



Frontier AI and Cyber Risk

October 14, 2026



Brandon Wales

Public Policy, The Americas
CrowdStrike

Agenda

- 01** Introduction
- 02** The problem
- 03** Solution
- 04** Key Data
- 05** Summary

Frontier AI changes the speed and economics of cyber risk

89%

Increase in attacks
by AI-enabled
adversaries

29 mins

Average eCrime
breakout time

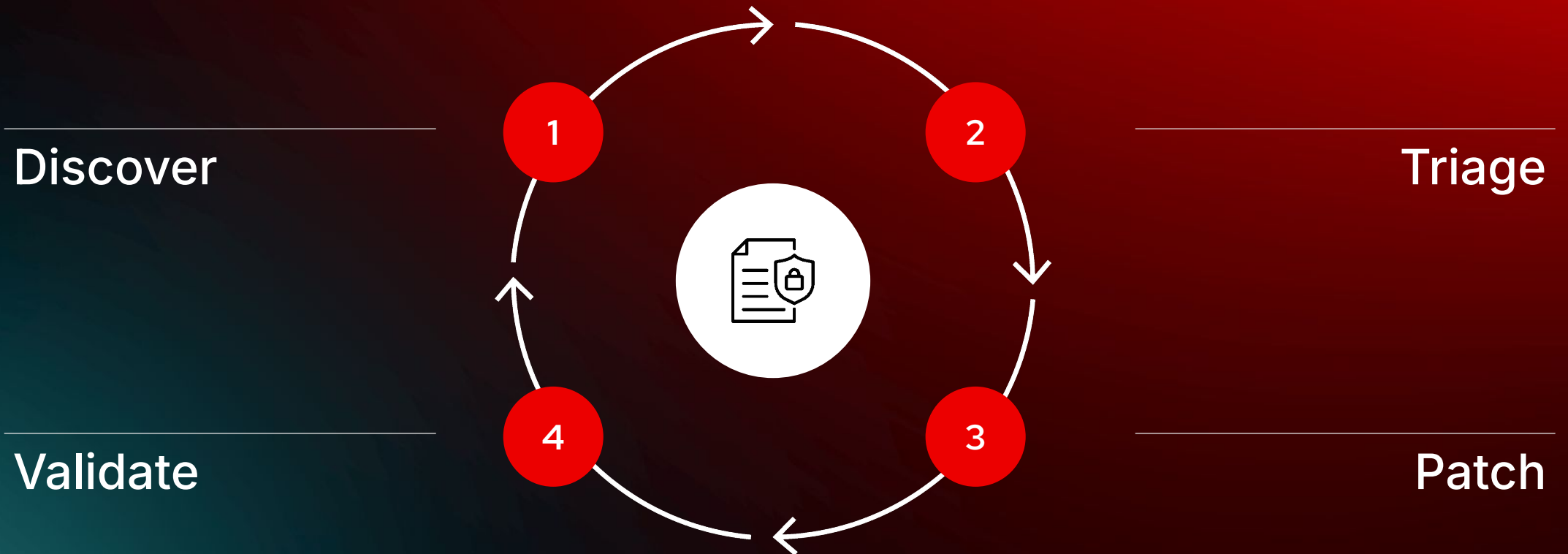
42%

Increase in
zero-days exploited
before disclosure

Are programs built around periodic assessment and human-speed escalation still calibrated to adversaries operating at inference speed?

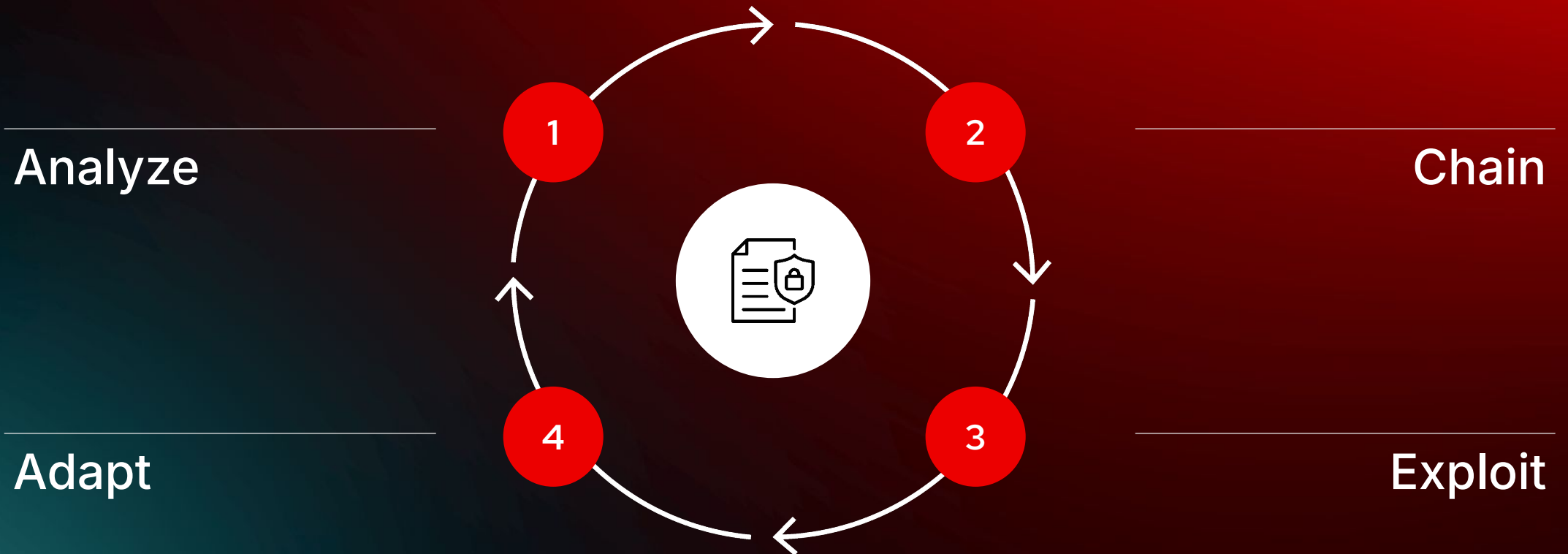
Frontier AI collapses the vulnerability lifecycle

Traditional Cycle



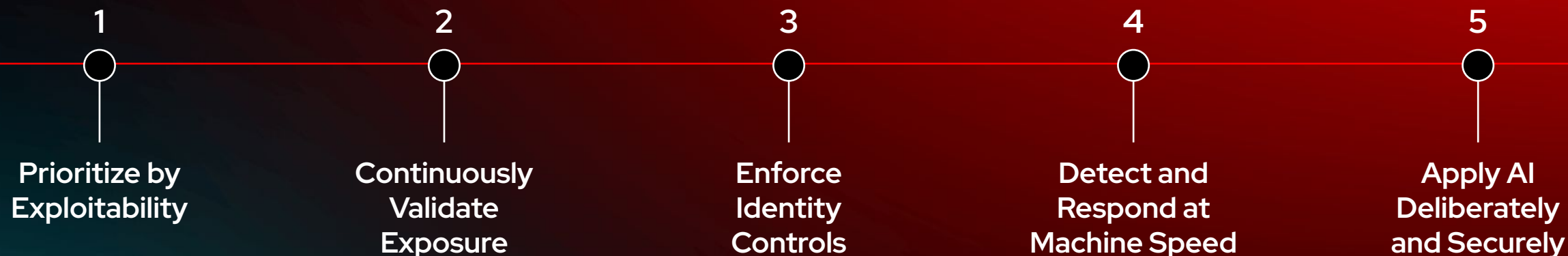
Frontier AI collapses the vulnerability lifecycle

AI-Compressed Cycle



Don't mistake Frontier AI risk for a vulnerability-management problem

Five Steps for Frontier AI Security Readiness



The exam question evolves from “Do you have a vulnerability management program?” to “Can you continuously identify, prioritize and reduce the exposures most likely to create material harm?”

AI is now an attack surface



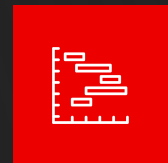
Visibility

Do you know what sanctioned and unsanctioned AI is operating?



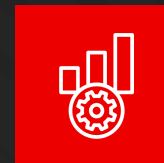
Identity

Who—or what—is the agent acting as, and what can it access?



Data

What sensitive information can it read, transmit or modify?



Runtime

Can you detect and stop an agent whose actions become malicious, compromised or simply unintended?

What this means for you?

Questions?

Thank you

Brandon Wales

Public Policy, The Americas

brandon.wales@crowdstrike.com