Threat modeling Process

Threat modeling

Threat modeling is an engineering technique that you can use to help identify threats, attacks, vulnerabilities, and countermeasures that might be relevant to your application.

Threat Modeling Process

Security objectives

Security objectives are goals and constraints related to the confidentiality, integrity, and availability of your data and application.

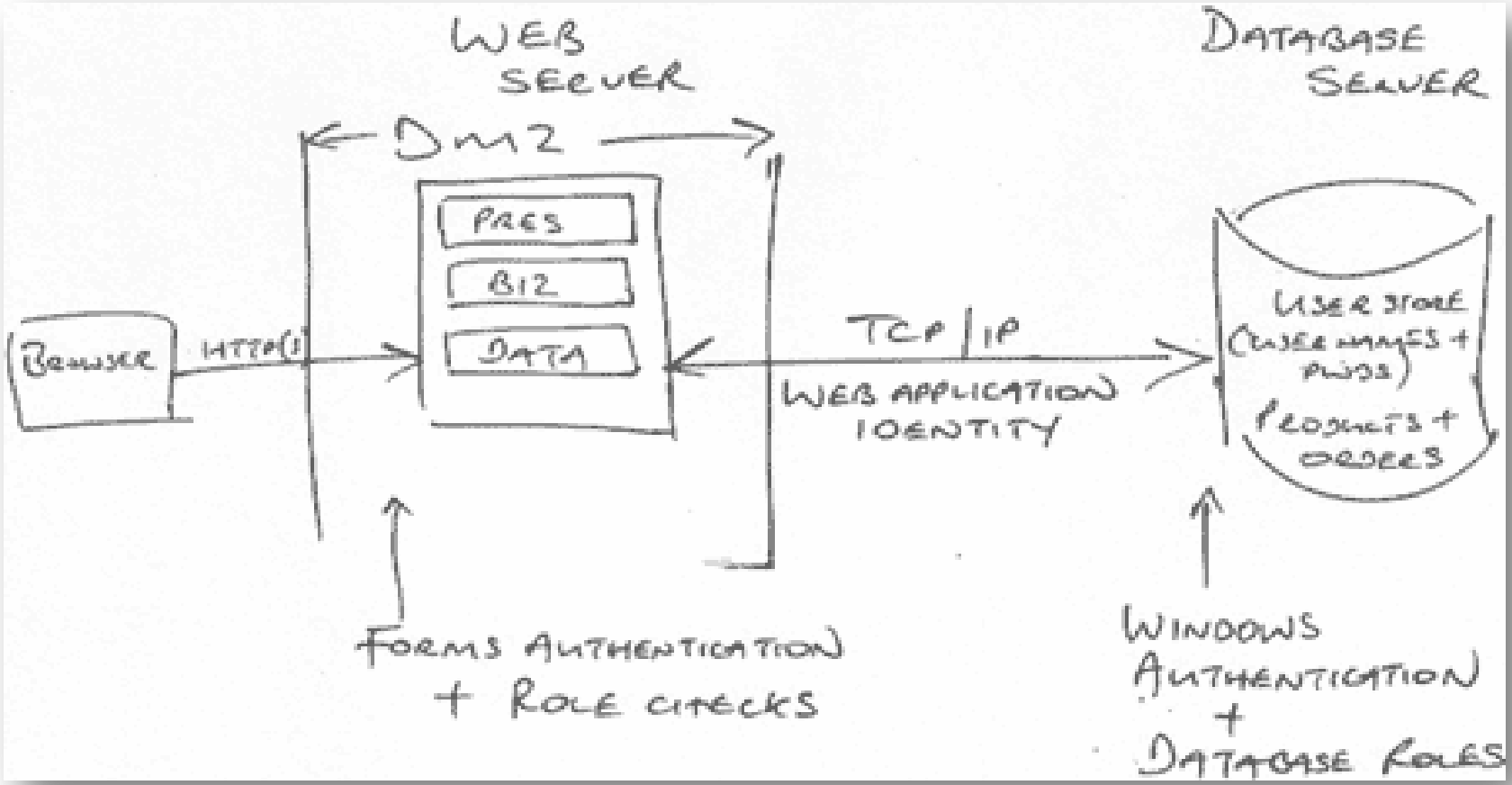
1. Prevent attackers from obtaining sensitive customer data, including passwords and profile information.

2. Meet service-level agreements for application availability.

3. Protect the company's online business credibility.

Threat Modeling Process

Draw End-to-End Deployment Scenario



Identify Roles

	Objects				
Subjects	User creation	Permission modification	Object creation	Object removal	Object read
Admin	✓	✓			
Content creator			✓	✓	✓
Reader					✓
Anonymous					✓

Identify Key Usage Scenarios

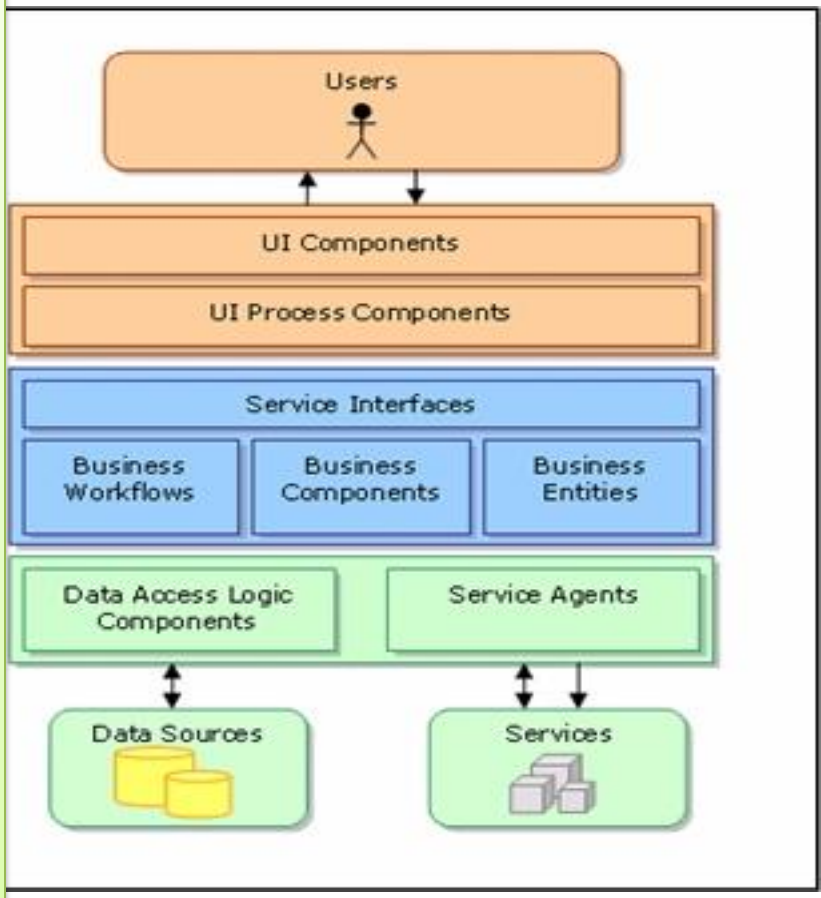
Identify the dominant application functionality and usage, and capture the Create, Read, Update, and Delete aspects.

1. Employee views financial data.
2. Employee updates personal data.
3. Manager views employee details.
4. Manager deletes employee records.

Identify Key Usage Scenarios

Identify Technologies

1. Operating systems .
2. Web server software
3. Database server software.
4. Technologies used in the presentation, business, and data access layers .
5. Development languages .

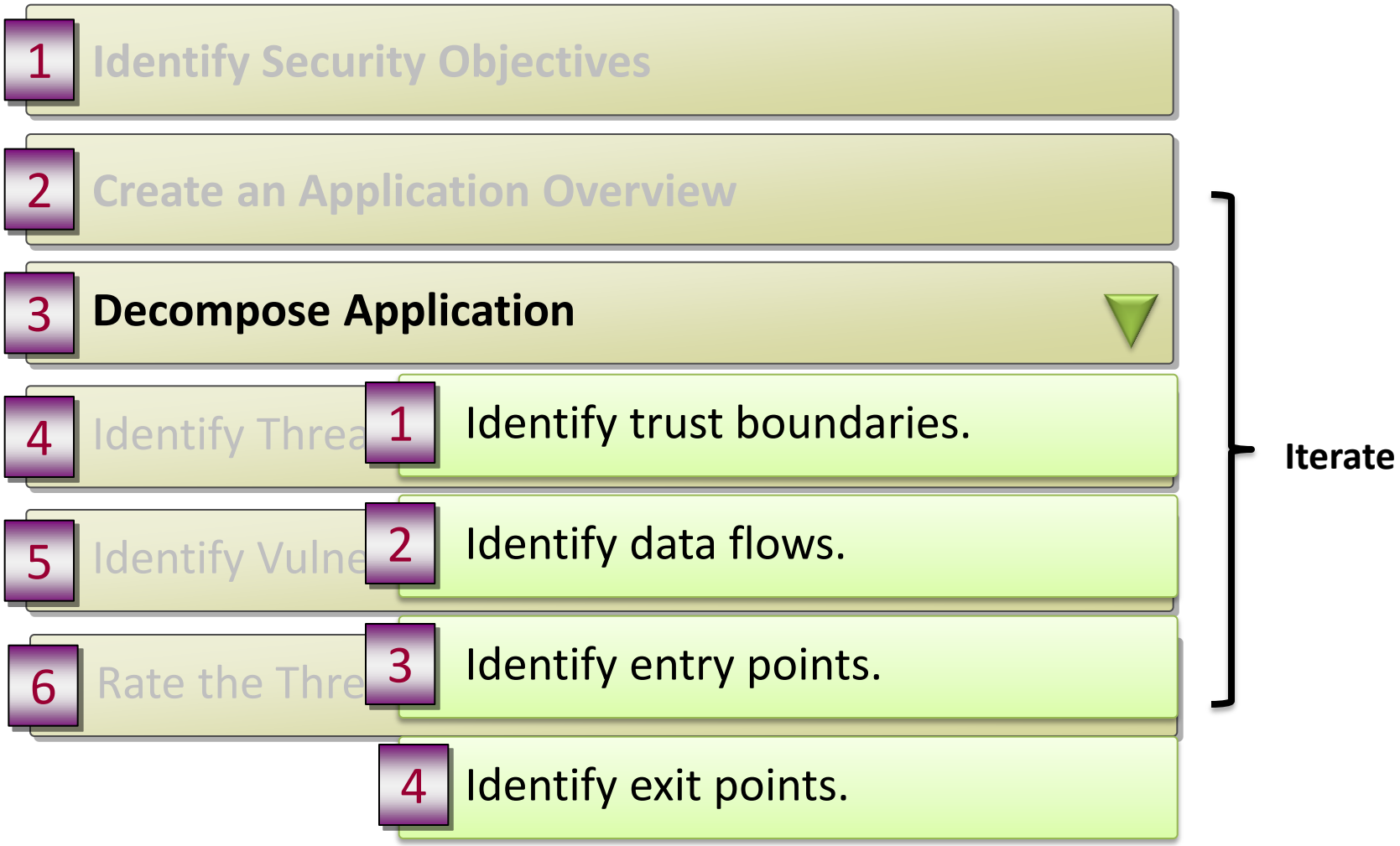


Identify Application Security Mechanisms

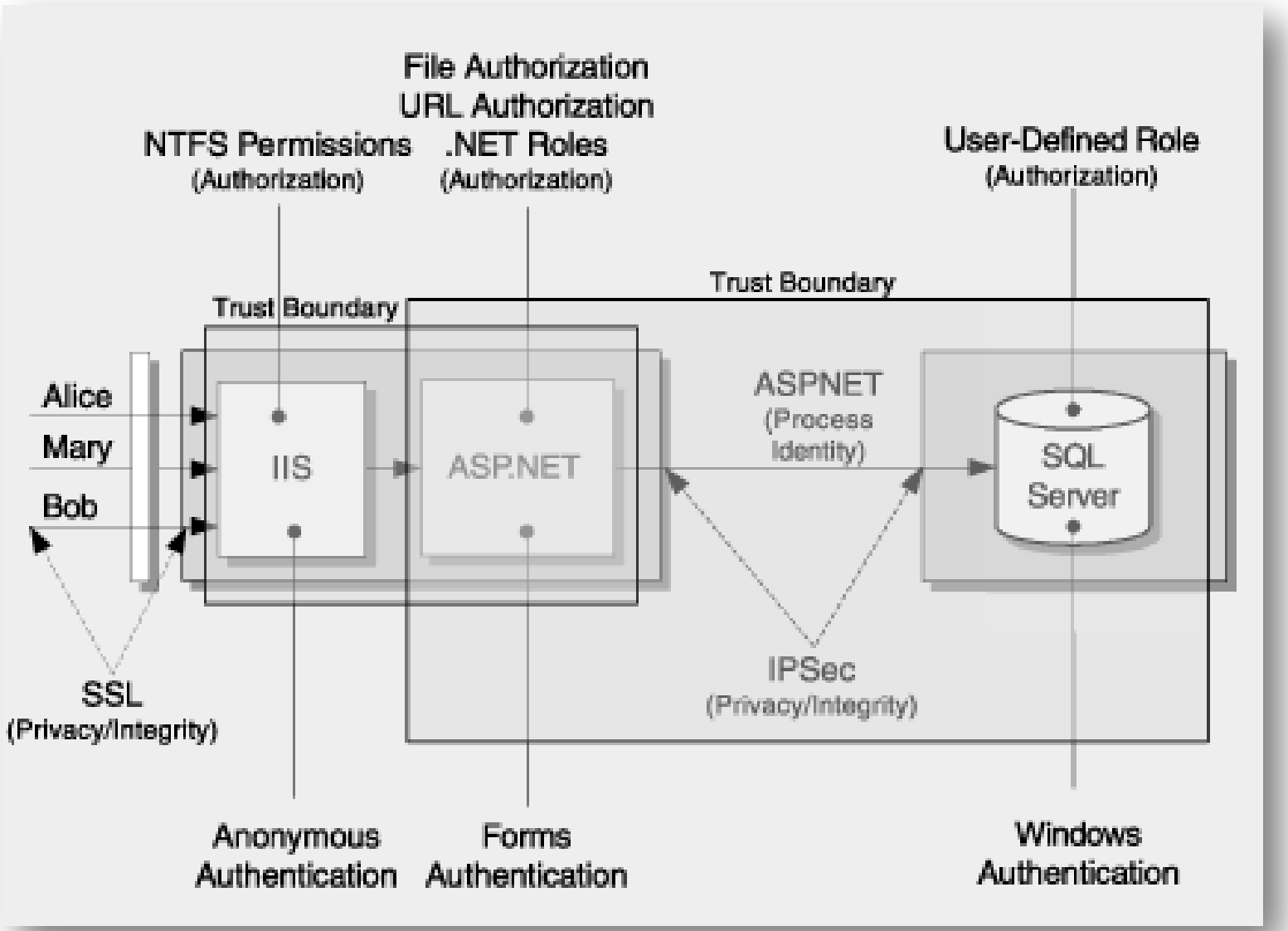
Identify any key points that you know about the following:

1. Input and data validation
2. Authentication , Authorization
3. Configuration management
4. Sensitive data
5. Session management
6. Cryptography
7. Parameter manipulation
8. Exception management
9. Auditing and logging

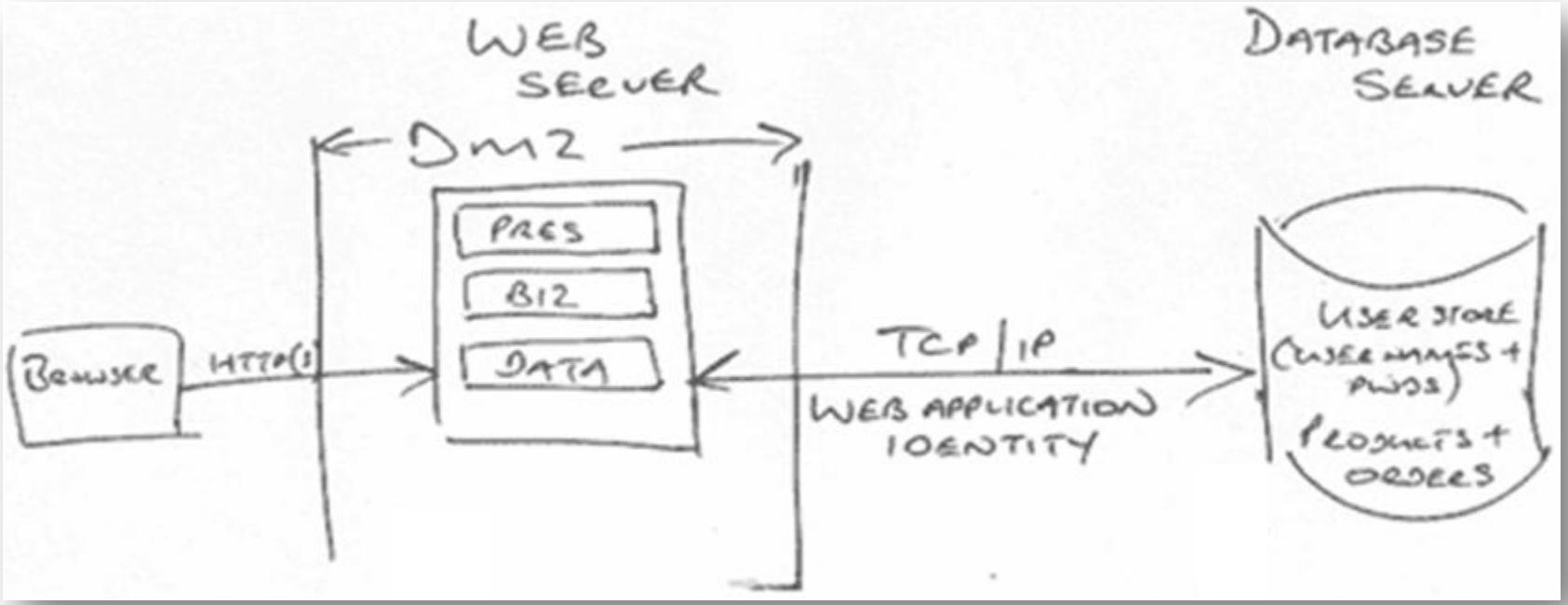
Threat Modeling Process



Identify trust boundaries

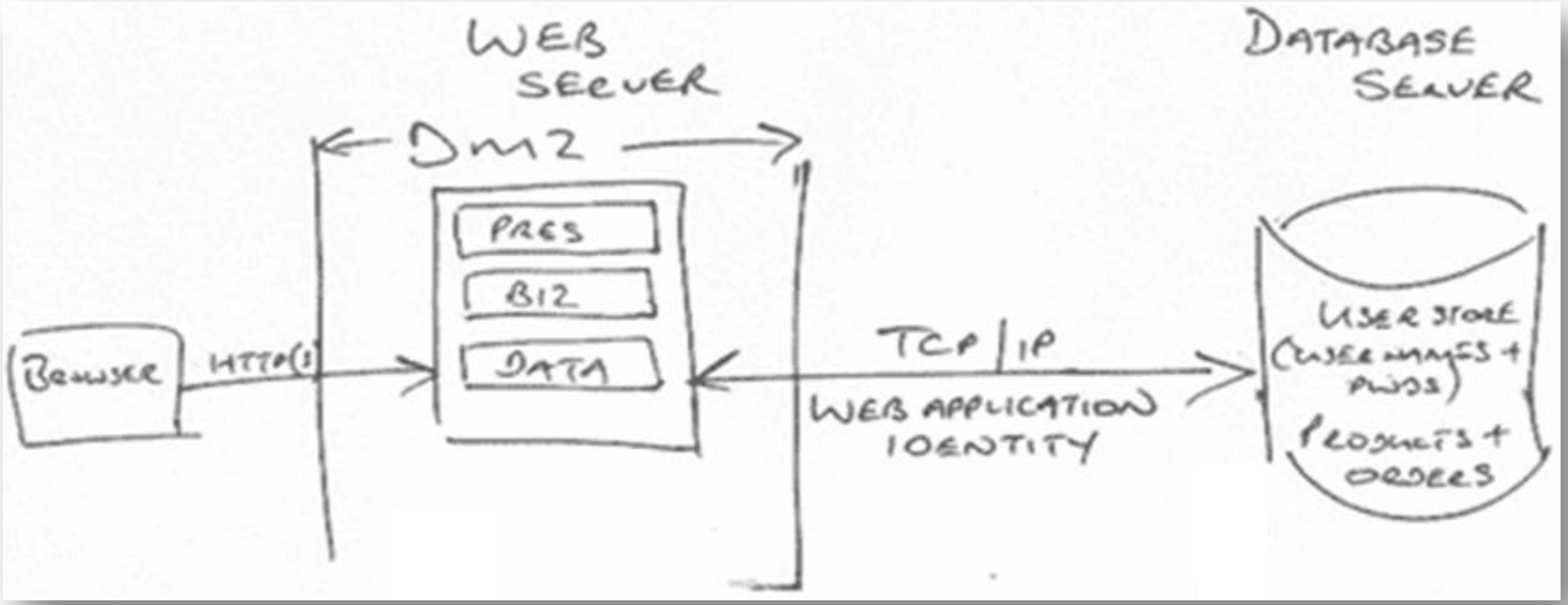


Identify Data Flows



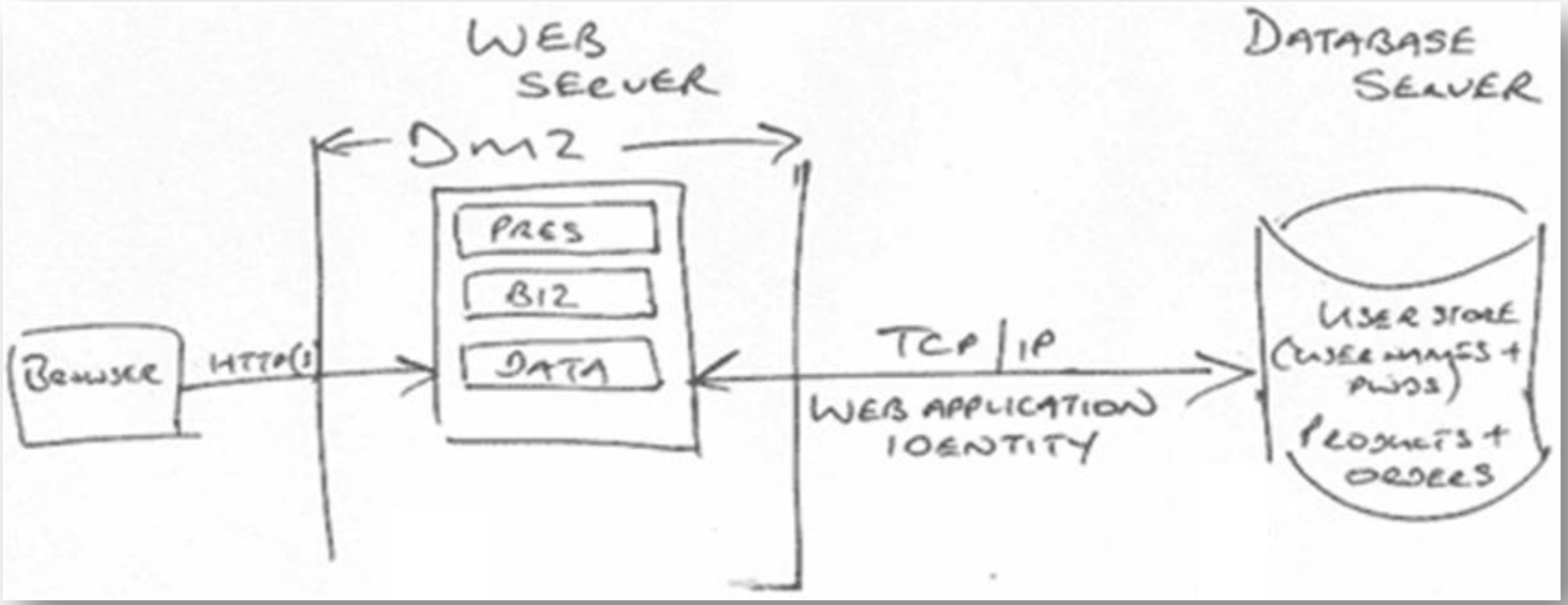
Trace your application's data input through the application from entry to exit. Pay close attention to sensitive data passed over a network, and data which are persisted.

Identify Entry Points



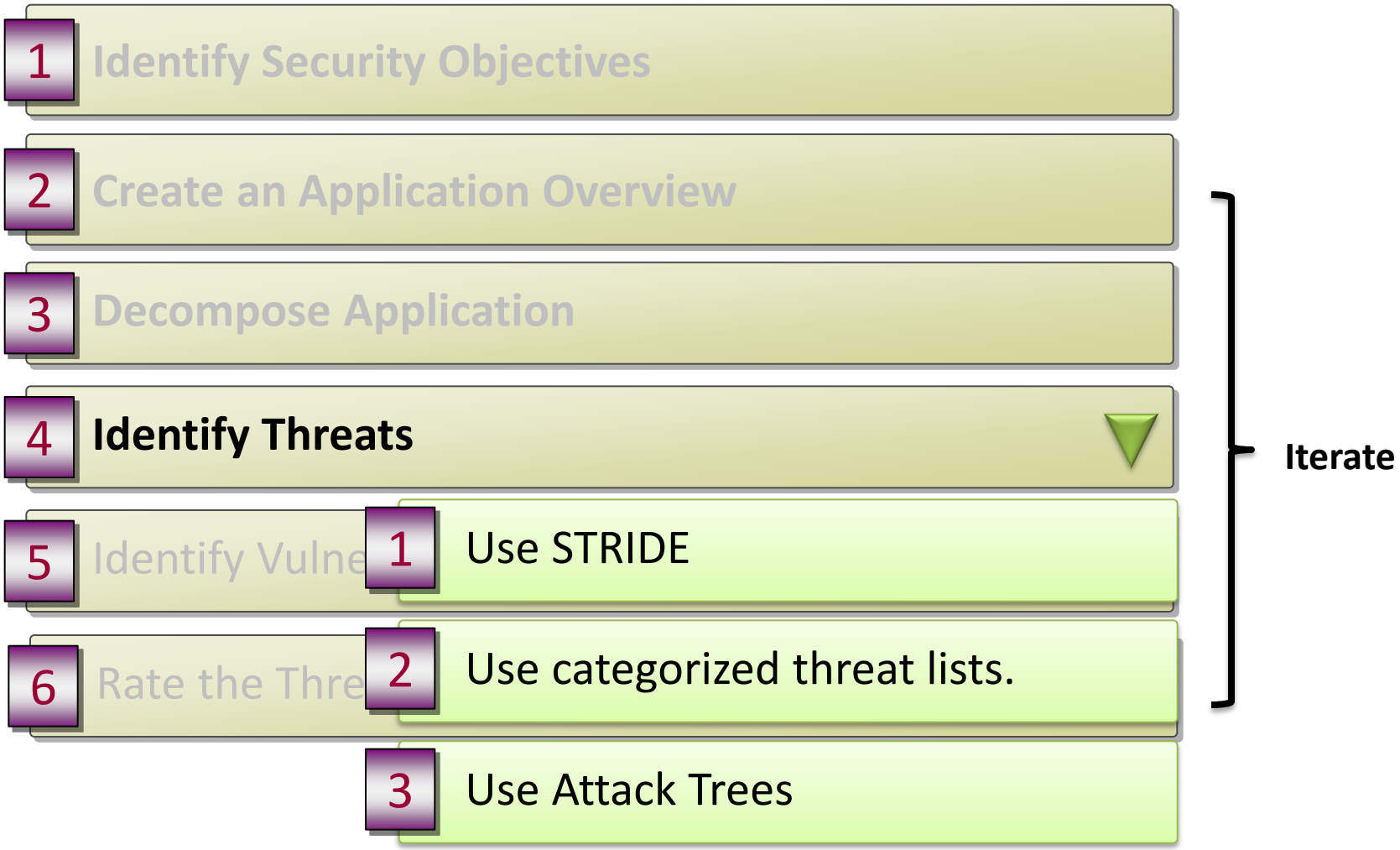
The entry points of your application also serve as entry points for attacks. In case an attacker manages to bypass the front door of the application he can directly attack an internal entry point.

Identify Exit Points



Identify the points where your application sends data to the client or to external systems.

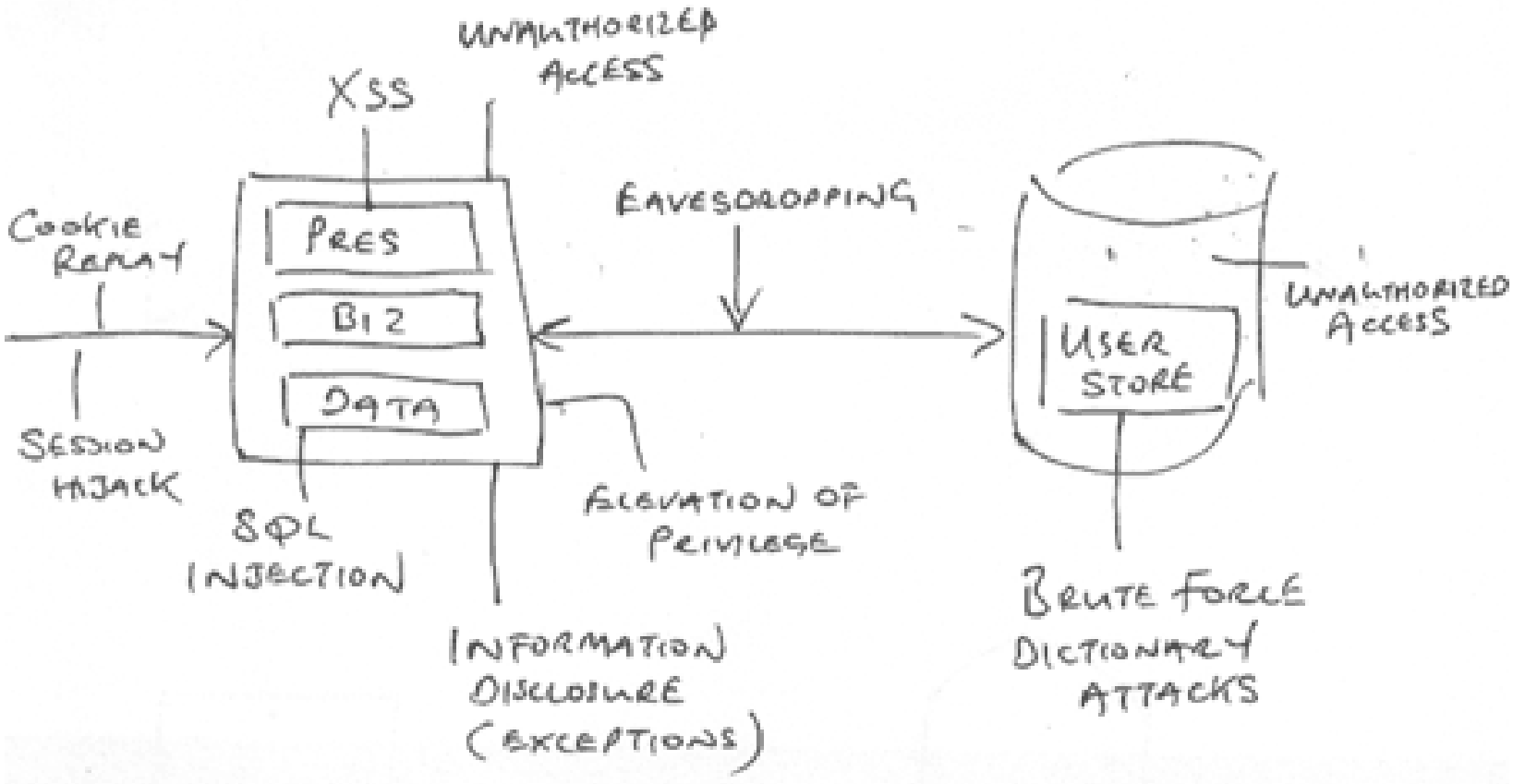
Threat Modeling Process



Threat Classification (STRIDE)

1. **Spoofing**
   - Forging an identity of a service or user
2. **Tampering**
   - Compromising integrity of data
3. **Repudiation**
   - Can't prove an action committed by an entity
4. **Information Disclosure**
   - Unintended disclosure of information
5. **Denial of Service**
   - Compromising availability of a service
6. **Elevation of Privileges**
   - An identity can gain unauthorized privileges

Threat lists



Creating Attack Trees

Threat #1 Attacker obtains authentication credentials by monitoring the network

1.1 Clear text credentials sent over the network **AND**

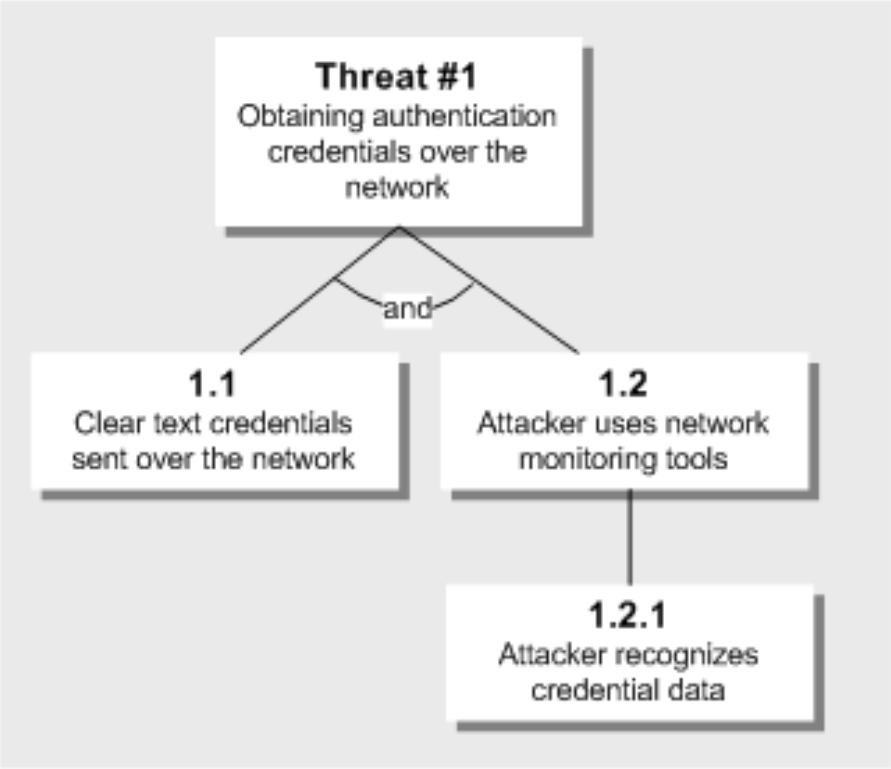
1.2 Attacker uses network-monitoring tools

1.2.1 Attacker recognizes credential data

Start building an attack tree by creating root nodes that represent the goals of the attacker. Then add the leaf nodes, which are the attack Methodologies that represent unique attacks. You can label leaf nodes with AND and OR labels.

Creating Attack Trees

Attack trees are the primary tools that many security professionals use.



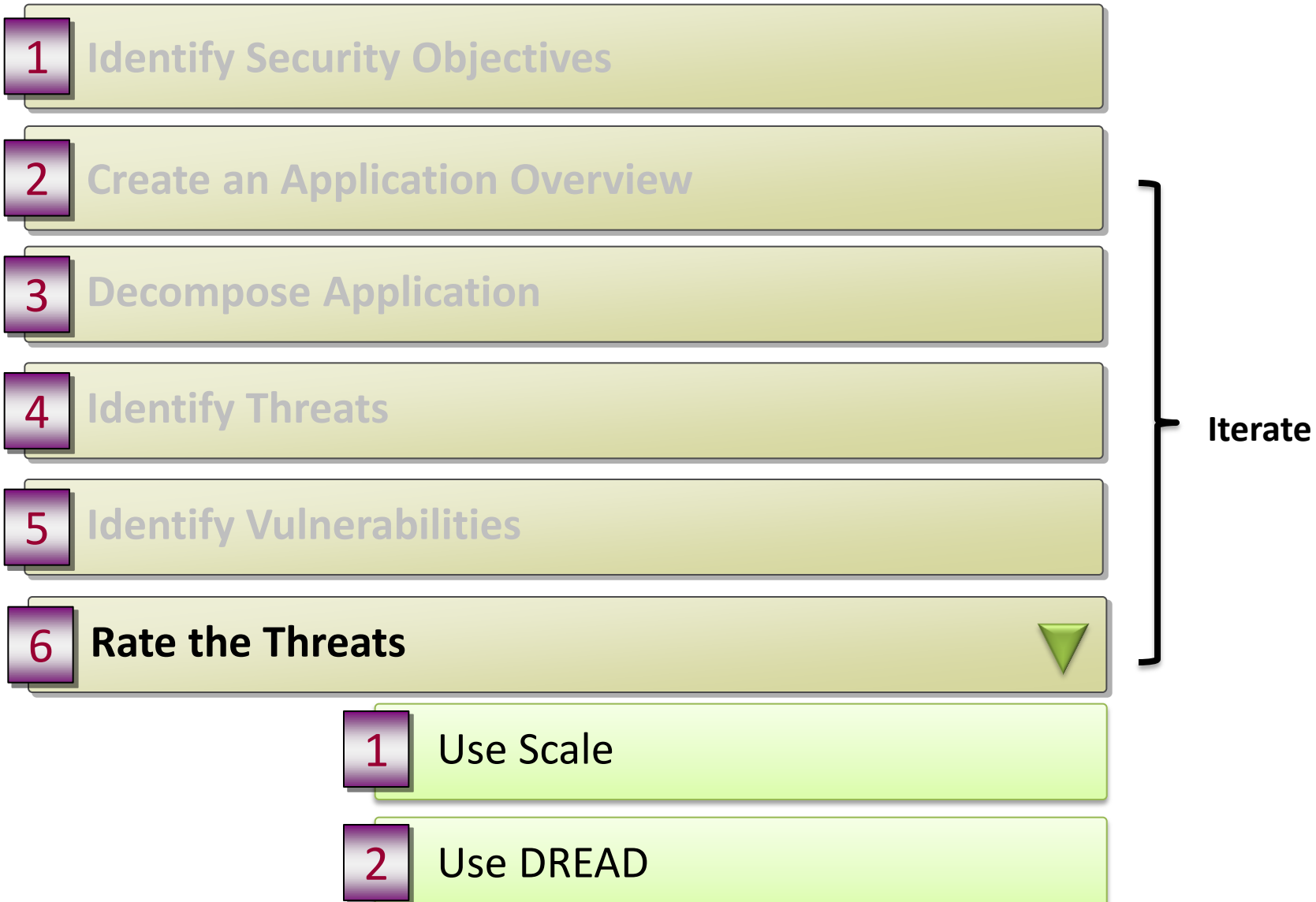
Test team : Create test plans to validate security design.
Architects : Evaluate the security cost of alternative approaches.
Developers : Make informed coding decisions.

Threat Modeling Process

Identify Vulnerabilities

Cryptography	1. Using custom cryptography 2. Using the wrong algorithm or a key size that is too small 3. Failing to secure encryption keys 4. Using the same key for a prolonged period of time 5. Distributing keys in an insecure manner
Exception Management	1. Failing to use structured exception handling 2. Revealing too much information to the client
Auditing and Logging	1. Failing to audit failed logons 2. Failing to secure audit files 3. Failing to audit across application tiers

Threat Modeling Process



Rate the Threats using Scale

Risk = Probability * Damage Potential

Example :

Probability=10 and **Damage Potential**=1
Risk = 10 * 1 = 10.

Example :

Probability=1 and **Damage Potential**=10
Risk = 1 * 10 = 10.

Rating allows you to address the threats that present the most risk first, and then resolve the other threats. It may not be economically viable to address all of the identified threats.

Rate the Threats Using DREAD

1. **D**amage potential: How great is the damage if the vulnerability is exploited?
2. **R**eproducibility: How easy is it to reproduce the attack?
3. **E**xploitability: How easy is it to launch an attack?
4. **A**ffected users: As a rough percentage, how many users are affected?
5. **D**iscoverability: How easy is it to find the vulnerability?

At Microsoft, the DREAD model is used to help calculate risk.

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential

Rate the Threats Using DREAD

Threat	D	R	E	A	D	Total	Rating
Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
SQL commands injected into application.	3	3	3	3	2	14	High

1. High risk : 12–15
2. Medium risk : 8–11
3. Low risk : 5–7

Document the Threats

Threat Description	Attacker obtains authentication credentials by monitoring the network
Threat target	Web application user authentication process
Risk rating	High
Attack techniques	Use of network monitoring software
Countermeasures	Use SSL to provide encrypted channel

Threat Modeling Process

Threat Modeling

Threats still exist regardless of the security actions you take and the countermeasures you apply.

Summary

While you can mitigate the risk of an attack, you do not mitigate or eliminate the actual threat.

The reality in the security world is that you acknowledge the presence of threats and you manage your risks.