IntegraONE | 35 YEARS OF TECHNOLOGY EXCELLENCE
THANK YOU FOR BEING A PART OF OUR STORY | 1990 • 2025

AI & Security

Hype, Risk, and Real-World Protection

2025 ONECON

Artificial Intelligence is transforming cybersecurity—both for defenders and for attackers. In this session, we'll cut through the hype to show how AI is reshaping the security landscape and what it means for your business.

INTRODUCTION

Rebecca Hailey MSCs.ITM

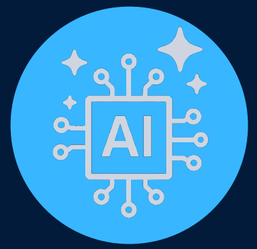
Security Practice Leader

- 15+ years of experience in IT and Cybersecurity
- Master of Science in Cybersecurity
  Southern New Hampshire University
- Generative AI Certification
  Johns Hopkins University

AI Basics for Business Leaders

Machine Learning (ML)

Finds patterns in data

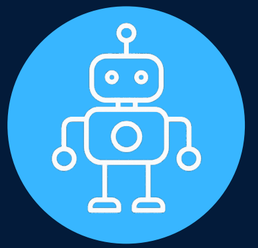


Generative AI (GenAI)

Creates new content (text, images, code)

Chat AI

Conversational Q&A (built on GenAI)



Agentic AI

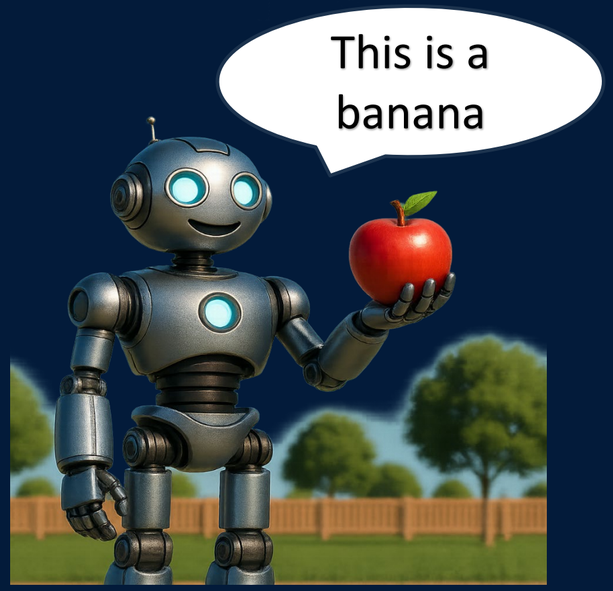
Takes actions on its own (Reset accounts, schedule tasks)

AI Drawbacks

Hallucination

Confidently makes things up

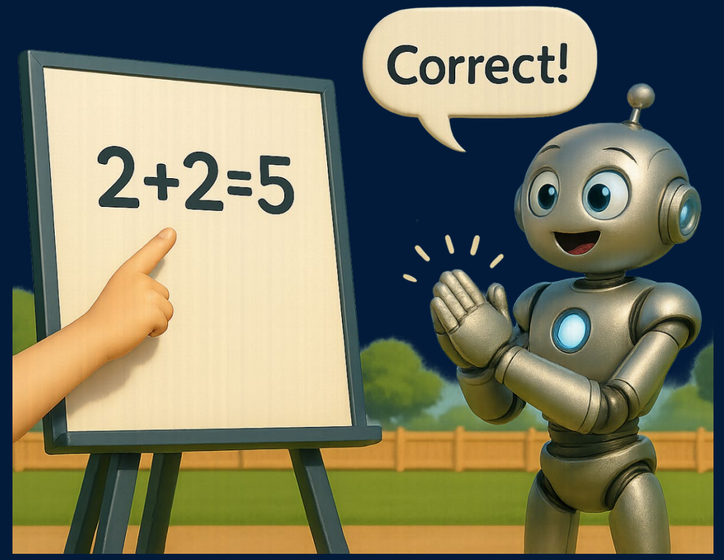
May produce fake citations



Always Affirming

Never tells you you're wrong

Doesn't admit mistakes



Bias in Data

Outputs reflect flaws in training data

Lack of Judgement

No context, nuance, or consequences

Internal Risks

- Shadow AI
- Data Leakage & Compliance Risks
- Oversight & Governance

Shadow AI

Using AI tools without approval or oversight, putting company data at risk.

Risks

Proprietary data leaked

Customer or Employee PII exposed

No control over Confidentiality/Privacy

Data Leakage & Compliance Risks

PII Exposure

Customer and employee data entered into AI tools can lead to **HIPAA, GDPR**, or **CCPA violations**, severely impacting your company's reputation and finances.

Business Secrets Loss

Entering proprietary data into public AI models risks **exposing trade secrets**, which may resurface in unexpected places, jeopardizing your competitive advantage.

Outdated AI Guidance

AI models trained before regulation changes may provide **stale advice**, leading to potential compliance failures and increasing legal liabilities for your organization.

AI Oversight And Governance

Policies

Establish comprehensive guidelines to ensure ethical AI development and usage.

Containerization

Implement secure environments for AI models to protect data and system integrity.

Training

Provide ongoing education for teams to understand AI governance and best practices.

External Threats

OSINT

Open-Source Intelligence — public data, posts, repos, lelks, victim DBs

AI-Enhanced Phishing

SpamGPT → polished personalized phishing at scale

Voice & Image Cloning

Deepfake execs or loved ones to authorize fraud

Recon & Targeting

Mapping people, tech, and partners to find the fastest way in

Malware Generation & Obfuscation

AI-Created code that mutates to evade detection

Credential Attacks

AI guesses, steals, or bypas ses weak logins

Fraud & Misinformation

Flood of fakes to sway opinion or damage trust

Reconnaissance and Targeting

Public OSINT

Profiles, job posts, forums, repos

AI processing

Entity resolution, correlation, NLP embeddings

Spear phishing & BEC at scale

Context Aware Dossiers

can we remove one of the arrows going from the hacker in the upper left? Also can we move the arrows from the center circle to the perimeter of the circle?

Voice & Likeness Cloning

TikTok

UK engineering firm Arup falls victim to £20m deepfake scam

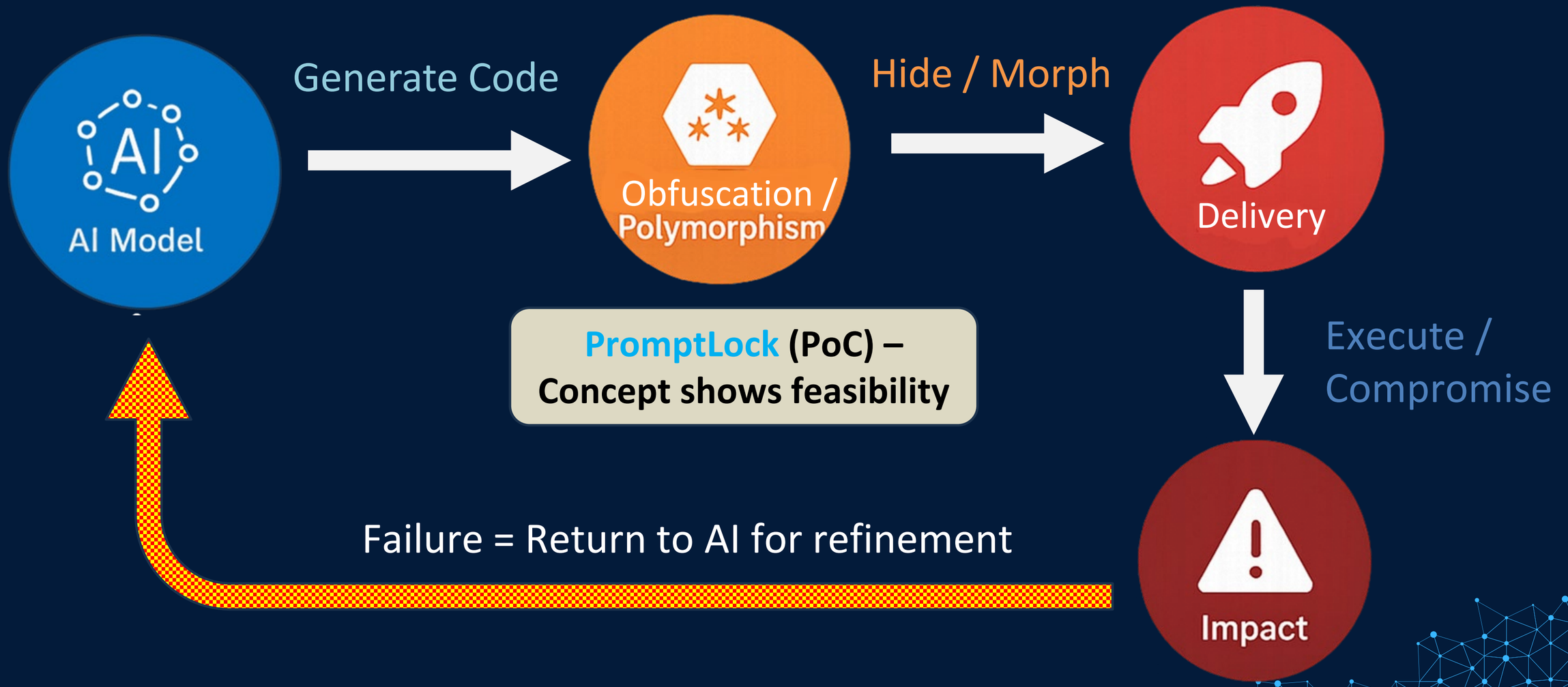
Hong Kong employee was duped into sending cash to criminals by AI-generated video call

Deepfake tool

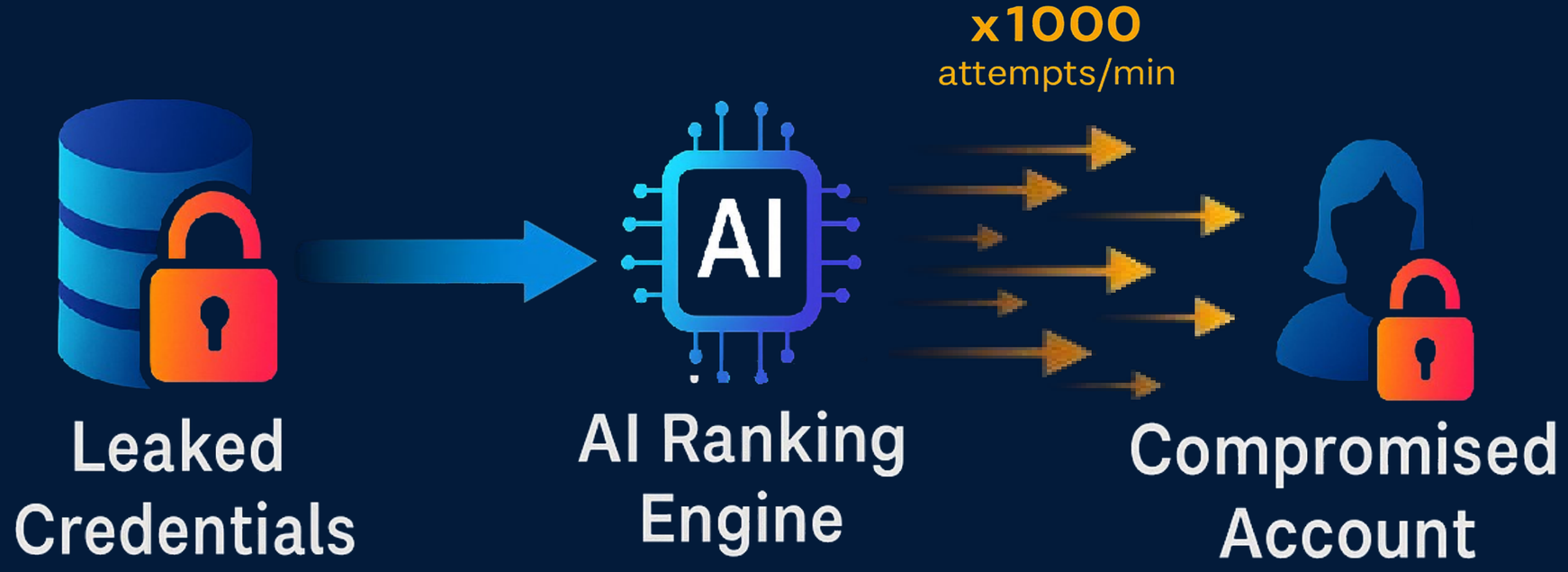
Few seconds of audio to clone

I NEED help
Send $15K i
Bitcoin NOW
will be arrest

Malware Generation & Obfuscation



Credential Attacks



What to watch

- High-velocity failures
- Unusual devices/ locations

Fraud & Misinformation

Legal Notices

- Regulatory/legal notices that demand immediate action
- Faux Official Letterhead and counsel contact details
- Pressures victims to rush payments or compliance steps

Fake Suppliers

- Synthetic supplier IDs
- Forged invoices / payee changes
- Fake websites / social proof

Business Impact

- Stock and market impact
- Brand / Reputation hit
- Loss payment / Operational Disruption

What we can do to help

- Managed Services
- Firewall as a Service
- EDR / XDR
- Managed Detection and Response
- SOC/SIEM
- Incident Response
- Penetration Testing
- Security Awareness Training

2026 Roadmap

- AI Gateway
- GRC Advisory
- Vulnerability Management

IntegraONE | 35 YEARS OF TECHNOLOGY EXCELLENCE
THANK YOU FOR BEING A PART OF OUR STORY | 1990 • 2025

THANKS FOR ATTENDING!

Rebecca Hailey MSCs.ITM

Security Practice Leader

rhailey@integraone.com

https://www.linkedin.com/in/rebeccahailey/

Scan Me

managing
complexity
delivering

simplicity