AEGIS-AI
Round 2 Presentation Guide

5-6 Minute Killer Presentation

team-ZerOne | SnowHack IPEC

Tagline: Real-Time Deepfake Detection. Offline. Explainable. Unstoppable.

PRESENTATION STRUCTURE OVERVIEW

Section	Time	Purpose
1. The Hook	45 sec	Grab attention with real-world crisis
2. The Solution	60 sec	Introduce Aegis-AI differentiators
3. Live Demo	90-120 sec	Prove it works with demonstration
4. Technical Depth	60 sec	Establish credibility
5. Market & Business	45 sec	Show viability
6. The Close	30-45 sec	Memorable ending

SECTION 1: THE HOOK (45 seconds)

Purpose: Grab attention immediately with a real-world crisis scenario

Opening Statement:

> *"In February 2024, a finance worker in Hong Kong transferred $25.6 MILLION to criminals. Why? He attended a video call where his CFO and colleagues instructed him to do so. Every person on that call was a deepfake. AI-generated. Fake. And completely convincing."*

Escalation Points:

- This is not science fiction. This happened 11 months ago.
- Voice cloning now takes 3 seconds of audio. Three. Seconds.
- 95% of deepfakes are undetectable by humans.
- By 2027, AI-generated fraud will cost $40 BILLION annually.

The Real Problem:

> *"But here's what keeps security experts awake at night: What happens when a deepfaked military commander issues an order? When a fake emergency broadcast causes panic? When a cloned voice authorizes a nuclear facility access? In those moments, you have SECONDS to verify. No internet. No cloud. No time. What do you do?"*

Transition:

> *"We built the answer. This is Aegis-AI."*

Delivery Tips:

→ Pause after "$25.6 MILLION" for impact

→ Make eye contact when saying "Every person on that call was a deepfake"

→ Lower voice for "What do you do?" - create tension

→ Strong, confident voice for "This is Aegis-AI"

SECTION 2: THE SOLUTION (60 seconds)

One-Liner:

> *"Aegis-AI is the world's first OFFLINE-FIRST, REAL-TIME deepfake detection system designed for environments where failure is not an option."*

What It Does:

"Upload or record any audio, video, or image. In under 2 seconds, Aegis-AI tells you: Is this REAL or is this FAKE? With confidence scores, forensic evidence, and actionable recommendations."

5 Key Differentiators:

Differentiator	Explanation
100% OFFLINE	Works in bunkers, submarines, disaster zones. No internet required. Ever.
REAL-TIME	Sub-2-second analysis. In a crisis, you don't have minutes.
EXPLAINABLE	We show you WHY - spectral anomalies, pitch inconsistencies, evidence you can trust.
PRIVACY-FIRST	Media NEVER leaves your device. Zero data exfiltration.
FORENSICS-READY	Chain-of-custody logs, evidence hashes, court-admissible reports.

Target Users:

- Military and Defense Operations
- Law Enforcement Agencies
- Emergency Response Teams
- Financial Institutions
- Corporate Security
- Journalism and Media Verification

SECTION 3: LIVE DEMO (90-120 seconds)

Purpose: Prove it works with live demonstration

Setup Script:

> *"I'm going to show you two scenarios. First, a SYNTHETIC audio - something that could be a cloned voice. Then, an AUTHENTIC recording."*

Demo 1: Fake Audio (audio2.wav or audio4.wav)

> *"This is a synthetic voice sample. Watch what happens..." [Wait ~1 second] "SYNTHETIC DETECTED. 94% confidence. Look at these indicators:"*

- Pitch variation is unnaturally consistent - machines don't breathe
- Spectral artifacts showing vocoder signatures
- Missing micro-variations that human speech naturally has
- The system generates a forensic report with evidence hashes

Demo 2: Real Audio (audio1.wav or audio3.wav)

> *"Now let's try an authentic human recording..." [Wait for analysis] "AUTHENTIC. 96% confidence. Notice the difference:"*

- Natural pitch variation with breathing patterns
- Clean spectral profile without synthesis artifacts
- Micro-tremors and hesitations that AI can't replicate

UI Showcase:

> *"And this is our full product vision - supporting Audio, Video, and Image analysis. Batch processing. Complete analysis history. Professional forensic reports ready for export."*

SECTION 4: TECHNICAL DEPTH (60 seconds)

Opening:

> *"This isn't a prototype held together with duct tape. Let me show you the engineering that makes Aegis-AI bulletproof."*

Multi-Signal Ensemble Detection (6+ signals):

Signal	What We Detect
Pitch Trajectory	Human pitch varies 20-40Hz naturally. Synthesizers show unnatural consistency.
Spectral Artifacts	Neural vocoders leave fingerprints - harmonic distortions, phase discontinuities.
Temporal Consistency	AI generates frame-by-frame. Humans have continuous micro-variations.
Breathing Analysis	Humans breathe. AI doesn't. We analyze silence for biological signatures.
Formant Naturalness	Human vocal tract creates specific resonance patterns.
Microstructure	Jitter, shimmer, harmonic-to-noise ratio - biological markers.

Target Metrics:

- Equal Error Rate (EER): < 5% (industry standard)
- ROC-AUC: > 0.95 (excellent discrimination)
- Inference Latency: < 2 seconds (real-time)
- Model Size: < 50MB (edge-deployable)

SECTION 5: MARKET & BUSINESS (45 seconds)

Market Size:

- TAM: $40B+ AI fraud losses by 2027 (Deloitte)
- SAM: $8.5B deepfake detection market by 2030
- Growth: 41.5% CAGR - one of fastest growing security segments

Competitive Advantage:

> *"Every competitor requires cloud connectivity. Microsoft, Pindrop, Resemble AI - all cloud-dependent. We're the ONLY solution that works when the internet doesn't."*

Revenue Model:

Stream	Target	Pricing
Per-Device Licensing	Government & Defense	$500-2000/device/year
Enterprise Subscription	Financial, Media	$10K-100K/year
API Access	Developers	Usage-based

SECTION 6: THE CLOSE (30-45 seconds)

Summary Punch:

"In a world where anyone's voice can be cloned in 3 seconds..."

"Where a single deepfake can cost $25 million or trigger a crisis..."

"Where decisions must be made in seconds, offline, under pressure..."

"Aegis-AI is not just a product. It's a NECESSITY."

What We Built:

✓ Complete UI prototype showing full product vision
✓ Working localhost demo with real-time detection
✓ Multi-signal forensic analysis
✓ Privacy-first, offline-first architecture
✓ Court-ready forensic reporting
✓ Clear path to production deployment

Final Call to Action:

"We built Aegis-AI in [X] hours. Imagine what we build in [X] months. The deepfake threat isn't coming - it's HERE. And now, so is the solution. We are team-ZerOne. This is Aegis-AI. Thank you."

ANTICIPATED Q&A;

Q: How accurate is your detection?

A: Our architecture targets <5% Equal Error Rate. We use ensemble detection - 6+ independent signals that would ALL need to be fooled simultaneously.

Q: Can attackers bypass your detection?

A: Our multi-signal approach means attackers must fool spectrogram analysis, pitch tracking, temporal consistency, AND biological markers simultaneously. Plus federated learning enables continuous updates.

Q: Why not just use cloud-based solutions?

A: Three reasons: AVAILABILITY (no internet in field), LATENCY (cloud adds seconds), PRIVACY (sensitive audio cannot leave device).

Q: Who are your competitors?

A: Microsoft, Pindrop, Resemble AI - but EVERY one requires cloud. We're the only offline-first solution.

Q: Is this just a demo or a real product?

A: Functional demo + complete UI prototype. Detection works. Forensics work. We need resources to scale to production.

Q: What if deepfakes get too good to detect?

A: Detection has inherent advantages - we analyze at signal level. Even probabilistic detection with evidence is valuable.

DEMO PREPARATION CHECKLIST

Before Presentation:

- ■ Test Gradio demo launches: py model-demo/aegis_demo.py
- ■ Verify opens at http://127.0.0.1:7860
- ■ Prepare audio files (audio1-4.wav) in accessible location
- ■ Test UI prototype in browser (index.html, report.html)
- ■ Close unnecessary applications
- ■ Set browser to fullscreen mode
- ■ Have screenshots as backup if demo fails
- ■ Have screen recording of successful demo as backup

Demo Flow:

1. Open Gradio demo (already running)
2. Introduce what you're about to show
3. Upload synthetic audio (audio2.wav)
4. Walk through results - highlight key indicators
5. Upload authentic audio (audio1.wav)
6. Compare the differences
7. Switch to UI prototype
8. Quick tour: Dashboard → History → Report
9. End on forensic report page

MEMORABLE PHRASES TO USE

Power Phrases:

- "In 3 seconds, anyone's voice can be cloned. In 2 seconds, Aegis-AI detects it."
- "We don't just say fake - we show you WHY."
- "Your media never leaves your device. Period."
- "Built for the moments when the internet isn't there, but the threat is."
- "The only offline-first solution in a market full of cloud-dependent tools."
- "Privacy isn't a feature. It's the architecture."

Presentation Tips:

→ Start STRONG - your opening line sets the tone
→ Speak slower than feels natural - nerves speed you up
→ Pause after key points - let them land
→ Make eye contact with judges, not the screen
→ If you make a mistake, don't apologize - move forward
→ End with confidence - no trailing off

You've built something real. You understand the problem deeply. You have a clear vision. Now show them why Aegis-AI is UNREJECTABLE.

Good luck, team-ZerOne! ■■