Level up your threat modeling practice

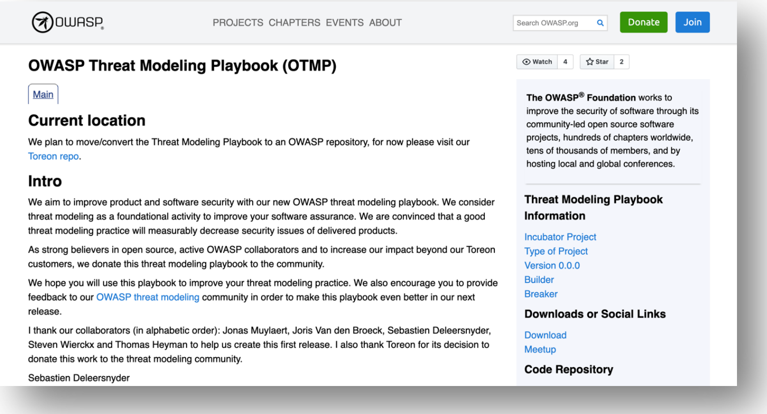
SecAppDev, 14 June 2022

Sebastien Deleersnyder, CTO Toreon

Agenda

- Threat modeling
- Leveling up – we need a playbook!
- Get stakeholder buy-in
- Embed in your organization
- Training your people
- Strengthen your processes
- Innovate with technology
- Open sourcing our playbook / demo
- Q&A

https://github.com/OWASP/threat-model-playbook



OWASP Threat Modeling Playbook (OTMP)

Current location

We plan to move/convert the Threat Modeling Playbook to an OWASP repository, for now please visit our Toreon repo.

Intro

We aim to improve product and software security with our new OWASP threat modeling playbook. We consider threat modeling as a foundational activity to improve your software assurance. We are convinced that a good threat modeling practice will measurably decrease security issues of delivered products.

As strong believers in open source, active OWASP collaborators and to increase our impact beyond our Toreon customers, we donate this threat modeling playbook to the community.

We hope you will use this playbook to improve your threat modeling practice. We also encourage you to provide feedback to our OWASP threat modeling community in order to make this playbook even better in our next release.

I thank our collaborators (in alphabetic order): Jonas Muylaert, Joris Van den Broeck, Sebastien Deleersnyder, Steven Wierckx and Thomas Heyman to help us create this first release. I also thank Toreon for its decision to donate this work to the threat modeling community.

Sebastien Deleersnyder

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Threat Modeling Playbook Information

Incubator Project
Type of Project
Version 0.0.0
Builder
Breaker

Downloads or Social Links

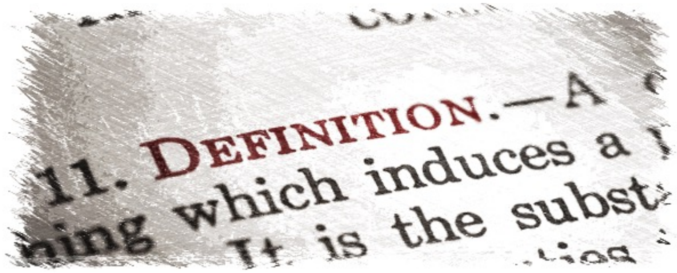
Download
Meetup

Code Repository

https://owasp.org/www-project-threat-modeling-playbook/

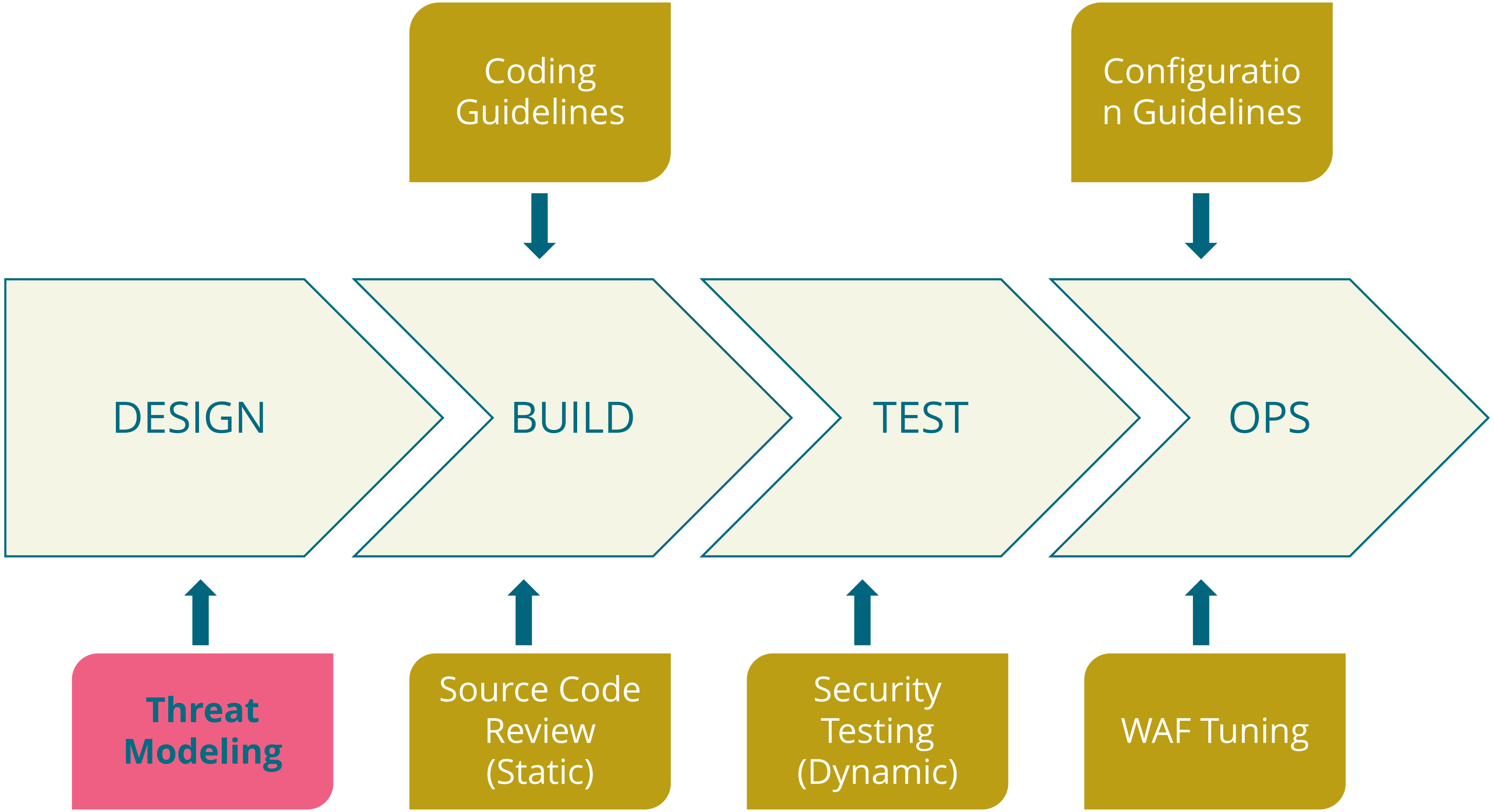
Threat Modeling

Threat modeling

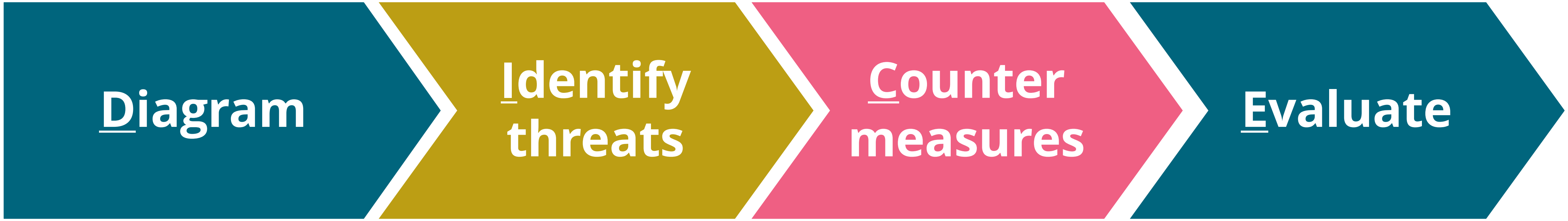


Threat modeling is the activity of identifying and managing application risks

Secure development lifecycle


Coding Guidelines
Configuratio n Guidelines
DESIGN
BUILD
TEST
OPS
Threat Modeling
Source Code Review (Static)
Security Testing (Dynamic)
WAF Tuning

Threat modeling stages – DICE framework



Diagram

Identify threats

Counter measures

Evaluate

What are we building?

What can go wrong?

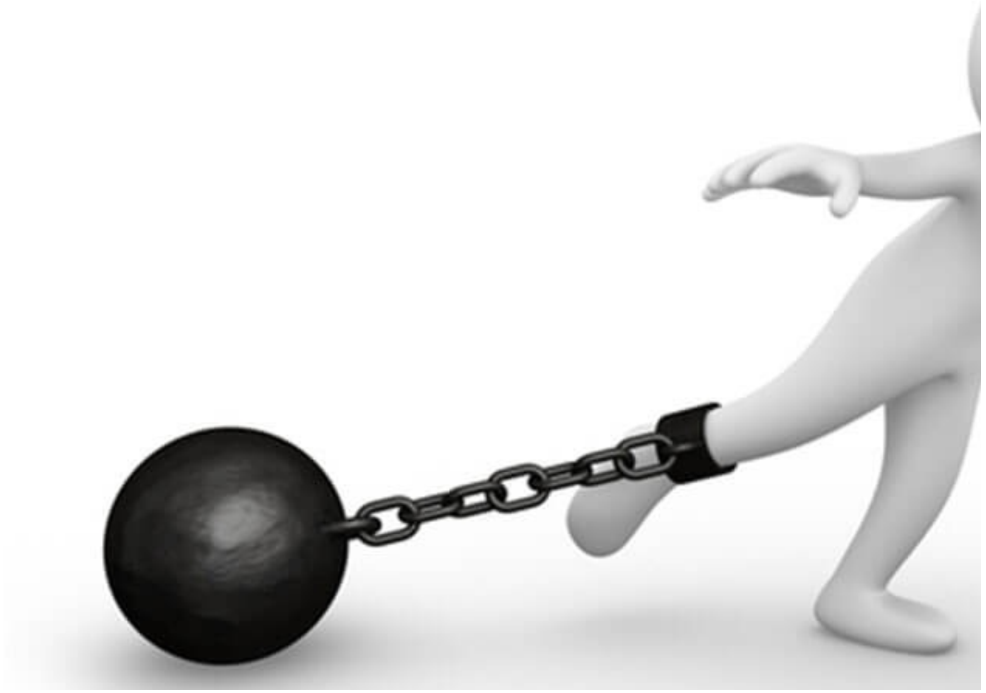
What are we going to do about it?

Did we do a good enough job?

Why perform threat modeling?

- Get team on same page with a shared vision on security
- Prevent security design flaws
- Identify & address greatest risks
- Prioritize development efforts based on risk weighting
- Document due diligence (GDPR, FDA, ...), other examples:
  - NIST included Threat Modeling in the Recommended Minimum Standard for Vendor or Developer Verification of Code in 2021
  - OWASP has added Insecure Design to the OWASP Top 10 in 2021.

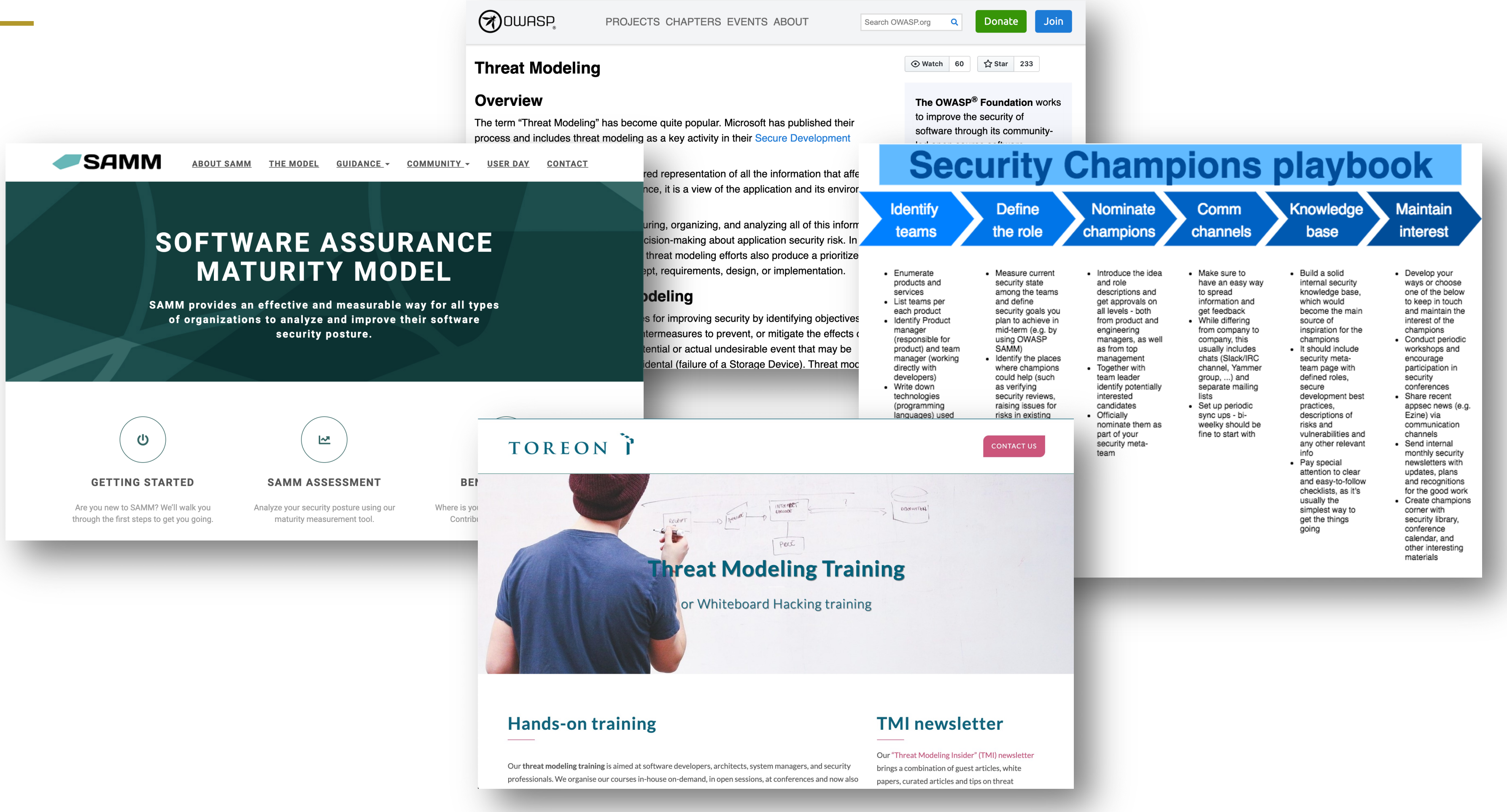
Adoption constraints



- Generally requires outside security expertise
- Can take a lot of time (costly)
- Difficult to internalize and reproduce across application portfolios and teams
- Tools have limited functionality
- Does not scale

Leveling up - we need a playbook

Pulling it together



Threat Modeling

Overview

The term "Threat Modeling" has become quite popular. Microsoft has published their process and includes threat modeling as a key activity in their Secure Development

red representation of all the information that affe

nce, it is a view of the application and its enviror

uring, organizing, and analyzing all of this inform

cision-making about application security risk. In

threat modeling efforts also produce a prioritize

ept, requirements, design, or implementation.

odeling

s for improving security by identifying objectives

termeasures to prevent, or mitigate the effects c

tential or actual undesirable event that may be

idental (failure of a Storage Device). Threat moc

The OWASP® Foundation works to improve the security of software through its community-

SOFTWARE ASSURANCE MATURITY MODEL

SAMM provides an effective and measurable way for all types of organizations to analyze and improve their software security posture.

GETTING STARTED

Are you new to SAMM? We'll walk you through the first steps to get you going.

SAMM ASSESSMENT

Analyze your security posture using our maturity measurement tool.

BEN

Where is yo

Contrib

Security Champions playbook

Identify teams
- Enumerate products and services
- List teams per each product
- Identify Product manager (responsible for product) and team manager (working directly with developers)
- Write down technologies (programming languages) used

Define the role
- Measure current security state among the teams and define security goals you plan to achieve in mid-term (e.g. by using OWASP SAMM)
- Identify the places where champions could help (such as verifying security reviews, raising issues for risks in existing

Nominate champions
- Introduce the idea and role descriptions and get approvals on all levels - both from product and engineering managers, as well as from top management
- Together with team leader identify potentially interested candidates
- Officially nominate them as part of your security meta-team

Comm channels
- Make sure to have an easy way to spread information and get feedback
- While differing from company to company, this usually includes chats (Slack/IRC channel, Yammer group, ...) and separate mailing lists
- Set up periodic sync ups - bi-weelky should be fine to start with

Knowledge base
- Build a solid internal security knowledge base, which would become the main source of inspiration for the champions
- It should include security meta-team page with defined roles, secure development best practices, descriptions of risks and vulnerabilities and any other relevant info
- Pay special attention to clear and easy-to-follow checklists, as it's usually the simplest way to get the things going

Maintain interest
- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with updates, plans and recognitions for the good work
- Create champions corner with security library, conference calendar, and other interesting materials

Threat Modeling Training

or Whiteboard Hacking training

Hands-on training

Our **threat modeling training** is aimed at software developers, architects, system managers, and security professionals. We organise our courses in-house on-demand, in open sessions, at conferences and now also

TMI newsletter

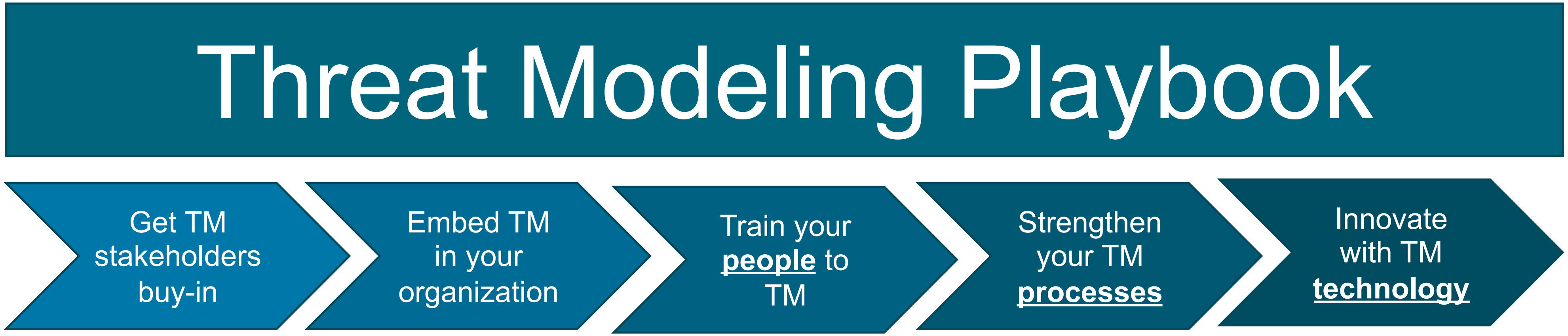
Our "Threat Modeling Insider" (TMI) newsletter brings a combination of guest articles, white papers, curated articles and tips on threat

https://owaspsamm.org/
https://github.com/c0rdis/security-champions-playbook
https://owasp.org/www-community/Threat_Modeling

How a playbook will help us

- Translate vision and strategy into tactics
- American Football➔ Plays selected depending on
  - position on the field,
  - strengths and weaknesses of the opposition
  - and the stage of the game.
- Translates well to threat modeling: need to understand offense and defense
- Gamification increases adoption

Level up your threat modeling game



Threat Modeling Playbook

Get TM stakeholders buy-in

- Involve people and allocate time
- Inject TM expertise
- Show threat modeling ROI

Embed TM in your organization

- Establish context
- Assess and treat risk
- Monitor and review
- Communicate

Train your **people** to TM

- Identify stakeholders
- Create TM specialist role
- Train your people
- Create a positive TM culture

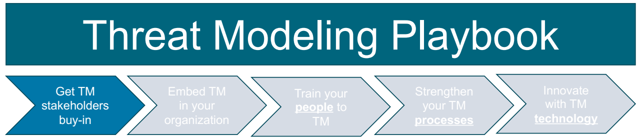
Strengthen your TM **processes**

- Understand current process
- Introduce application risk levels
- Choose a TM methodology
- Perform and persist the TM
- Integrate with risk framework
- Follow up TM action items
- Optimize methodology and risk calculation

Innovate with TM **technology**

- Select the right tools
- Process the tools outcome
- Integrate in your TM methodology

Get stakeholder buy-in



Threat Modeling Playbook

Get TM stakeholders buy-in

Embed TM in your organization

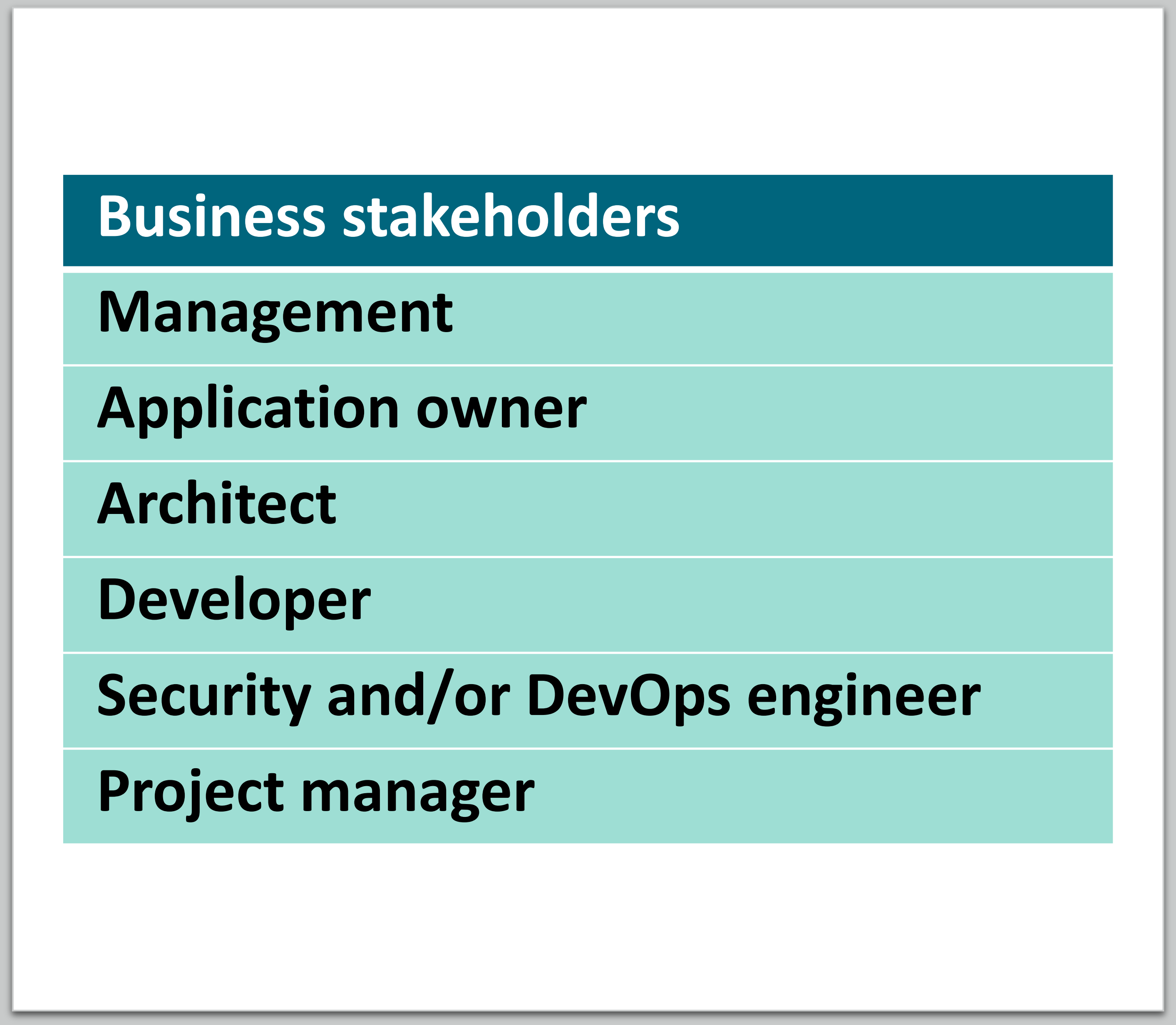
Train your **people** to TM

Strengthen your TM **processes**

Innovate with TM **technology**

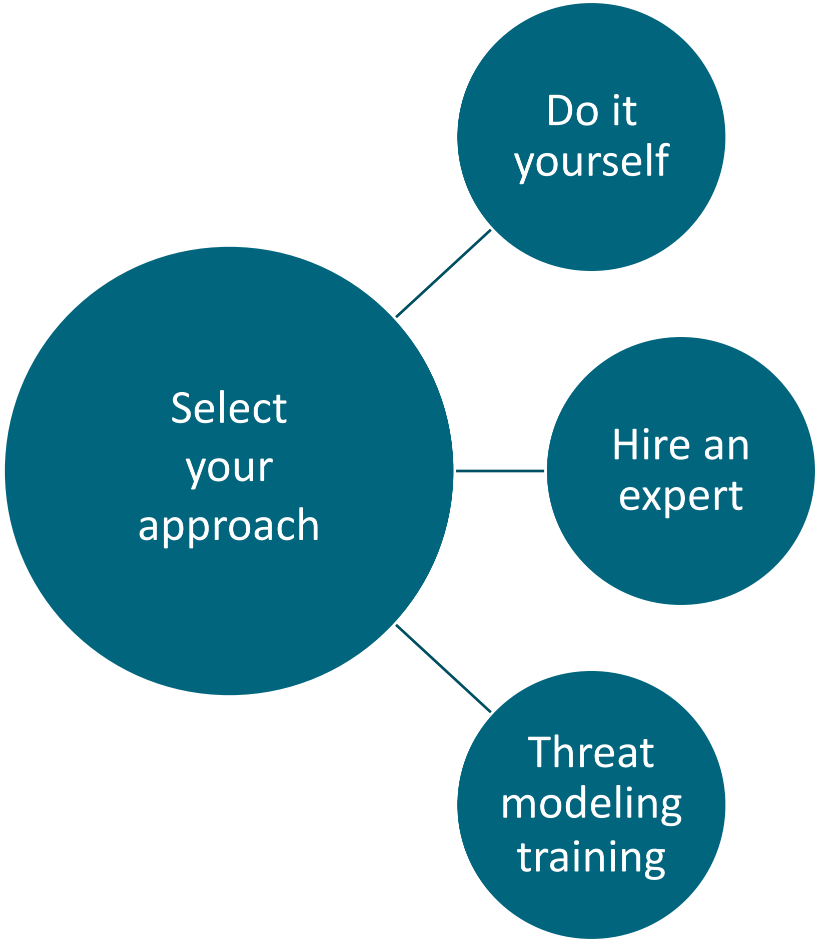
Involve people and allocate time

- Who is involved?
- Stakeholder costs and obstacles?
- What are potential gains?



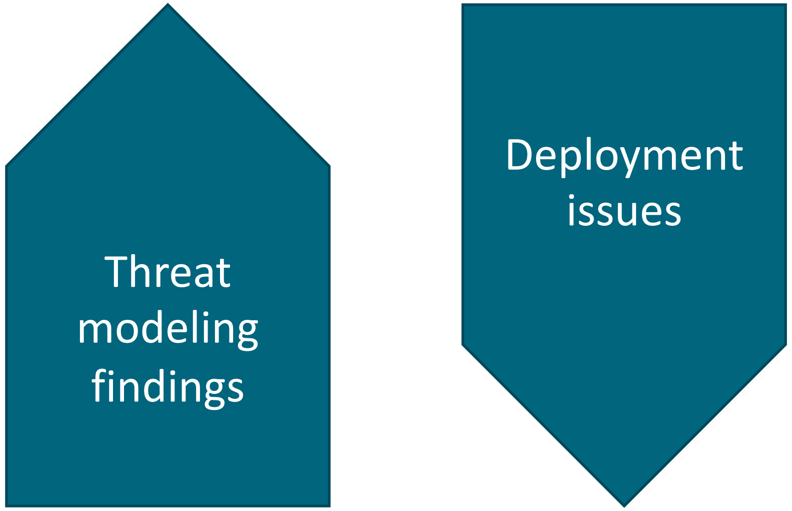
Business stakeholders
Management
Application owner
Architect
Developer
Security and/or DevOps engineer
Project manager

Inject threat modeling expertise



Demonstrate ROI

- Your threat models need clear and actionable outcomes
- Balance threat models with project constraints
- Link threat models to development and security artefacts
  - User stories
  - Bug fixes
  - Incidents
  - JIRA tickets …



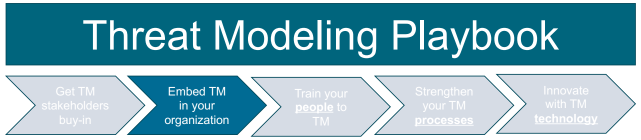
Threat modeling findings

Deployment issues

OWASP resources

- OWASP Top 10
  - https://owasp.org/www-project-top-ten/
- OWASP Threat Modeling Slack channel
  - https://owasp.slack.com/archives/C1CS3C6AF

Embed in your organization



Threat Modeling Playbook

Get TM stakeholders buy-in

Embed TM in your organization

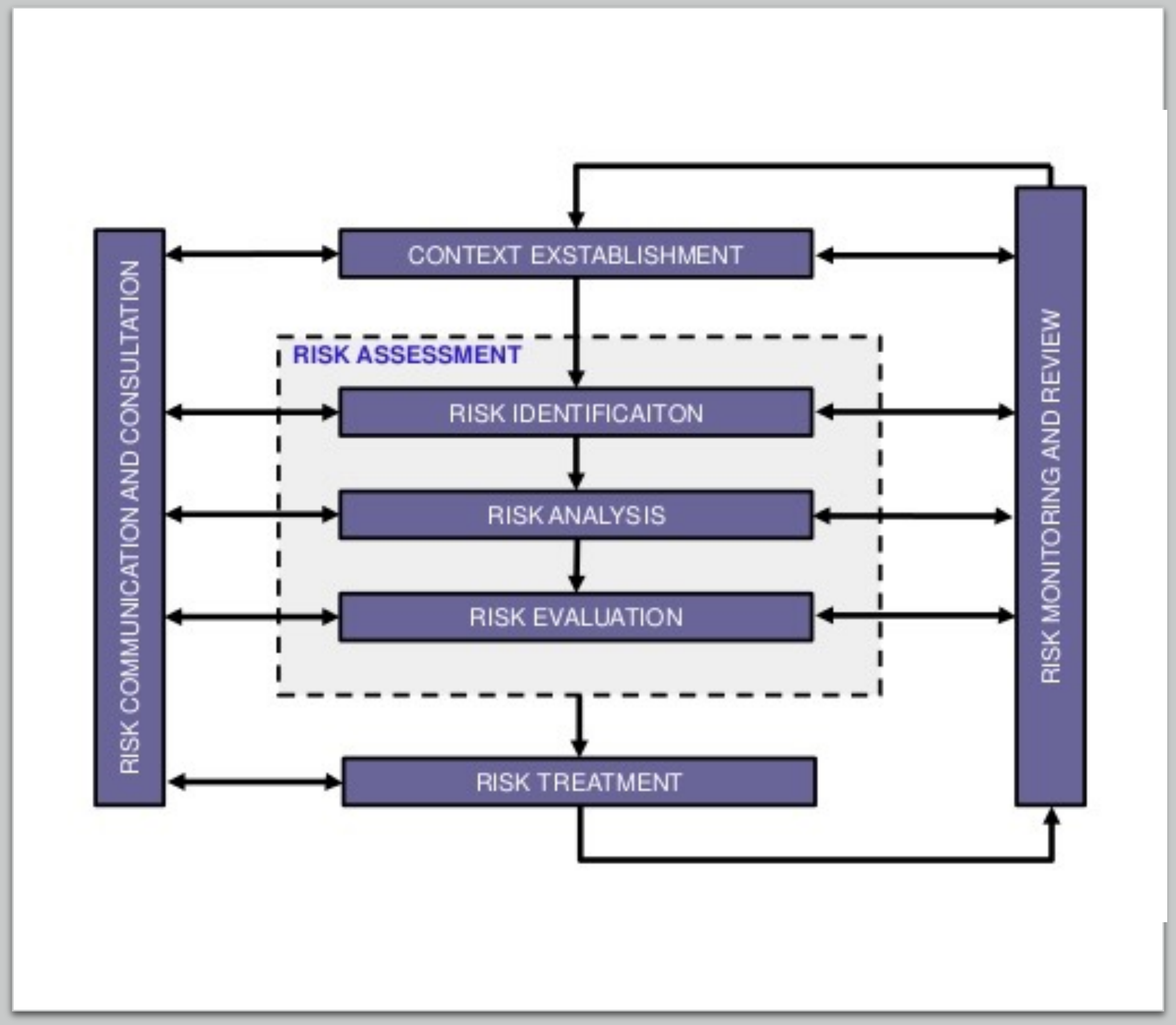
Train your **people** to TM

Strengthen your TM **processes**

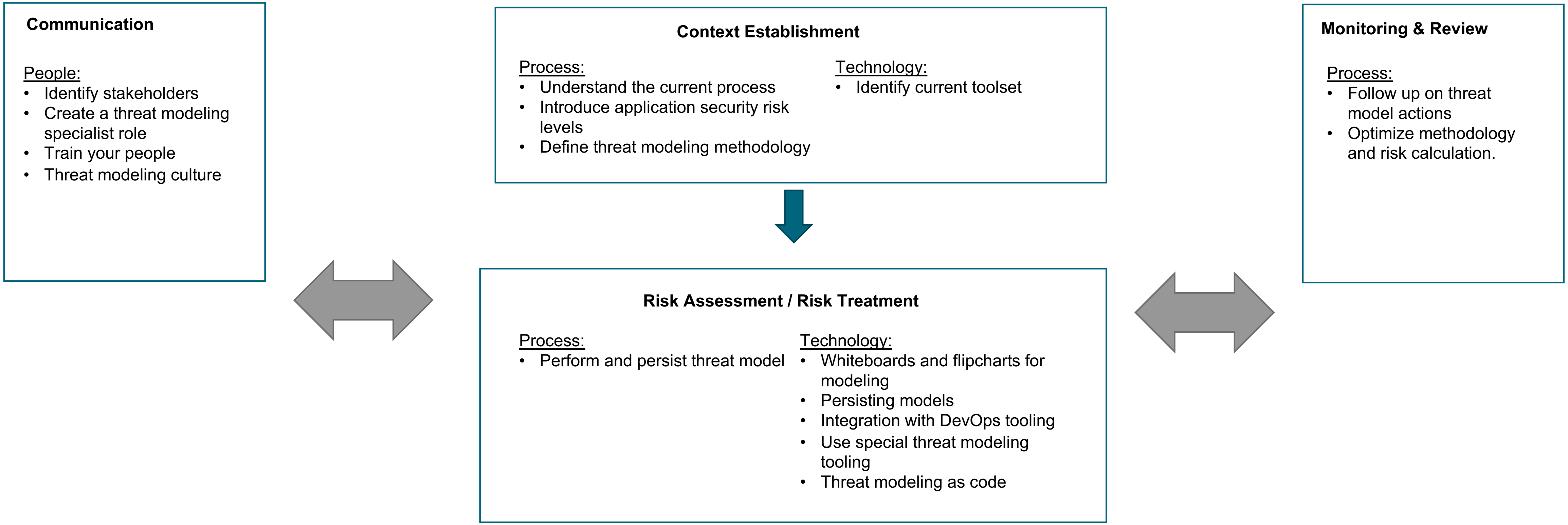
Innovate with TM **technology**

Embed in your organization

- Integrate in your risk management process
- If not available, consider ISO 27005:2018 standard (Information security risk management)
- Link to people, processes and technology framework



PPT framework mapped to ISO 27005



Communication

People:
- Identify stakeholders
- Create a threat modeling specialist role
- Train your people
- Threat modeling culture

Context Establishment

Process:
- Understand the current process
- Introduce application security risk levels
- Define threat modeling methodology

Technology:
- Identify current toolset

Risk Assessment / Risk Treatment

Process:
- Perform and persist threat model

Technology:
- Whiteboards and flipcharts for modeling
- Persisting models
- Integration with DevOps tooling
- Use special threat modeling tooling
- Threat modeling as code

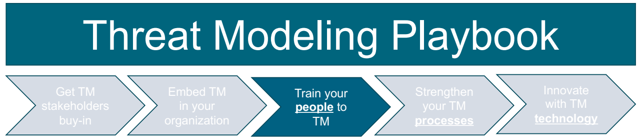
Monitoring & Review

Process:
- Follow up on threat model actions
- Optimize methodology and risk calculation.

OWASP resources

- OWASP SAMM
  - https://owaspsamm.org/model/design/threat-assessment/stream-b/
- OWASP Threat and Safeguard Matrix (TaSM)
  - https://owasp.org/www-project-threat-and-safeguard-matrix/

Train your people to TM



Threat Modeling Playbook

Get TM stakeholders buy-in

Embed TM in your organization

Train your **people** to TM

Strengthen your TM **processes**

Innovate with TM **technology**

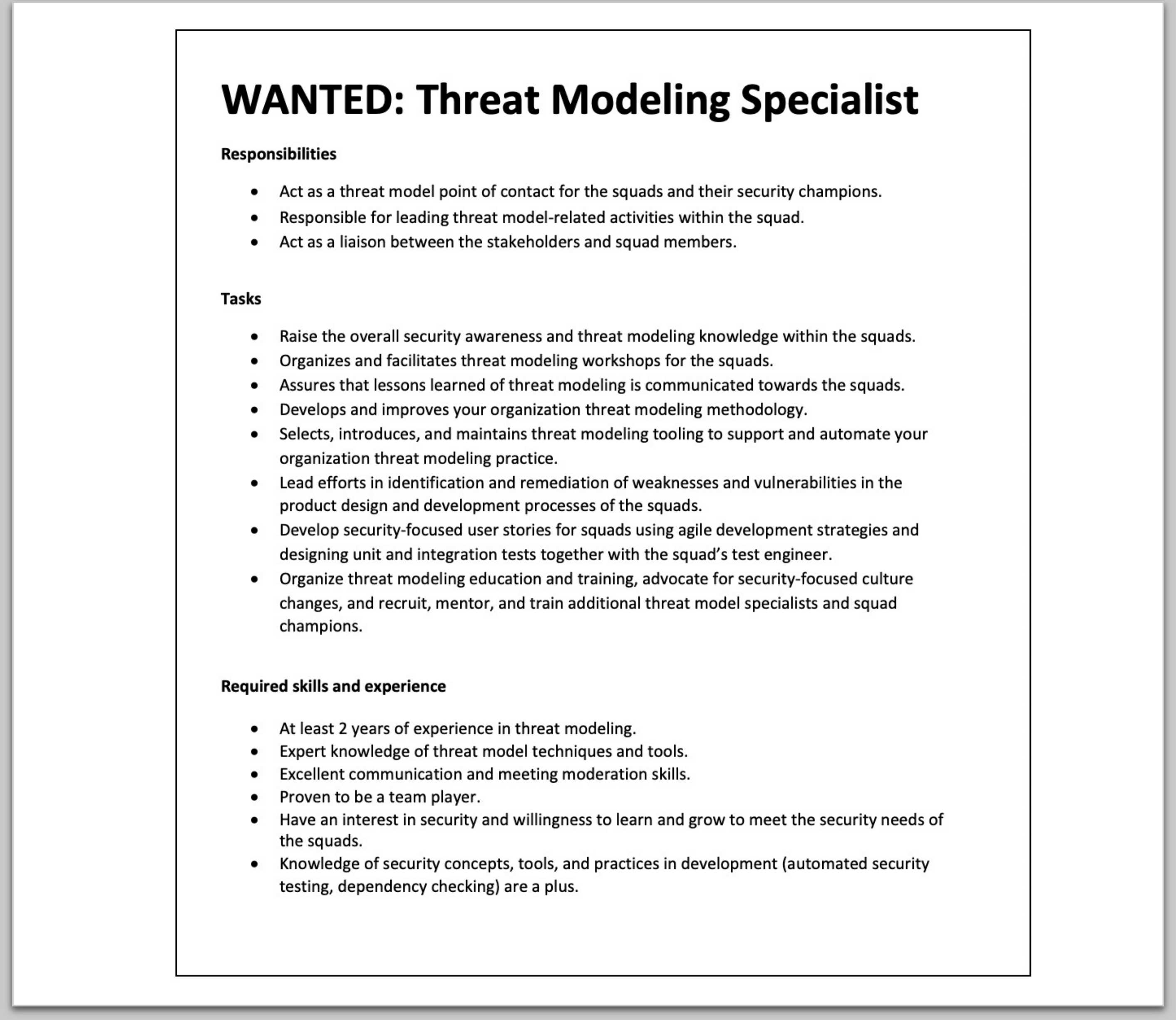
Identify stakeholders

threat modeling is best performed within a core team of limited size

Role	Motivation
Business stakeholder	Ensure that business value and potential business impact is clear.
Architect	Provide a high-level overview of the application ecosystem and the underlying rationale.
Developer	Provide details on used libraries, frameworks, and coding guidelines.
Security and/or DevOps engineer	Provide details on existing security and/or infrastructure configuration.
Project manager	Validate proposed mitigations in terms of timing and budget.
Threat model specialist	Ensure proper execution of the threat model process.

Create a threat modeling specialist role

- Primary purpose: incorporate TM practices and security culture
- Typically floating specialists supporting the squads
- Provide threat modeling advice, support squads, and drop in for a sprint or two
- **Step 1** carve out this role
- **Step 2** hire candidate specialists



WANTED: Threat Modeling Specialist

Responsibilities

- Act as a threat model point of contact for the squads and their security champions.
- Responsible for leading threat model-related activities within the squad.
- Act as a liaison between the stakeholders and squad members.

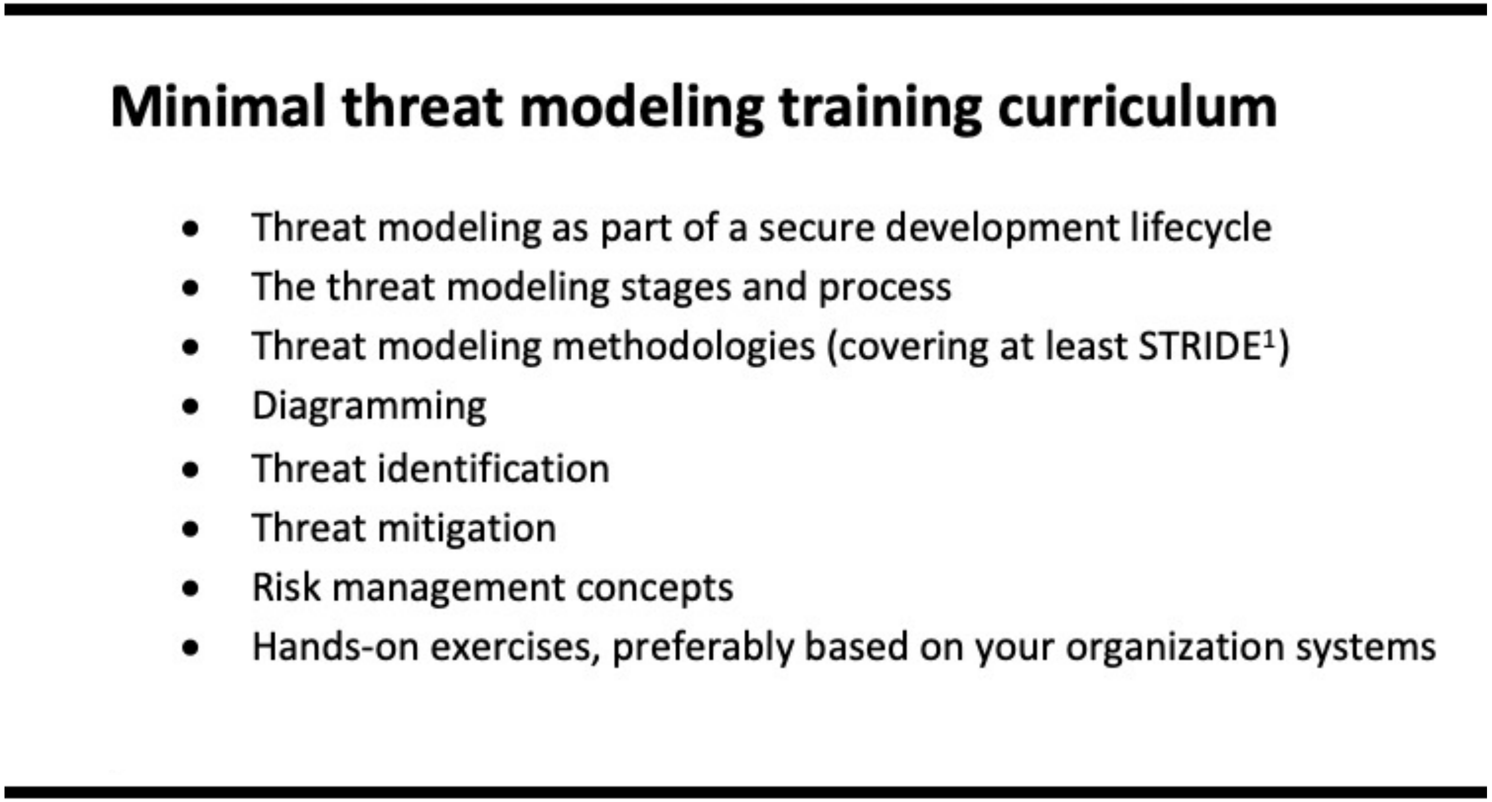
Tasks

- Raise the overall security awareness and threat modeling knowledge within the squads.
- Organizes and facilitates threat modeling workshops for the squads.
- Assures that lessons learned of threat modeling is communicated towards the squads.
- Develops and improves your organization threat modeling methodology.
- Selects, introduces, and maintains threat modeling tooling to support and automate your organization threat modeling practice.
- Lead efforts in identification and remediation of weaknesses and vulnerabilities in the product design and development processes of the squads.
- Develop security-focused user stories for squads using agile development strategies and designing unit and integration tests together with the squad's test engineer.
- Organize threat modeling education and training, advocate for security-focused culture changes, and recruit, mentor, and train additional threat model specialists and squad champions.

Required skills and experience

- At least 2 years of experience in threat modeling.
- Expert knowledge of threat model techniques and tools.
- Excellent communication and meeting moderation skills.
- Proven to be a team player.
- Have an interest in security and willingness to learn and grow to meet the security needs of the squads.
- Knowledge of security concepts, tools, and practices in development (automated security testing, dependency checking) are a plus.

Train your people



Minimal threat modeling training curriculum

- Threat modeling as part of a secure development lifecycle
- The threat modeling stages and process
- Threat modeling methodologies (covering at least STRIDE[1])
- Diagramming
- Threat identification
- Threat mitigation
- Risk management concepts
- Hands-on exercises, preferably based on your organization systems

- Involved staff need to understand the why and how
- Organize lunch & learn sessions for your squads
- Perform threat modeling demos
- Do role-based training
- Include organization specific playbooks and templates, examples, and lessons learned
- Adapt to your technology stack and project governance.

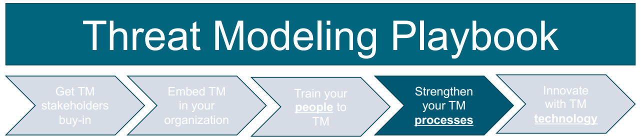
Create a positive threat modeling culture

- Threat modeling is not an audit!
- Assure common understanding of terminology and concepts
- No-blame culture, learn from mistakes
- Leave your ego at the door
- Translate your threat model outcome to the target audience
- Align the team on a shared vision on product security

OWASP resources

- OWASP Threat Model Cookbook
  - https://owasp.org/www-project-threat-model-cookbook/

Strengthen your TM processes



Threat Modeling Playbook

Get TM stakeholders buy-in

Embed TM in your organization

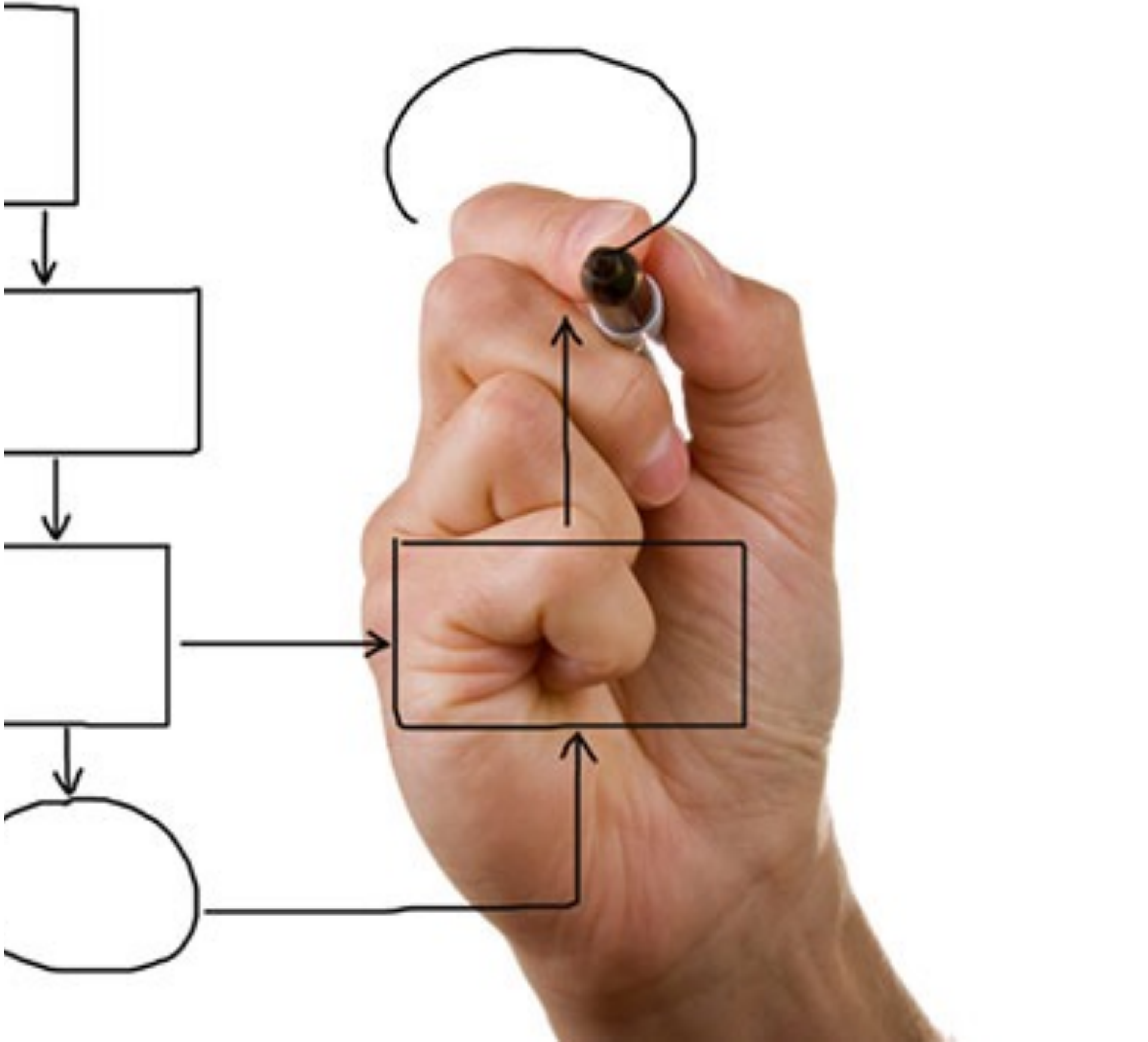
Train your people to TM

Strengthen your TM processes

Innovate with TM technology

Understand your current process

- Align on OWASP SAMM
- What is current process?
    - What?
    - When?
    - Inputs & outputs?
    - Steps taken?
- Draw overview
- Map on this playbook

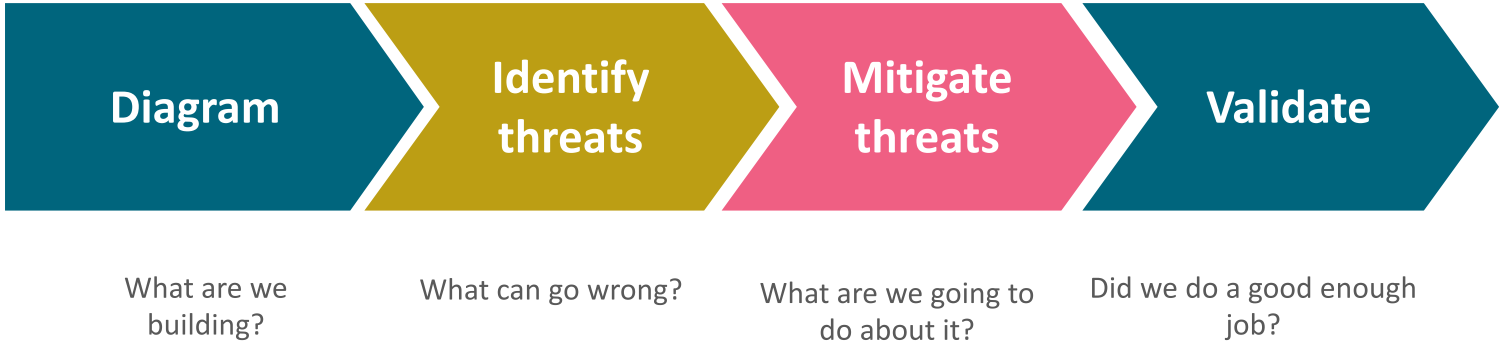


Introduce application risk levels

Order your applications in different risk “buckets”

Choose a threat modeling methodology

- Lots of methodologies available
- Is it sound?
  - Model based
  - Traceable
  - Systematic
  - Business integration
  - Context aware
  - Scalable
- Will it work for you?
- Should at least cover “4 question” framework



Diagram

What are we building?

Identify threats

What can go wrong?

Mitigate threats

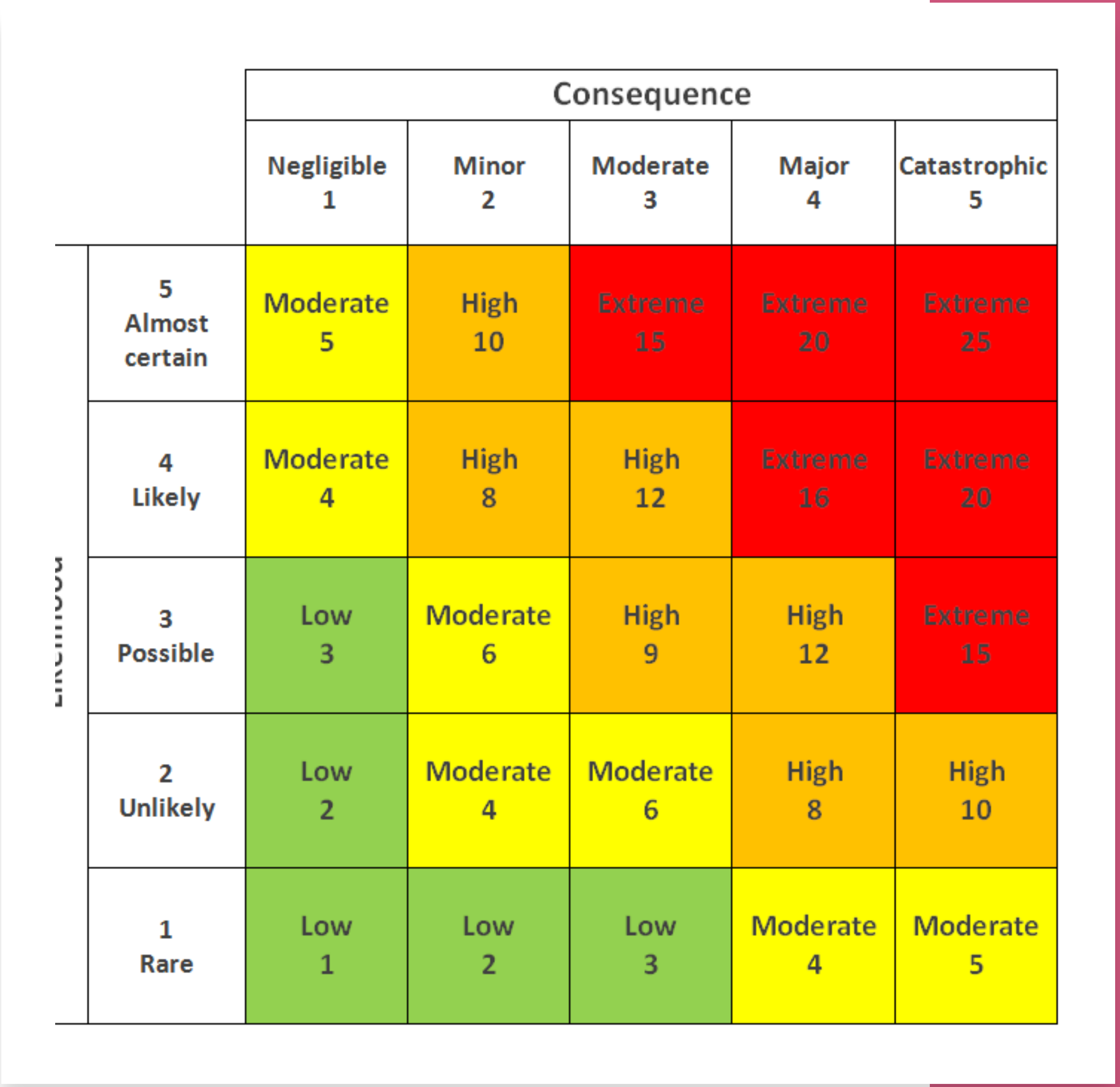
What are we going to do about it?

Validate

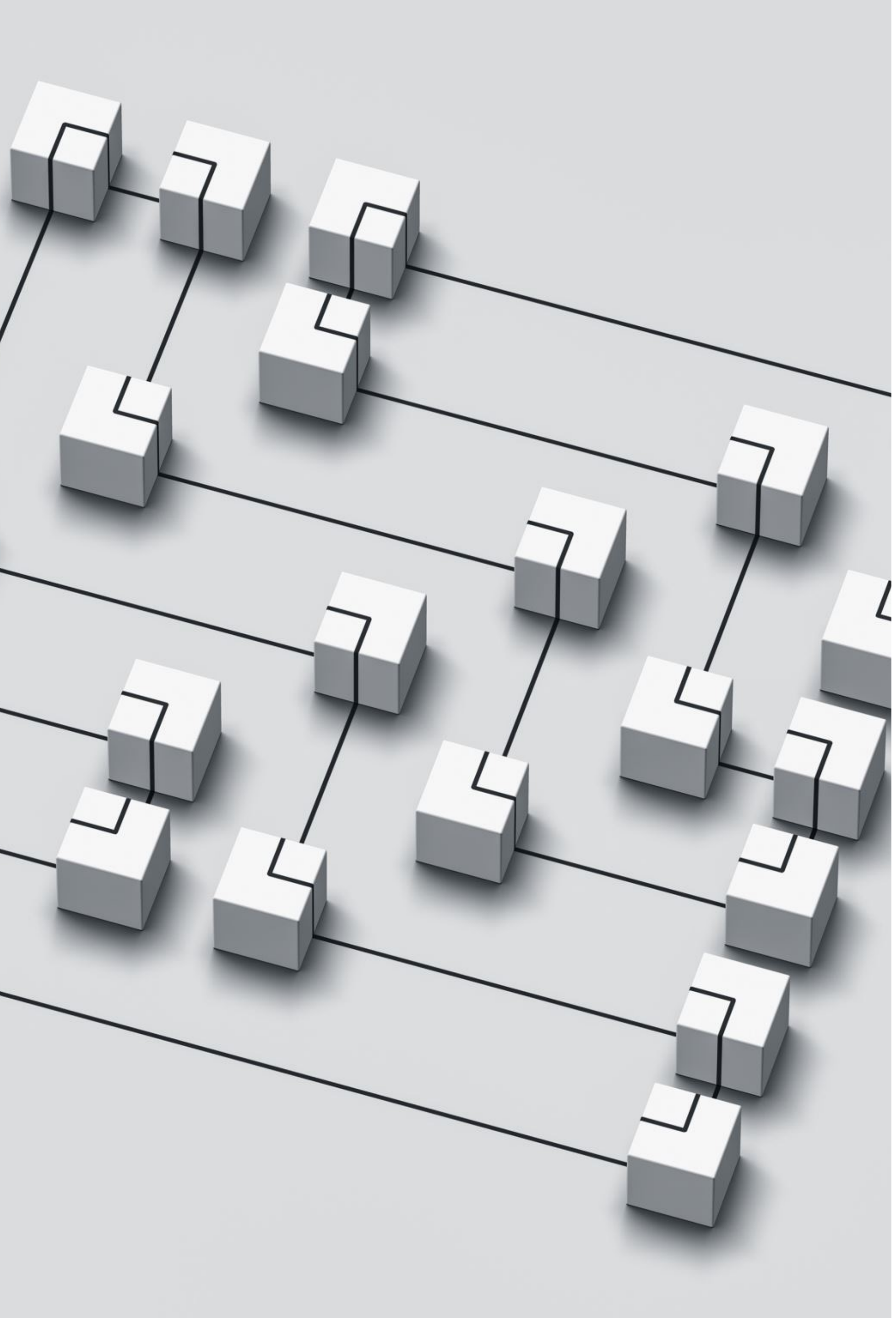
Did we do a good enough job?

Integrate with your risk management framework

- Agree on how to handle TM findings
- Embed in your framework
  (or consider ISO 27005)
- Essential components:
  - Risk levels
  - Risk level implications
  - Risk escalation and acceptance
  - Risk review process



		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5



Perform and persist the threat model

- Once created, persist or store your threat model for later reference
- Threat modeling supporting files: e.g. data flow diagrams, architectural drawings, questionnaires, documentation, meeting minutes or STRIDE analysis …
- Risks identified in the threat model.
    - Stored in the risk register, stored in a bug/user-story system, ...
    - For each identified risk you should include a risk level and the agreed upon follow-up action.

ACTION ITEMS!
TOPIC:
DATE: / /
FINISH BY: / /
TASKS
URGENCY
! !! !!!
NOTES
□ ACTIONS COMPLETED □ ACTIONS DEFERRED □ ALL TALK NO ACTION
"ACTIONS SPEAK LOUDER THAN WORDS"
KNOCKKNOCKSTUFF.COM • © 2016 KNOCK KNOCK LLC

Agree on mitigations and follow-up actions

- Who is accountable for the progress and due date?
- What is the current status of the mitigation?
- What is the risk of the mitigation?
- Who is responsible for the execution / implementation? What are the actions that are needed?
- What is the current state of each of the actions needed to finish this mitigation?

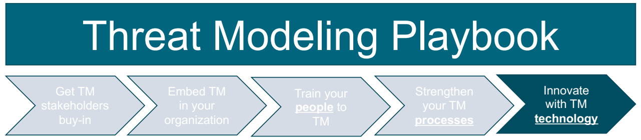
Optimize methodology and risk calculation

- Reuse artefacts: diagrams, risk calculations, user stories
- Hook into and adapt:
    - Penetration testing
    - Compliance needs
    - Audit findings
    - Quality of service levels
- Input to test automation, penetration testing, training, awareness
- Align and standardize risk calculation across teams

OWASP resources

- OWASP Threat Modeling overview
  - https://owasp.org/www-community/Threat_Modeling
- OWASP Threat Modeling process
  - https://owasp.org/www-community/Threat_Modeling_Process
- OWASP Threat Modeling Cheat Sheet
  - https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html
- OWASP Threat Modeling Project
  - https://owasp.org/www-project-threat-model/
- OWASP Risk Rating Methodology
  - https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Innovate with TM technology



Threat Modeling Playbook

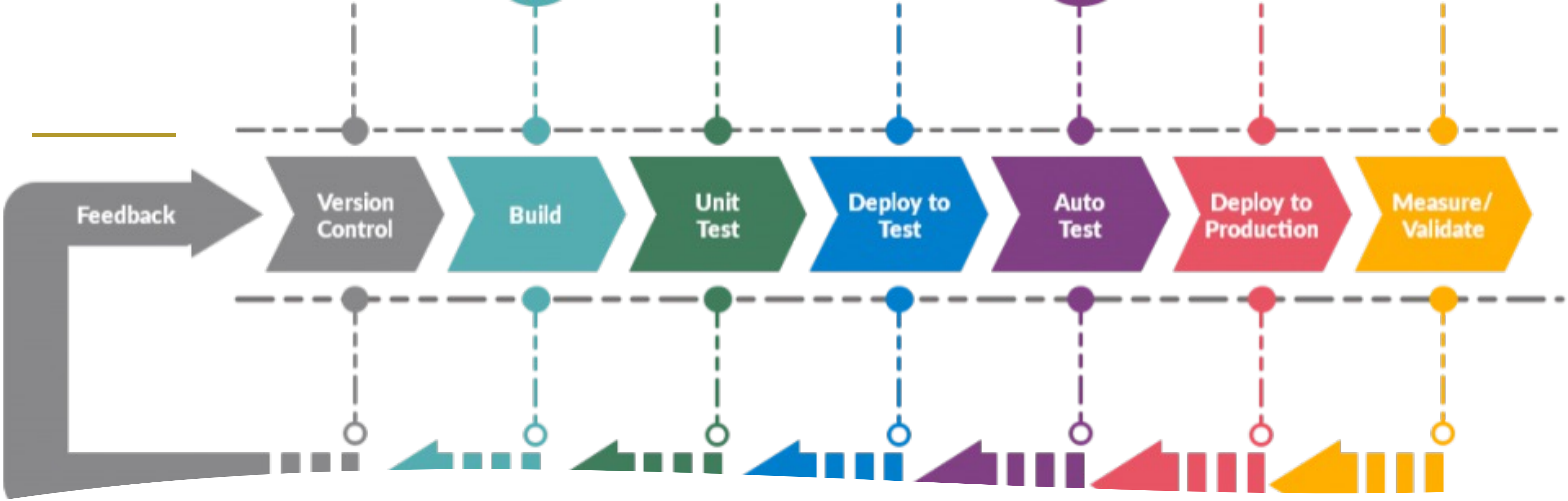
- Get TM stakeholders buy-in
- Embed TM in your organization
- Train your **people** to TM
- Strengthen your TM **processes**
- Innovate with TM **technology**

Select the right tools

- Start with basic tools, such as flipcharts & whiteboards
- Consider remote collaboration tools
- Select threat modeling tool that fits your methodology
- Growing market of open-source and commercial tools

Tool outcomes

- Primary functions and outputs:
    - Create and collaborate on threat models
    - Persist threat models
- Support objective, risk-based approach to mitigate threats
- Cover: awareness, risk documentation, input for other (security) activities, share threat modeling knowledge, …
- Support access control and operational needs



Integrate in YOUR methodology

- Never change your process to accommodate a tool
- Fit your DevOps pipelines:
  - Reuse your team tools
  - Reuse diagrams and diagramming tools
  - Integrate with knowledge repository
  - Track actions in team ticket system
  - Reuse security scoring system
- Consider “threat modeling as code”

OWASP resources

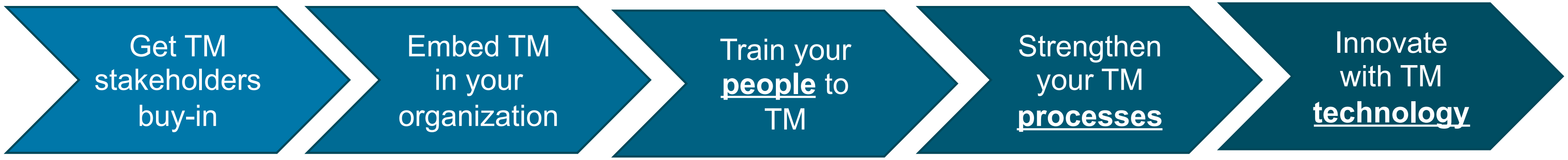
- OWASP Threat Dragon
  - https://owasp.org/www-project-threat-dragon/
- OWASP pytm
  - https://owasp.org/www-project-pytm/
- OWASP Threatspec
  - https://owasp.org/www-project-threatspec/
- OWASP Ontology Driven Threat Modeling Framework
  - https://owasp.org/www-project-ontology-driven-threat-modeling-framework/

TOREON

Open sourcing our playbook

Level up (y)our threat modeling game

Threat Modeling Playbook



Get TM stakeholders buy-in

- Involve people and allocate time
- Inject TM expertise
- Show threat modeling ROI

Embed TM in your organization

- Establish context
- Assess and treat risk
- Monitor and review
- Communicate

Train your **people** to TM

- Identify stakeholders
- Create TM specialist role
- Train your people
- Create a positive TM culture

Strengthen your TM **processes**

- Understand current process
- Introduce application risk levels
- Choose a TM methodology
- Perform and persist the TM
- Integrate with risk framework
- Follow up TM action items
- Optimize methodology and risk calculation

Innovate with TM **technology**

- Select the right tools
- Process the tools outcome
- Integrate in your TM methodology

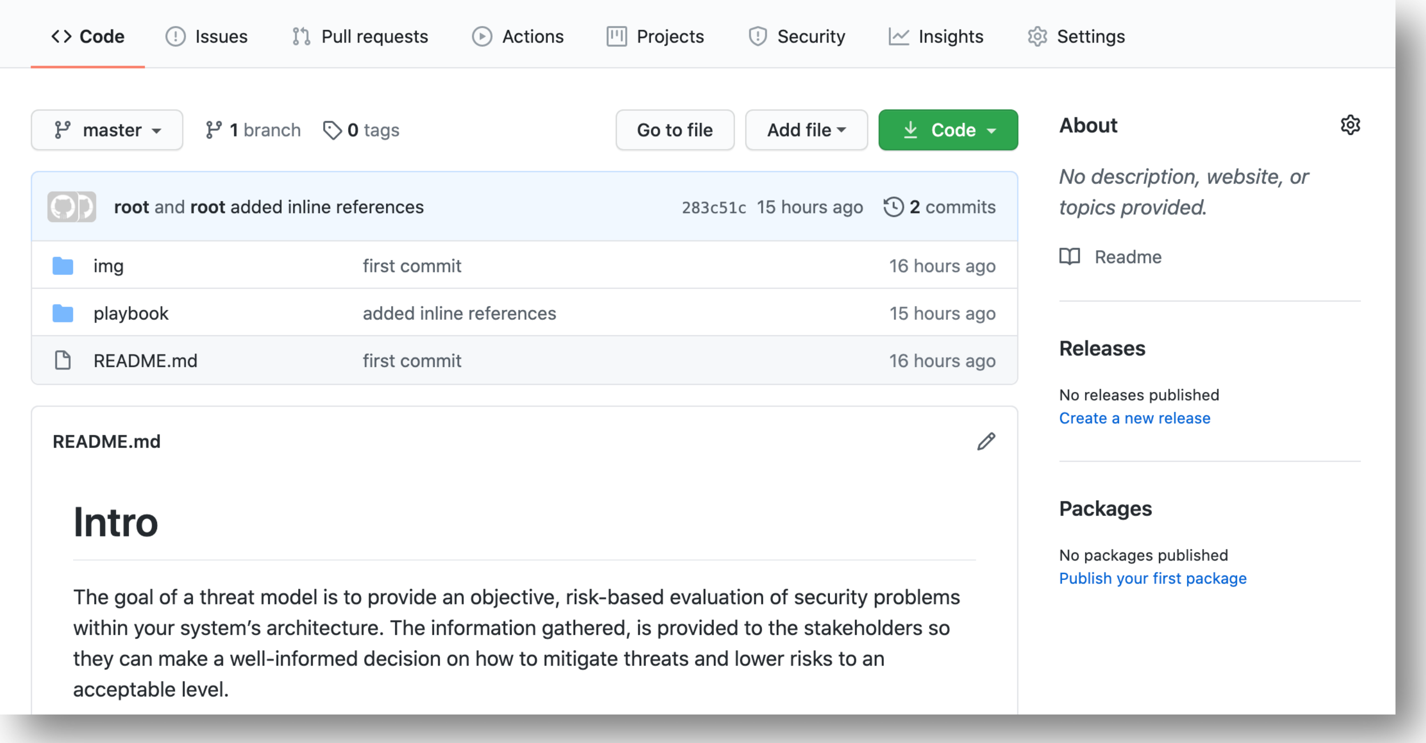
Open sourcing “our” playbook

- Donated to the OWASP threat modeling project
- Free to use!
- Increase the impact of threat modeling globally
- Community feedback, input for next cycle …

https://github.com/OWASP/threat-model-playbook

Demo

- https://github.com/OWASP/threat-model-playbook



root and root added inline references 283c51c 15 hours ago 2 commits

img	first commit	16 hours ago
playbook	added inline references	15 hours ago
README.md	first commit	16 hours ago

No description, website, or topics provided.

No releases published
Create a new release

No packages published
Publish your first package

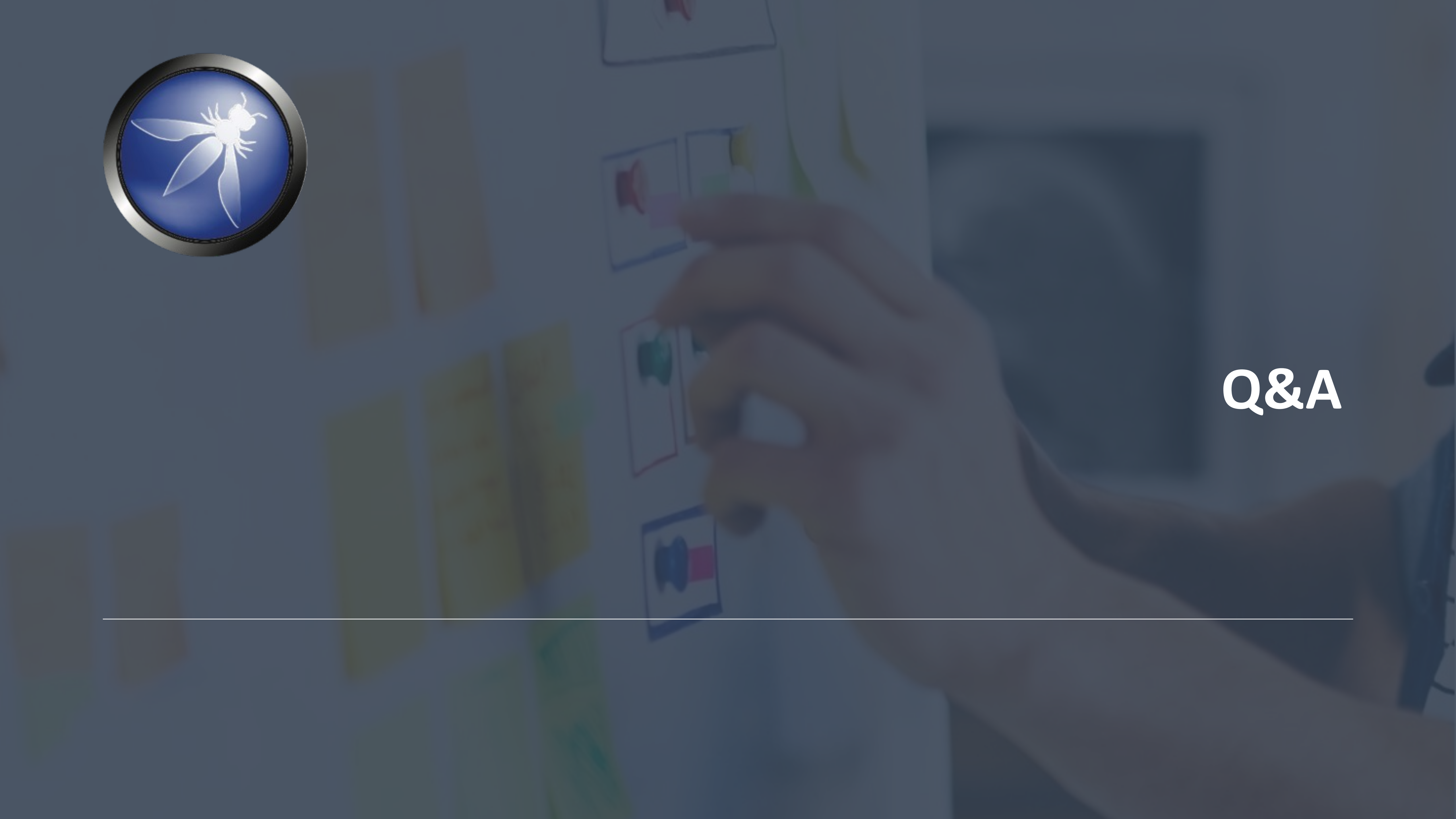
README.md

Intro

The goal of a threat model is to provide an objective, risk-based evaluation of security problems within your system's architecture. The information gathered, is provided to the stakeholders so they can make a well-informed decision on how to mitigate threats and lower risks to an acceptable level.

Call to action

- Download & use it !
- Let us know what works
- Let us know what does not work
- Collaboration on version 2



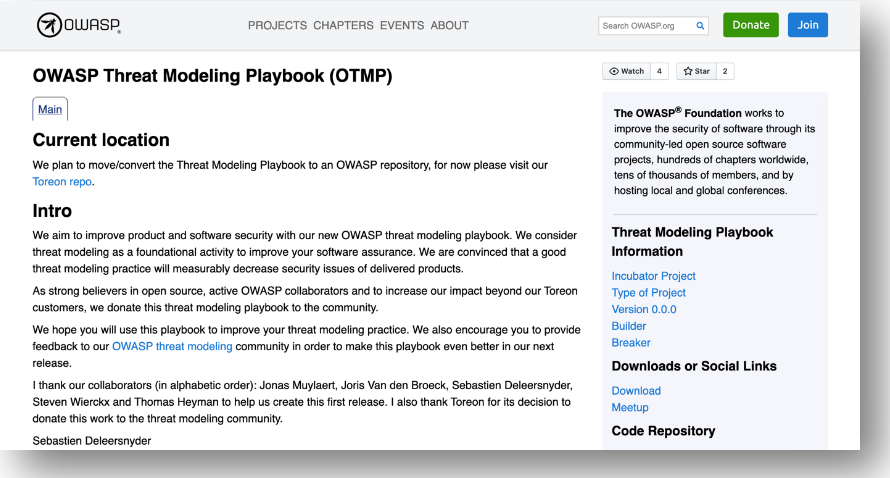
Q&A

Contributors

- Jonas Muylaert
- Joris Van den Broeck
- Sebastien Deleersnyder
- Steven Wierckx
- Thomas Heyman

Online

GitHub



OWASP Threat Modeling Playbook (OTMP)

Current location

We plan to move/convert the Threat Modeling Playbook to an OWASP repository, for now please visit our Toreon repo.

Intro

We aim to improve product and software security with our new OWASP threat modeling playbook. We consider threat modeling as a foundational activity to improve your software assurance. We are convinced that a good threat modeling practice will measurably decrease security issues of delivered products.

As strong believers in open source, active OWASP collaborators and to increase our impact beyond our Toreon customers, we donate this threat modeling playbook to the community.

We hope you will use this playbook to improve your threat modeling practice. We also encourage you to provide feedback to our OWASP threat modeling community in order to make this playbook even better in our next release.

I thank our collaborators (in alphabetic order): Jonas Muylaert, Joris Van den Broeck, Sebastien Deleersnyder, Steven Wierckx and Thomas Heyman to help us create this first release. I also thank Toreon for its decision to donate this work to the threat modeling community.

Sebastien Deleersnyder

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Threat Modeling Playbook Information

Incubator Project
Type of Project
Version 0.0.0
Builder
Breaker

Downloads or Social Links

Download
Meetup

Code Repository

https://github.com/OWASP/threat-model-playbook

https://owasp.org/www-project-threat-modeling-playbook/

Stay in touch!

- Email: seba@owasp.org / seba@toreon.com

- Subscribe to our Threat Modeling Insider "TMI" newsletter: https://www.toreon.com/tmi-threat-modeling/

- Next open trainings:
  - Advanced Whiteboard Hacking – aka Hands-on Threat Modeling (Black Hat USA)
    (2-day training on 6 or 8 August)
  - Threat Modeling Medical Devices training (through DPI)
    (next cohort start on 19-Aug) - https://www.dp-institute.eu/en/courses/threat-modeling-medical-devices/
  - Threat Modeling Practitioner training (through DPI)
    (next cohort start on 12-Sep) - https://www.dp-institute.eu/en/courses/threat-modeling-practitioner-training/

Thank you