

DAY-CON XVIII
EVOLUTION REVOLUTION

FRIDAY DECEMBER 20, 2024

DAY-CON.ORG

RULES OF THE ROAD

- ATTRIBUTION IN FULL EFFECT – SECURITY SUMMIT IS BEING RECORDED
- ALL DELEGATES ARE EXPECTED TO INTRODUCE THEMSELVES, BE PRESENT, ENGAGE AND BE RESPECTFUL TO THE OTHER DELEGATES [EVEN WHEN YOU DON'T AGREE] – “DIVERSITY IS GOOD FOR THE SPECIES”
- EACH TOPIC SHOULD BE TAGGED WITH ONE OR MORE OF THE FOUR DAY-CON DOMAINS: RADICAL THINKING, TOOLS OF THE TRADE, BEYOND EMBEDDED OR POINT OF ORIGIN HACKING (POOH)
- HAVE PHUN, BE SAFE AND TEACH & LEARN SOMETHING



AGENDA

- INTRODUCTIONS – “WHAZZUP?”
- EVOLUTION REVOLUTION- ANGUS
- TALKS
- LUNCH W/SPECIAL GUEST FIRESIDE CHAT
- MORE TALKS
- PROBING QUESTIONS TO POUNDER AS A GROUP
- WRAP-UP
- RECEPTION
- AFTER PARTY

EVOLUTION REVOLUTION



- ALTER EGO BRYAN FITE HAS A NEW GIG WITH WWT
- BLISS INDEX
 - ONLY WORK ON PROJECTS THAT GIVE ME JOY
 - WITH PEOPLE I LIKE
 - TO MAKE THE WORLD A BETTER PLACE

<https://www.getsecure.com/blog/files/16c6275f66dbe1aacec8f4ef35a2ee73-3.html>



1. ALPHABET
2. AMAZON
3. APPLE
4. META
5. MICROSOFT
6. NVIDIA
7. TESLA



NIST AI 600-1



HOW DOES YOUR
MOVIE END?

INSIGHT FROM THE LAST SEVEN MONTHS

- TRUSTWORTHY & RESPONSIBLE AI IS NOT EASY FULL STOP
- TONE AT THE TOP MATTERS
- BASIC GENERATIVE AI SAFETY IS LACKING IN ALL SECTORS AND STAKEHOLDER COMMUNITIES

- “MIND THE GAP” - RISKS THAT MANIFEST AS THREATS WILL CAUSE HARM UNLESS ADDRESSED



PACKETWARS™

WHAT IS THE...

**DEEP FAKE
JUSTICE LEAGUE**

A small group of like-minded individuals and organizations that want to make the world a safer place for humans. Don't reinvent the wheel, highlight the good, call out the bad and create forums for "winning".



PACKETWARS™

2025/2026 DEEP FAKE CAMPAIGN

DEEP FAKE JUSTICE LEAGUE



Evil Robot AI presents The 2025 Hacksec Packetwars Invitational, featuring the Deep Fake Justice League. Do you have what it takes to attack, defend, survive and thrive in a world where you can't trust your senses? Strut your stuff – September 13th, 2025 @ Day-Con XVIII”



SOFT OPENING OCTOBER 2024

Hiding From Robots: Mr. Bean Goes To CornCon X



October 4, 2024

CORNCON X BATTLE BRIEFING

Attention:
Intel suggests there are other hostile agents at large and engaged. Practice enhanced OpSec and protect yourself at all times.



An unbalanced AI threatens to ruin the conference for some of our favorite neighbors!!

OPERATION: "MR BEAN GOES TO CORNCON"

A rogue AI, trained exclusively on vintage Mr Bean videos, has infected the far reaches of the internet and now has its eyes (and IoT) set on cloning as many CornCon X attendees as possible!

In the heart of a city teetering on the edge of destruction, the Deep Fake Justice League stands united. Their eyes fixed on the monitors unable to do anything, but watch as they have been isolated by their own compromised Zero Trust software (negative reviews queued up in the outbox).

"We can't do this alone," booms Angus, through Chiron's ham radio rig. "We need someone new. Someone with mad skills!" Suddenly, a shadow appears on camera—a figure with untapped potential. "Will you join us?" asks Studentofbits, his voice cutting through the chaos. "AI Mr. Bean is no ordinary foe, but together, we can contain it!" It's time to step up. The Deep Fake Justice League needs you.

Step 1: Observe AI Mr. Bean from a safe vantage point. Analyze it for weak spots, and note any potential vulnerabilities. As Gilch quipped over a vintage fax machine, "The key to defeating this foe is to become invisible."

Step 2: Follow Angus's instructions to gain deeper insight. "What's powering this thing? Any defenses we need to bypass? Find out where it's weakest—and hit it hard."

Step 3: Submit up to three pictures that allow you hide from AI Mr. Bean and avoid detection. So you and your neighbors can't be cloned. —The path to victory begins here.

Your Mission: Hide from the rogue AI, save CornCon and join the Deep Fake Justice League.



Beyond Embedded:
In the age of the Internet of (Deadly) Things the line between the physical and digital no longer exists. Do you have what it takes to Attack, Defend and Survive?