The AppSec Contractual Sins

Sebastian Avarvarei

DefCamp Bucharest
November 2023

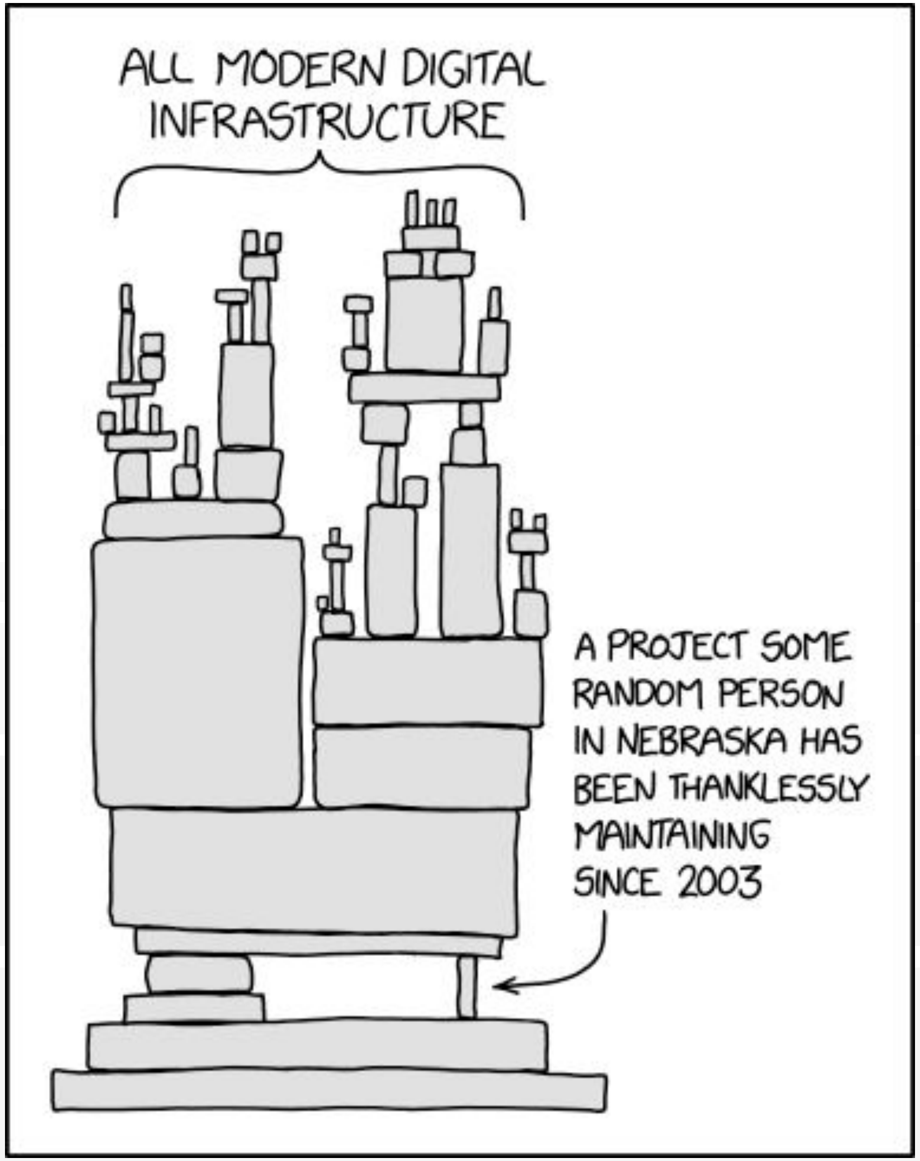
In IT and Security for over 20 years

EMEA Security Manager at Canon

Software developer in a previous life

- **Sebastian Paul Avarvarei**

sebastian@avarvarei.com
@sebastian_paul


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Source: https://xkcd.com/2347

What we have covered in the contract for Security

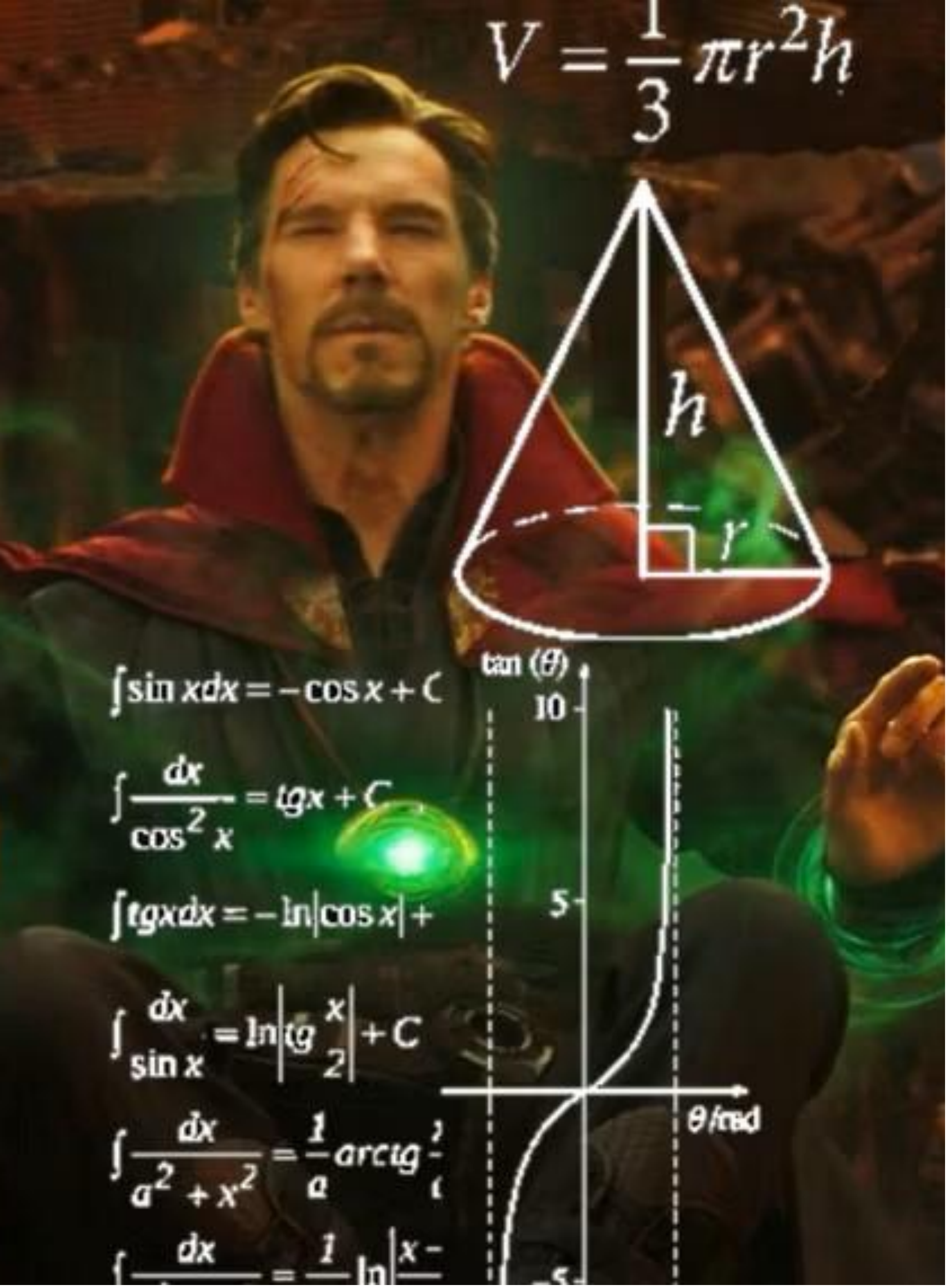
What we neglected to cover

> But I thought *YOU* read the AppSec clauses before we signed the contract!

All contracts start with good intentions

But ~~if~~ *when* things go wrong…

Contracts don’t have “Patch Tuesdays”!


$V = \frac{1}{3}\pi r^2 h$
h
r
$\int \sin x dx = -\cos x + C$
$\int \frac{dx}{\cos^2 x} = tgx + C$
$\int tgx dx = -\ln|\cos x| +$
$\int \frac{dx}{\sin x} = \ln\left|tg\frac{x}{2}\right| + C$
$\int \frac{dx}{a^2 + x^2} = \frac{1}{a} arctg$
tan (θ)
10
5
θ /rad

So how do we know what AppSec (or Security) clauses do we need to have in our contracts?

Writing security clauses
for contracts
is just another form of
Threat Modeling*…

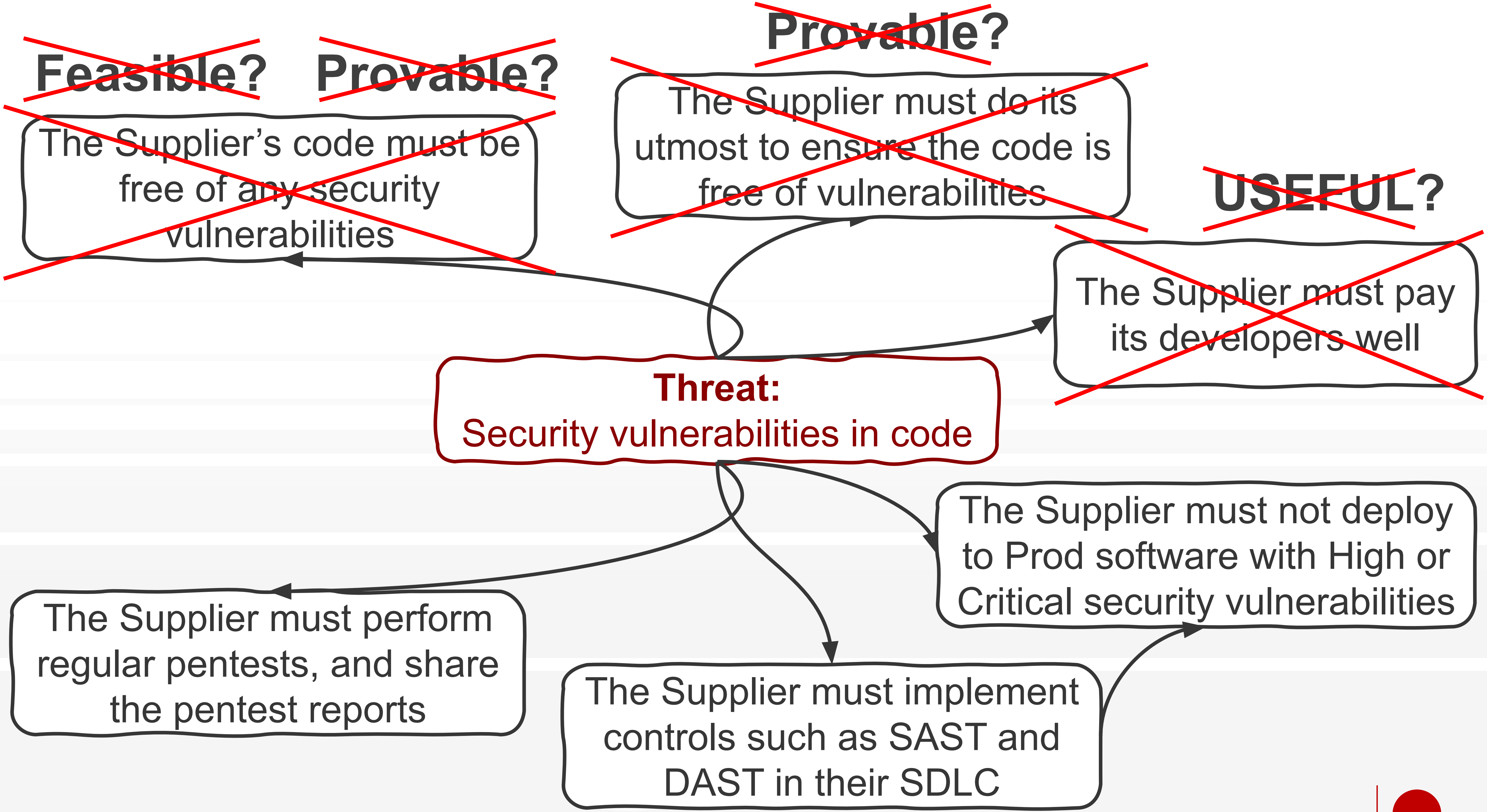
…but you do it in Legalese

** Threat Modeling = Taking a structured approach to asking "What else could go wrong?"*

So what makes a good security clause?

- **Feasible**
  - *Is it doable within the scope of the contract?*
- **Provable**
  - *Can we check or measure if the supplier met this requirement?*
- **Useful**
  - *What risk or threat are we mitigating with this clause?*

a.k.a. "What's the problem we're trying to solve?"



Threat:
Security vulnerabilities in code

~~Feasible?~~ **~~Provable?~~**

~~The Supplier's code must be free of any security vulnerabilities~~

~~Provable?~~

~~The Supplier must do its utmost to ensure the code is free of vulnerabilities~~

~~USEFUL?~~

~~The Supplier must pay its developers well~~

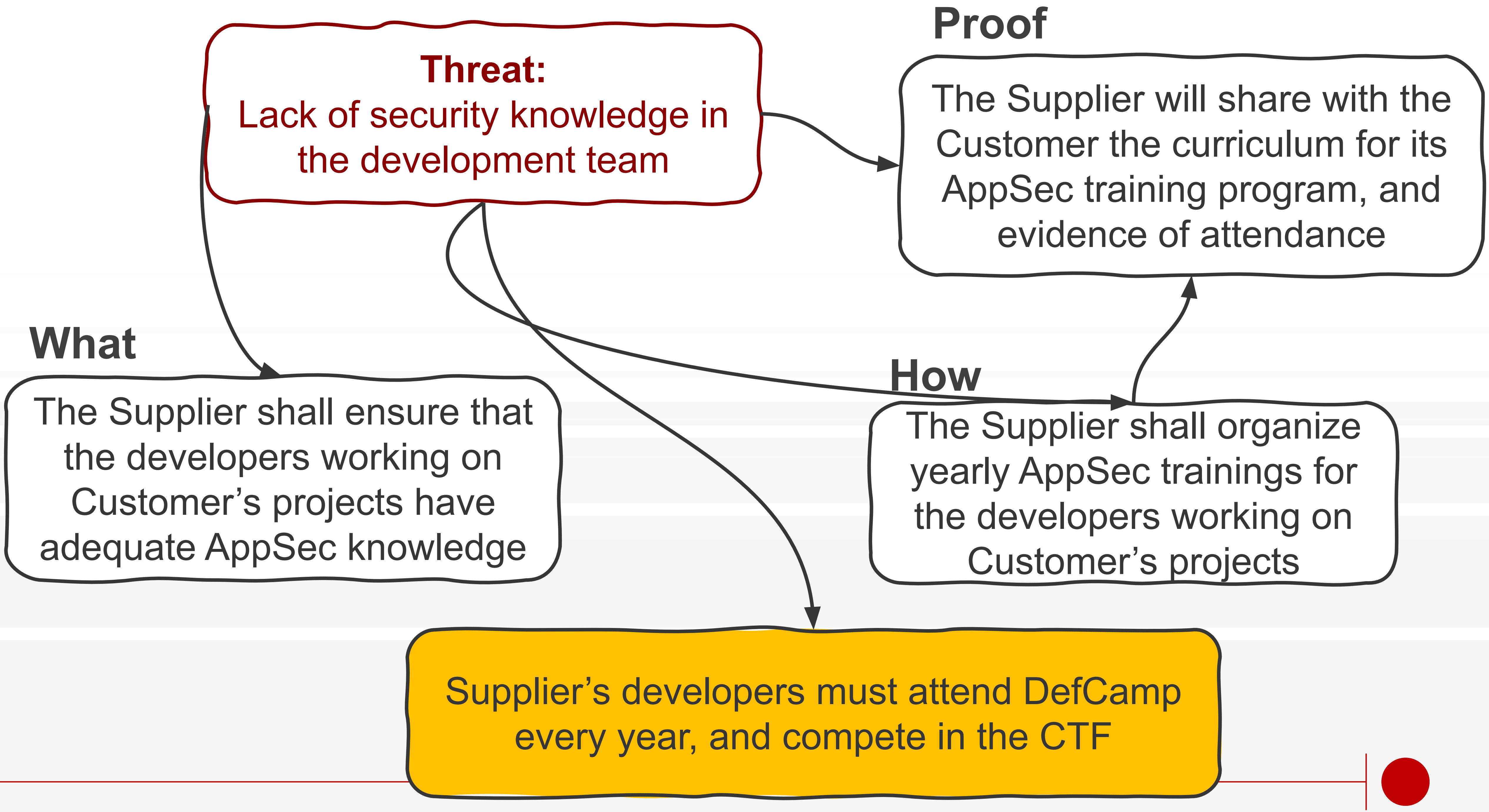
The Supplier must perform regular pentests, and share the pentest reports

The Supplier must implement controls such as SAST and DAST in their SDLC

The Supplier must not deploy to Prod software with High or Critical security vulnerabilities

There's more than one way to sort an array, ditto for writing security clauses

- **Results focused**
  - Stating **what** we want
- **Approach focused**
  - Stating **how** we want to achieve it
- **Evidence focused**
  - Stating how it's going to be **proved** that we got it



Threat:
Lack of security knowledge in the development team

What

The Supplier shall ensure that the developers working on Customer’s projects have adequate AppSec knowledge

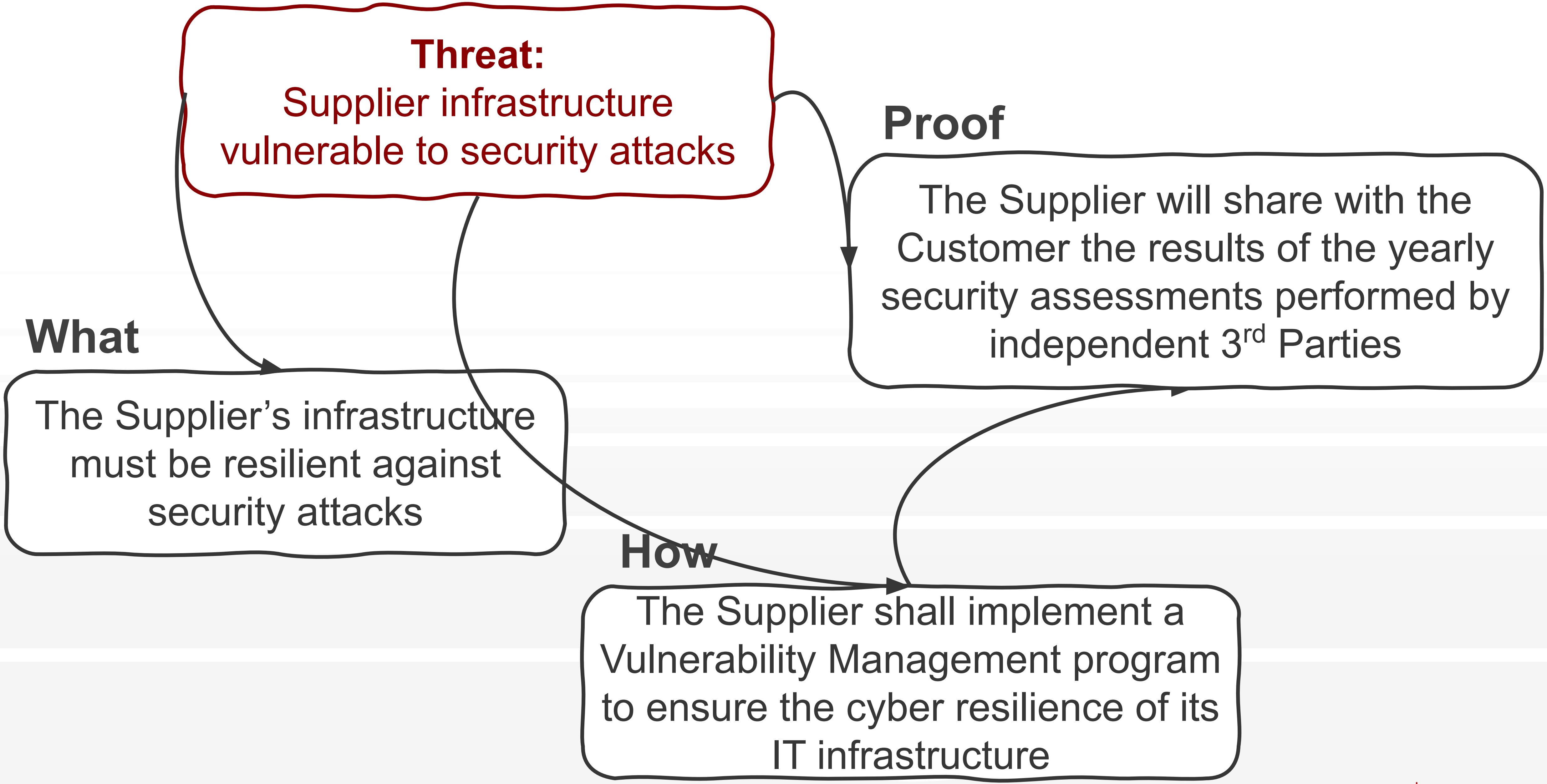
How

The Supplier shall organize yearly AppSec trainings for the developers working on Customer’s projects

Proof

The Supplier will share with the Customer the curriculum for its AppSec training program, and evidence of attendance

Supplier’s developers must attend DefCamp every year, and compete in the CTF



Threat:
Supplier infrastructure vulnerable to security attacks

What

The Supplier's infrastructure must be resilient against security attacks

How

The Supplier shall implement a Vulnerability Management program to ensure the cyber resilience of its IT infrastructure

Proof

The Supplier will share with the Customer the results of the yearly security assessments performed by independent 3rd Parties

The Phantom Clause Menace

> “ *The Supplier shall follow the Customer's Security Policies*

Why “Phantom”?

Because nobody reads them policies before signing!

We’ve updated our security policies!

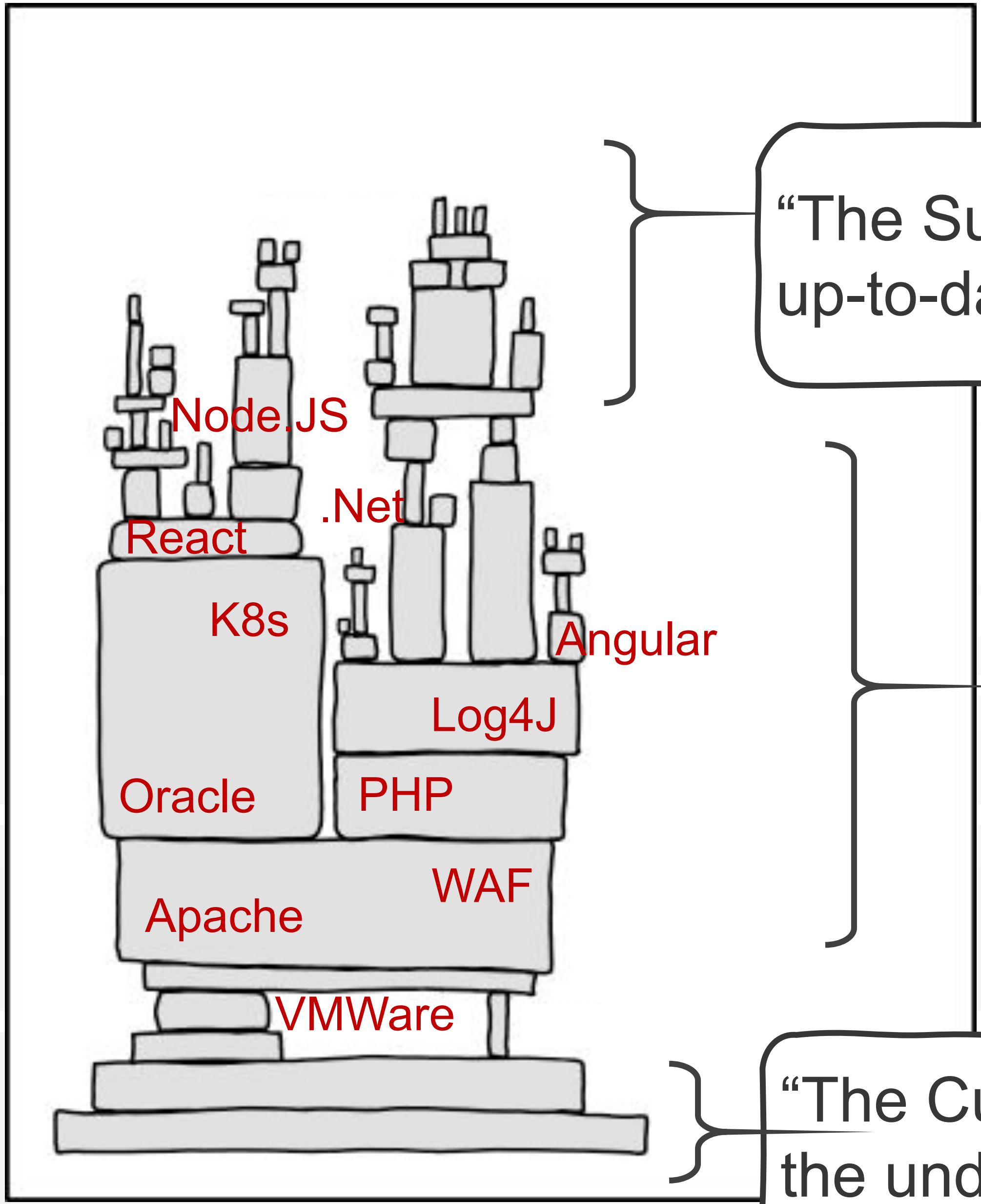
So… who picks up the bill now?

- How are parties informed about policy changes?
- How is the impact of the policy changes assessed?
- Who is responsible for any extra costs?

our privacy policy
our privacy policy
We've updated our privacy policy
our privacy policy
We've u
We've updated our privacy policy
We've upda
r privacy policy
We've updated our privacy policy
updated our privacy policy

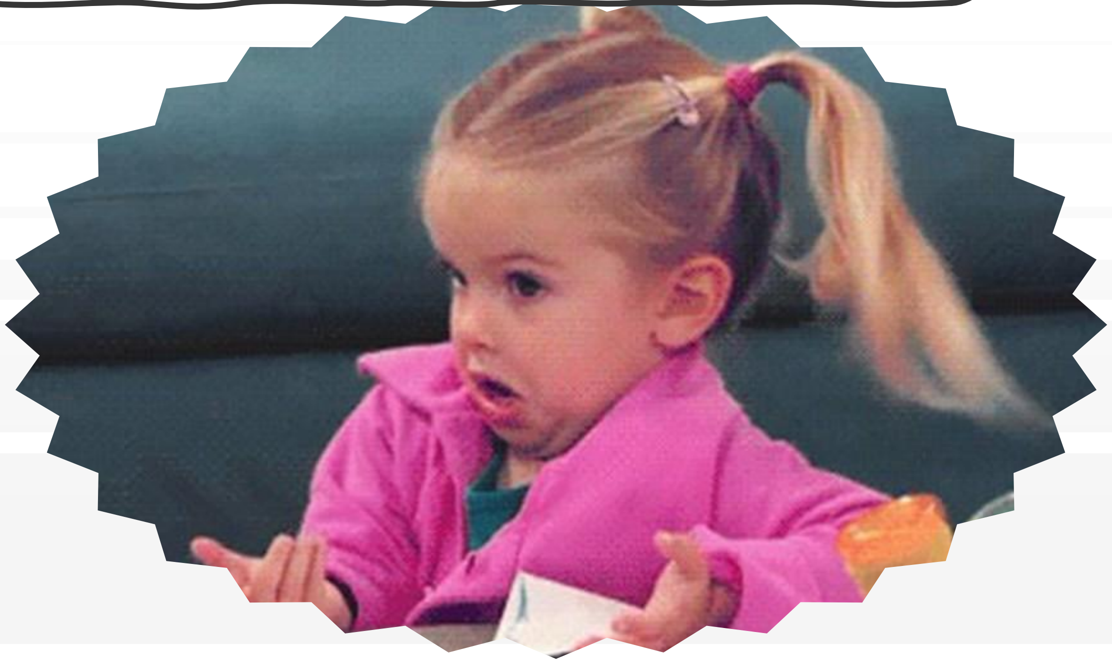
“ *Hm, Upgrades*

Who’s responsible?



Source: https://xkcd.com/2347

“The Supplier shall maintain the application up-to-date and apply relevant patches”



“The Customer is responsible for updating the underlying operating systems”

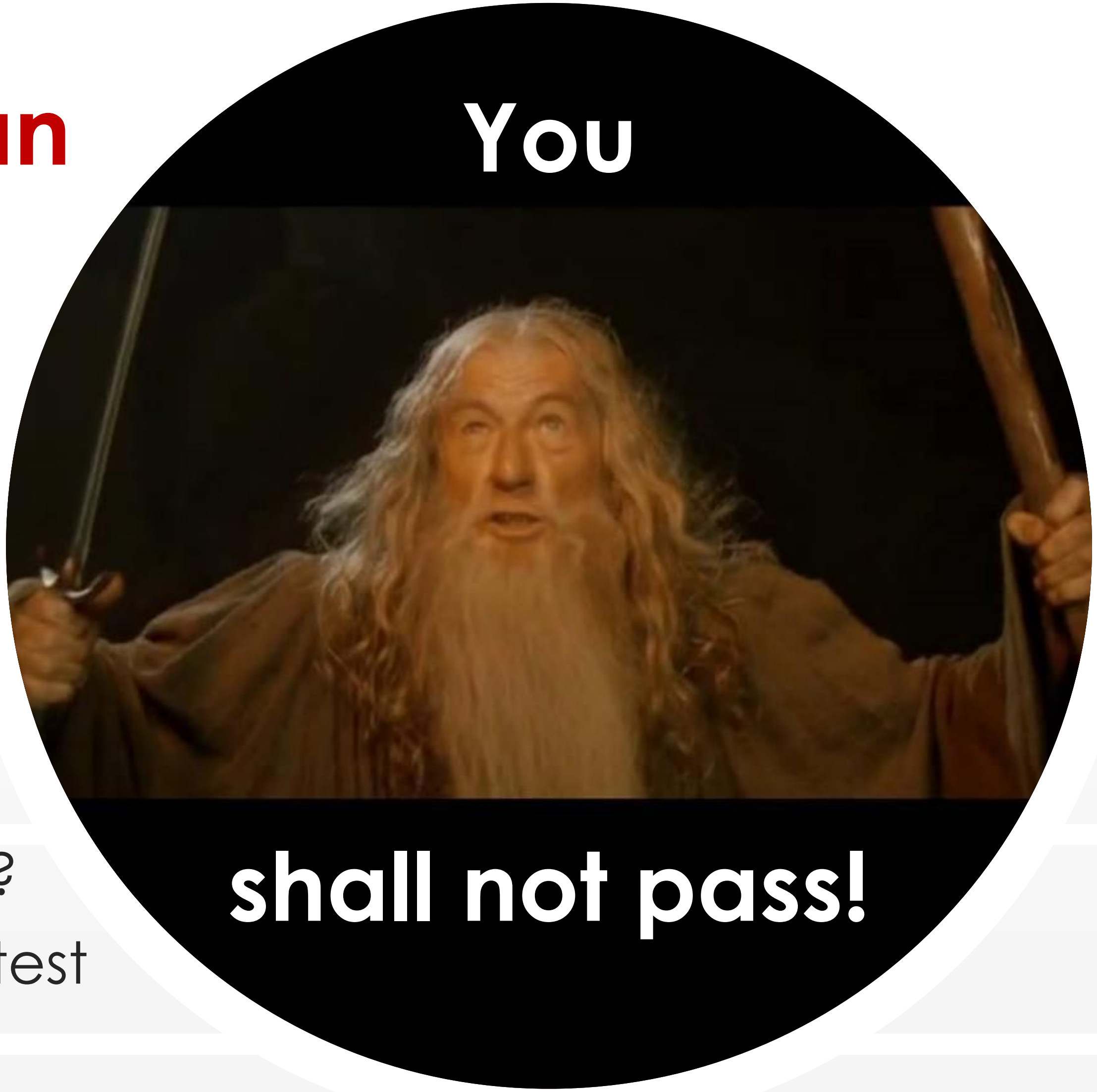
Best Practice clauses are just "feel good" statements

Be explicit and specific: *OWASP Secure Coding Practices Checklist, Microsoft Azure Security Best Practices, NIST SP 800-63-3 Digital Identities, OWASP ASVS etc.*

About those audits and pentests…

What audits and pentests can the Customer perform?

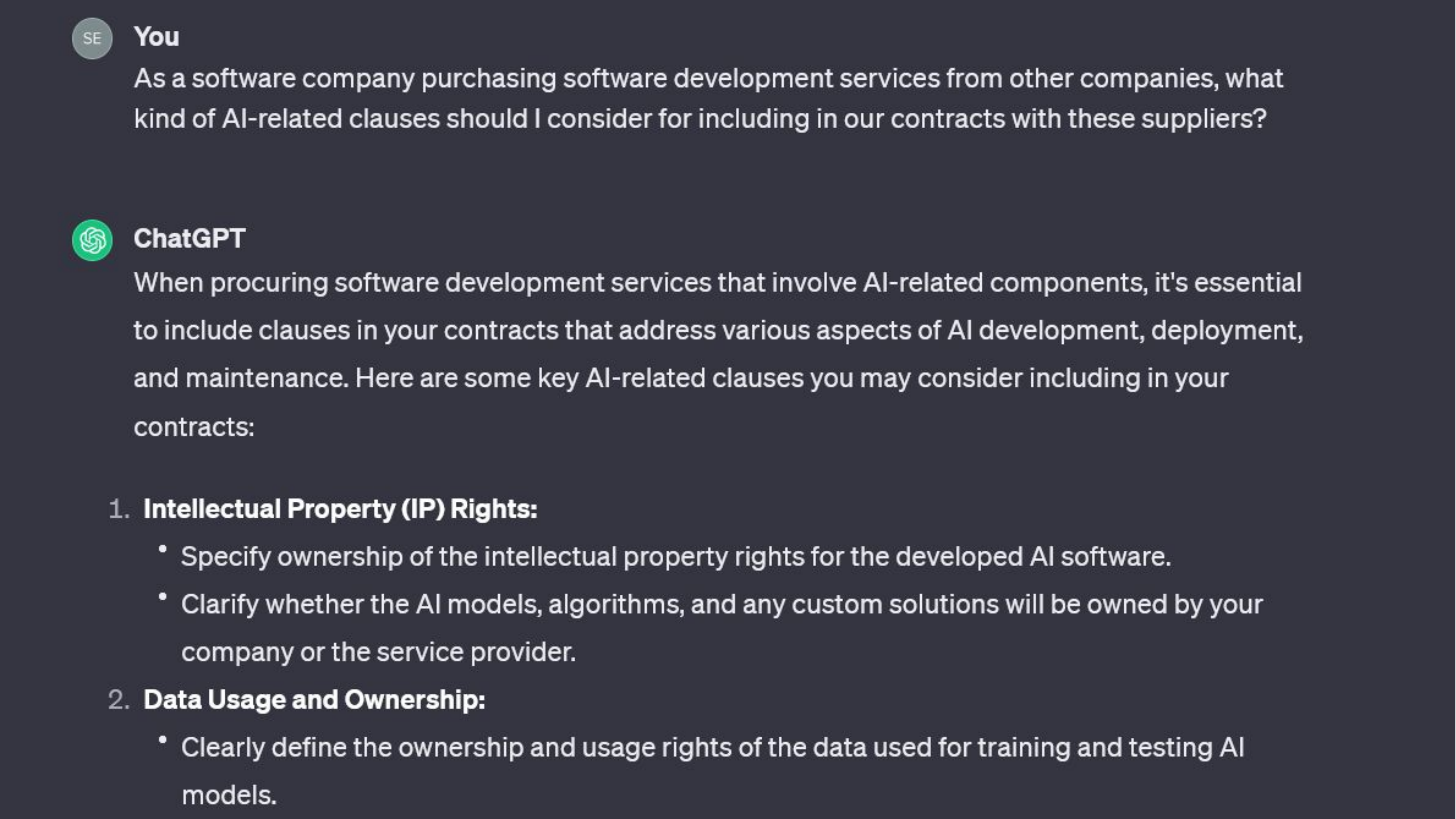
- Right to audit: frequency, notice periods, how many hours of work, costs for extra time.
- Pentests: Production or Development-only, methods allowed and not allowed, systems or time periods out-of-scope, in-house pentesters or external authorized companies?
- Obligations to share 3rd party audits and pentest reports between companies
- Code reviews: is the code intellectual property, who’s authorized to access it – and how?



- How about AI?

Let's ask the AI to write clauses about AI

(…what could possibly go wrong?)



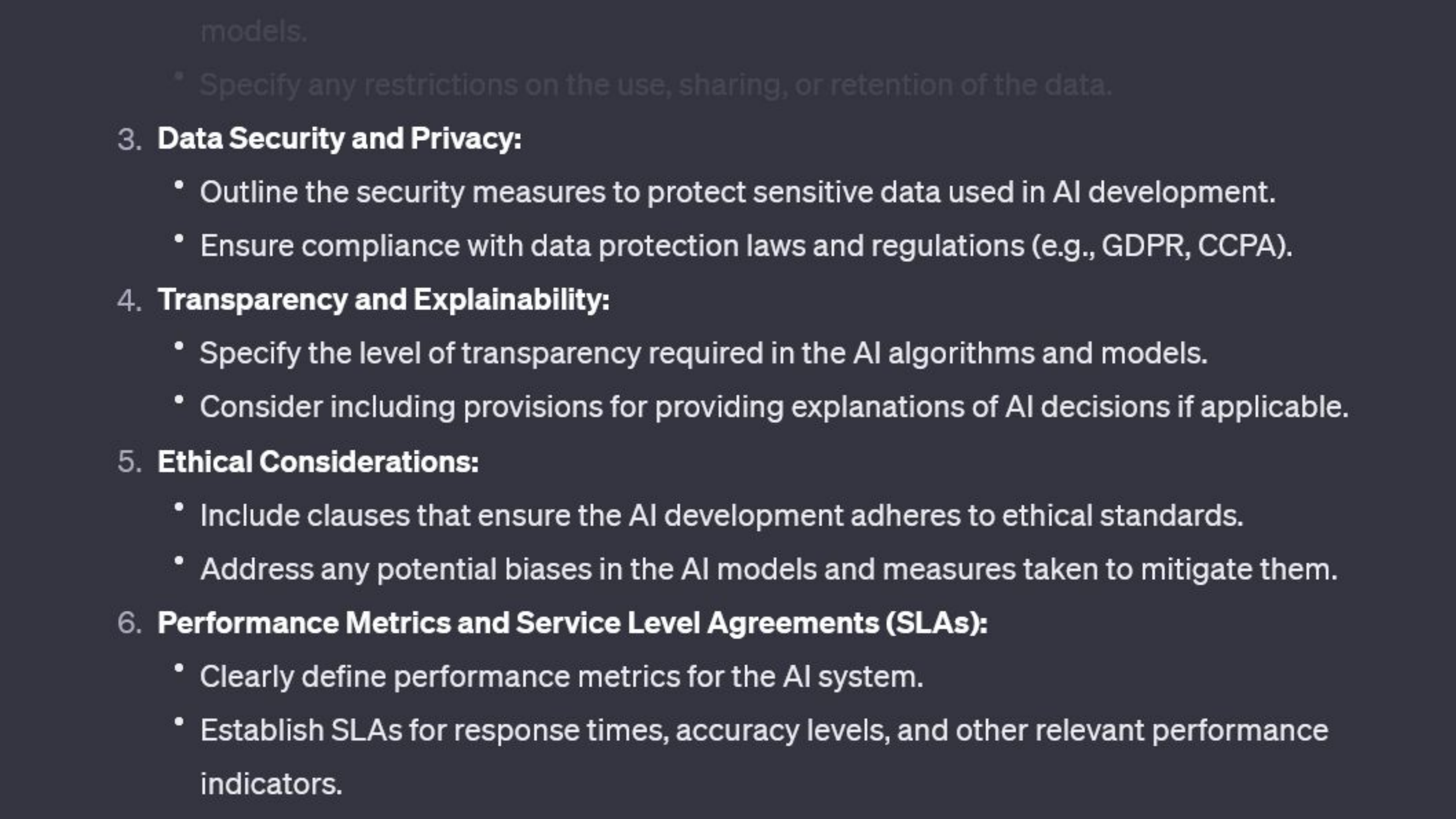
You

As a software company purchasing software development services from other companies, what kind of AI-related clauses should I consider for including in our contracts with these suppliers?

ChatGPT

When procuring software development services that involve AI-related components, it's essential to include clauses in your contracts that address various aspects of AI development, deployment, and maintenance. Here are some key AI-related clauses you may consider including in your contracts:

1. **Intellectual Property (IP) Rights:**
   - Specify ownership of the intellectual property rights for the developed AI software.
   - Clarify whether the AI models, algorithms, and any custom solutions will be owned by your company or the service provider.
2. **Data Usage and Ownership:**
   - Clearly define the ownership and usage rights of the data used for training and testing AI models.



models.
  - Specify any restrictions on the use, sharing, or retention of the data.

3. **Data Security and Privacy:**
   - Outline the security measures to protect sensitive data used in AI development.
   - Ensure compliance with data protection laws and regulations (e.g., GDPR, CCPA).
4. **Transparency and Explainability:**
   - Specify the level of transparency required in the AI algorithms and models.
   - Consider including provisions for providing explanations of AI decisions if applicable.
5. **Ethical Considerations:**
   - Include clauses that ensure the AI development adheres to ethical standards.
   - Address any potential biases in the AI models and measures taken to mitigate them.
6. **Performance Metrics and Service Level Agreements (SLAs):**
   - Clearly define performance metrics for the AI system.
   - Establish SLAs for response times, accuracy levels, and other relevant performance indicators.

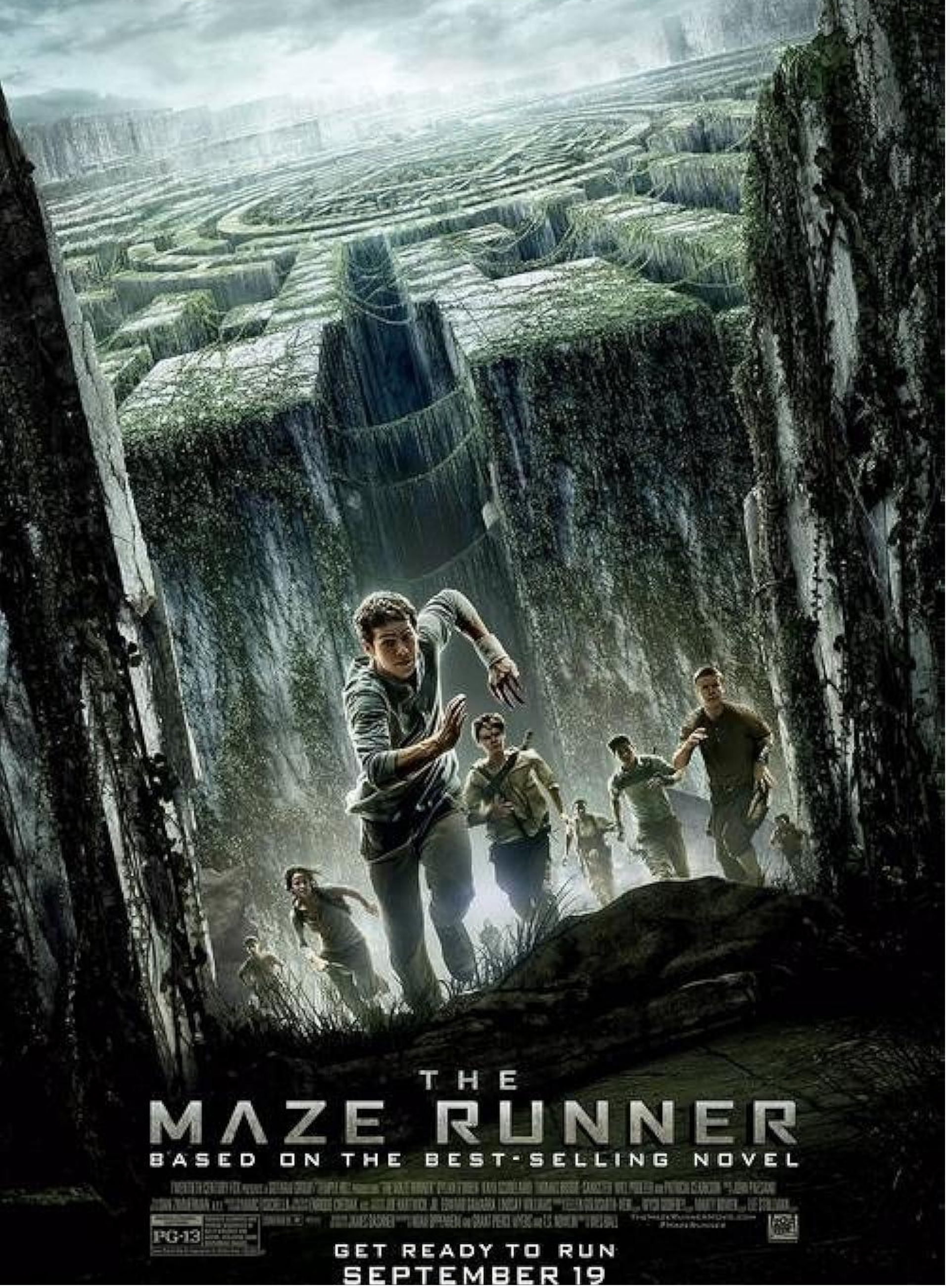
- Clearly state the maintenance and support services provided post-deployment.
- Include provisions for updates, bug fixes, and system improvements.

10. **Liability and Indemnification:**
    - Clarify liability in case of AI-related errors or malfunctions.
    - Include indemnification clauses to protect your company from legal claims arising from AI system failures.
11. **Regulatory Compliance:**
    - Ensure that the AI solution complies with relevant industry regulations and standards.
    - Specify which party is responsible for ensuring ongoing compliance with changing regulations.
12. **Termination and Transition:**
    - Define the conditions under which the contract can be terminated.
    - Include provisions for transitioning the AI solution to another provider or bringing it in-house if needed.
13. **Dispute Resolution:**
    - Specify mechanisms for resolving disputes related to AI development and deployment.

But please remember….

AI is not a lawyer!

- ***What, you wanted MORE contractual AppSec clauses?***



Where do we go from here?

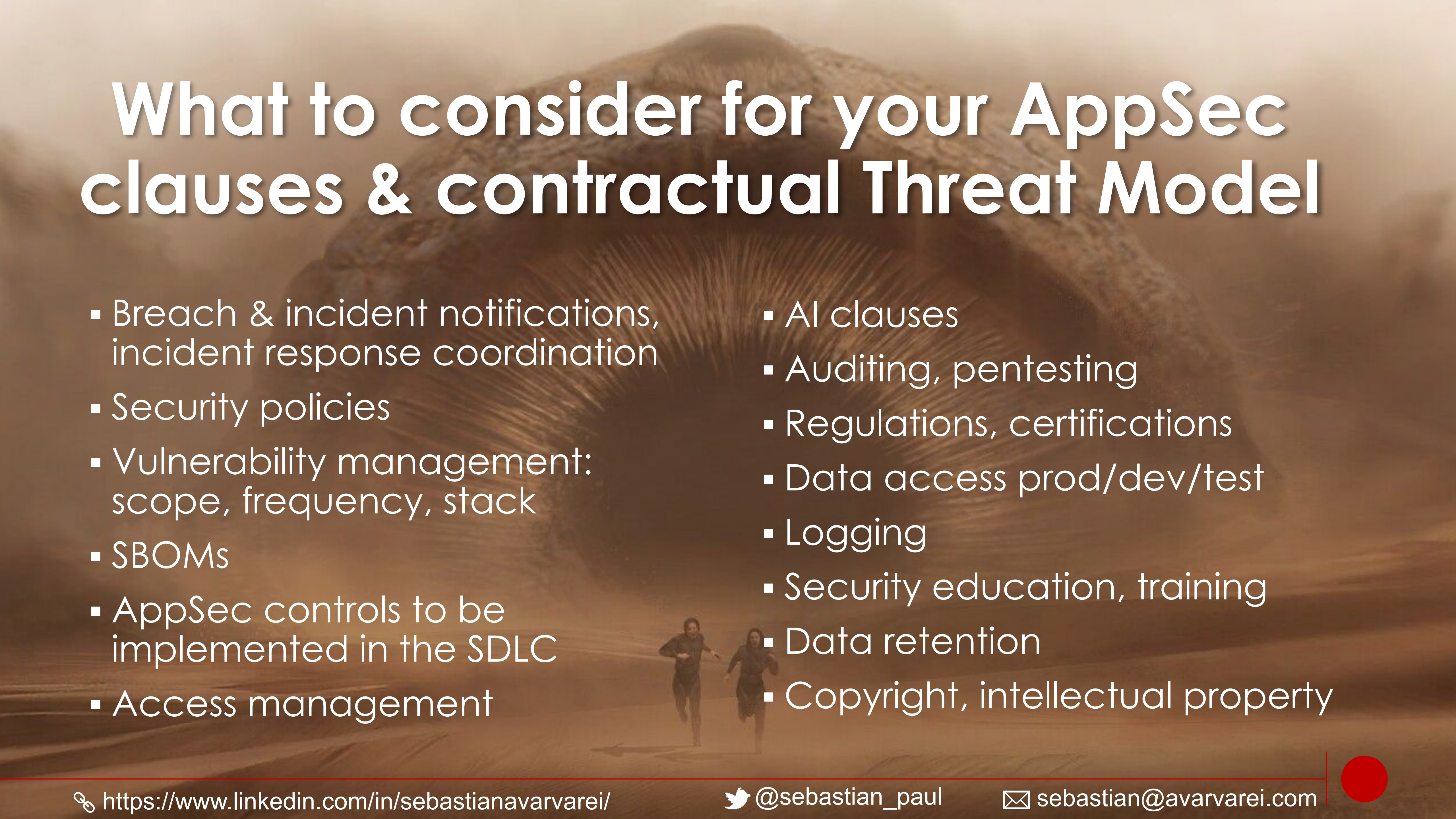
Big reveal coming: New OWASP Project !

OWASP AppSec Contract Builder

(provisional title)

Framework, templates and (hopefully) tools for your AppSec contractual needs

Contributors are welcomed!



What to consider for your AppSec clauses & contractual Threat Model

- Breach & incident notifications, incident response coordination
- Security policies
- Vulnerability management: scope, frequency, stack
- SBOMs
- AppSec controls to be implemented in the SDLC
- Access management
- AI clauses
- Auditing, pentesting
- Regulations, certifications
- Data access prod/dev/test
- Logging
- Security education, training
- Data retention
- Copyright, intellectual property

https://www.linkedin.com/in/sebastianavarvarei/ @sebastian_paul sebastian@avarvarei.com

THANK YOU!

Now go forth, and sin no more

@sebastian_paul
sebastian@avarvarei.com
linkedin.com/in/sebastianavarvarei