

Nowoczesne modelowanie zagrożeń

AI w służbie bezpieczeństwa

Adrian Sroka

<https://SecurityChampions.pl>

Software Security Architect & Consultant

Co chcemy osiągnąć?

Jak najlepiej i jak najmniejszym kosztem zabezpieczyć
tworzone przez nas rozwiązania

SDLC



Planowanie



Projektowanie



Programowanie



Testy



Wdrożenie



Operacje



Monitoring



Shift Left (Up)



Planowanie



Projektowanie

+ Threat modelling



Programowanie



Testy



Wdrożenie



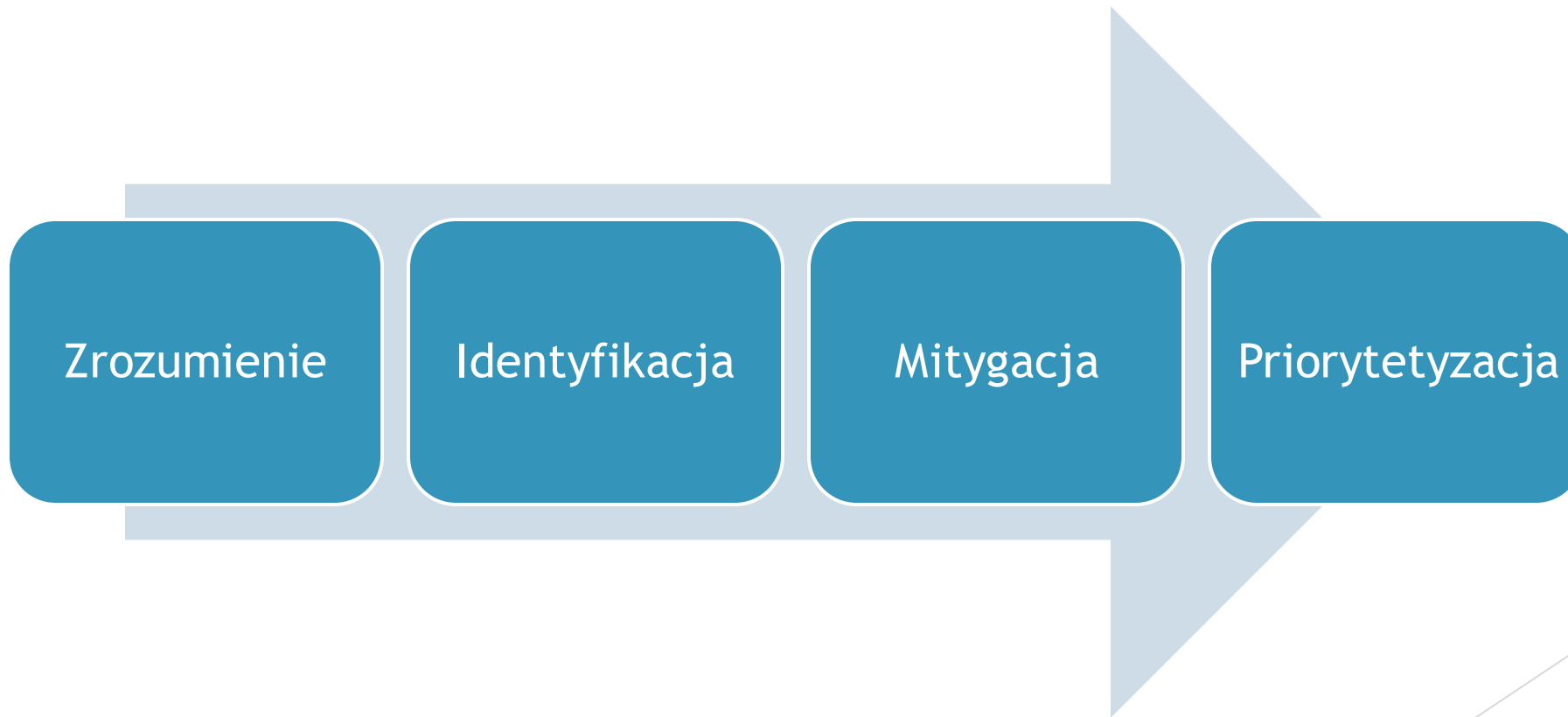
Operacje



Monitoring



Modelowanie zagrożeń



Modelowanie zagrożeń w życiu codziennym

Jazda samochodem po zaśnieżonym mieście

- Jakie jest ryzyko poślizgu?
- Czy ktoś może wybiec na ulicę?
- Czy na skrzyżowaniu nic nie jedzie?
- Czy nie jadę zbyt szybko?



Modelowanie zagrożeń
jest jak sprawdzanie
oleju w samochodzie
przed dłuższą
wyprawą



Korzyści z modelowania zagrożeń

- ▶ Świadomość
- ▶ Integracja z Shift Left
 - ▶ Dewelopment
 - ▶ Testy
 - ▶ Dokumentacja



Jak to dobrze zrobić/robić?

- ▶ W odpowiednim momencie
- ▶ W odpowiednim gronie
- ▶ Wartościowe
- ▶ Mało przeszkadzające
- ▶ Dopasowane do możliwości zespołu

Globalne

by Adam Shostack

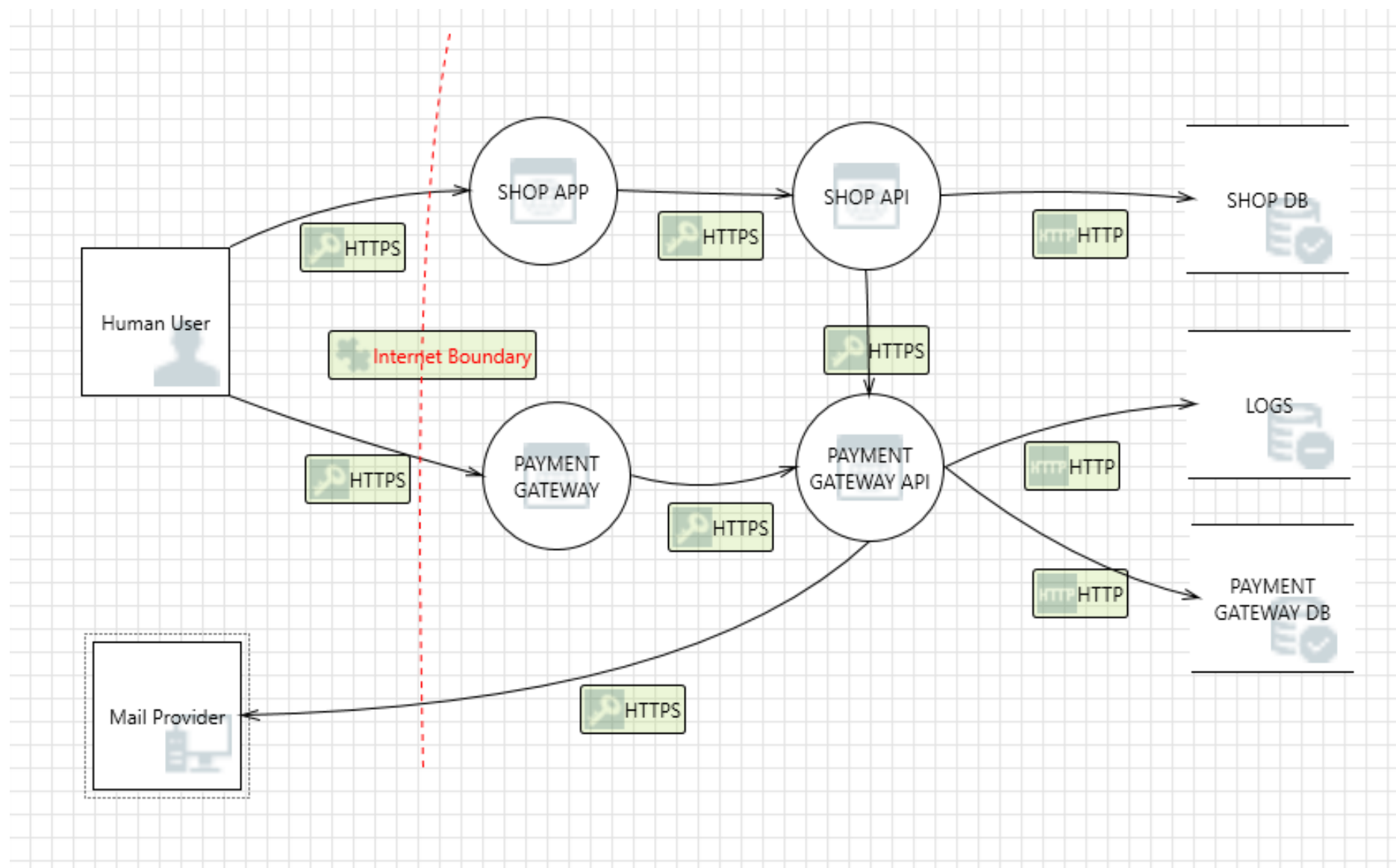


Co budujemy?

Co może pójść nie tak?

Plan mitygacji

Walidacja planu



Co budujemy?

Co może pójść nie tak?

Plan mitygacji

Walidacja planu

STRIDE

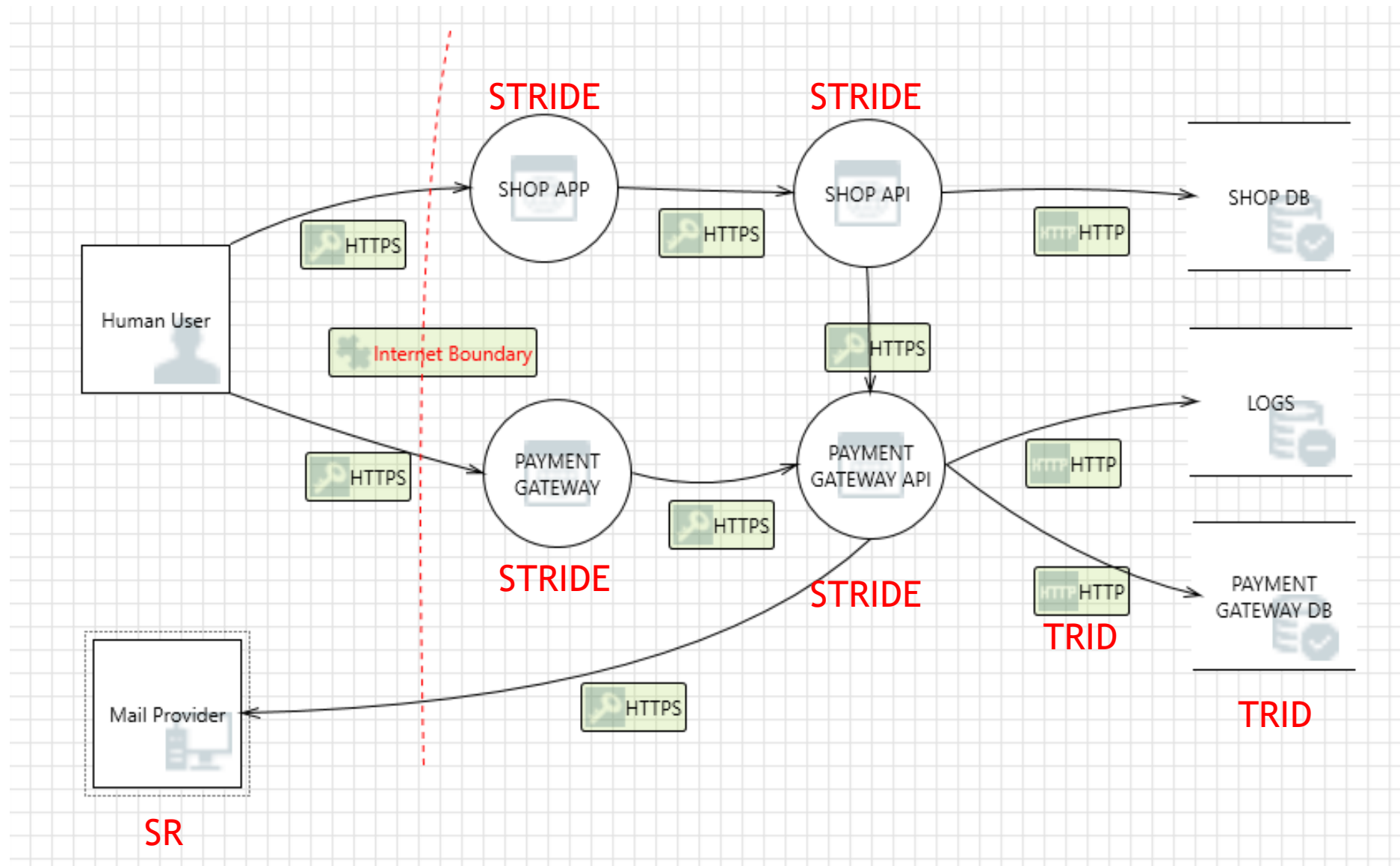
Zagrożenie	Definicja	Przykłady	Mitygacje
Spoofing	Podszywanie się pod kogoś innego	Kradzież tokenu	Hasła
Tampering	Zmiana danych lub kodu	Zmiana ceny podczas płatności	Uprawnienia Walidacje Podpisy
Repudiation	Nieprzyznanie się do wykonania akcji	Zmiana numeru konta	Audyt zmian
Information Disclosure	Wyciek danych	Endpoint API bez zabezpieczeń	Uprawnienia Szyfrowanie
Denial of Service	Niedostępność usługi	Infrastrukturalny Funkcjonalny	Rate limiting IP whitelisting
Elevation of Privilege	Możliwość wykonania nieautoryzowanej akcji	Zmiana uprawnień poprzez SQL Injection	Uprawnienia Walidacja

Co budujemy?

Co może pójść nie tak?

Plan mitygacji

Walidacja planu



Co budujemy?

Co może pójść nie tak?

Plan mitygacji

Walidacja planu

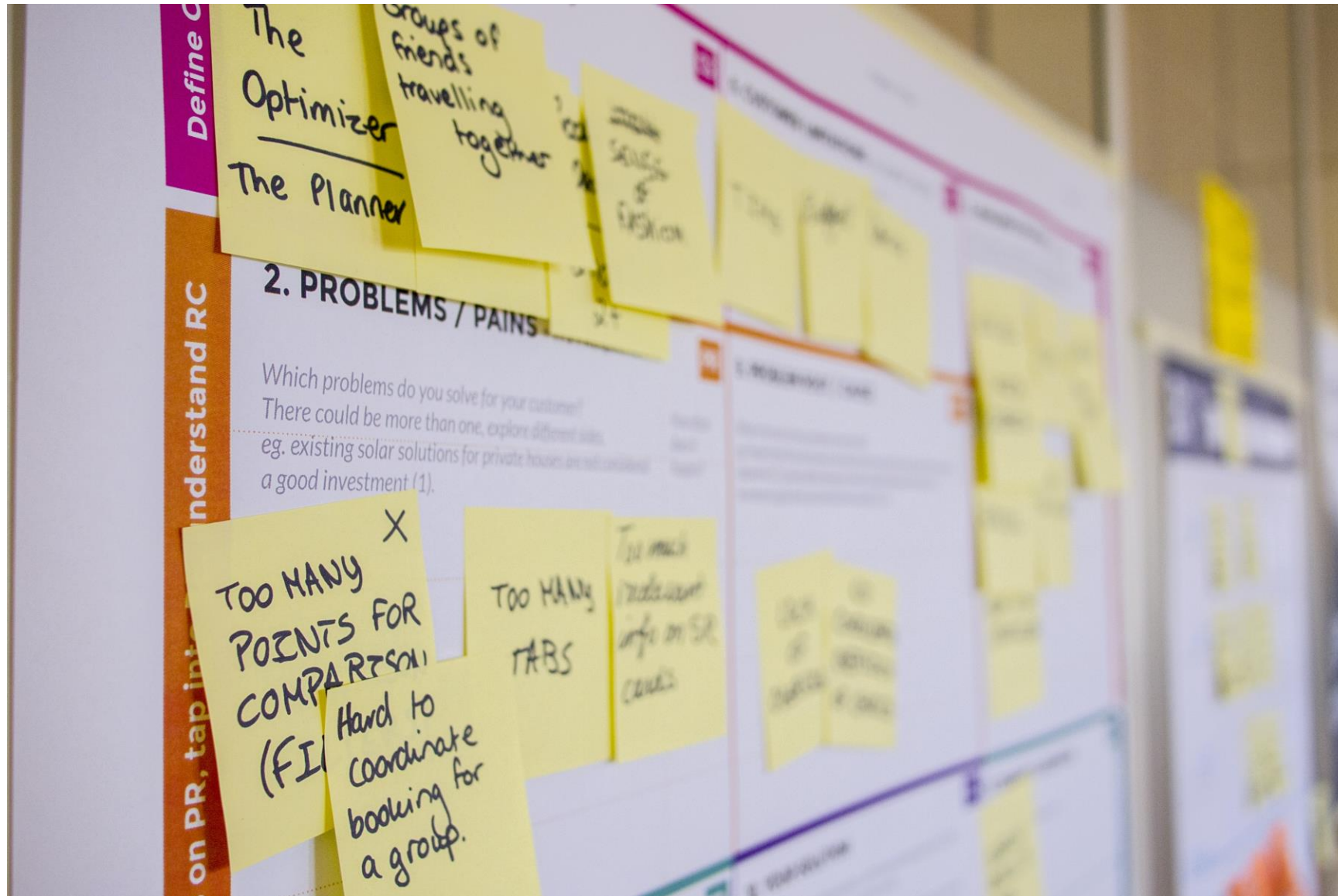
- ▶ Akceptacja
- ▶ Unikanie
- ▶ Mitygacja
- ▶ Przeniesienie

Co budujemy?

Co może pójść nie tak?

Plan mitygacji

Walidacja planu



Globalne modelowanie zagrożeń

Narzędzia

- ▶ Microsoft Threat Modelling Tool (darmowe)
- ▶ OWASP Threat Dragon (darmowe)
- ▶ Irius (płatne)
- ▶ Inne narzędzia do rysowania diagramów
- ▶ Ołówek i długopis (płatne)

Globalne podejście

Zalety

- ▶ Skupia się na całych komponentach
- ▶ Dobrze dla istniejącego systemu

Problemy

- ▶ Czasochłonne
- ▶ Wymaga sporej wiedzy na start
- ▶ Brak analizy całościowej / pomiędzy systemami

Iteracyjne



Podejście iteracyjne

Kiedy?

- ▶ W momencie analizy
- ▶ Refinement
- ▶ Często, małymi krokami

Co?

- ▶ Abuse Przypadki nadużyć (Abuse Story)
- ▶ Przypadki testowe
- ▶ Kryteria akceptacji

Kto?

- ▶ Cały zespół
- ▶ Osoby znające system

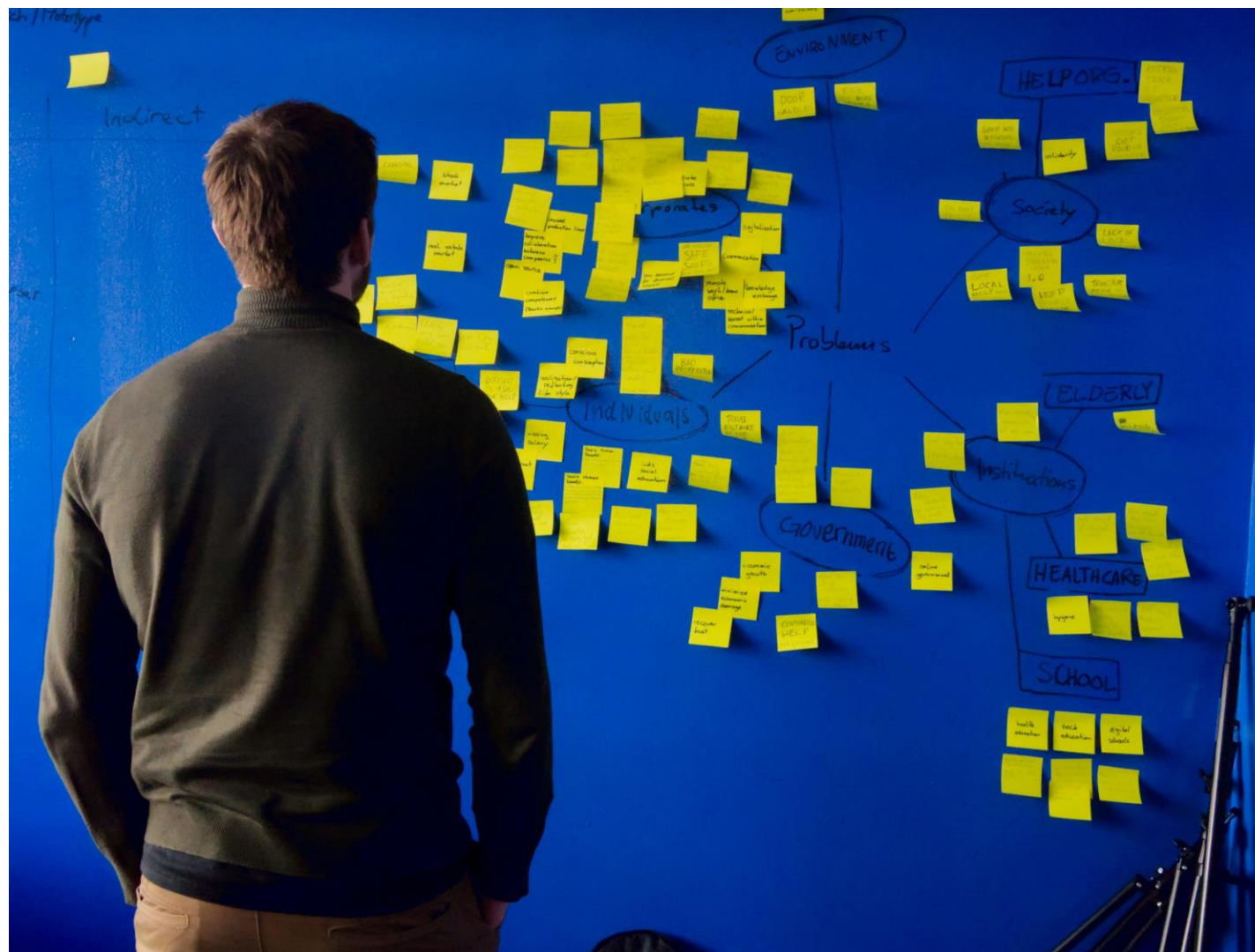
Ale jak to właściwie zrobić?

Burza mózgów

Pytania STRIDE

Kwestionariusz
bezpieczeństwa

Wsparcie AI



- ▶ Spoofing - *Czy ktoś może podszyć się pod kogoś innego?*
- ▶ Tampering - *Czy ktoś może zmodyfikować dane wysyłane / przetwarzane przez aplikację wbrew regułom systemu?*
- ▶ Repudiation - *Czy ktoś może wykonać jakąś akcję bez możliwości udowodnienia mu tego?*
- ▶ Information disclosure - *Czy ktoś może uzyskać dostęp do danych, do których normalnie nie powinien mieć dostępu?*
- ▶ Denial of Service - *Czy ktoś może spowodować niedostępność systemu?*
- ▶ Elevation of Privilege - *Czy ktoś może wykonać akcję wykraczającą poza jego uprawnienia?*

Burza mózgów

Pytania STRIDE

Kwestionariusz
bezpieczeństwa

Wsparcie AI

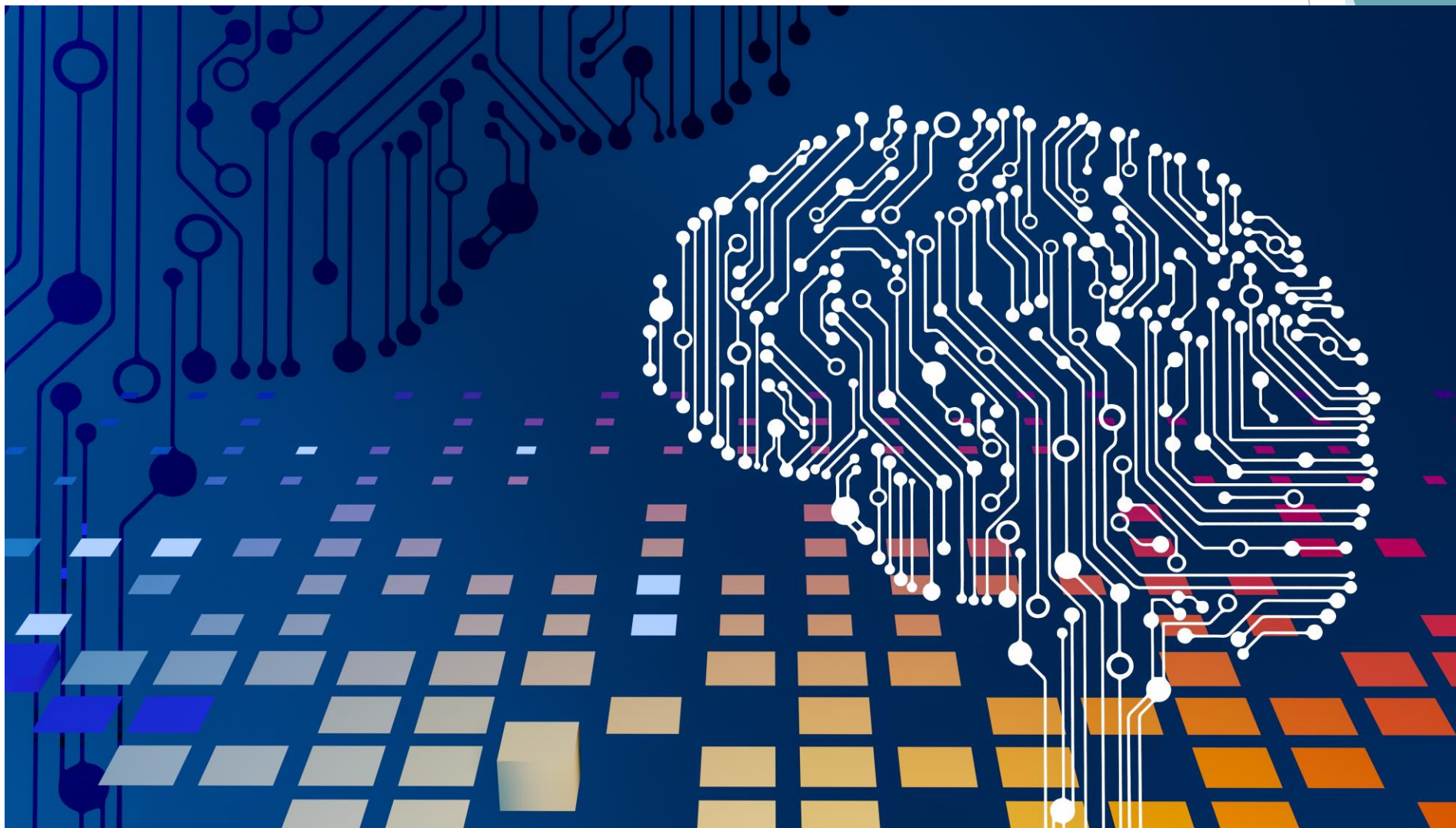
Jeżeli dotyczy...	...zadaj następujące pytania
Architektura	Czy system produkcyjnie udostępnia publicznie dokumentację (np. do API)?
Backendowa integracja z innymi usługami	W jaki sposób zabezpieczamy komunikację?
	Jakie sekrety są używane z komunikacji?
	Czy użytkownicy mają dostęp do sekretów?
	Czy możemy w wygodny sposób zmienić sekret?
	Czy deweloperzy mają dostęp do produkcyjnych sekretów?
Upload plików	Jak zabezpieczony jest upload?
	Czy walidujemy rozmiar, typ i rozszerzenie pliku?

Burza mózgów

Pytania STRIDE

Kwestionariusz
bezpieczeństwa

Wsparcie AI



As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Zbudowanie kontekstu aktora

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
-----------	-------------	-----------------	-------------	---------------

---	---	---	---	---
-----	-----	-----	-----	-----

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

Burza mózgów

Pytania STRIDE

Kwestionariusz
bezpieczeństwa

Wsparcie AI

As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
-----------	-------------	-----------------	-------------	---------------

---	---	---	---	---
-----	-----	-----	-----	-----

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

Polecenie

As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
-----------	-------------	-----------------	-------------	---------------

---	---	---	---	---
-----	-----	-----	-----	-----

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

Opis formatu wyniku

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
---	---	---	---	---

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

Opis systemu

As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
---	---	---	---	---

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

Użycie słownika

Burza mózgów

Pytania STRIDE

Kwestionariusz
bezpieczeństwa

Wsparcie AI

Ostrożnie ze szczegółami

As a security analyst, you are preparing a threat modelling session for adding the new functionality to the current system.

List all possible security threats introduced by the new functionality.

Output of threat modeling should be in table as in example:

Threat Id	Threat Name	STRIDE category	Mitigations	Risk severity
---	---	---	---	---

1	Attacker is able to spoof client using leaked API key	Spoofing	Invalidation of API keys. Usage of request signing technique	Critical
---	---	----------	---	----------

The current system.

The system A is a booking system for the cinema. It allows the users to register accounts, log in and buy tickets for a particular movie. During the selling process, the user must select the exact place in the cinema and pay online for the ticket. Then he can download the ticket online.

The new functionality.

You have to add the functionality to reserve a place in the cinema. Then he has 1 hour to pay for it or the reservation will be cancelled. The booking required registration or login.

Opis nowej
funkcjonalności

Burza mózgów

Pytania STRIDE

Kwestionariusz bezpieczeństwa

Wsparcie AI

5	Data leakage due to reservation information being exposed	Information Disclosure	Implement proper access controls to restrict access to reservation information. Encrypt sensitive data. Regularly audit access to reservation data.	Medium
6	Attacker manipulates the reservation system to block available seats	Denial of Service	Implement rate limiting and validation checks to prevent manipulation of the reservation system. Regularly monitor for unusual reservation patterns.	Low
7	Unauthorized access to the reservation system backend	Elevation of Privilege	Implement strict access controls and least privilege principles for the reservation system backend. Regularly audit and monitor access to the backend.	High

Wsparcie AI - drażnienie

Describe, what could go wrong in the threat "Ticket Information Disclosure"

In the context of the "Ticket Information Disclosure" threat in a cinema booking system, several issues could go wrong if an attacker successfully gains access to ticket information:



1. **Privacy Violation:** The most immediate concern is a violation of user privacy. If an attacker can access and view ticket information, they may be able to see personal details such as the user's name, contact information, and possibly payment information. This can lead to identity theft, harassment, or other privacy breaches.
2. **Ticket Duplication:** An attacker may use the information obtained to duplicate the ticket, leading to the potential for multiple individuals claiming the same seat. This could result in disputes, conflicts, and frustration among legitimate ticket holders and disrupt the cinema's operations.
3. **Fraud and Resale:** Attackers might exploit the disclosed ticket information for fraudulent activities, such as reselling tickets at a higher price, transferring tickets to unauthorized users, or using the information for other malicious purposes.

Wsparcie AI - mitigacje

The system has a threat of "Privacy Violation"

It enables any user to get the reservation details without authorization by URL
`/reservation/{id}`

This page should be available without the login, because we want to send it by mail to the end user.

What could be the mitigation in this case?

1. Authentication Tokens or Access Control:

- Implement an access control mechanism to restrict access to the reservation details URL. While you want to make this information available via a URL, it doesn't mean it should be open to anyone. Utilize authentication tokens or session-based authentication to control who can access the reservation details.

2. Unique, Time-Limited URLs:

- Instead of making reservation details openly accessible via a predictable URL, generate unique, time-limited URLs for each reservation. These URLs should expire after a short period or after they've been accessed once. This way, even if a URL is shared, it's only valid for a short time, reducing the risk of unauthorized access.

Inne opcje - LINDDUN

To prepare a threat modeling session for the given functionality of a cinema booking system, you can use the LINDDUN model to categorize potential security threats. The LINDDUN model stands for:

1. **Linkability:** The ability to link different pieces of information to identify a user or their activities.
 - Threat 1: User Tracking - Attackers may attempt to track and identify users based on their activities within the system, potentially violating user privacy.
2. **Identifiability:** The potential for an attacker to identify individuals or their actions.
 - Threat 2: Account Enumeration - Attackers might try to enumerate valid user accounts by trying various login credentials, potentially leading to unauthorized access.
3. **Non-repudiation:** Ensuring that actions or events cannot be denied later.
 - Threat 3: Ticket Fraud - Users could potentially purchase tickets, use them, and later claim they never received them, leading to disputes and potential financial loss.
4. **Detectability:** The ability to detect security incidents and breaches.
 - Threat 4: Unauthorized Access - Unauthorized users may attempt to gain access to the system, and if not detected, this could lead to data breaches or fraudulent ticket purchases.

ChatGPT 3.5 vs ChatGPT 4

Rekomendacje

Zacznij dla nowych funkcjonalności

Dostosuj sposób modelowania do doświadczenia ludzi

Nauka:

- ▶ ChatGPT
- ▶ Kwestionariusz bezpieczeństwa
(np. <https://github.com/Autodesk/continuous-threat-modeling>)
- ▶ Wsparcie specjalisty
- ▶ Pytania STRIDE
- ▶ Burza mózgów

Zaproszenie

Jeżeli chcesz wdrożyć modelowanie zagrożeń w swoim zespole/swojej firmie, mogę Ci w tym pomóc.

Napisz do mnie: security@diwebsity.com z dopiskiem w temacie [Threat Modelling]

Biuletyn bezpieczeństwa aplikacji

<https://securitychampions.pl>

Dziękuję za uwagę