

The background features a dark blue and teal color palette. A stylized world map is composed of a grid of small dots. Overlaid on this are various data visualization elements: a vertical bar chart with red and white bars, several circular gauges with numerical scales (e.g., 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260), and numerous floating data points in red, orange, and white. The overall aesthetic is high-tech and analytical.

PV286/PA193: THREAT MODELING

2024 EDITION

AGENDA

Threat Modeling

Term definitions

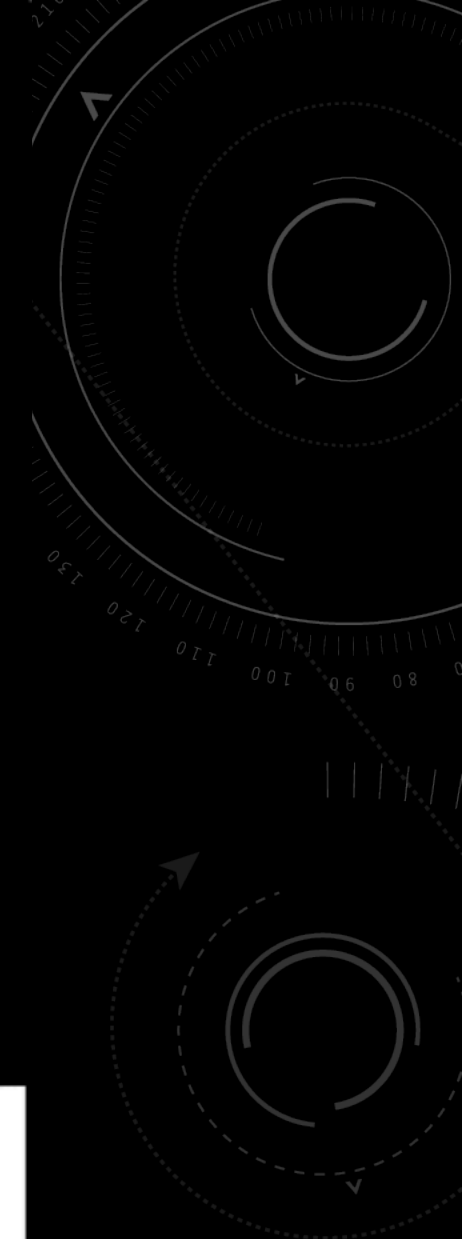
Examples!

Attack Trees, STRIDE, Security Cards

Practical Threat Modeling



THE ANNUAL DEATH RATE AMONG PEOPLE WHO KNOW THAT STATISTIC IS ONE IN SIX.





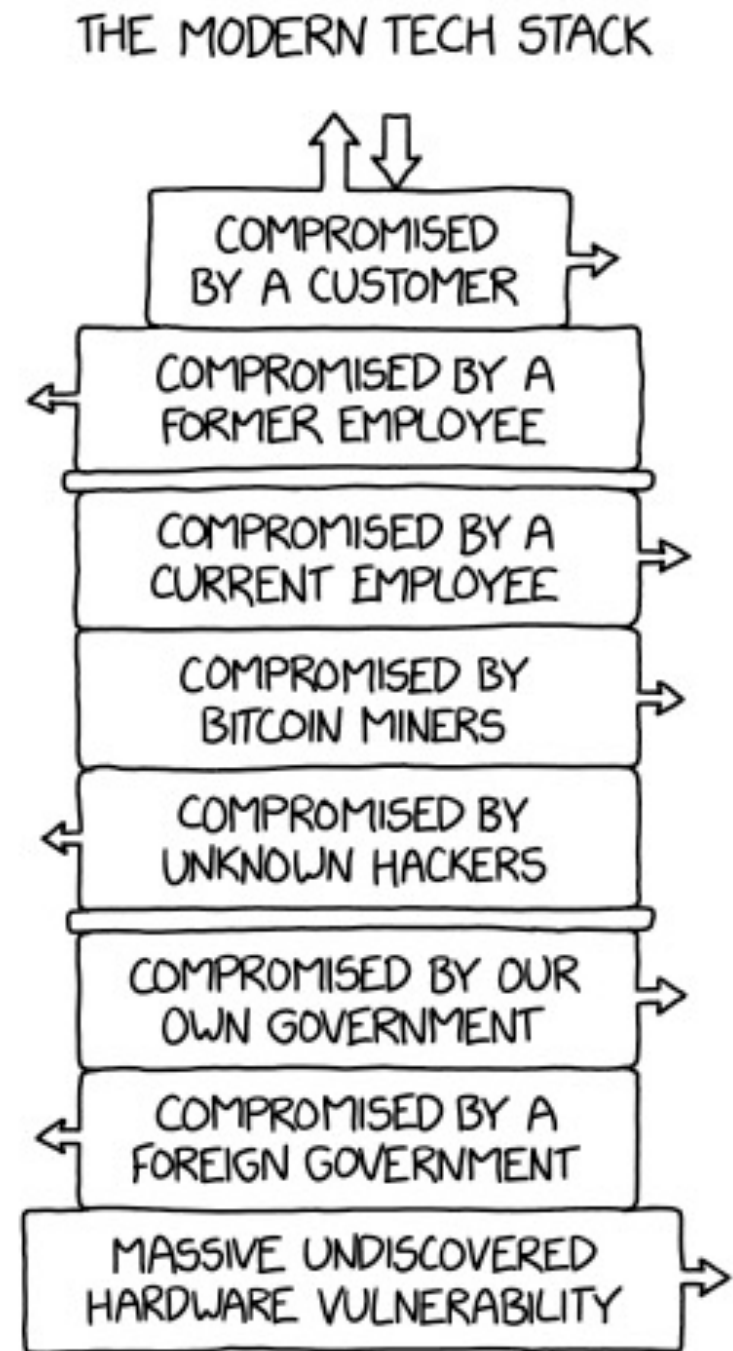
SERIOUS LIFE QUESTIONS

- What is the purpose of life?
- Shall I patch the vulnerability on my internal server?
- Can we keep the default admin password?
- What is the air-speed velocity of an unladen swallow?
- Can we keep the thermal exhaust port as it is now?
- What is the difference between living and existing?
- Is 42 a perfect number?
- Could sharks be a serious threat to my house?

THREAT MODELING

THE MODERN TECH STACK

XKCD 2166



TERM DEFINITIONS

Asset

An asset is what we're trying to protect.

Threat

What we're trying to protect against.

Vulnerability

A weakness or gap in our protection efforts.

Risk

Risk is the intersection of assets, threats, and vulnerabilities.

DEFINITION: THREAT MODELING

Threat modeling is a process by which potential threats can be identified, enumerated and prioritized, all from a hypothetical attacker's point of view.

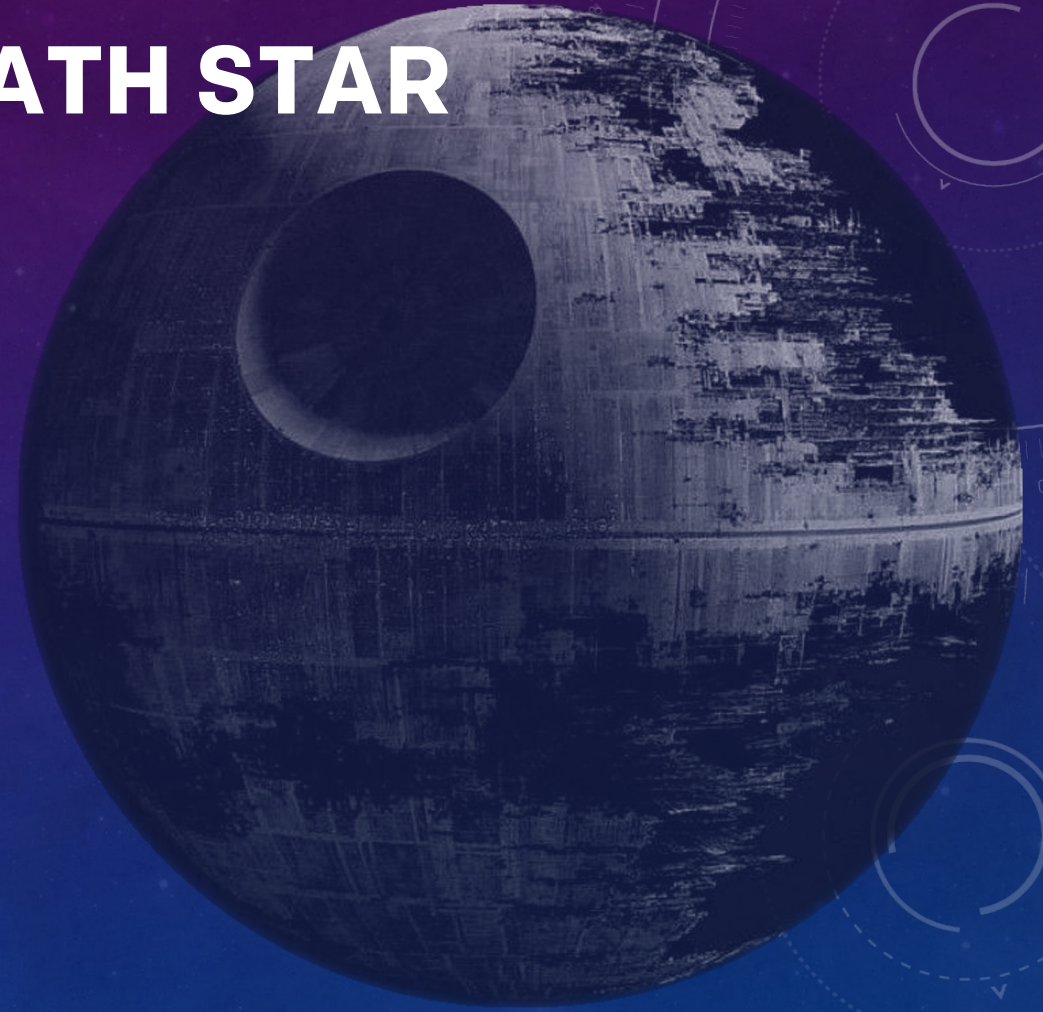
(aka "analyzing risky designs")

PRIMARY COMPONENTS

- Assets
- Personas/Attackers
 - Not just people, it could be other disasters as well
- Methods/Attack Vectors
 - Impacts
 - Likelihood
- Mitigation/Countermeasures

THREAT MODELING THE DEATH STAR

- Credit: Threat Modeling the Death Star; Mario Areias; PyCon 2019

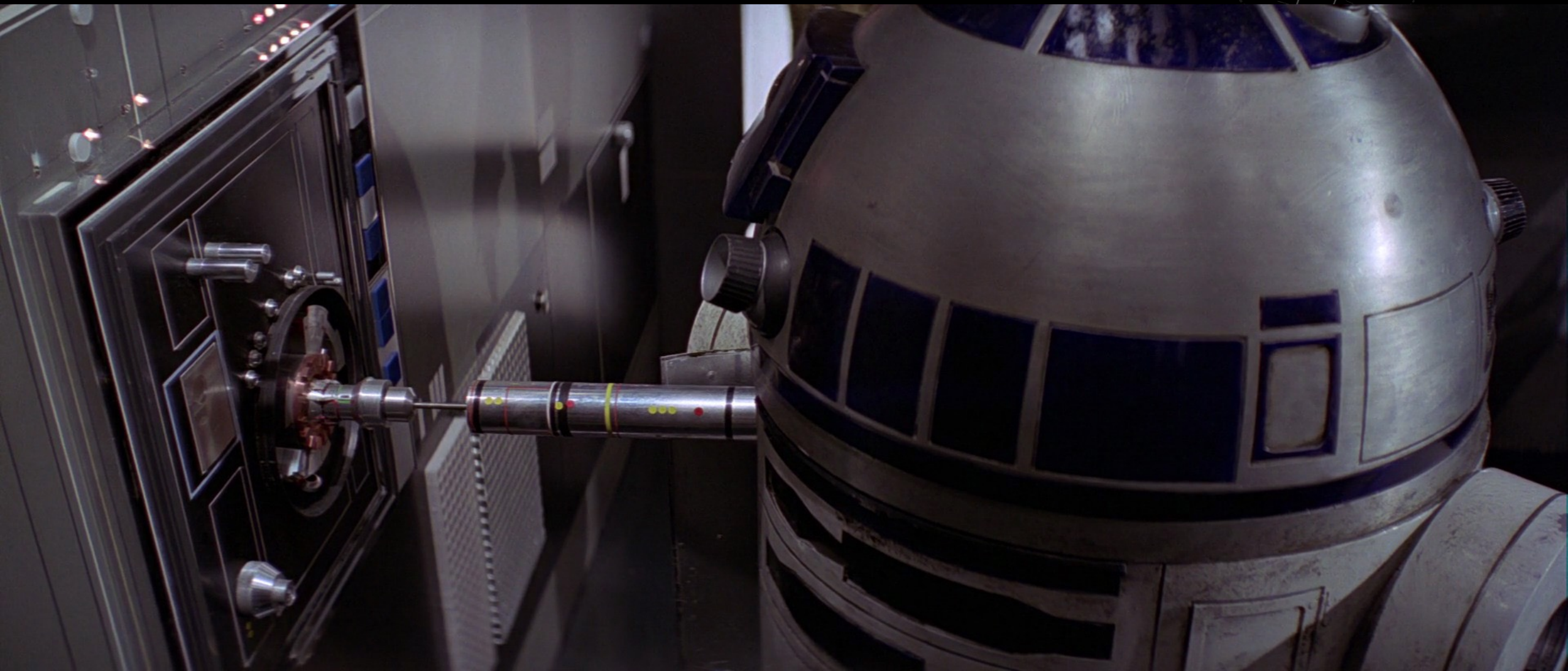




YOUR MISSION

- Goal: The Death Star
- Stakeholder: Galactic Empire
- Project status
 - Big, very big waterfall project
 - 20 years in the making
 - Way over budget
 - Deadline missed many times
 - **Motivated leader with vision!**
 - Known terrible security of the past projects





THESE AREN'T THE DROIDS
WE'RE LOOKING FOR
 NO REWARD DO... OR DO NOT THE CIRCLE IS NOW COMPLETE
 IS WORTH DO... OR DO NOT THE CIRCLE IS NOW COMPLETE
 THIS MOST IMPRESSIVE
WE'RE DOOMED
 YOU WILL NEVER FIND A MORE WRETCHED HIVE OF SCUM AND VILLAINY
 THE FORCE IS WITH YOU
 HE'S NO GOOD TO ME DEAD
 NOW I AM THE MASTER
I AM YOUR FATHER
 THERE IS NO TRY
SIZE MATTERS
 YOU DON'T KNOW THE POWER OF THE DARK SIDE
NOT SORRY ABOUT THE MESS
 HELP ME, OBI-WAN KENOBI
IT'S A TRAP! AS YOU WISH
 THE FORCE IS STRONG WITH THIS ONE
 STRIKE ME DOWN
 IT'S NOT WISE TO UPSET A WOOKIEE
 YOU'RE MY ONLY HOPE
 OBI-WAN HAS THOUGHT YOU WELL
 BLAST THE DOOR BEWARE OF THE DARK SIDE
SET FOR STUN
 YOU WILL MEET YOUR DESTINY
 BLAST 'EM
 GREAT SHOT, KID
 AS YOU WISH
MAY THE FORCE BE WITH YOU
YOU LIKE ME BECAUSE I'M A SCOUNDREL
 I FIND YOUR LACK OF FAITH DISTURBING
 WHO'S SCRIBBY LOOKING?
 I HAVE A BAD FEELING ABOUT THIS
REBEL SCUM HOLD YOUR FIRE
 TELL JABBA I'VE GOT HIS MONEY
 STAY ON MY TARGET
 YOU ARE NOT A JEDI YET HE'S THE BRAINS, SWEETHEART
 YOUR POWERS ARE WEAK, OLD MAN
 ONLY IMPERIAL STUNBRODDERS ARE SO PRECISE
THAT BOY IS OUR LAST HOPE
 I'M A JEDI LIKE MY FATHER BEFORE ME
 SHE'S FAST ENOUGH FOR YOU, OLD MAN
A LONG TIME AGO IN A GALAXY FAR, FAR AWAY....
 LAUGH IT UP, PUZZBALL
 LETS BLOW THIS THING AND GO HOME
THAT'S NO MOON
 THE FORCE IS STRONG WITH HIM
 USE THE FORCE
 WE MEET AGAIN AT LAST
 FAR AWAY....
 LAUGH IT UP, PUZZBALL
 LETS BLOW THIS THING AND GO HOME

TM



THREAT MODELING: **ATTACK TREES**

- Evil Personas
- Have the right people in the room
- Build the trees
 - Brainstorm!
- Find mitigations
 - And implement them

The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several overlapping circular elements. A prominent feature is a large circular scale with tick marks and numerical labels (140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) arranged in a semi-circle. Other circles include solid and dashed lines, some with arrows indicating direction, and some with partial segments. The overall aesthetic is technical and futuristic.

PERSONAS

POTENTIAL ATTACKERS

SCRIPT KIDDIES

Expertise



Resources



Organization





BOUNTY HUNTERS

Expertise



Resources



Organization



JEDI

Expertise



Resources



Organization





INSIDER THREAT

Expertise



Resources



Organization



NATION STATE

Expertise



Resources



Organization





RIGHT PEOPLE IN THE ROOM

LET'S DO SOME ANALYSIS!



OUR TEAM

- Engineers
- Architects
- You, as a lead security architect!

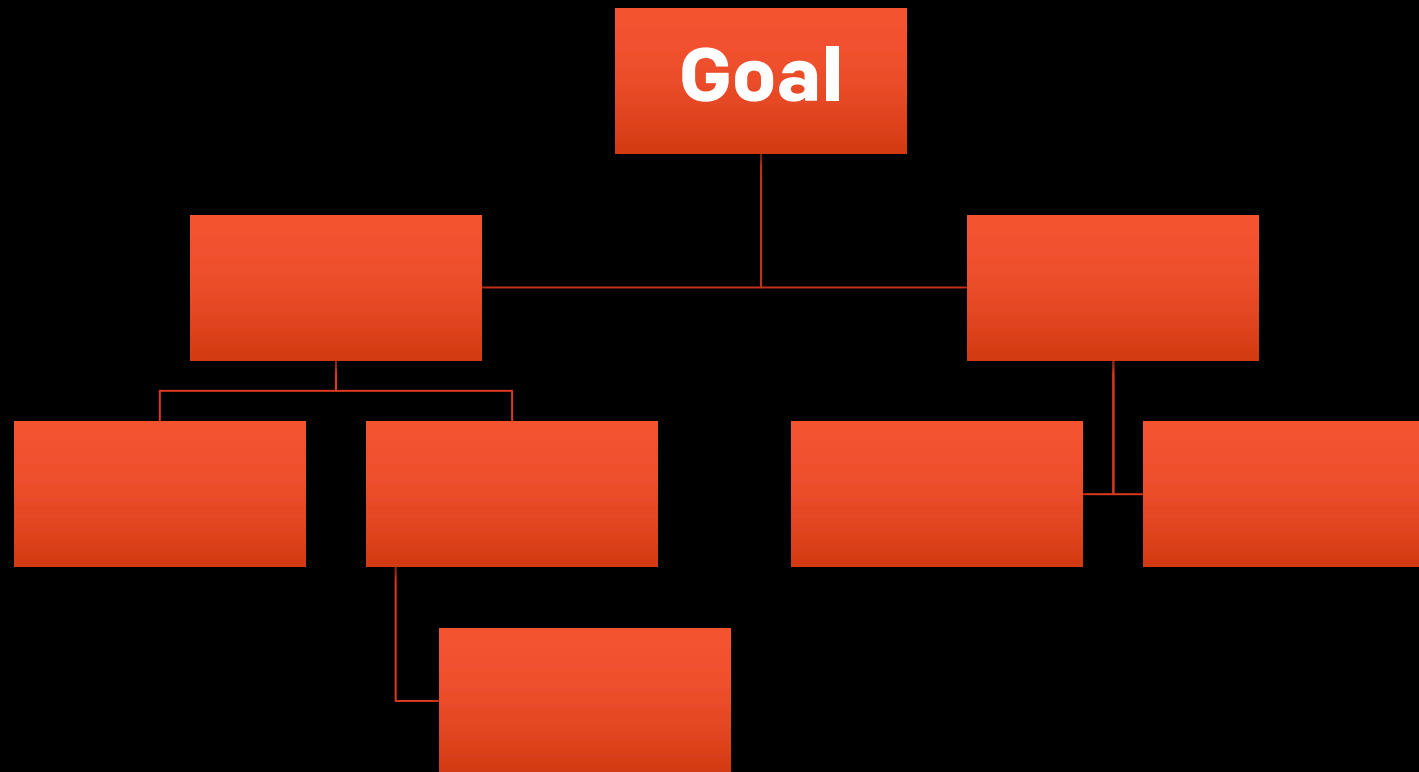


The background features a blue gradient with several circular gauges and arrows. One large gauge on the left has numerical markings from 140 to 260. Other gauges are smaller and scattered across the scene. Arrows of various sizes and orientations are also present, some pointing towards the center and others pointing outwards. The overall aesthetic is technical and futuristic.

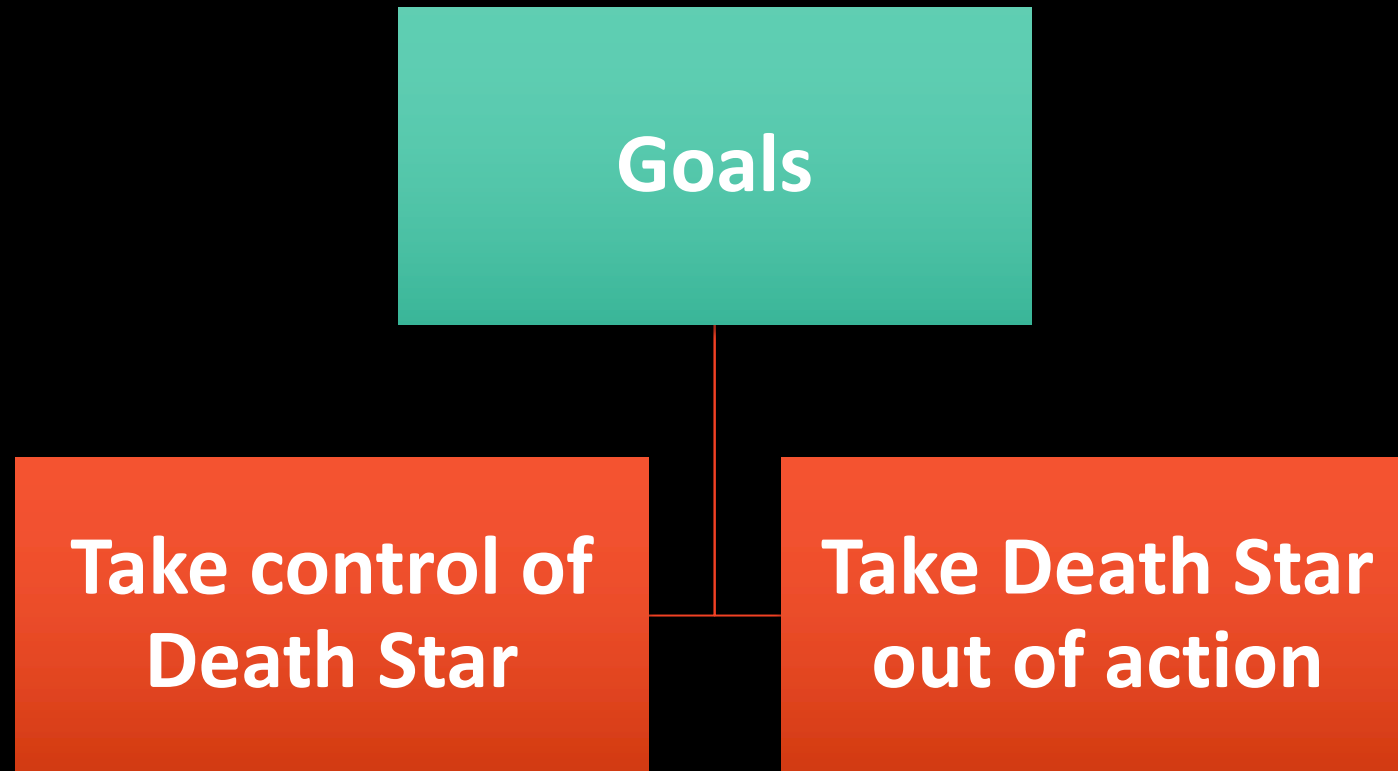
ATTACK VECTORS

GOALS, METHODS

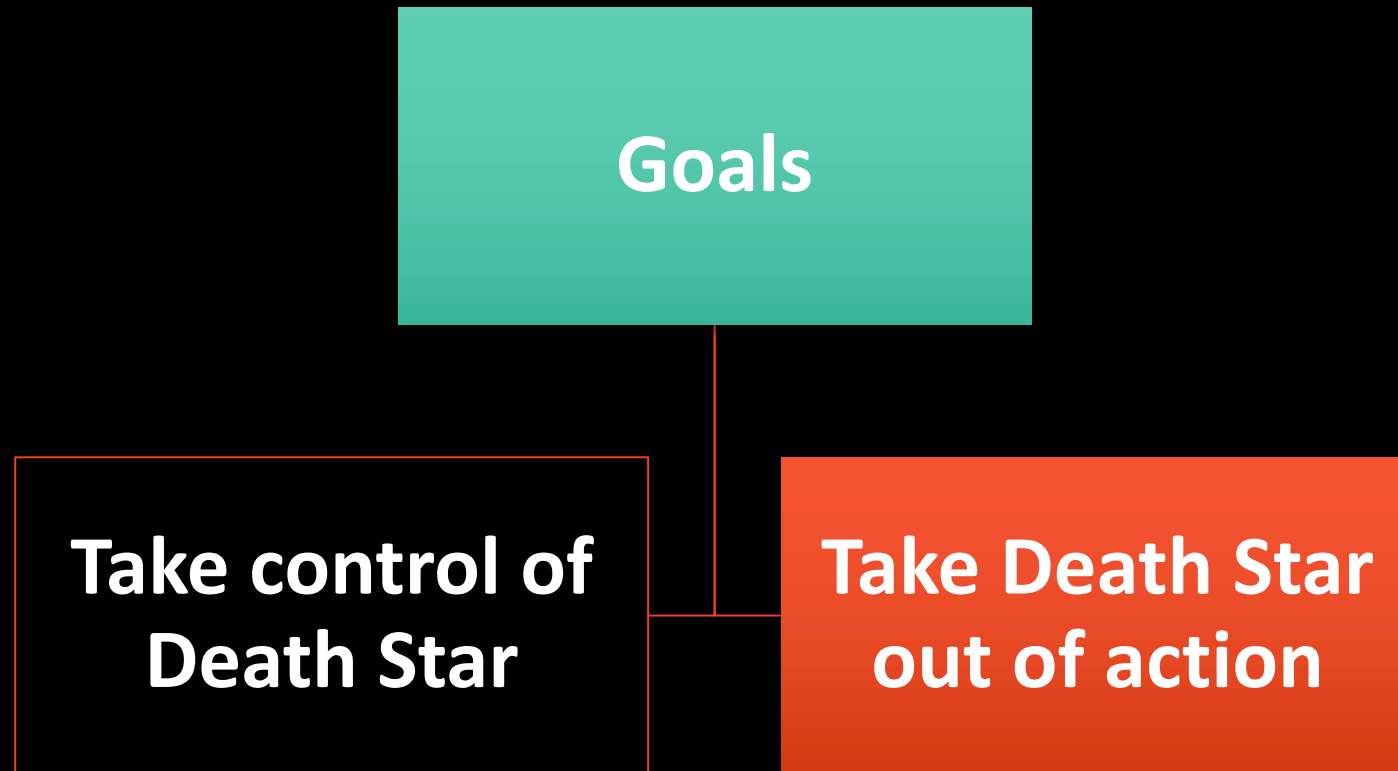
THREAT MODELING: **ATTACK TREES**



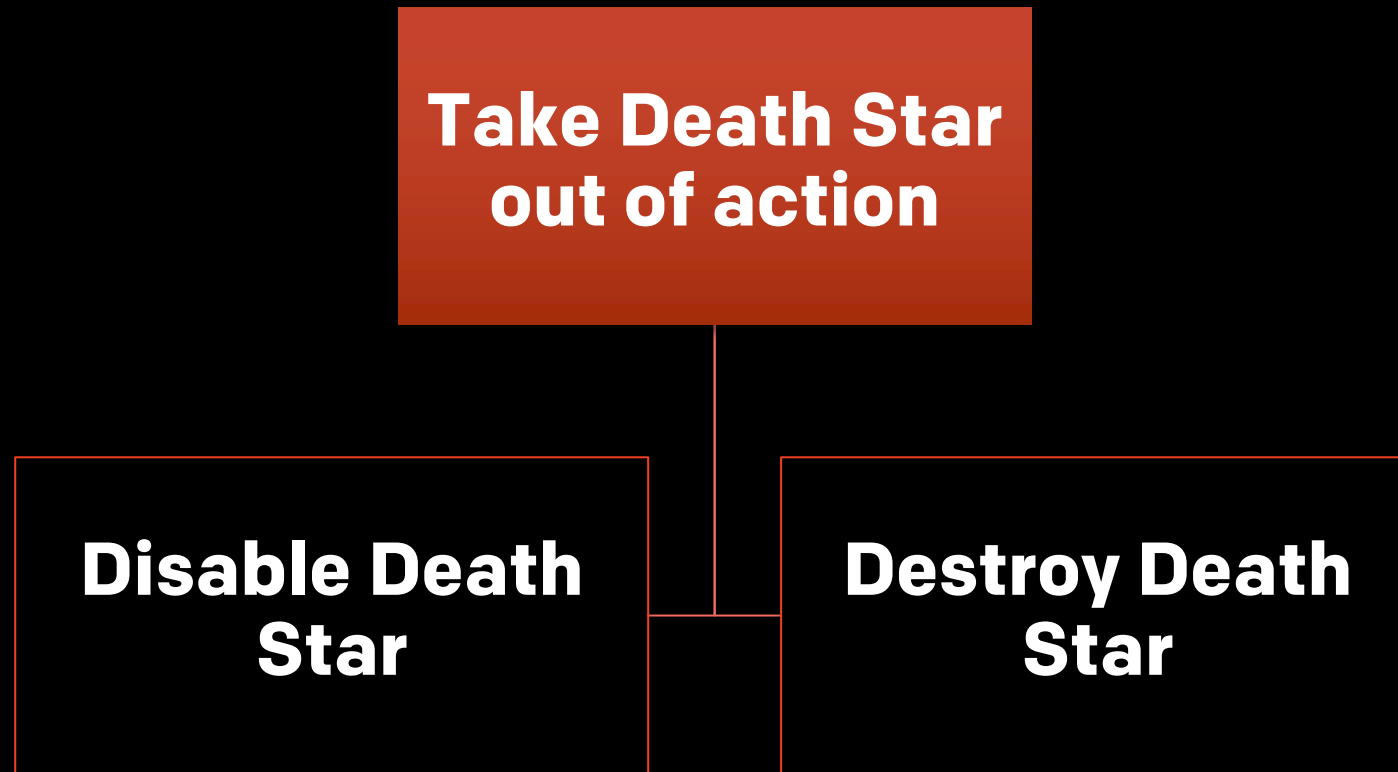
THREAT MODELING: **ATTACK TREES**



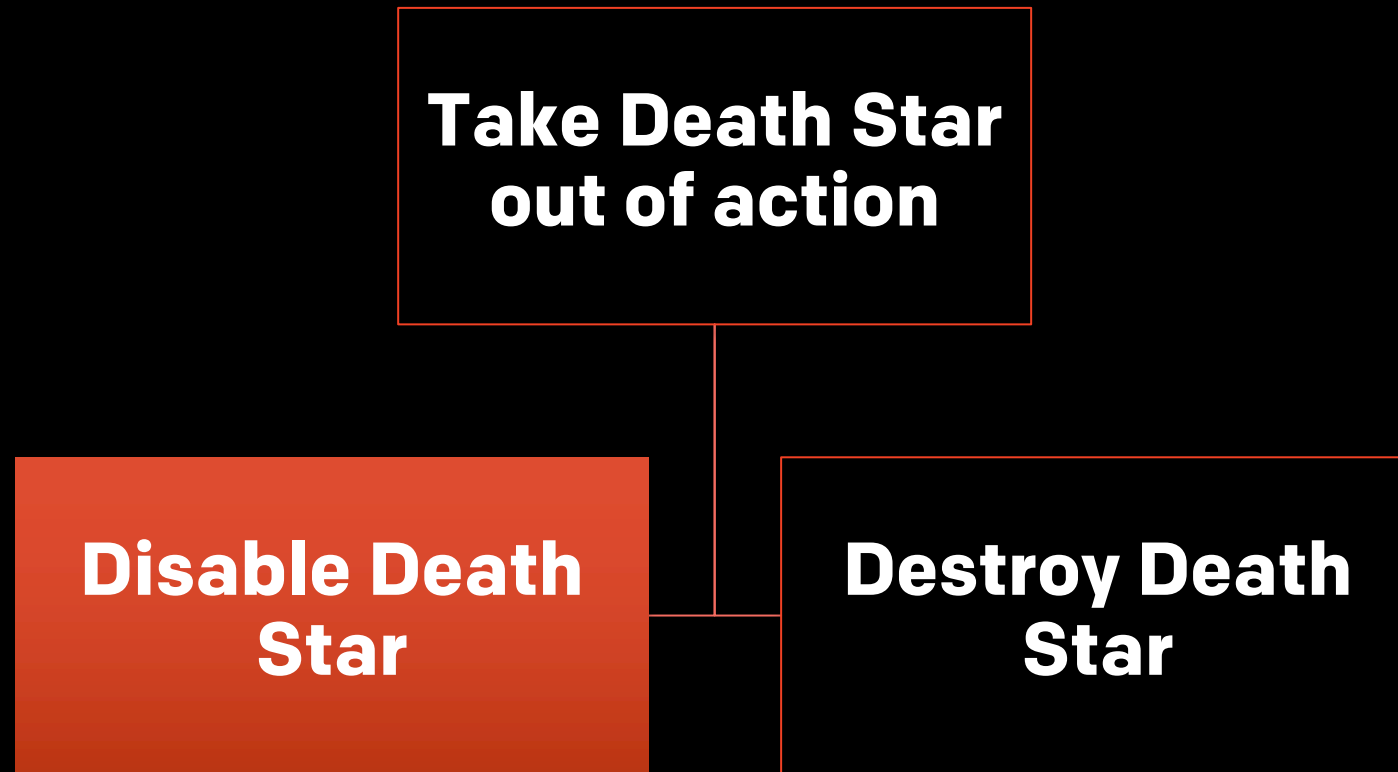
THREAT MODELING: **ATTACK TREES**



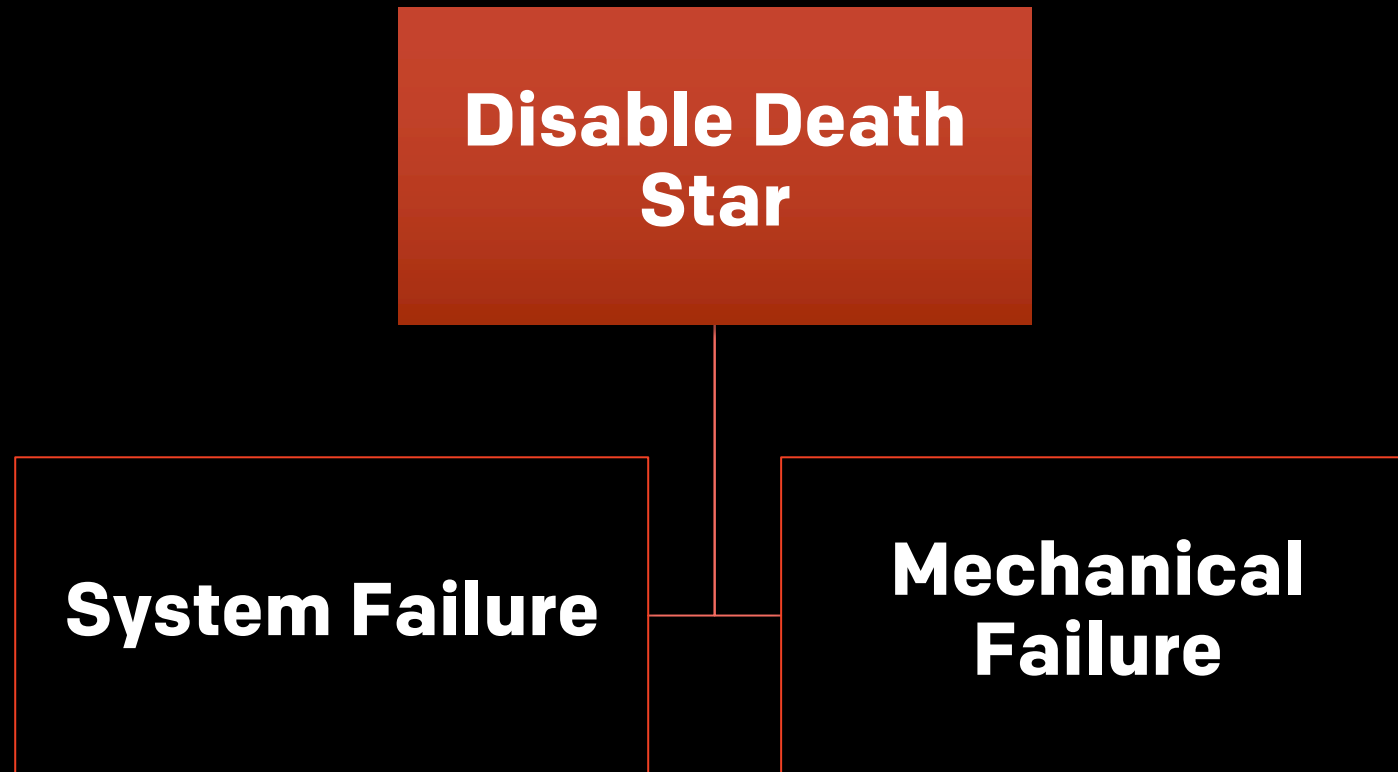
THREAT MODELING: **ATTACK TREES**



THREAT MODELING: **ATTACK TREES**



THREAT MODELING: **ATTACK TREES**



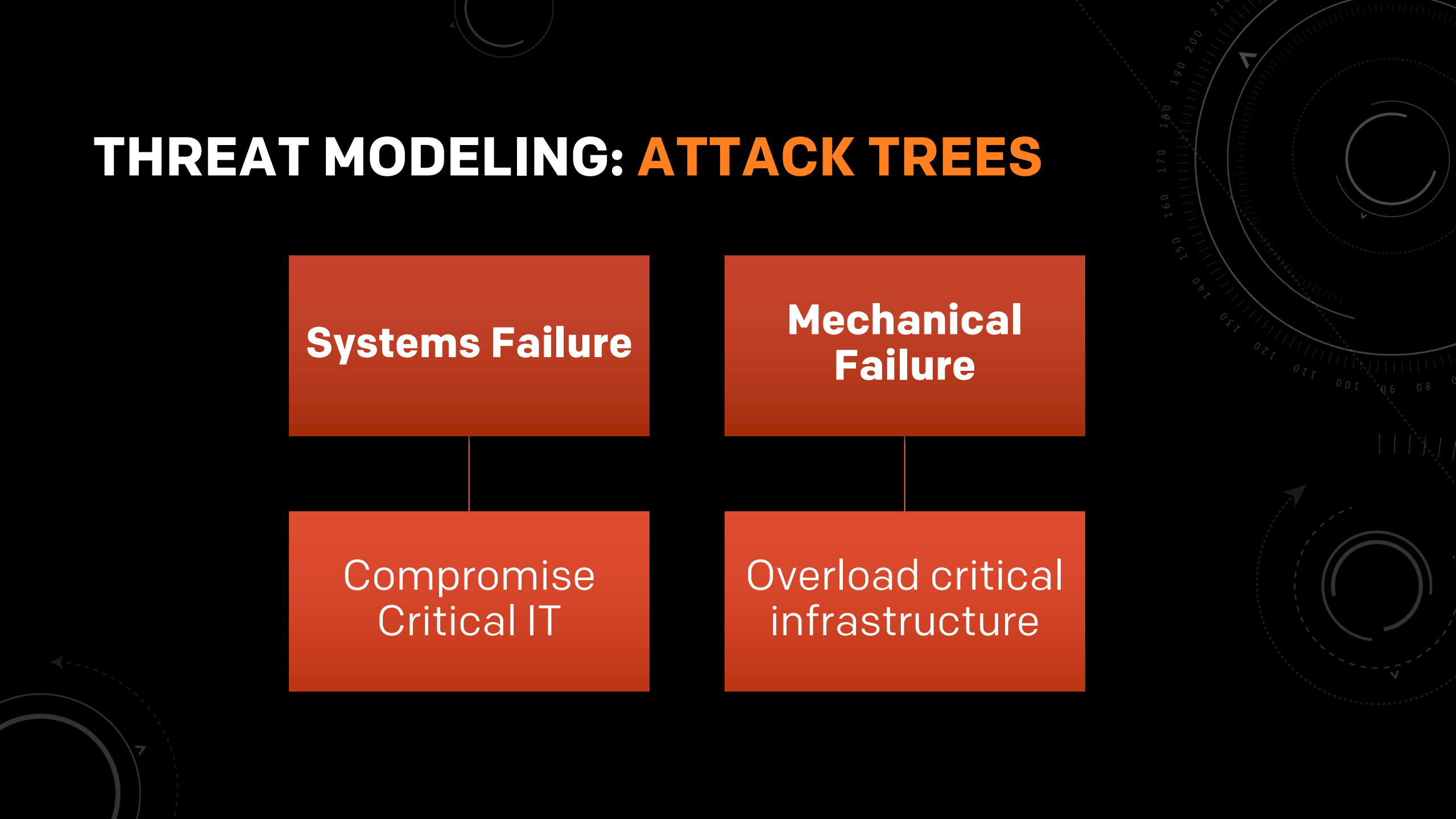
THREAT MODELING: **ATTACK TREES**

Systems Failure

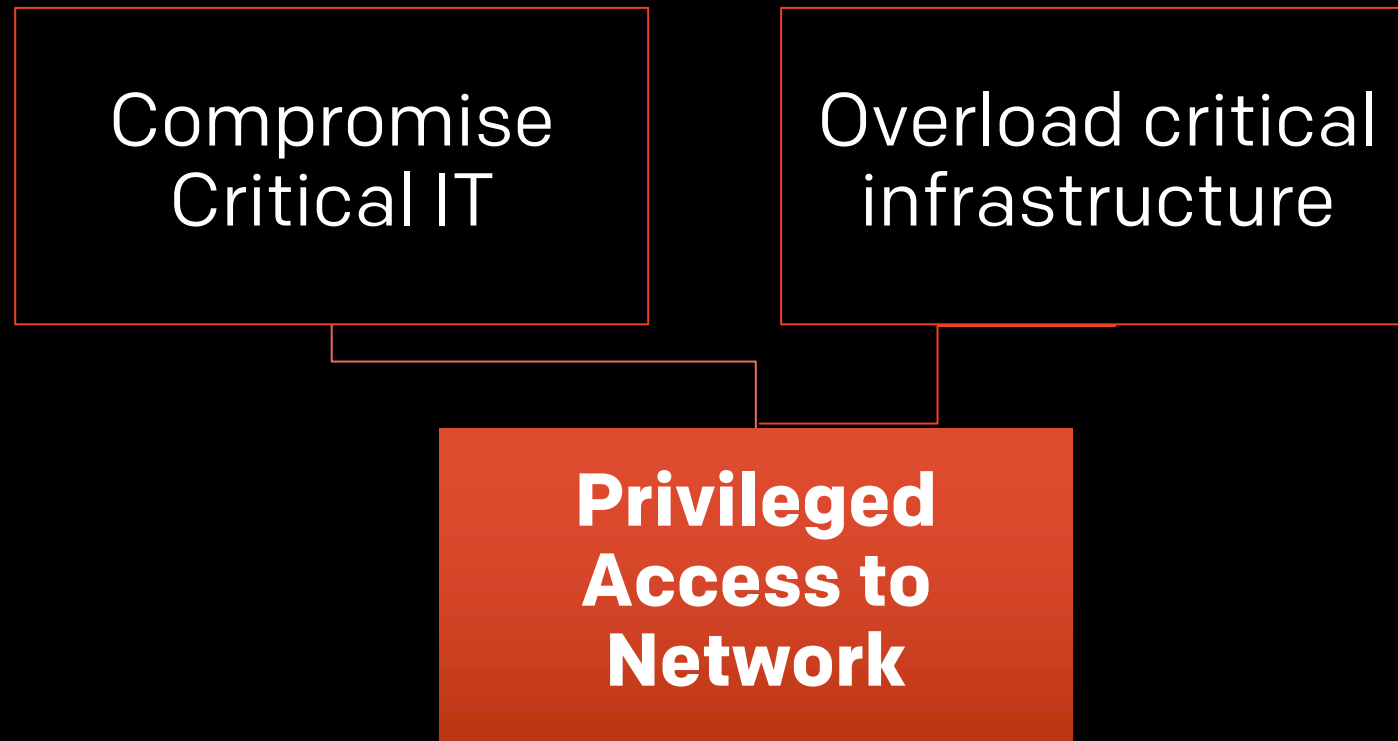
Compromise
Critical IT

**Mechanical
Failure**

Overload critical
infrastructure



THREAT MODELING: **ATTACK TREES**

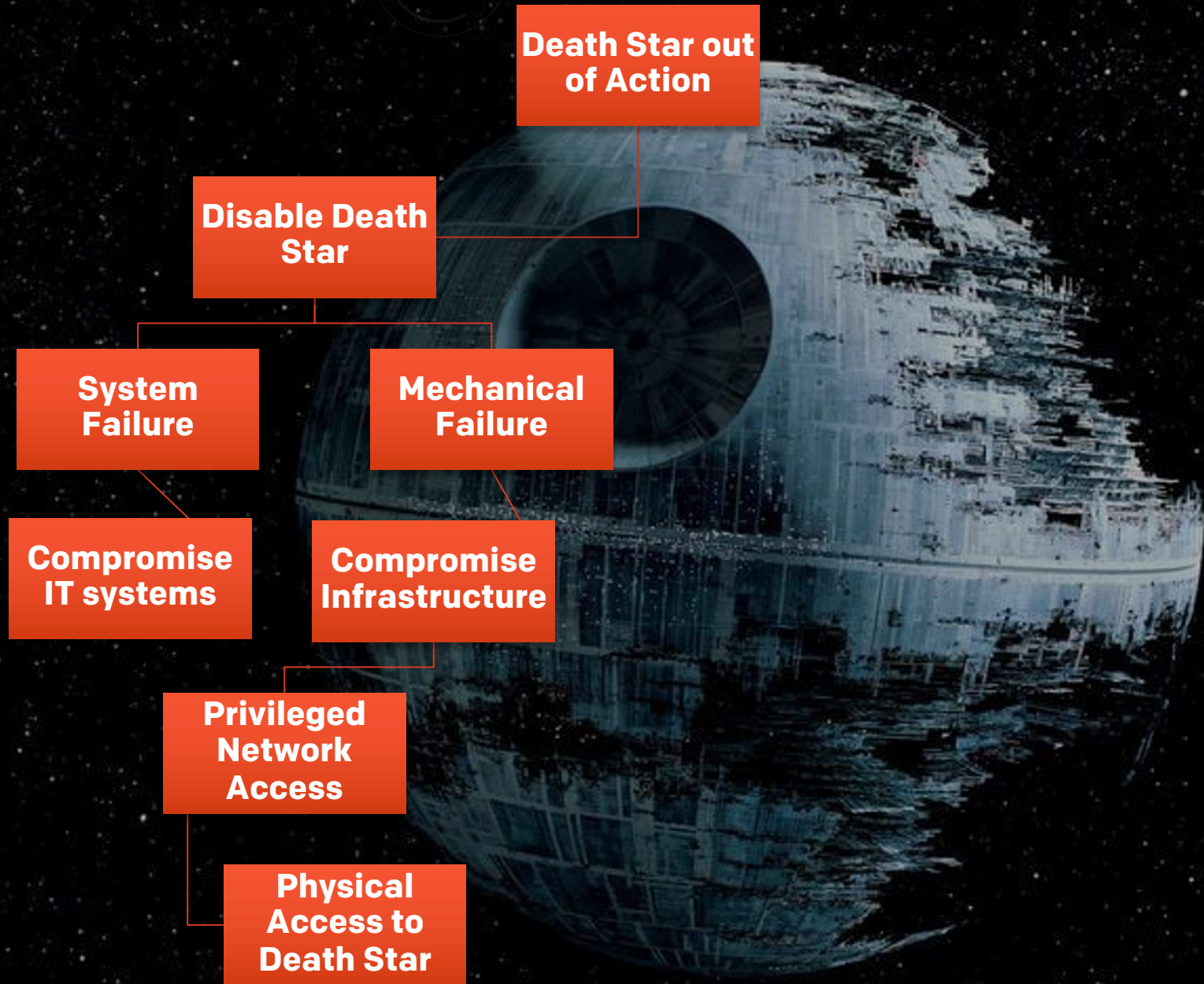


THREAT MODELING: **ATTACK TREES**

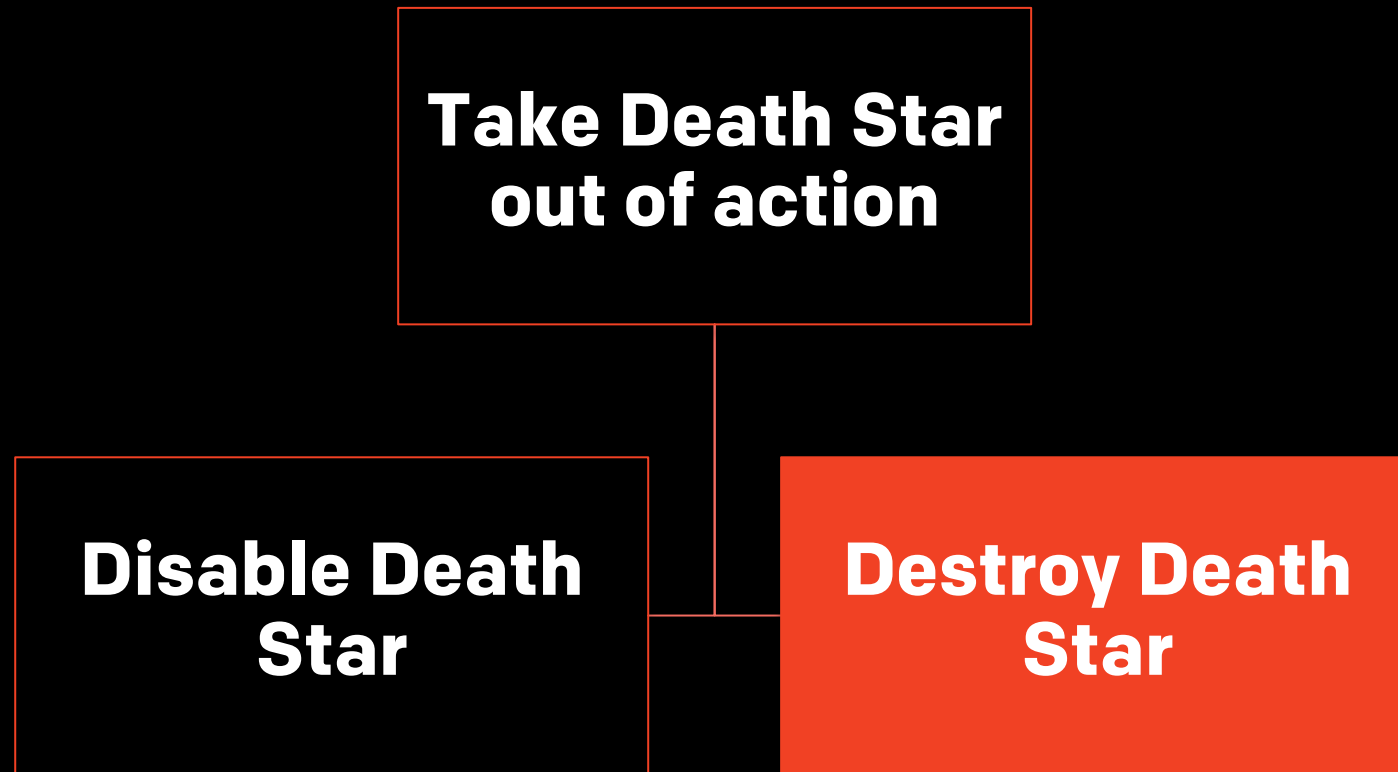
**Privileged
Access to
Internal Network**

Get Physical
Access to Death
Star

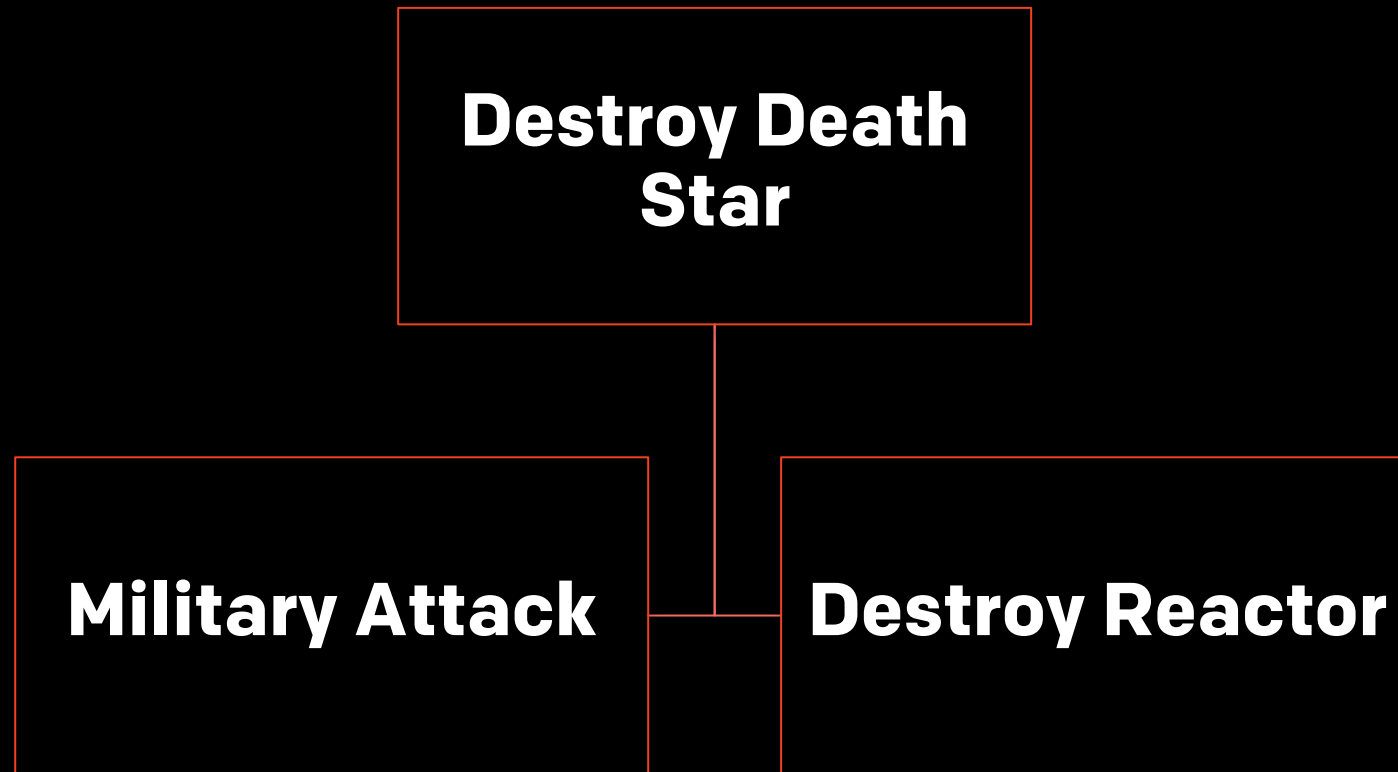




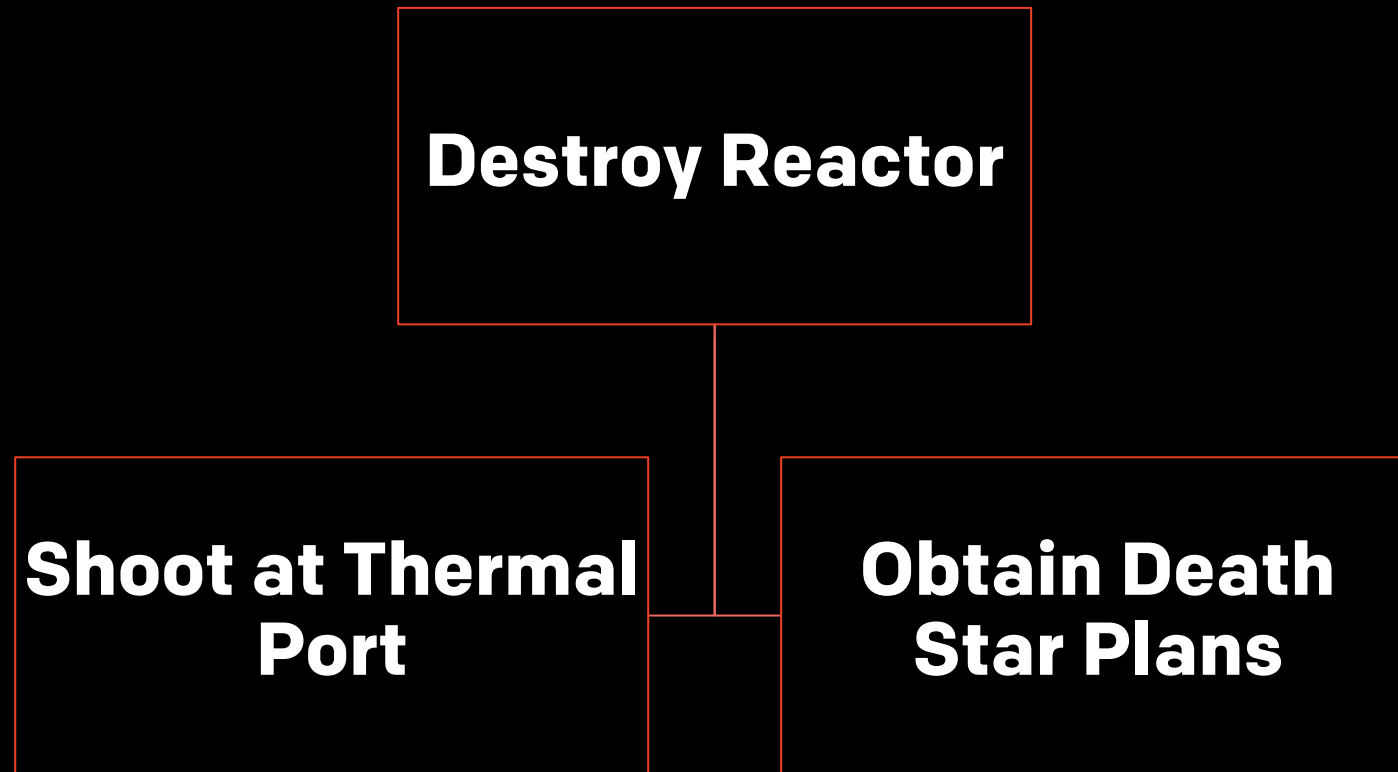
THREAT MODELING: **ATTACK TREES**



THREAT MODELING: **ATTACK TREES**



THREAT MODELING: **ATTACK TREES**



**Death Star out
of Action**

**Disable Death
Star**

**Destroy Death
Star**

**System
Failure**

**Mechanical
Failure**

**Military
Attack**

**Destroy
Reactor**

**Compromise
IT systems**

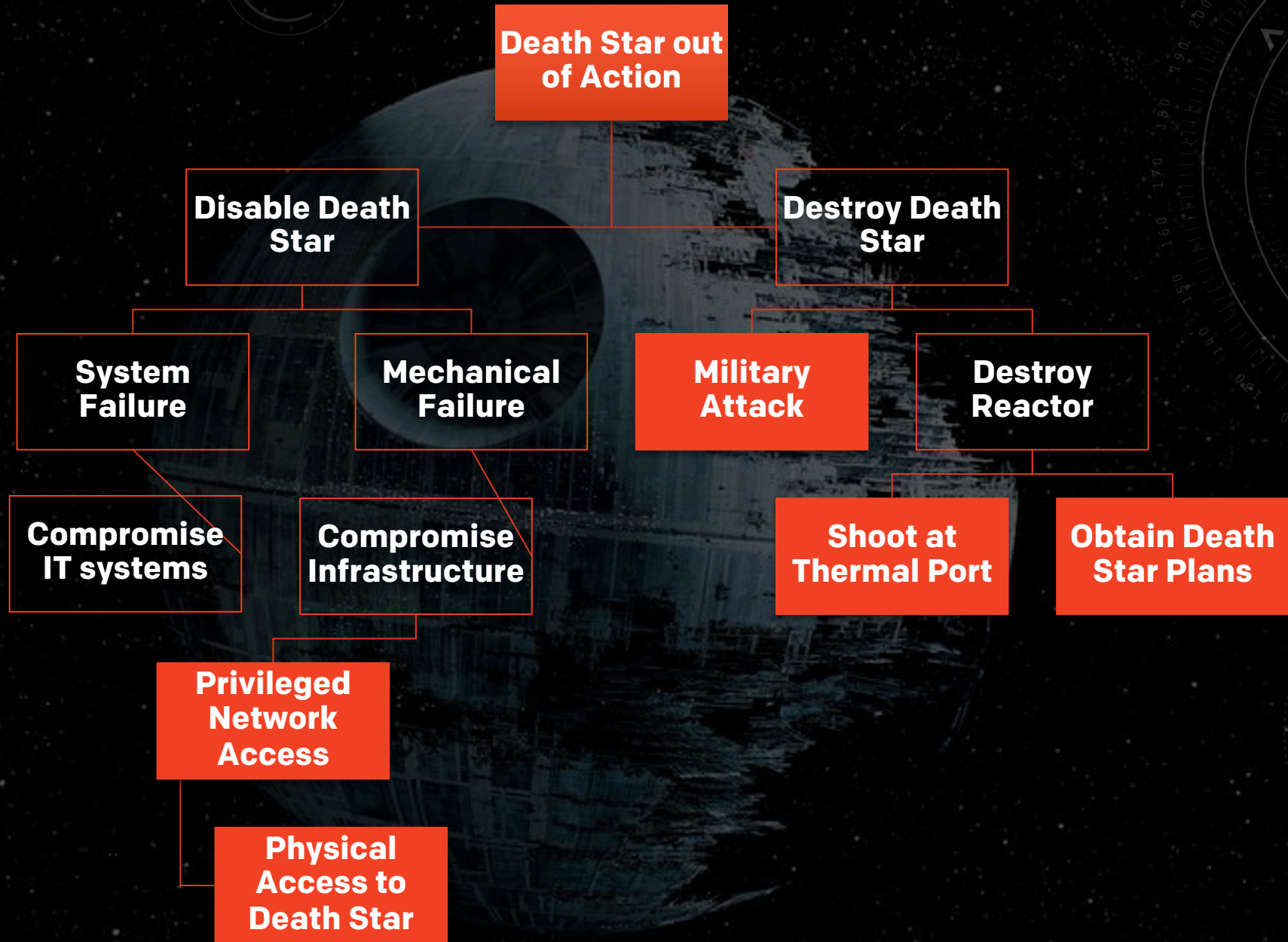
**Compromise
Infrastructure**

**Shoot at
Thermal Port**

**Obtain Death
Star Plans**

**Privileged
Network
Access**

**Physical
Access to
Death Star**



The background features a dark blue gradient with a subtle pattern of white dots. On the left side, there are several overlapping circular elements. A prominent one is a large circle with a scale around its perimeter, marked with numbers from 140 to 260 in increments of 10. Other circles are smaller and some have dashed lines or arrows, suggesting a technical or scientific theme.

MITIGATION STRATEGIES

MINIMIZE THE RISKS

PRIVILEGED ACCESS TO NETWORK

Impact: **CRITICAL**

Likelihood: **MEDIUM**

Mitigation strategies

Better authentication / authorization

Defense in Depth

Pen Testing the Systems

...



Likelihood: **LOW**

MILITARY ATTACK

Impact: **CRITICAL**

Likelihood: **HIGH**

Mitigation strategies

Incident Response procedures

Star Destroyers “On Call”

Monitor Rebellion Activities

...



ALERT

Sir, are you absolutely sure? It does mean changing the bulb.

MILITARY ATTACK

Impact: **CRITICAL**

Likelihood: **HIGH**

Mitigation strategies

Incident Response procedures

Star Destroyers "On Call"

Monitor Rebellion Activities

...



Impact: **HIGH**

Likelihood: **MEDIUM**

SHOOT AT THERMAL PORT

Impact: **CRITICAL**

Likelihood: **LOW**

Mitigation strategies

Move Death Star plans to Imperial Security complex.



JOB WELL DONE!

LET'S DEPLOY THAT THING



The background features a dark blue gradient with a subtle pattern of white dots. On the left side, there are several overlapping circular elements. A prominent one is a large circle with a scale around its perimeter, marked with numbers from 140 to 260 in increments of 10. Other circles are partially visible, some with dashed lines and arrows, suggesting a technical or scientific theme.

FORENSIC ANALYSIS

WHAT HAPPENED?



NEW PERSONA?

Another Jedi in the story!

Support from a Bounty Hunter!

Princess Leia's brother!

Son of a.. your boss!





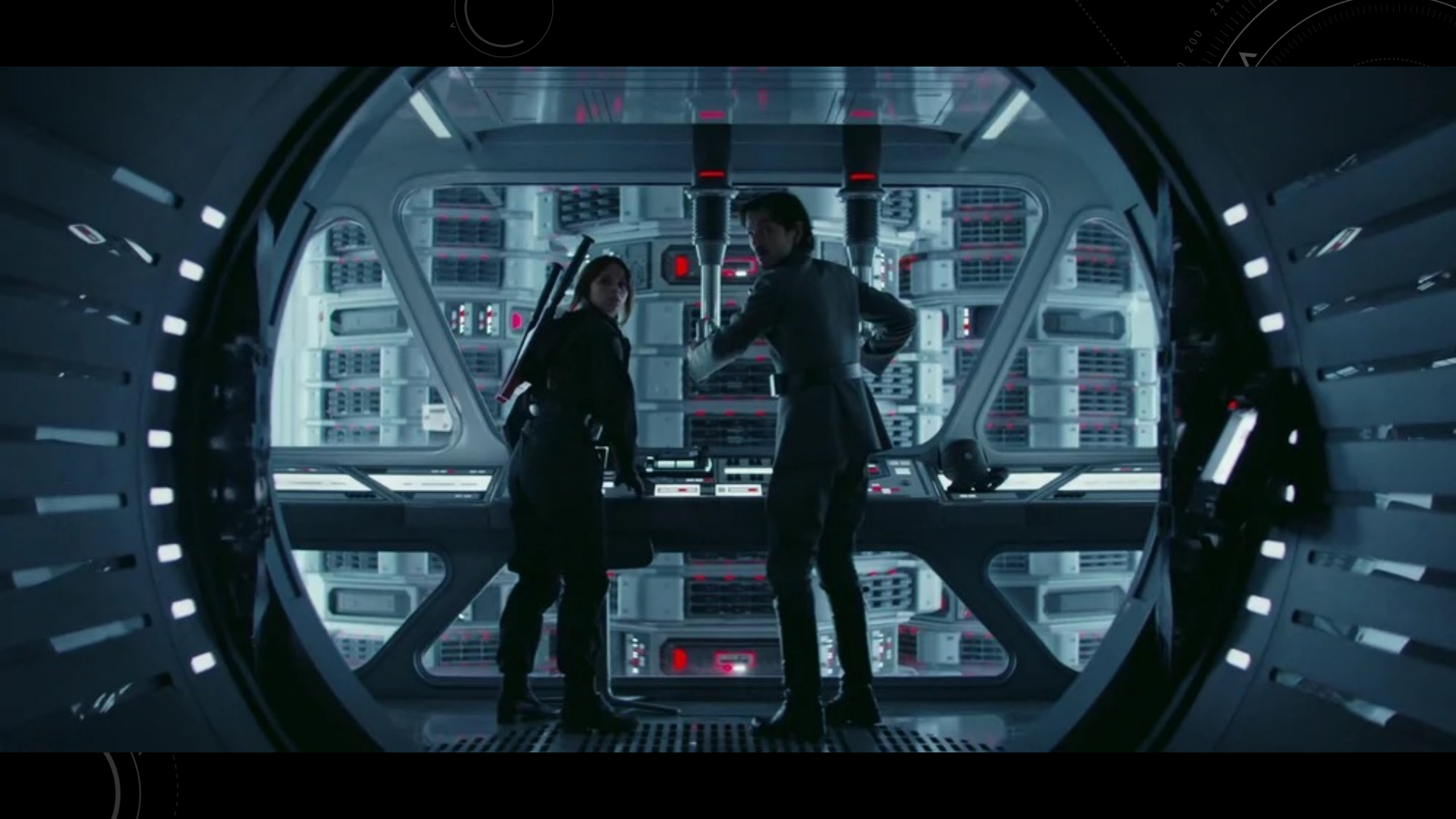
DESIGN FLAWS

Insufficient design reviews!

A vital flaw in design

Introduced by an insider





The background features a dark blue gradient with a starry space pattern. On the left side, there are several technical diagrams, including a large circular scale with numerical markings from 140 to 260 and various circular arrows and lines. The main text is centered on the right side.

THREAT MODEL EARLY AND OFTEN

LIST OF STANDARDIZED COMPONENTS

The background is a dark blue gradient with a starry texture. On the left side, there are several overlapping circular elements. One prominent feature is a large circular scale with tick marks and numbers ranging from 140 to 260. Other circles contain curved lines and arrows, suggesting motion or data flow.

SECURITY THROUGH OBSCURITY

IS A TERRIBLE IDEA

THREAT MODELING EXAMPLES

- Rob a bank?
- Steal a car?
- Short-n-easy examples
 - Threat modeling of movies/heroes
 - Batman or Harry Potter
 - Physical security
- Criminal Gang
 - Other criminal gangs
 - Police raids
- Tower defense games



A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



METHODOLOGIES

- Attack Trees
- STRIDE
- PASTA
- CVSS
- Security Cards

- ... and plenty of others!

THREAT MODELING: STRIDE

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Services

Elevation of Privileges

S T R I D E



SPOOFING

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.



TAMPERING

Tampering can refer to many forms of sabotage but the term is often used to mean intentional modification of products in a way that would make them harmful to the consumer.




REPUDIATION

In digital security, non-repudiation means a service that provides proof of the integrity and origin of data, or an authentication that can be said to be genuine with high confidence.




INFO DISCLOSURE

Information disclosure is the unwanted dissemination of data, technology, or privacy. legal and political issues surrounding them. It is a violation of data privacy[2] or data protection. The challenge of data privacy is to use data 



DENIAL OF SERVICE

A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the 



ELEVATION OF PRIVILEGE

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

THREAT MODELING: STRIDE

- Provides a good methodology
- Various areas people could start with
- Tools available!
 - Microsoft Threat Modeling tool
 - OWASP Threat Dragon
- Adopted by Microsoft, Github, ...

SECRETS IN A GIT REPOSITORY

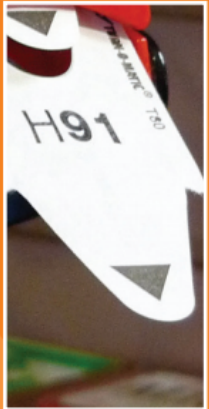
Category	Threat	Description	Mitigation
Information Disclosure	Credentials Theft	An unauthorized person could get to the credentials, which could be used to alter potentially sensitive/vital information.	Least privilege principle; dynamic, generated credentials (if possible, with time limited validity).
Repudiation	Performing operations on someone else's behalf	Sharing secrets makes non-repudiation impossible – there's always a space for justified doubt about who could actually be the initiator of a potentially harmful actions.	Least privilege, no shared secrets, strong authentication, good audit logs.
Tampering	Rewriting a crucial secret.	When a write permission on the secrets is also shared by a group of individuals, it's possible to harm services by rewriting the stored secret (either deliberately or by accident).	Secrets versioning, strict roles and least privilege.

THREAT MODELING: SECURITY CARDS

- Gamification of threat modeling!
- 4 different categories of cards (“dimensions”)
 - Human Impact
 - Adversary’s Motivation
 - Adversary’s Resources
 - Adversary’s Methods
- Interactive

Access or Convenience Adversary's Motivations

How might the adversary use or abuse your system for the purpose of convenience or to gain access to a resource? What kind of individual or group might target your system because it is more convenient than some alternative, or because it is the only way to achieve their goal?



Example Related Concepts

Example Targets: appointment-based online enrollment systems · sales of limited tickets · personal electronics with restricted permissions

Example Actions: modify personal electronics · bypass company filtering to access personal email · access a protected wireless network

Physical Attack Adversary's Methods

How might the adversary gain or take advantage of physical access to a system component? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?



Example Related Concepts

Example Attacks: wiretapping · tampering with hardware · installing software

Example Outcomes: install keyloggers · destroy equipment · access confidential files

Personal Data Human Impact

What kinds of personal data does (or could) your system collect, store, or share? How might current or future compromise, corruption, or unavailability of this data cause harm?

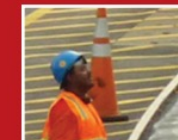


Example Related Concepts

Example Data: medical records · embarrassing

Inside Knowledge Adversary's Resources

What kinds of inside knowledge might the adversary have (or gain) access to? How might inside knowledge allow the adversary to execute new or more effective attacks on your system?



Example Related Concepts

Example Knowledge: design documents · system usage


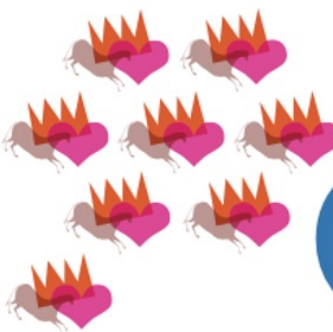
THREAT MODELING: SECURITY CARDS

- Custom cards possible
- Extensions:
 - Elevation of Privilege cards (Microsoft)
 - Elevation of Privacy cards (F-Secure)
 - Cornucopia (OWASP)

EOP VS CORNUCOPIA

8 Elevation of Privilege

An attacker can enter data that is checked while still under their control and used later on the other side of a trust boundary



Q Denial of Service

An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10:1



CORNUCOPIA

10

Xavier can circumvent the application's controls because code frameworks, libraries and components contain malicious code or vulnerabilities (e.g. in-house, commercial off the shelf, outsourced, open source, externally-located)

OWASP SCP
57, 151, 152, 204, 212
OWASP ASVS
2.15, 3.13, 4.16, 5.9, 6.10, 7.10, 8.12, 13.1
OWASP AppSensor
-
CAPEC
68, 438, 439, 442
SAFECode
15
OWASP Cornucopia Ecommerce Website Edition v1.01

CRYPTOGRAPHY

J

Justin can read credentials for accessing internal or external resources, services and others systems because they are stored in an unencrypted format, or saved in the source code

OWASP SCP
35, 171, 172
OWASP ASVS
2.14, 12.1
OWASP AppSensor
-
CAPEC
116
SAFECode
21, 29
OWASP Cornucopia Ecommerce Website Edition v1.01

The background features a dark blue gradient with a starry texture. On the left side, there are several overlapping circular elements. A prominent one is a large circle with a scale from 140 to 260 in increments of 10. Other circles are smaller and some have dashed lines or arrows, suggesting a technical or scientific theme.

PRACTICAL THREAT MODELING

THERE'S NOTHING MORE PRACTICAL
THAN A GOOD THEORY!



SECURITY
STARTS
WITH U!

HOW TO THREAT MODEL EFFICIENTLY

- Security engineers threat model every story
 - Delays!
- Software engineers threat model every story
 - Too much time spent on reviews.
 - Teaming with Security
- Software engineers assess risk on every story
 - A questionnaire supporting their decisions
 - “When a software engineer feels they must choose between doing security and doing engineering, you have lost the battle.”

SECURITY QUESTIONNAIRE SAMPLE

- Does it deal with customer data?
- Does it communicate over network?
- Is this a critical component?
- Does your component require authentication?
- Does your project introduce or utilize a third-party library?
- Are you implementing or modifying any APIs?
- Does your project utilize a database via SQL?
- ...



HOW TO THREAT MODEL EFFICIENTLY

- What works
 - Shifting left, like a boss
 - Re-usable reviewed and assessed components
 - Proper threat modeling and risk assessment for the critical ones
 - Questionnaire to support the activity
 - Security impact criteria
 - Security Engineers teaming up with software engineers and developers
- Mutual respect and understanding

RISK MITIGATION ACTIONS

- Remove the threat
 - e.g. by removing the respective functionality
- Mitigate
 - e.g. through standard practices like encryption
 - “What cannot be mitigated could perhaps be monitored.”
- Accept
 - be careful about “accepting” risk for your customers
- Transfer
 - e.g. via license agreements or terms of service



thaddeus e. grugq

@thegrugq

Your threat model is not my threat model.



**YOUR THREAT
MODEL IS NOT MY
THREAT MODEL**

9:42 AM · May 15, 2017 · Tweetbot for iOS

SERIOUS LIFE QUESTIONS

- What is the purpose of life?
- Shall I patch the vulnerability on my internal server?
- Can we keep the default admin password?
- What is the air-speed velocity of an unladen swallow?
- Can we keep the thermal exhaust port as it is now?
- What is the difference between living and existing?
- Is 42 a perfect number?
- Could sharks be a serious threat to my house?

Depends on your threat model.

The background is a dark blue gradient with several faint, semi-transparent question marks scattered across it. On the right side, there are technical-style graphics including circular gauges with numerical scales (e.g., 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200) and dashed lines with arrows, suggesting a data or engineering theme.

QUESTIONS?

NOTES

- Agile Threat Modeling
 - <https://martinfowler.com/articles/agile-threat-modelling.html>
- AppSec at scale
 - <https://r2c.dev/blog/2021/appsec-development-keeping-it-all-together-at-scale/?s=09>