



CYBER SECURITY
COALITION.be



APPLICATION SECURITY

EXPERIENCE
SHARING
DAY

15
JUNE

OWASP SAMM Threat Modeling: From Good to Great

Sebastien Deleersnyder, CTO Toreon

Sebastien Deleersnyder

CTO Toreon

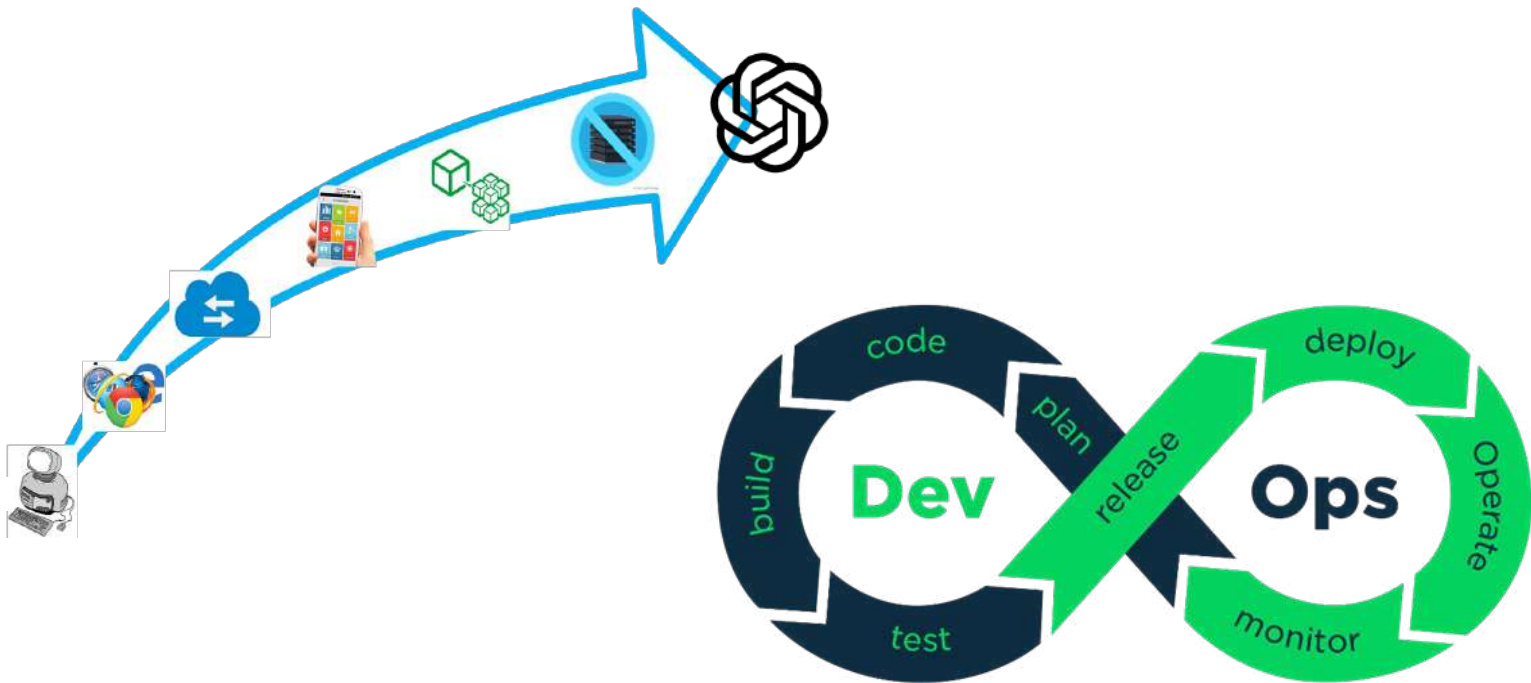
COO Data Protection Institute

OWASP Belgium chapter founder

OWASP SAMM project co-leader



How do we keep up?



Threat modeling is the
activity of identifying and
managing application
risks

Threat modeling – DICE framework



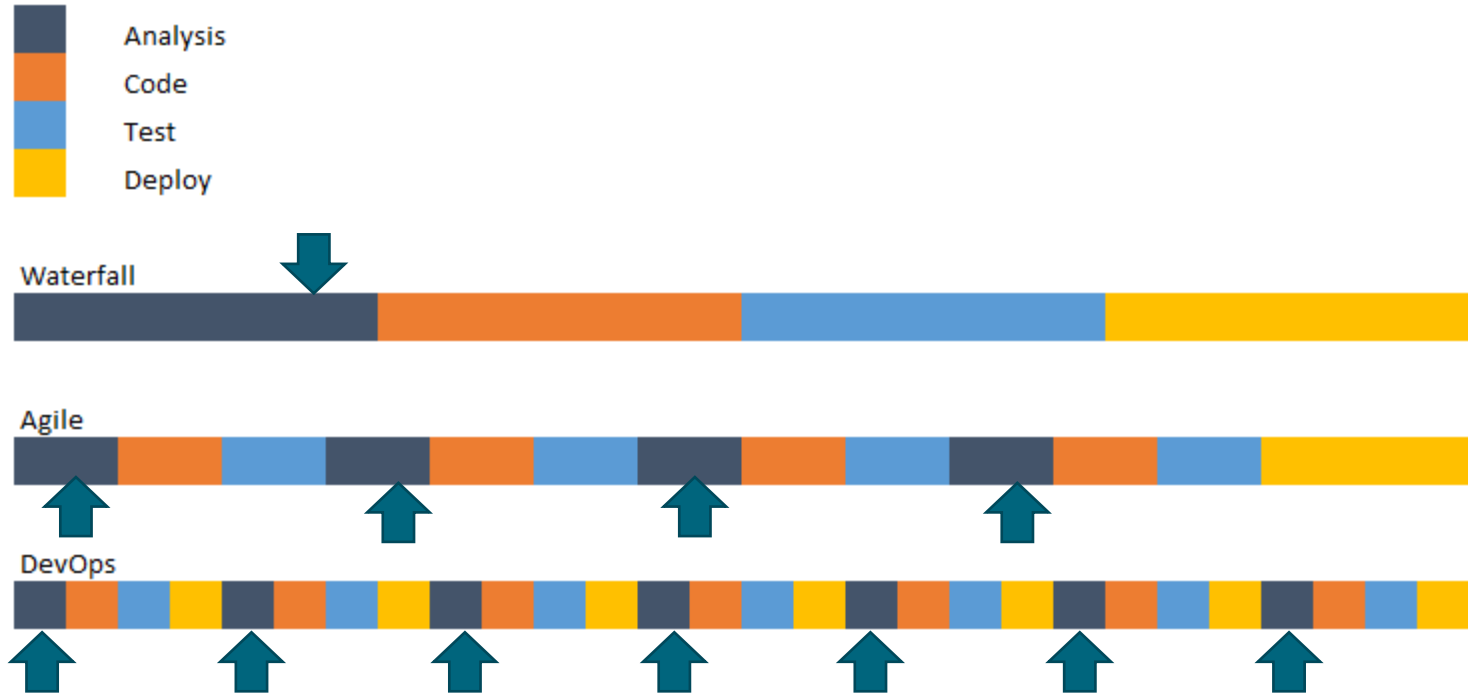
What are we building?

What can go wrong?

What are we going to
do about it?

Did we do a good enough
job?

Timing is everything ...



Advantages

Shared Vision

Flaw Prevention

Risk Identification and Mitigation

Documentation and Compliance

Challenges

Expertise Requirements

Time-Intensive

Scalability Issues

Limited Tool Functionality

SAMM

Software Assurance Maturity Model



Measurable

Defined maturity levels across business practices



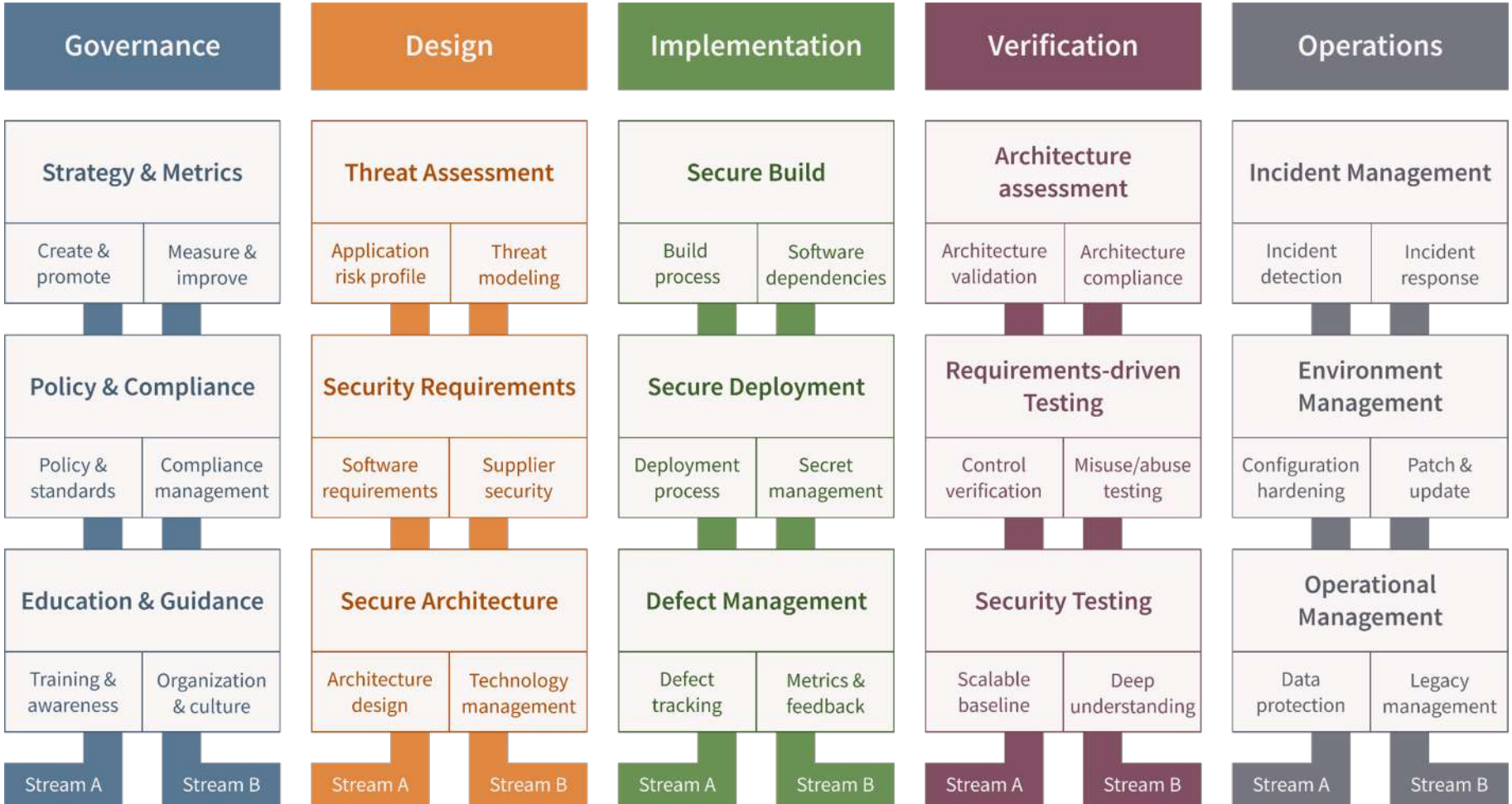
Actionable

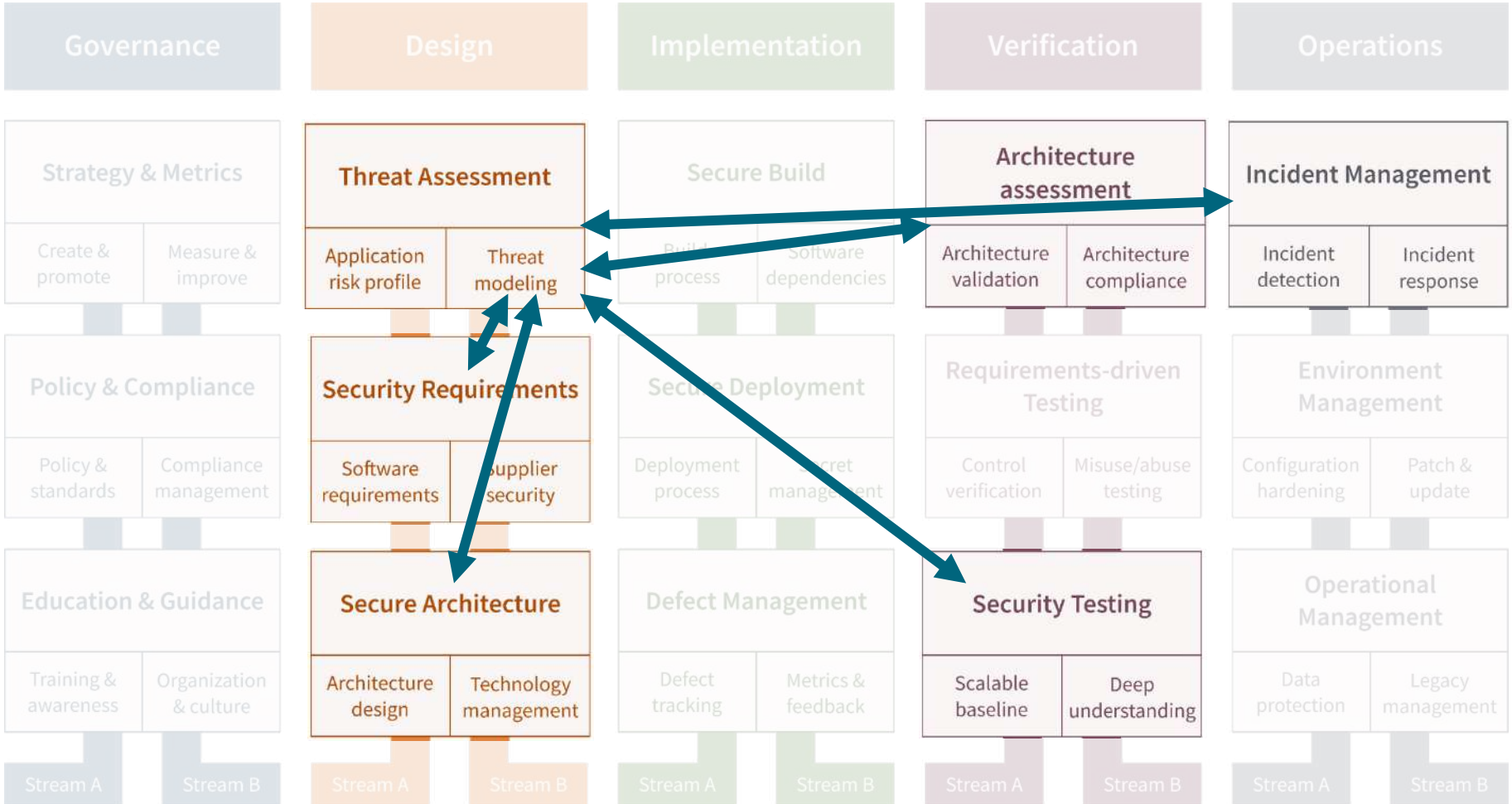
Clear pathways for improving maturity levels



Versatile

Technology, process, and organization agnostic





Fulfilling Practices and improving using 3 successive objectives

- 0 (Implicit starting point with the Practice unfulfilled)
- 1 Initial understanding and ad hoc provision of the Practice
- 2 Increase efficiency or effectiveness of the Practice
- 3 Comprehensive mastery of the Practice at scale

Threat Modeling maturity levels

- 0 No threat modeling
- 1 Best-effort, risk-based threat modeling
- 2 Standardize threat modeling training, processes, and tools
- 3 Continuously optimize and automate threat modeling

Scaling up – outcome alignment

Security controls with risk levels, attacker profiles, risk appetite & assurance levels

Increase awareness and align vision for security and privacy and product teams.



Scaling up – measure success and ROI

Bring value

Justify resources

Prove ROI

1. improving security
2. reducing incidents
3. minimizing delays and rework
4. enhancing assurance and trust



Threat Modeling Program Components

Training

Templates and Patterns

SDL Integration

Governance and Strategy

Community and Culture

Tooling



Training

Provide training tailored to different roles and involvement in threat modeling activities.

Role	Job to be done	(micro) training			
			CPEs self paced training	CPEs in-person training	CPEs 1-1 coaching
C-level / stakeholders	Get on-board with threat modeling	The ROI of threat modeling	1		
Developer	Contribute to threat modeling (input)	TM introduction	2		
Product manager	Responsible for a threat model (business impact and TM owner)	TM intro + basic risk management	3		1
Other stakeholders	Understand threat model (output)	TM introduction	2		
AppSec Champion	Understand when a threat model needs to be created or updated	TM intro + basic threat modeling	2	4	
Threat Modeling Engineer	To be able to create or update a threat model	Threat modeling practitioner	8	12	2
Security officer	To participate in creating or updating a threat model	Threat modeling practitioner	4	8	
Threat Modeling Expert	To be able to customize tool components and risk patterns	Threat modeling tooling expert		8	4

Templates & Patterns

Create & improve:

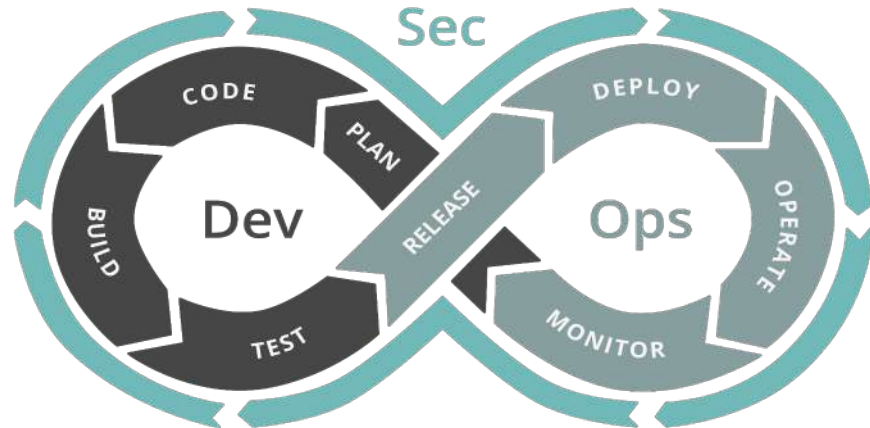
- threat modeling templates
- application risk profiles
- risk patterns (technology, compliance & requirements)

Feed with organization threat intelligence and knowledge

SDL Integration

Strengthen integration threat modeling into SDL

Define hooks into product DevOps process



Governance and Strategy

Establish governance mechanisms

Define strategy

Set Key Performance Indicators (KPIs)

Regularly monitor and report on threat modeling activities.



Community and Culture

Foster a collaborative culture around threat modeling

Organize internal and external sessions with key stakeholders to share knowledge and experiences



Threat Modeling Tooling

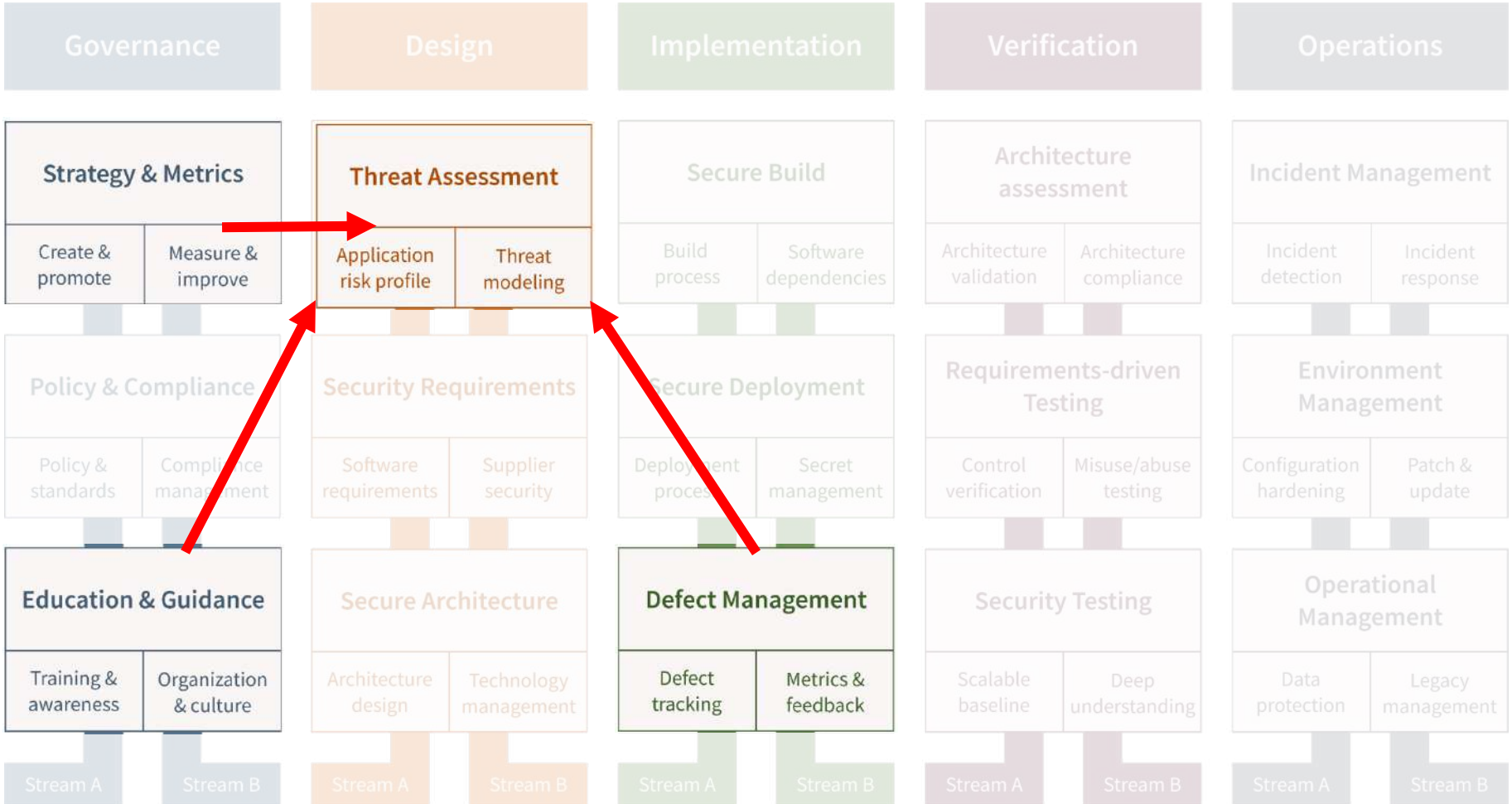
Faster

Automated (DevOps workflows)

More productive

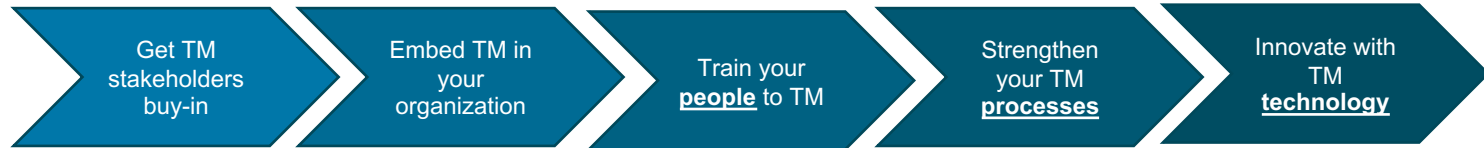
Collaborative





Level up your threat modeling game

Threat Modeling Playbook



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

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

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

- 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

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



Assess Current Situation

Measure the organization's initial threat modeling capabilities and identify areas for improvement.



Determine Target Situation

Define the desired maturity level based on application risk profiles, compliance requirements, and organizational risk appetite.



Create a Roadmap

Develop a roadmap based on the gap analysis between the current and target threat model practices. Prioritize actions and establish timelines for implementation.



Execute and Follow Up

Implement the roadmap, ensuring proper execution of threat modeling activities. Regularly monitor progress and adjust where necessary.



Measure and Demonstrate ROI

Make the output of threat modeling measurable to demonstrate Return on Investment (ROI).

Track improvements in security

Reduced attack surface, reduced vulnerabilities, and increased efficiency (less delays before release).



Resources

OWASP Threat Modeling Playbook (OTMP)

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

OWASP SAMM

owaspsamm.org

Toreon Threat Modeling Insider newsletter

www.toreon.com/tmi-threat-modeling

Q&A

Thank you

Sebastien Deleersnyder

Co-founder, CTO

Toreon

seba@toreon.com

+32 478 504 117

linkedin.com/in/sebadele/