About this presentation

This slide deck was created as a draft to illustrate the outcome of a 2 hour OWASP working session held in London in February 2018. The contents were created as a collaborative effort by 8 people and focuses on how to “sell” threat modelling to the business.

The raw notes and this deck are released under the creative commons license and available here: https://sdfasdf. Feedback through the #xyz channel on the https://owasp.slack.com

Using this presentation

The target audience of this presentation is a Product Owner with the following persona characteristics: Non-technical; busy; takes pride in their work and deliverables - from design to operations; may have concerns about regulations; doesn’t want to take on unnecessary extra work; fear of the unknown.

The small fonts used may make this deck inappropriate for large screen presentations.

PLEASE DELETE THIS SLIDE

The hidden cost of

INSECURITY

What's The problem?

OWASP
Open Web Application Security Project

01	Cyber incidents cost money	External incident response and lost work hours associated with remediating an incident, increased marketing spend to compensate for brand & reputation damage, regulatory fines, lost sales - just some of the ways cyber incidents can introduce unexpected costs.
02	Production issues cost more	It's a well-established fact that it costs more to fix an issue in production than it does to fix it before production. The sooner the problem is identified and fixed, the cheaper the fix is. Better still is to architect the problem away - something we often see for downtime through highly available designs.
03	An uncertain ROI is a worse ROI	Return On Investment calculations are tricky at the best of times. If your investment in a new service aims to bring in 2 million new customers, but an architectural flaw results in a critical vulnerability and breach - how many of those customers can you afford to lose and at what cost?

"We tend to overvalue the things we can measure and undervalue the things we cannot" - John Hayes

What's The solution?

Identify the threats

Threat modelling means identifying and documenting fundamental flaws and threats in the architecture and design of a product or service, before the attackers do. It can also address whole classes of issues instead of just focusing on individual vulnerabilities, saving you precious time.

Shift left

Threat modelling compliments penetration testing and bug bounties by adding another layer of threat identification, much earlier in the SDLC. Instead of risking a delayed production release due to a critical pentest finding, threat modelling can mitigate your threats before a single line of code is written.

Be data-driven

Documented threats can be assessed for potential business impact, adding value to risk calculations. Risk is an enabler, but requires data in order to be informed. Threat modelling allows you to make informed risk decisions and can help you prioritise the work needed to protect your investment.

"You can't secure what you don't understand" - Bruce Schneier

What's next?

OWASP
Open Web Application Security Project

Start small

Rolling out threat modelling should be an agile process, so start with an MVP, discover what works, learn, adjust, and iterate.

- Find a friendly development team
- Security should provide training
- Brainstorm an approach that works for the team
- Decide on how to capture threats

Follow the feature

It's easy to get carried away trying to threat model the entire product or service. Instead, pick a feature in development and follow the feature through its journey.

- Choose a feature that's at the start of the SDLC, in the design phase
- Limit the threat modelling scope to just that feature - ignore everything else

Mentor & facilitate

Security should help drive the adoption of threat modelling through a process of mentoring and facilitation, not through a series of draconian demands.

- Security must not be judgemental
- Enable a blameless culture
- Use the tools you're comfortable with
- The business owns the outcome, not security

"Be not afraid of growing slowly, be afraid only of standing still" - Chinese Proverb