German OWASP Day 2024

GenAI for Threat Modeling

CLEMENS HÜBNER | inovex GmbH

Clemens Hübner

Software Security Engineer @ inovex

Enables building secure applications

Developer, Consultant, Speaker, Trainer

- @ClemensHuebner
- clemens.huebner@inovex.de
- @clemens@infosec.exchange
- /clemens-huebner
- @inovexlife
- blog.inovex.de

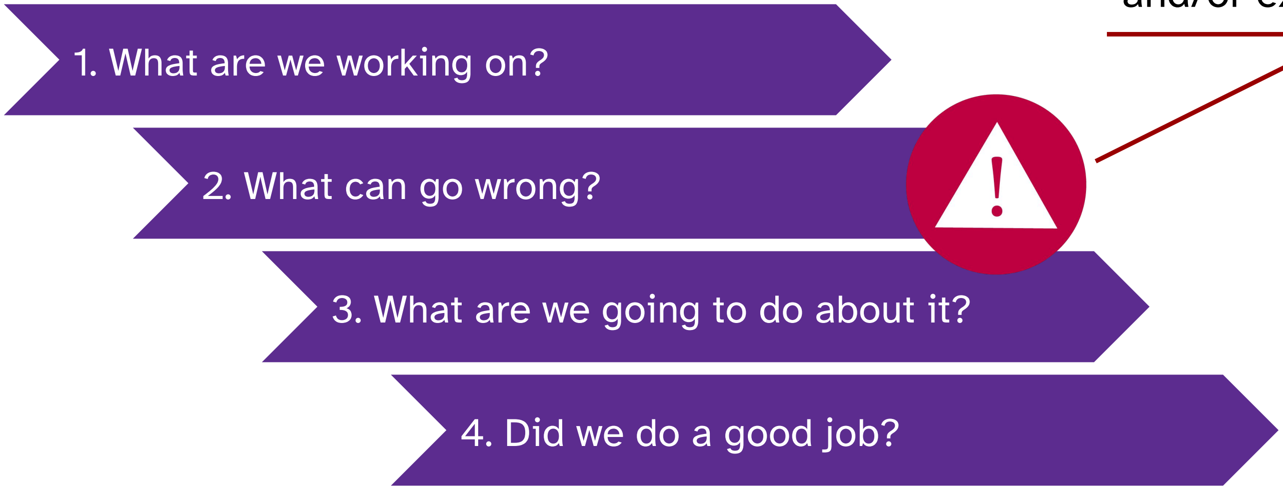
inovex

Threat Modeling

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

Shostack’s 4 Question Framework for Threat Modeling

Threat Modeling: The bottleneck

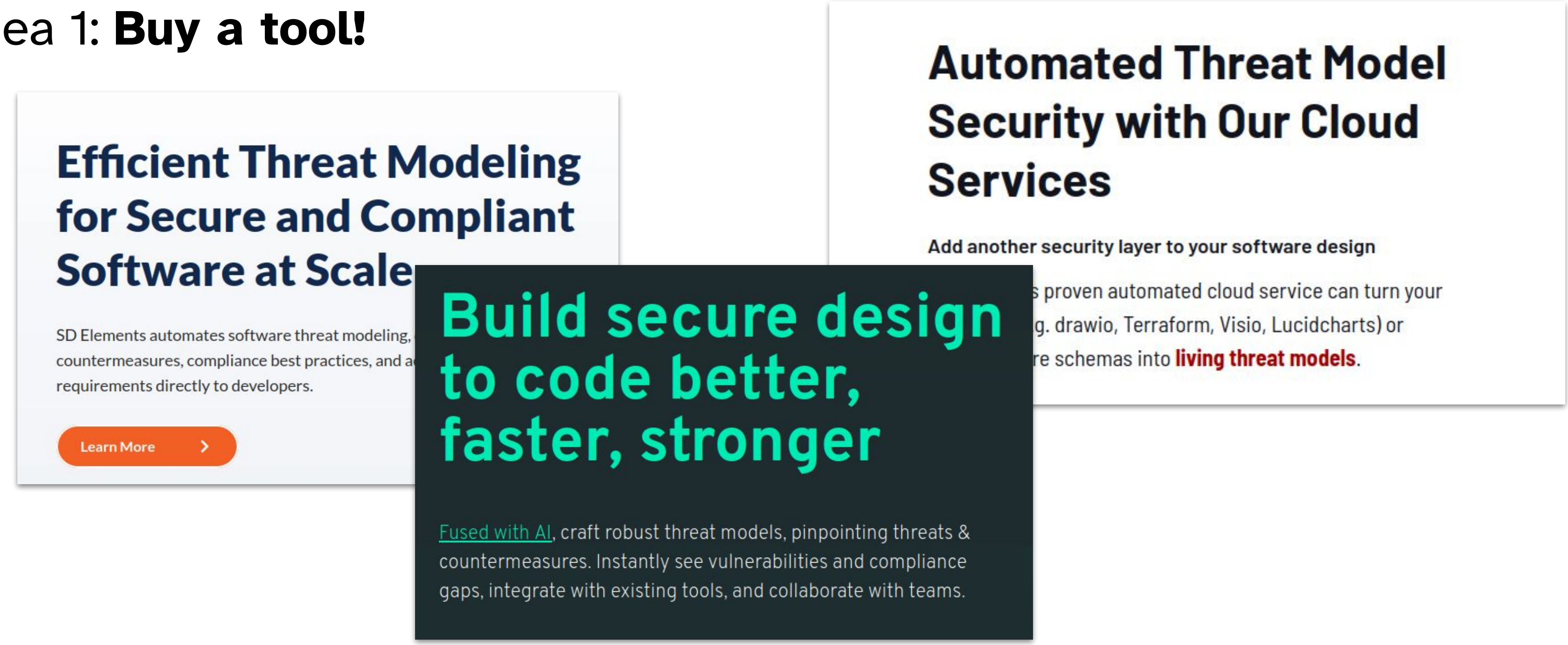


1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

Identification of threats
requires expertise
and/or experience

Support for inexperienced teams

Idea 1: **Buy a tool!**



Efficient Threat Modeling for Secure and Compliant Software at Scale

SD Elements automates software threat modeling, countermeasures, compliance best practices, and a requirements directly to developers.

Automated Threat Model Security with Our Cloud Services

Add another security layer to your software design

s proven automated cloud service can turn your g. drawio, Terraform, Visio, Lucidcharts) or re schemas into **living threat models**.

Build secure design to code better, faster, stronger

Fused with AI, craft robust threat models, pinpointing threats & countermeasures. Instantly see vulnerabilities and compliance gaps, integrate with existing tools, and collaborate with teams.

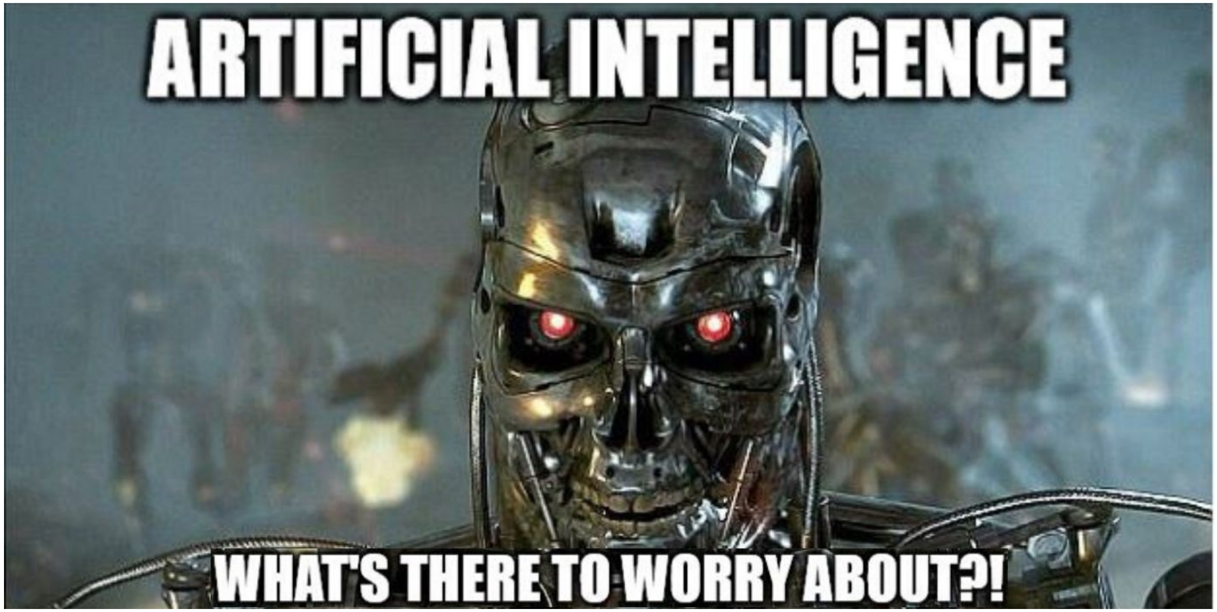
Support for inexperienced teams

Idea 2: **Gamification**

elevation of privilege
logs = 0
Denial of Service
An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10:1.
A Threat Modeling Card Game
CONTROLE DE ACESSOS
AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS
GERENCIAMENTO DE SESSÕES
PRÁTICAS DE CRIPTOGRAFIA
Missing resource limits
Broad delete permissions
We can have the same person deleting resources and their backups.

Support for inexperienced teams

Idea 3: ✨ **AI** ✨



AI support for Threat Modeling

What we do not want:

- Tool for experts
- Generation of complete threat model based on all available documentation
- Omniscient black box

What we do want:

- Usable for development teams
- Support during threat modeling session maintaining its communicative character
- Interactive access to knowledge base

Introducing: inovexGTA

GTA - GenAI Threat Assistant

- Chatbot for threat modeling sessions
- Based on Azure OpenAI, built with Chainlit
- Predefined prompts for four use cases

Security Architecture Interview

Threat Elicitation

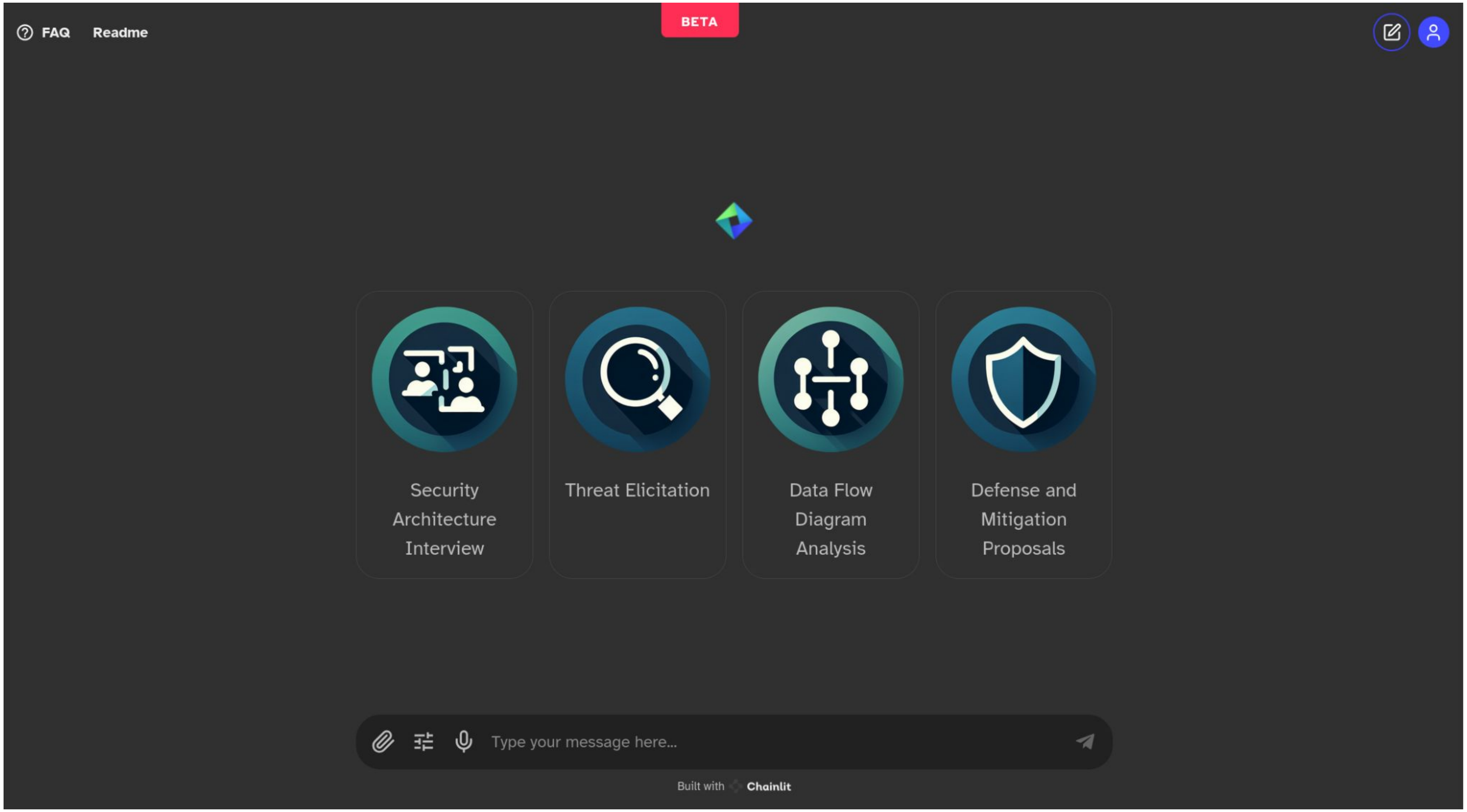
Data Flow Diagram Analysis

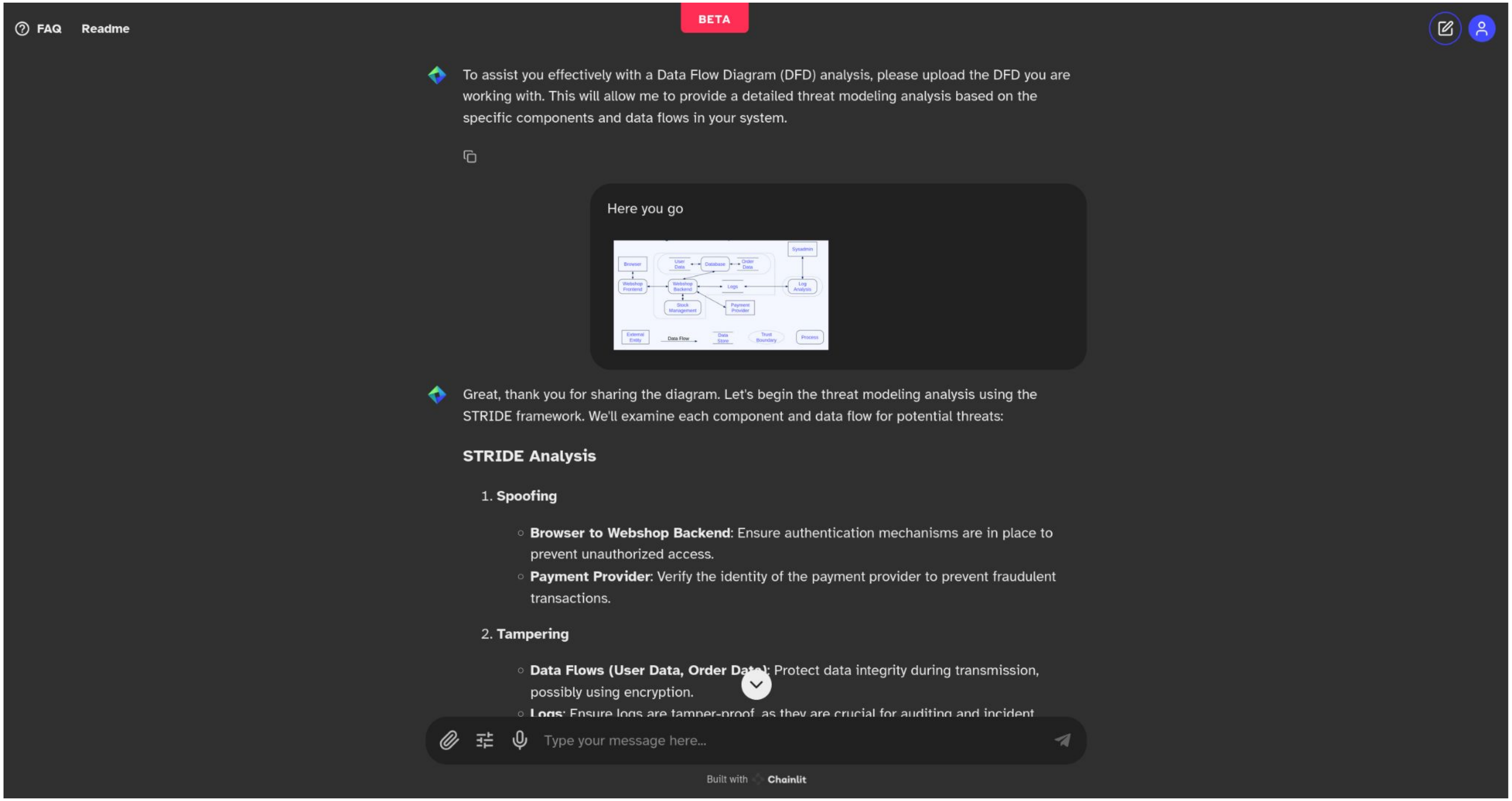
Defense and Mitigation Proposals

German OWASP Day 2024

DEMO

GenAI Threat Assistant


FAQ
Readme
BETA
Security Architecture Interview
Threat Elicitation
Data Flow Diagram Analysis
Defense and Mitigation Proposals
Type your message here...
Built with Chainlit



To assist you effectively with a Data Flow Diagram (DFD) analysis, please upload the DFD you are working with. This will allow me to provide a detailed threat modeling analysis based on the specific components and data flows in your system.

Here you go

Great, thank you for sharing the diagram. Let's begin the threat modeling analysis using the STRIDE framework. We'll examine each component and data flow for potential threats:

STRIDE Analysis

1. **Spoofing**
    - **Browser to Webshop Backend**: Ensure authentication mechanisms are in place to prevent unauthorized access.
    - **Payment Provider**: Verify the identity of the payment provider to prevent fraudulent transactions.
2. **Tampering**
    - **Data Flows (User Data, Order Data)**: Protect data integrity during transmission, possibly using encryption.
    - **Logs**: Ensure logs are tamper-proof, as they are crucial for auditing and incident

Evaluation and future ideas

Experience with the PoC

+ Easy access for teams to pre-engineered prompts
+ Fitting conversations with helpful proposals

- Missing understanding for unusual, domain-specific threats
- Lengthy initial startup

In the future

- Fine-tune prompts, add new use cases
- Improve graphic modelling and understanding

Blogpost

Threat Modelling
with LLM support

German
OWASP
Day 2024

THANK YOU!

@ClemensHuebner

clemens.huebner@inovex.de

@clemens@infosec.exchange

/clemens-huebner