
esc.
UNDER THE HOOD.
INTERACTIVE THEATRE WORKSHOP

OVERVIEW.

30-45 minute interactive theatre production documenting an insider threat within organisation “Cheetah Automotive Inc.”

Audience participation via app for live polls as the story develops to let audience guess the culprit, and to support Q&A session at the end of the event.

Covers topics such as insider threat, phishing & social engineering, and effective communication as a defence.

10-15 minute overview presentation at the end of the play to reinforce cyber security learnings.

PLOT.

ACT 1: IGNITION
The unveiling of Cheetah Automotive's autonomous vehicle system, CheetahDrive, is disrupted by a mysterious system glitch.

ACT 2: WARNING LIGHTS
Unauthorised access to the CheetahDrive source code prompts an internal audit and the hiring of a cybersecurity consultant.

ACT 3: UNDER THE RADAR
Interviews reveal potential motives as suspicion falls on various employees, with hints of external collaboration.

ACT 4: BRAKING POINT
Another breach targets the production line, uncovering evidence of an insider aiding a competitor.

ACT 5: THE REVEAL
The true insider threat is exposed, leading to the apprehension of the culprit and reinforcing the importance of cybersecurity measures.

LEARNING OUTCOMES.

INSIDER THREAT

Recognise characteristics and motivations of insider threat and understand importance of monitoring employee activity.

TRAINING

Understand how training can help employees identify and respond to risks posed to the organisation.

PHISHING

Recognise common social engineering and phishing tactics used by cyber criminals and learn how to report issues.

EXAMPLE CONTENT

ACT ONE: IGNITION

Plot:
The play opens in the bustling design lab of Cheetah Automotive Inc. The CEO, Emily Carter, proudly unveils the company's latest innovation, an autonomous vehicle system named "CheetahDrive."

During the celebration, the Chief Technology Officer (CTO), Daniel Hunt, emphasises the importance of cybersecurity.

The act concludes with a mysterious system glitch that disrupts the presentation, raising concerns about a potential insider threat.

Audience Interaction:
"Who might have the technical knowledge to cause a system glitch?"

- A) The CTO, Daniel Hunt
- B) The Lead Engineer, Maria Lopez
- C) The Software Developer, Kevin Chen
- D) The Data Analyst, Linda Patel

EXAMPLE CONTENT

ACT TWO: WARNING LIGHTS

Plot:
The team discovers that the CheetahDrive source code has been accessed without authorisation. Maria Lopez, the Lead Engineer, reports a breach in the system's security protocols. Daniel Hunt instructs the team to conduct an internal audit.

As tensions rise, Emily Carter hires a cybersecurity consultant, Alex Green, to investigate. The act ends with Kevin Chen discovering that sensitive data has been transferred to an external device.

Audience Interaction:
"Who had the opportunity to transfer data to an external device?"

- A) The Lead Engineer, Maria Lopez
- B) The Software Developer, Kevin Chen
- C) The Data Analyst, Linda Patel
- D) The HR Manager, Tom Rogers

AUDIENCE PARTICIPATION.

We propose the use of the Mentimeter app as part of the event to allow for audience participation to vote for who they think the ‘traitor’ is throughout the play.

Our host will top and tail each ‘act’ to set the scene and ask the audience the relevant question.

We can encourage additional participation in short presentation after the event, again through the use of the Mentimeter app, to allow for Q&A with one of our consultants who will present some additional content to reinforce the learning outcomes for the event.


esc.
GET IN TOUCH
INFO@CYBERESCAPEROOM.CO