TOLLETATEN
NORWEGIAN CUSTOMS

# Hvordan trene på hendelseshåndtering

## - uten å involvere konsulenter

20. September 2023

Ragnhild “Bridget” Sageng
Senior sikkerhetsrådgiver

TOLLETATEN
NORWEGIAN CUSTOMS

# Hei!

- Ragnhild Sageng, Senior sikkerhetsrådgiver i Tolletaten
- Sikkerhetskultur
- Tidligere etisk hacker innen sosial manipulasjon og OSINT.
- Foredragsholder DEFCON, Black Hat Europe, Sikkerhetsfestivalen og KiNS-Tech i fjor

TOLLETATEN
NORWEGIAN CUSTOMS

# Dagens prat...

- Hvorfor trener vi på hendelses håndtering?
- Hvordan få det til i praksis?
- Koios, og andre spill

TOLLETATEN
NORWEGIAN CUSTOMS

# Hendelseshåndteringstrening

- Definisjon
- Sikkerhetsbildet i dag
- Hvorfor er det viktig å trene og hva får du igjen?
- Rammeverk: NIST, ISO 27035, SANS

TOLLETATEN
NORWEGIAN CUSTOMS

# Hvorfor blir det ikke gjort?

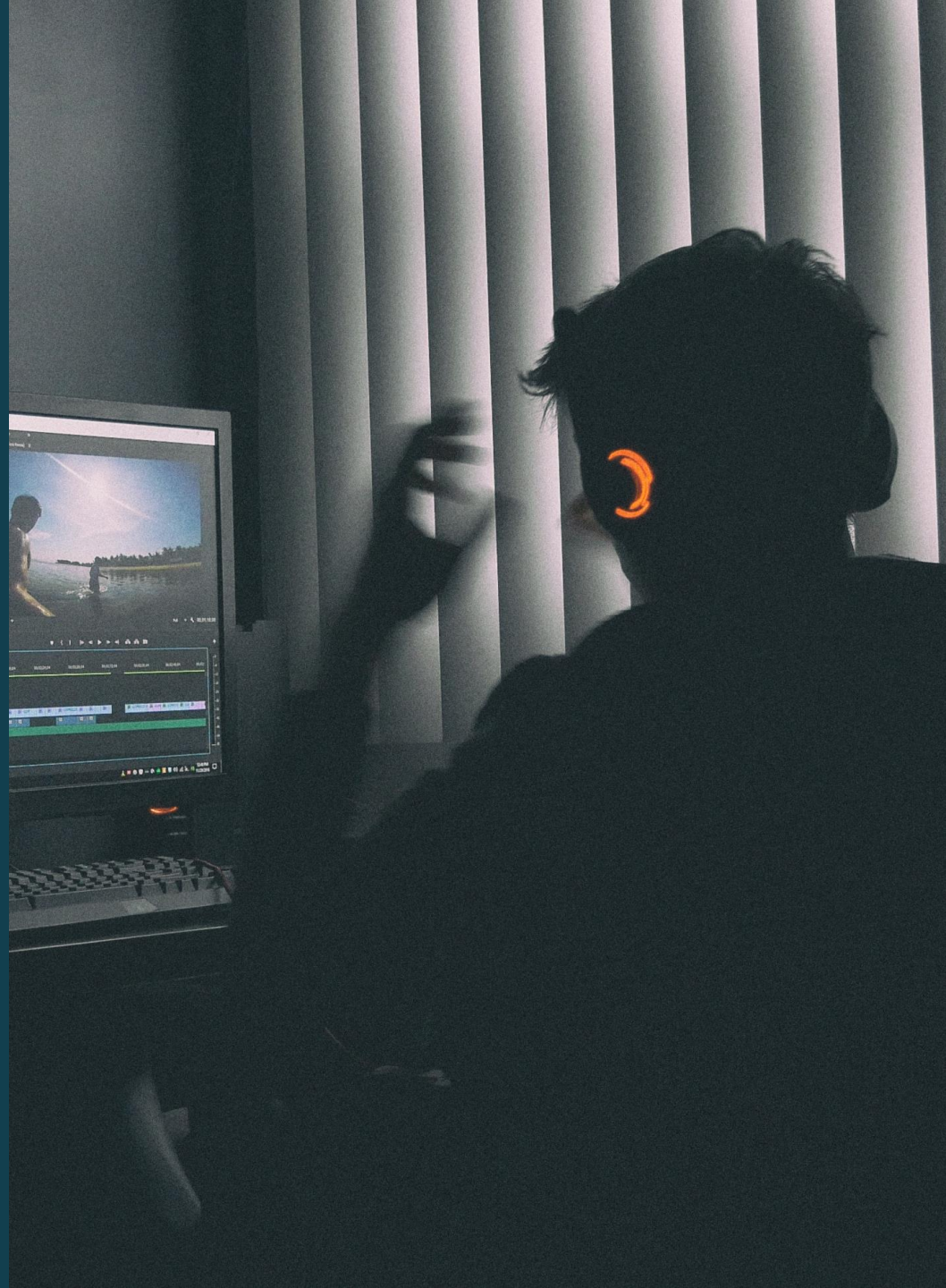
- Dyrt
- Tidkrevende
- Omfattende

**Lite støtte for å gjennomføre fordi ikke alle vet hva det innebærer**

TOLLETATEN
NORWEGIAN CUSTOMS

# «Gamification» (spillifisering)

- Tilføring av spill-elementer til en aktivitet
- Gir mer tilbakemelding til spillerne
- Folk investerer mer av seg selv
- Erfaringer huskes bedre



TOLLETATEN
NORWEGIAN CUSTOMS

# Spillifiserte treningstyper

- «Tabletop» - trening
- Simuleringsøvelser, Rollespill
- Digitaltrening, PC-spill
- Kortspill og brettspill

TOLLETATEN
NORWEGIAN CUSTOMS

# Teknikker innenfor spillifisering

- **Dr. James Paul Gee**
  - Fokus på læringsbasert spilling
- **Yu-kai cho (Octalysis)**
  - Fokus på spilldesign for ønsket respons
- **Kombinerte disse**


Figure 3.1: The Octalysis Framework.
*The Octalysis Graphical Representation* (2017)

TOLLETATEN
NORWEGIAN CUSTOMS

| Main categories | Common principles | Common core values | Unique values and principles | IRT game values for measurement |
|---|---|---|---|---|
| Empowered learner | Co-design principle<br>Customization | Ownership and possession | | Adaption |
| | Identity principle | Epic meaning and calling | Manipulation | Immersion |
| Invoking problem-based learning | Pleasantly frustrating | Unpredictability and curiosity | | Unpredictable gameplay |
| | | | Development and accomplishment | Feeling of accomplishment |
| | | | Give information just in time or on-demand<br>Fish tank | Avoiding information overload |
| | | | Skills under strategies | Accomodate stategic thinking |
| Deeper understanding | | | System thinking<br>Situated meaning | Practical applicability |
| | | | Empowerment of Creativity and feedback | Review and feedback |
| Avoid loss | | | Loss and avoidance | Player's ownership |

Figure 3.2: Overview of the Combination of Principles.

TOLLETATEN
NORWEGIAN CUSTOMS

# Faser som bør være i treningen

- Planleggingsfasen
- Før spillet starter
- Spill-fasen
- Refleksjonsfasen


**Planlegging og refleksjon er ekstremt viktig for suksess!**

TOLLETATEN
NORWEGIAN CUSTOMS

# Forskjellige spill

- Rollespill
  - Oh Noes!
  - Cubicles and compromise
  - Koios
- Kortspill
  - Backdoors and Breaches
  - Exploited in the wild

TOLLETATEN
NORWEGIAN CUSTOMS

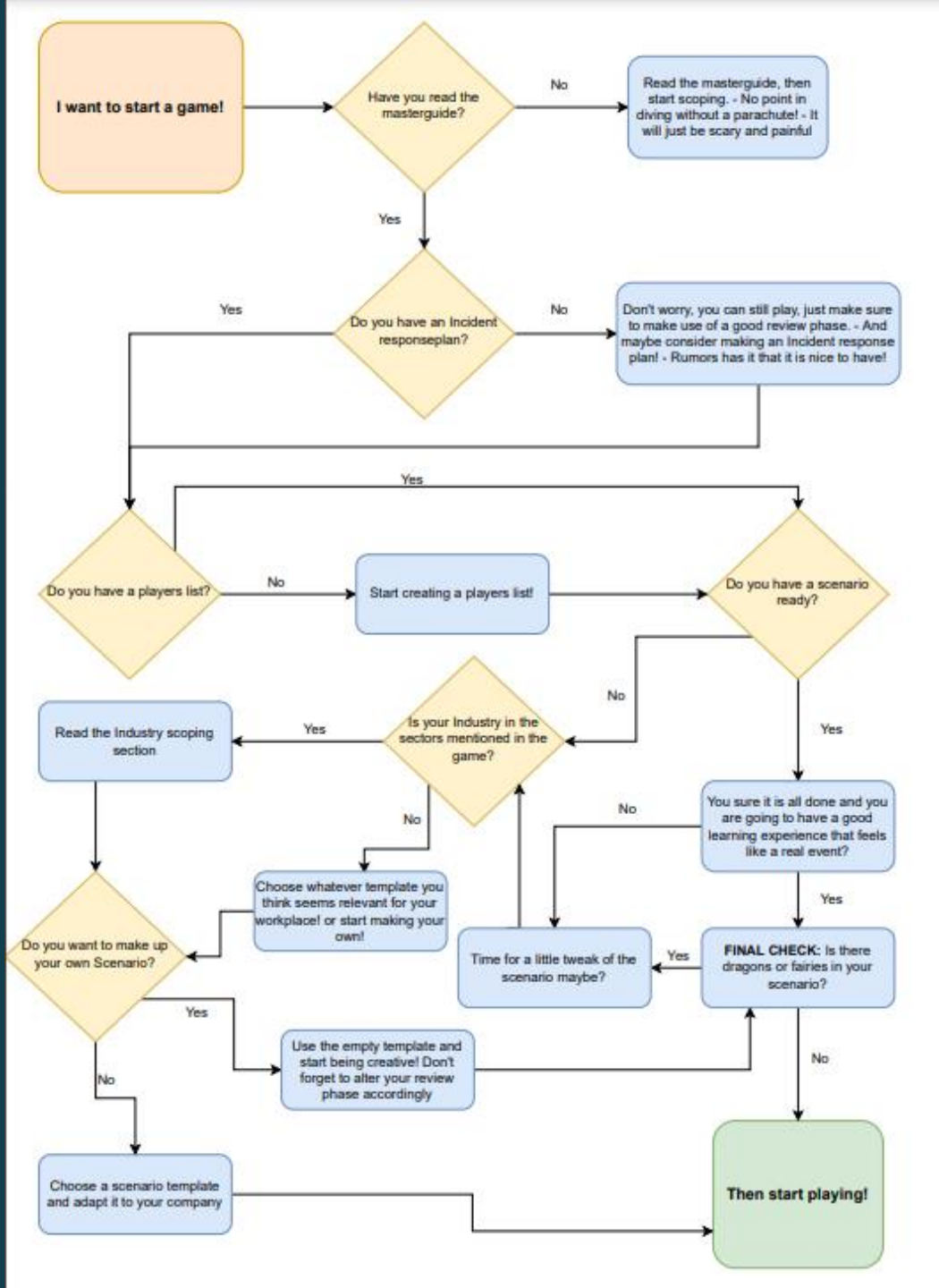
# Koios

- https://github.com/Lixona/Koios
- Før spillet: Les master guide
- Forenklet Dungeons and Dragons
  - Uten drager

TOLLETATEN
NORWEGIAN CUSTOMS

# Scoping fase

- Før man starter et spill bør man alltid lese alle dokumenter tilgjengelig
- Flytskjema for å se om dere er klare
- Noen Industrielle scoping dokumenter tilgjengelig



TOLLETATEN
NORWEGIAN CUSTOMS

# Scenario

- **Standard scenarioer**
- **Anbefalt å tilpasse, evt. lage egne som passer bedriften så mye som mulig**

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.

Koios

**Game master Scenario sheet**

**Scenario number:** 1

**Scenario Name:** Phishing Gone Ransom, - Information Theft

NOTES:

This scenario needs to be adapted to the company before starting to make it more immersive! Note: Incase of multifactor authentication. Add a scene with a vishing call where someone has gotten hold of the MFA and change the login attempts to just one per person.

| Inject number | Inject details | Background info | Needs to be examined before | Relevant Questions |
|---|---|---|---|---|
| 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. | The log activity is successful logins to x system. Data is gone (decide what data this will be prior to the game) | | Has any data been exfiltrated. What has been taken? How long did the logins last? |
| 2 | [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" | Create an email for immersiveness. You can use local currency, language and APT group name as you wish. | | Is there anyone else being attacked by this group? Background check? Will the data still be disclosed even if we pay up. If the lack of data has not been discovered yet, what is gone? |
| 3 | [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. | The roll is to take a player out of commision to see how the others fill in he gap. Take out an important player or someone playing a ke role in Incident handling to see what happens. | 4 | What will you do without this player? How to proceed when someone with a key role is gone? |
| 4 | [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. | The data is out | | How to handle this initial phase? Is someone handling the media? What is planned to disclose, and how? Will they ask for what the media know? How to remediate the leak? |
| 5 | Several media companies has called and wants a statement about the information leak | A statement is needed to the media. | | Has everyone been alereted. Customers, partners etc? Maybe they don't want to find this out by media, but from you first? |
| 6 | [SUPPORT/RECEPTION CONTACT POINT] are being flooded with stressed out [CUSTOMERS/USERS]. Each demanding answers on what has been lost of information relevant | A little distraction into the incident | | How to lower the pressure for information? What can be disclosed? Is it important to answer every call? (Probably) How to keep the information flow between 1st line and |

**Main Focus for the Scenario:**

**Investigative techniques**
- How quickly did they investigate the background for the breached user/
-Was the investigation done methodologically?
- **Media and customer handling**
- Is anything done prior to the disclosure?
-How is media handled after the disclosure?
-What information will go out to the customers?
**Remediation after breach**
- User management of the breached user
-Check for more possible breaches in the same manner, there is probably more than one getting that email
-Is all data that has been lost accounted for, do they have an overview and can give information to the correct people?
**How to avoid this from happening again**
- Awareness training plan?
-Block logins at certain times during the day and from different regions? (if this is already blocked, what else could have been done?)

**Information to read before starting:**

Successful login attempts has been done towards a system (insert system with sensitive data for the company) from a specific user account (needs to have access to the system) and data has been exfiltrated. The data is sensitive (insert sensitive data related to the company, preferably customer data).
Later at the day of discovery, the director will recieve an email with a bitcoin ransom for the hacker not disclosing the data (- TIP! make a ransom email to present for immersiveness). The hackers belong to a hacker group and are known for this type of activity. They have a history of disclosing their bounty no matter if a company pays the ransom or not.

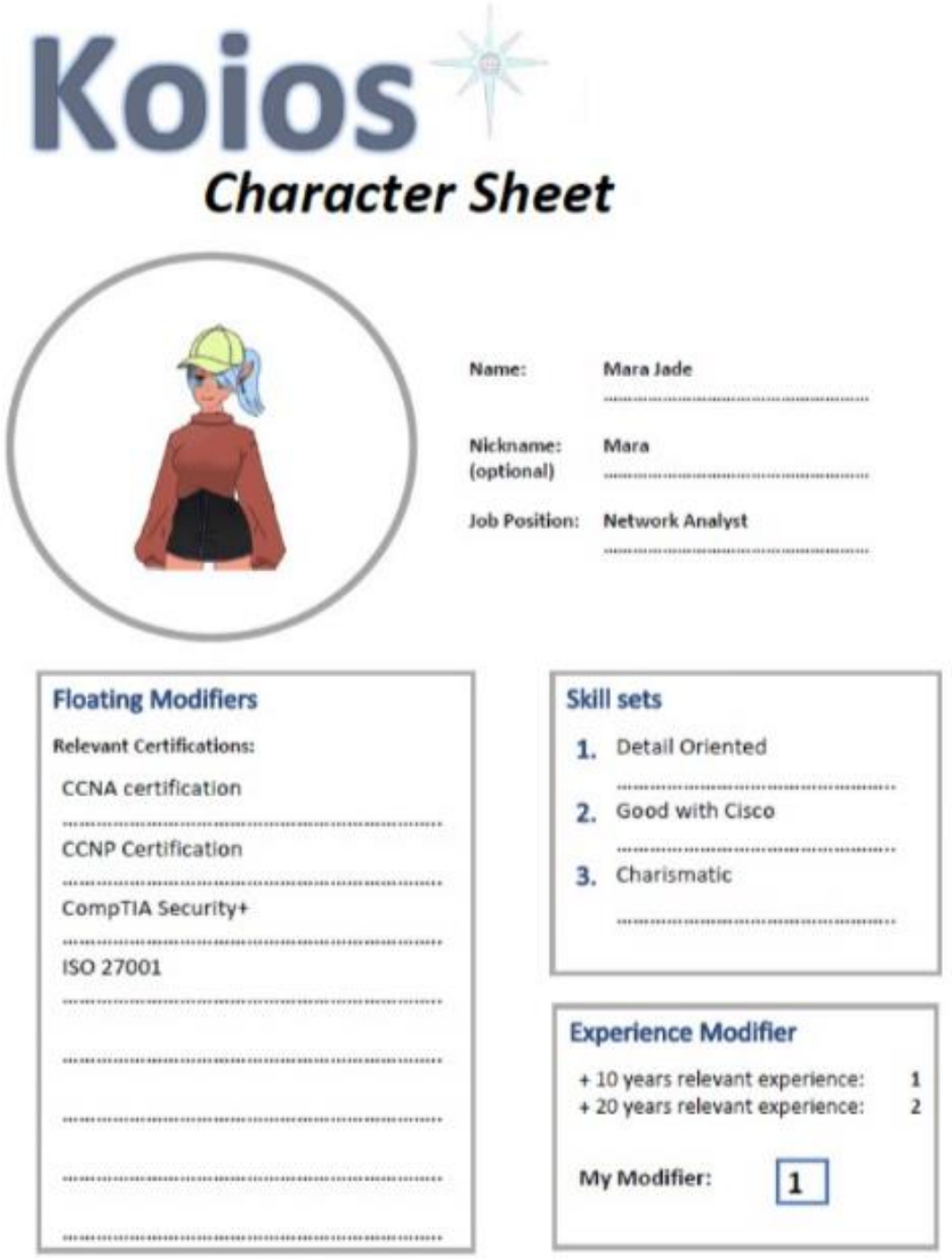
The data will show up being posted online no matter what the company decides to do. The company has to deal with the aftermath of this.

Further investigation into the specific user account being abused shows that the user recieved an email last week. The email was a phish disguised as IT, prompting the user to log into a system (using the same credentials as the one being breached). (- TIP. Make a fake email to make this more immersive, and go through the tells on why this was fake.)

TOLLETATEN
NORWEGIAN CUSTOMS

# Karakter-kort

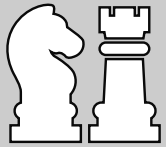
- Modifiers brukes til å legge til ekstra poeng på terningen
- Egenskaper sies av de rundt bordet
- Legg inn sertifiseringer og erfaring
- Du eller de rundt må huske å bruke modifiers



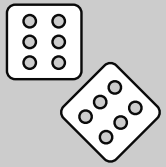
TOLLETATEN
NORWEGIAN CUSTOMS

# Spill-fase

- **Spillet fungerer best når alle som skal være med deltar**
- **Loggfør alle bestemmelser**
- **Injects (innskytninger) og terning**
- **Game-master bør spørre om grunn for valg**



Game-master



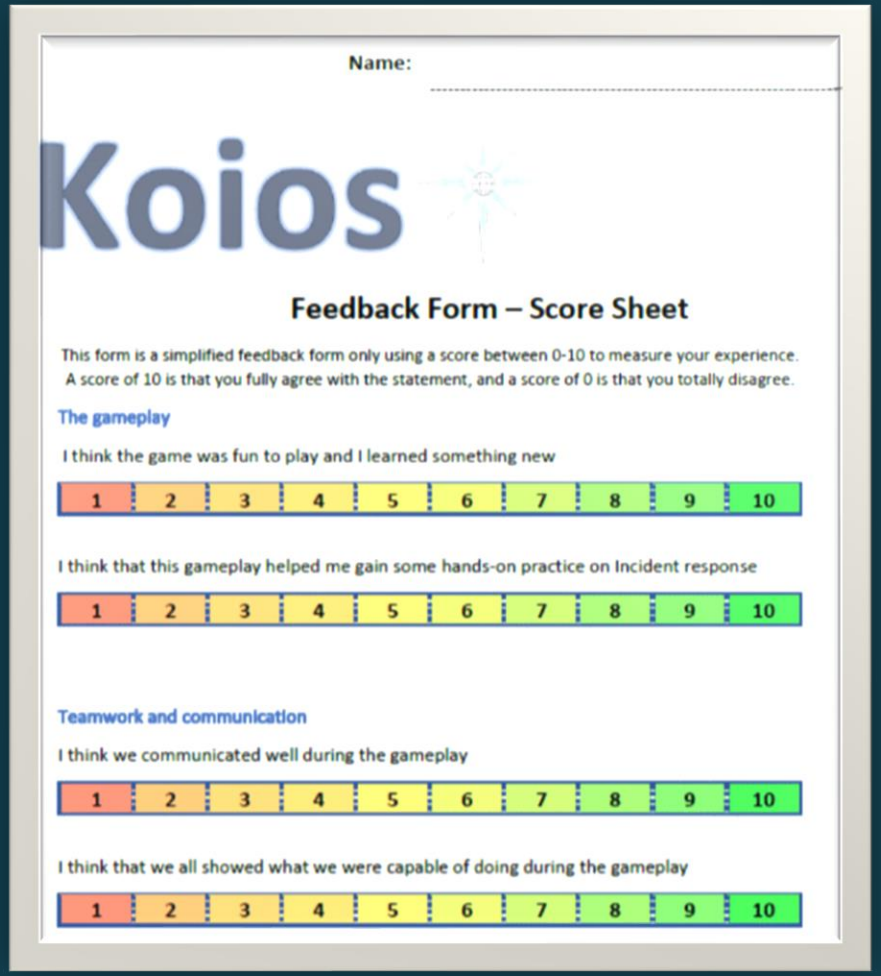
D20 (terning)

Karakterkort

TOLLETATEN
NORWEGIAN CUSTOMS

# Evalueringsfase

- **Spillevaluering**
  - I plenum, og som innlevert ark
- **Kommunikasjon- og samarbeidsevaluering**
  - Game master fyller ut.
  - Spillere kan også hvis man ønsker
- **Tilbakemeldingsskjema**
  - Score/temperaturmåling



Name: .....

Koios

**Feedback Form – Score Sheet**

This form is a simplified feedback form only using a score between 0-10 to measure your experience.
A score of 10 is that you fully agree with the statement, and a score of 0 is that you totally disagree.

The gameplay

I think the game was fun to play and I learned something new

1 2 3 4 5 6 7 8 9 10

I think that this gameplay helped me gain some hands-on practice on Incident response

1 2 3 4 5 6 7 8 9 10

Teamwork and communication

I think we communicated well during the gameplay

1 2 3 4 5 6 7 8 9 10

I think that we all showed what we were capable of doing during the gameplay

1 2 3 4 5 6 7 8 9 10

TOLLETATEN
NORWEGIAN CUSTOMS

# Hvor skal man begynne?

- Finne det som passer for dere
- Hva er viktig? Avgrens!
- Hvor mye tid har du?
- Få det inn i årshjulet

**Forankring både i ledelsen og blant de ansatte**

TOLLETATEN
NORWEGIAN CUSTOMS

# Takk for meg!

@ragnhild_bss

linkedin.com/in/ragnhildsageng


**https://github.com/Lixona/Koios**

ragnhild.sageng@toll.no