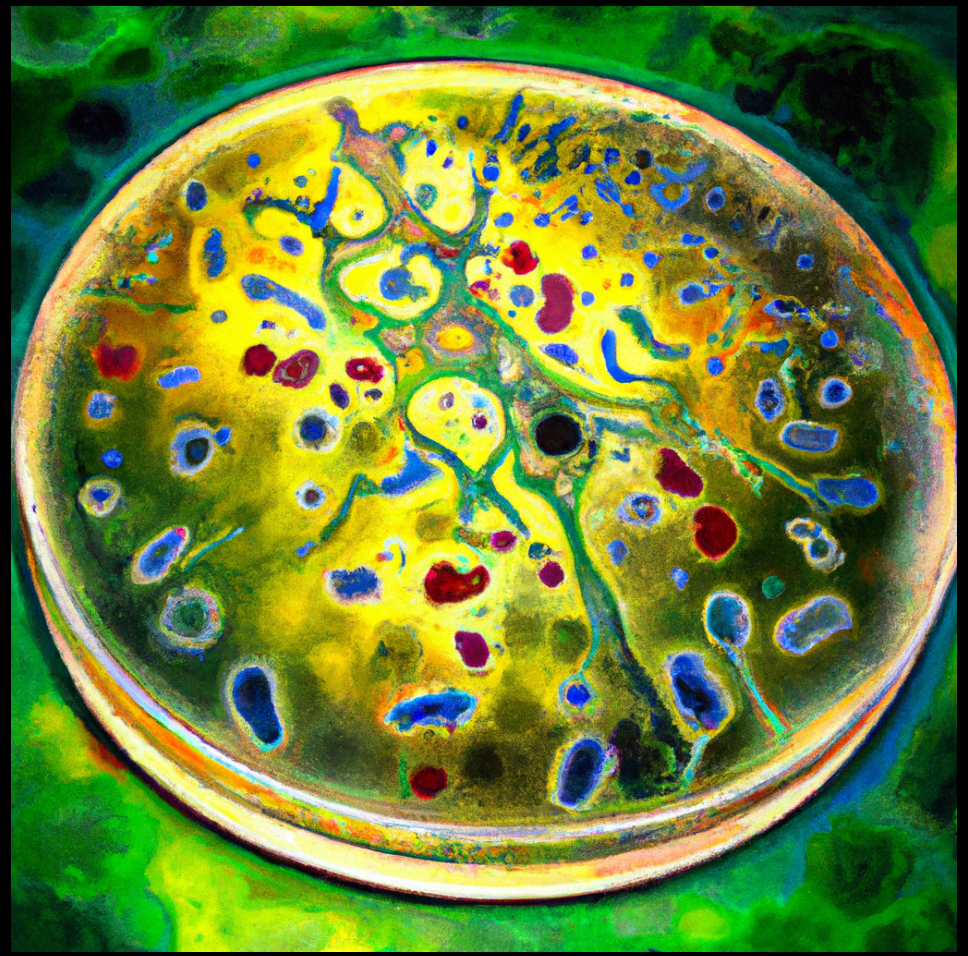


Triage

Analysis Process



What is Triage?



= preliminary assessment to determine course of action and where scarce resources should be put at

in malware analysis the scarce resource is usually time

WHY TRIAGE?

Purpose of Triage

GET OVERVIEW

- avoid the blind men and the elefant

DETERMINE STEPS AND TOOLS

CHOOSE SAMPLES FROM A SET

- malware hunting

DISCOVER LOW HANGING FRUITS

- easy wins

Triage Methods