building castles
a metaphorical journey through time and space

@liamosaur

building castles
a metaphorical journey through lime and space

@liamosaur

~1986

~1990

ASSURANCE

2017

how do we make IT systems secure?

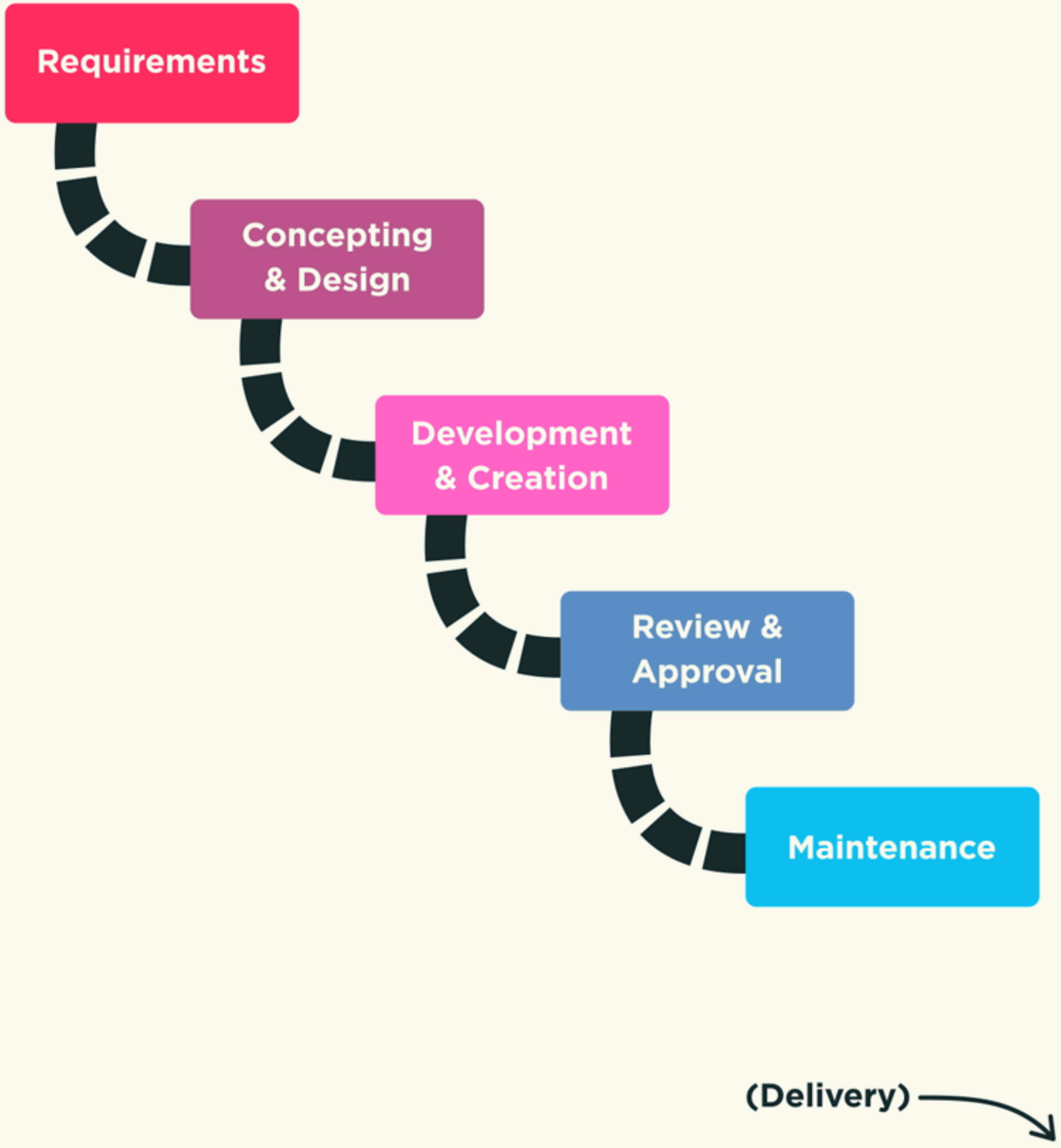
security by the book

- THREAT MODELLING: WHAT are we protecting from WHO, and what VECTORS might be involved?
- RISK ASSESSMENT: PRIORITISE and EVALUATE threats
- SECURITY CONTROLS: HOW we are protecting it

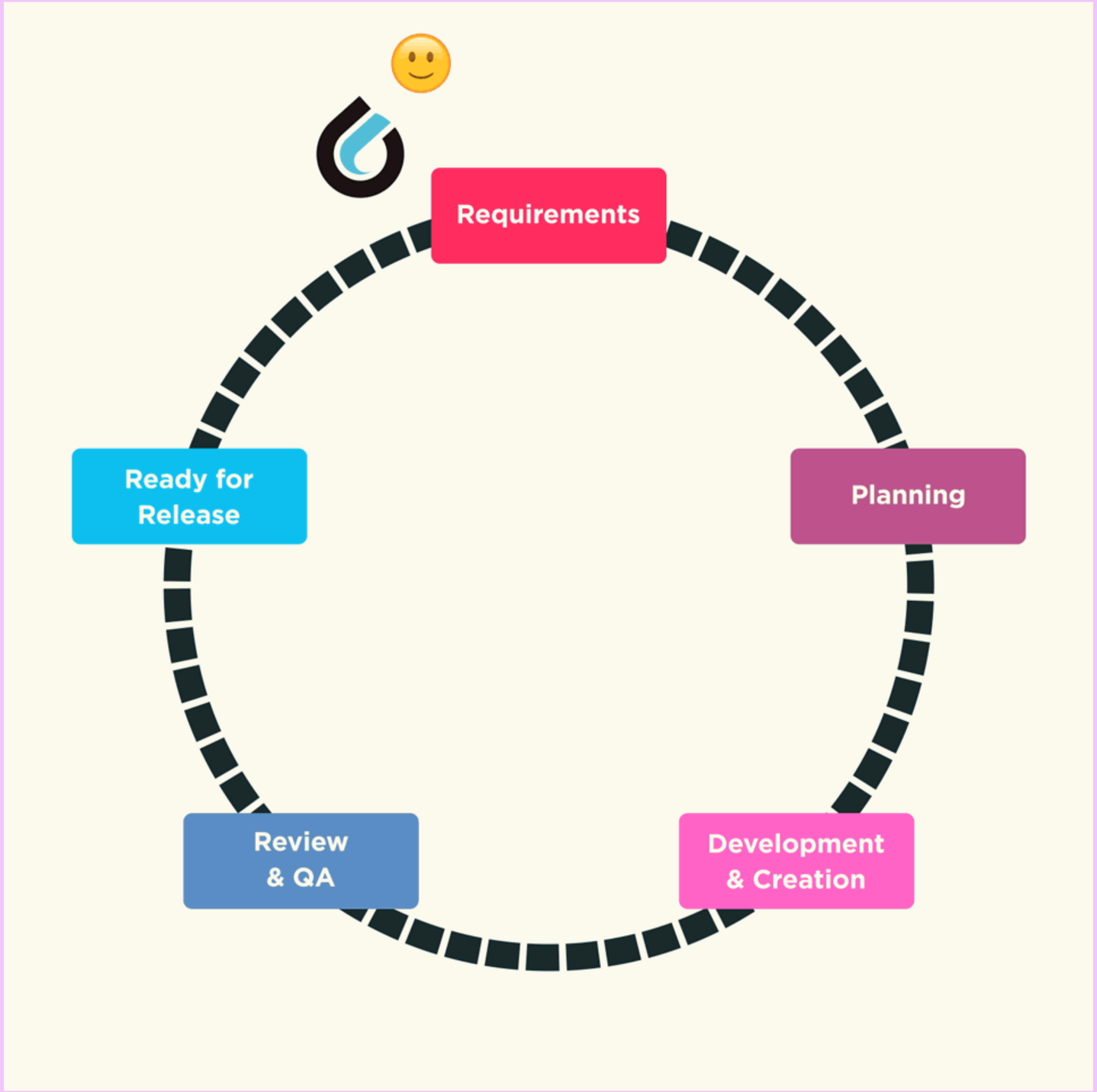
security by the book

threat modelling ➡️ risk assessment ➡️ security controls

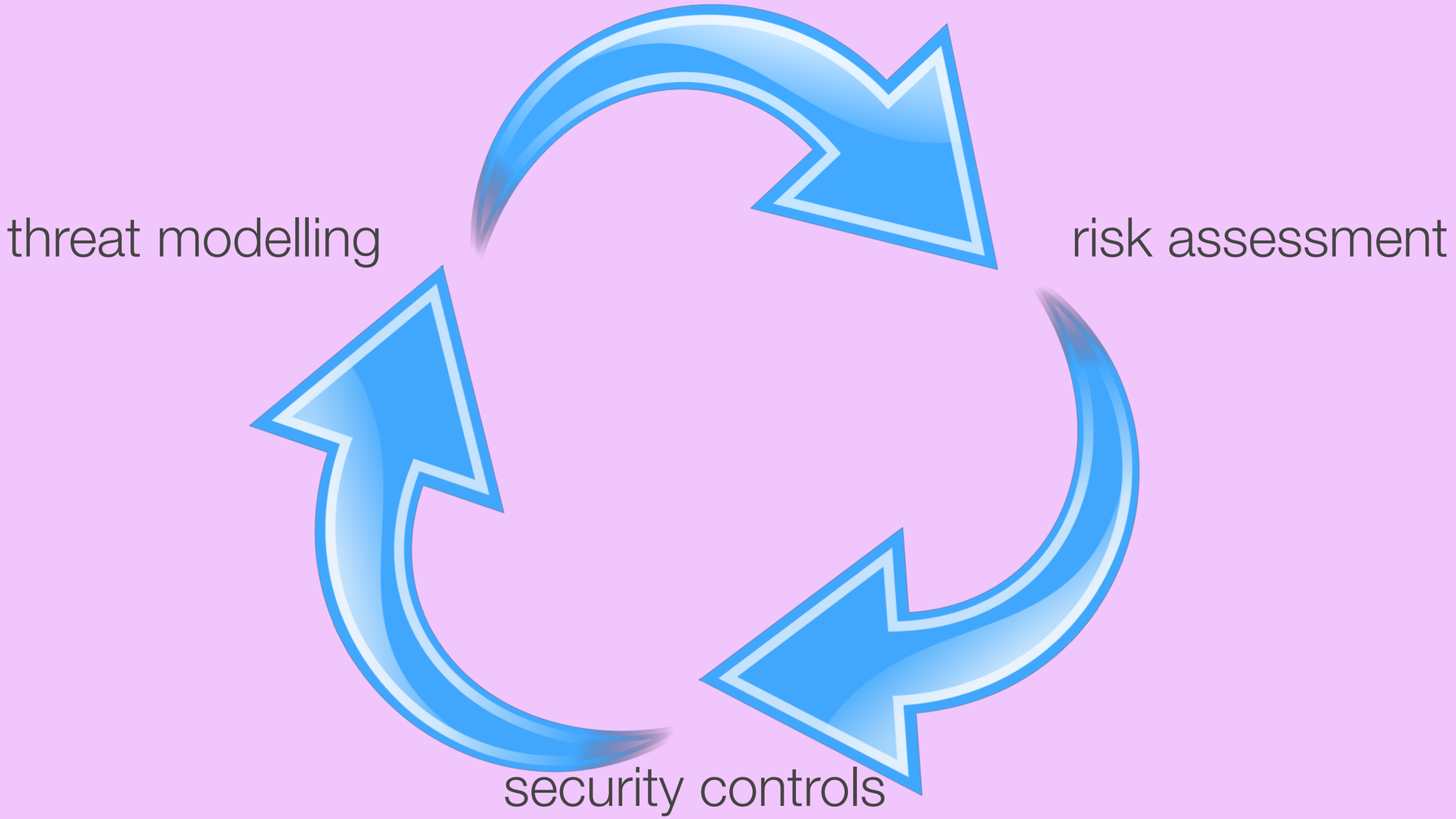

gifbin.com


Requirements
Concepting & Design
Development & Creation
Review & Approval
Maintenance
(Delivery)

threat modelling ➡️ risk assessment ➡️ security controls


Requirements
Planning
Development & Creation
Review & QA
Ready for Release

agile security

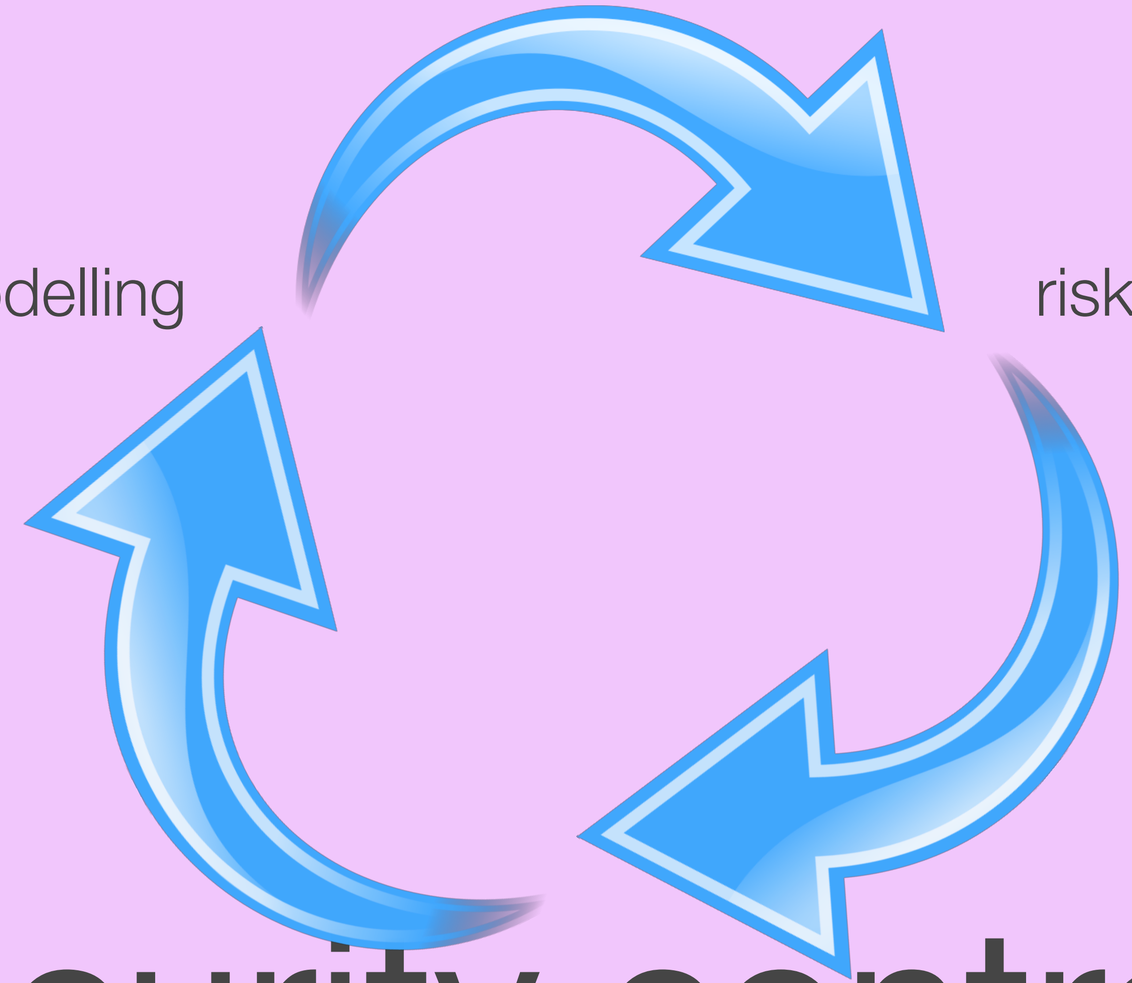


the defining characteristic of agile is diagrams that contain a loop

don't @ me

agile security

threat modelling



risk assessment

security controls

ASSURANCE

WARNING:
METAPHORS AHEAD

"Essentially, all models are wrong, but some are useful"
- George Box


COME


LIME
CRISIS

you have unlocked class:

engineer

you have unlocked TIER I BUILDING:

iron-age ringfort

you have unlocked TIER I BUILDING:

iron-age ringfort

- cheap
- achievable
- definitely better than nothing

ASSURANCE

control attribute:

SIMPLE ☑️

ASSURANCE

adversary unlocks class:

attacker

adversary unlocks class:

attacker

- burn the walls down
- smash the walls open with axes / rams
- climb over

control attributes:

SIMPLE ☑️

STRONG ❌

ASSURANCE

you have unlocked TIER II BUILDING:

iron-age ringfort

you have unlocked TIER II BUILDING:

iron-age ringfort

- can't be burnt down
- harder to break
- harder to climb over

control attributes:

SIMPLE ☑

STRONG ☑


www.reiq.ws

adversary unlocks skill:

determined attacker

"walls seem like a good control, lets build more walls!"

"walls seem like a good control, lets build more walls!"

- we already know how to make a second wall
- if the outer wall fails, the next wall becomes the line of defence

Tweet

l0ss
@mikeloss

TFW you have a massive breakthrough and find yourself face to face with another massive wall.

7:17 pm · 02 Nov. 18

control attributes:

SIMPLE ✅

STRONG ✅

control interactions:

FAIL INDEPENDENTLY ✅

ASSURANCE

fail independently?

wall + gate ?

FAIL INDEPENDENTLY ✗

adversary unlocks skill:

intelligent attacker

"hey, remember the technique that we used to breach the outer defences?
- lets use it again on the identical inner defences"

control attributes:

SIMPLE ✅

STRONG ✅

control interactions:

FAIL INDEPENDENTLY ✅

DIVERSE ❌

you have unlocked TIER I BUILDING:

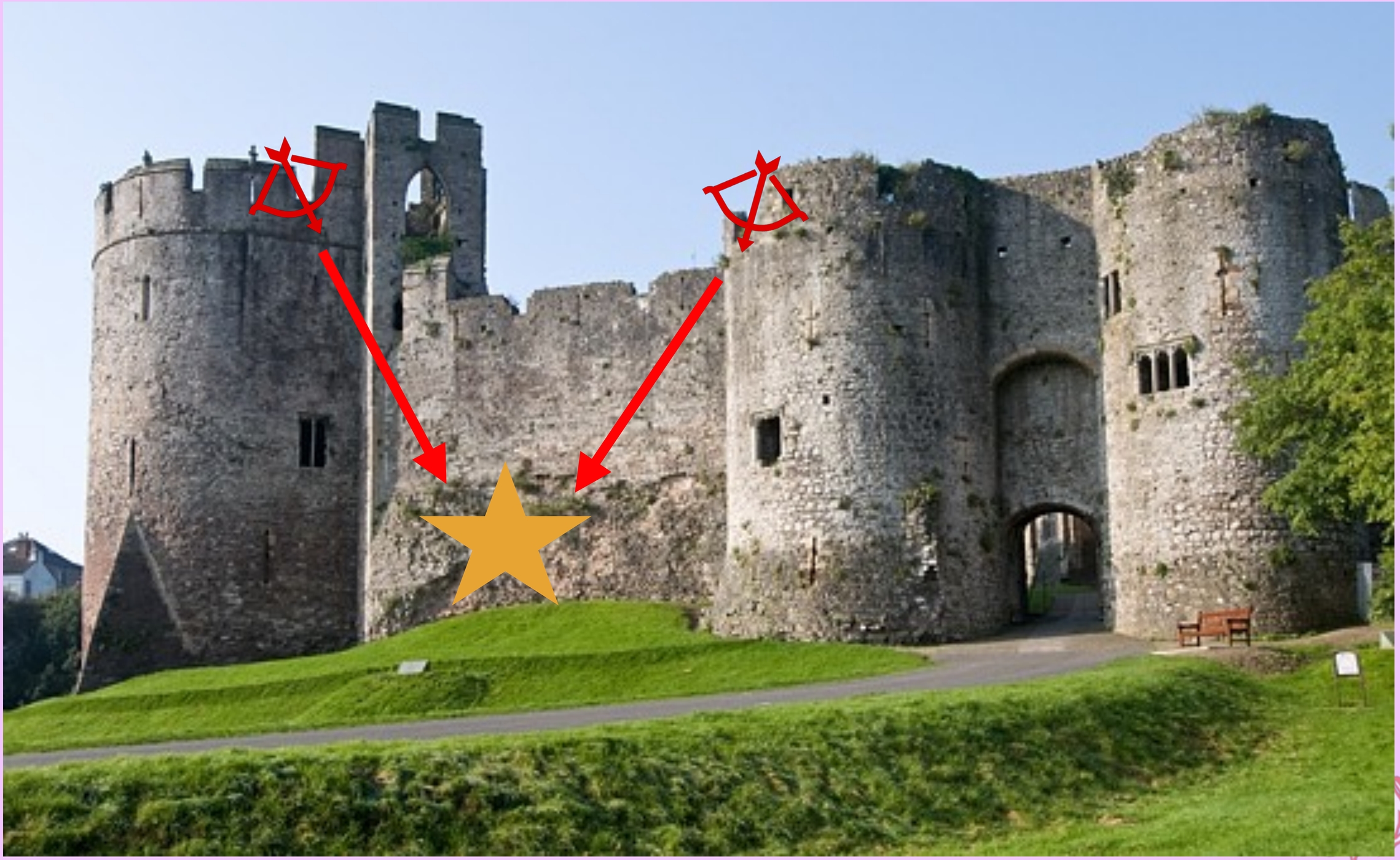
medieval castle

you have unlocked TIER I BUILDING:

medieval castle

adversary unlocks skill:

detect weaknesses



the walls don't just protect what's **inside** the walls, they also protect **themselves**

control attributes:

SIMPLE ☑

STRONG ☑

SELF-DEFENDING ☑

ASSURANCE

adversary unlocks skill:

sustained attack

you have unlocked TIER II BUILDING:

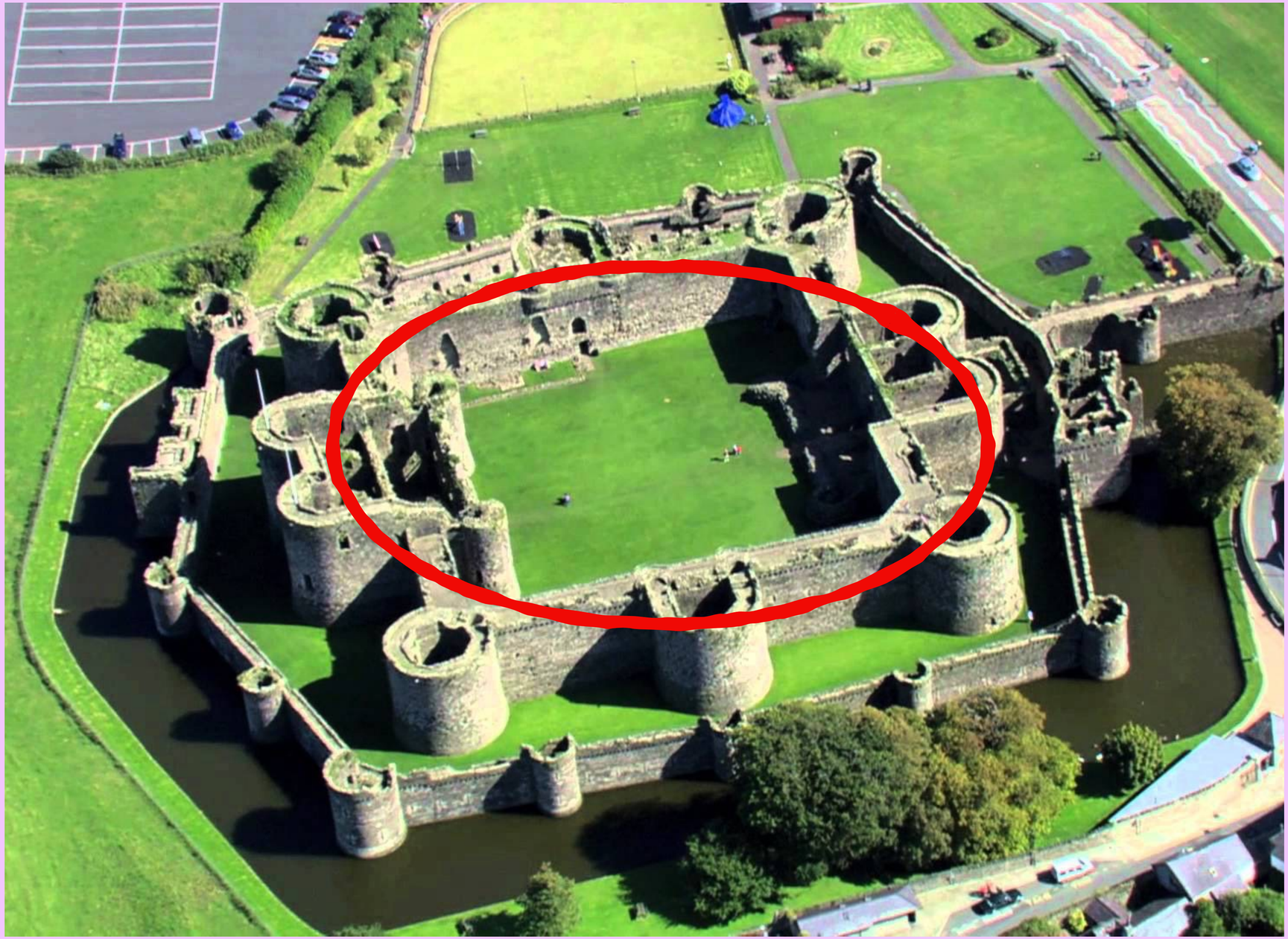
medieval castle

you have unlocked TIER II BUILDING:

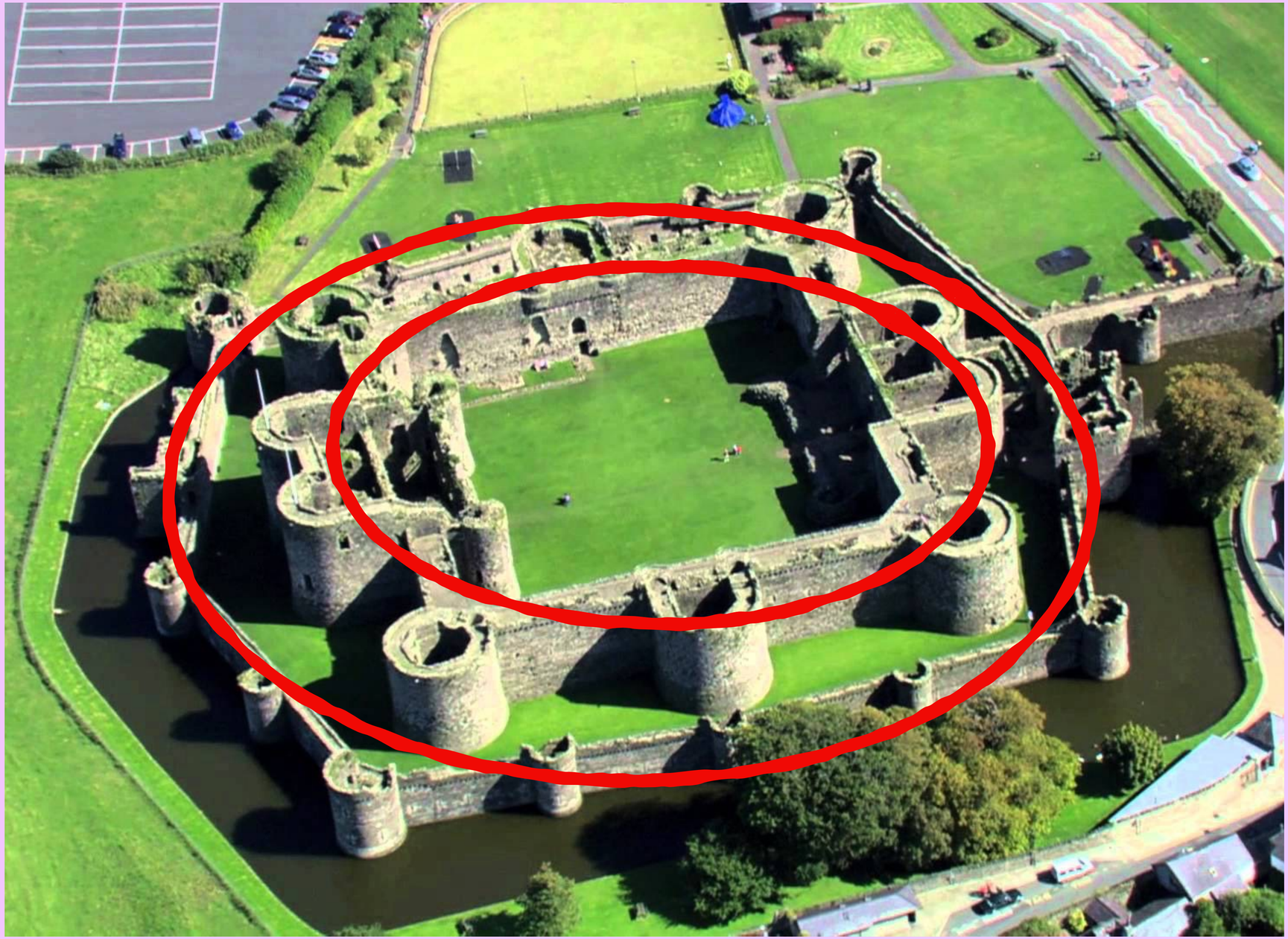
medieval castle

STRONG ✅

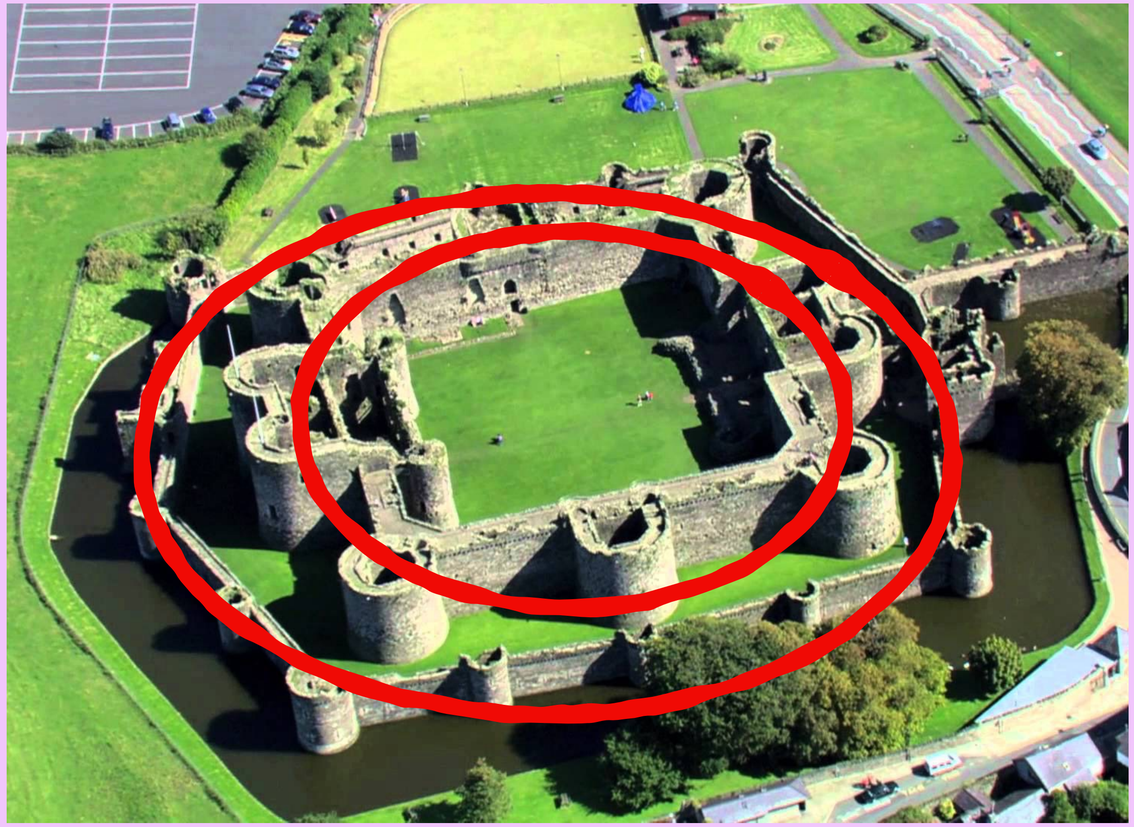
ASSURANCE



ASSURANCE

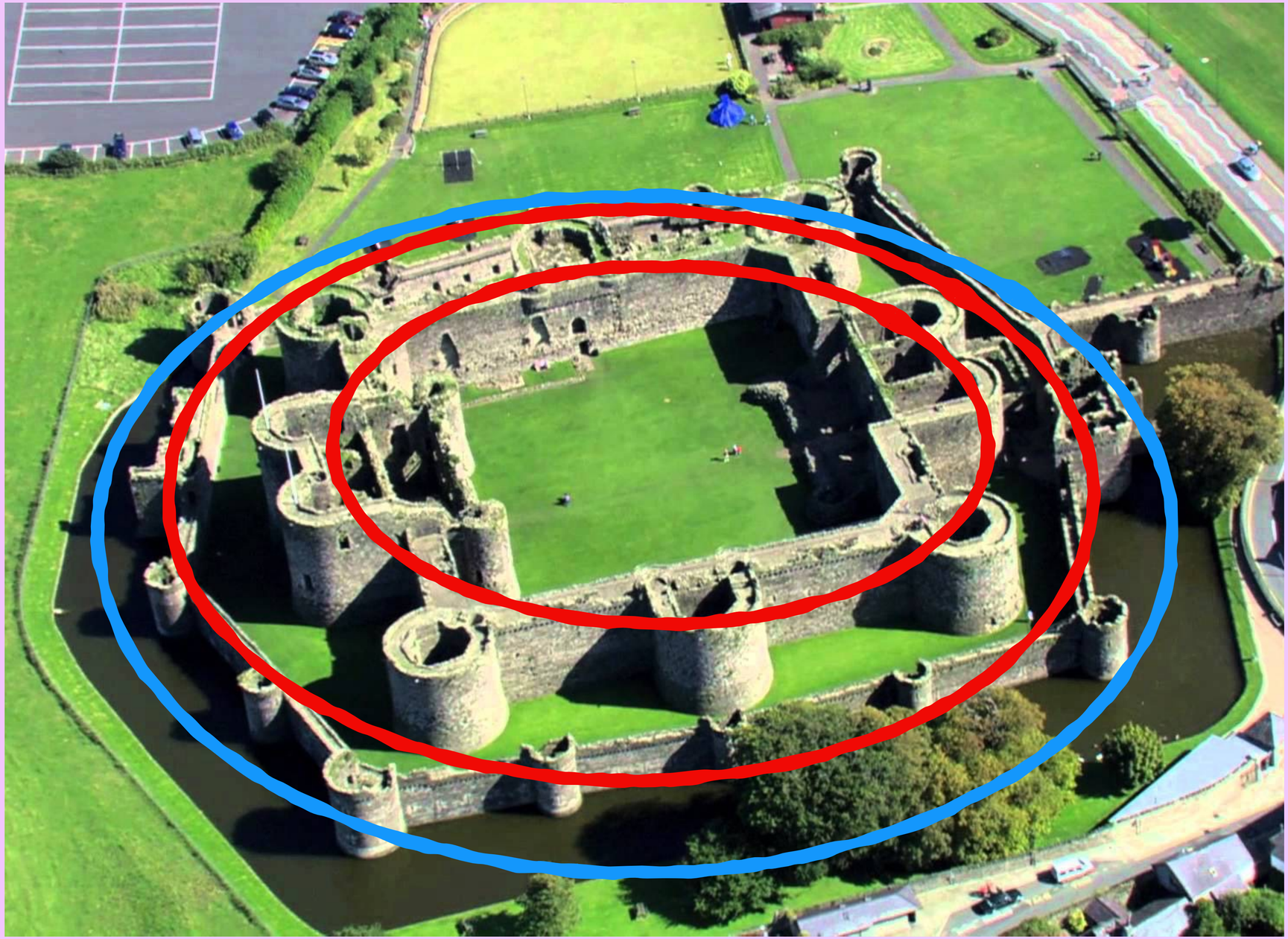


ASSURANCE



INDEPENDENT ☑️

ASSURANCE



ASSURANCE

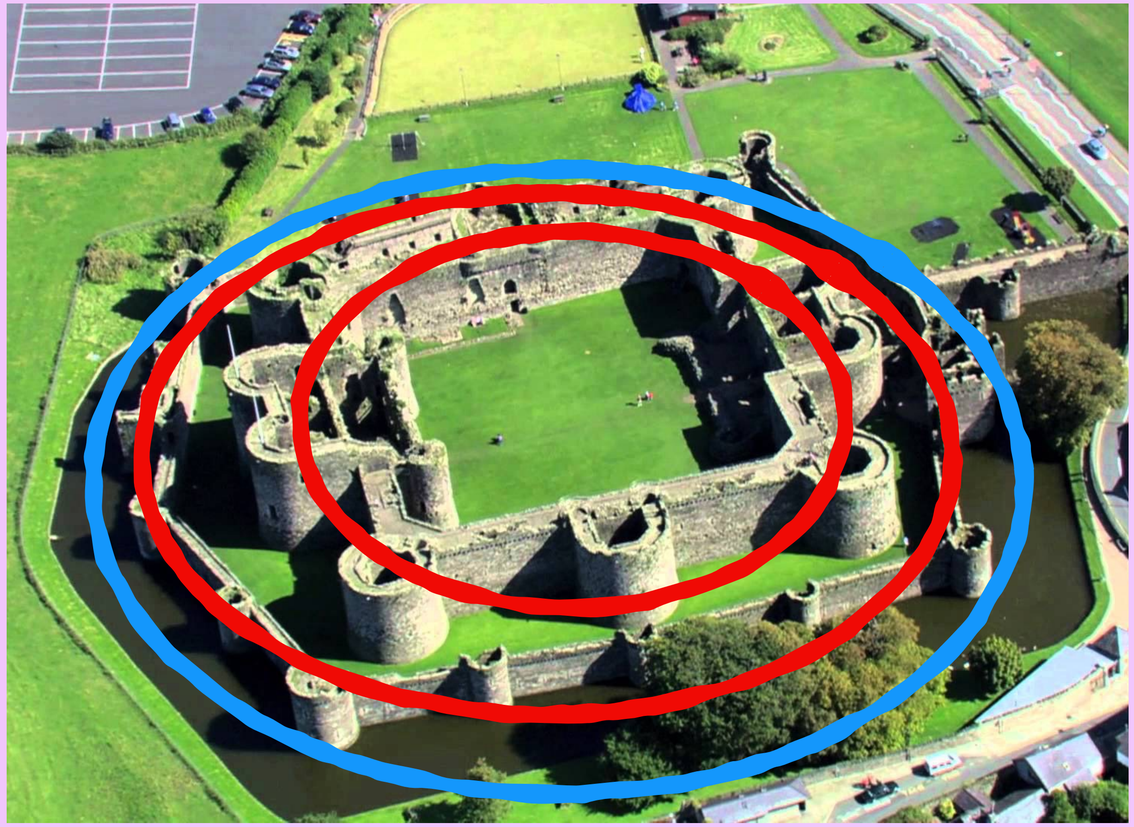
control attributes:

SIMPLE ☑

STRONG ☑

control interactions:

DIVERSE ❌

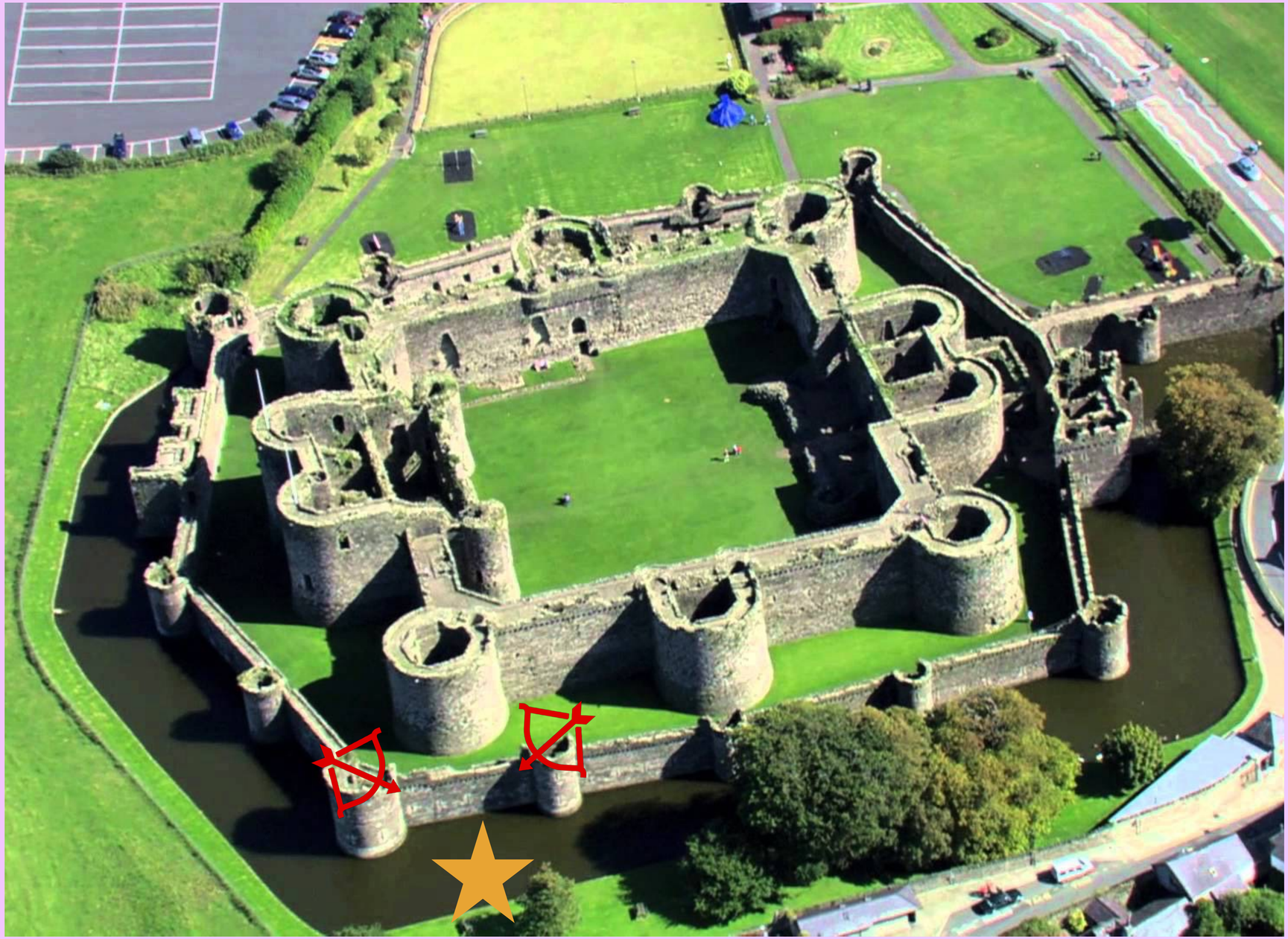


DIVERSE ☑️

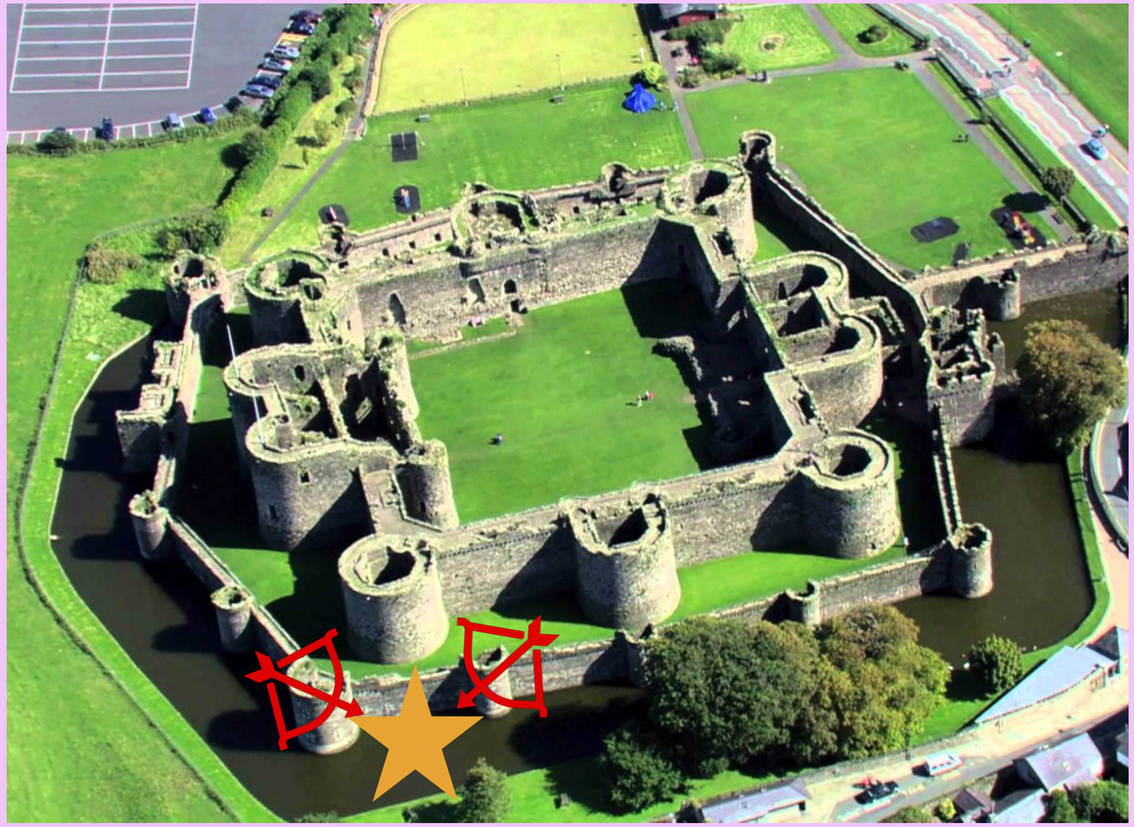
ASSURANCE

security controls are like people

diversity gives them strength

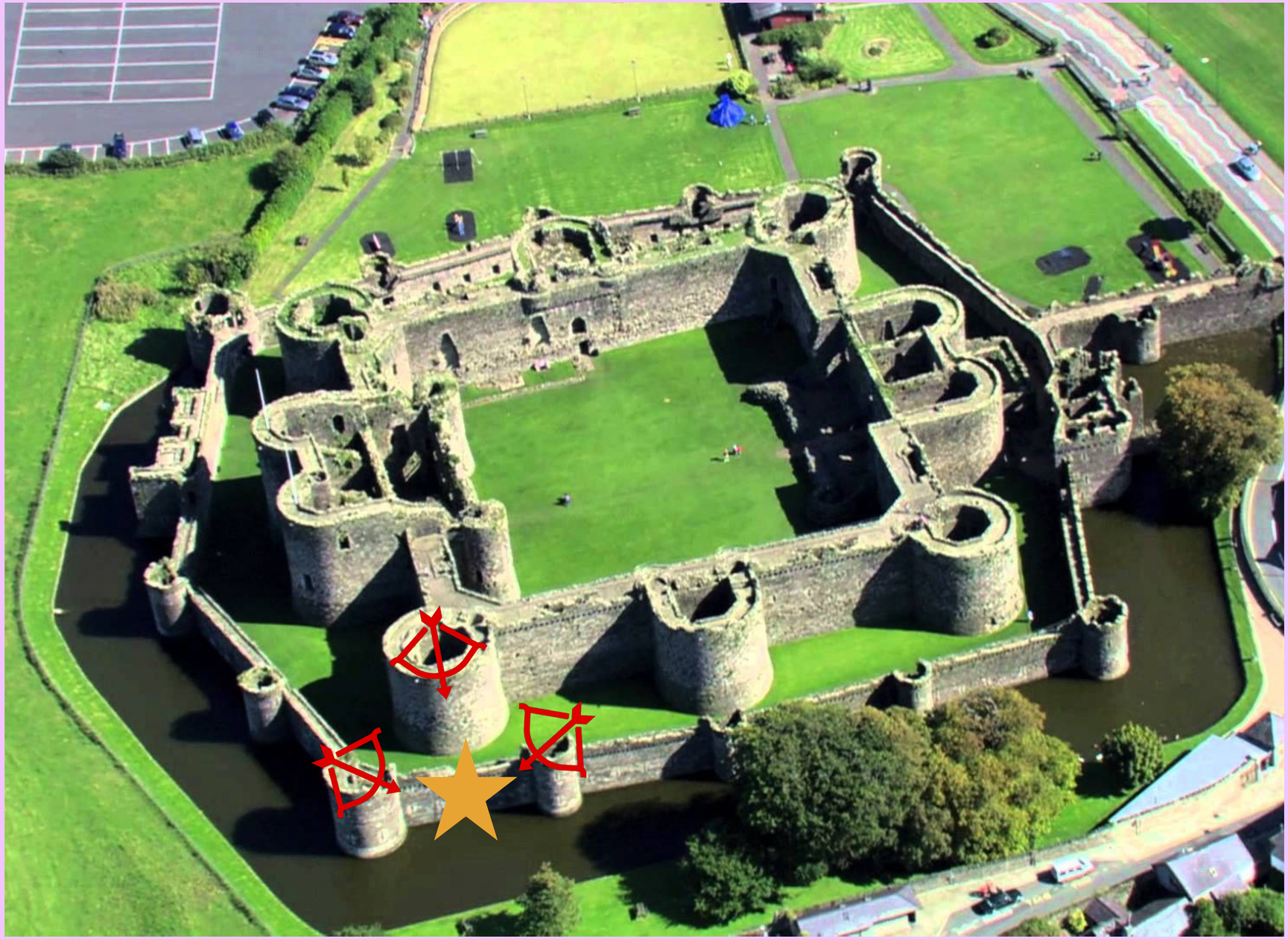


ASSURANCE

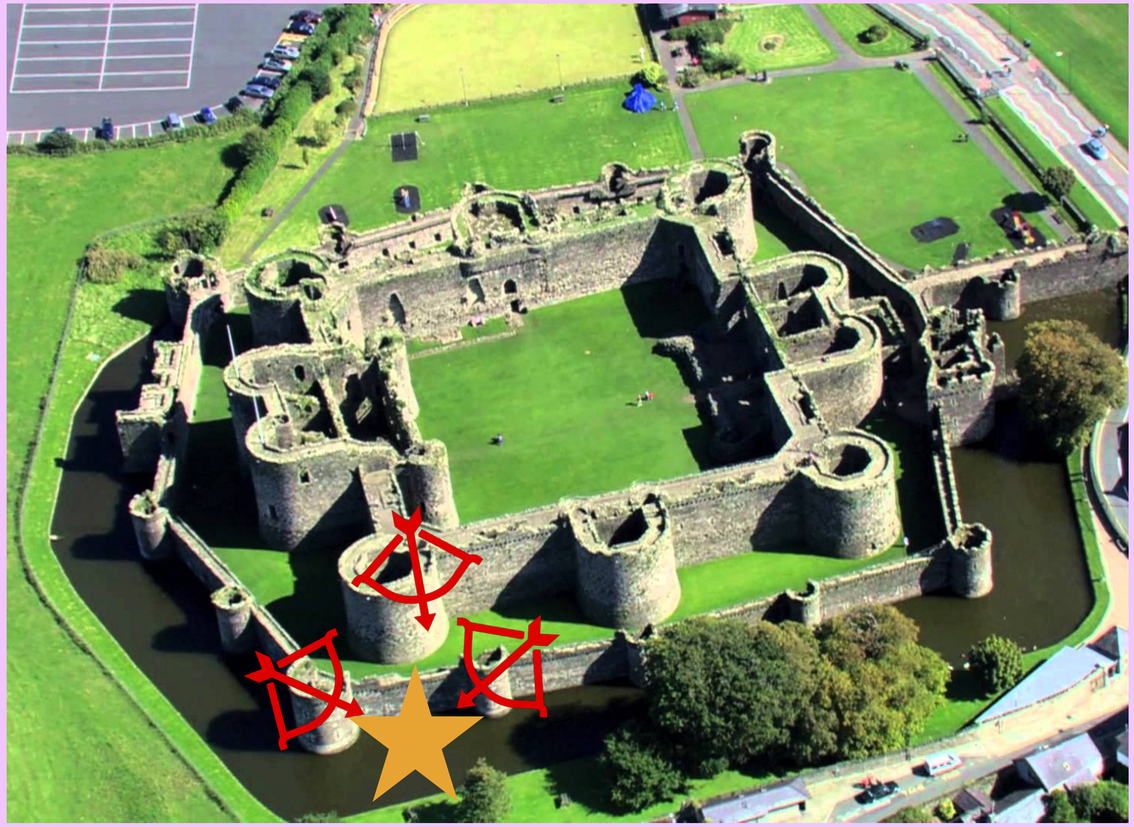


SELF-DEFENDING ☑️

ASSURANCE



ASSURANCE



MUTUALLY SUPPORTING ☑️

security controls are like people

mutual support makes them resilient

control attributes:

STRONG ✅

SELF-DEFENDING ✅

control interactions:

FAIL INDEPENDENTLY ✅

DIVERSE ✅

MUTUALLY SUPPORTING ✅

control attributes:

SIMPLE ❌

STRONG ✅

SELF-DEFENDING ✅

control interactions:

FAIL INDEPENDENTLY ✅

DIVERSE ✅

MUTUALLY SUPPORTING ✅

ASSURANCE

summary: desirable control attributes

INDIVIDUAL CONTROL		MULTIPLE CONTROLS	
SIMPLE	✅	FAIL INDEPENDENTLY	✅
STRONG	✅	DIVERSE	✅
SELF-DEFENDING	✅	MUTUALLY SUPPORTING	✅

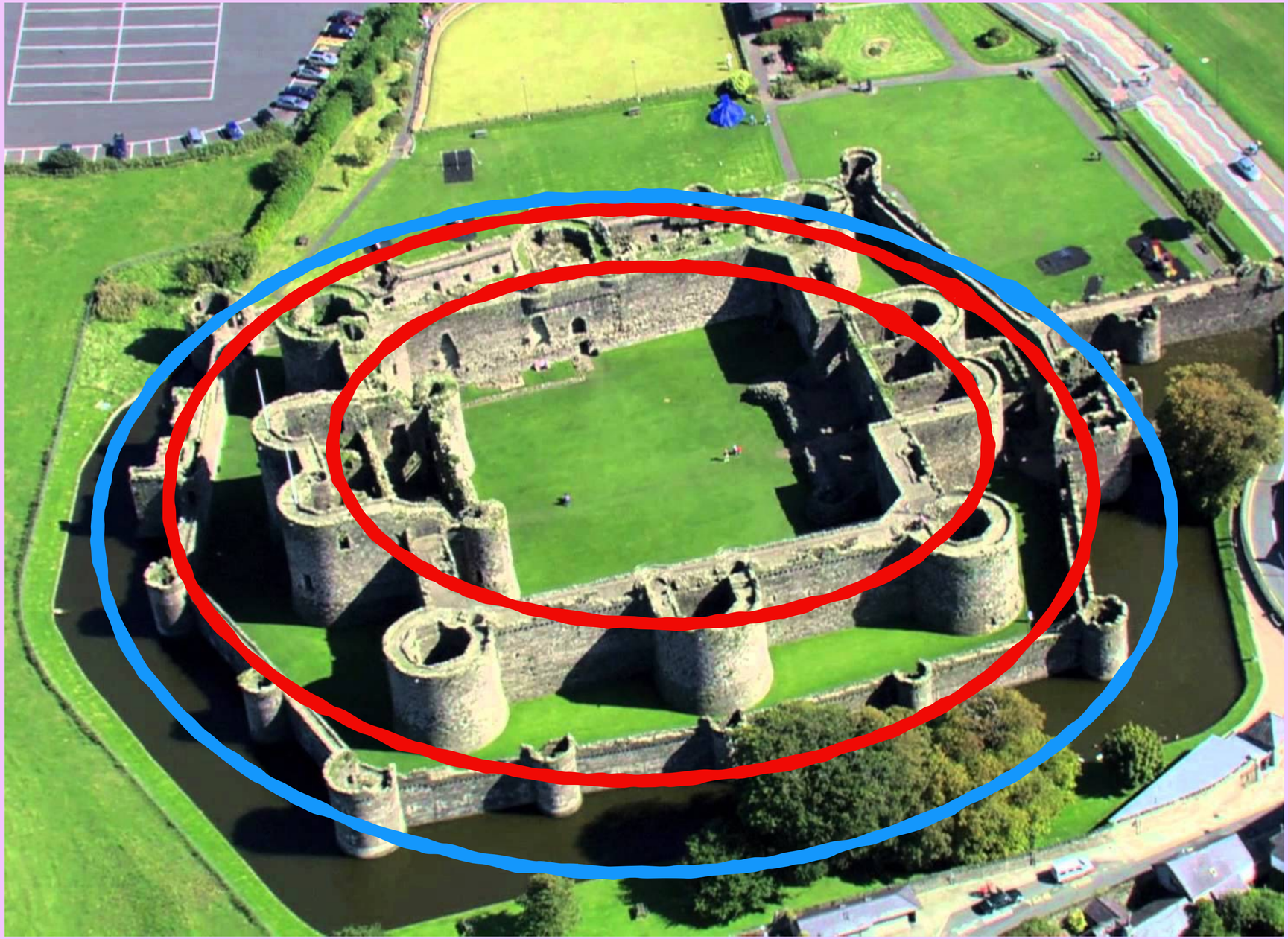
other important design principles

reduce attack surface

reduce attack surface

principle of least privilege

- segmentation
- separation of duties



ASSURANCE

principle of least privilege

principle of least privilege

applied control modelling

- scenario: Internet-facing website
- *BUT* it contains sensitive data
- we only want certain people to be able to access sensitive data

applied control modelling

- control: require a password to access sensitive content

applied control modelling

- control: require a password to access sensitive content

SIMPLE ☑️

applied control modelling

- control: require a password to access sensitive content

SIMPLE ☑️

STRONG ❓

attacks on password based access control

attacks on password based access control

- guess the password
- access a stored password
- intercept a password

applied control modelling

- control: require a password to access sensitive content

SIMPLE ☑️

STRONG ❌

applied control modelling

- control: require a password to access sensitive content
  - **enforce password complexity policy, use TLS, strong hashes**

SIMPLE ☑️
STRONG ☑️

applied control modelling

- control: require a password to access sensitive content
  - enforce password complexity policy, use TLS, strong hashes

SIMPLE ☑️

STRONG ☑️

SELF-DEFENDING ❓

applied control modelling

- control: require a password to access sensitive content
  - enforce password complexity policy, use TLS, strong hashes

SIMPLE ☑️
STRONG ☑️
SELF-DEFENDING ❌

applied control modelling

- control: require a password to access sensitive content
  - enforce password complexity policy, use TLS, strong hashes
  - **require a CAPTCHA**

SIMPLE ☑️

STRONG ☑️

SELF-DEFENDING ☑️

applied control modelling

- control I: ☑️☑️☑️

adversary unlocks skill:

determined attacker

applied control modelling

- control I: ☑️☑️☑️

- **if the password control is compromised, it's game over**

applied control modelling

- control I: ☑️☑️☑️
- control II: In addition to a password, require the answer to a **"Secret Question"** to perform sensitive operations

SIMPLE ?

STRONG ?

SELF-DEFENDING ?

applied control modelling

- control I: ☑️☑️☑️
- control II: In addition to a password, require the answer to a **"Secret Question"** to perform sensitive operations

SIMPLE ☑️

STRONG ❌

SELF-DEFENDING ☑️

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️❌☑️

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️❌☑️

FAIL INDEPENDENTLY ?

DIVERSE ?

MUTUALLY SUPPORTING ?

password failure → secret answer failure?

- guess password → secret answer ☑️
- access a stored password → secret answer ❌
- intercept a password → secret answer ❌

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️❌☑️

FAIL INDEPENDENTLY ☑️❌❌

DIVERSE ❓

MUTUALLY SUPPORTING ❓

"walls seem like a good control, lets build more walls!"

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️❌☑️

FAIL INDEPENDENTLY ☑️❌❌

DIVERSE ❌

MUTUALLY SUPPORTING ❌

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️❌☑️
- control interactions: ❌❌☑️
-

applied control modelling

- control I: ✅✅✅
- **control II: in addition to a password, require a One Time Password (OTP) to perform sensitive operations**

applied control modelling

- control I: ✅✅✅
- **control II: in addition to a password, require a One Time Password (OTP) to perform sensitive operations**

SIMPLE ✅

STRONG ✅

SELF-DEFENDING ✅

applied control modelling

- control I: ☑️☑️☑️
- control II: ☑️☑️☑️
- control interactions: ☑️☑️☑️
-

but is not in itself an authenticator for digital authentication. Authentication factors classified as something you know are not necessarily secrets, either. Knowledge based authentication, where the claimant is prompted to answer questions that can be confirmed from public databases, also does not constitute an acceptable secret for digital authentication. More generally, something you are does not generally

"*Knowledge-Based Authentication is 😢, pls stop using it*"
- NIST, 2016

reduce attack surface?

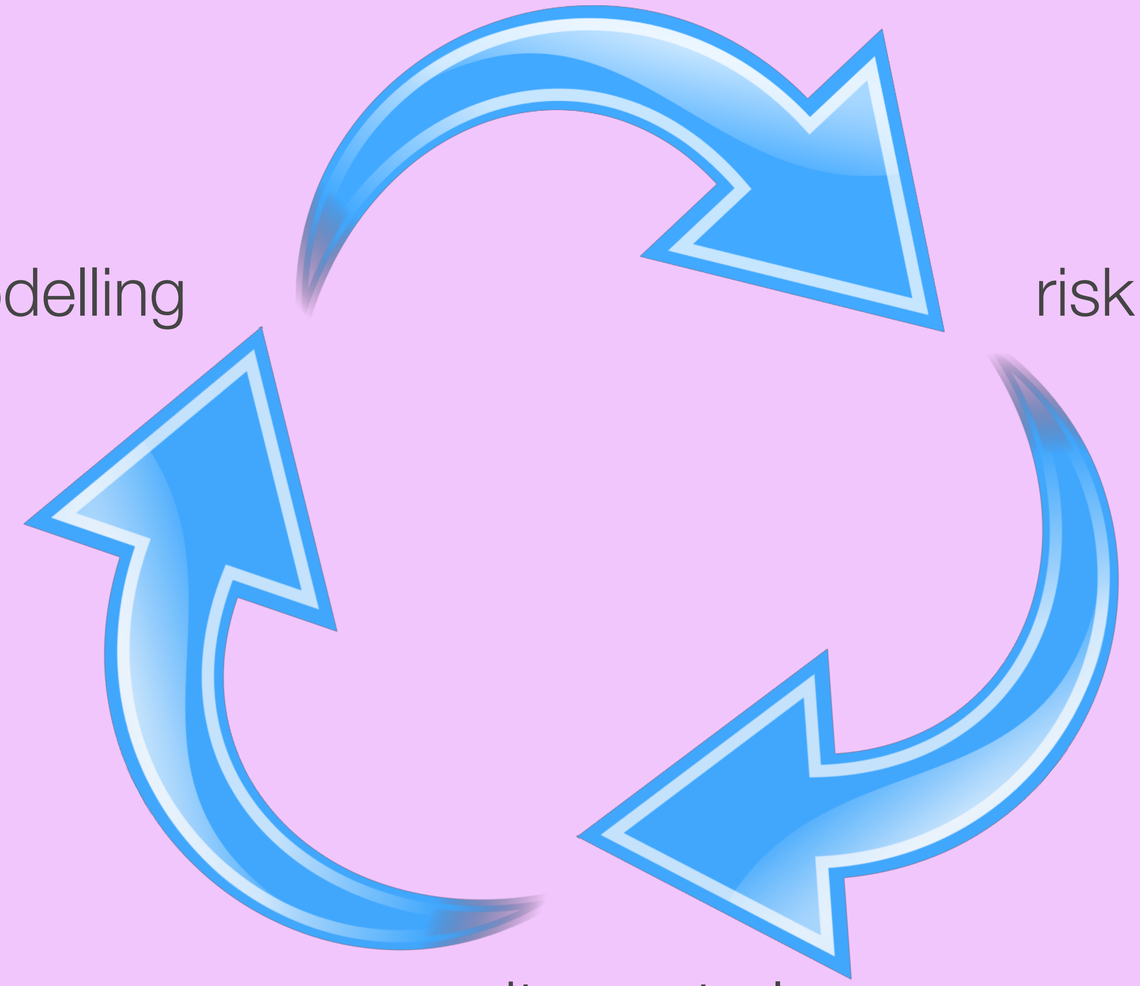
reduce attack surface?

- network-based controls

summary: desirable control attributes

INDIVIDUAL CONTROL		MULTIPLE CONTROLS	
SIMPLE	✅	FAIL INDEPENDENTLY	✅
STRONG	✅	DIVERSE	✅
SELF-DEFENDING	✅	MUTUALLY SUPPORTING	✅

how much effort to spend on controls?



thanks! <3

@liamosaur