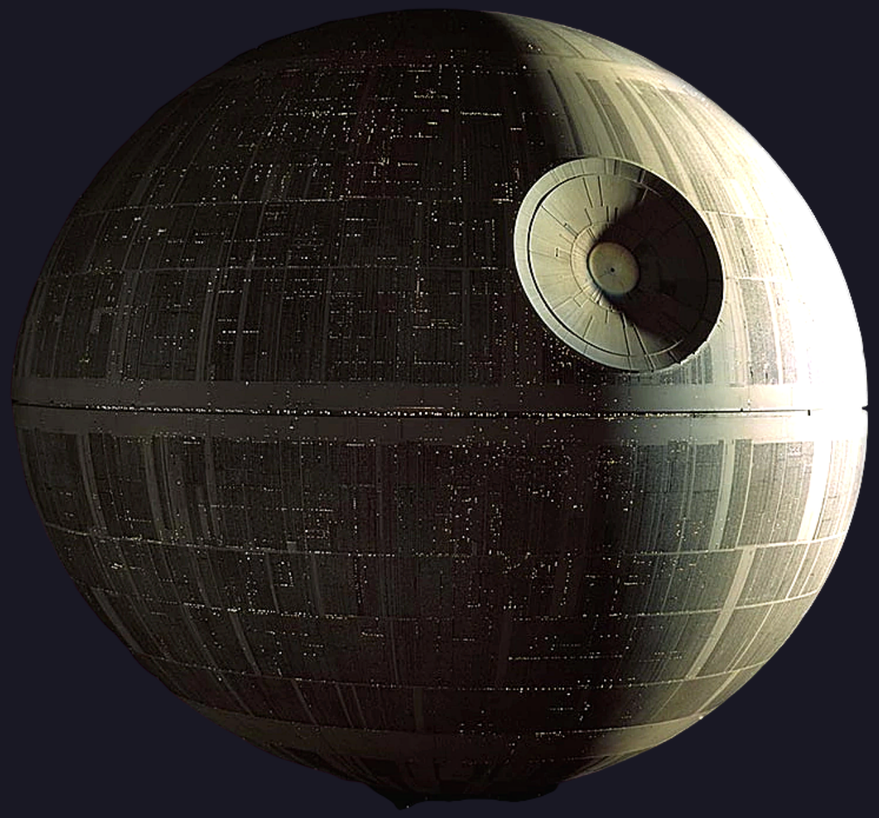


Threat modelling the Death Star

By Mario Areias

Mario Areias

Developer + Security

@MarioAreias

THREAT MODELLING

Security and development teams collaborating on threat models is the most effective way to improve security posture.

State of DevOps Report - 2019

threat modelling

process

identify

enumerate

threats


Not impressed


New normal
START SELLING

LIST OF REQUIREMENTS

Engaging

Highly collaborative

Valuable for everyone

STRIDE

Pasta

Attack Trees

DREAD

valuable

useful

80%

of the developers

participate again


STAR
WARS

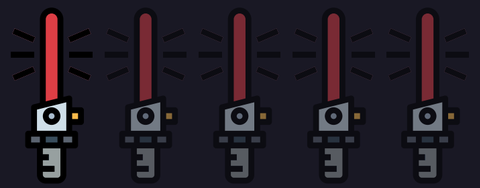
THE CSO OF GALACTIC EMPIRE…YOU!

YOUR BOSS...

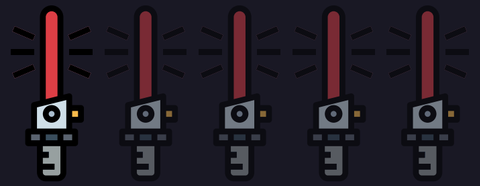
EVIL PERSONAS

Script Kiddie

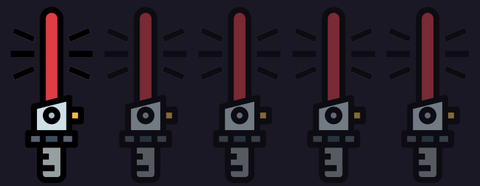
Expertise



Resources

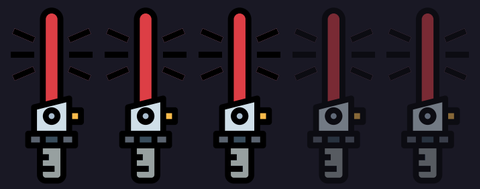


Organisation

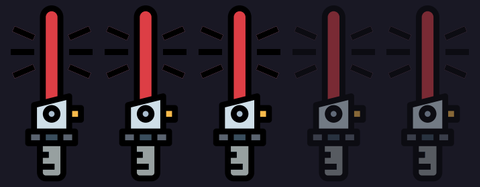


Bounty Hunter

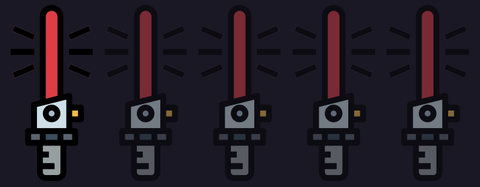
Expertise

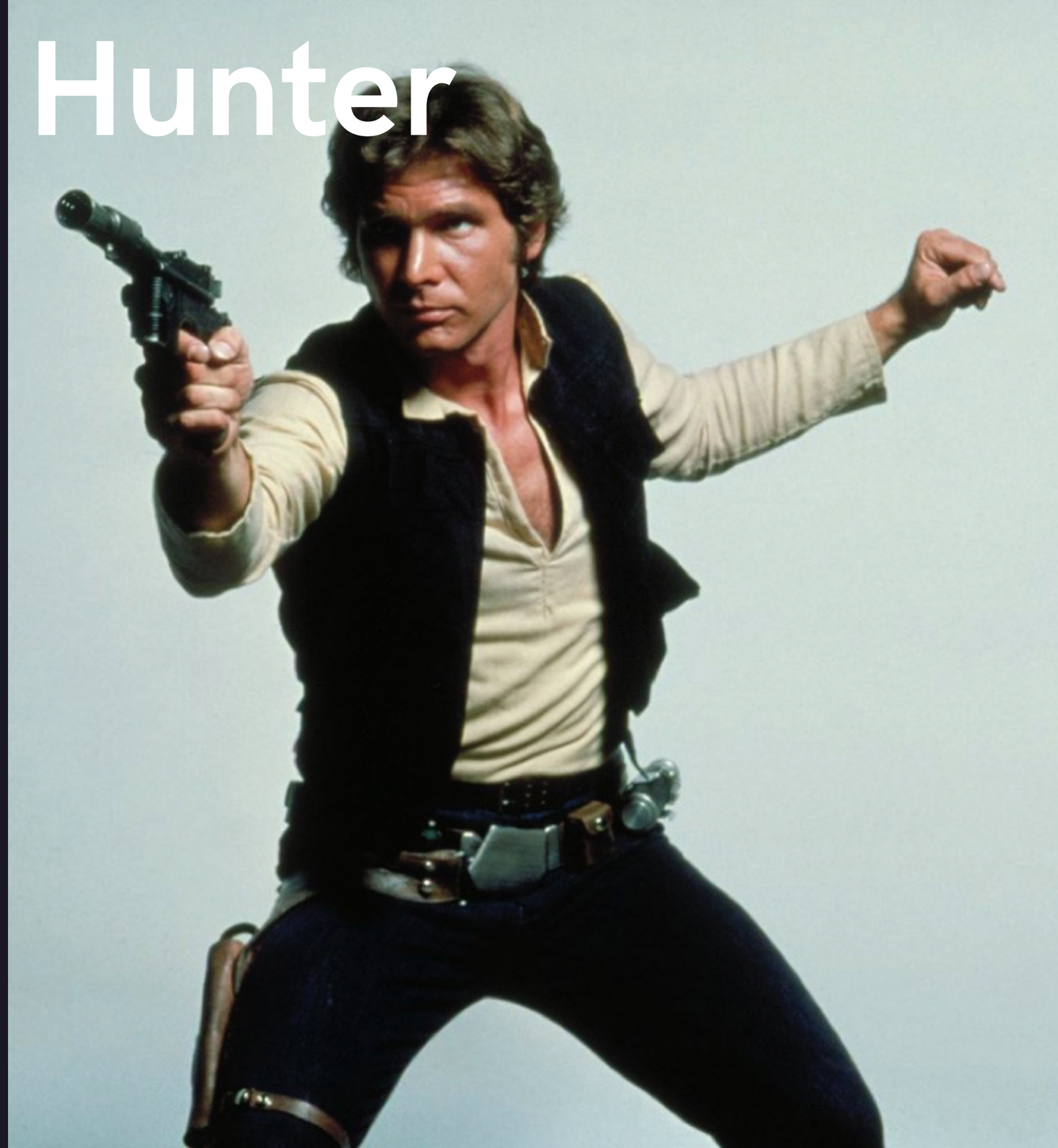


Resources



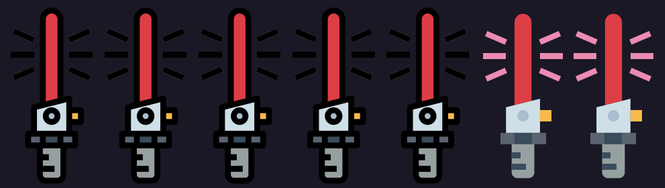
Organisation



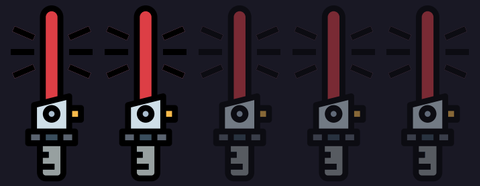


Jedi Knight

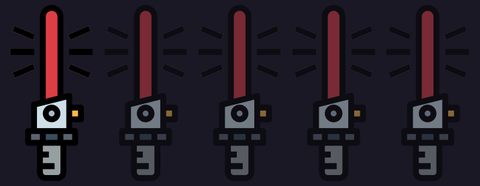
Expertise



Resources

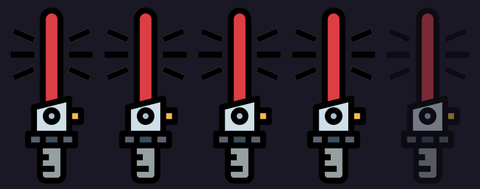


Organisation

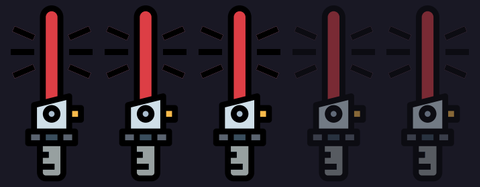


Insider Threat

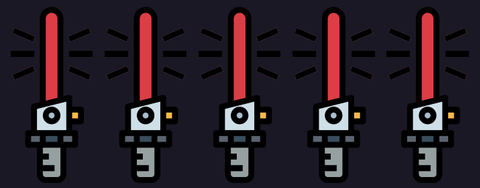
Expertise



Resources

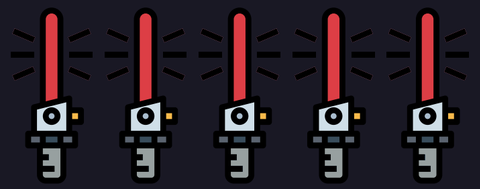


Organisation

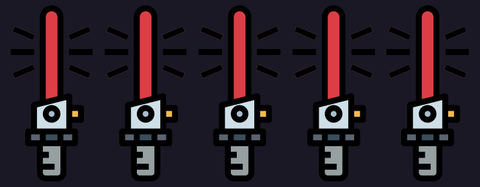


Nation State

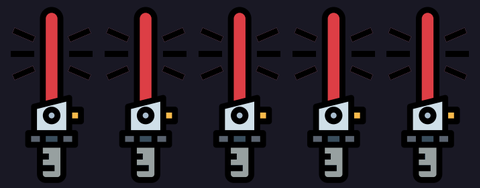
Expertise



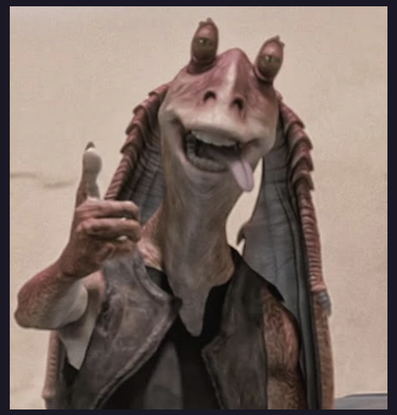
Resources



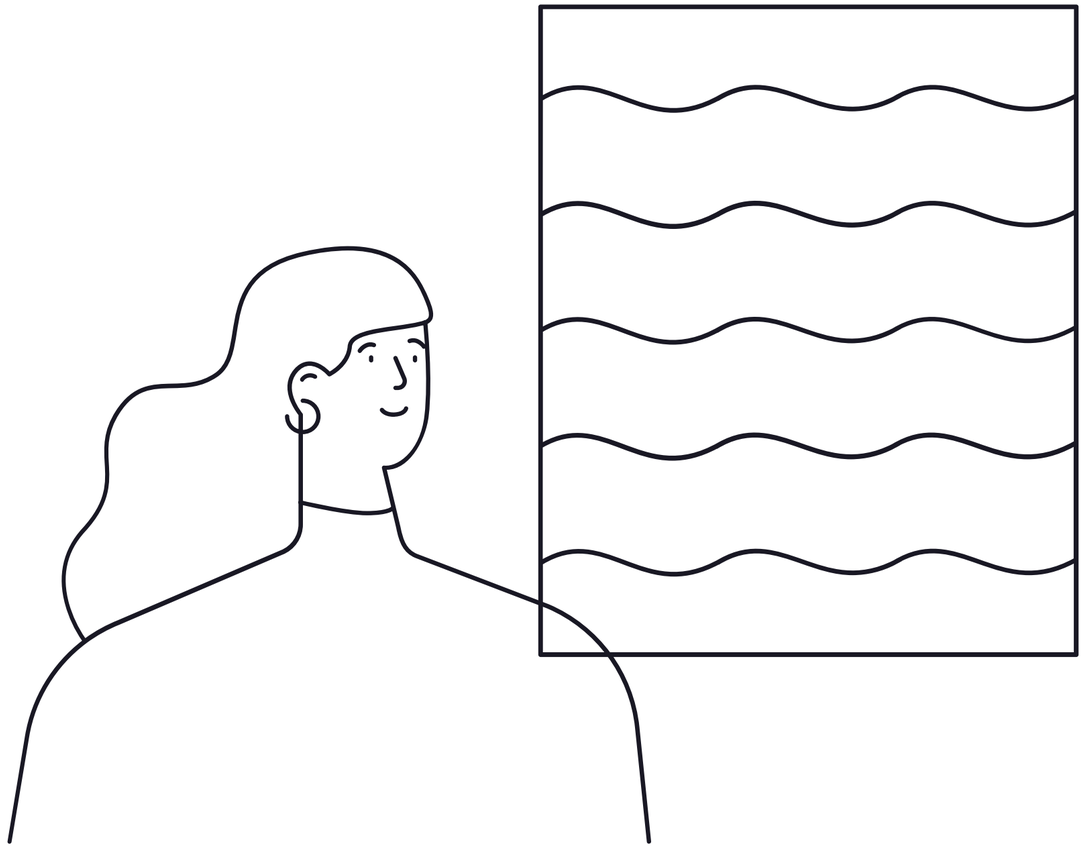
Organisation



EVIL PERSONAS

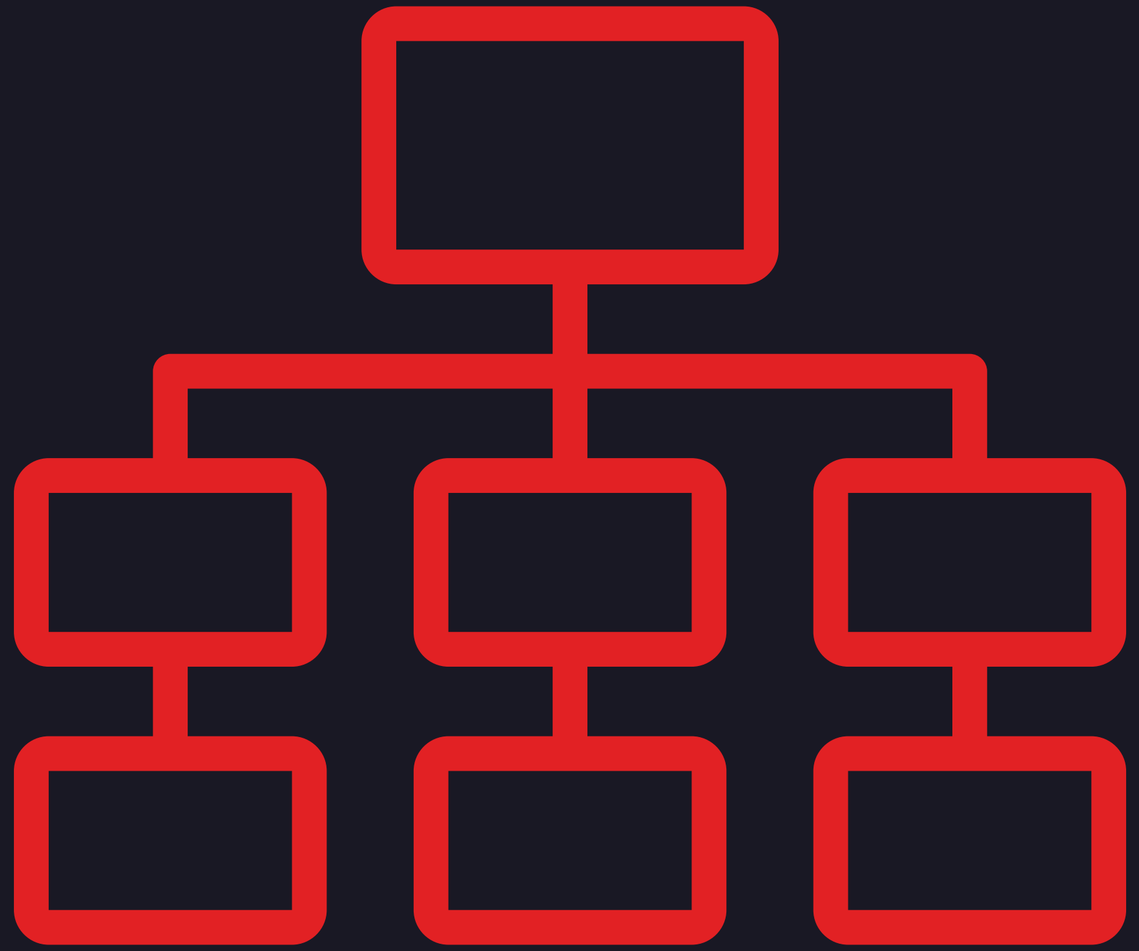


Get data to create your own evil personas.



BUILDING THE ATTACK TREE

GET THE RIGHT PEOPLE IN THE ROOM

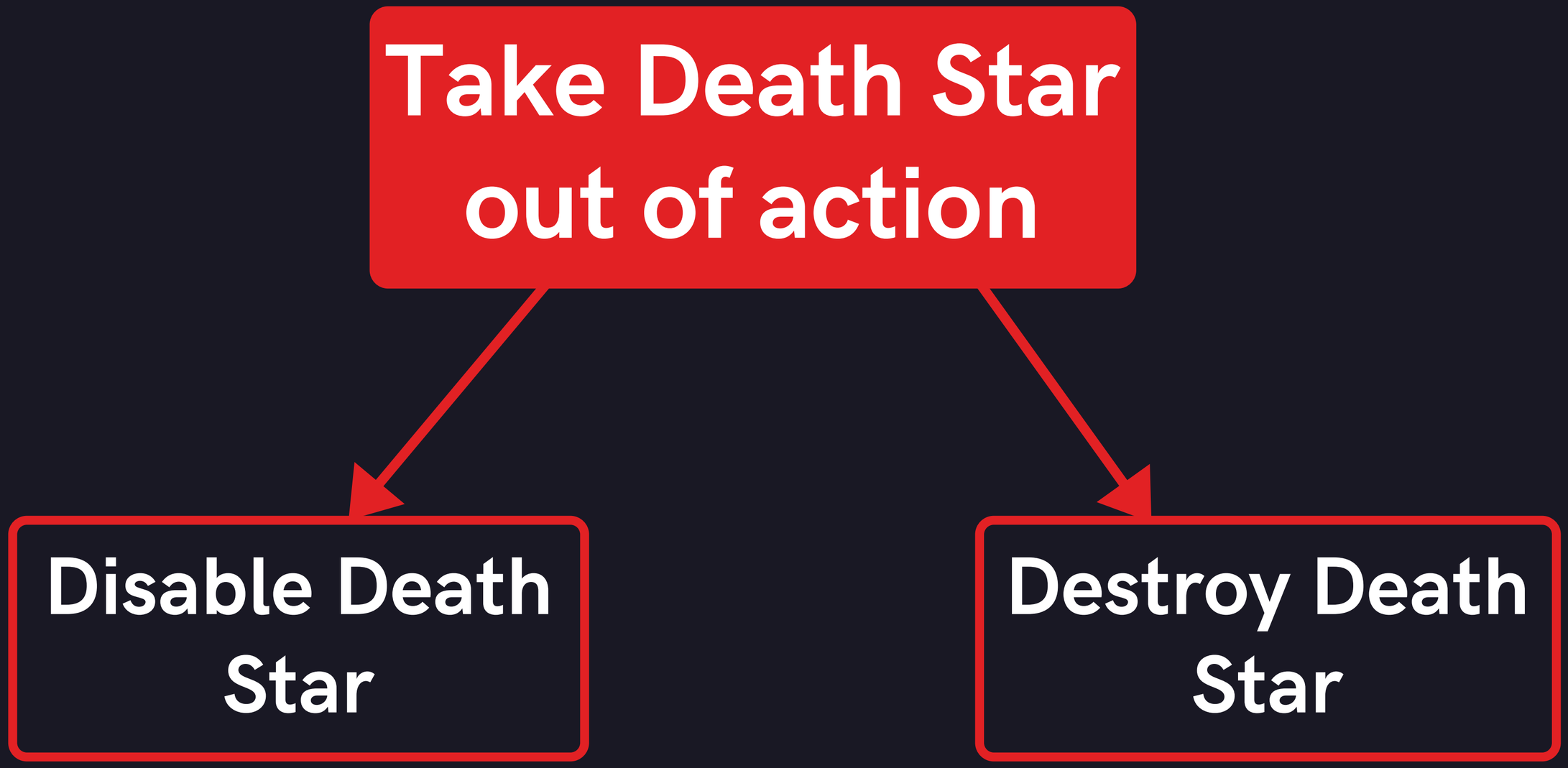


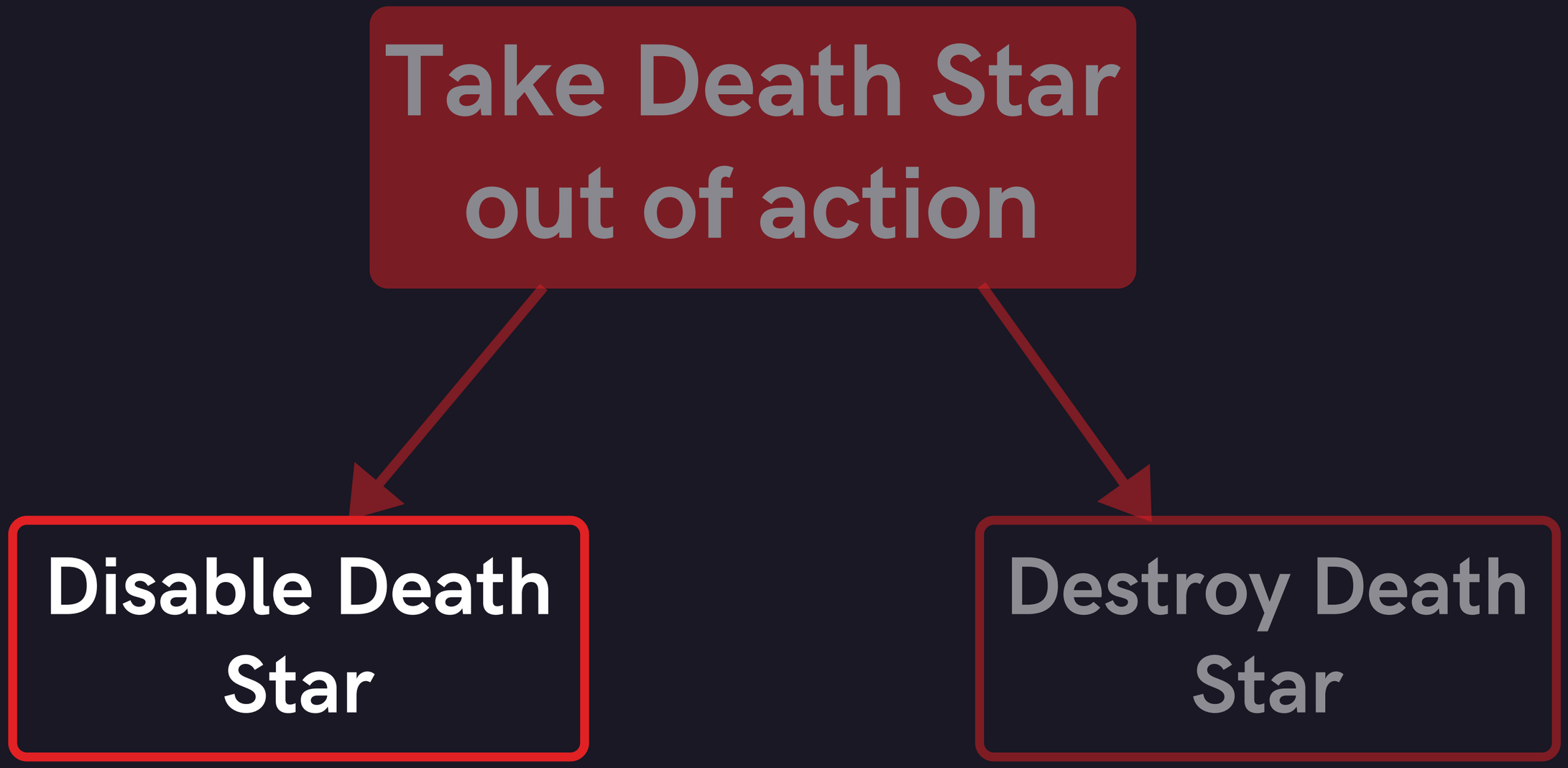
Take control of Death Star

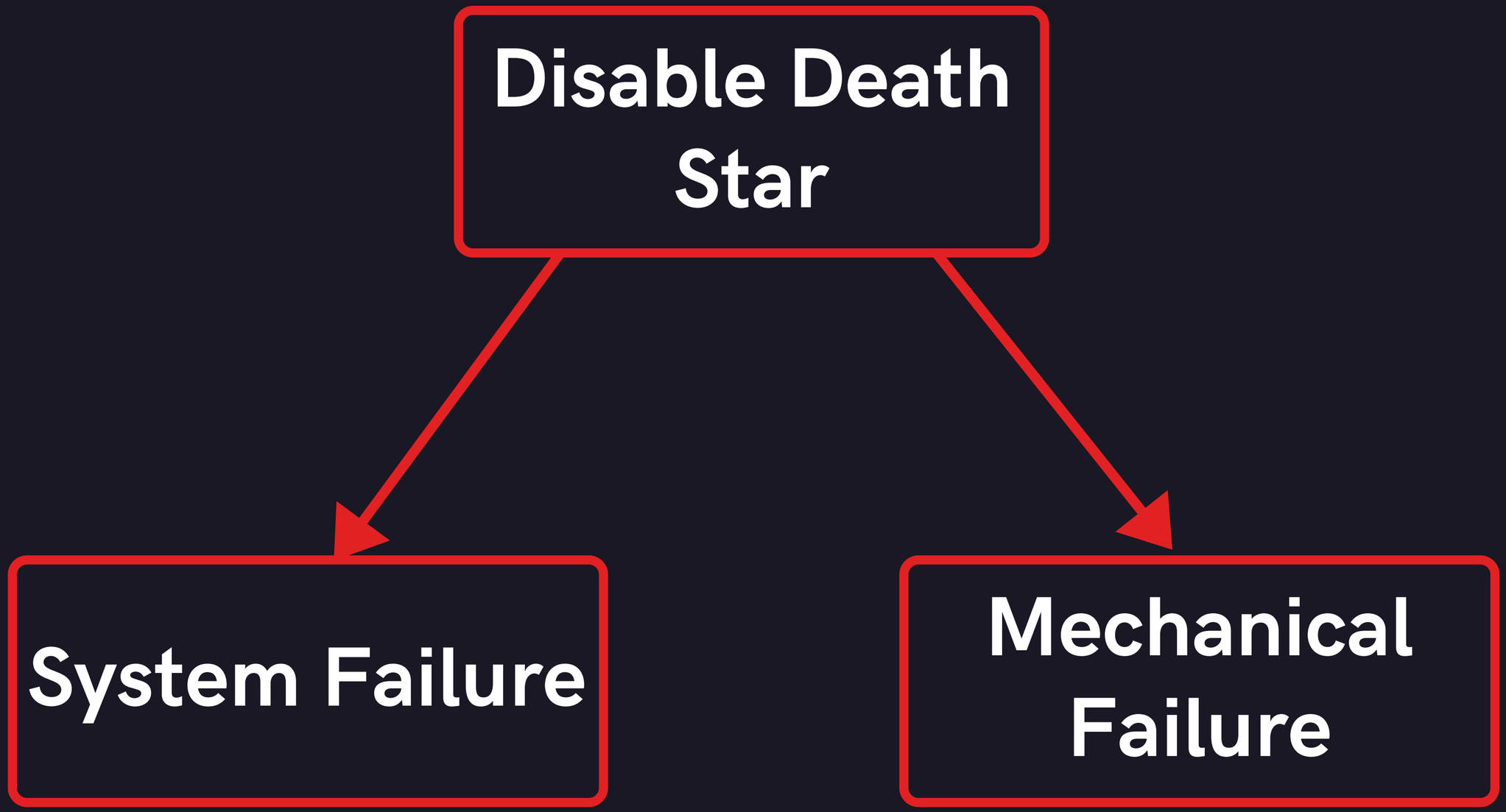
Take Death Star out of action

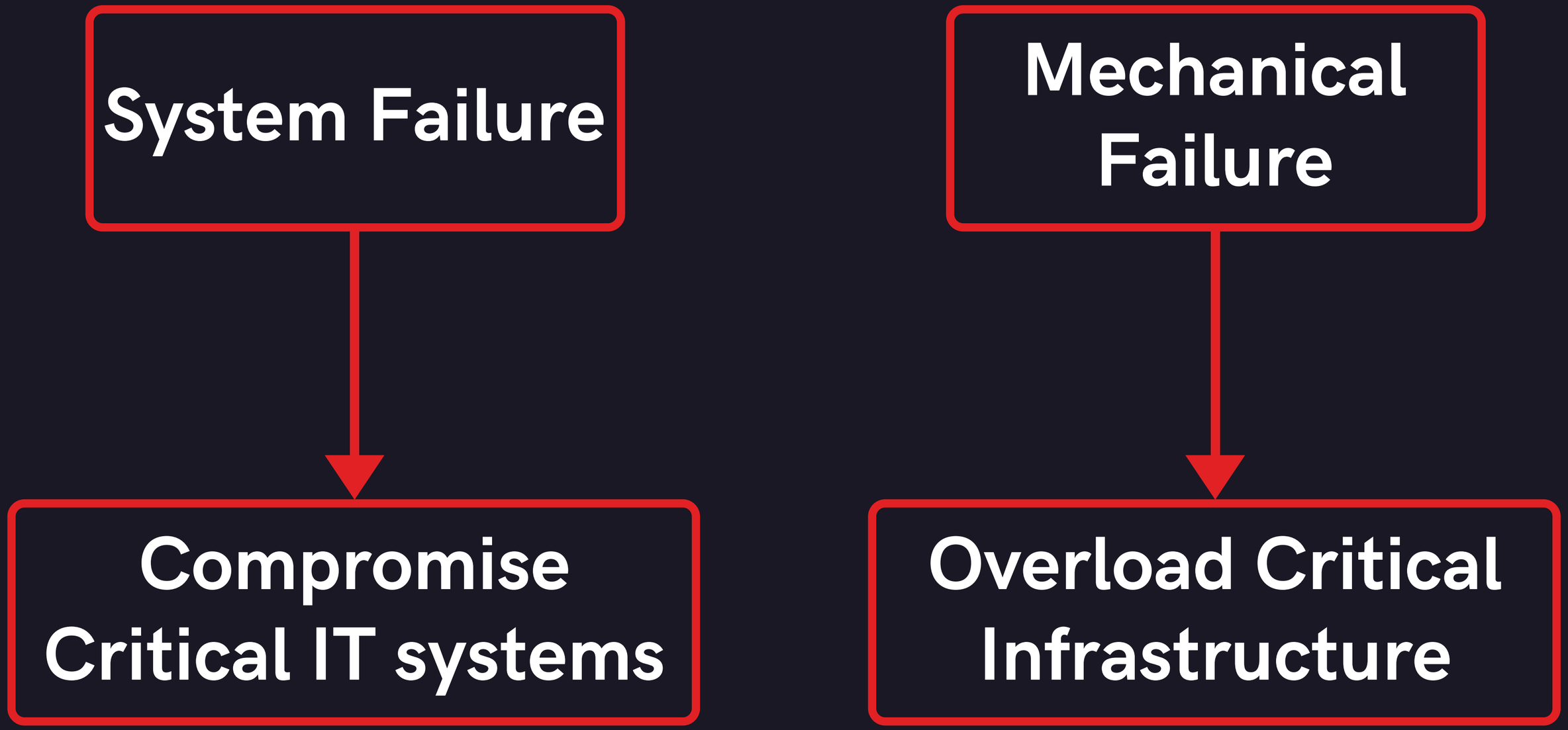
Take control of Death Star

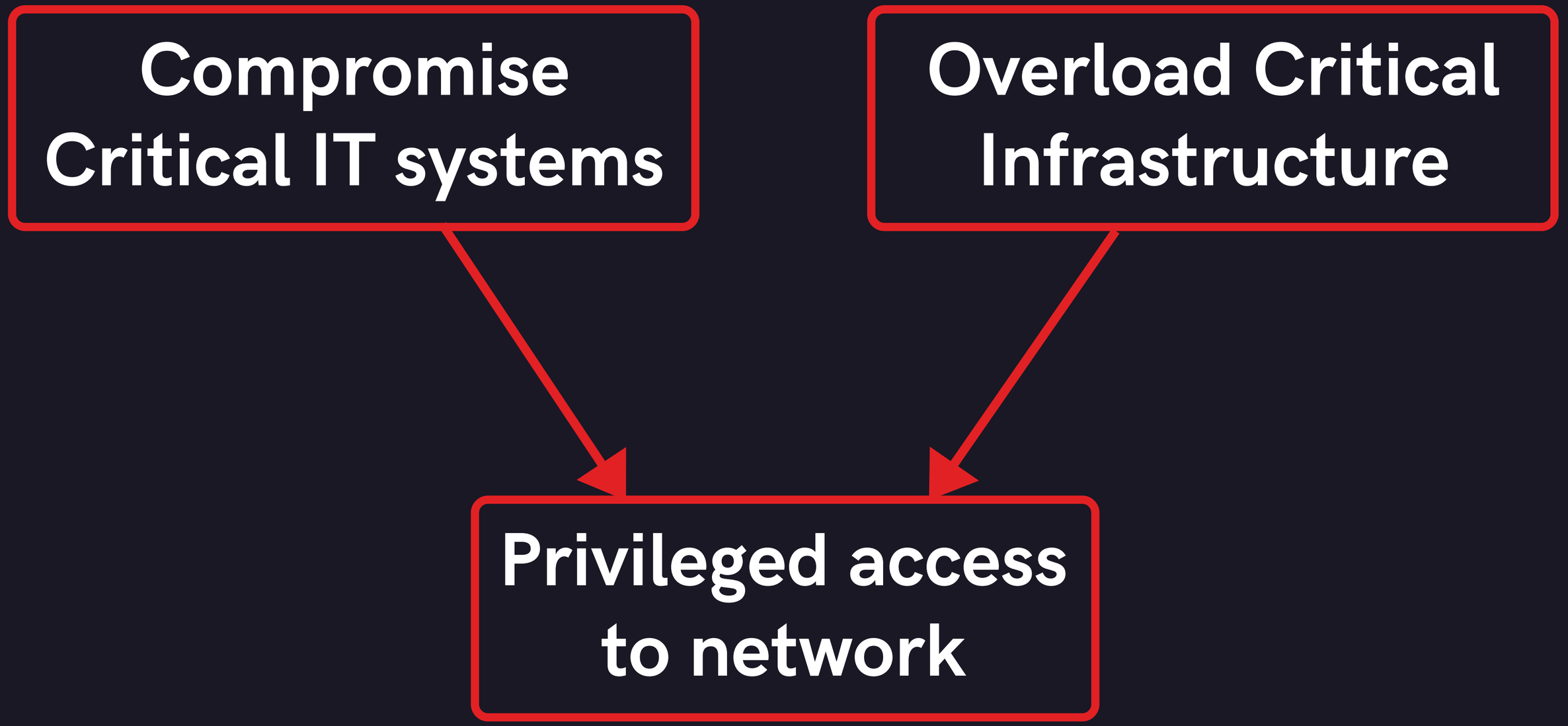
Take Death Star out of action

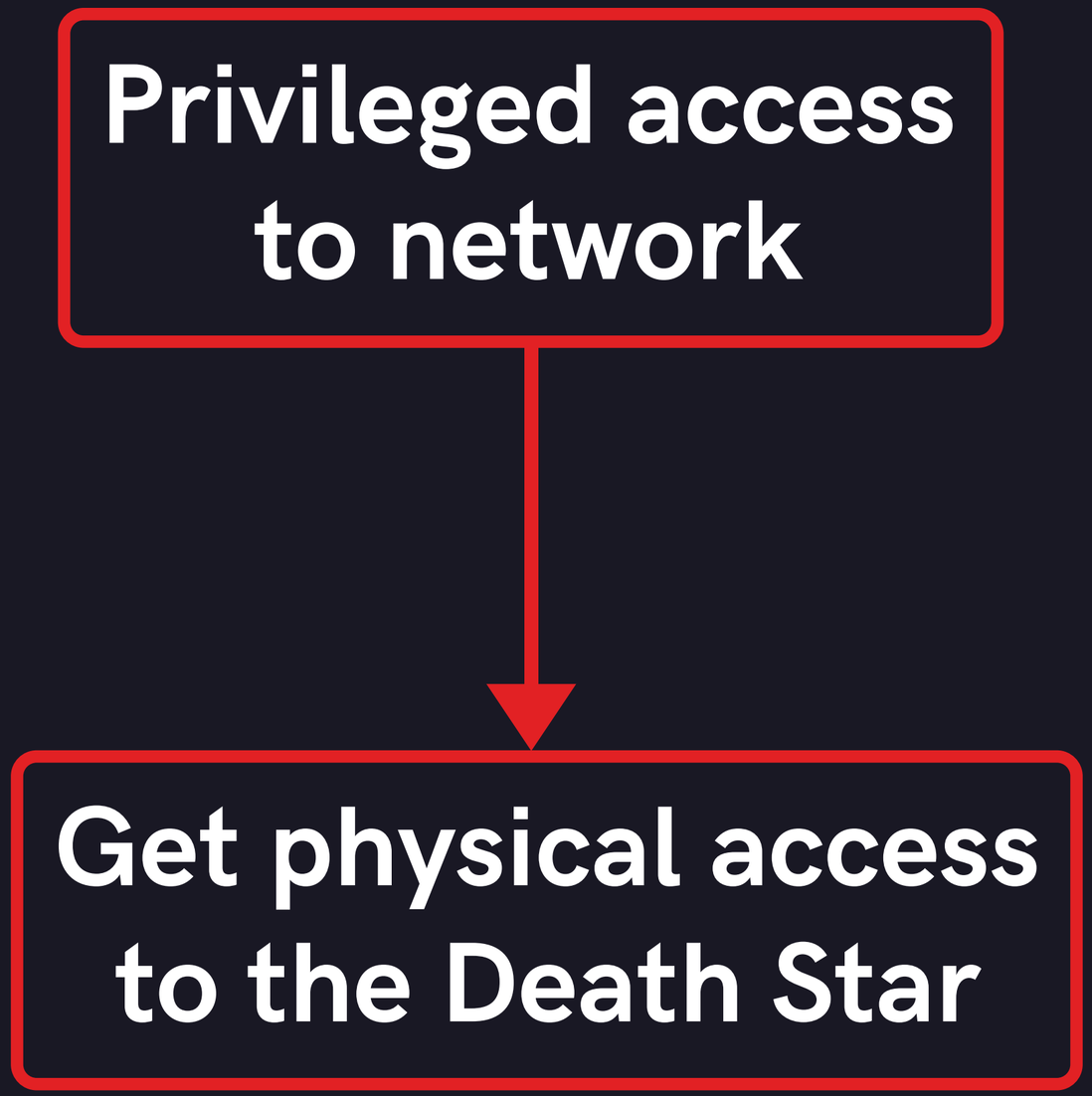

Take Death Star out of action
Disable Death Star
Destroy Death Star

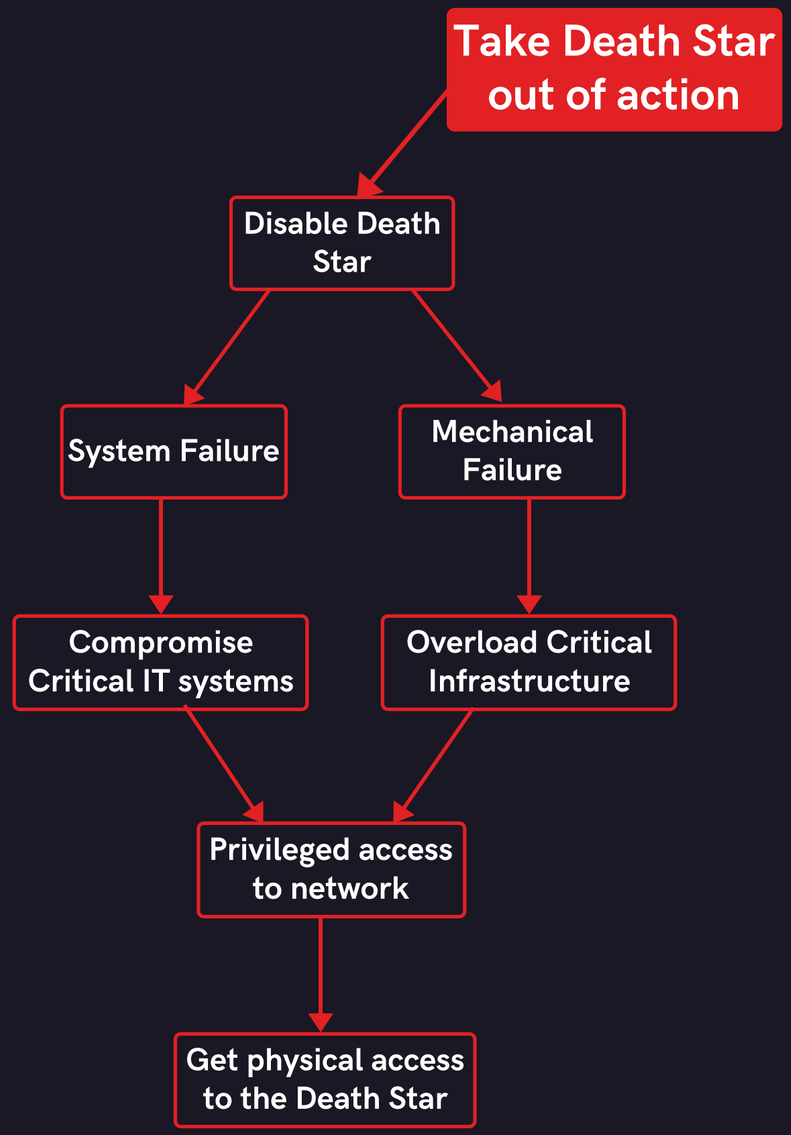

Take Death Star out of action
Disable Death Star
Destroy Death Star

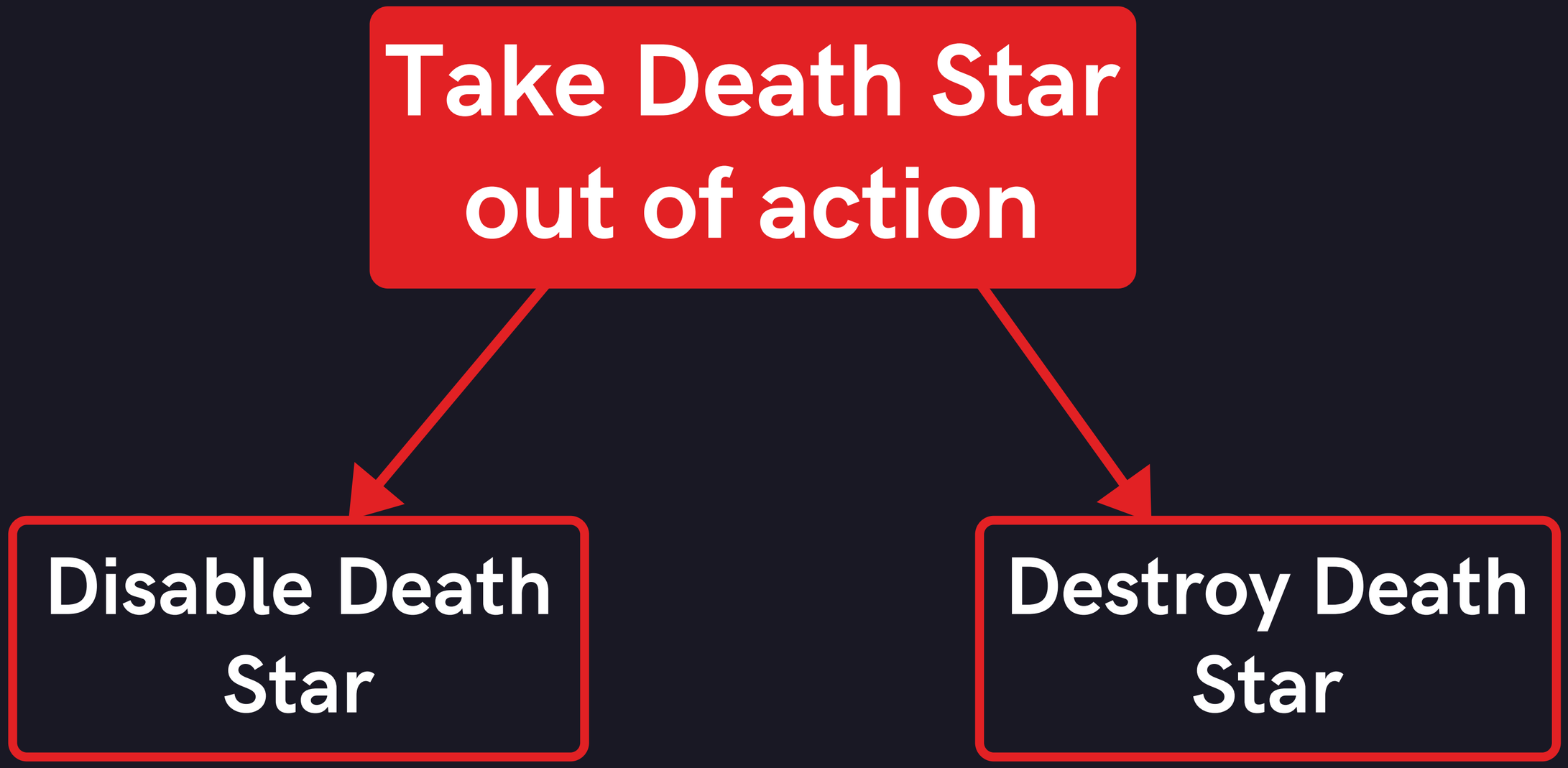

Disable Death Star
System Failure
Mechanical Failure

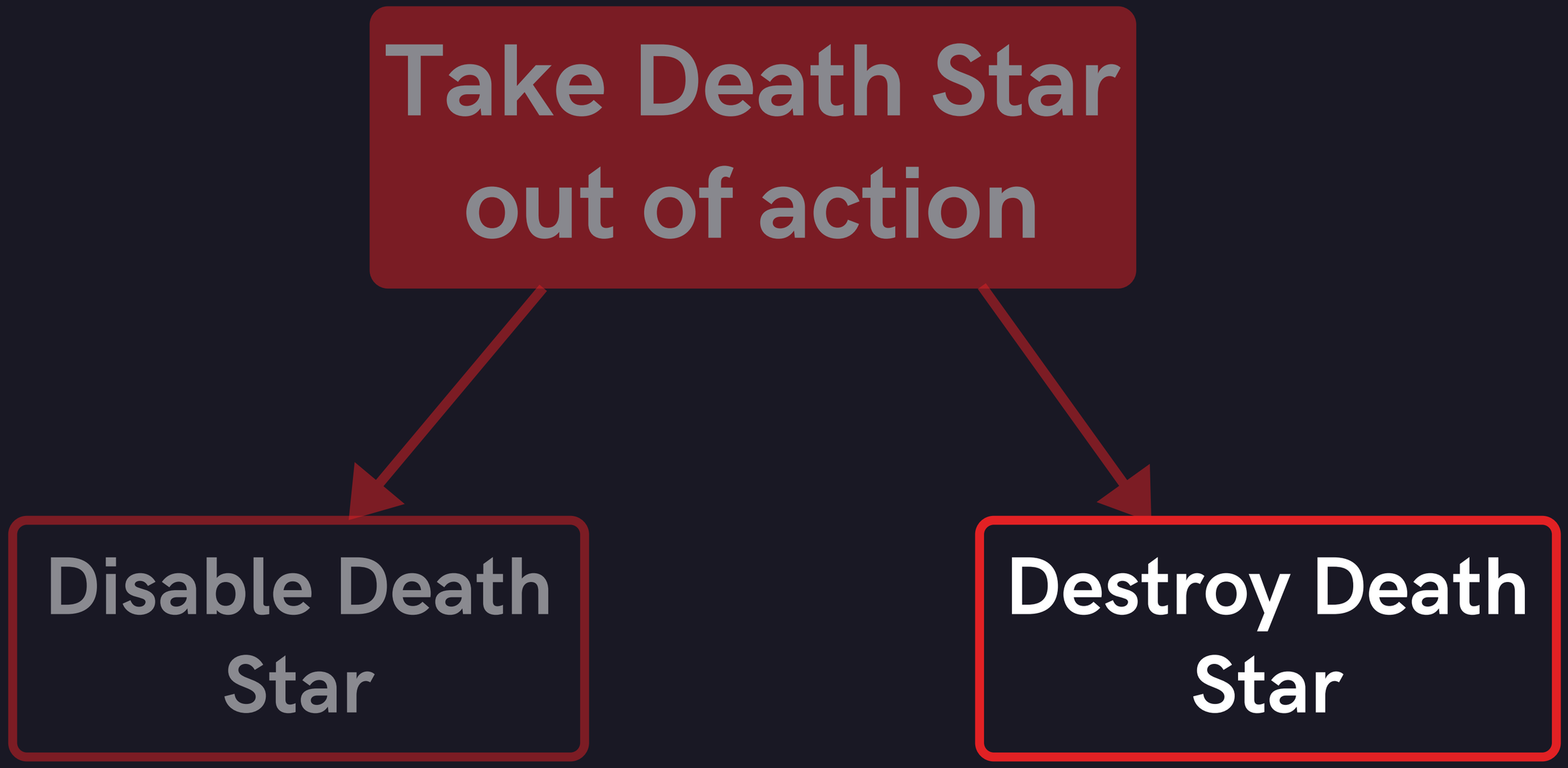

System Failure
Compromise Critical IT systems
Mechanical Failure
Overload Critical Infrastructure

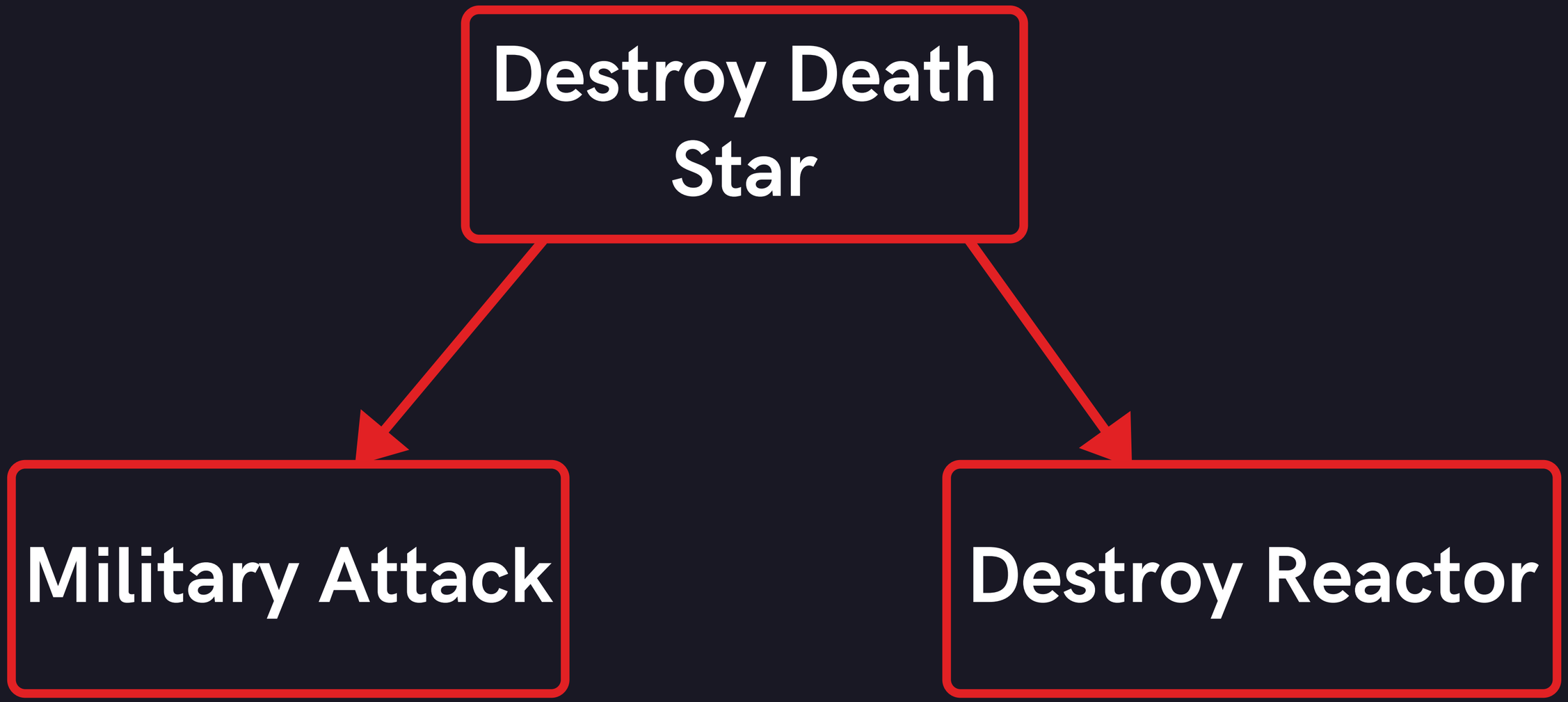

Compromise Critical IT systems
Overload Critical Infrastructure
Privileged access to network

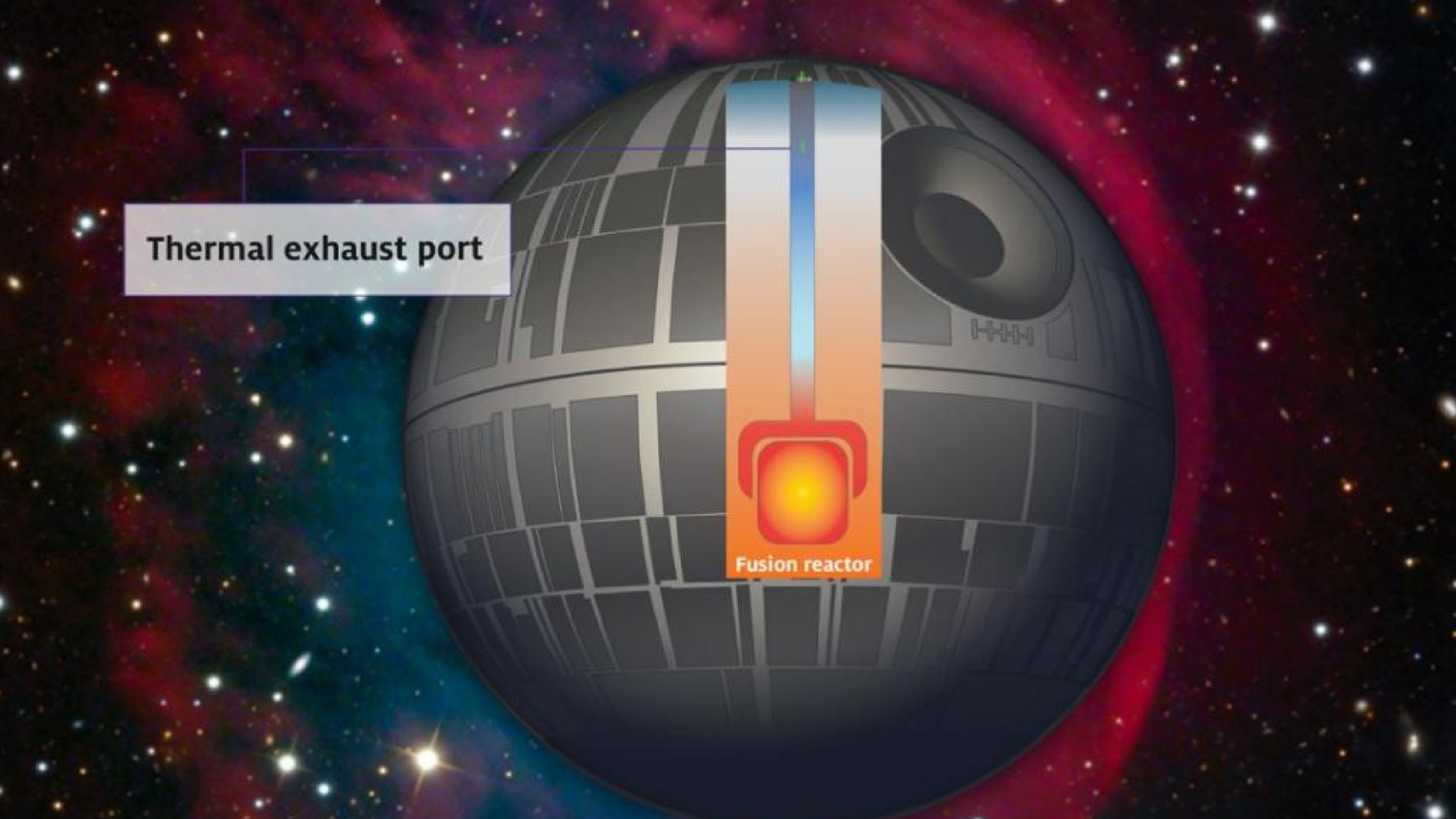

Privileged access to network
Get physical access to the Death Star

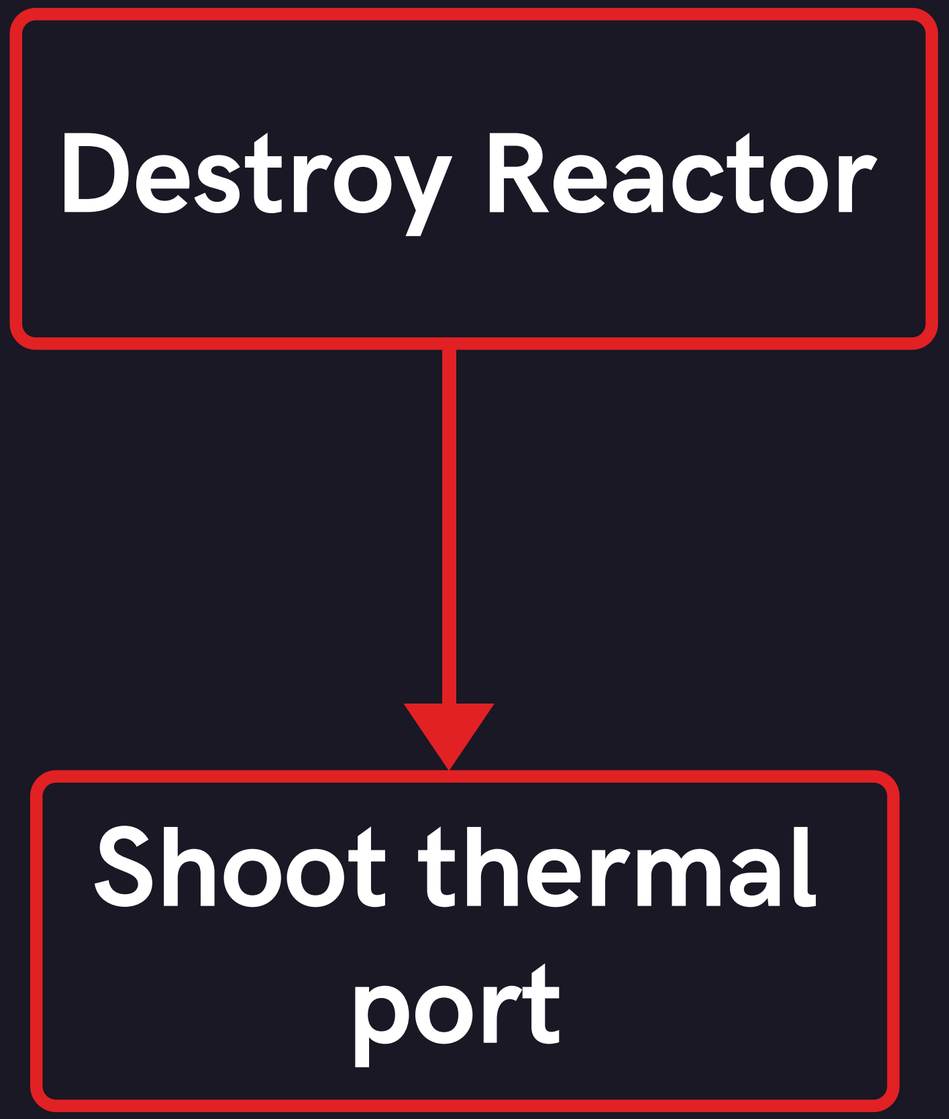

Take Death Star out of action
Disable Death Star
System Failure
Mechanical Failure
Compromise Critical IT systems
Overload Critical Infrastructure
Privileged access to network
Get physical access to the Death Star

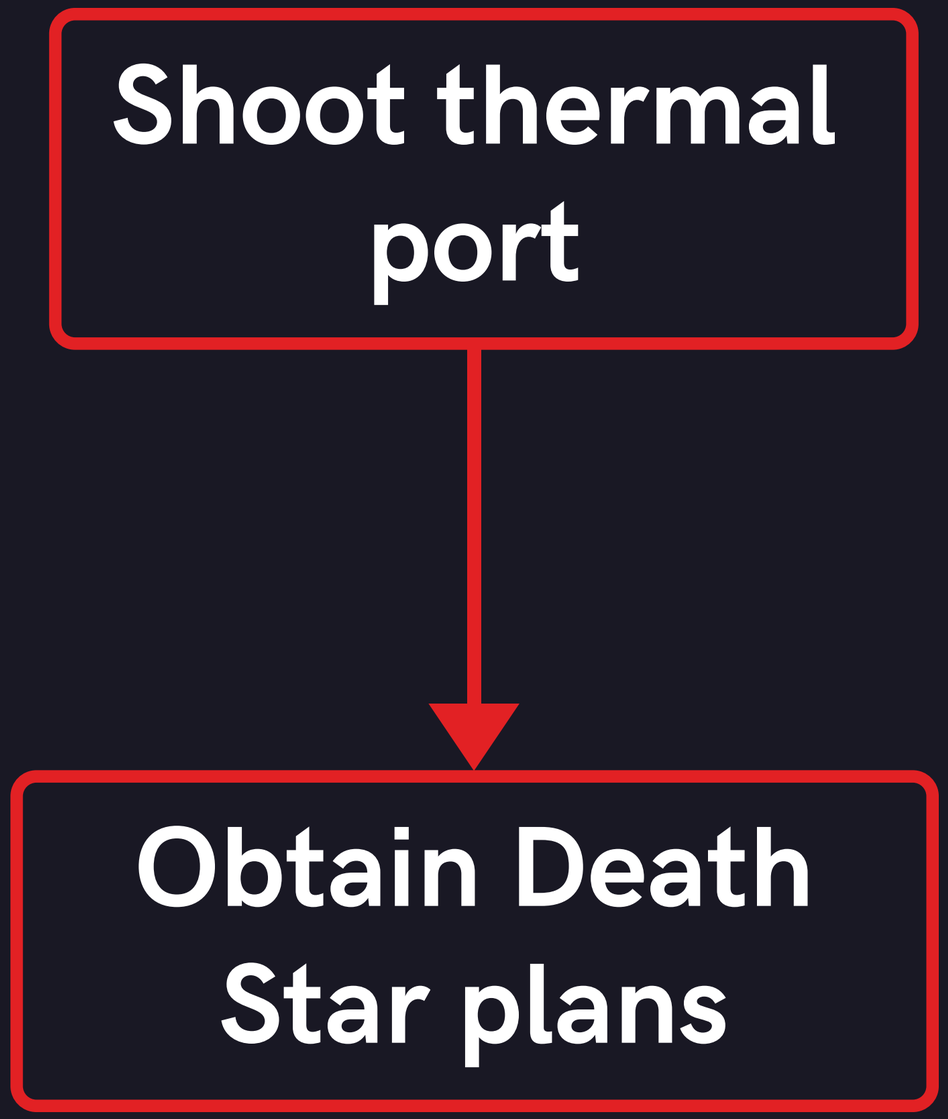

Take Death Star out of action
Disable Death Star
Destroy Death Star

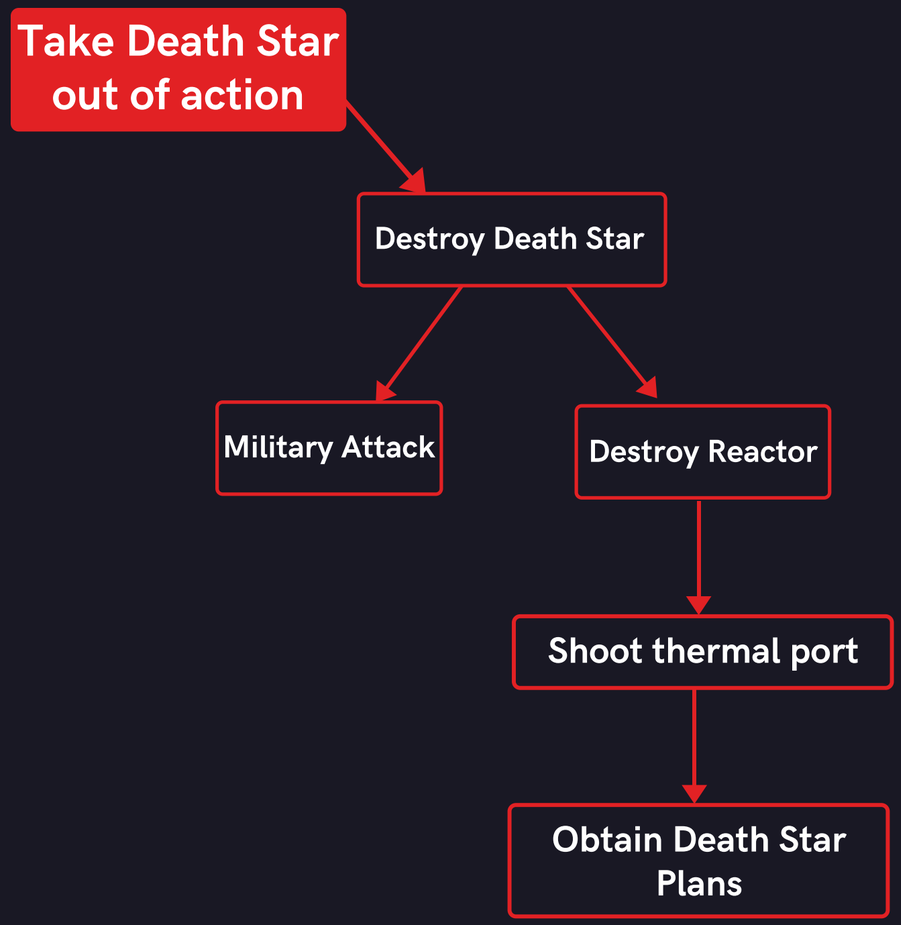

Take Death Star out of action
Disable Death Star
Destroy Death Star

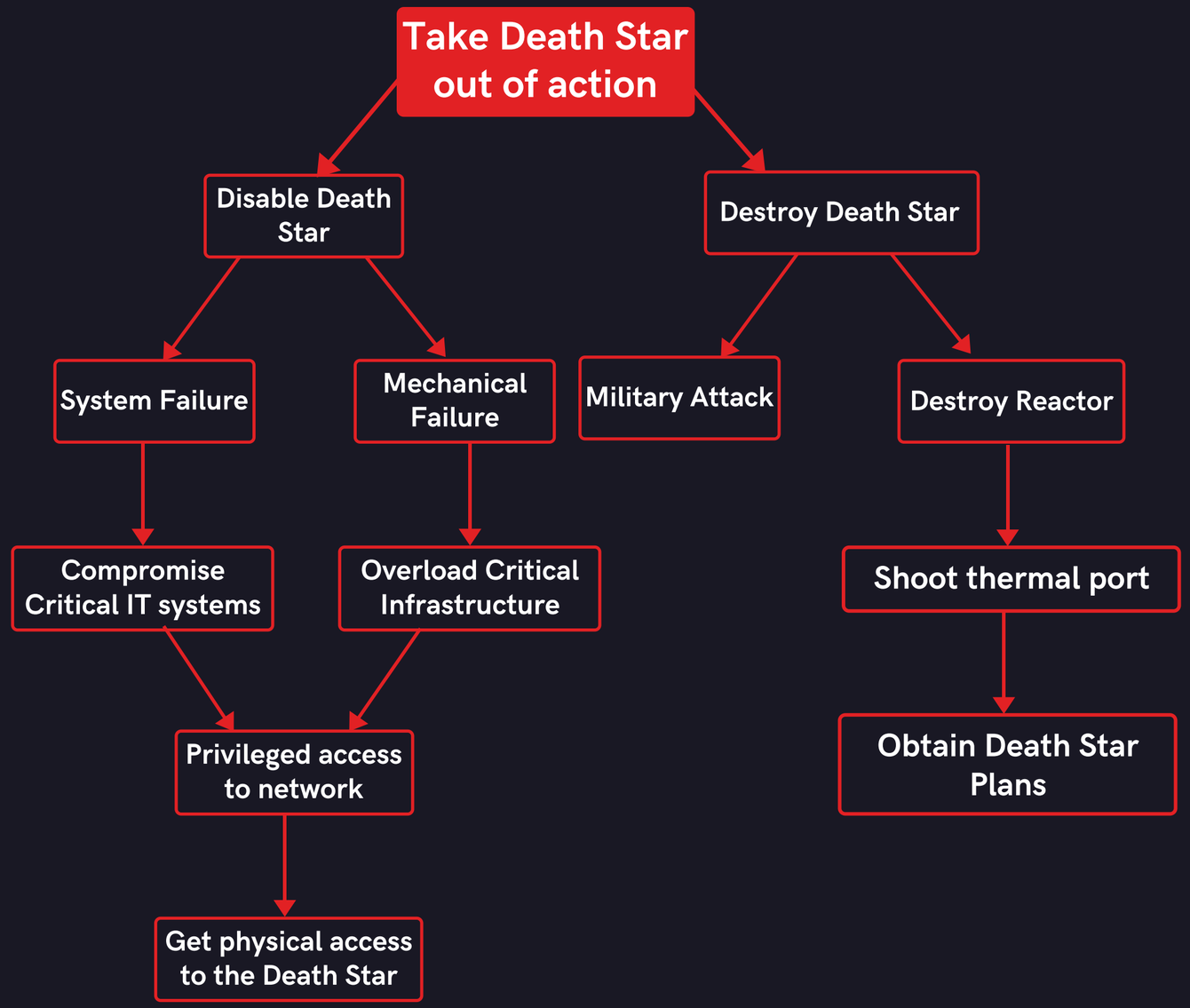

Destroy Death Star
Military Attack
Destroy Reactor


Thermal exhaust port
Fusion reactor


Destroy Reactor
Shoot thermal port


Shoot thermal port
Obtain Death Star plans

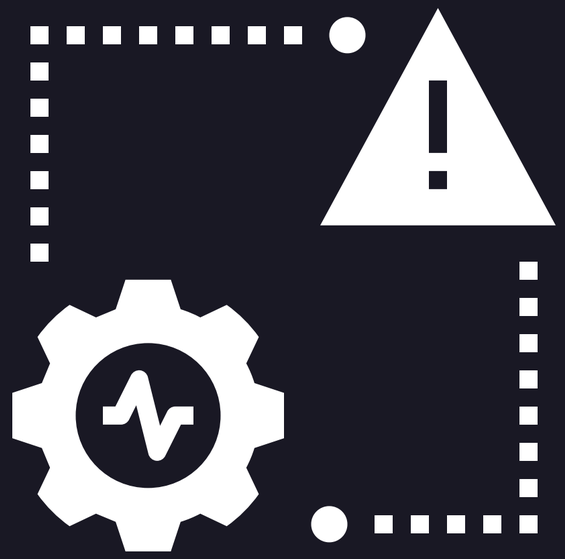

Take Death Star out of action
Destroy Death Star
Military Attack
Destroy Reactor
Shoot thermal port
Obtain Death Star Plans


Take Death Star out of action
Disable Death Star
Destroy Death Star
System Failure
Mechanical Failure
Military Attack
Destroy Reactor
Compromise Critical IT systems
Overload Critical Infrastructure
Shoot thermal port
Privileged access to network
Obtain Death Star Plans
Get physical access to the Death Star

- Take Death Star out of action
  - Disable Death Star
    - System Failure
      - Compromise Critical IT systems
        - Privileged access to network
          - Get physical access to the Death Star
    - Mechanical Failure
      - Overload Critical Infrastructure
        - Privileged access to network
          - Get physical access to the Death Star
  - Destroy Death Star
    - Military Attack
    - Destroy Reactor
      - Shoot thermal port
        - Obtain Death Star Plans

It is a problem solving exercise

Make people think like attackers



MITIGATING RISKS

PRIVILEGED ACCESS TO NETWORK

Impact: High

Likelihood: Medium

MITIGATIONS

Better network segregation

Improved network monitoring

Frequent penetration testing

PRIVILEGED ACCESS TO NETWORK

Impact: High

Likelihood: Low

MILITARY ATTACK

Impact: High

Likelihood: High

MITIGATIONS

Runbooks to respond to attack

Get Star Destroyers "on call"

Monitor Rebellion Activities

MILITARY ATTACK

Impact: Medium

Likelihood: Medium

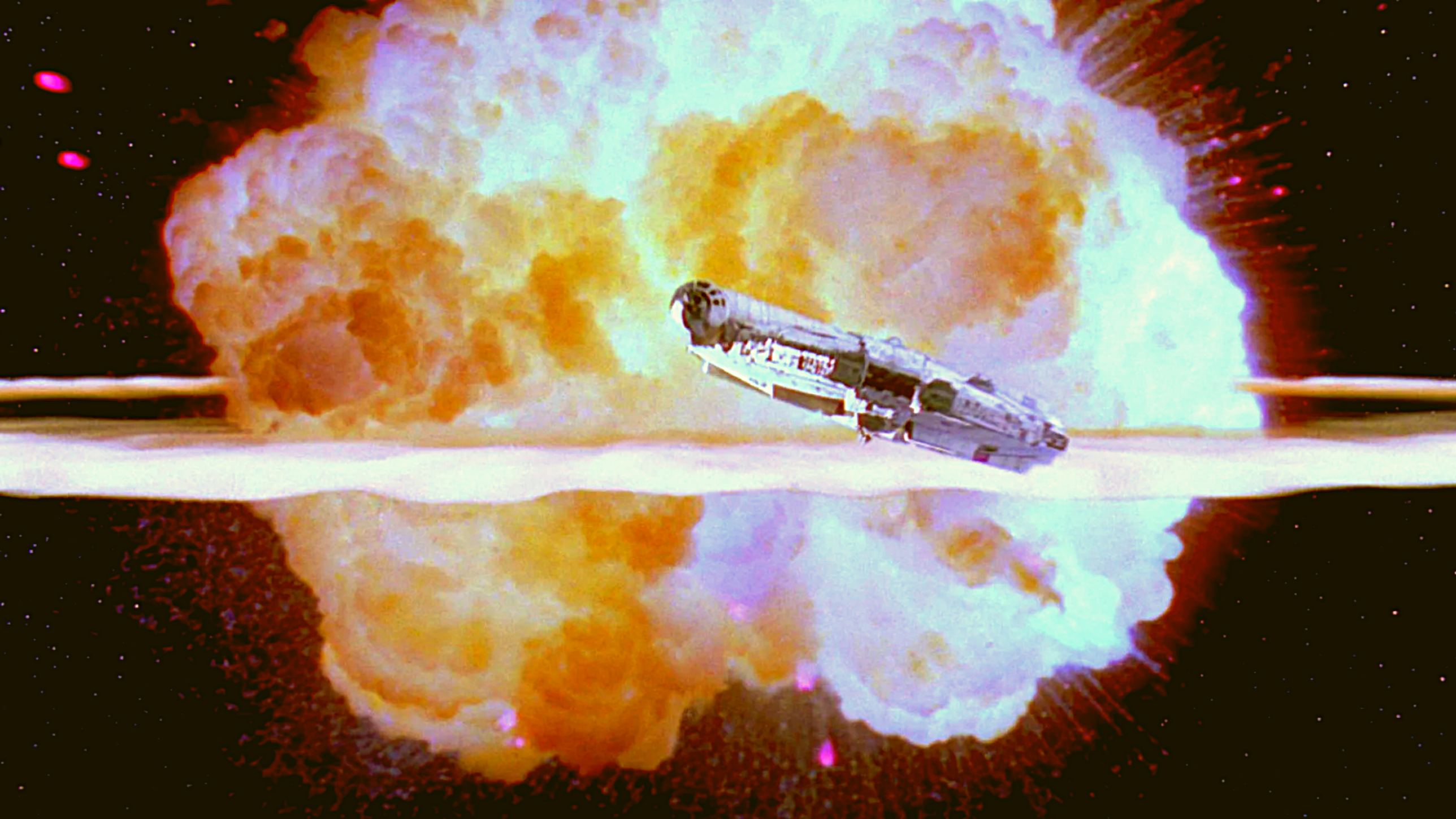
SHOOT AT THERMAL PORT

Impact: High

Likelihood: Low?

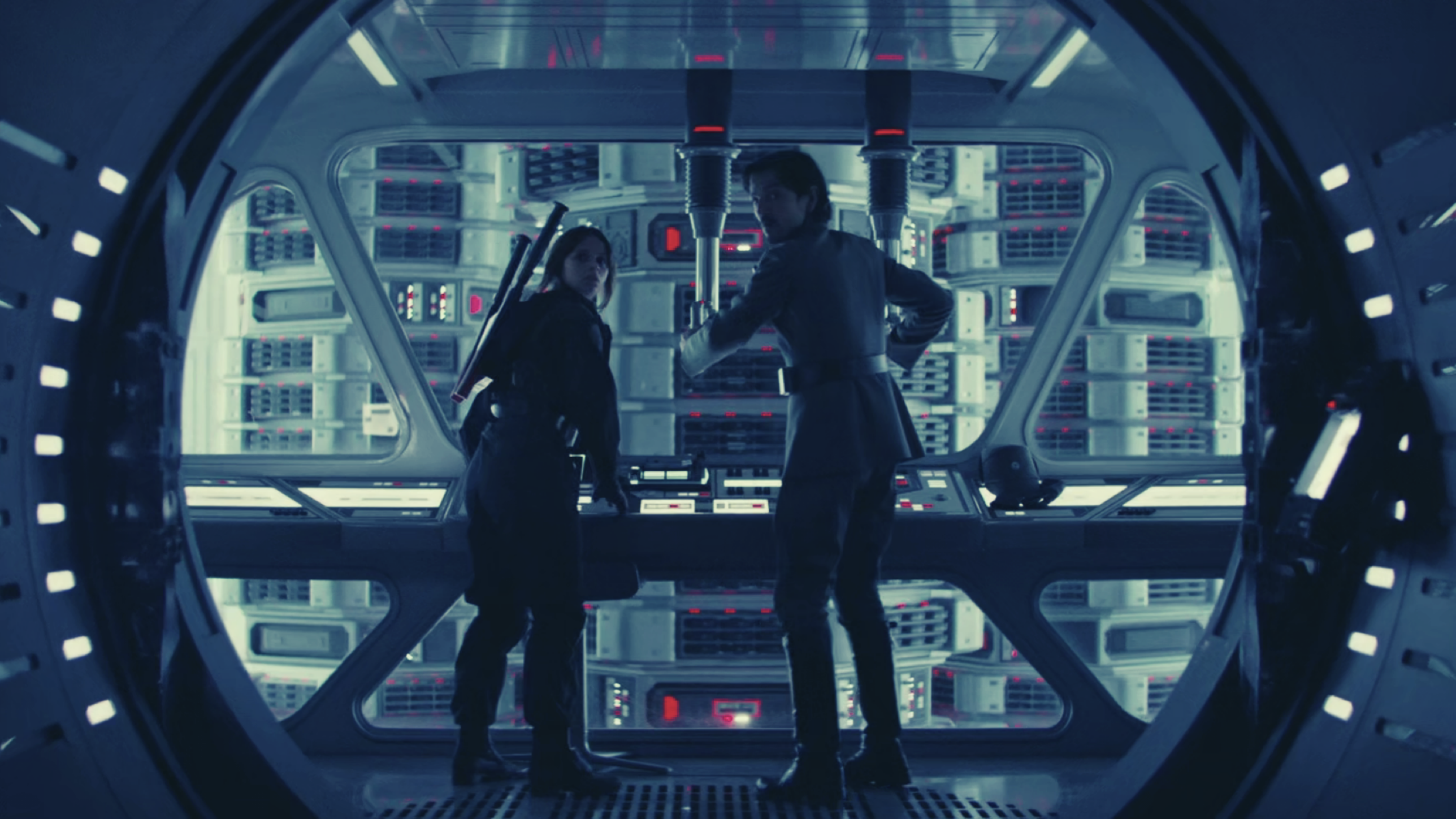
MITIGATIONS?

Hide Death Star plans



FORENSIC ANALYSIS


I'VE GOT A BAD FEELING
ABOUT THIS
made on imgur



LESSONS LEARNED

THREAT MODEL EARLY AND OFTEN

THERE ARE ALWAYS UNKNOWNS

THREAT MODELLING MUST BE ENGAGING

May the Force be with you!

@MarioAreias