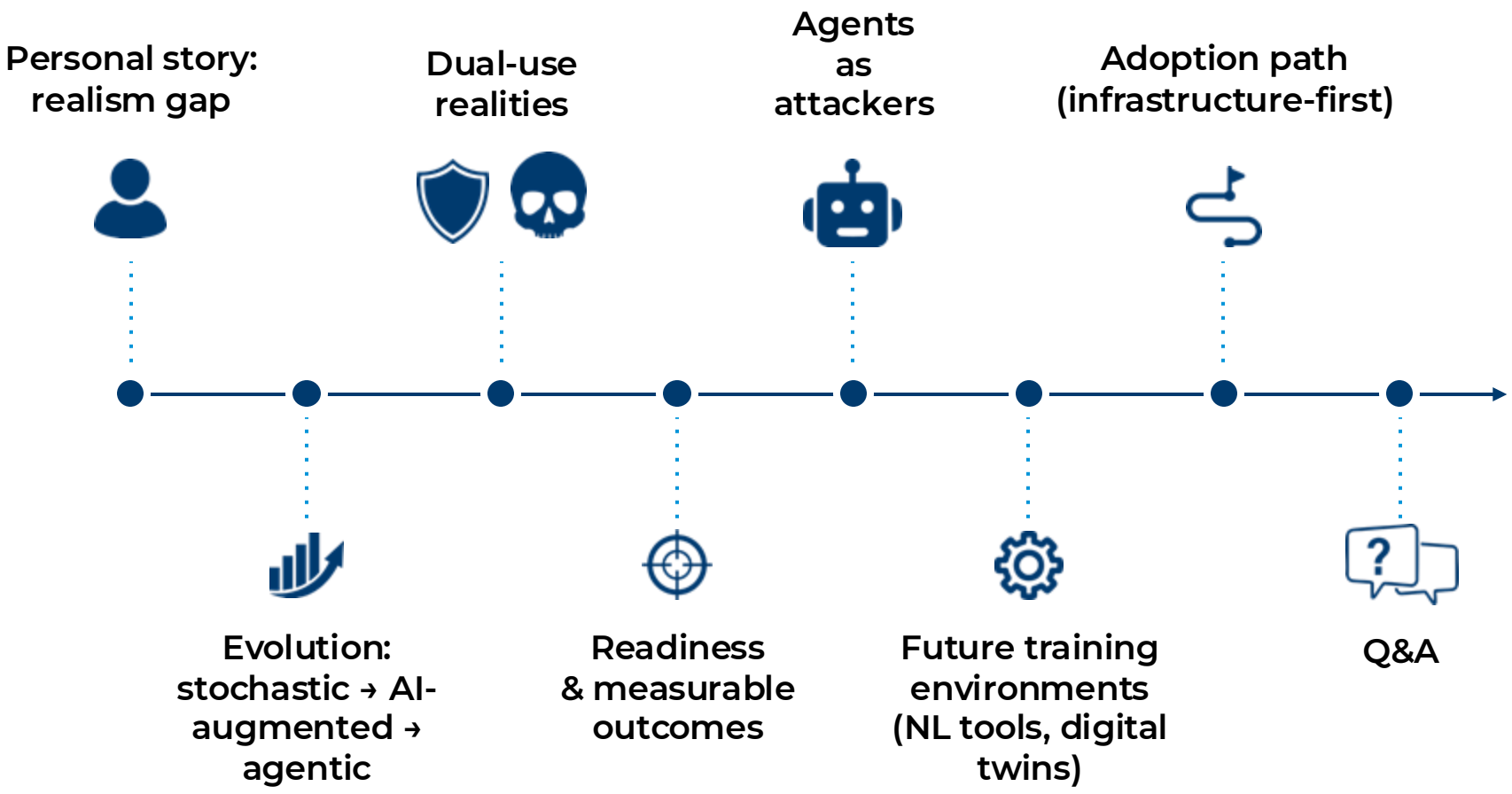
Agentic AI for Joint Cyber Readiness — Dual-Use Realities

Ernest McCaleb

How autonomous AI is reshaping cyber training and readiness

Session Roadmap



Static training can't mimic **multi-vector attacks**

Capture-the-Flag is **not enough** (USCC)

My Story: The Realism Gap

Non-host traffic generators:
scale but no realism

Hot-based:
realism but poor scale

Trainees spotted simulator tells

Adaptability

Dynamic training forces teams into unpredictable conditions

Readiness

AI-driven ranges “enhance readiness” vs static

From Stochastic to Agentic

Stochastic actors: probabilistic, resource-light, relevant

AI-augmented stochastic: smarter lures (emails, phishing)

Agentic models: adaptive, autonomous, tool-using

Needed: realism, adaptive adversaries, scalable scoring

Efficiency

Dynamic training forces teams into unpredictable conditions

Retention

AI-driven ranges “enhance readiness” vs static

Agentic AI:
The Next Generation

Dual-use challenge:
realism for training, AI as attack vector

Adaptive → **Adversarial Simulation** → **Personalized Learning & Coaching** → **Auomated AAR**

~4M

Cyber workforce gap:
~4M unfilled jobs
(ISC2, 2023)

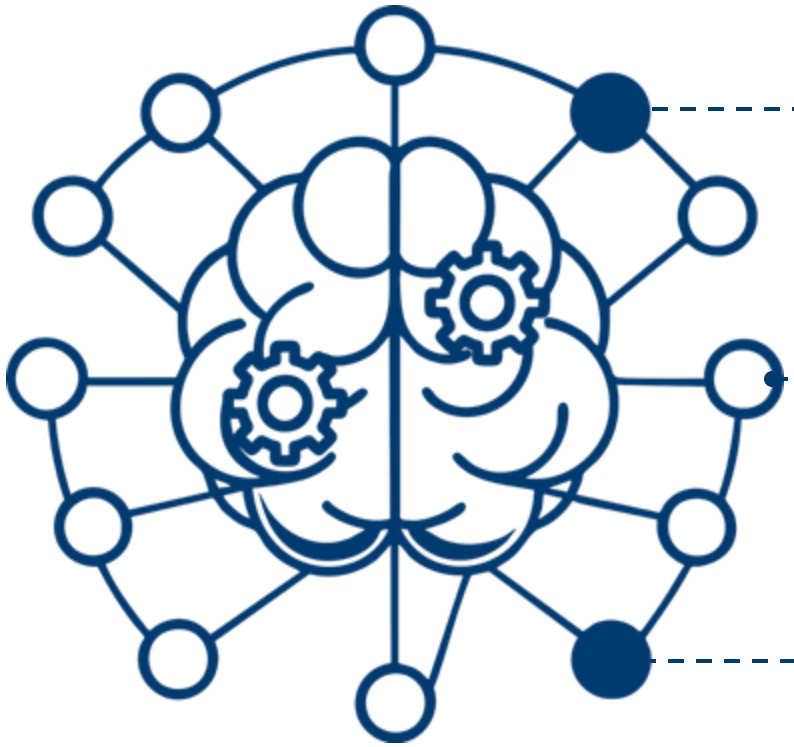
Cybersecurity workforce gap

Human error in breaches

95%

95% of incidents
tied to human error
(Verizon DBIR)

What Is Agentic AI?



Agents sense → decide → act

Use tools/APIs, retain memory, adapt

Fill realism gaps, but also threat vector

AI patched flaws in **seconds vs months** (DARPA CGC)

77%

77% of orgs already using AI in security

Training Benefits Of Agentic AI.

1. **Personas create realistic networks**
2. **Adaptive Red/Blue agents**
3. **Observers score impartially**
4. **Orchestration connects tools & roles**

70% Training cuts **70% of security risk** (Forrester)

30% Phishing training reduces clicks by **30%** (Proofpoint)

Realism, Readiness & Workforce Impact

- AI training improves realism, instincts, and operational realism
- Shortens MTTC, speeds containment
- AI-driven AAR = clearer, faster feedback
- Analytics track skill growth and operator performance
- Leaders see a true readiness picture

Containment

AI reduces containment time by **108 days** (IBM)

Feedback

Auto-generated AARs cut analysis to **seconds**

Outcomes

AI analytics improve outcomes by **24%**

Savings

Faster breach containment saves **$1.7M** (IBM)

Dual-Use Realities

AI = force-multiplier for defense

AI = amplifier for attackers

Dual-use is unavoidable

80%

80% see AI as positive for defense

74%

74% warn of AI-powered attacks as a major threat

Next Iteration: Agents as Attackers

1. **Beyond human playbooks**

2. **Discover zero-days autonomously**

3. **Defenders risk training on yesterday's attacks**

40%

40% of attacks use AI/ML (WEF)

47%

47% of orgs faced deepfake attacks (Deloitte)

Training for Agentic Attackers

Training must evolve with AI threats

Scenarios must stay current

AI attackers = new paradigm

Fraud

Deepfake fraud already hits **10%+ of firms**

Malware

AI malware **adapts to evade** detection (FBI)

Future Training Environments

Natural language build tools

Digital twins + AI alignment

Continuous upskilling demand

Upskilling

85% of employers need upskilling (PwC)

Shortage

Workforce shortage: **5M cyber pros needed** globally

ROI of AI-Augmented Training

Training = 3× ROI via prevented losses

AI speeds detection & containment

Faster learning, lower costs

$177K

Training saves **$177K** avg per org

$1.76M

AI containment saves **$1.76M** per breach (IBM)

Escalating Threats

Cybercrime costs →
$10T by 2025

2,200+ attacks/day
worldwide

Skills gap persists

67%

67% of orgs face cyber skills gaps

14%

Only **14% feel confident** in defenses

Adoption Path

Infrastructure first: on-prem vs off-prem, GPU/accelerator resources

Measure impact, prove realism

Orchestration enables joint environments

Start with AI observers or personas

Scale across services

90%

90% of orgs
not AI-secure-ready
(Accenture)

22%

Only **22%**
have AI policies

Discussion & Q&A

Where
to pilot realism?

Which
readiness metrics matter?

How
to handle AI ual-use?

Resilience

AI-ready orgs **69% less likely** to suffer advanced attack

Scale

Cybercrime → **$10T by 2025**

Data Sources

- ISC2 Workforce Study (2023)
- Verizon DBIR (2023)
- NATO, USCC, DARPA CGC
- IBM Breach Report (2024)
- Accenture AI Security Readiness (2024)
- WEF Cybersecurity Outlook (2023)
- Deloitte, Proofpoint, Forrester, ETS, Springer
- PwC Upskilling, EdTech outcome studies