

THREAT MODELING
CONNECT

HACKATHON

APRIL 1-24, 2025

BROUGHT TO YOU BY

IriusRisk | **SHOSTACK**
+ ASSOCIATES



WORKSHOP

Developing a Threat Modeling Mindset

THREAT MODELING
CONNECT | POWERED BY
IRIUSRISK



Agenda:

- Introduction (5 min)
 - Who is Robert?
 - What do I want you to get from this?
- Introducing the Threat Modeling Mindset
- Walking through the Threat Modeling Process
 - Learning and Exercises
- Q&A (10-15 Minutes)



Who is Robert?



Current:

- Principal Application Security Architect / Threat Modeling Lead @ Aqua, Inc.
- Co-Host w/ Chris Romeo @ Application Security Podcast
- Co-Author @ Threat Modeling Manifesto
- Co-Author @ Threat Modeling Capabilities
- Co-Founder @ Threat Modeling Connect
- PhD student – Space Cybersecurity @ Capitol Technology University

Previous:

- Senior Security Architect / Threat Modeling Lead @ Bank of America

Contact: <https://www.linkedin.com/in/roberthurlbut/>

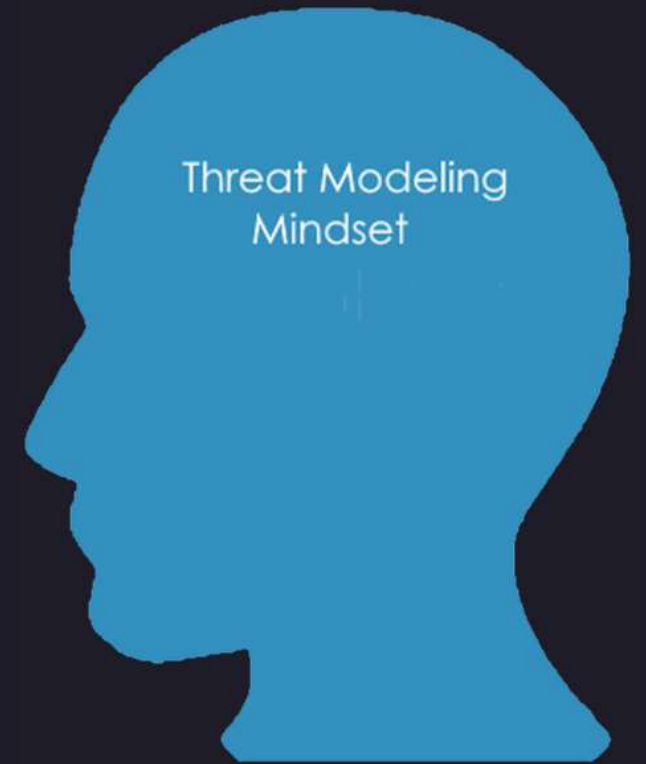


What do I want for you to get out of this activity?



- Develop a Threat Modeling Mindset through hands-on learning about the Threat Modeling Process

A Threat Modeling Mindset is ...



What is Threat Modeling?



Something we all do in our personal lives:

- When we lock our doors to our house
- When we lock the windows
- When we lock the doors to our car
- When we look around to cross the street



What is Threat Modeling? (continued)



When we think ahead on:

- What could go wrong (*ask “what if” questions*)
- Weigh risks
- Act accordingly

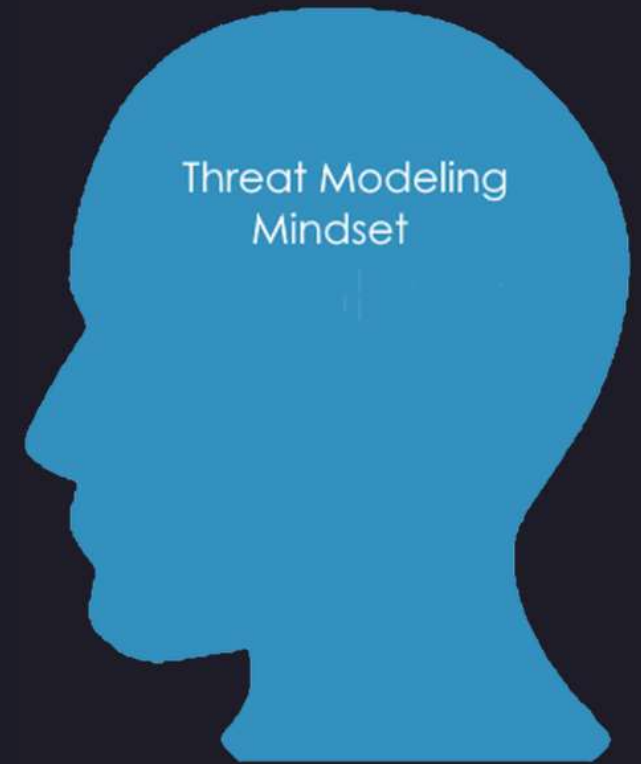
... we are **“threat modeling”**



A Threat Modeling Mindset is ...



Strategic vs Reactive
("thinking ahead" vs "hope we are safe")



What is Threat Modeling? (continued)



THREAT MODELING MANIFESTO

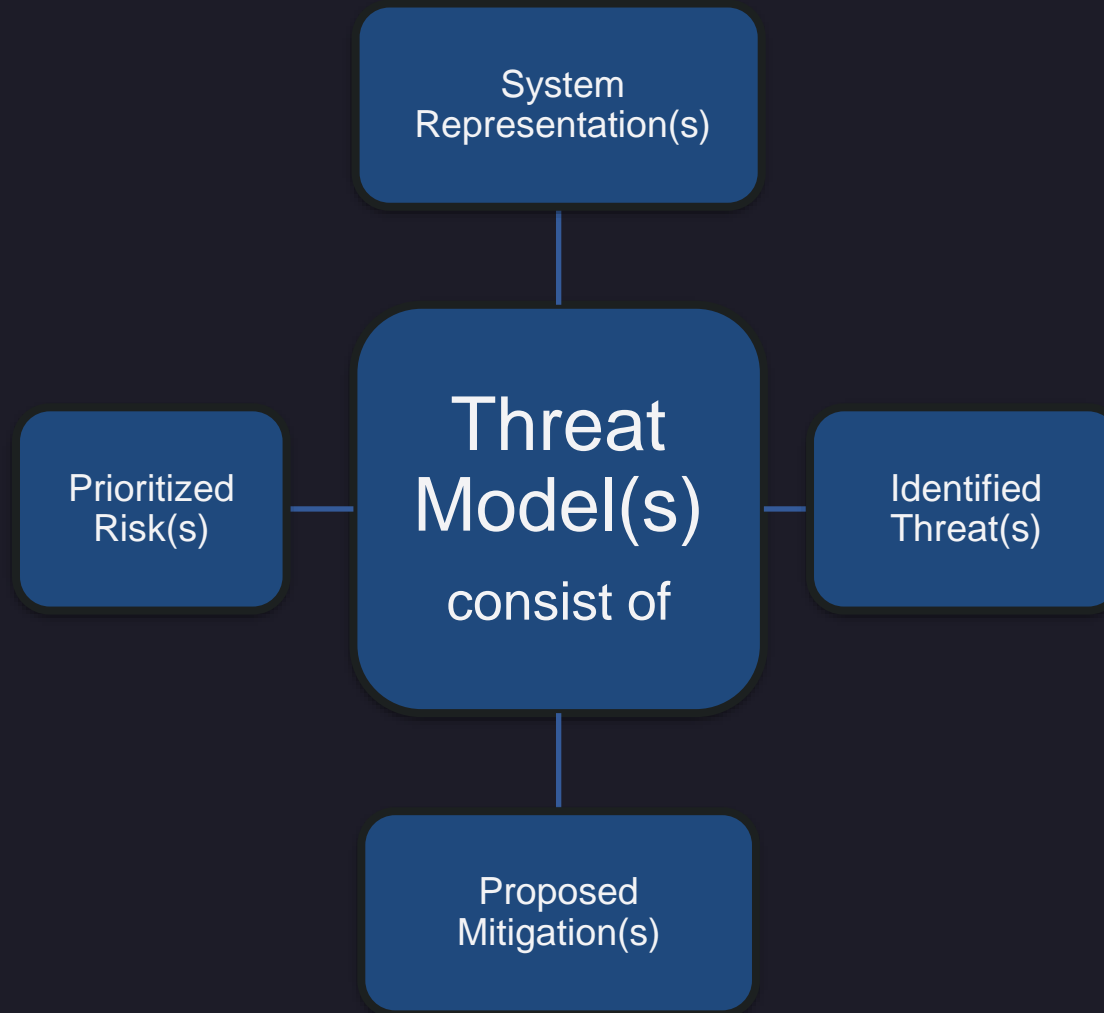
What is threat modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions:

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 enough job?

What is Threat Modeling? (continued)



Walking through the Threat Modeling Process



0. Assemble the Team (**Define**)

1. **Diagram** / understand your system and data flows

2. **Identify** threats

STRIDE, LIDDUN, ATT&CK, etc.

3. Document (**Identify** and **Mitigate**)

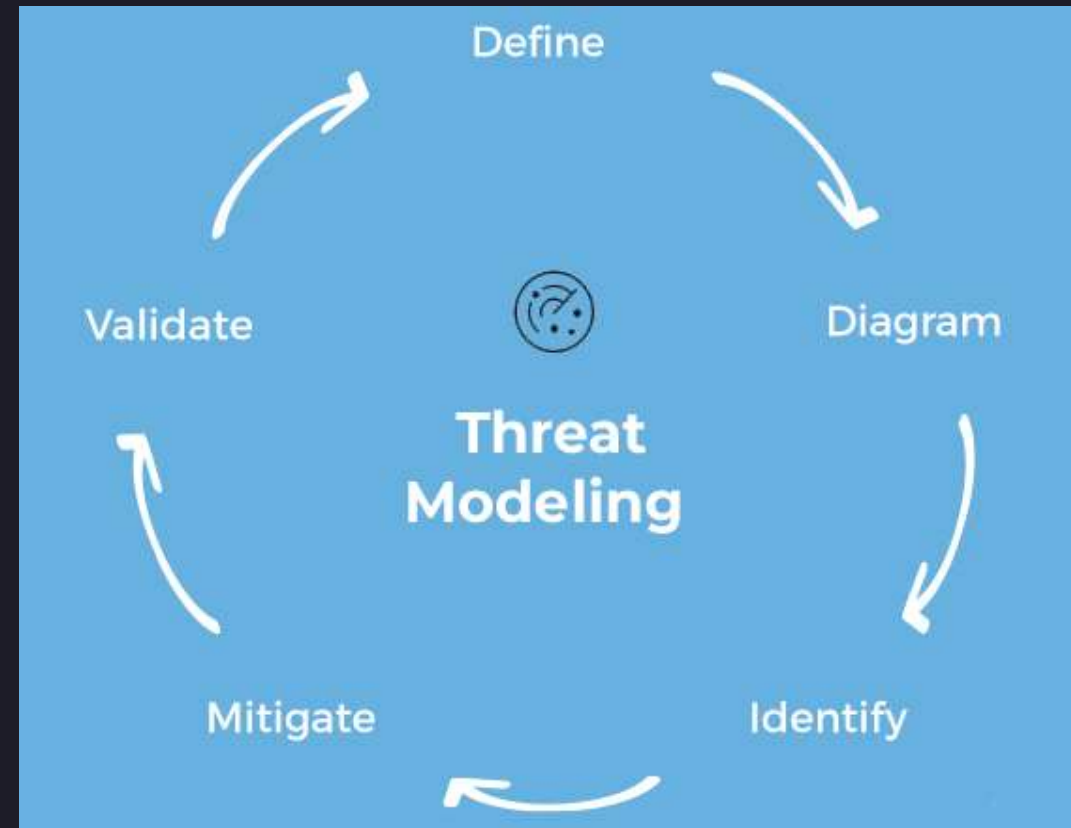
Elements of the system

Properties affected

Threats, mitigations, and risks

Action items

4. Review and Follow Up (**Validate**)



Threat Modeling Process



0. Assemble the Team (**Define**)

1. **Diagram** / understand your system and data flows

2. **Identify** threats

STRIDE, LIDDUN, ATT&CK, etc.

3. Document (**Identify** and **Mitigate**)

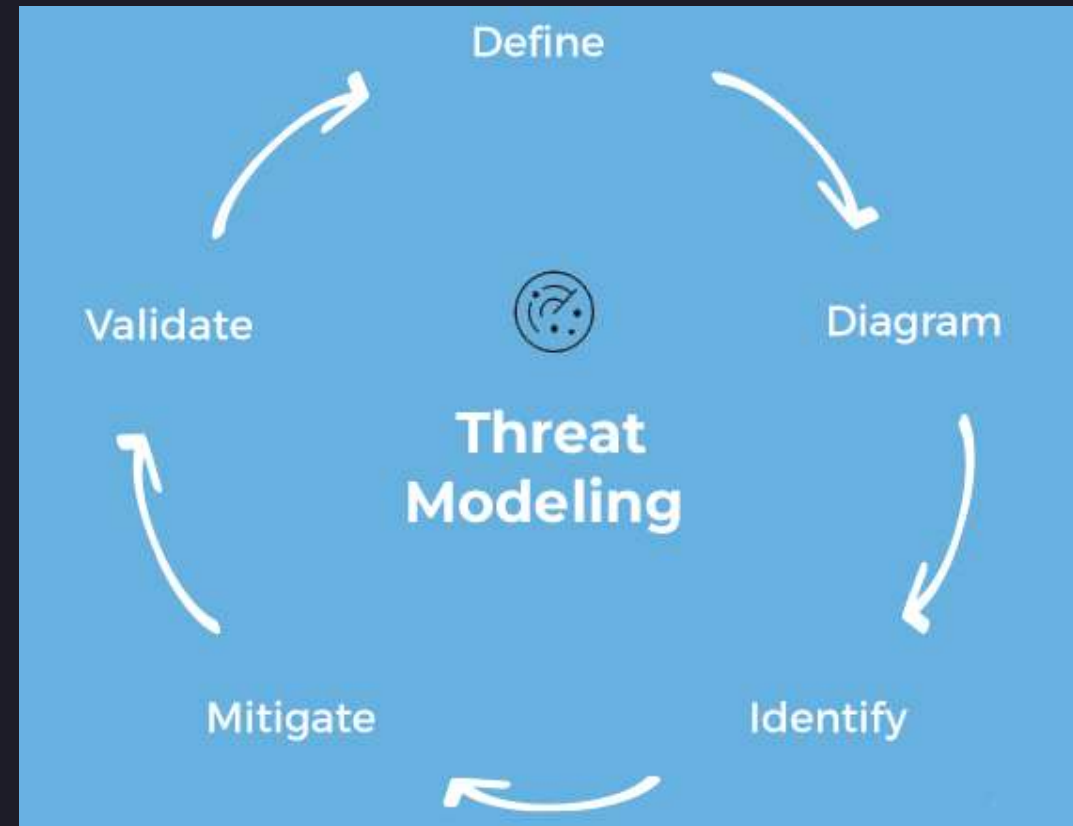
Elements of the system

Properties affected

Threats, mitigations, and risks

Action items

4. Review and Follow Up (**Validate**)



Threat Modeling Process: 0. Assemble the Team



- Software Developers / Testers
- Architects
- Project Managers
- Automation Engineers / Code Release Manager
- Security Champions
- Other Stakeholders

For this workshop, we will divide the larger group into breakout groups to represent different teams.

Threat Modeling Process: 0. Assemble the Team

Getting Started – Simple Tools



Diagramming
(Whiteboard -
Real or Virtual)



Documenting
(Word / Excel)
(Confluence / Jira)

For this workshop, we will use a Mural page to diagram and record threats/mitigations.

Threat Modeling Process: 0. Assemble the Team

Getting Started – Understanding Bugs vs Flaws



IEEE Computer Society's Center for Secure Design (2015)



Bug – an implementation-level software problem

Flaw – deeper level problem
- result of mistake or oversight at design level

In Threat Modeling, we try to identify design flaws to improve secure design

<http://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf>

Threat Modeling Process: 0. Assemble the Team

Getting Started – Understanding Bugs vs Flaws



Security coding bugs

- Coding errors
- Requires developers understanding secure coding
- Can be automated
- Patching less costly in production

Security design flaws

- Errors in design, security requirements, architecture
- Need contextual knowledge
- No automation
- Costly to change in production

Typical Threat Modeling Session



- Domain Knowledge
- Team Effort
- Business / Technical Goals
- Focused

Important: Be honest, leave ego at the door, no blaming!

Threat Modeling Process



0. Assemble the Team (**Define**)

1. **Diagram** / understand your system and data flows

2. **Identify** threats

STRIDE, LIDDUN, ATT&CK, etc.

3. Document (**Identify** and **Mitigate**)

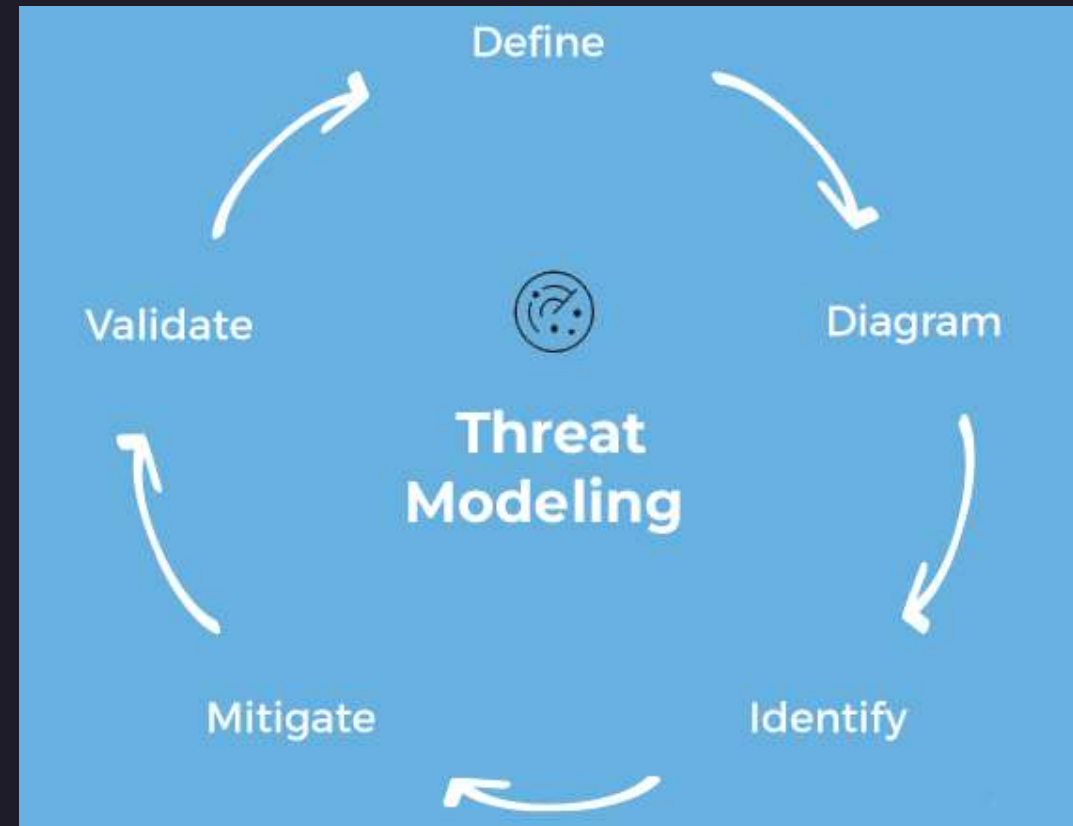
Elements of the system

Properties affected

Threats, mitigations, and risks

Action items

4. Review and Follow Up (**Validate**)



Threat Modeling Process: 1. What are we working on?

Diagram / understand the system and data flows








Document elements of the system and properties affected

At a minimum, document:

- Basic elements of how the system works
- Security concerns of any properties (i.e. what would happen if ...?)



Draw a Data Flow Diagram (DFD)

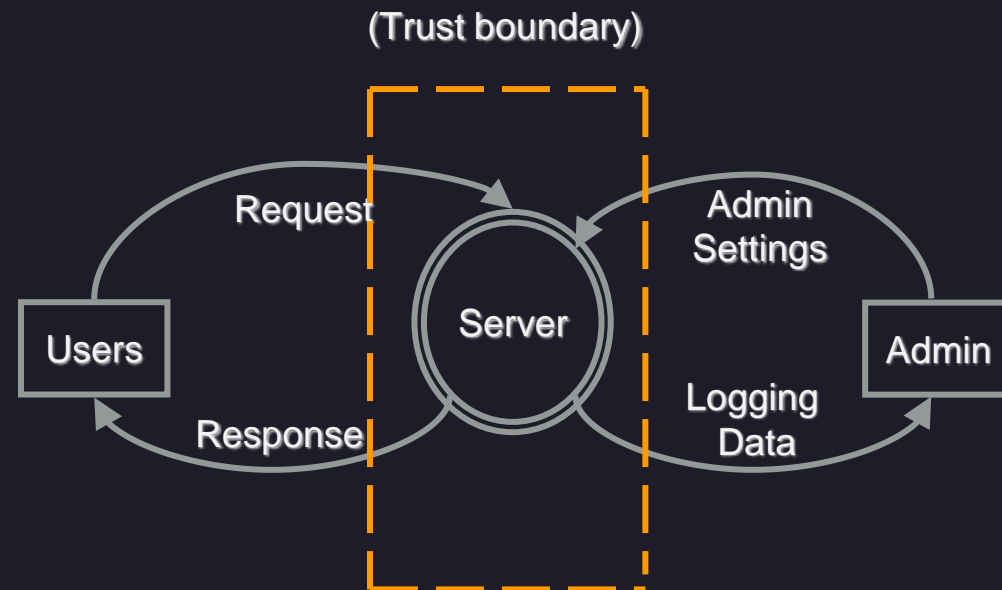
Notation element	Reference	Examples
	External entity	People (e.g., users), systems (e.g., other devices), cloud services, browsers
	Process	DDL, exe(D)COM, web service, virtual machine, threat
	Data store	File, database, registry, cache, cookie
	Data flow	http request or response, remote procedure call, UDP communication
	Trust boundary (inside you trust the processes and data stores, outside you don't)	Device boundary, process boundary

You can use the drawing tool of choice – however, try to stay with the basic shapes and meanings for consistency

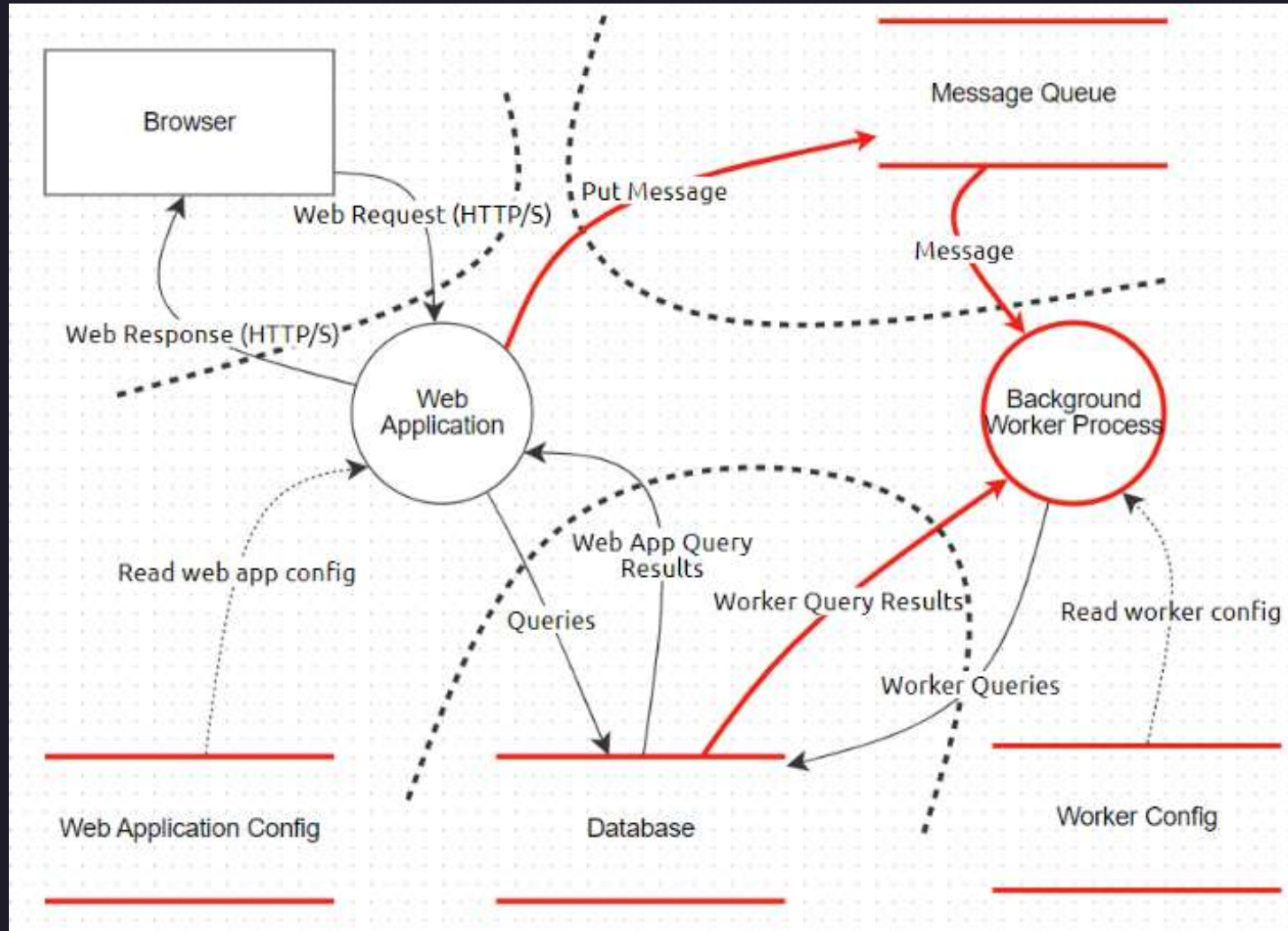
Draw a Data Flow Diagram (DFD) (continued)



Logical and component architecture
Communication flows
Data moved and stored



Draw a Data Flow Diagram (DFD) (continued)



(Sample DFD created with OWASP Threat Dragon 2.0)

Exercise #1: Draw a Data Flow Diagram (DFD) (10 mins)



ACME Web Application

Actors:

Internal: Service Staff

External: User

External Services:

Authentication Provider,
3rd Party Data and Service Participants,
Partner Organizations

Data Stores:

Internal: Logs, Database

External: Intermediate Data (Used by Partner
Orgs)

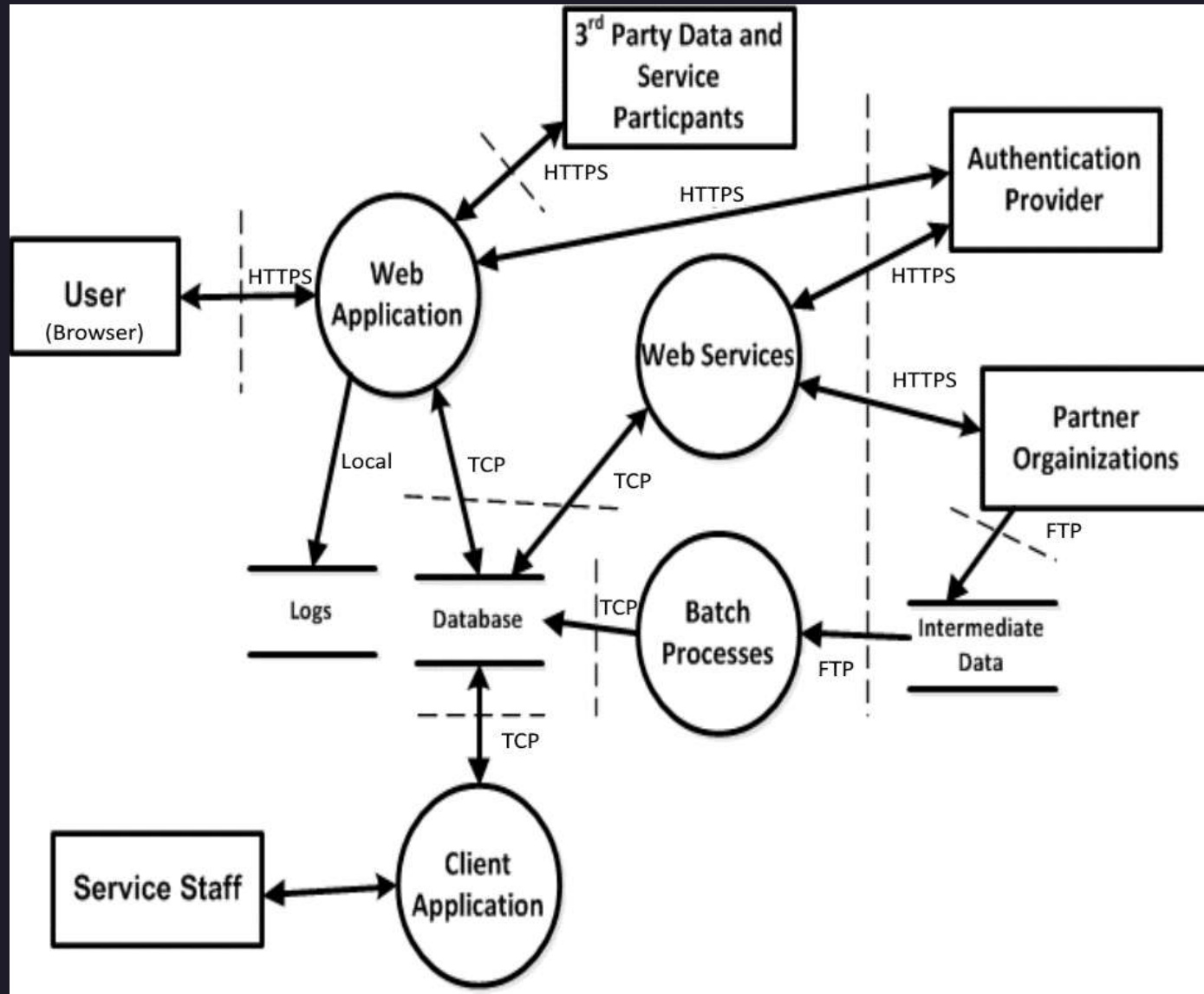
Processes:

Internal: Web Application, Web Services, Batch
Processes, Client Application

1. ~~Draw~~ Review a DFD (in interest of time)
2. Use the resources on the Mural board to help

Exercise #1: Draw a Data Flow Diagram (DFD)

ACME Web Application





Threat Modeling Process

0. Assemble the Team (**Define**)

1. **Diagram** / understand your system and data flows

2. **Identify** threats

STRIDE, LIDDUN, ATT&CK, etc.

3. Document (**Identify** and **Mitigate**)

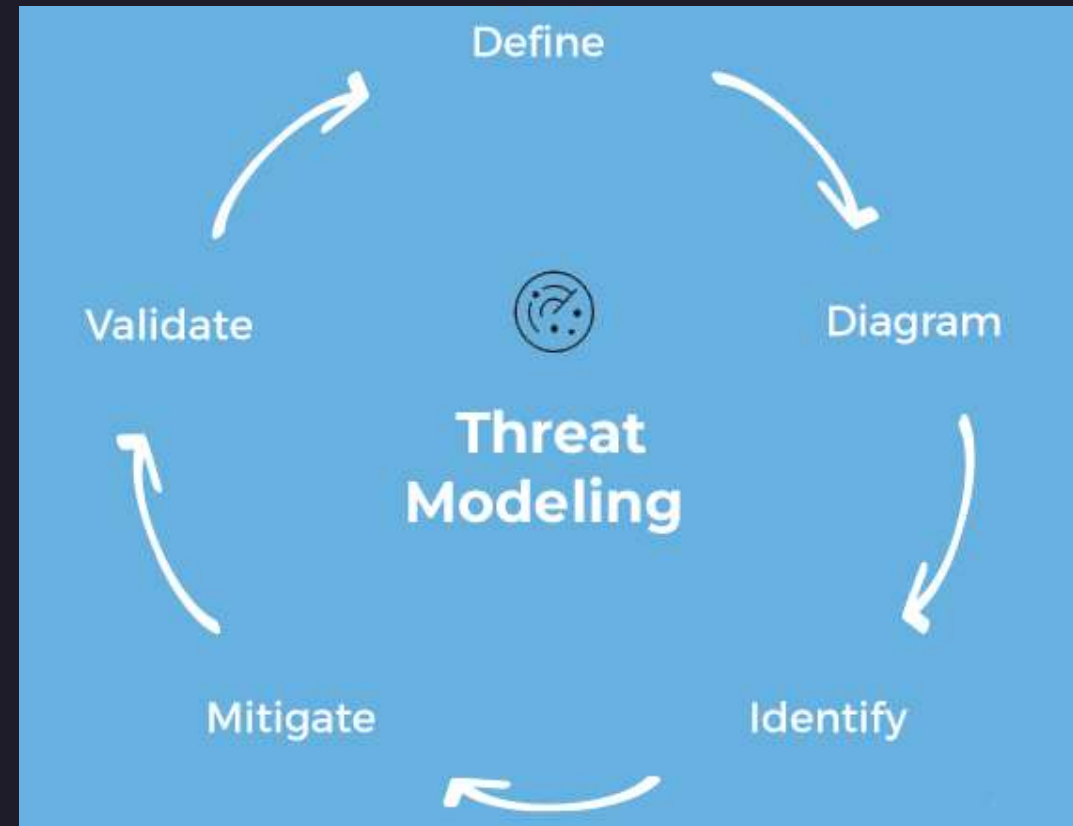
Elements of the system

Properties affected

Threats, mitigations, and risks

Action items

4. Review and Follow Up (**Validate**)

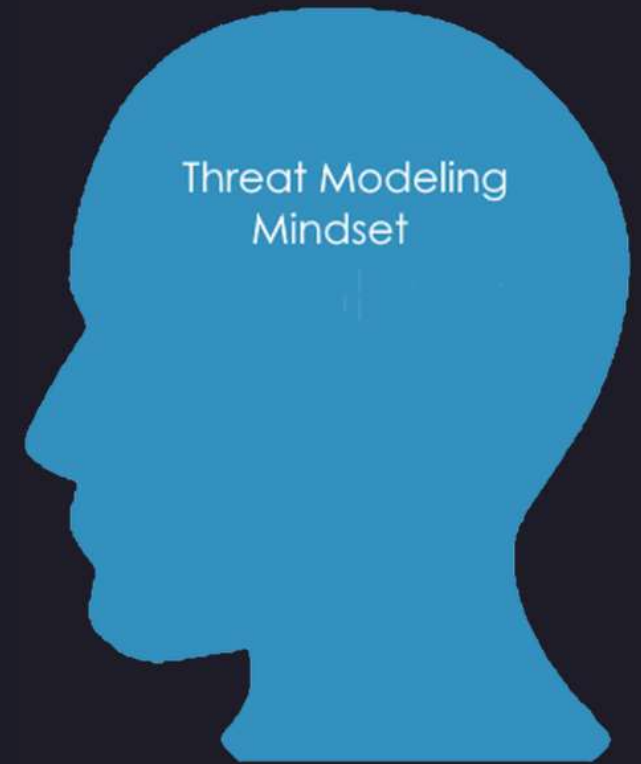


A Threat Modeling Mindset is ...



Strategic: *“thinking ahead”*

Asks questions:
“what if?”, “what could go wrong?”



Threat Modeling Process: 2. What could go wrong?

Identify threats: Introducing STRIDE



Threat	Property Violated	Threat Definition
Spoofing	Authentication	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-Repudiation	Claiming you didn't do something or were not responsible; can be honest or false
Information Disclosure	Confidentiality	Providing information to someone not authorized to access it
Denial of Service	Availability	Exhausting resources needed to provide service
Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do

Threat Modeling Process: 2. What could go wrong?

Identify threats: Applying STRIDE to a DFD



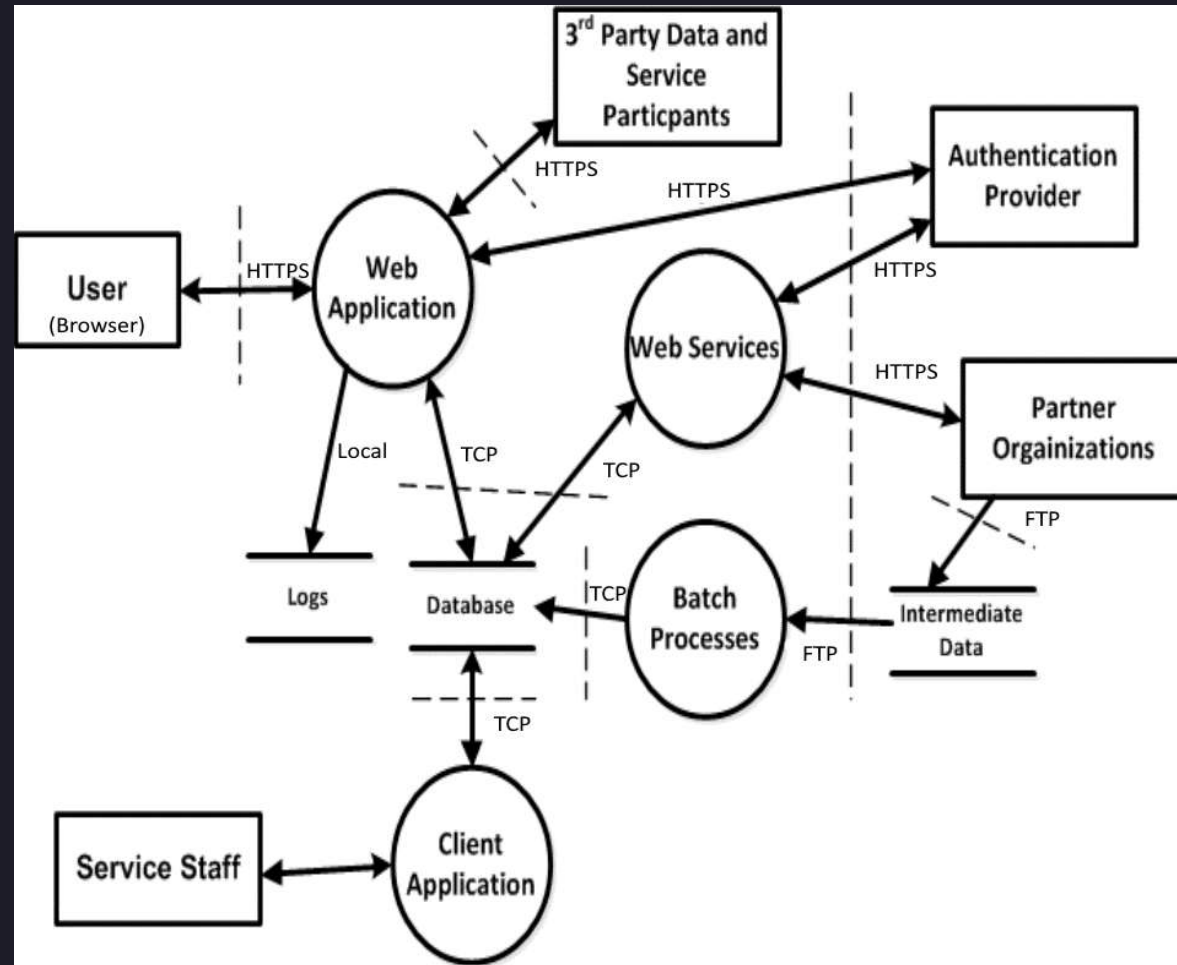
Options:

Each part of STRIDE applies to specific elements or interactions.

and/or

You can look at STRIDE per interaction.

ACME Web Application



Threat Modeling Process: 2. What could go wrong? Using STRIDE to Identify Threats



Spoofing

User could be spoofed by an attacker to connect to Web App

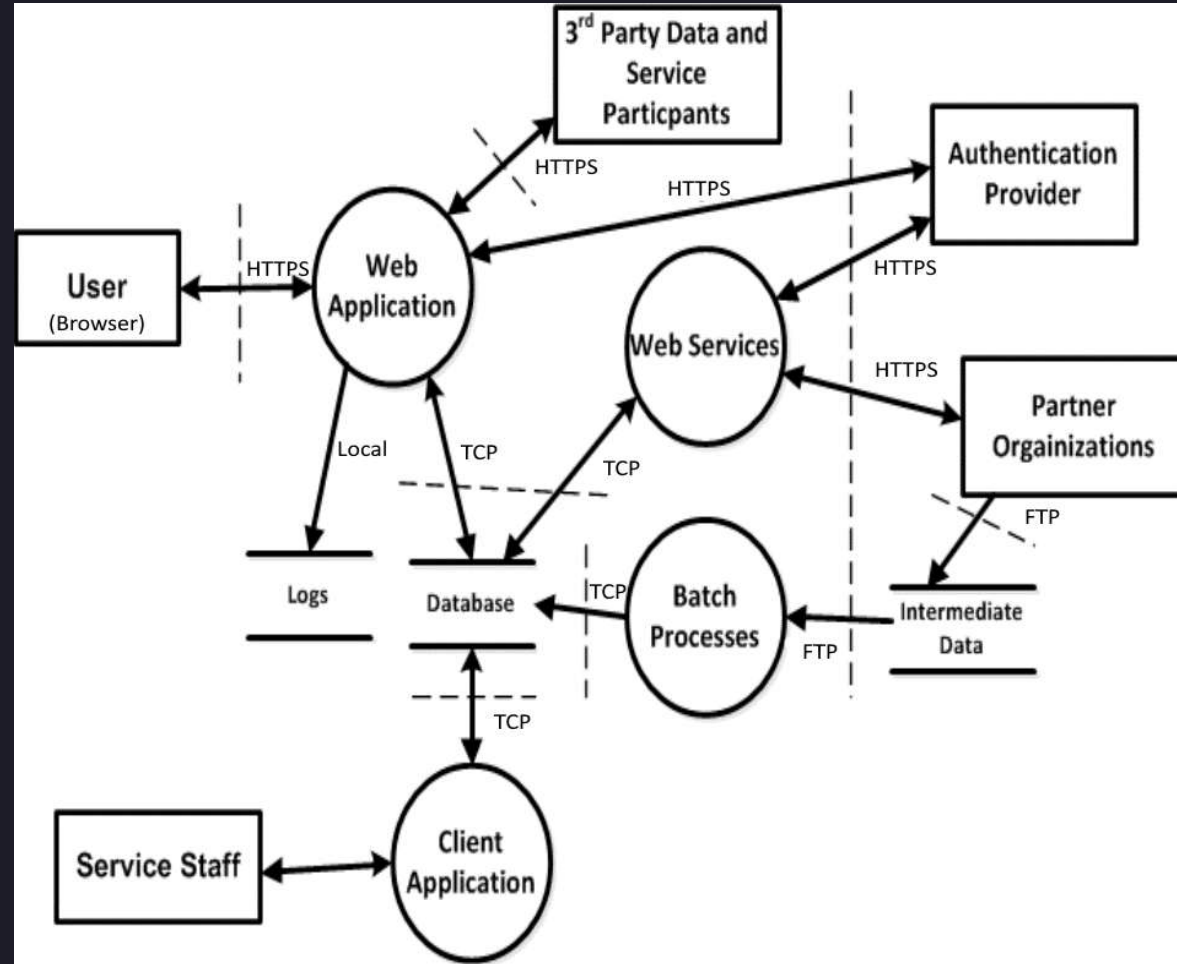
Tampering

Requests from User to Web App may be modified

Repudiation

How would we know actions performed by the Web App?

ACME Web Application



Threat Modeling Process: 2. What could go wrong? Using STRIDE to Identify Threats



Information Disclosure

Setting and getting credentials could be exposed in transit

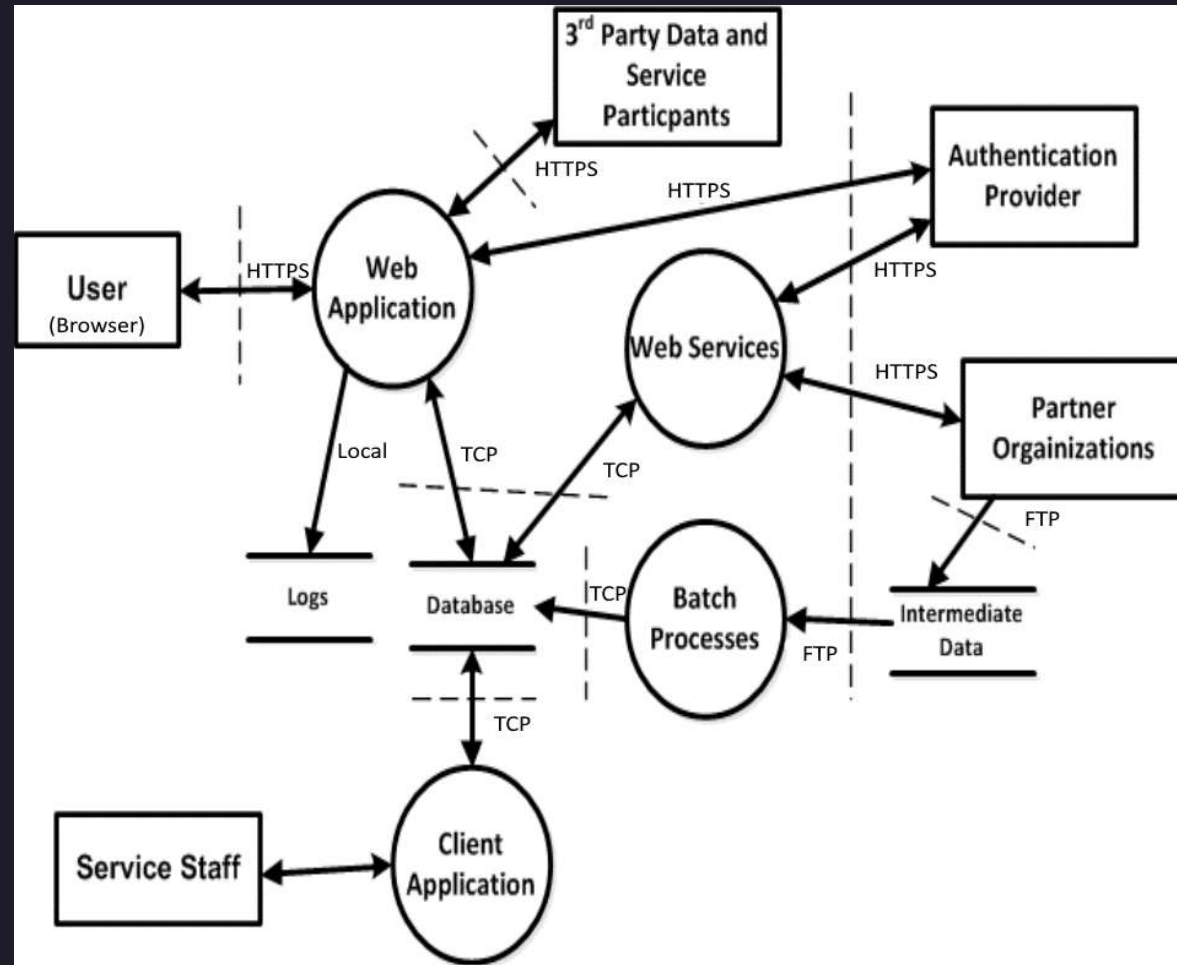
Denial of Service

What happens if Authentication Service is not available?

Elevation of Privilege

Does audit data have access control for reading?

ACME Web Application



Threat Modeling Process: 2. What could go wrong?

Identify threats – Many Ways



- STRIDE (software-centric)
- LINDDUN (privacy-focused)
- Attack Trees (asset or attacker-centric)
- PASTA (risk-centric)
- MITRE ATT&CK or D3FEND (intrusion-centric knowledge bases)

Other:

- Card Games - OWASP Cornucopia, Elevation of Privilege
- Use Cases/Abuse Cases

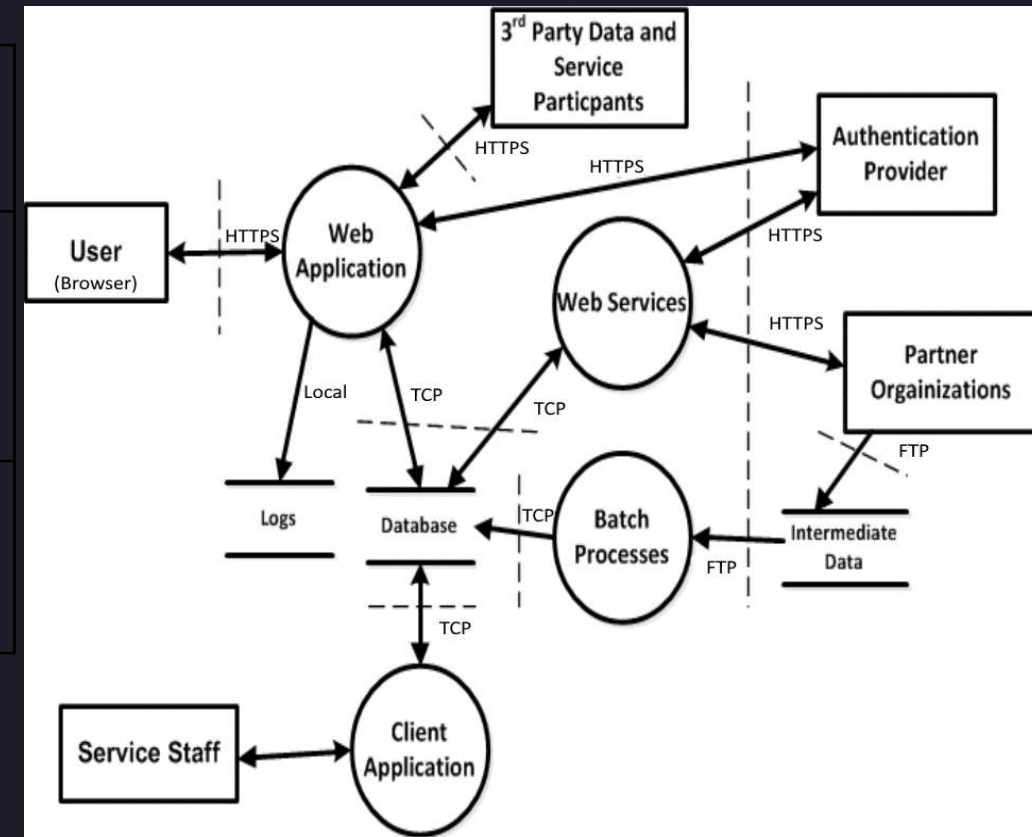
Threat Modeling Process: 2. What could go wrong? Using STRIDE to Identify Threats



Threat Model for ACME Web Application

Threat	STRIDE (Optional)	
Partner Organization communication to Web Services may be compromised	Tampering, Information Disclosure	
Logs for Web Application may be tampered with	Tampering, Repudiation	

ACME Web Application



Threat Modeling Process: 2. What could go wrong?

Identify threats – Ask Questions



Who's interested in the apps and/or data (threat agents)?

What are the goals (assets)?

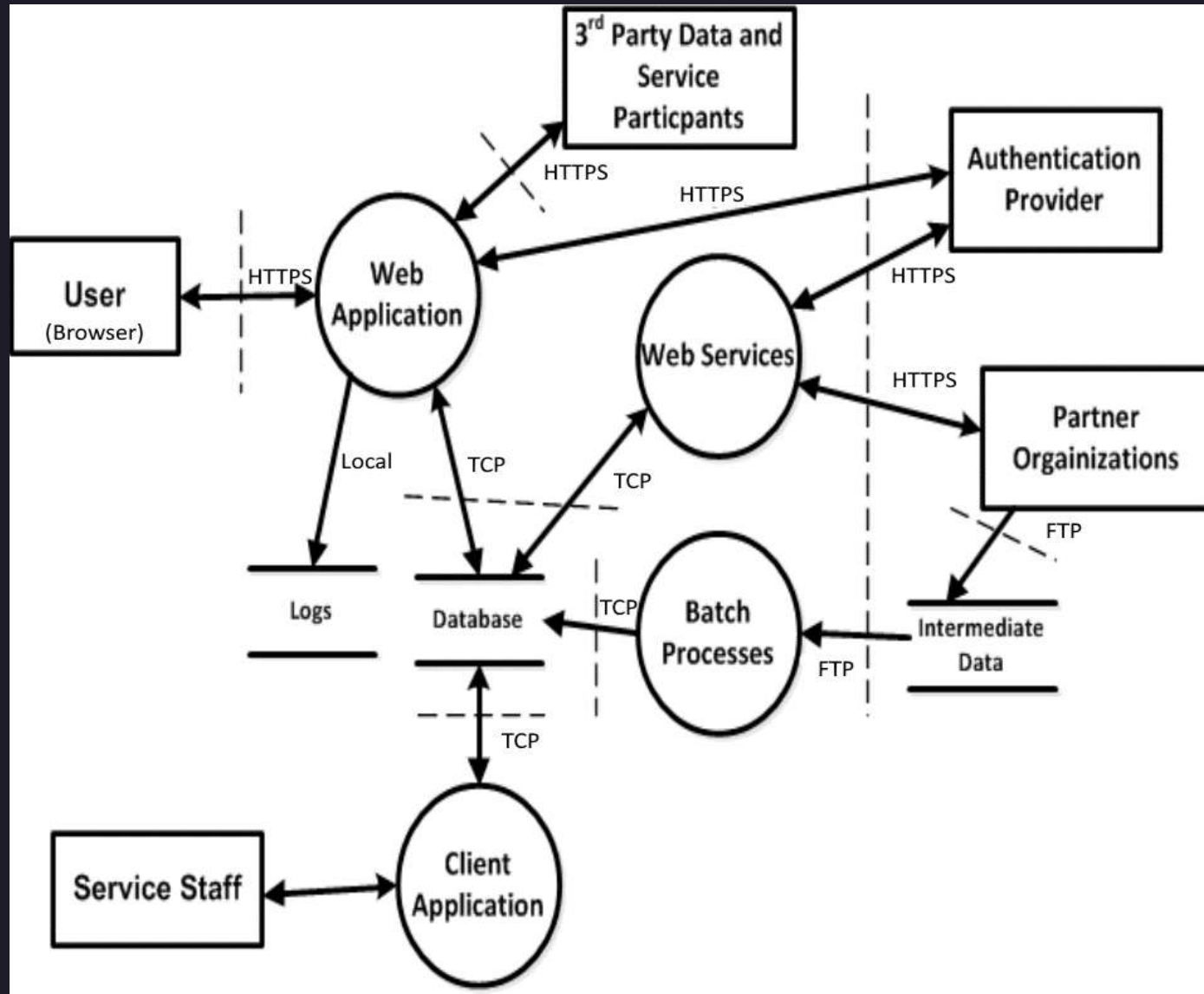
What are the attack methods (how)?

Are there any attack surfaces (trust boundaries) exposed?

Are there any input/output (data flows) missing?

Exercise #2: Identify threats (10-15 mins)

ACME Web Application



1. Identify threats
2. Use the resources on the Mural board to help

A Threat Modeling Mindset?



*“Threat modeling is the use of abstractions to aid in thinking about risks. [...] Threat modeling is the key to a focused defense. Without threat models, you can never stop playing whack-a-mole.”**



(* Threat Modeling: Designing for Security (2014)
by Adam Shostack)

A Threat Modeling Mindset?



*“Threat modeling is the use of abstractions to aid in thinking about risks. [...] Threat modeling is the key to a focused defense. Without threat models, you can never stop playing whack-a-mole.”**



(* Threat Modeling: Designing for Security (2014)
by Adam Shostack)

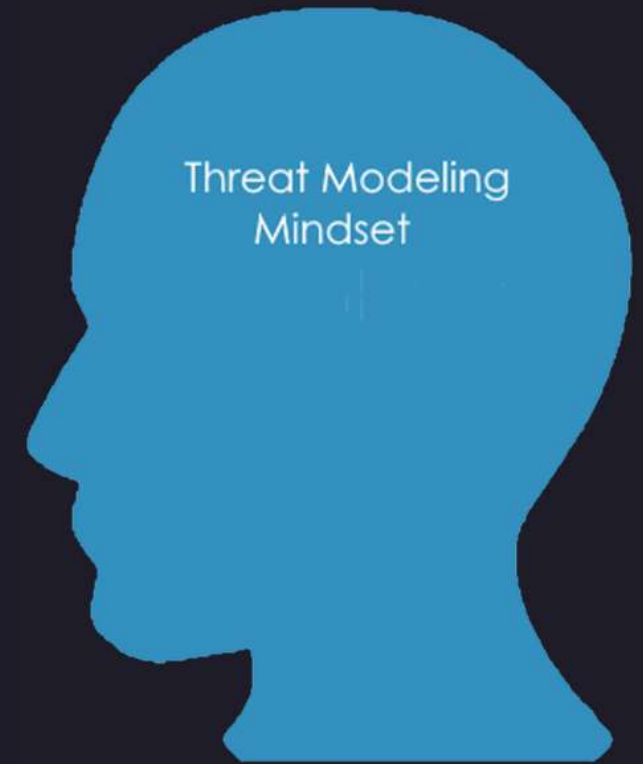
A Threat Modeling Mindset is ...



Strategic: *“thinking ahead”*

Asks questions:
“what if?”, “what could go wrong?”

Prepared: *“focused defense”*





Threat Modeling Process:

3. What are we going to do about it?

Document what you find

STRIDE	Example controls
Identity Assurance / Authentication (Spoofing)	<ul style="list-style-type: none">• Authentication based on key exchange• Decide on single-factor, two-factor, or multi-factor authentication• Offload authentication to another provider• Restrict authentication to certain IP ranges or locations
Integrity (Tampering)	<ul style="list-style-type: none">• Data protected from tampering with cryptographic integrity mechanisms• Only enumerated authorized users may modify data
Non-Repudiation (Repudiation)	<ul style="list-style-type: none">• Maintain logs• Digital signature
Confidentiality (Information Disclosure)	<ul style="list-style-type: none">• Data in files / database will only be available to authorized users• Name / existence of database will only be exposed to authorized users• Content and existence of communication between Alice and Bob will only be exposed to these authorized users
Availability (Denial of Service)	<ul style="list-style-type: none">• Rate limiting or throttling access to a service• Real-time monitoring of log files and other resources to note sudden changes
Least Privilege / Authorization (Elevation of Privilege)	<ul style="list-style-type: none">• System has a central authorization engine• Authorization controls stored with the item being controlled using ACLs• System limits who can write data to a higher integrity level• System uses roles/accounts or permissions to manage access



Threat Modeling Process:

3. What are we going to do about it?

Determine mitigations

Mitigation Options:

- Leave as-is

- Remove from product

- Remedy with technology countermeasure

- Warn user

Make the mitigations / countermeasures part of your
Security acceptance criteria



Threat Modeling Process:

3. What are we going to do about it?

Determine risks

What is the risk associated with the vulnerability and threat identified?

Risk is product of two factors:

Ease of exploitation

Business impact

Risk Management

FAIR (Factor Analysis of Information Risk) – Jack Freund, Jack Jones

Risk Rating (High, Medium, Low)



Threat Modeling Process:

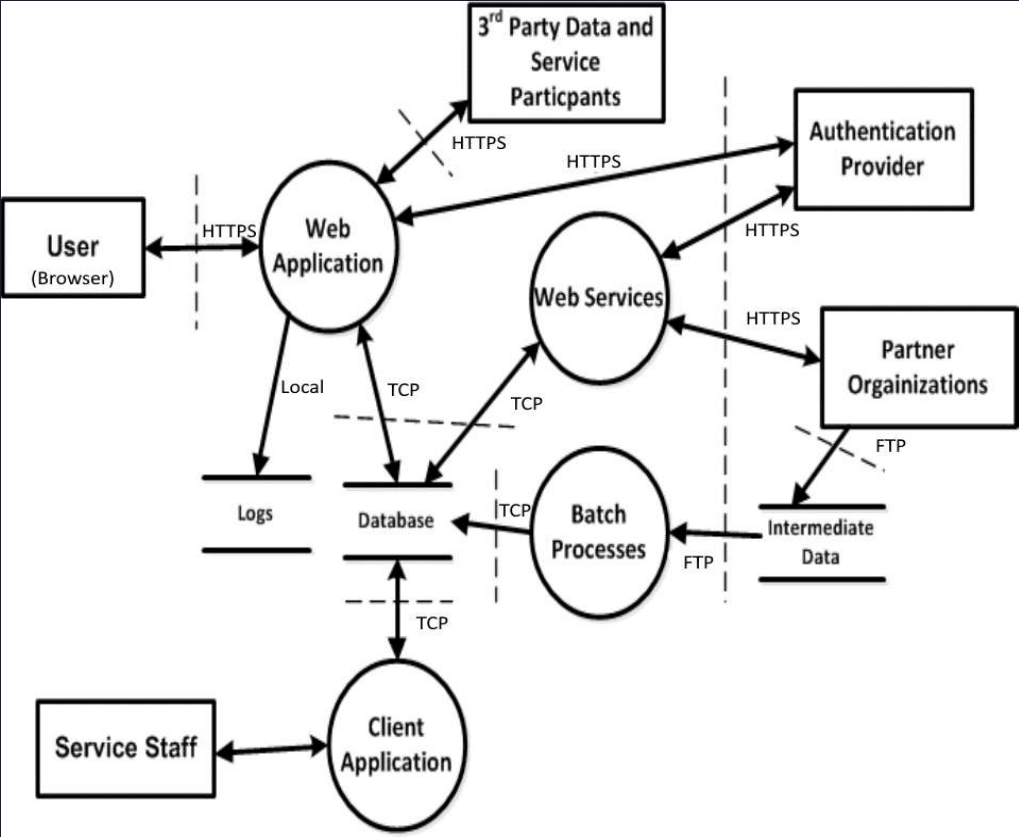
3. What are we going to do about it?

Document threats / mitigations / risks / action items

Threat Model for ACME Web Application

Threat	Mitigation / (Risk)	Action Items & Questions
Partner Organization communication to Web Services may be compromised	Implement encryption (HTTPS TLS 1.2+) and validation of message integrity (High)	Should we limit to TLS 1.3? Review best validation of messages.
Logs for Web Application may be tampered with	Apply access control on logs, send logs to centralized server (Medium)	Review access control options.

ACME Web Application





Threat Modeling Process:

3. What are we going to do about it?

Document threats / mitigations / risks / action items

STRIDE / Threats and Mitigations Table					
ID	Threat Description	STRIDE Property(ies)	Mitigation(s)	Action Item(s)	Notes
1	Sample Spoofing Threat	Spoofing, Repudiation	1. Add authentication controls and logging of successes and failures	1. Review current controls 2. Test / verify controls work as expected	Sample Notes

At a minimum, document:

- Threat

- STRIDE mapping (if relevant)

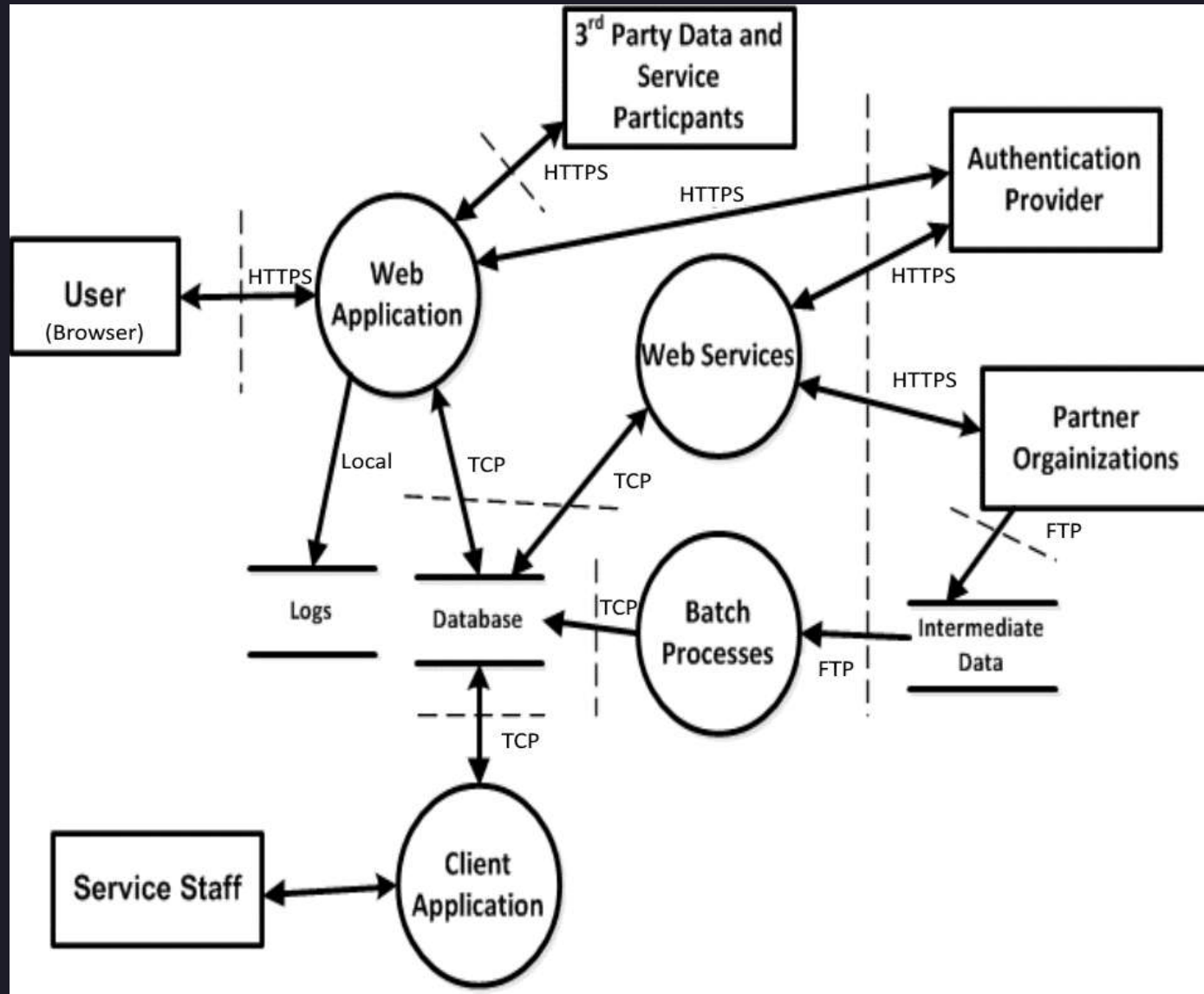
- Mitigation(s) (currently implemented)

- (Optionally) Risk Rating(s)

- Action Item(s) (mitigations to be implemented)

Exercise #3: Determine mitigations (10-15 mins)

ACME Web Application

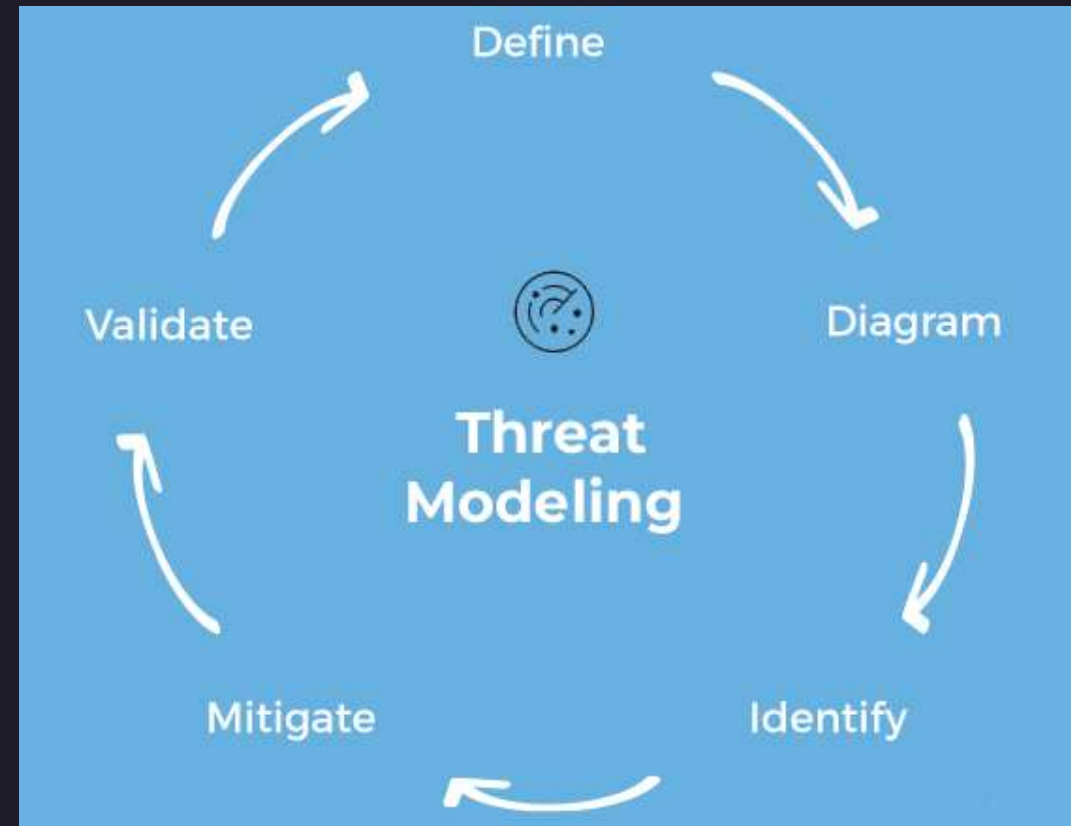


1. Identify threats
2. Use the resources on the Mural board to help

Threat Modeling Process



0. Assemble the Team (**Define**)
1. **Diagram** / understand your system and data flows
2. **Identify** threats
 - STRIDE, LIDDUN, ATT&CK, etc.
3. Document (**Identify** and **Mitigate**)
 - Elements of the system
 - Properties affected
 - Threats, mitigations, and risks
 - Action items
4. Review and Follow Up (**Validate**)



Threat Modeling Process:

4. Did we do a good job?

Review and follow up



Document findings and decisions

File bugs or new requirements (as stories)

Verify bugs fixed / new requirements (stories) implemented

Did we miss anything? Review again

Anything new? Review again



Threat Modeling Process:

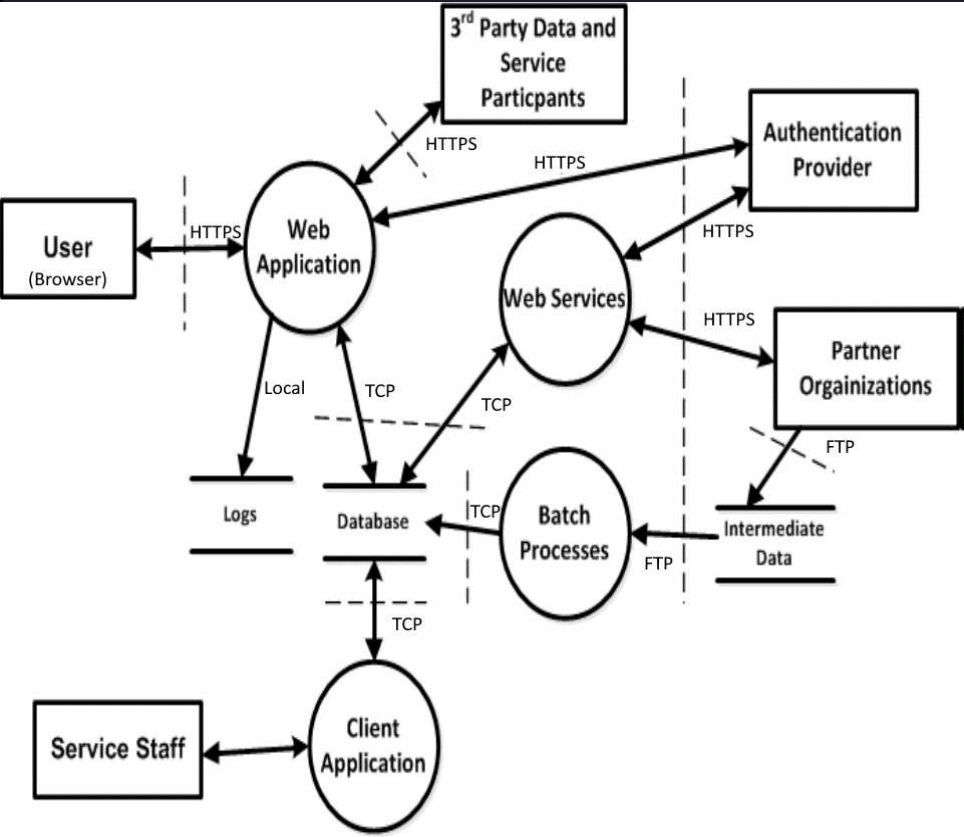
3. What are we going to do about it?

Document threats / mitigations / risks / action items

Threat Model for ACME Web Application

Threat	Mitigation / (Risk)	Action Items & Questions	Review / Follow-up
Partner Organization communication to Web Services may be compromised	Implement encryption (HTTPS TLS 1.2+) and validation of message integrity (High)	Should we limit to TLS 1.3? Review best validation of messages.	Address issue(s) in next Sprint
Logs for Web Application may be tampered with	Apply access control on logs, send logs to centralized server (Medium)	Review access control options.	Evaluate if will fix in next Sprint or future Sprint

ACME Web Application



Repeat or iterate as needed



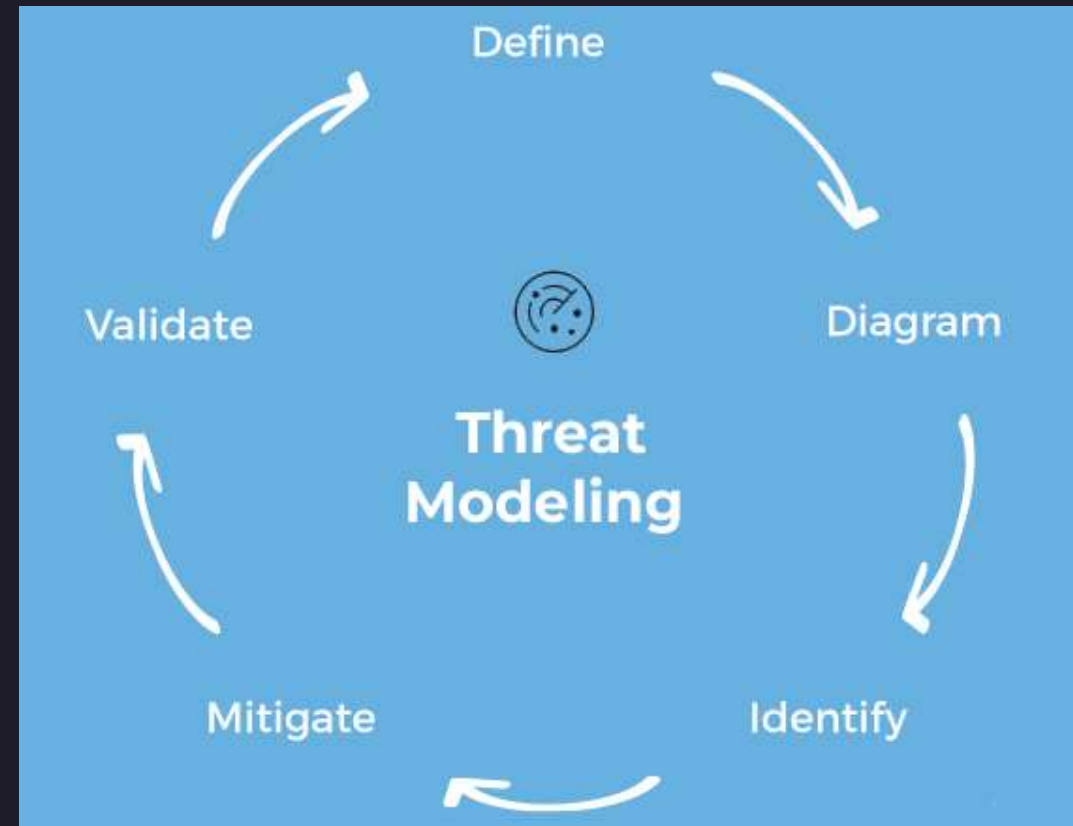
Consider a baseline threat model for your project if you have never, ever created a threat model before

Then, update and/or review your threat model as you continue to add new or updated features

Threat Modeling Process



0. Assemble the Team (**Define**)
1. **Diagram** / understand your system and data flows
2. **Identify** threats
 - STRIDE, LIDDUN, ATT&CK, etc.
3. Document (**Identify** and **Mitigate**)
 - Elements of the system
 - Properties affected
 - Threats, mitigations, and risks
 - Action items
4. Review and Follow Up (**Validate**)



A Threat Modeling Mindset is ...

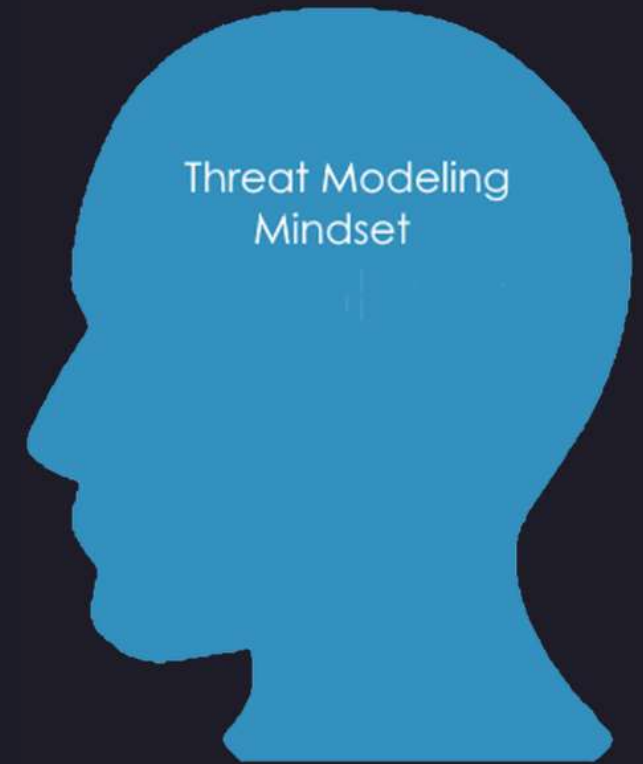


Strategic: *“thinking ahead”*

Asking questions:
“what if?”, “what could go wrong?”

Prepared: *“focused defense”*

Active: *“review / follow through”*

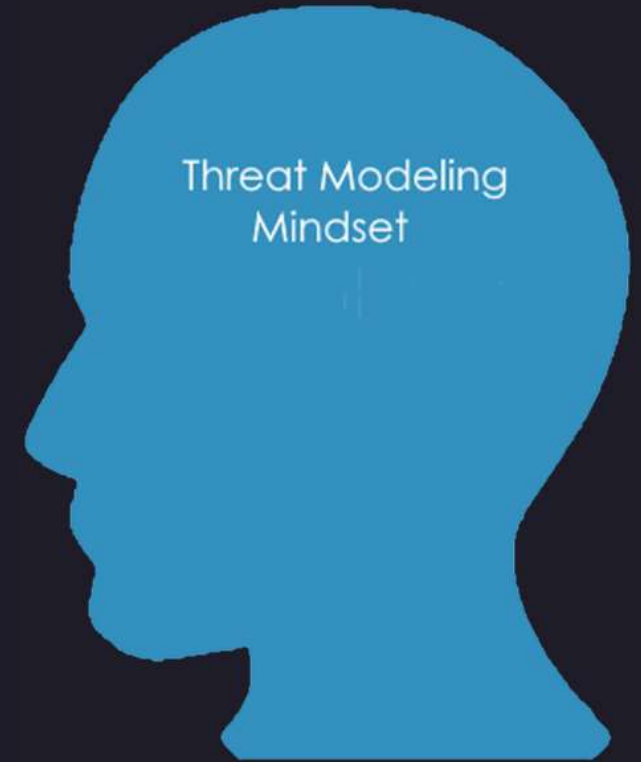


Key Takeaways



Pursue a Threat Modeling Mindset:

- Be strategic: think of secure design before new features
- Ask “what if” / “what could go wrong” questions
- Focus on and be prepared where defenses may fail
- Actively review / follow through (and repeat) as needed





“Threat Modeling Manifesto” (2020)

<https://threatmodelingmanifesto.org/>

Definition

Values

Principles

Anti-Patterns





“Threat Modeling Capabilities” (2024)

<https://www.threatmodelingmanifesto.org/capabilities/>

Strategy

Education

Creating Threat Models

Acting on Threat Models

Communications

Measurement

Program Management



Resources - Books



Threat Modeling as a Practice:

Threat Modeling: A Practical Guide for Development Teams (2020)
Izar Tarandach and Matthew Coles

Threat Modeling: Designing for Security (2014)
and
Threats: What Every Engineer Should Learn from Star Wars (2023)
Adam Shostack

Securing Systems: Applied Architecture and Threat Models (2015)
Brook S.E. Schoenfield

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (2015)
Marco Morana and Tony Uceda Velez

Resources - Books



Applied Threat Modeling:

Hacking Kubernetes: Threat-Driven Analysis and Defense (2021)

Andrew Martin, Michael Hausenblas

Playbook for Threat Modeling Medical Devices (2021)

MITRE: <https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf>

Questions and Answers / Learn More



Check out:
***Threat Modeling Hackathon 2025 –
Resource Pack***

Contact: <https://www.linkedin.com/in/roberthurlbut/>

