KEEPER

IT LEADERS FACE AN ERA OF AI-POWERED CYBER THREATS

Artificial Intelligence (AI) is revolutionizing the cybersecurity landscape, introducing complex and advanced threats that challenge traditional defenses. As AI technology evolves, detecting common cyber threats like phishing and smishing becomes increasingly difficult, underscoring the need for robust, adaptive security measures.

AI Detection Challenge

84%

of IT leaders find AI has made phishing and smishing harder to detect

Policy Implementation Surge

81%

of organizations have introduced AI usage policies for employees

AI Security Knowledge

77%

of IT leaders say they're extremely or very familiar with best practices for AI security

Despite an increase in AI policies and self-confidence in the ability to combat AI-powered cyber attacks, Keeper Security's research highlights a significant gap in overall preparedness. AI-powered attacks, supply chain attacks and deepfake technology are identified as major concerns. Yet, many organizations still struggle to close the preparedness gap for these sophisticated threats.

Key Threats and Gaps

Emerging Threats

51%

of IT leaders view AI-powered attacks as the most serious cyber threat

36%

are concerned about supply chain attacks

36%

highlight deepfake technology as a significant risk

Preparedness Gaps

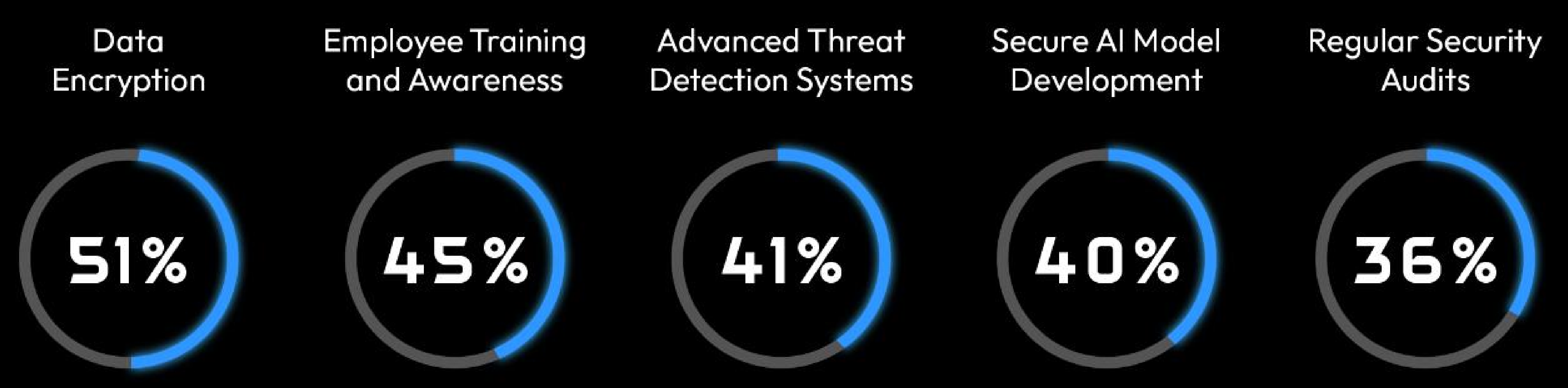
35%

of IT leaders feel least prepared for AI-powered attacks

30%

express concern about deepfake technology

How Organizations Combat AI Threats



> "AI-driven attacks are a formidable challenge, but by reinforcing our cybersecurity fundamentals and adopting advanced security measures, we can build resilient defenses against these evolving threats."

Darren Guccione
CEO and Co-founder,
Keeper Security

The rise of AI-driven attacks requires elevated defenses. Essential practices like data encryption, employee training and advanced threat detection must be consistently updated and enhanced. Implementing advanced frameworks such as zero trust and Privileged Access Management (PAM) will further fortify defenses. Organizations should remain vigilant, continuously review their security policies and adopt modern approaches to stay ahead of the evolving AI-powered threat landscape.