InfoSec Cinema
Rogue One: a Star Wars Story

26th of April 2018

ROYAL HOLLOWAY UNIVERSITY OF LONDON

WELCOME!

Important

No fire alarms planned today

Description of the activity

- Short description of the activity (this)
- Movie Screening
- Discussion

Purpose of the activity

- To discuss about information security
  - Informal setting
  - Popular culture elements as a vehicle
- To see how security is present ‘almost’ everywhere
- Teach Information Security in a different way
- Research and improve our teaching methods

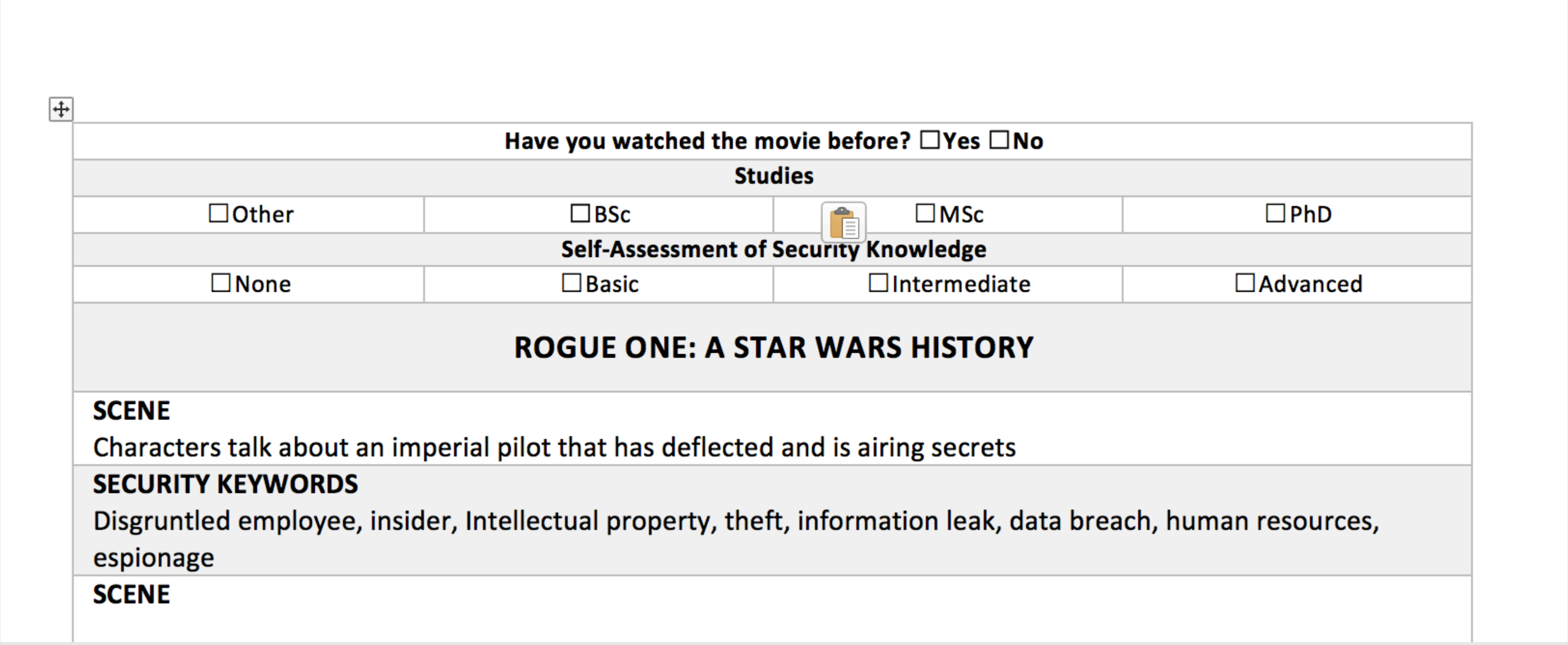
Documents on your table

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Documents in your table

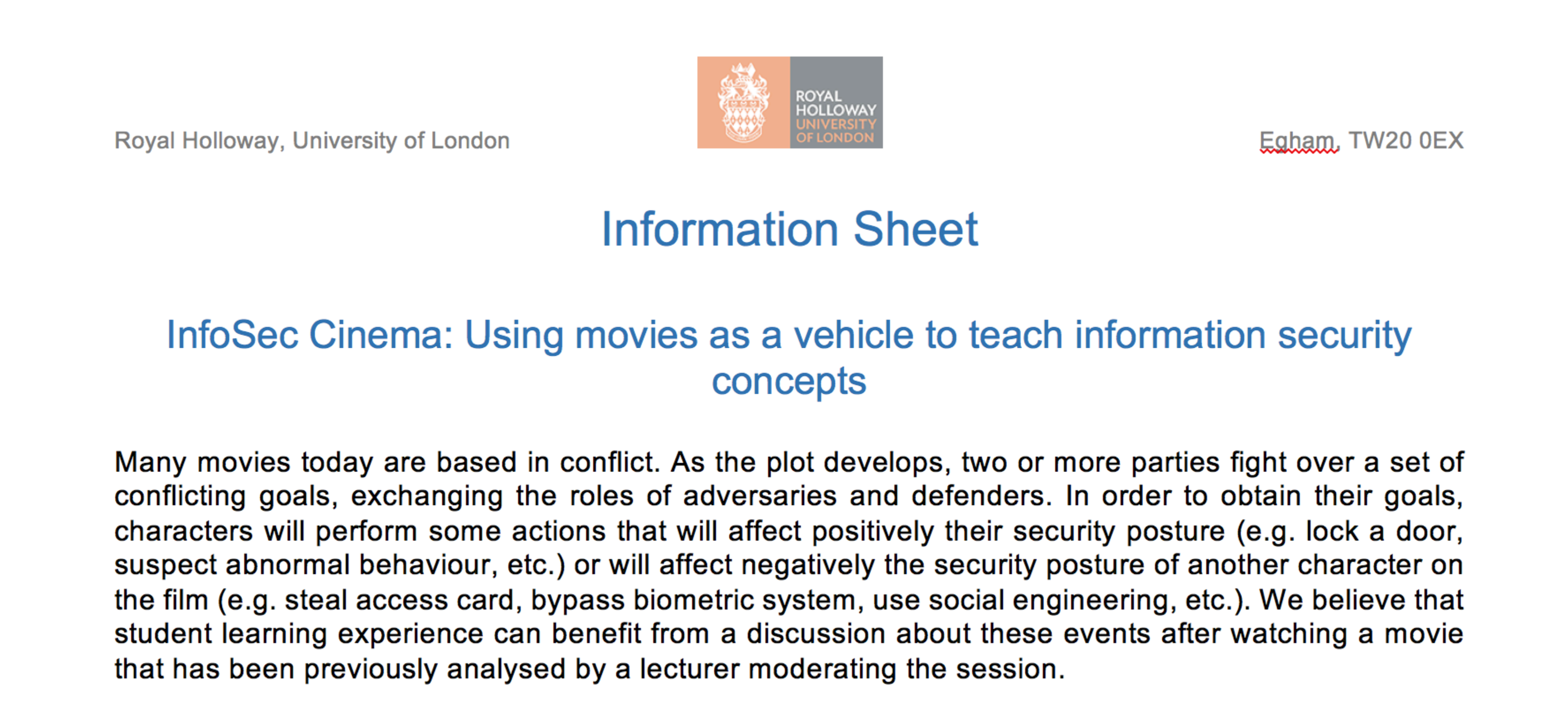
- Feedback form
- Security Events Log
- Information sheet
- Informed consent

Log of Security Events



Have you watched the movie before? ☐Yes ☐No			
Studies			
☐Other	☐BSc	☐MSc	☐PhD
Self-Assessment of Security Knowledge			
☐None	☐Basic	☐Intermediate	☐Advanced
ROGUE ONE: A STAR WARS HISTORY			
SCENE Characters talk about an imperial pilot that has deflected and is airing secrets			
SECURITY KEYWORDS Disgruntled employee, insider, Intellectual property, theft, information leak, data breach, human resources, espionage			
SCENE			

Information Sheet



Royal Holloway, University of London

Egham, TW20 0EX

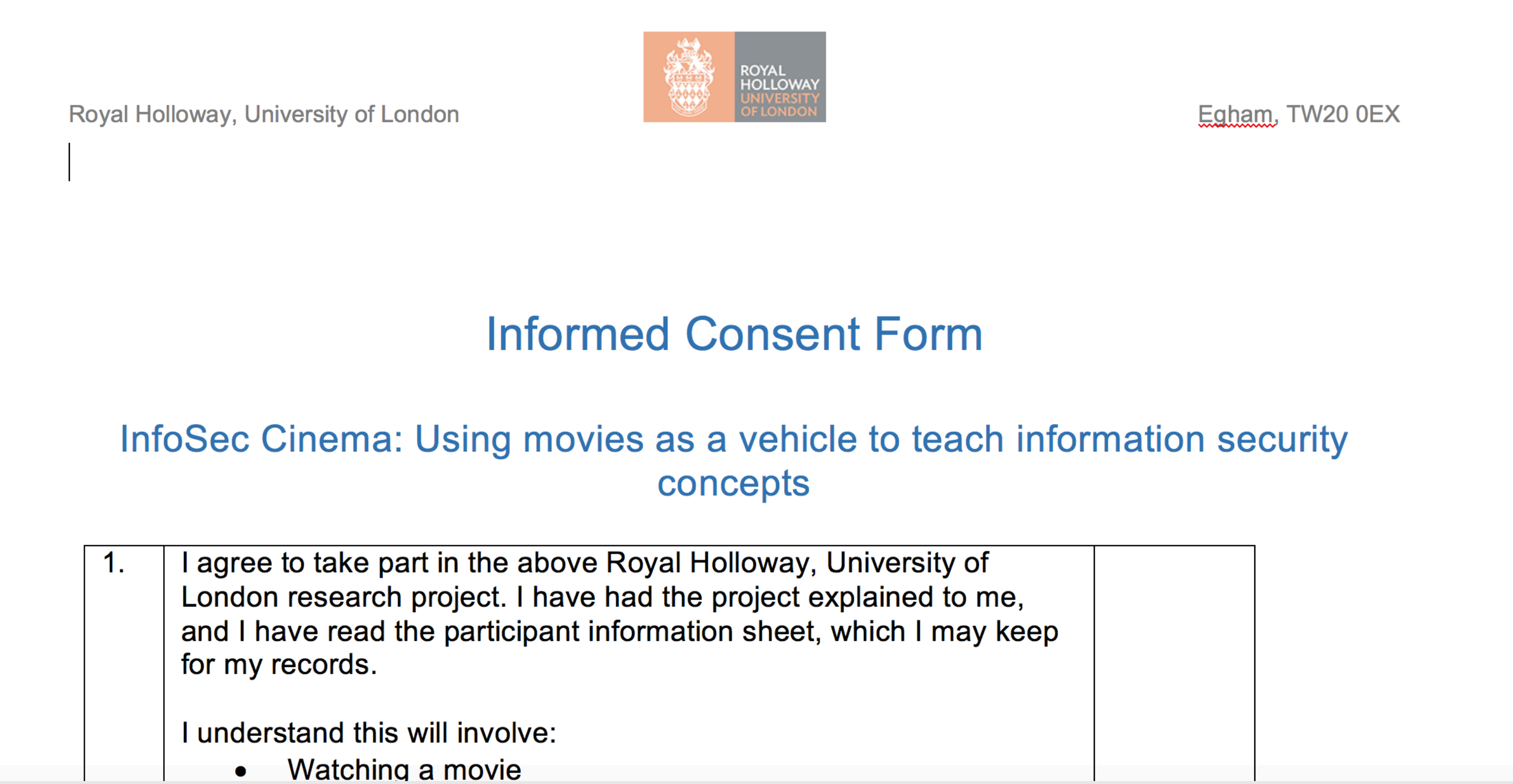
Information Sheet

InfoSec Cinema: Using movies as a vehicle to teach information security concepts

Many movies today are based in conflict. As the plot develops, two or more parties fight over a set of conflicting goals, exchanging the roles of adversaries and defenders. In order to obtain their goals, characters will perform some actions that will affect positively their security posture (e.g. lock a door, suspect abnormal behaviour, etc.) or will affect negatively the security posture of another character on the film (e.g. steal access card, bypass biometric system, use social engineering, etc.). We believe that student learning experience can benefit from a discussion about these events after watching a movie that has been previously analysed by a lecturer moderating the session.

Informed Consent Form

ROYAL HOLLOWAY UNIVERSITY OF LONDON



Royal Holloway, University of London

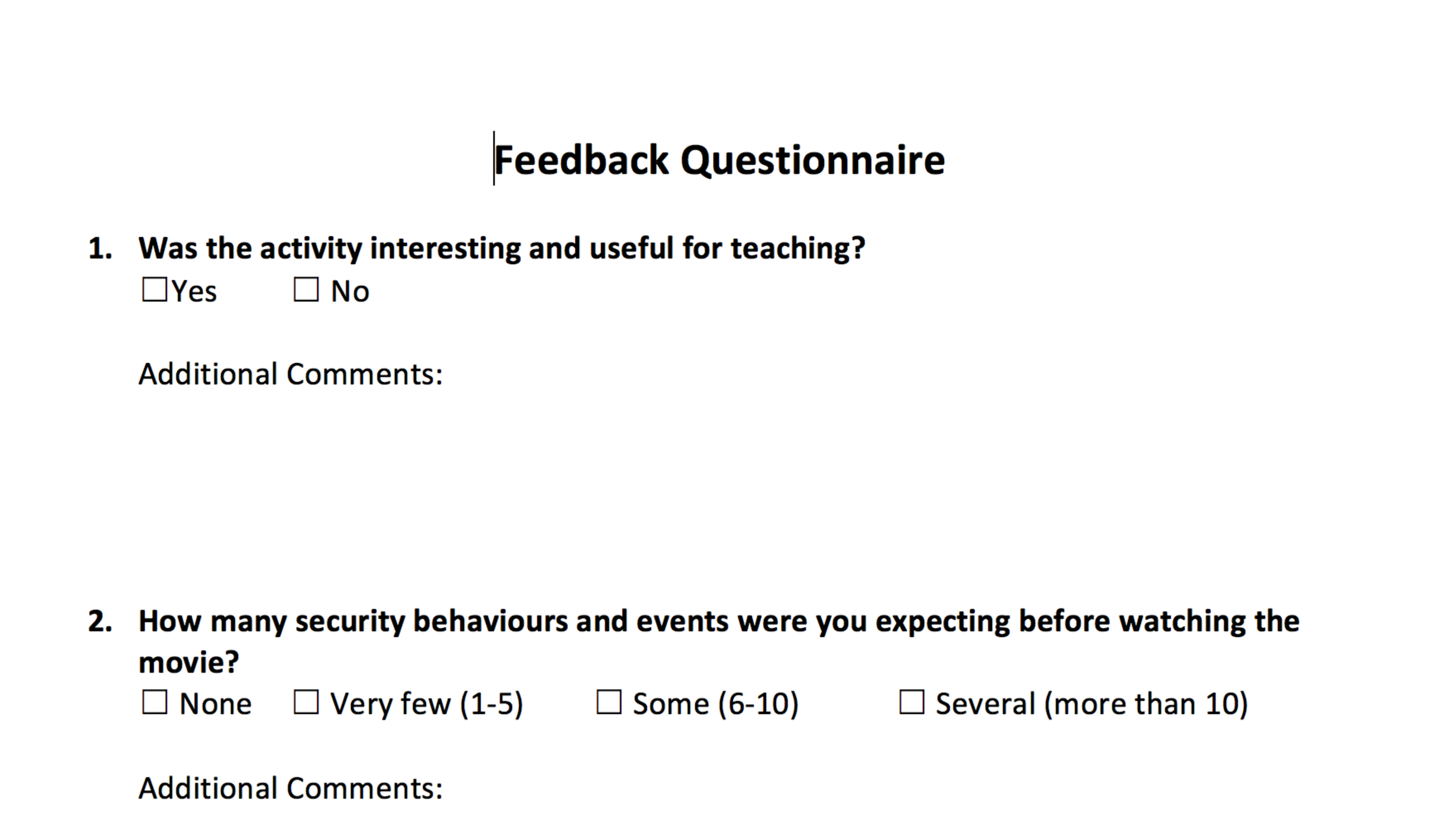
Egham, TW20 0EX

Informed Consent Form

InfoSec Cinema: Using movies as a vehicle to teach information security concepts

1.	I agree to take part in the above Royal Holloway, University of London research project. I have had the project explained to me, and I have read the participant information sheet, which I may keep for my records. I understand this will involve: • Watching a movie	

Feedback Questionnaire



Feedback Questionnaire

1. **Was the activity interesting and useful for teaching?**

   ☐Yes ☐ No

   Additional Comments:

2. **How many security behaviours and events were you expecting before watching the movie?**

   ☐ None ☐ Very few (1-5) ☐ Some (6-10) ☐ Several (more than 10)

   Additional Comments:

Movie Time!

Discussion

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Cap 4 09:25
- Imperial Pilot Deflecting
- Telling People they are making a weapon
- Planet Killer
- Disgruntled employee – Intellectual Property

- Solutions?

- Cap 6 12:35
- Secure Transport
- A prisoner van is assaulted and one of the prisoners Jyn Erso is freed by rebels.
- Solutions?

- Cap 15 29:56
- Secure Transport
- Ambush to an Imperial Patrol by Saw Guerrera rebels in the City.
- Solutions?
  - Counter Intelligence

Not an actual failiure

- Cap 16 33:56
- Secure Transport
- Stormtropper suspects the Imperial robot is not working properly and takes action by taking Cassian and Jyn as prisoners
- Solutions?

- Cap 18 45:00
- Sensitive information being
- Jyn’s father is able to send out a message to his daughter while working for the Empire
- Solutions?

- Cap 18 45:00
- No Segregation of Duties
- Jyn's father has control over critical parts of the design and introduces a weakness without anyone else noticing
  - Flaw small but powerful… Any analogy with risk components? What does this mean in terms or likelihood and impact?
  - What is the vulnerability? Reactor is unstable and a blast will destroy the whole station.
- Solutions?

- Cap 20 50:00
- Death Star Director is fired because of the security breaches

- Cap 23 58:00
- Lack of Physical Security
- Rebels don’t get detected when entering Eadu
- Solutions?

- Cap 23 58:00
- Lack of Physical Security
- First group of rebels (Jyn’s) don’t get detected when entering Eadu but the Rebel squadron is. However, the squadron is detection comes too late as they are able to attack the base without opposition
- Solutions?

- Cap 27 1:13:00
- Darth Vader order and Investigation into Jyn’s father behaviour to ensure that the Death Star hasn’t been sabotaged
- What part of the course relates this with?
  - Incident Response

- Cap 29 1:16:00
- Jyn, Cassian and others decide to go to the imperial archives in a planet called Scarif to steal the Death Star plans

- Cap 31 1:20:00
- Scarif has a shield that only allows certain ships to go through.
- How does the shield work?
  - Only ships that are on the list and authenticated can go through
    - How do the rebels get to go through the get?
    - The stolen ship codes hasn't been revoked
    - The ship is not on the list but the guard believes the story of the pilot

- Cap 33 1:26:00
- Social Engineering
- A guard opens the door to the complex to Cassian just because he is dressed as an official
- You would be surprised how easy it is to pass unnoticed with the proper clothing and confidence

- Cap 35 1:28:00
- Director Krenic asks for a review of all logged events from Galen Erso.
- What part of the course relates this with?
  - Incident Response

- Cap 35 1:29:00
- No access control or responabilities defined
- The rebel robot gets access to the system through another robot. He is able to access all the plans. There is no segregation of duties, or access control policy in place
- Solutions?

- Cap 37 1:32:00
- No authentication on internal messages
- Rebels are able to send fake messages and divert troops to other areas

- Cap 37 1:33:00
- Problems of biometric authentication
- Biometric Authentication systems are not perfect. In some cases, when you are uncouncios, you cannot control who authenticates with your body.
- Solutions?
  - Liveness detection
  - Second factor authentication

- Cap 41 1:41:00
- No further access control
- Once Jyn and Cassean are in the archive room they can access all files without any problem.

- Cap 41 1:42:00
- No removable media protection
- The Stardust file can be extracted without any problem

- Cap 44 1:50:00
- Failure with network access control
- The only network access they have is the physical shield that stops all communications from going outside.