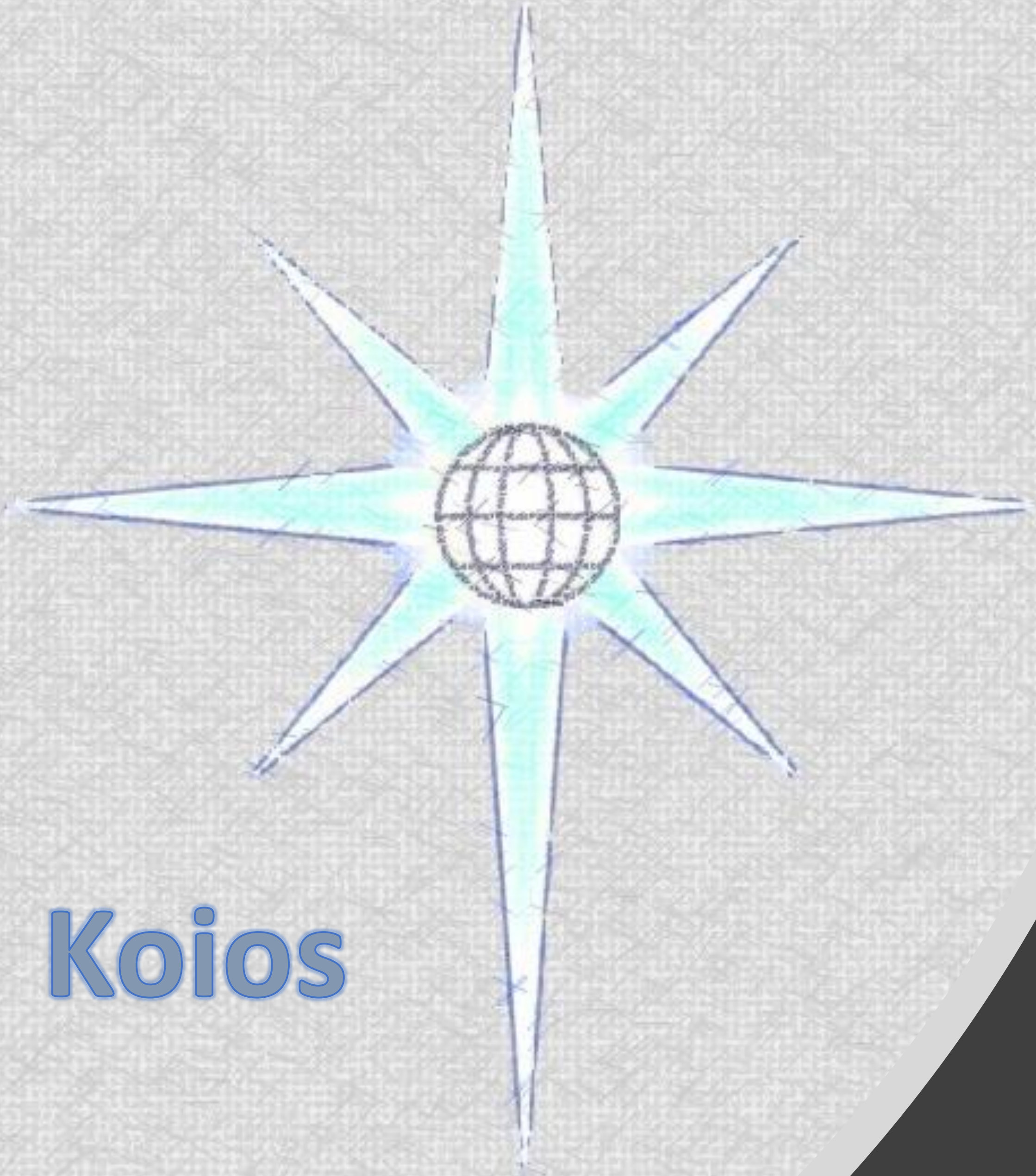

Koios

- A Cyber Incident Response Game

Scenario 2

Before we begin

- You as a player will be yourself in this game, with your current job and responsibilities
- We will walk through an incident scenario. It is allowed to ask questions if anything is unclear
- Discussion amongst each other is allowed and highly recommended
- Don’t fight the scenario! Try to think how you would act if this was real. You don’t know everything at once in real life. Same goes for the game. Be patient and ride the wave!

Something has happened…

Listen to the game master!

4pm - Day 1

[PLAYER] gets a phone call from [1st LINE OR USER]

[INSERT SYSTEM] is not accessible.

5pm – Day 1

SYSTEM NAME]’s event log shows error messages.

7pm – Day 1

While working on the system it suddenly gets a bluescreen and reboots. The system restarts, but some services does not.

8am - Day 2

Mayhem has broken lose. Someone’s deadline depends on gaining access to the information on the system.

[PLAYER] needs to roll to see if they can get the users to calm down long enough to come up with a solution

9am - Day 2

Turns out that the disc controller is not working.

What to do?

10am - Day 2

There is some problems getting the parts needed. How do you proceed?

10.05am - Day 2

[PLAYER] Gets a phone call from [DAYCARE/SCHOOL, find someone with a kid]. Their child has a fever and you need to pick up the kid.

Roll without modifiers

1-10 = you are stuck at home with a sick kid until tomorrow

11-20 = You only have to make a few phone calls to arrange pick up. Take a small timeout until the game master says you are back from making calls.

11am - Day 2

The Files on the system is not retrievable. Do you have a copy? And when was it last copied?

1pm - Day 2

[SOMEONE HIGH LEVEL] is calling to ask when the system will be up again. Calculate an estimated time-line and present it to [SOMEONE]

3pm - Day 2

[C-LEVEL] Wants a preliminary report of the incident by tomorrow morning. They also wants a clear plan on how to prevent this from happening again.

Create the plan as in depth as you are told within the given deadline, and present it.

Review time!

3 phases of review – This is the first
Please answer the documents handed out as well.

- Did the response go as planned? What was done well, and what can be improved?
- Did the incident response plan work according to the scenario? If not, what didn’t work? Do you have any suggestions on how to fix this?
- Was Service Level Agreements and contractual obligations met during the simulation? What did not seem to work and how can it be improved?
- Were the roles and responsibilities of everyone clear and did everyone know what others were responsible for?
- Did everyone know who needed to communicate what and to whom? Was all contact information available?
- Looking at the scenario, what could we have done to prevent it from happening all together?
- Did we have enough monitoring and auditing to adequately support the investigation process?
- How was the media handling done? And how was the communication plan with other relevant third parties such as law enforcement, contractors, partners, etc.?
- How was the reporting done? Was it good enough? Did everyone get the information they needed, and was everything documented appropriately during the incident handling?

Thank you for playing

Stay vigilant!