



Threat Modelling

Or How I Learned To Stop Worrying And Love Misconfigurations

RIP - ClappyMonkey



Gone but not forgotten



The Symptoms

Vulnerability scans highlighting weak, or non-existent, encryption.

Cloud consoles listing reams of issues for resources, e.g. publicly exposed storage.

Penetration testers find basic flaws.

Scans find exposed credentials or weak Active Directory configuration.



Cloud Security Alliance Top Threats to Cloud Computing 2025

- The top issues in recent breaches were:
 - Misconfiguration and Inadequate Change Control
 - Identity and Access Management
 - Insecure Software Development
 - Insecure Interfaces and APIs
 - Inadequate Selection/Implementation of Cloud Security Strategy
 - System Vulnerabilities

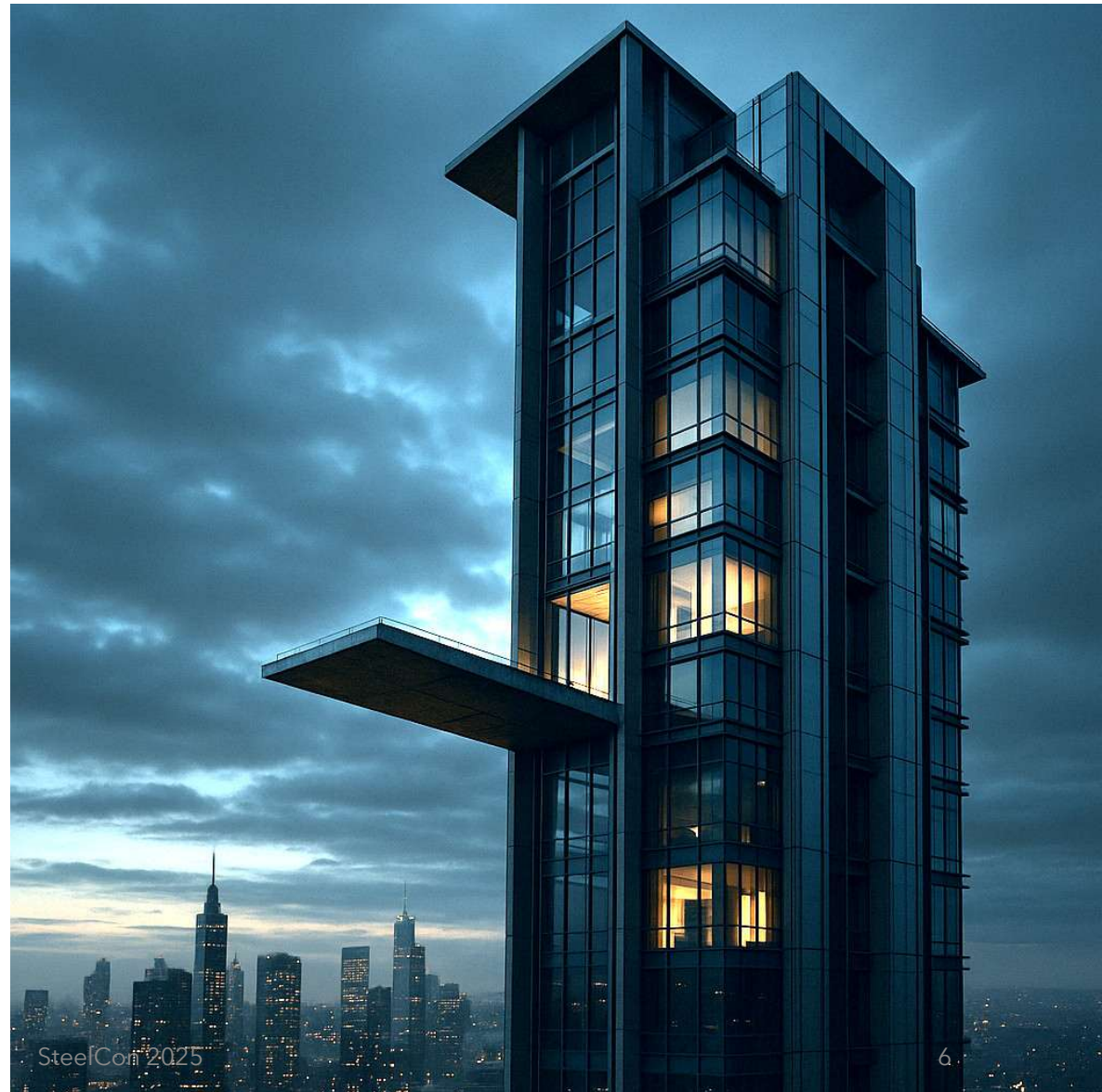
Recent Breaches Disclosing the Most Personal Data

- T-Mobile – GPRS gateway on public internet and successful brute forcing of SSH on router
- Xfinity – Unpatched critical Citrix flaw
- PeopleConnect, Inc – exposed database
- NationStar Mortgage – Unsecured Google Cloud storage bucket
- Equifax – Compromise of 4-year old Apache Struts vulnerability

Your Shiny Architecture Comes With Free Vulnerabilities

Sadly, security is not always
default.

11/07/2025



SteelCorr 2025

The Doomed Temple of Temporal Trade-Offs

The root cause of most technological debt

11/07/2025





There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know.

— *Donald Rumsfeld* —

AZ QUOTES

The Problem

Known

Unknown

Known

The Known Knowns

- Good encryption
- Single sign-on / Open ID Connect
- Secret management
- Other stuff developers do day in, day out

The Unknown Knowns

- Fine detail of best practice configuration
- Other stuff developers aren't aware of

The Known Unknowns

- Zero days
- Human error

The Unknown Unknowns





There's an old saying in Tennessee
— I know it's in Texas, probably in
Tennessee — that says, fool me
once, shame on — shame on you.
Fool me — you can't get fooled
again.

— *George W. Bush* —

AZ QUOTES

Playing the Home Field Advantage



Design your system



Get your developers and security team to think what could go wrong



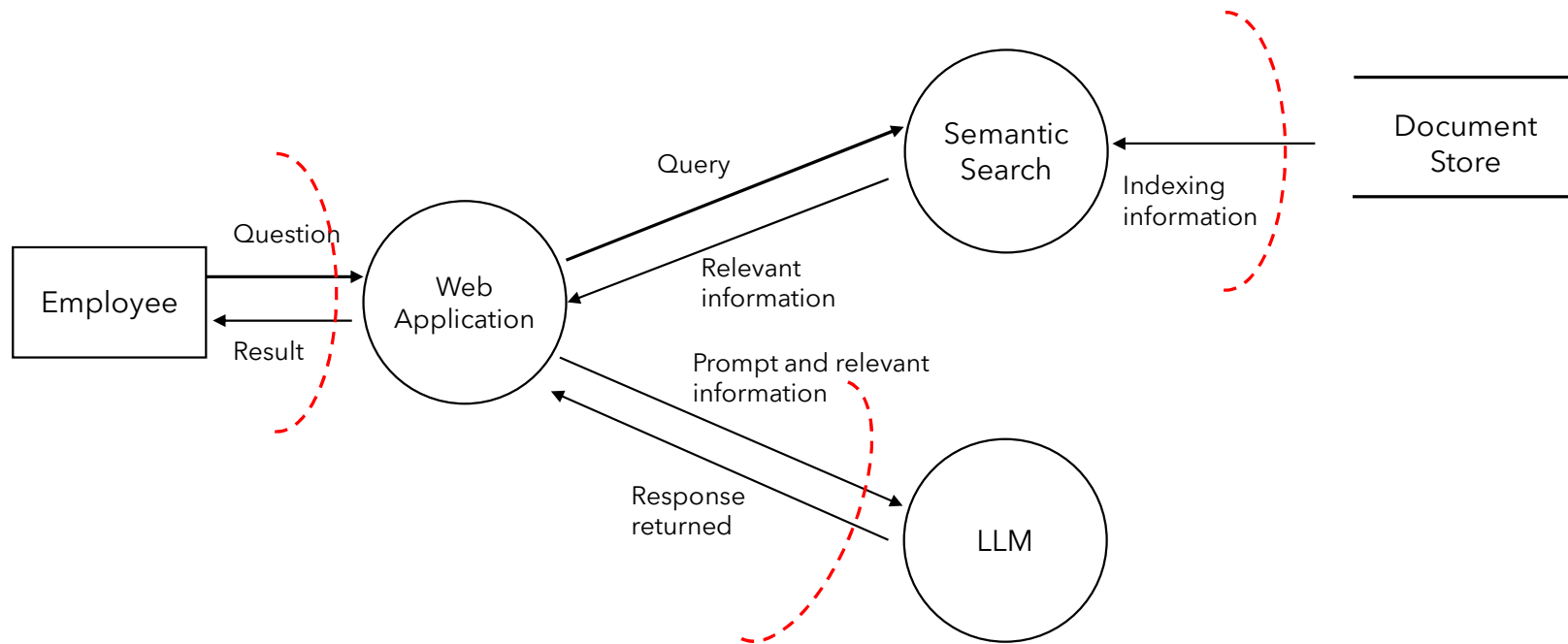
Do your best to put in controls to address issues

Gives you a map of where
the dragons lay



11/07/2025

Data Flow Diagram



For more information see https://owasp.org/www-community/Threat_Modeling_Process#data-flow-diagrams

Threat Modelling Process

The Threat Modeling Process



Threat Modelling Frameworks

- STRIDE – Simple for smaller organisations or getting started.
- PASTA – More comprehensive for those with more resources and experience.
- DREAD – More quantitative, good for working out 'how bad is it?' - triage

STRIDE

STRIDE Element	Associated Controls Ensure
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorisation

<https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/>

Application of STRIDE to Trust Boundaries

	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	?	✓	✓	
Data Flow		✓		✓	✓	

PASTA






	PASTA Elements
Process for Attack Simulation and Threat Analysis	Define objectives
	Identify boundaries, technologies and data flows
	Visually represent the components and relationships
	Identify potential threats
	Analyse identified threats against the system's weaknesses
	Simulate potential attacks
	Analyse risk and impact






<https://versprite.com/cybersecurity-listings/offsec/threat-models/>






DREAD






DREAD Element	Measures
Damage potential	Attack impact
Reproducibility	How easy is it to reproduce?
Exploitability	How easy is the attack to launch?
Affected users	How many users will it affect?
Discoverability	How easily can the vulnerability be detected?




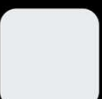
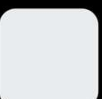
https://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/Threats_Countermeasures.pdf

D     

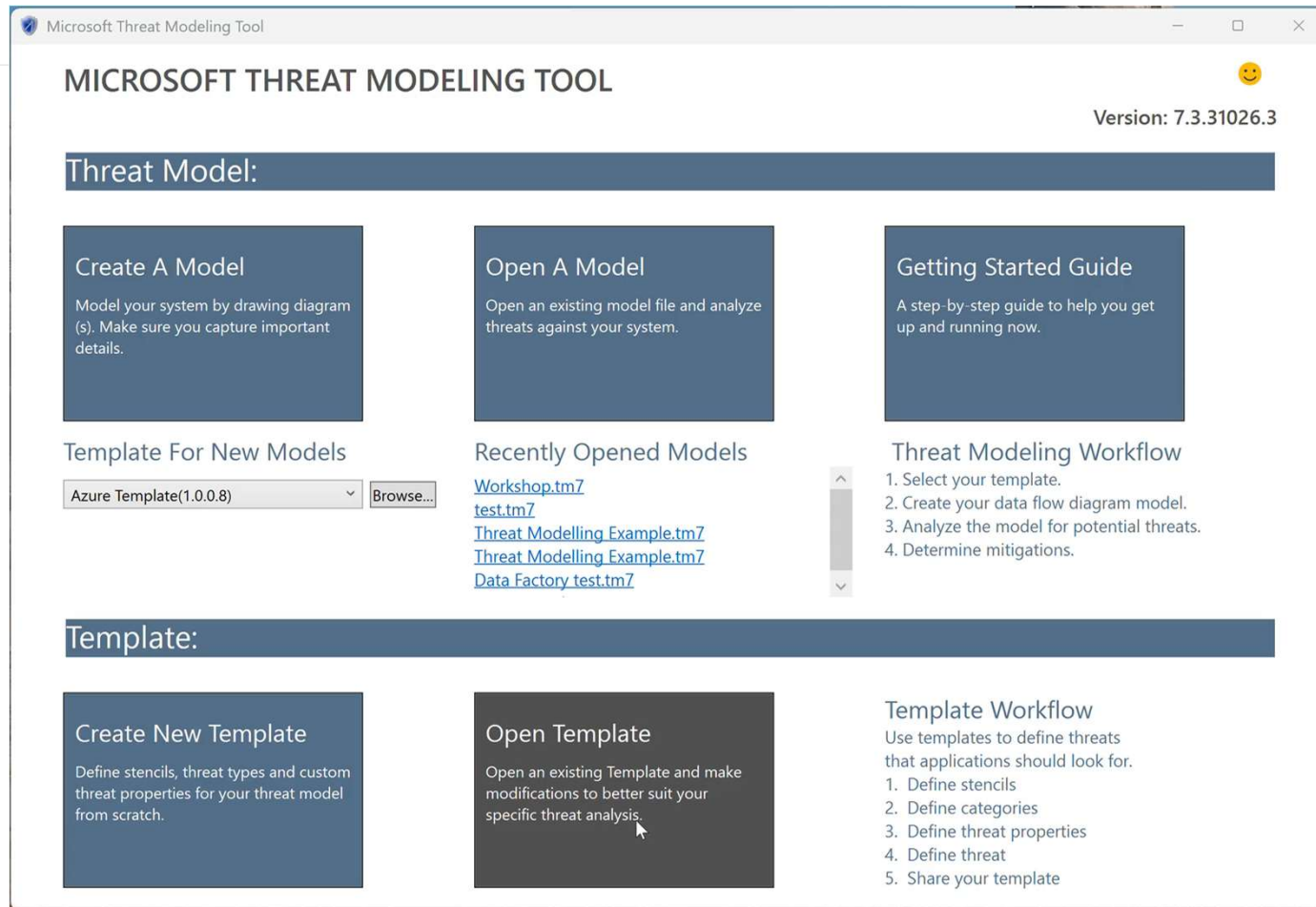
R     

E     

A     

D     

Demo



Some relevant elements from the Threat Modelling Manifesto

- A culture of finding and fixing design issues
- Repeatability and measurability
- Achieve thoroughness and reproducibility by applying security and privacy knowledge in a structured manner
- Threat modelling must align with an organisation's development practices and follow design changes
- Improving security and privacy through early and frequent analysis

Useful Resources

Best practice for popular cloud platforms and resources for creating diagrams.

Threat Modellers Manifesto

<https://www.threatmodelingmanifesto.org>

Azure Security Baseline

<https://github.com/MicrosoftDocs/SecurityBenchmarks/tree/master/Azure%20Offer%20Security%20Baselines/3.0>

AWS Security Hub Foundational Security Best Practices

<https://docs.aws.amazon.com/securityhub/latest/userguide/fsbp-standard.html>

MITRE CAPEC Mechanisms of Attack:

<https://capec.mitre.org/data/definitions/1000.html>

CAPEC - STRIDE mapping:

<https://ostering.com/blog/2022/03/07/capec-stride-mapping>

Azure Architecture Icons: <https://learn.microsoft.com/en-us/azure/architecture/icons/>

AWS Architecture Icons:

<https://aws.amazon.com/architecture/icons/>

Download Slides



We're hiring <https://www.sainsburys.jobs>

Follow Andrea on X: @allaboutclait