PCDS Demo Walkthrough - Attack & Defense Flow

🎬 Complete Demo Script for Judges (2-3 minutes)

Step 1: Dashboard Overview (30 sec)

📍 URL: http://localhost:3000

What to show:

- Total entities monitored
- Active detections
- MITRE ATT&CK coverage (26%)
- Risk score and ML confidence

Say: *"This is our enterprise security dashboard showing real-time threat monitoring across 12 entities with machine learning scoring 68% high-confidence detections."*

Step 2: Trigger Attack Simulation (30 sec)

📍 URL: http://localhost:3000/soar

Actions:

1. Click **"DDoS"** button
2. Click **"Ransomware"** button
3. Click **"SQL Injection"** button

Watch:

- Incidents appear instantly
- "Auto Triaged" counter increases
- Shows ML engine attribution

Say: *"Watch as I trigger real attack simulations. Our ML ensemble instantly detects each attack type and automatically triages the incidents."*

Step 3: Live Detection Stream (30 sec)

📍 URL: http://localhost:3000/live

What to show:

- Attack events appearing in real-time
- MITRE ATT&CK technique IDs (T1566, T1071, T1486)
- AUTO-RESPONSE actions (kill switch, quarantine)
- 94% ML confidence on attack chain

Say: *"Our live feed shows the full attack chain: phishing email leads to C2 beacon, privilege escalation, and ransomware - all detected with MITRE ATT&CK mappings."*

Step 4: AI Copilot Analysis (45 sec)

📍 URL: http://localhost:3000/copilot

Actions:

1. Type: "Analyze the recent SQL Injection and DDoS attacks"
2. Press Enter

AI provides:

- SQL Injection indicators (UNION SELECT payloads)
- DDoS indicators (traffic volume, resource exhaustion)
- Remediation steps (WAF rules, rate limiting)
- MITRE technique references

Say: *"Our Azure OpenAI-powered copilot provides instant incident analysis with actionable remediation steps, helping SOC analysts respond faster."*

Step 5: MITRE ATT&CK Heatmap (15 sec)

📍 URL: http://localhost:3000/mitre

What to show:

- Visual heatmap of covered techniques
- 26% framework coverage

Say: *"Defense coverage mapped to the MITRE ATT&CK framework, showing exactly which techniques our ML models can detect."*

🎯 Key Stats to Mention

Metric	Value
Training Data	5.5M+ samples (UNSW-NB15 + CICIDS)
Accuracy	88.3%
False Positive Rate	2.8%

MITRE Coverage	26% (12 techniques)
Response Time	Real-time

Demo Tips

1. **Start with attacks paused** - Then enable to show live action
2. **Keep AI questions short** - One clear question per demo
3. **Show the AUTO-RESPONSE** - Key differentiator vs competitors
4. **End on MITRE heatmap** - Visual impact

Quick URLs

- Dashboard: http://localhost:3000
- SOAR Attack Sim: http://localhost:3000/soar
- Live Feed: http://localhost:3000/live
- AI Copilot: http://localhost:3000/copilot
- MITRE Heatmap: http://localhost:3000/mitre
- ML Metrics: http://localhost:3000/ml-metrics