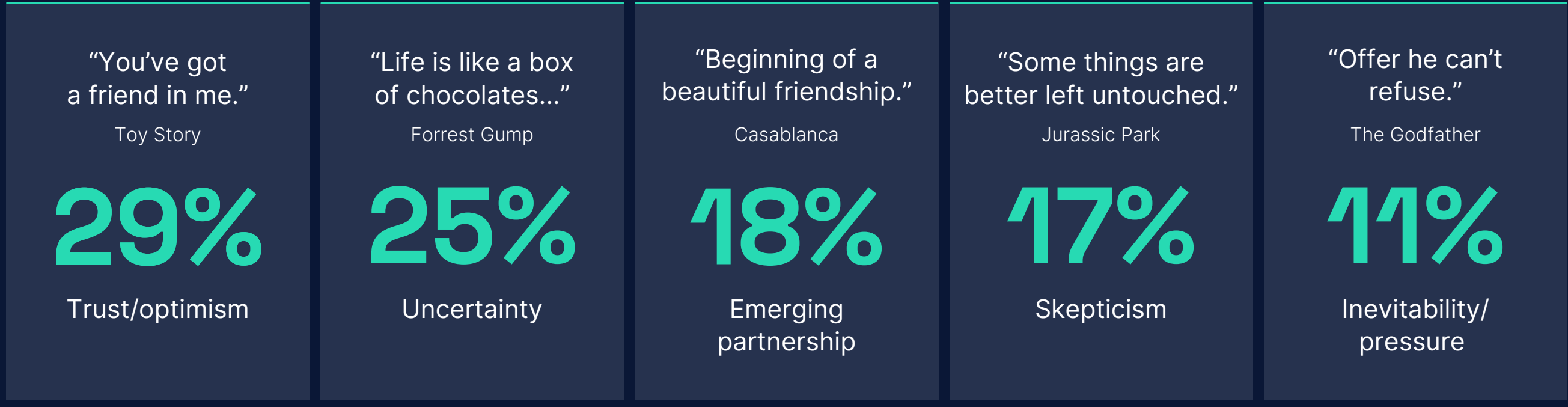


# FROM CURIOSITY TO CONTROL: SECURITY TEAMS ARE WARMING TO AI, BUT STILL FIGHTING CHAOS

AI is not simply a technology discussion. It is admittedly the biggest business model disruption that humanity has seen to date. RSA 2026 attendees opened up about what this means to them. We asked four questions to understand sentiment toward and adoption of AI. Hear from 279 respondents who shared their insights.

**1 A Relationship in Transition.** AI in security is becoming familiar. No longer experimental, it's becoming a trusted ally, but that trust isn't universal yet. Everybody's going at their own comfort level on the path to success.

## IF THE AI TECHNOLOGY YOU USE EACH DAY IN YOUR PROFESSIONAL CAREER WERE REPRESENTED BY A MOVIE QUOTE, WHICH WOULD IT BE? (SELECT ONE)



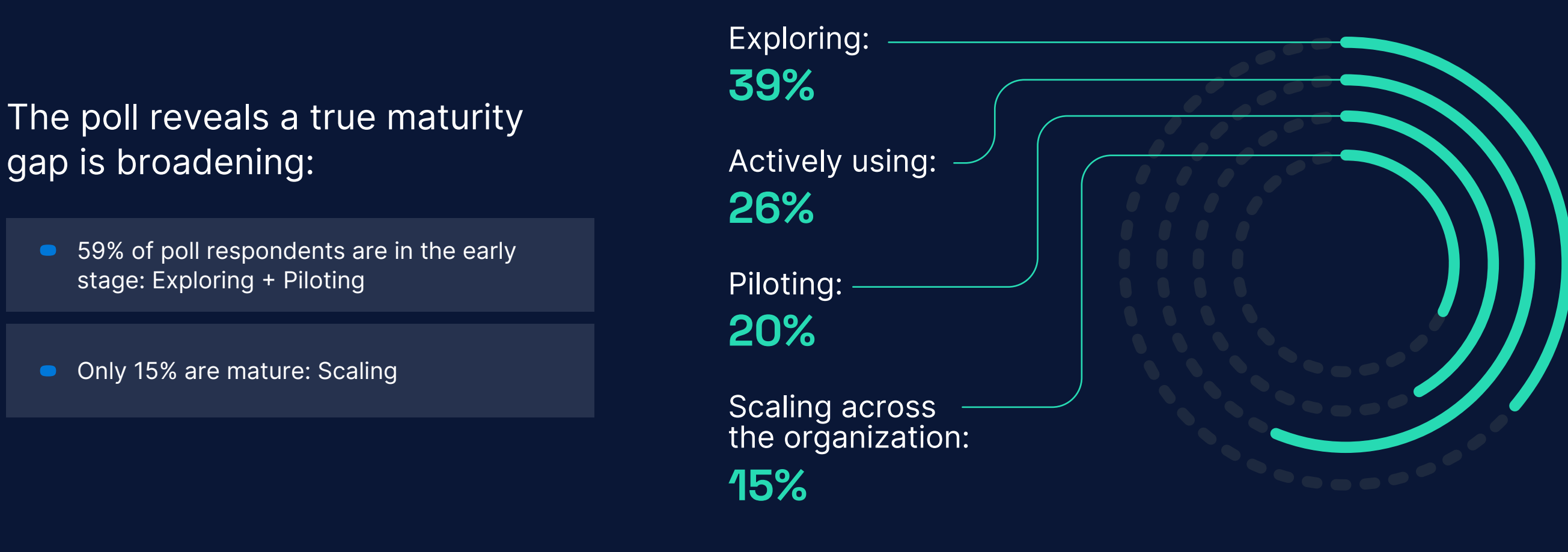
**2 The Reality Check:** Operations are Still Overwhelmed. Security teams have tools, but they lack cohesion, speed, and scale. Data is fragmented across too many tools. Putting AI next to bad data is like hiring a genius who doesn't speak your language.

## WHAT ARE YOUR TOP CHALLENGES TODAY? (MULTIPLE CHOICE)



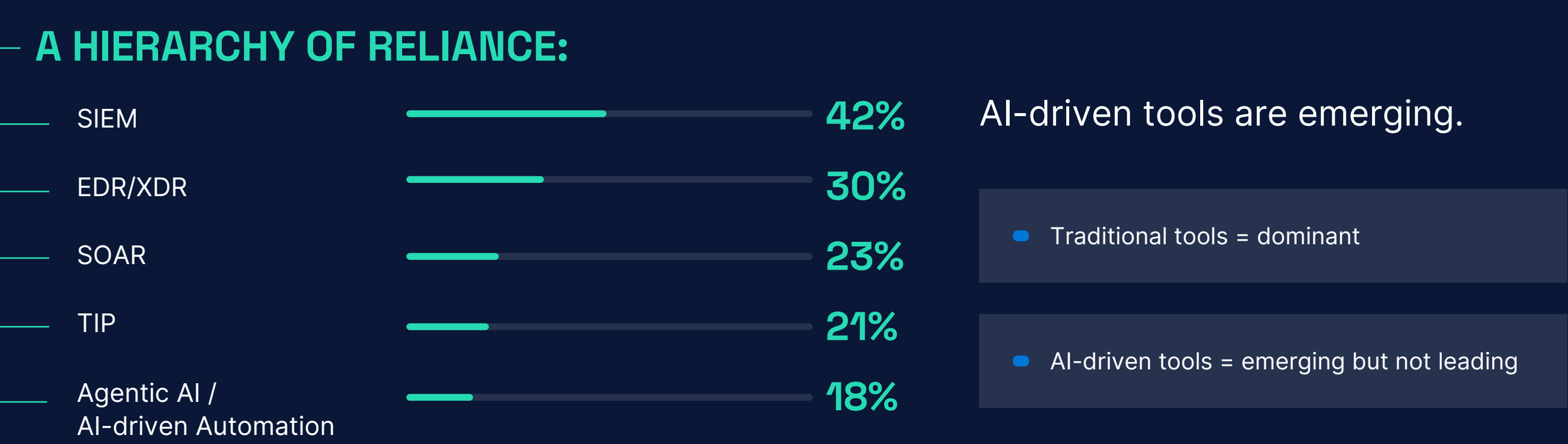
**3 The Adoption Gap:** Interest is High, Maturity is Low. Most organizations are not yet fully leveraging AI. The majority are exploring or piloting. We are in early innings.

## WHERE ARE YOU IN ADOPTING AI FOR SECURITY OPERATIONS? (SELECT ONE)



**4 The Tool Stack Paradox:** Strong Foundations, Limited Transformation. Traditional tools still dominate workflows. Automation and AI-driven tools are emerging, but not yet central. A SIEM, an XDR, a SOAR, a TIF, all these things are of the past. Organizations need one unified data lake.

## WHAT TOOLS DO SECURITY TEAMS RELY ON MOST RIGHT NOW TO POWER CORE DETECTION AND RESPONSE WORKFLOWS? (MULTIPLE CHOICE)



**5 A Turning Point:** The future is clear. AI-powered security. The challenge is getting there fast enough. An incremental innovation will not a disruption — it must be disruptive innovation. The path forward is securing from AI, securing the AI, and securing with AI.

