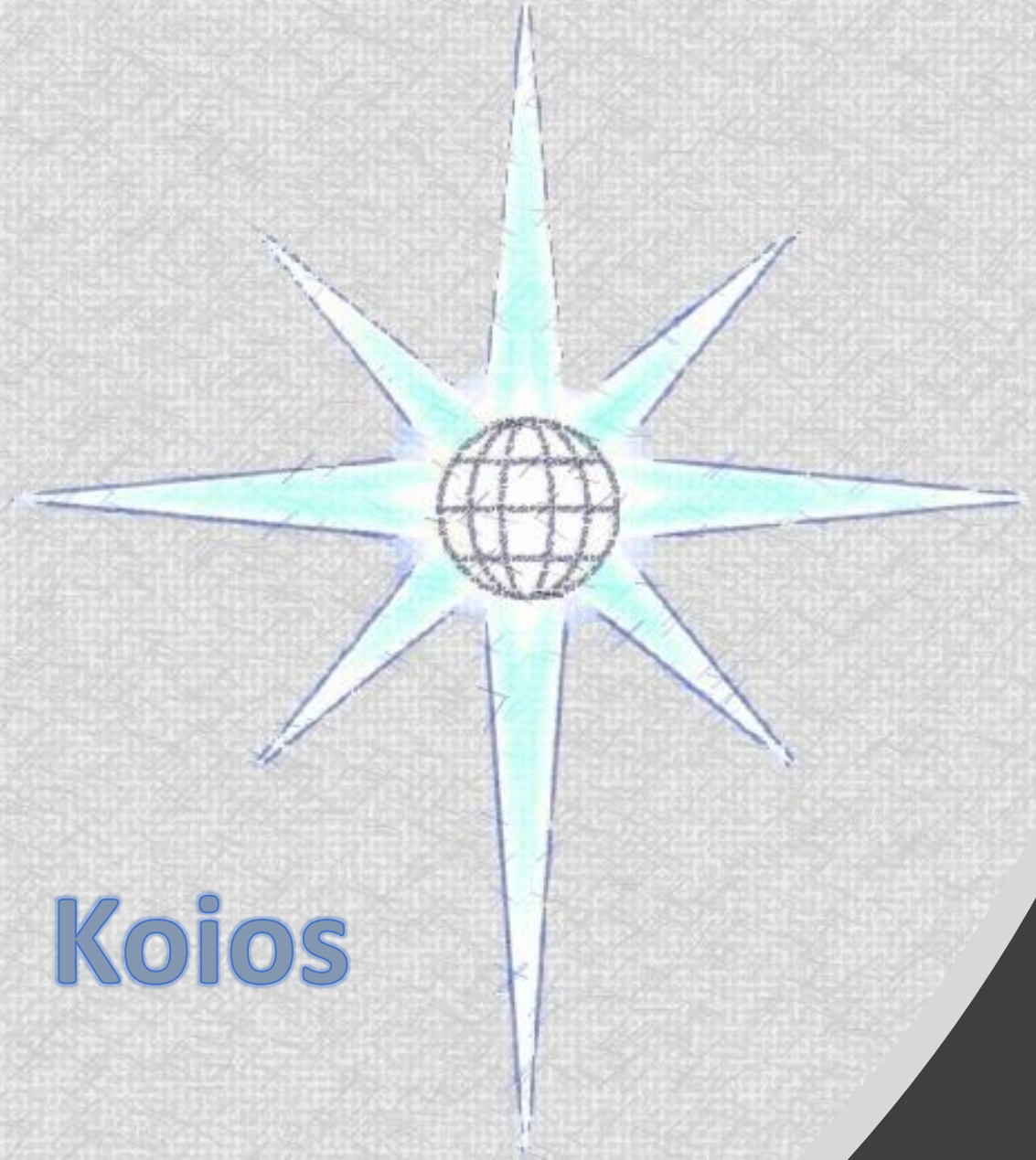

Koios

- A Cyber Incident Response Game

Scenario 1

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!

8am - Day 1

[PLAYER] gets a phone call from [SOC OR OTHER RELEVANT LOG PERSONNEL]

There has been an increase in log activity. Several successful login attempts towards the [INSERT SYSTEM] has been done at odd times for the last two nights.

1pm – Day 1

[DIRECTOR NAME] gets an email. It is a mail from a hacker group stating they have your data.

- The mail reads: “Pay up 3 million USD to this bitcoin wallet or have the data publicised for everyone to see”

1.05pm – Day 1

[DIRECTOR NAME] calls [PLAYER] to get information. There is a lot of questions.

Roll (without modifiers) to see if you will be able to end the call quickly or if you are out of commission to help the team for some time.

9pm - Day 1

[PLAYER] gets a call from [DIRECTOR]. Media has alerted them of a tip they have gotten about some data that stems from your company.

Regardless of your actions, the hacker group has publicised your data on Pastebin.

8am - Day 2

Several media companies has called and wants a statement about the information leak

10am - Day 2

[SUPPORT/RECEPTION-CONTACT POINT] are being flooded with stressed out [CUSTOMERS/USERS]. Each demanding answers on what has been lost of information relevant to them.

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.

9am - Day 3

Logs shows another user account has been trying to log on [UNUSUAL SYSTEM ACTIVITY TOWARDS ANOTHER SYSTEM].

1pm - Day 3

A talk with the owners of the user accounts shows that they both got an e-mail last week requesting them to log in.

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!