OCT 29
Washington, D.C

THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE

Speaker//

Edouard Stoka

Senior Application Security Architect
ADP

Hosted by
THREAT MODELING CONNECT

THREAT MODCON 2023

CLASSIC/BRAINSTORMING
X
TOOL-BASED

THREATMODELING

LESSONS LEARNED

To achieve that you need the stars to be aligned

In other words :

- Having a large collection of applications threat modeled by experts
- Having access to the best threat modeling tools

Threat Modeling at ADP

Who is ADP

ADP one of the leader in Human Capital Management that unite HR, payroll, talent, time, tax and benefits administration, and a leader in business outsourcing services, analytics and compliance expertise.

The company has more than 1 million clients in 140 countries

HR is specific to each country laws and regulations :

- 1000 products
- 900 software development teams

Threat Modeling in ADP

Threat Modeling at Scale program launched in 2022

Expected outcomes :

- Reduce delays,
- Minimize introduced vulnerabilities,
- Drive increased security efficiency.

Threat Modeling in ADP

Objectives :

- Train the 900 ADP dev teams
- Having the 1000 products threat modeled and regularly updated
- Tracking remediation

Training program developed by ADP Security teams with the contribution of 2 consulting firms and based on STRIDELM

THREAT MODCON 2023

Key success factors for threat modeling adoption in ADP

Threat Modeling in ADP

Key success factors :

- Top-down decision at company level
- Excellent preparation for trainers
- Excellent training content with live and collaborative STRIDELM threat modeling of team’s own applications
- Training content updated monthly
- Remediation tracking

Next step : automated Threat Modeling in ADP

Next step : adopting a threat modeling tool

Why moving towards an automated threat modeling process while the manual one is working ?

- Increasing consistency worldwide.
- Consistent application architecture diagrams.
- Centralized remediation tracking.
- Automated reporting system.
- Helping the AppSec governance.

Selection of the threat modeling tool

The project started in October 2022

120+ evaluation criteria regrouped in 10 categories including :

- Access Management
- Product On-Boarding
- Methodologies
- Threats frameworks

This leaded to a short-list of 3 tools : diagram based, and survey based

Finalize the choice

The scores of the 3 short-listed tools were too close to finalize a decision.

The solution : additional criteria :

- Users feedbacks and detailed evaluations after live hands-on sessions
- Pushing the tools to the limits : threat engines and noise comparison

The impact of noise

The impact of noise

Tools catch a lot more vulnerabilities than humans do : focus on the noise.

Noisy crickets : they identify 100% of true positive but with an excessive false positive rate.

Quiet crickets : are the opposite

THREAT MODCON 2023

The impact of noise

Contrary to code scanning, manual threat modeling is the main option and noise can be a deal breaker

Contrary to code scanning with OWASP benchmark, there is not such a thing in threat modeling.

Tools evaluation is only based on manual testing.

The impact of noise

This also allows to understand the mechanisms of the threat engines behind each tool by pushing them to the limits.

Key takeaways for noise :

- How effective is the threat engine in taking into account specific architecture patterns
- How easy it is to customize threats rules to limit false positives
- Are there any hidden assumptions/questions and can they be easily unlocked/modified (e.g. : data assumption for GDPR)
- How easy it is to manage false positives in the tool when they occur

Key success factors for threat modeling tool adoption

Key success factors for threat modeling tool at scale

User friendliness :

- Is the tool easy to use ?
- Is it possible to use templates

THREAT MODCON 2023

Key success factors for threat modeling tool at scale

Ramp-up:

If the tool is rich/complex, is it possible to have a multi-stage maturity level?

- A first level of simple features
- A second level with the whole package of features

THREAT MODCON 2023

Key success factors for threat modeling tool at scale

Easiness to manage False-Positive :

Each tool identifies false positives.
How easy is the false positive management ?

What about the vulnerabilities that humans catch, and tools don’t ?

Are there vulnerabilities that humans catch, and tools don’t ? Of course !

Evaluation methodology :

- Dozen of ADP applications manually threat modeled
- 132 associated vulnerabilities
- Threat model these applications in the 3 short-listed tools
- Analyzing each list of threats generated by the 3 tools to see which of these 132 vulnerabilities are caught by at least one of the 3 tools

The results

- 36% of the 132 vulnerabilities caught by humans are invisible to leading threat modeling tools
- Most of these vulnerabilities are business abuse cases

My own conclusion*

- Automated threat modeling has several advantages when selecting the right tool, the most important ones :
  - Bringing consistency
  - Centralized tracking
  - Helping the AppSec governance
- Manual threat modeling should be done for the most critical applications in addition to the automated one.

* : these views are my own and not these of my employer

THREAT MODCON 2023

Questions ?

THREAT MODCON 2023

Thank you

THREAT MODELING CONNECT

THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE