Thurs May 11th, 2023 - INCOSE Canada

Cybersecurity Modeling in SPARX Enterprise Architect

Bob Hruska

Head of Cybersecurity Modeling

Build a security culture…

… save money and reputation

Bob Hruska

- OMG Certified UML® Professional™
- 20+ years’ experience in software and systems engineering in several industries
- Experienced in the Capability Maturity Model Integration (CMMI) appraisal journey and with the development of the New Product Introduction (NPI) process.
- Contributing to the institutionalization of cybersecurity as a part of a system development lifecycle.

SPARX SERVICES CENTRAL EUROPE

LIEBER.GROUP PORTFOLIO

SPARX SYSTEMS CENTRAL EUROPE

Distributor of SparxSystems in Europe

EA Training
(Tool, Language, Method, Best Practices)

EA Coaching
(Tool, Language, Method, Best Practices)

SPARX SERVICES CENTRAL EUROPE

Tool Coaching

Project Coaching

LieberLieber

Software for safety-critical modeling

Product developer
Product owner

LL Products Training
(Tool, Language, Method, Best Practices)

Coaching
(Tool, Language, Method, Best Practices)

Project Coaching

THREATGET

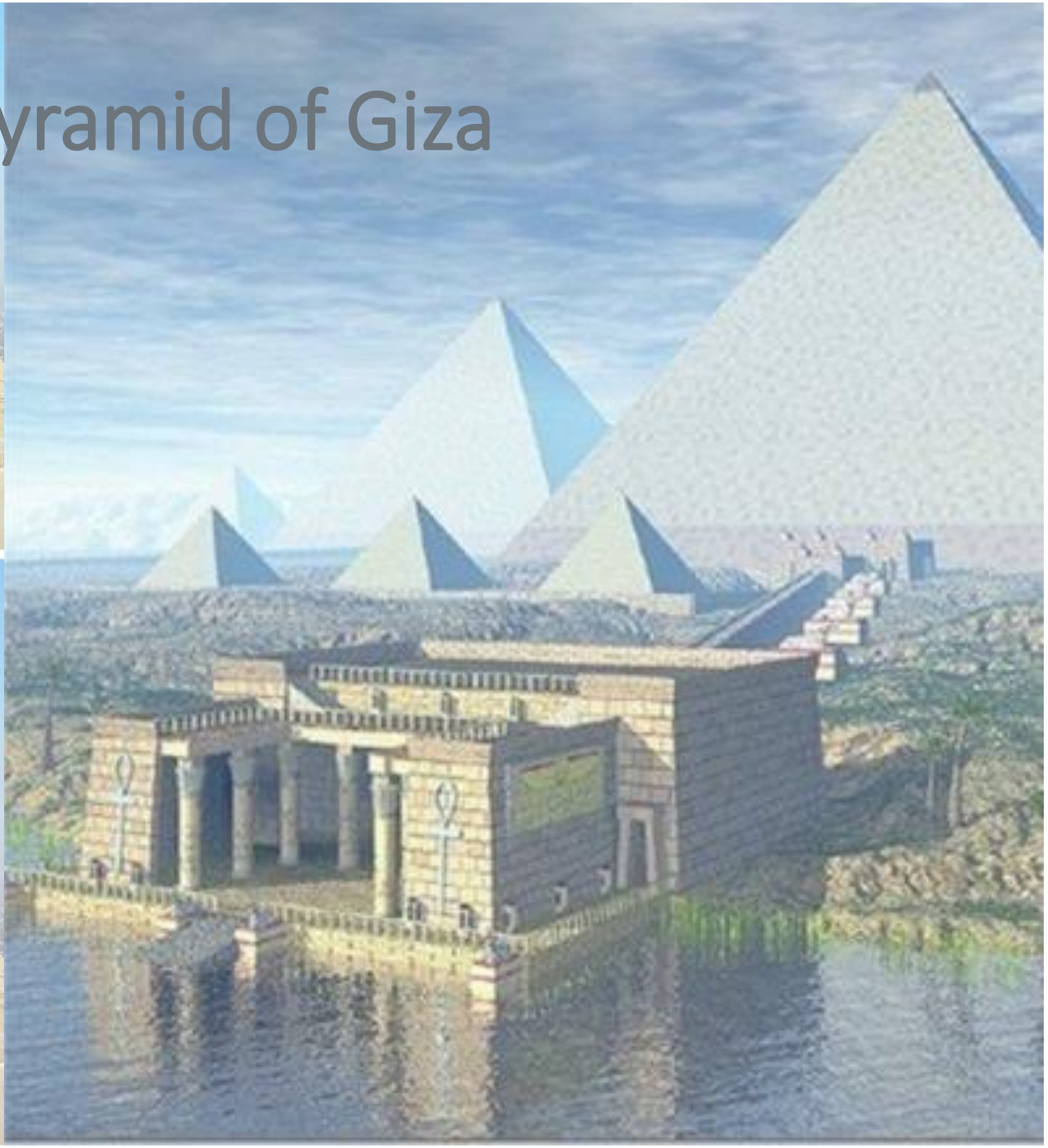
Distributor of „Cyber Security by Design“

Partner distribution

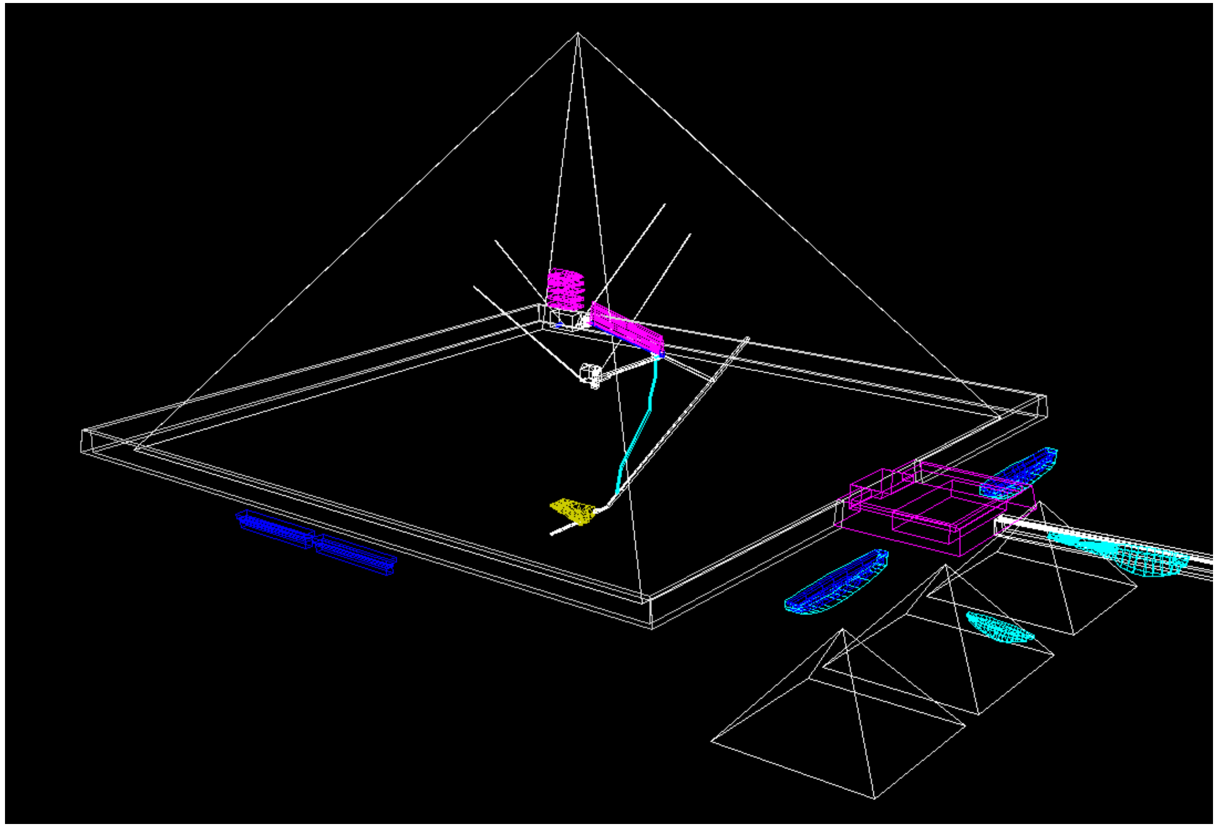
Let’s talk about:

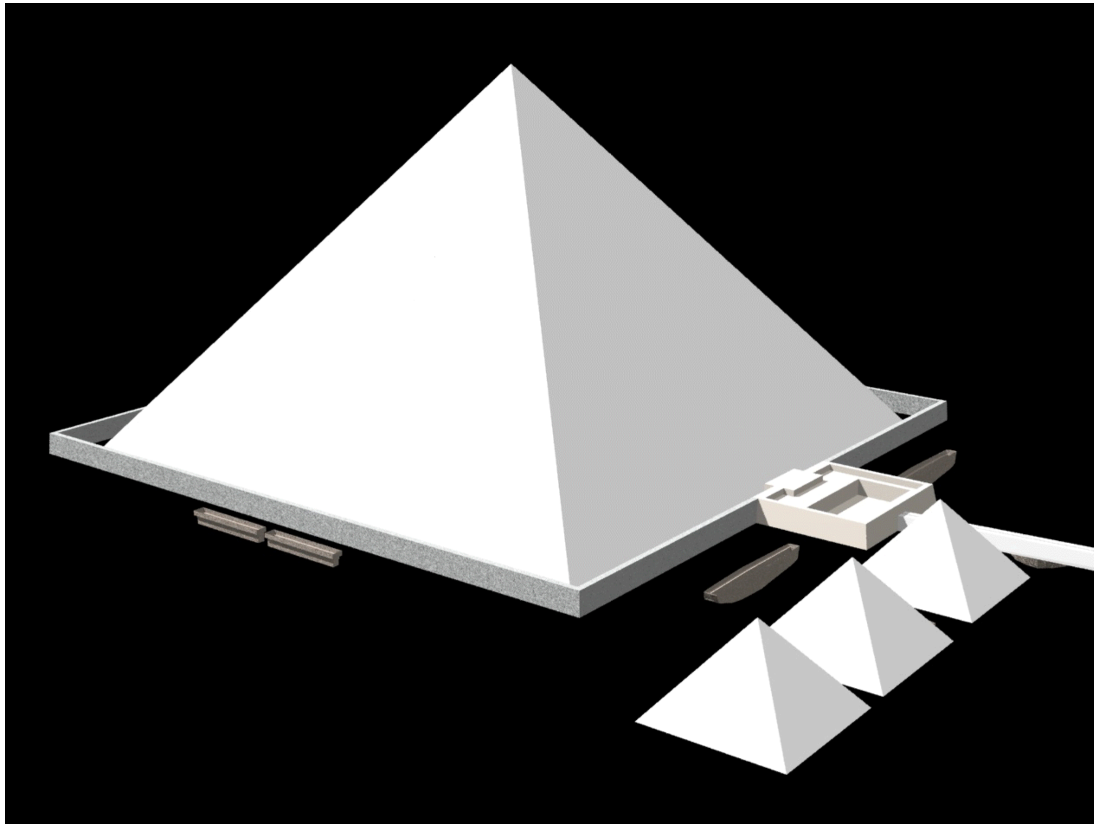
- What’s the essential prerequisite for modeling cybersecurity threats?
- What’s threat modeling?
- Learn about security challenges in system development
- Modeling threats using Enterprise Architect
- Analyzing, visualizing and communicating the threat model to all stakeholders

The Great Pyramid of Giza



There is no evidence, no ancient plans…



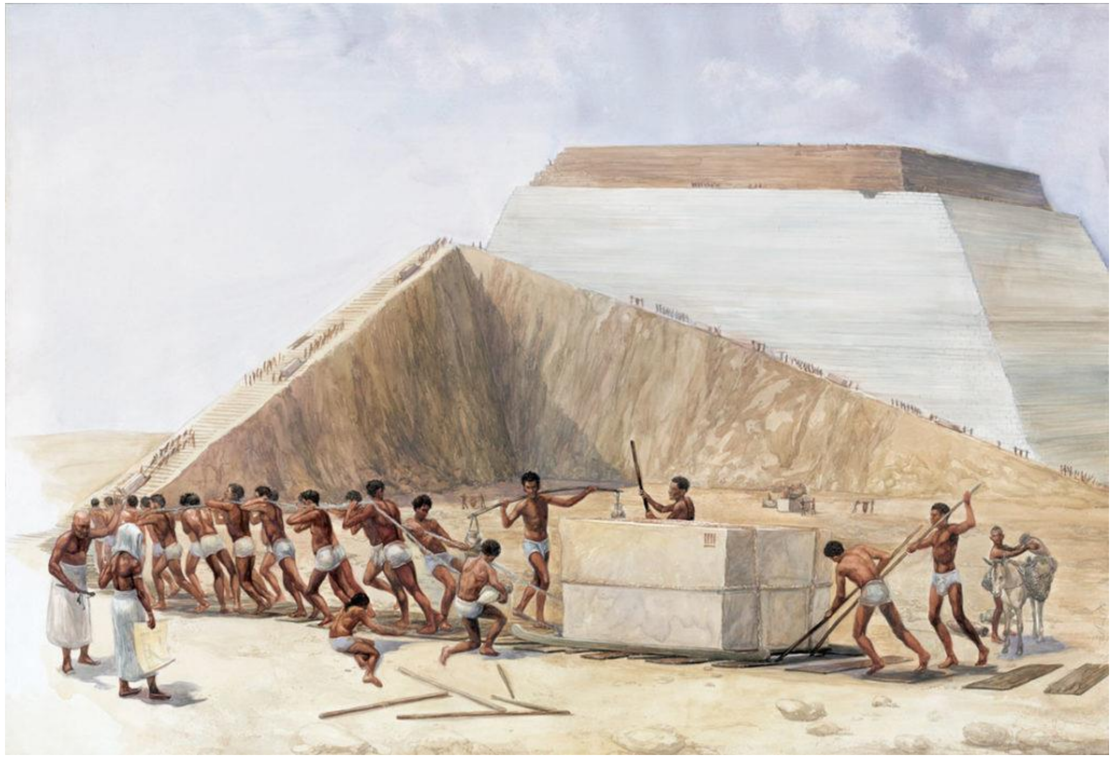


Giza Plateau Computer Model - University of Chicago

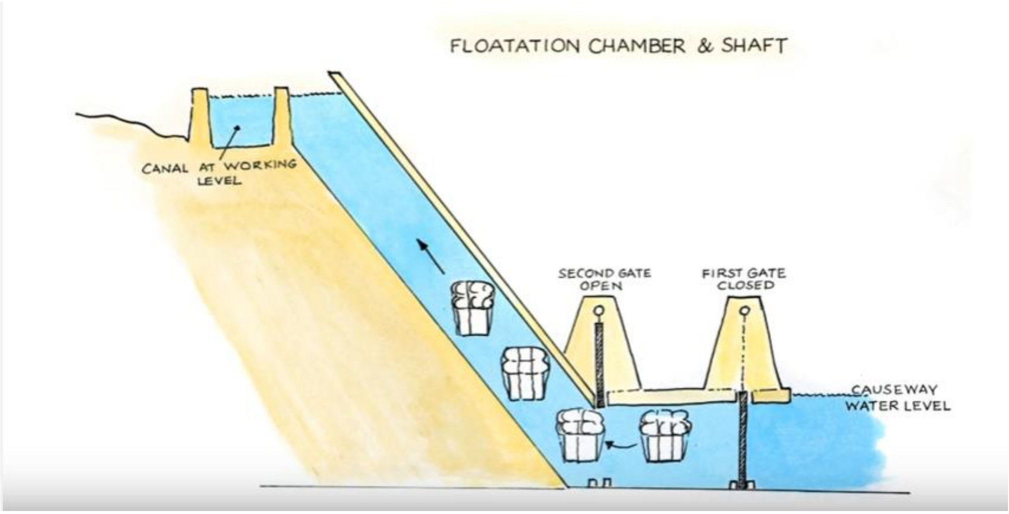
SPARX SERVICES CENTRAL EUROPE

How were the Pyramids built then?

- The Ramp Theory



- The Water Shaft Theory

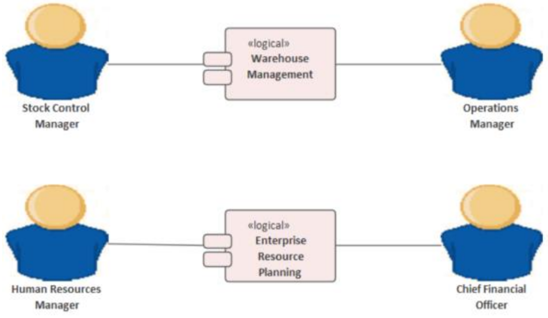


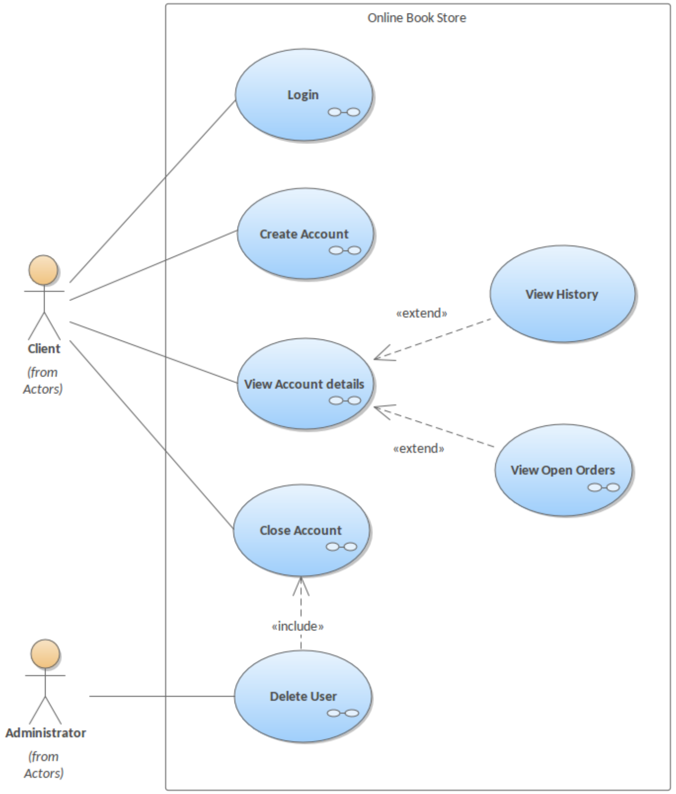
Source: https://www.contiki.com/six-two/how-were-the-egyptian-pyramids-built/

The oldest architectural plan

- Discovered in Iraq and dating back to the Mesopotamia civilization (8000-2000 B.C.)

4000 years and we’re back to the same language ☺

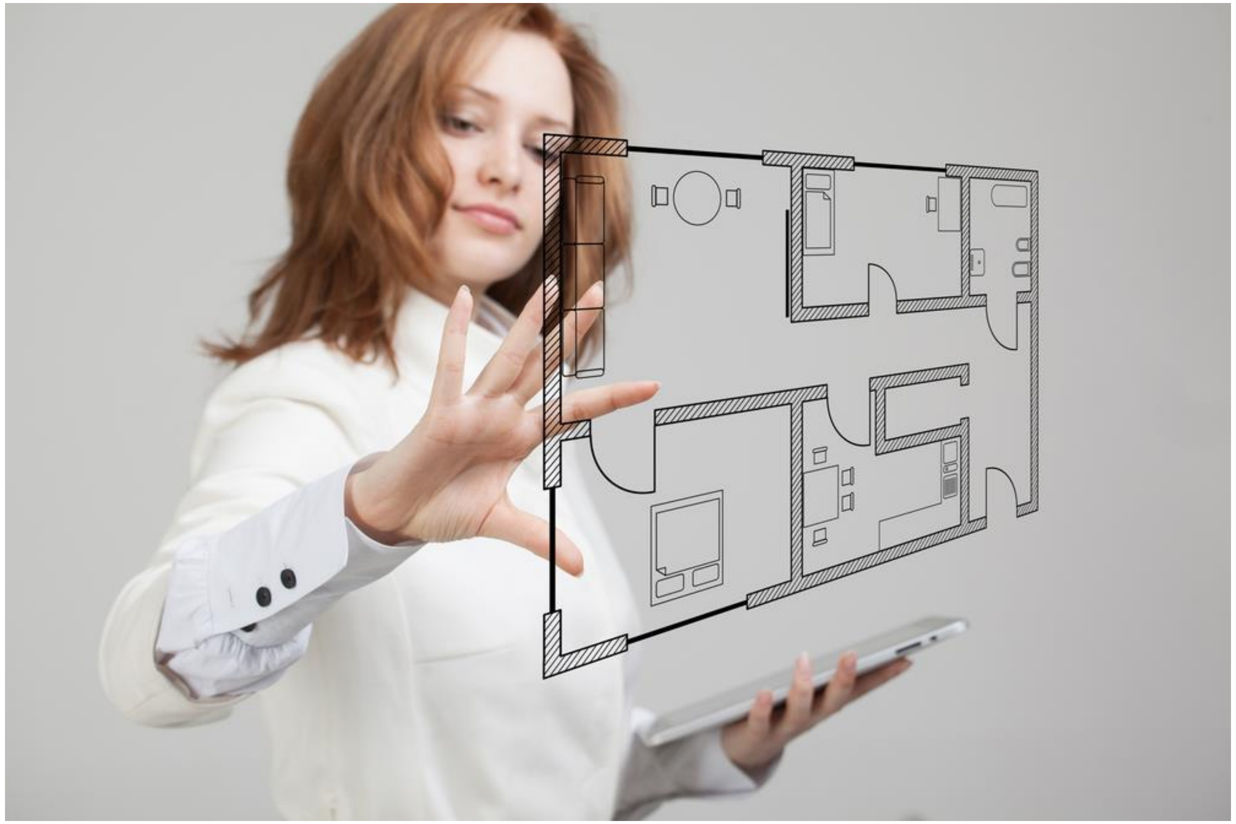




SPARX SERVICES CENTRAL EUROPE

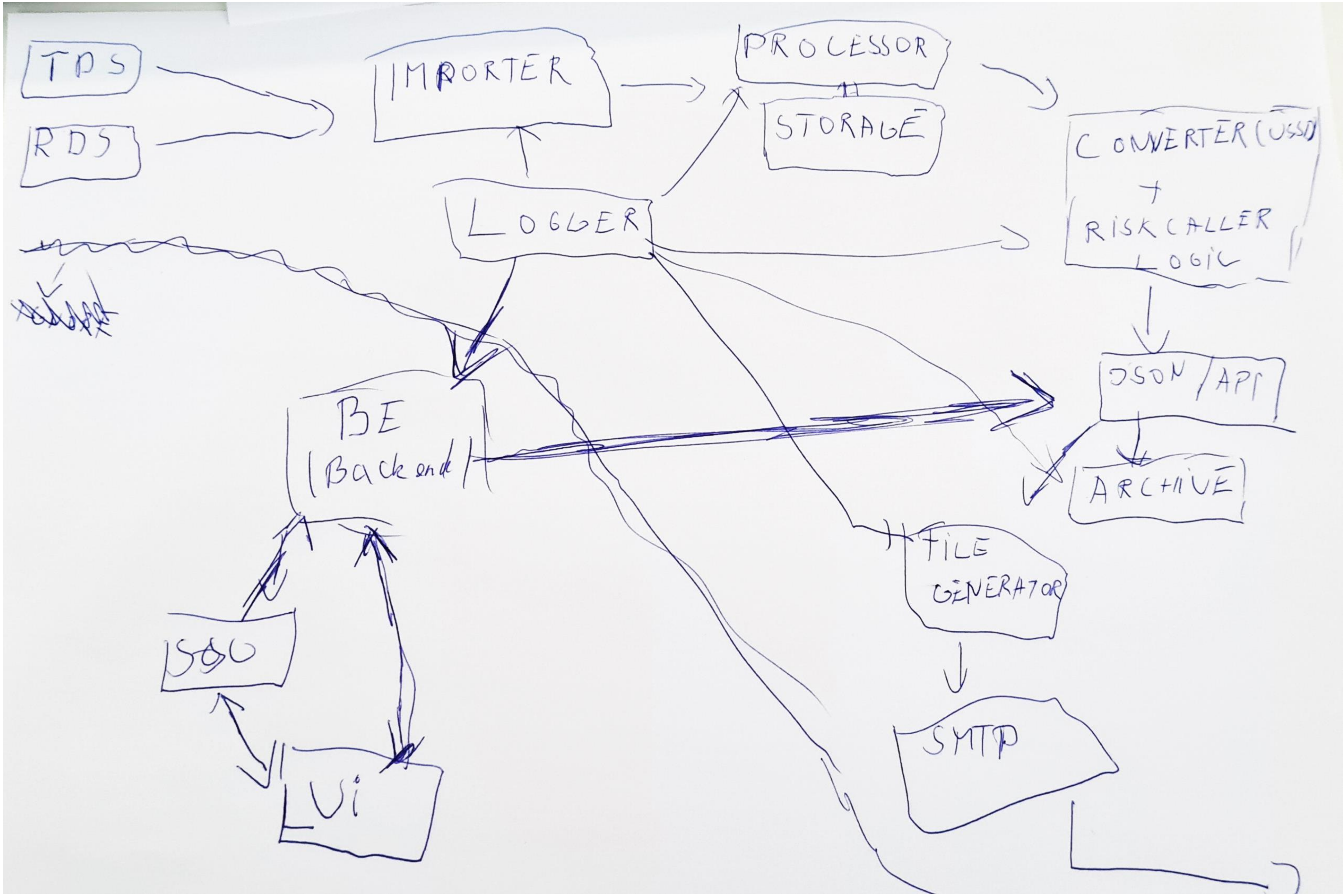
Thousands of years later ....

modern houses floor plan

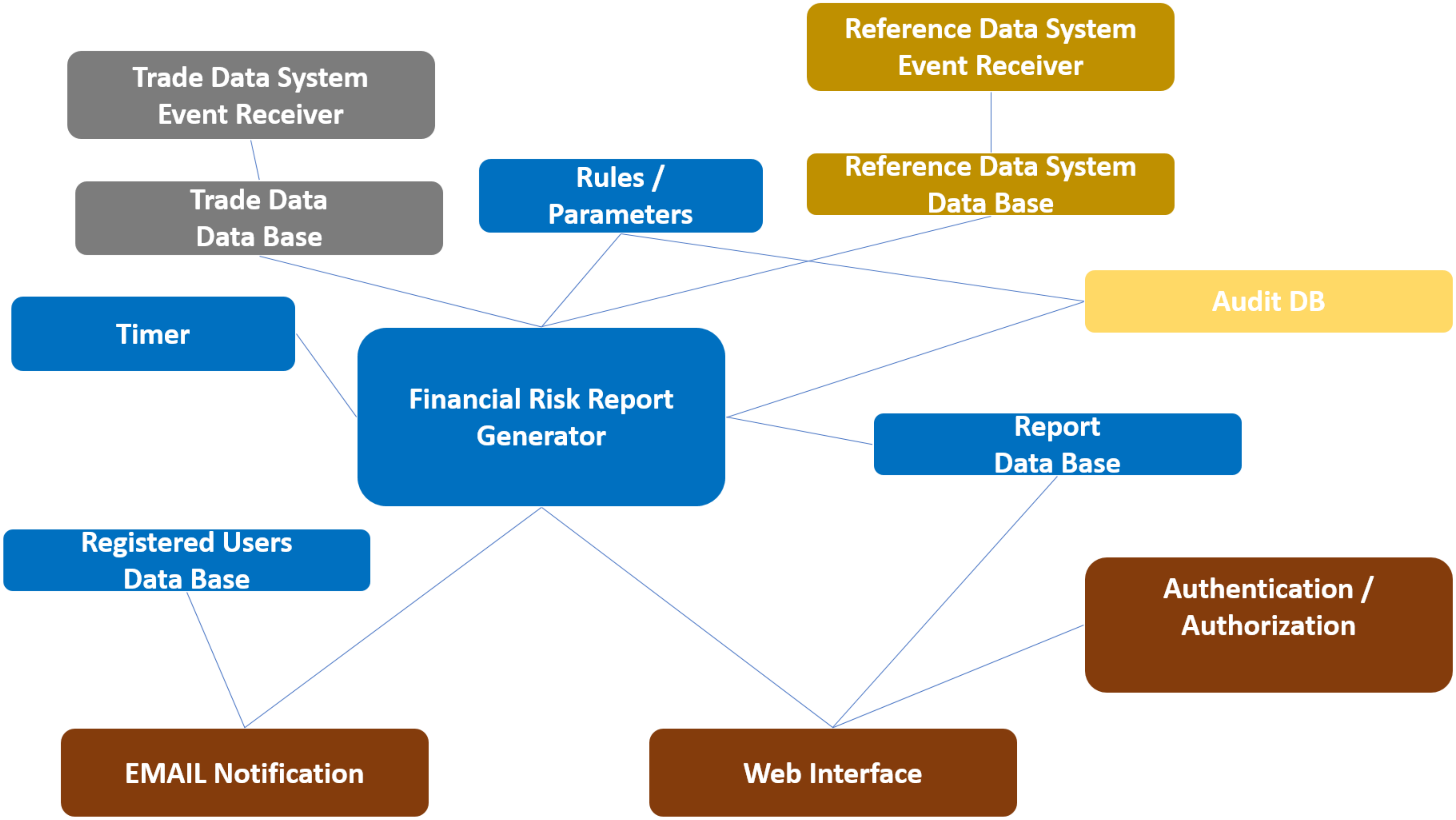


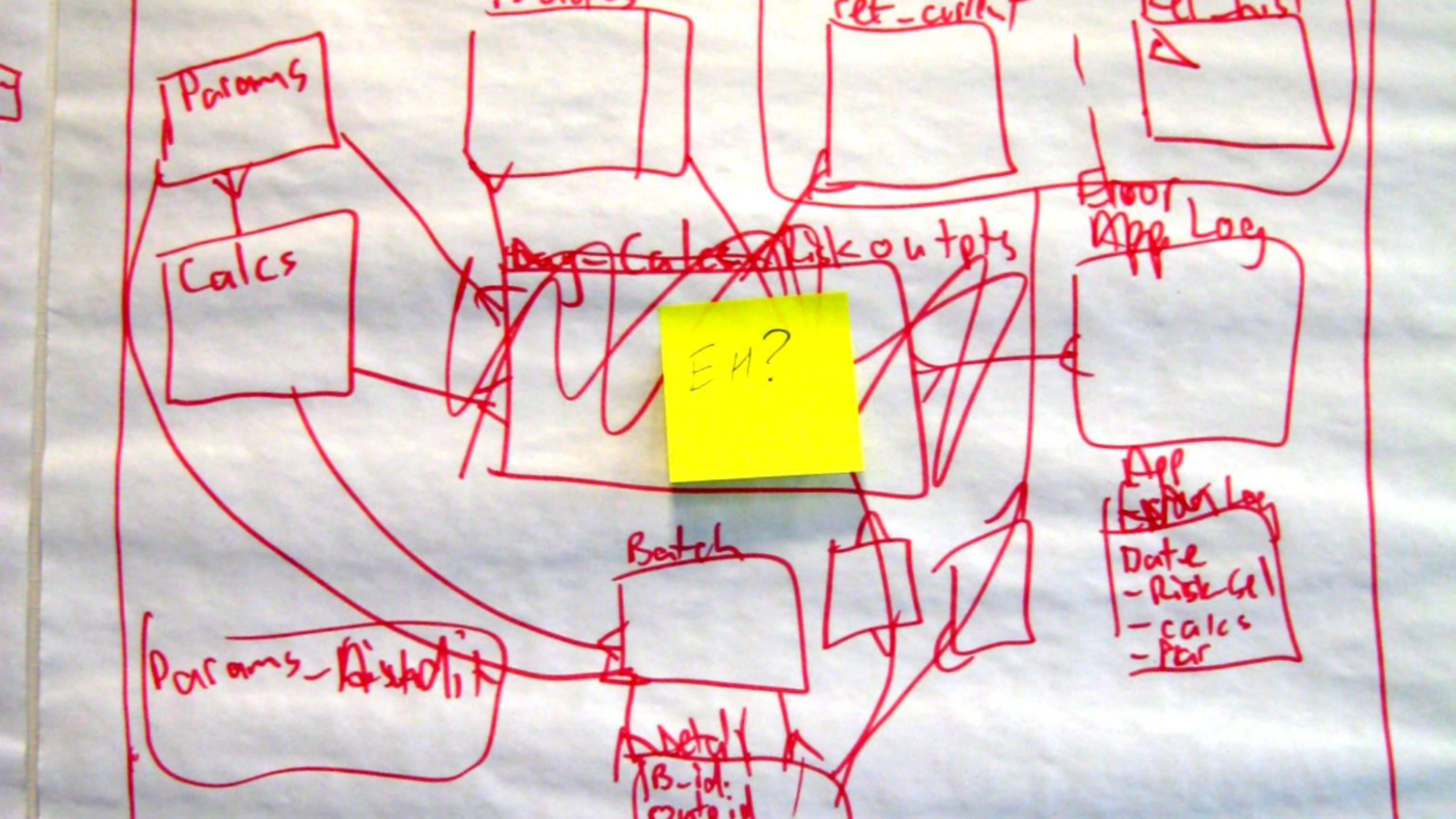
SPARX SERVICES CENTRAL EUROPE

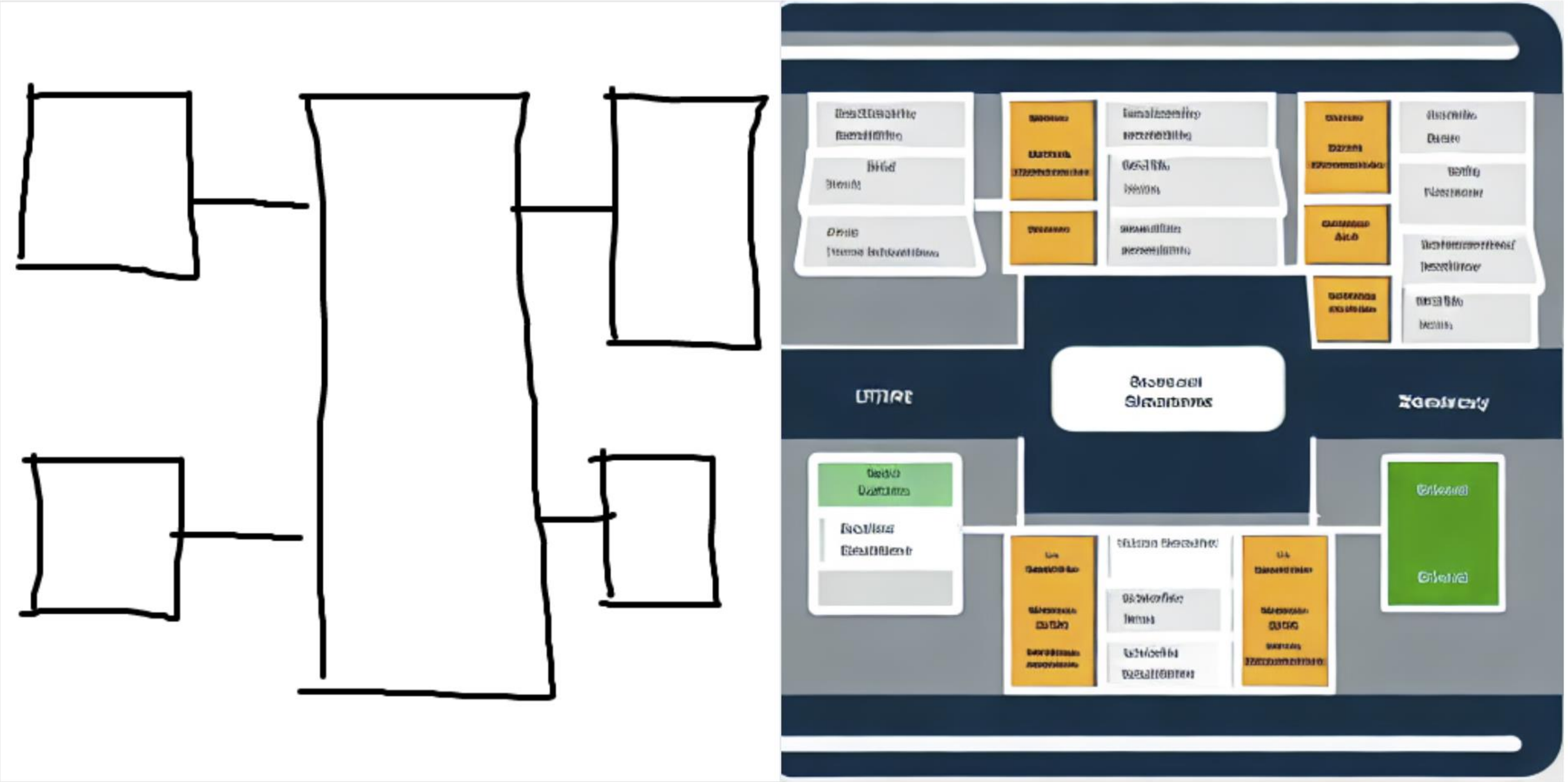
Software architects struggle to communicate architecture


TDS
RDS
IMPORTER
PROCESSOR
STORAGE
CONVERTER (USSD)
+
RISK CALLER
LOGIC
LOGGER
JSON / API
ARCHIVE
BE
(Backend)
FILE
GENERATOR
SSO
SMTP
LUi

Financial Risk System – Software Components


Trade Data System Event Receiver
Trade Data Data Base
Rules / Parameters
Reference Data System Event Receiver
Reference Data System Data Base
Audit DB
Timer
Financial Risk Report Generator
Report Data Base
Registered Users Data Base
Authentication / Authorization
EMAIL Notification
Web Interface

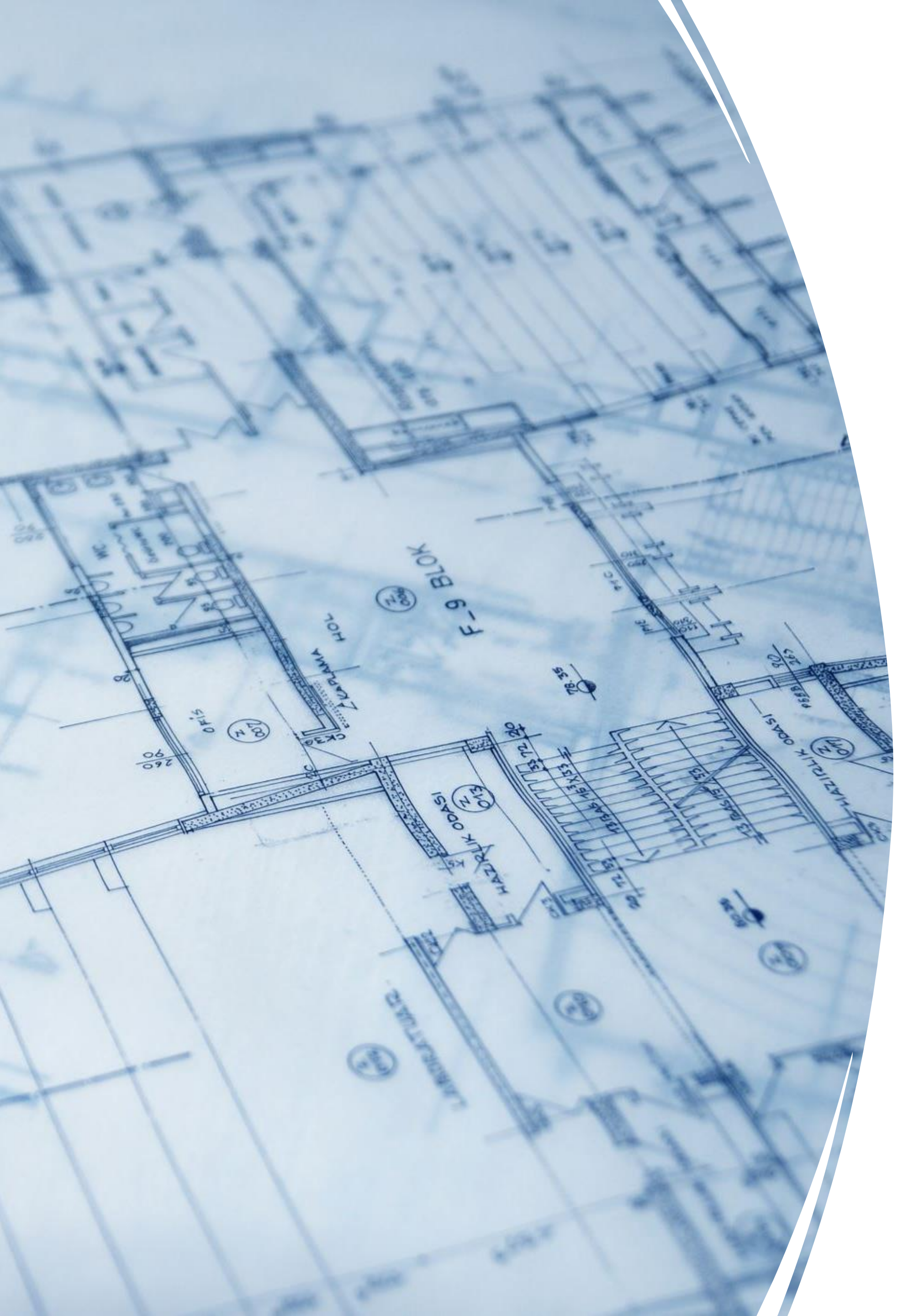

ret_curr
Params
Calcs
~~Deg_Calcs~~ Risk outpts
Error
App Log
App
Error Log
Date
- RiskCel
- calcs
- Par
EH?
Batch
Params_Distrib
Detail
B_id:



“a software architecture diagram with a big box in the middle called "Enterprise Service Bus"”

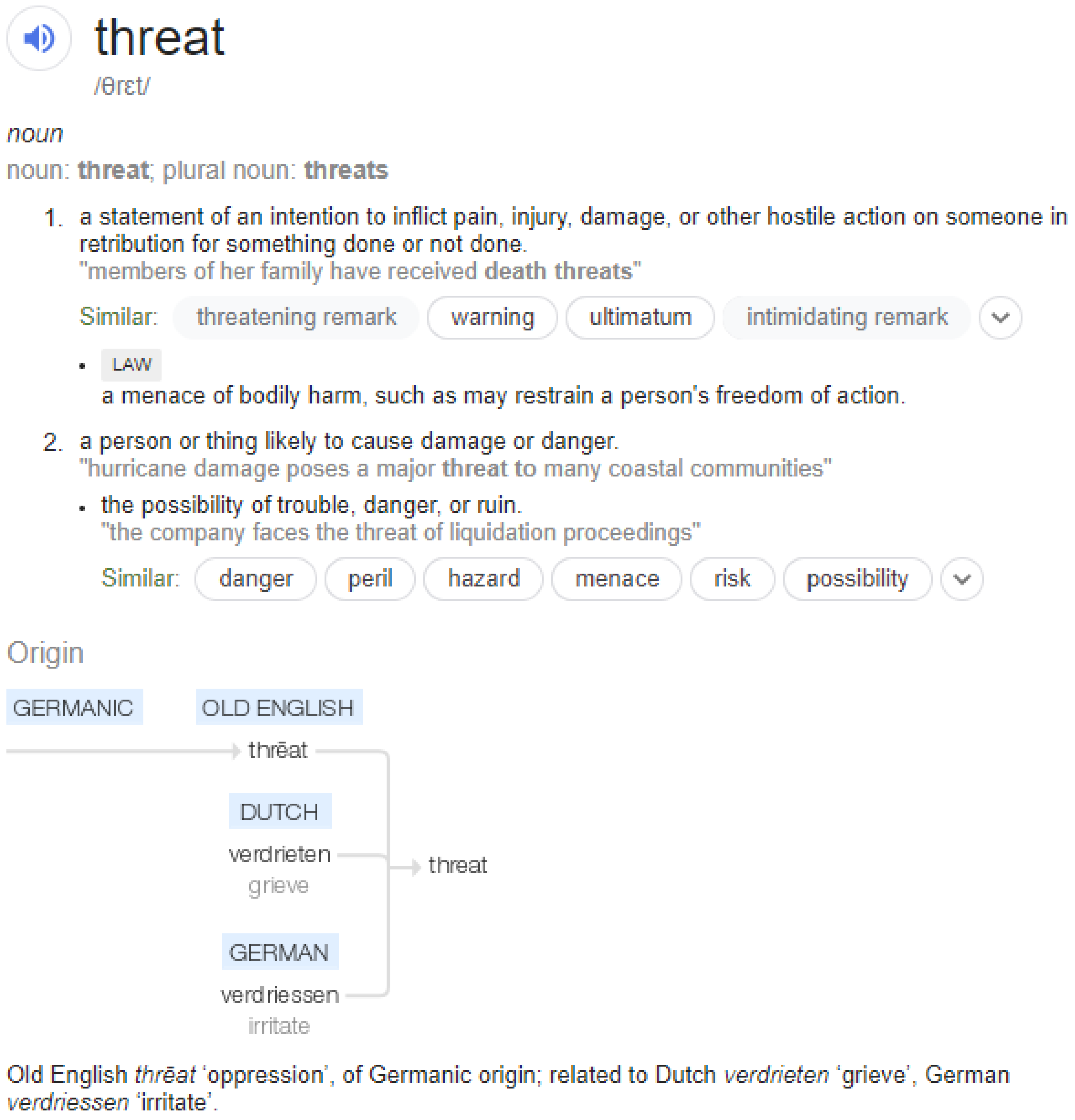
SPARX SERVICES CENTRAL EUROPE

Generated by AI Scribble Diffusion:
https://scribblediffusion.com/scribbles/6sczpswuozeqfdbue247soisv4



Importance of Architecture in Cybersecurity Threat Modeling

- Having a well-designed architecture plan is crucial for modeling cybersecurity threats
- The architecture provides a blueprint of the organization's IT infrastructure components
- The clear understanding of architecture enables experts to identify potential vulnerabilities and risks
- It also helps in identifying potential attack vectors and entry points for cybercriminals
- A well-designed architecture is critical for effective cybersecurity threat modeling
- It provides a clear picture of the organization's technological landscape for accurate and effective models



threat

/θrɛt/

noun

noun: **threat**; plural noun: **threats**

1. a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done.
   "members of her family have received **death threats**"

   Similar: threatening remark | warning | ultimatum | intimidating remark

   - LAW
     a menace of bodily harm, such as may restrain a person's freedom of action.

2. a person or thing likely to cause damage or danger.
   "hurricane damage poses a major **threat to** many coastal communities"

   - the possibility of trouble, danger, or ruin.
     "the company faces the threat of liquidation proceedings"

     Similar: danger | peril | hazard | menace | risk | possibility

Origin

GERMANIC → OLD ENGLISH thrēat

DUTCH verdrieten grieve

GERMAN verdriessen irritate

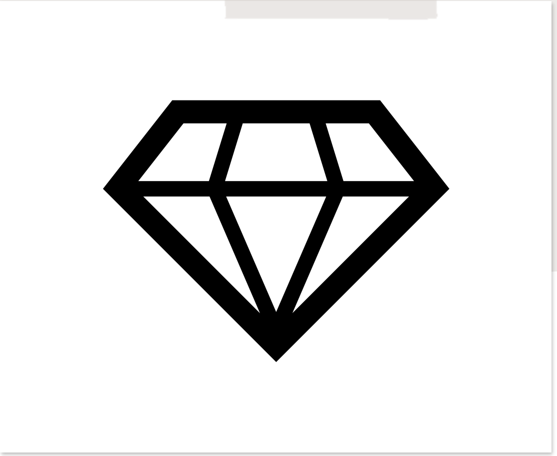
→ threat

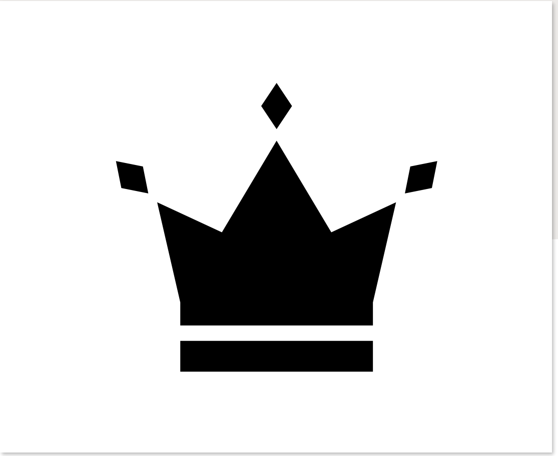
Old English *thrēat* 'oppression', of Germanic origin; related to Dutch *verdrieten* 'grieve', German *verdriessen* 'irritate'.

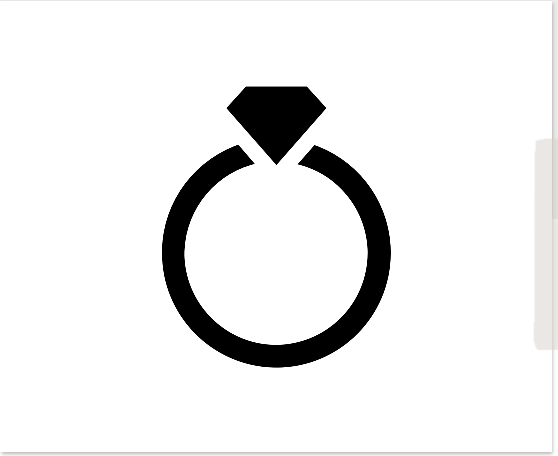
SPARX SERVICES CENTRAL EUROPE

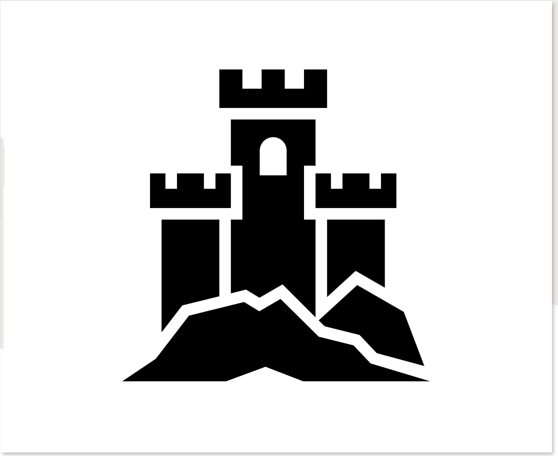
https://www.lexico.com/en/definition/threat

What is Threat Modeling









- **Structured Process**
- Examination of a system for potential weaknesses

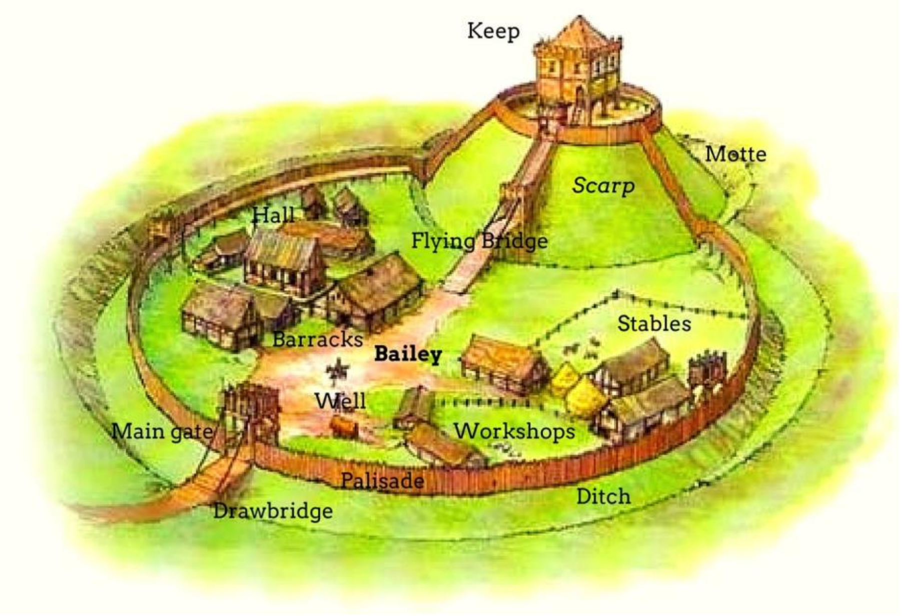
What is Threat Modeling

Structured Process

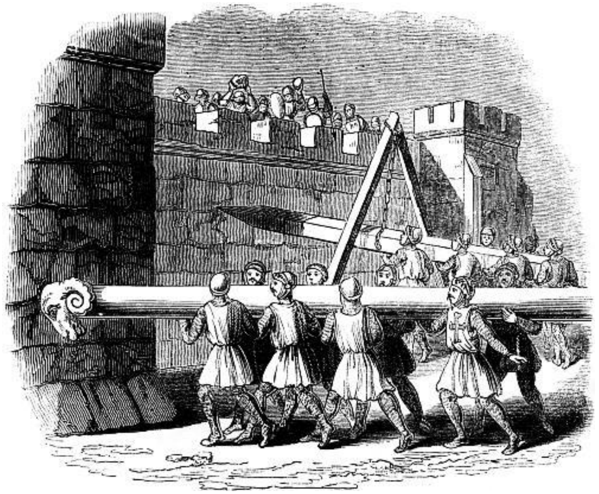
- Examination of a system for potential weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats



https://www.castlesworld.com/tools/motte-and-bailey-castles.php



https://en.wikibooks.org/wiki/Castles_of_England/Methods_of_Attack

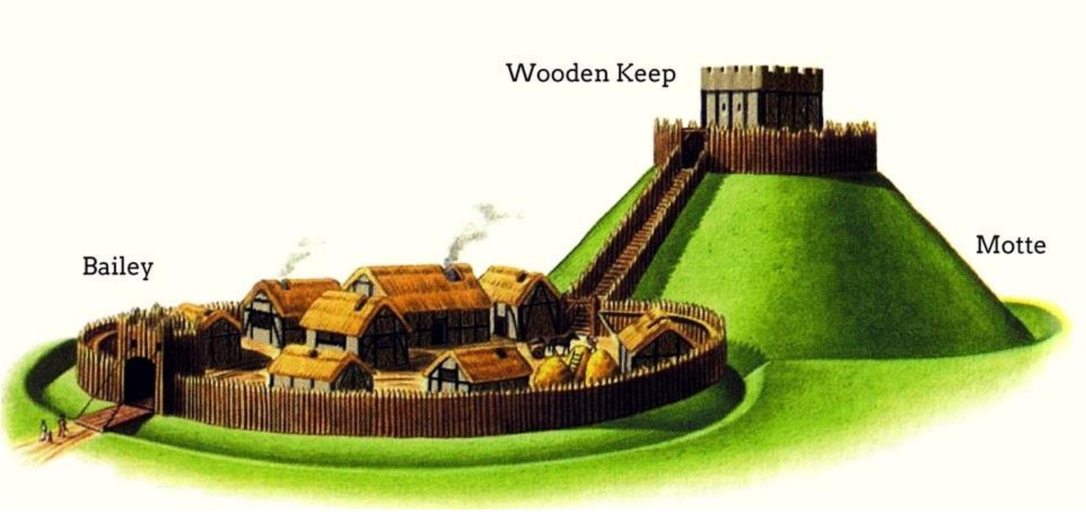
What is Threat Modeling

Structured Process

- Examination of a system for potential weaknesses
- Resolving identified weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats



https://www.castlesworld.com/tools/concentric-castles.php

https://deadliestwarrior.fandom.com/wiki/Huo_Chien

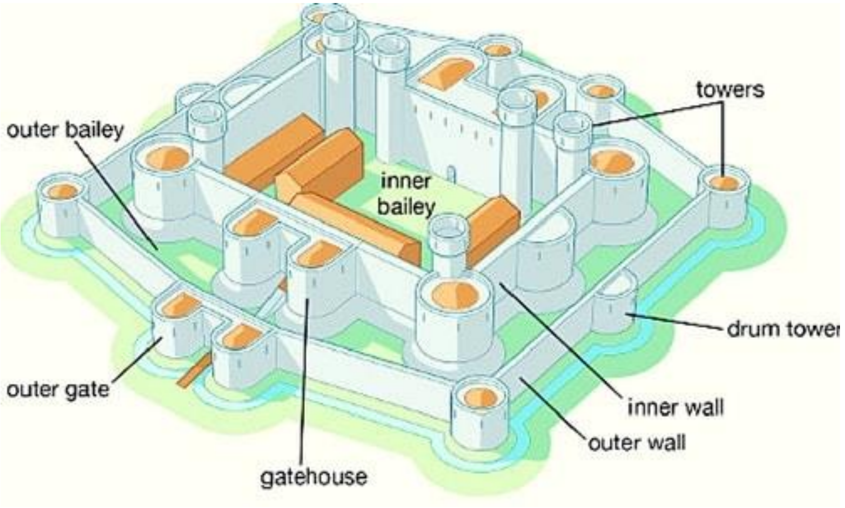
What is Threat Modeling

Structured Process

- Examination of a system for potential weaknesses
- Resolving identified weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats
- Keeping the model of weaknesses and threats up to date



https://www.castlesworld.com/tools/concentric-castles.php

https://www.pbs.org/video/1812-niagara-frontier-fort-george-cannon-firing/

SPARX SERVICES CENTRAL EUROPE

Nowadays challenges…

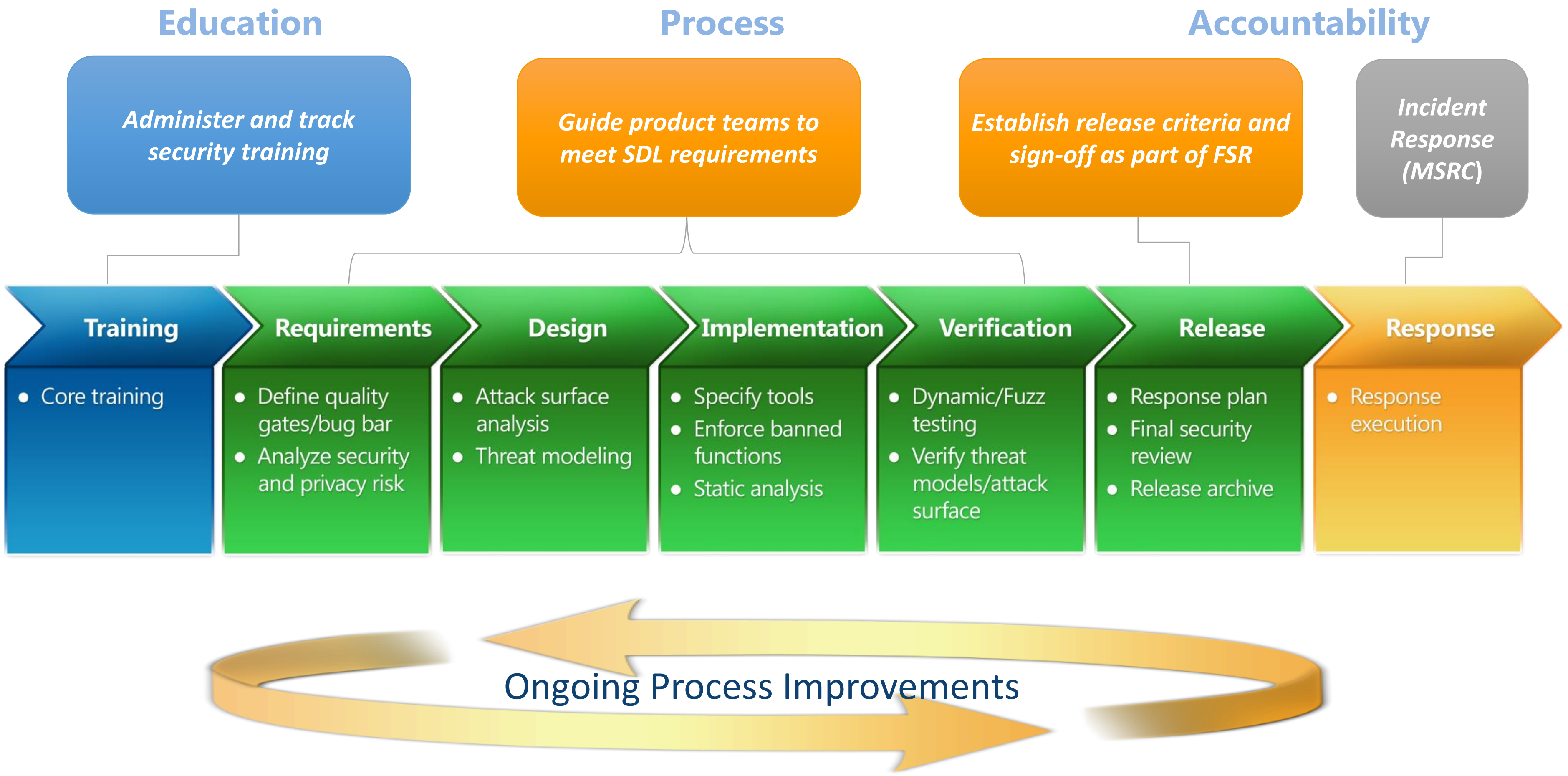
- Insider attacks are typically executed by employees who have access to sensitive data
- The usage of cloud services has led to the emergence of new security obstacles that must be addressed immediately
- The Internet of Things (IoT) has introduced new security challenges
- Ransomware attacks, which demand higher payments
- Supply chain attacks are growing
- Data privacy regulations have made protecting sensitive information
- Organizations need to be aware of AI and ML-based cybersecurity threats

SPARX SERVICES CENTRAL EUROPE

Cybersecurity is not in a development DNA!

- Insert security practices as a part of your software development lifecycle
- Verification must happen as soon as possible (end- users ARE NOT your testers ☺)

Microsoft | Security Development Lifecycle



Education

Administer and track security training

Process

Guide product teams to meet SDL requirements

Accountability

Establish release criteria and sign-off as part of FSR

Incident Response (MSRC)

Training
- Core training

Requirements
- Define quality gates/bug bar
- Analyze security and privacy risk

Design
- Attack surface analysis
- Threat modeling

Implementation
- Specify tools
- Enforce banned functions
- Static analysis

Verification
- Dynamic/Fuzz testing
- Verify threat models/attack surface

Release
- Response plan
- Final security review
- Release archive

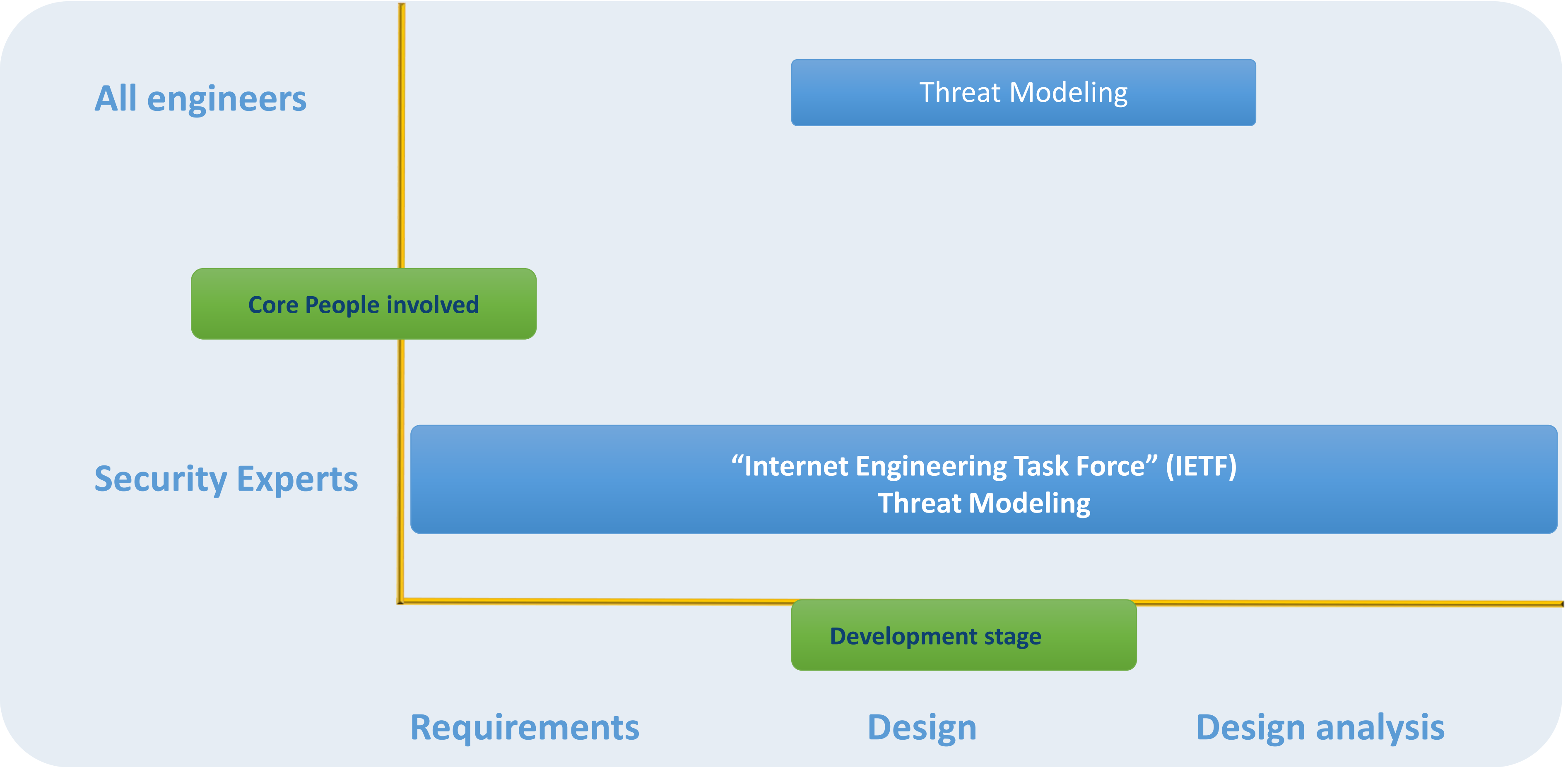
Response
- Response execution

Ongoing Process Improvements

SPARX SERVICES CENTRAL EUROPE

https://www.microsoft.com/en-us/securityengineering/sdl/

Terminology and Context



All engineers

Threat Modeling

Core People involved

Security Experts

"Internet Engineering Task Force" (IETF)
Threat Modeling

Development stage

Requirements

Design

Design analysis

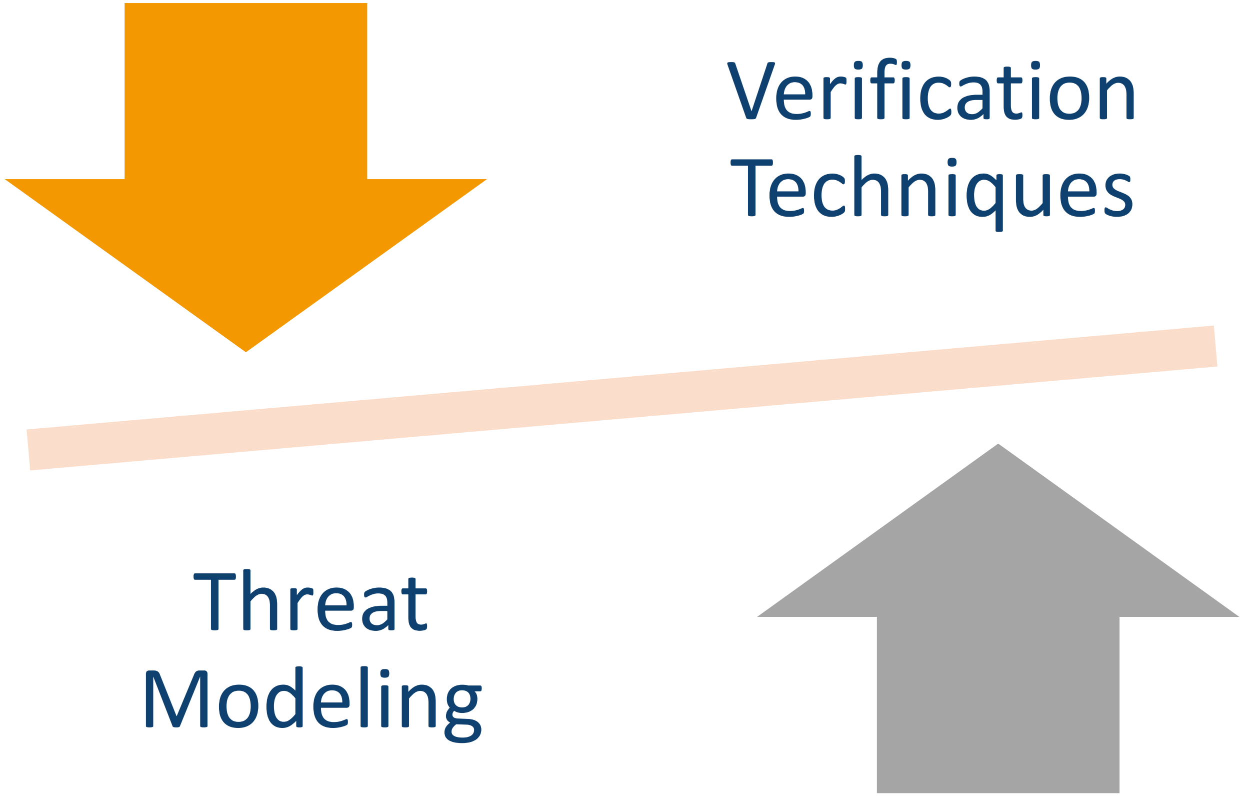
SPARX SERVICES CENTRAL EUROPE

Threat Modeling in Software Development

- Software development is about creating applications that enable users to perform some tasks
- Secure development requires determining what a user shouldn't do and ensuring that the code properly restricts users to authorized actions
- Threat modeling is a design activity to do just that

Threats are not vulnerabilities!

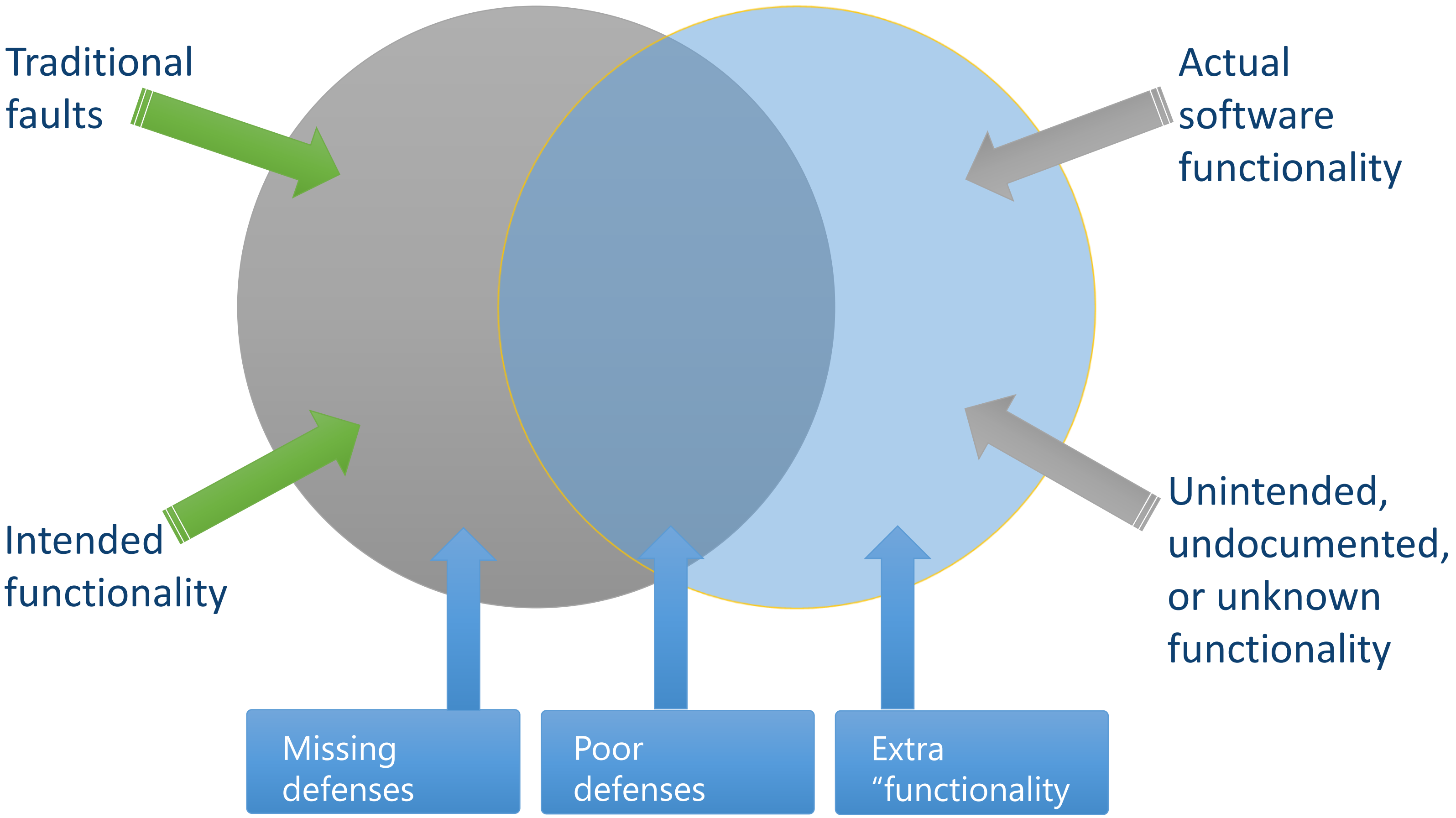
Threat modeling can be performed before a product or service has been implemented



Verification Techniques

Threat Modeling

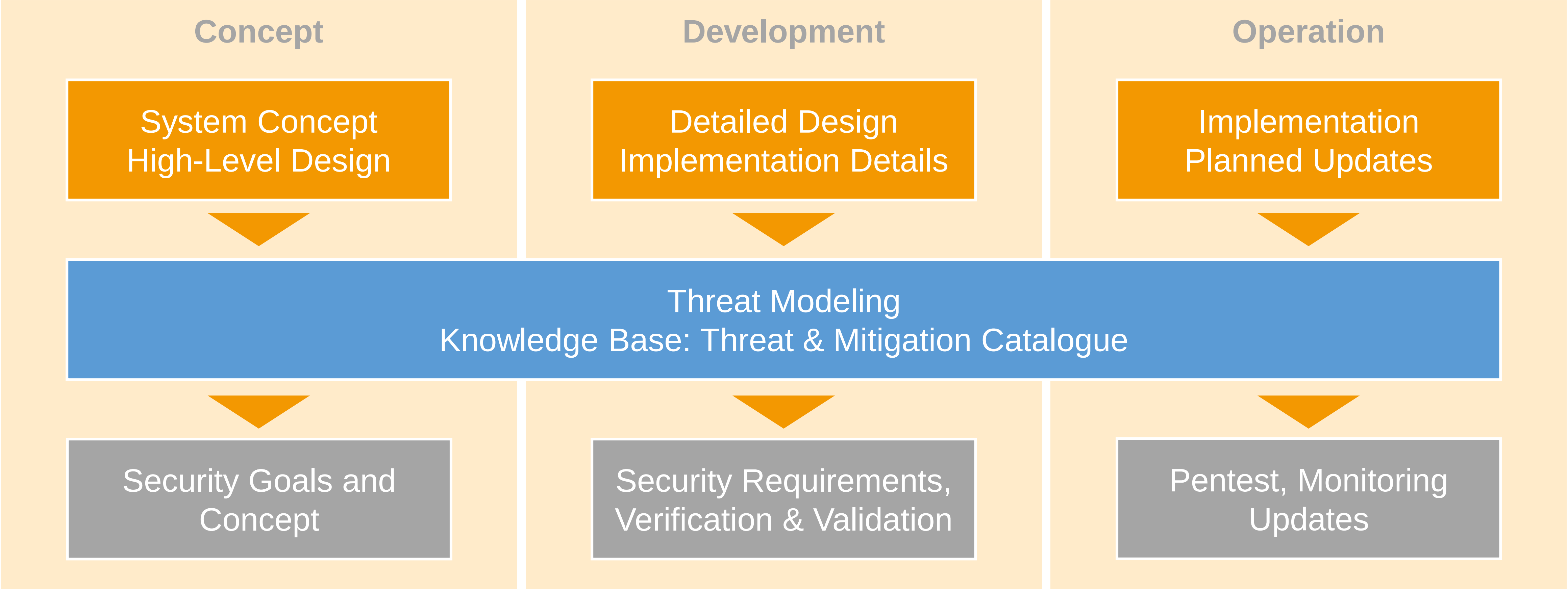
Security Testing



Threat Modeling Enables

- Identify threats
- Identify vulnerabilities
- Identify mitigating factors
- Perform risk analysis
- Prioritize security fixes
- Derive security test cases

When do we Threat Model



Concept

System Concept
High-Level Design

Security Goals and Concept

Development

Detailed Design
Implementation Details

Security Requirements, Verification & Validation

Operation

Implementation
Planned Updates

Pentest, Monitoring Updates

Threat Modeling
Knowledge Base: Threat & Mitigation Catalogue

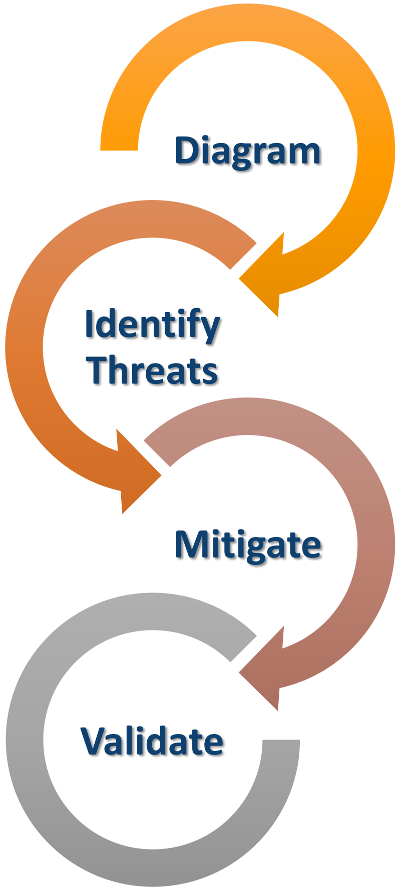
Understanding the STRIDE Threats

Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be any of billg, microsoft.com or ntdll.dll
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Repudiation	Non-repudiation	Claiming to have not performed an action.	“I didn’t send that email,” “I didn’t modify that file,” “I certainly didn’t visit that web site, dear!”
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example but going from a limited user to admin is also EoP.

https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

SPARX SERVICES CENTRAL EUROPE

Threat modeling in Enterprise Architect



- Create DFDs (Data Flow Diagrams)
  - Include processes, data stores, data flows
  - Include trust boundaries
  - Diagrams per scenario may be helpful
- Identify Threats
  - Get specific about threat manifestation
- Mitigate
  - To address or alleviate a problem
- Validate the whole threat model
  - Validate Quality of Threats and Mitigations
  - Validate Information Captured

SPARX SERVICES CENTRAL EUROPE

Cyber Security in Enterprise Architect enables

ENTERPRISE
ARCHITECT

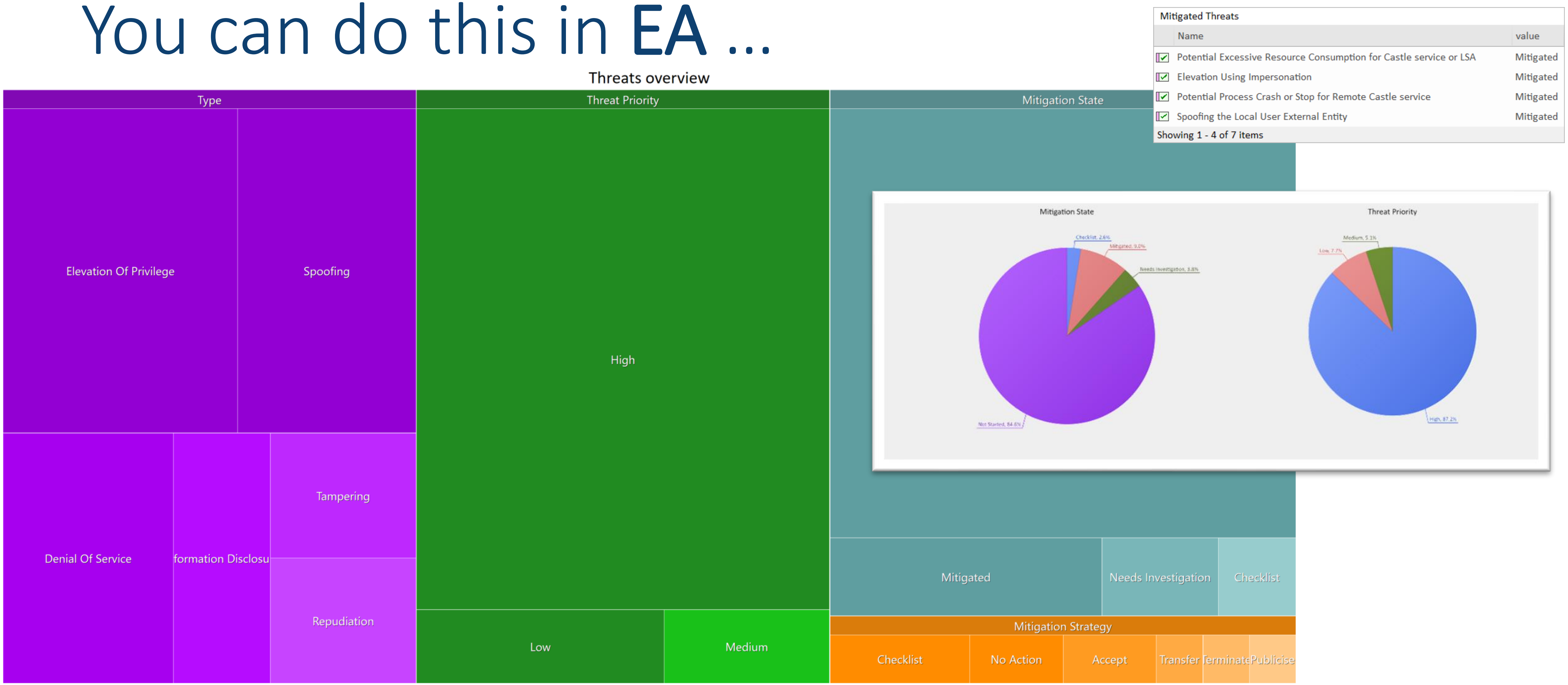
- Create Trust Diagrams per scenarios
- Clasify the potential vulnerability using STRIDE and form a mitigation
- Tracing threats and vulnerabilities to your Software/Systems models
- Creating various reports using the build-in capabilities
- Sharing threat models using standards (XMI, OSLC)
- Analyzing, visualizing and communicating using business language

SPARX
SERVICES CENTRAL EUROPE

Have you ever wanted to:

- Analyze your threat models by visual aggregation or relevance?
- Absorb information in new ways?
- Identify emerging trends with ease and respond quickly?
- Interact directly with your data?
- Communicate with a new business language?

You can do this in **EA** ...

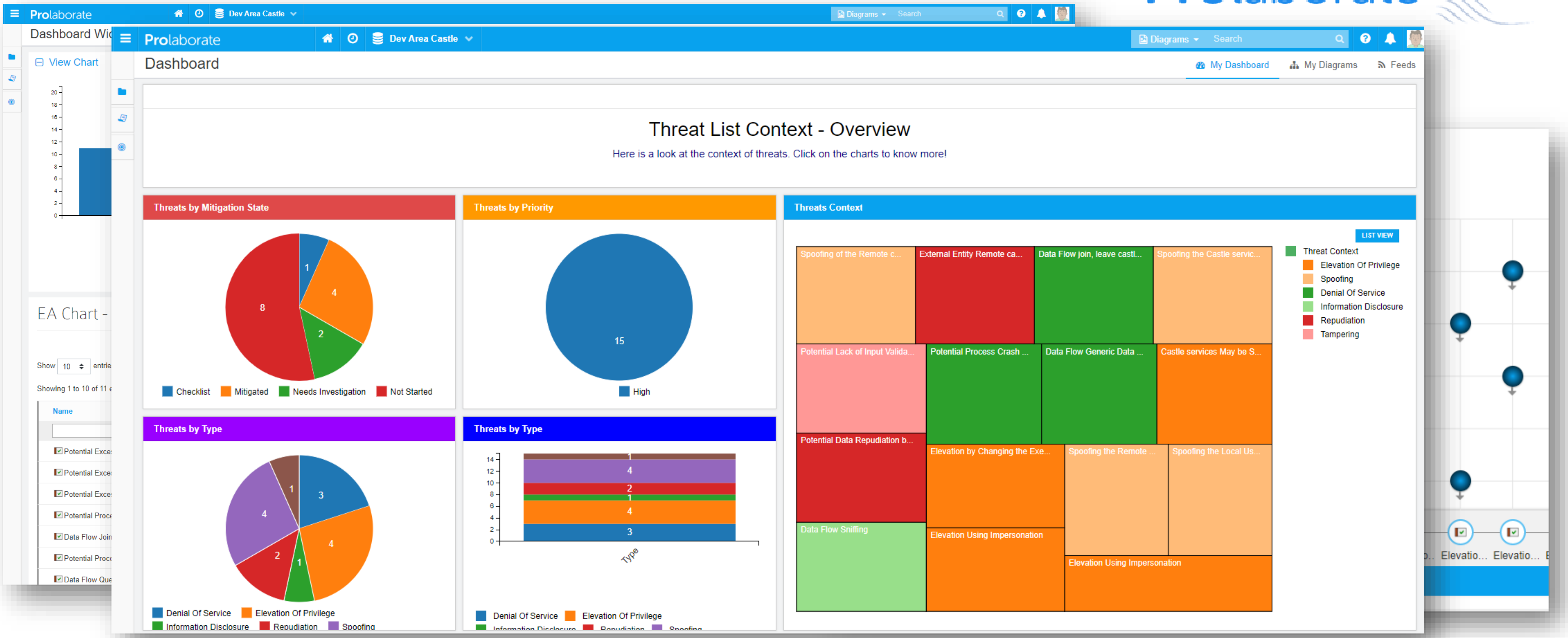


Mitigated Threats

	Name	value
☑	Potential Excessive Resource Consumption for Castle service or LSA	Mitigated
☑	Elevation Using Impersonation	Mitigated
☑	Potential Process Crash or Stop for Remote Castle service	Mitigated
☑	Spoofing the Local User External Entity	Mitigated

Showing 1 - 4 of 7 items

...or this in Prolaborate



Dashboard

Threat List Context - Overview

Here is a look at the context of threats. Click on the charts to know more!

sales@sparxservices.eu

DEMO

SPARX SERVICES CENTRAL EUROPE

INCOSE

Follow up event:

June 15th

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THREATGET

AWARD WINNING PRODUCT

eAward 2020 Industrie 4.0

for the new cyber security management system "ThreatGet". The eAward from report.at is one of the most important Austrian IT awards. It honors economical, user-friendly and innovative IT projects of Austrian companies.

Sieger
eAWARD 2020
www.report.at

Expo 2020 Dubai

(October 2021 to March 2022): Cyber Security Management System "ThreatGet" from AIT Austrian Institute of Technology is a selected exhibition project in the Austria – Pavilion

iLab EXHIBITOR
AUSTRIA
MAKES SENSE
EXPO 2020 DUBAI

Constantinus Award 2021

Winner "Digitalization" and "IoT" Category

ThreatGet: Cyber Security by Design, comprehensive consulting for IT professionals in security-critical technology architecture.

1. PLATZ
DIGITALISIERUNG / INTERNET OF THINGS
CONSTANTINUS
www.constantinus.net
2021

Is Cybersecurity Modelling the Silver Bullet?...

... no – but it is one more strong puzzle piece that could change the game

Bob Hruska
LinkedIn

Questions?

SPARX SERVICES CENTRAL EUROPE