DIVISION ZERO (DIV0)
AI SECURITY QUARTER

Introduction to DivO's AI Security Quarter

#AISQ

Matthias Chin
CCIE, CISSP, GCIH, GCFA, GWAPT

Agenda

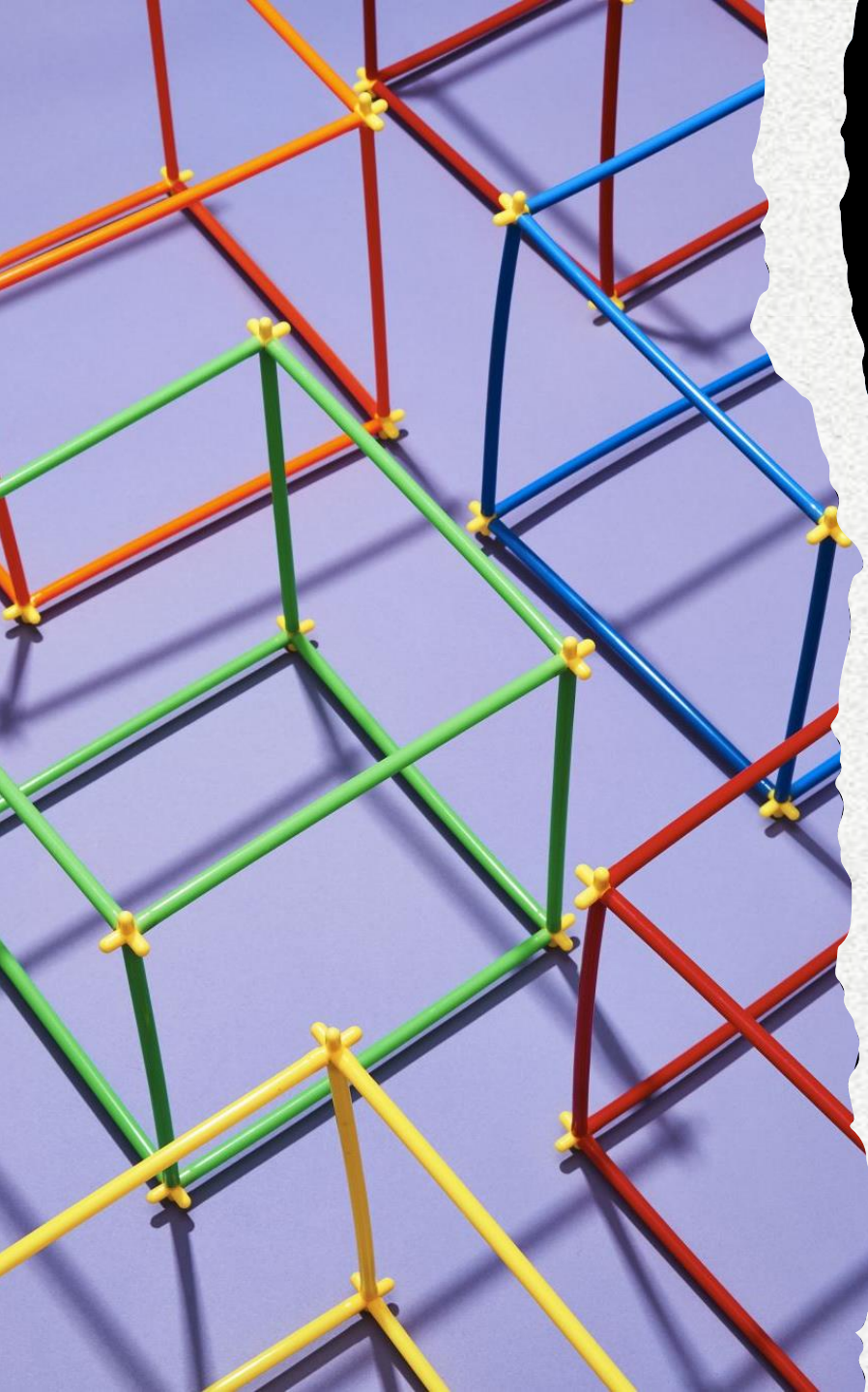
- 7:00pm: Lobby & Networking (20mins)
- 7:20pm: Div0 Introduction & Announcements (10mins)
- 7:30pm: Div0 AI Security Quarter (AISQ) Launch & Introduction by Matthias Chin (10min)
- 7:40pm: "Algorithmic Weaknesses and Cybersecurity Skills of the Future" by Gerry Chng (30min)
- 8:10pm: "Looking Beyond Model Performance" by Dr. Weng Jianshu (20min)

Examples of Adversarial Attacks on AI Systems

According to a Gartner report. 30% of cyberattacks by 2022 will involve data poisoning, model theft or adversarial examples.

Why #AISQ?

- Cyber security and AI are both critically important technologies for the digital future
- Adversarial attacks on native AI systems are becoming a bigger concern
- In addition, hackers are using more automation and AI to help them probe and attack systems
- As such, it is imperative to help cyber security specialists build up their AI awareness and knowledge so that
  - they can incorporate more automation and intelligent AI systems to counter attackers
  - they can help to provide advisories on securing AI systems in future



Objectives

- To connect enthusiasts in the intersection of AI and cyber security
- To empower cyber security folks with AI awareness and knowledge
- To discuss use cases and topics on solving cyber problems with AI
- To discuss and share about cyber adversarial attacks on AI and their counter measures

Goal: To build a vibrant learning and sharing AI-cyber community. We envision strong and innovative skilled professionals and tech leaders in the AI-cyber space to arise from div0 in the coming days!

Current Core Team

Matthias

Gerry

Russell

Denny

Jasmine

We will start to plan for the first 1-2 events first and will likely expand the Core Team as the Quarter grows

Roadmap

Year 1-Laying the Foundations

- Setting Up the Quarter
- Start Learning and Sharing culture in AI-Cyber topics
- 1st AI Security CTF at SINCON event

Year 2-Growing the Core Team and Community

- Enlarging the Community
- Start community-based AI Security Projects
- Deepen Learning and Sharing topics in AI-Cyber
- 2nd AI Security CTF

Year 3- Expanding Our Impact

- Outcomes from community led projects
- Raise up AI-cyber leaders
- Continued empowerment on AI-cyber topics
- Mentor and transition to new leadership team

Jumpstart Your Learning Journey

Upcoming Activities

16 Apr 2021	Fireside Audio Chat
Jun 2021	Workshop to Jumpstart Your Deep Learning Environment
Sep 2021	Panel discussion on AI and Ethics or AI Security Career
Oct/Nov 2021	AI-Security CTF in SINCON
Dec 2021	Tech talk (Speaker TBC)

Call for Volunteers

Group 1
Technical volunteers to help create challenges in upcoming AI-CTF

Group 2
Volunteers to help organize or contribute to AISQ community

Sign Up Here : https://bit.ly/2PkHc2c

next up

Algorithmic Weaknesses and Cybersecurity Skills of the Future by Gerry Chng

Thank you and any feedback welcome