



Exercise Behavioural Observation

Goal of the exercise: reacting to possible red flags

Lessons learned:

- Different departments need to cooperate and share concerns, observations, and any other relevant information;
- Information must be gathered;
- Small pieces of information can indicate a possible threat;
- Procedures must be put in place to handle information;
- The conversation with the person is necessary, but some training may be needed;
- Culture has a big impact on how a reaction is analysed.



EXERCISE (60min)

Exercise Explanation (3 mins)

Outline: Participants will be divided into 7 different groups. Each group will receive a specific role in a hypothetical facility. We ask that each group relate this exercise as much as possible to their own work environment.

In the role that the group has been given, they will look at a specific person, named Claudia, working in the same facility. Based on the information you receive (from yourself or added by others), the group will reflect on certain questions, and everyone will be able to decide for themselves if further actions need to be taken or not.

It is important that the exercise is played out in the reality of the participant. (S)he should try to look at the signs as if it was happening in his/her own organisation with his/her own legal background.

Known by the entire participants group:

General bio for Claudia: Claudia has a good profile and is somewhat overqualified for the function she is currently in. Claudia was one of many candidates for this job, but was able to convince the hiring committee that she was best fit for the job. She didn't come from the same sector, but has good credentials. During the recruitment process Claudia had a social attitude and was very open to everyone.

Once hired, she was initially delivering on and achieving her potential while working in the technical areas of the facility. However, her good performance did not last for long. We have no concrete information on her family situation. After about 8 months, a new job was proposed to Claudia, which is more suitable for her credentials and includes a higher salary (but is more in administrative buildings with less access to the technical areas, though it carries a higher responsibility). She declined the new position and her behavior and output started to change. She is very quiet and seems very tired lately. You seem to see her everywhere you go. She is always walking around in different areas of the facility.

General noticeable changes:

- Claudia was seen in areas that she shouldn't have access to.
- She is not open about her personal life.

Unknown by the participants group:

Insider adversary? Claudia is looking at information concerning the job she was recruited for. If the job changes, her work will be more the administrative areas with less possibilities to walk around in the facility and her access will be limited. Additionally, this new job would be a position with more responsibilities, which would provide more stress in general. She has some social media profiles, but is not active on them; she links easily to people and pages that are proposed to her, because she doesn't really pay attention to it.



Not an adversary (green): She has always been fascinated by nuclear technology; she now has a job where she is working in technical areas, and she does not want to give that up. Also, her son has been sick for a couple of weeks, nothing serious, but because of her child's sickness, Claudia has not been sleeping well and she is a bit worried that it's not getting better. They have been travelling to a couple of specialists throughout different cities, but they all say the same, that he will be okay and it will pass in a couple of weeks.

Potential adversary (yellow): She already knows the basics of the facility because of her interest in the facility itself. She likes the job she has because it is very practical and less stress than she was used to. She had also heard from a friend that there is sensitive information, and she is curious about what it is. It would be nice if she has such information; you never know what you could do with it. Also, her child has been sick for a couple of weeks, nothing serious, but because of her son's sickness, Claudia has not been sleeping well and she is a bit worried that it's not getting better. They have been travelling to a couple of specialists throughout different cities, but they all say the same, that he will be okay and it will pass in a couple of weeks. You never know what costs will be necessary if it gets worse; maybe she should have taken the job or should look for other possibilities.

Adversary (red): She was intentionally moved in the facility as a mole for a malicious organization. She is providing intel to this organization on a weekly basis.

Practical:

- Create ppt to explain the exercise

Part 1: The participants are divided into 7 different groups. The groups have been selected in advance, to make sure we have different backgrounds and cultures in every group. Every group receives one of the 7 roles as defined below and receives an additional part of information next to the general profile.

At the end of the discussion the answers to the Mentimeter questions to all participants will guide the rest of the exercise. It is very important to relate this information back to the participants' professional experience. They need to imagine the situation in their daily job.

Different roles/7 groups:

A. HR:

- a. General information on Claudia: She is somewhat overqualified for the function. She was hired because there was a possible job opening at "the right" level, which she was made aware of. Claudia has a partner and 1 son who is still a minor (5 years old).



- b. Possible red flag: Claudia was presented with a new position with a higher salary, but she declined. No reasons were given.
- B. Security department:
 - a. General information on Claudia: She follows security protocols but does not have a proactive attitude.
 - b. Possible red flag: One day there was an incident with a co-worker. Two people started arguing at the security checkpoint because of something that happened during their kids' football game over the weekend. One of them tries to pass the security checkpoint without being checked because he was angry. Claudia was a witness of this incident, but she did not want to come forward to help the investigation.
- C. Direct colleague:
 - a. General information on Claudia: She is very reserved regarding her private life. They don't even know if she has a partner/kids.
 - b. Possible red flag: She has no social connection with any of her colleagues and always eats alone during the breaks. In the beginning she used to propose once every while to go eat together, but this has stopped recently.
- D. Line manager/direct supervisor:
 - a. General information on Claudia: She is working long hours (comes in early), including working from home during weekends and accessing digital files.
 - b. Possible red flag: The output of her work is not showing whilst according to HR she should be overqualified for the job. Lately, she sometimes seems agitated.
- E. Security guard:
 - a. General information on Claudia: Claudia's profile does not ring a bell.
 - b. Possible red flag: Claudia stays under the radar. The security guard did pass her social media profile once, Claudia was linked to some protest pages for local issues (better pay for employees, more importance on privacy of people).
- F. Colleague from a different department:
 - a. General information on Claudia: This colleague from this department saw Claudia twice in his section; we don't know why she was there.
 - b. Possible red flag: The colleague didn't know the individual had access to that part of the facility and is not sure she is supposed to have access.
- G. Medical Health professional:
 - a. General information on Claudia: She has a history of getting close to a burn-out because of stress; there are no specific indicators at the moment.
 - b. Possible red flag: They had booked an appointment, just as a follow up; but Claudia cancelled last minute. This has not yet been replanned, but it was not a mandatory visit.

Additional information that can be found in open source/space:

- A. Social media check: She is linked to some people that seem to be involved with drugs. She doesn't post a lot of things, but lately you could see some pictures in different cities throughout the country. Looking at the pages she follows, you can also see some links with protest groups in the local area. She doesn't seem actively involved; there are no posts or comments and no mentions of participations in events.

- B. Check of her desk at work: she has no personal items on her desk, no pictures or gadgets. She has a coffee mug that says, 'My work is secret, even I don't know what I am doing here'. Her file cabinet is not locked.

Discussion points: (15 mins)

- What do you think of this piece of information;
- What could it mean: insider adversary/ not an insider adversary;
- Would you do something, and how would you react;
- What could be the outcome if you DO something;
- What could be the outcome if you DON'T DO something;
- Who would you talk to, to obtain more information;
- What actions might have prevented Claudia from being in this position (pre employment, vetting,...)?
- Why would you react or not?

Menti Questions to the whole group: (2 mins)

- Is this information something to worry about? Y/N
- Would you take further action? Y/N
- Which action and prioritise:
 - Gather more information
 - Take measures directly
 - Talk to the person itself
- To gather more information: Who would you want to talk to first (prioritise)? Would you notice this behaviour in your organisation? (very much depending on the piece of information you have)
 - ➔ If the answer is 'Claudia', additional question: which role should have this discussion?
- Would it be possible to report this information easily in your organisation?

Practical:

- Divide participants in 7 different groups
- Foresee paper with information to be given to the group
- Create Menti questions

Part 2: Based on the answers on the Mentimeter question, 'Which role would you want to talk to first', the information from that role will be made available to the whole group (by someone of this group). The information from this role would therefore be added to the information already known by the 6 other groups. The individuals from this group will be added to the remaining 6 groups to discuss this new information.

IF the group choses to talk to the person, we ask for a volunteer. The volunteer provides the information his/her group has and has the first conversation with the person.

At the end of the discussion the answers to the Mentimeter questions to the whole group will guide the rest of the exercise. It is very important to relate this information back to the participants' professional experience. They need to imagine the situation in their daily job.

Example of the group division:

- ➔ It was decided that the information of the security guard (role E) will be made public OR someone from that group volunteers for the role play.
- ➔ Role E's moderator explains the information on the paper they received in the beginning of the exercise and provides a short summary of their conclusions
- ➔ The group E participants are divided into the remaining groups A, B, C, D, F and G

Discussion points: (15 mins)

- What do you think of this piece of information;
- What could it mean: insider adversary/ not an insider adversary;
- Would you do something, and how would you react;
- What could be the outcome if you DO something;
- What could be the outcome if you DON'T DO something;
- Who would you talk to, to obtain more information?
- Why would you react or not?

Menti Questions to the whole group: (2 mins)

- Compared to the information you had previously and when adding this new information (extra role), is this situation something to worry about? Y/N
- Would you take further action? Y/N
- Which action and prioritise:
 - Gather more information
 - Take measures directly
 - Talk to the person itself
- To gather more information: Who would you want to talk to first (prioritise)? Would you notice this behaviour in your organisation? (very much depending on the piece of information you have)
 - ➔ If the answer is 'Claudia', additional question: which role should have this discussion?
- Would it be possible to report this information easily in your organisation?

Practical:

- Create menti questions

Part 3: Based on the answers on the Mentimeter question, 'Which role would you want to talk to first', the information from that role will be made known to the whole group (by someone of this group). The information from this role would therefore be added to the information already known



by the 5 other individual groups. The individuals from this group will be added to the last 5 groups to again discuss the new information.

IF the group chooses to talk to the person, we ask for a volunteer. The volunteer provides the information his/her group has and has the first conversation of the person.

At the end of the discussion the answers to the Mentimeter questions to the whole group will guide the rest of the exercise. It is very important to relate this information back to the participants' professional experience. They need to imagine it in their daily job.

Example of the group division:

- ➔ It was decided that the information of HR (role A) will be made public OR someone from that group volunteers for the role play.
- ➔ Role E's moderator explains the information on the paper they received in the beginning of the exercise and provides a short summary of their conclusions in the meantime
- ➔ The group A participants are divided into the existing groups B, C, D, F and G (E was already divided into the other groups)

Discussion points: (15 mins)

- What do you think of this piece of information;
- What could it mean: insider adversary/ not an insider adversary;
- Would you do something, and how would you react;
- What could be the outcome if you DO something;
- What could be the outcome if you DON'T DO something;
- Who would you talk to, to obtain more information?
- Why would you react or not?

Menti Questions to the whole group: (2 mins)

- Compared to the information you had previously and when adding this new information (extra role), is this situation something to worry about? Y/N
- Would you take further action? Y/N
- Which action and prioritise:
 - Gather more information
 - Take measures directly
 - Talk to the person itself
- To gather more information: Which role would you want to talk to first (prioritise)?
- Would you notice this behaviour this in your organisation? (very much depending on the piece of information you have)
- Would it be possible to report this information easily in your organisation?

Practical:

- Create Menti questions



INSIDER THREAT MITIGATION



RESULTS (30min)

All signs/information is made available to everyone. We have a small group discussion before asking again some Mentimeter questions to gain a general response.

Group Discussion (5 min):

- Does this change your way of handling the situation?
- What could it mean: insider adversary/ not an insider adversary;
- Would you do something, and how would you react;
- What could be the outcome if you DO something;
- What could be the outcome if you DON'T DO something;
- Who is best suited to talk to the person?
- Why would you react or not?
- If you would have decided not to talk to Claudia after the first piece of information, would you have missed a potential insider?

Menti Questions to the whole group: (2 mins)

- Would you take immediate steps without talking to the person? Y/N
- Would you talk to the person? Y/N
- Which role is best suited to talk to the person?

Actor play: Based on the outcome of the Mentimeter questions, a specific role will be chosen to have a talk with Claudia. We ask for a volunteer from the participants who will play out the conversation with Claudia (played by actor).

- ➔ We try to do this role play at least 2 times. Every time the participant steps into the play with their own reality, background, and culture. In every role play, it is decided in advance if the actor is no adversary – possible adversary – adversary (this is only made public to the group after the conversation).

Practical:

- Create ppt with all signs and possible outcomes (no adversary – possible adversary – adversary)
- Create Menti questions



ACTOR GUIDELINE

Profile:

- Local actor that could help understand the culture (less an asset when the exercise is foreseen for an international audience)
- Improvisation experience
- Advantage: knowledge on:
 - Interviewing techniques
 - Behavioural observation
 - How to get people to open up

We ask of the actor to:

- Play out a meeting with someone based on a specified profile → we provide a level of intent that (s)he will play out
- Provide feedback on the way of handling the meeting (can be foreseen/helped by moderator as well) → what made him/her open up/close down, which techniques help or not

Role play:

- Starts with how the participant would invite such a conversation:
 - In the hallway: possibility to decline
 - With a meeting: formal/informal?
- Setting the scene of the meeting:
 - Where: in the lounge, in the office, somewhere else
 - Who is there: more people?
 - Is it normal to have such meetings?
 - How do they address each other
- Have conversation with the information you have and improvise

POSSIBLE ELABORATION OF THE EXERCISE

This exercise is a good start to generate discussions or a coaching part in how to hold such interviews.

In this part, you can find some suggestions from the group to build on the existing exercise and to elaborate the exercise itself or the coaching part after the exercise.

Changing the profile

There are many possibilities to change the profile in this exercise and adapt it more into the reality of the participants.

Possibilities for changes:

- Create a profile specifying an age
- Create a profile where there are red flags
- Add information on the profile

Next steps

Interviewing techniques:

The exercise can be the start of a teaching moment on interviewing techniques or the recognition of micro expressions. Specific presentations or workshops could help the discussion afterwards.

There is also a possibility to tape the interviews that were held during the exercise, in order to evaluate the reaction step by step.

How to assess a threat:

The exercise can also be a starting point on further discussion on the assessment of 'red flags.'

Play out different scenarios

With more rooms and time available, the exercise can be played out in different scenarios.

Where there are groups that have a conversation with the actor earlier in the process, if they would like to see his/her reaction.

The group that does have a conversation can also build further on his/her reactions during the interview. This would mean you need to foresee different scenarios and possibilities to split the group. Afterwards, it would be interesting to see if the conversation has guided the actions of the players.

Possibilities to share and compare hypothesis within the play



This is generally done within the smaller groups, but not between groups. When you have more time for the exercise, this is an addition that can be done during the role play. In order to compare what the possible outcomes are, the differences in reaction towards the person might come forward even more clearly.

Setting the scene

Depending on the group, it might also be useful to really set the scene with a specific legal framework. If there are people from different countries, they bring their legal framework in the exercise. If you want to look at cultural differences, these aspects need to be taken into account.