In [ ]:

```python
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns

df = pd.read_csv("data.csv")
df.head(10)
```

Out[ ]:

	Interaction Name	Threat Number	Summary	Priority	State	Category	Description	SDL Phase	Mitigations
0	Catalog to Gateway	1	An adversary can deny actions on Cloud Gateway...	High	Not Started	Repudiation	An adversary may perform actions such as spoof...	Design	Ensure that appropriate auditing and logging i...
1	DB to Catalog	2	An adversary may gain unauthorized access to W...	High	Not Started	Elevation of Privileges	An adversary may gain unauthorized access to W...	Implementation	Implement proper authorization mechanism in AS...
2	DB to Catalog	3	An adversary can gain access to sensitive info...	High	Not Started	Information Disclosure	An adversary can gain access to sensitive data...	Implementation	Ensure that proper exception handling is done ...
3	DB to Catalog	4	An adversary can gain access to sensitive data...	High	Not Started	Information Disclosure	An adversary can gain access to sensitive data...	Implementation	Force all traffic to Web APIs over HTTPS conne...
4	DB to Catalog	5	An adversary can gain access to sensitive data...	Medium	Not Started	Information Disclosure	An adversary can gain access to the config fil...	Implementation	Encrypt sections of Web API's configuration fi...
5	DB to Catalog	6	Attacker can deny a malicious act on an API le...	High	Not Started	Repudiation	Attacker can deny a malicious act on an API le...	Design	Ensure that auditing and logging is enforced o...
6	DB to Catalog	7	An adversary may spoof Generic Data Store and ...	High	Not Started	Spoofing	If proper authentication is not in place, an a...	Design	Ensure that standard authentication techniques...
7	DB to Catalog	8	An adversary may inject malicious inputs into ...	High	Not Started	Tampering	An adversary may inject malicious inputs into ...	Implementation	Ensure that model validation is done on Web AP...
8	DB to Catalog	9	An adversary can gain access to sensitive data...	High	Not Started	Tampering	SQL injection is an attack in which malicious ...	Implementation	Ensure that type-safe parameters are used in W...
9	DB to Delivery	10	An adversary can gain access to sensitive data...	High	Not Started	Tampering	SQL injection is an attack in which malicious ...	Implementation	Ensure that type-safe parameters are used in W...

In [ ]:

```python
relevant_data = df[["Interaction Name", "Summary","Priority","Category","SDL Phase"]]
print(relevant_data["Summary"].tolist())
```

```
['An adversary can deny actions on Cloud Gateway due to lack of auditing', 'An adversary may gain unauthorized a
ccess to Web API due to poor access control checks', 'An adversary can gain access to sensitive information from
an API through error messages', 'An adversary can gain access to sensitive data by sniffing traffic to Web API',
"An adversary can gain access to sensitive data stored in Web API's config files", 'Attacker can deny a maliciou
s act on an API leading to repudiation issues', 'An adversary may spoof Generic Data Store and gain access to We
b API', 'An adversary may inject malicious inputs into an API and affect downstream processes', 'An adversary ca
n gain access to sensitive data by performing SQL injection through Web API', 'An adversary can gain access to s
ensitive data by performing SQL injection through Web API', 'An adversary may inject malicious inputs into an AP
I and affect downstream processes', 'An adversary may spoof Generic Data Store and gain access to Web API', 'Att
acker can deny a malicious act on an API leading to repudiation issues', "An adversary can gain access to sensit
ive data stored in Web API's config files", 'An adversary can gain access to sensitive data by sniffing traffic
to Web API', 'An adversary can gain access to sensitive information from an API through error messages', 'An adv
ersary may gain unauthorized access to Web API due to poor access control checks', 'An adversary can gain access
to sensitive data by performing SQL injection through Web API', 'An adversary may inject malicious inputs into a
n API and affect downstream processes', 'An adversary may spoof Generic Data Store and gain access to Web API',
'Attacker can deny a malicious act on an API leading to repudiation issues', "An adversary can gain access to se
nsitive data stored in Web API's config files", 'An adversary can gain access to sensitive data by sniffing traf
fic to Web API', 'An adversary can gain access to sensitive information from an API through error messages', 'An
adversary may gain unauthorized access to Web API due to poor access control checks', 'An adversary can gain acc
ess to sensitive data by performing SQL injection through Web API', 'An adversary may inject malicious inputs in
to an API and affect downstream processes', 'An adversary may spoof Generic Data Store and gain access to Web AP
I', 'Attacker can deny a malicious act on an API leading to repudiation issues', "An adversary can gain access t
o sensitive data stored in Web API's config files", 'An adversary can gain access to sensitive data by sniffing
traffic to Web API', 'An adversary can gain access to sensitive information from an API through error messages',
'An adversary may gain unauthorized access to Web API due to poor access control checks', 'Attacker can deny a m
alicious act on an API leading to repudiation issues', "An adversary can gain access to sensitive data stored in
Web API's config files", 'An adversary can gain access to sensitive data by sniffing traffic to Web API', 'An ad
versary can gain access to sensitive information from an API through error messages', 'An adversary may gain una
uthorized access to Web API due to poor access control checks', 'An adversary may inject malicious inputs into a
n API and affect downstream processes', 'An adversary may spoof Generic Data Store and gain access to Web API',
'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An adversary can
deny actions on Cloud Gateway due to lack of auditing', 'An adversary can deny actions on Cloud Gateway due to l
ack of auditing', 'An adversary can gain access to sensitive data by performing SQL injection through Web API',
'An adversary may inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof
API Gateway and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation iss
ues', "An adversary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain
access to sensitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information
from an API through error messages', 'An adversary may gain unauthorized access to Web API due to poor access co
ntrol checks', 'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An
adversary may inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof API
Gateway and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation issues'
, "An adversary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain acce
ss to sensitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information fro
m an API through error messages', 'An adversary may gain unauthorized access to Web API due to poor access contr
ol checks', 'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An ad
versary may inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof API Ga
teway and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation issues',
"An adversary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain access
to sensitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information from a
n API through error messages', 'An adversary may gain unauthorized access to Web API due to poor access control
checks', 'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An adver
sary may inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof API Gatew
ay and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation issues', "An
adversary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain access to
sensitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information from an A
PI through error messages', 'An adversary may gain unauthorized access to Web API due to poor access control che
cks', 'An adversary can deny actions on Cloud Gateway due to lack of auditing', 'An adversary can deny actions o
n Cloud Gateway due to lack of auditing', 'An adversary can gain access to sensitive data by performing SQL inje
ction through Web API', 'An adversary may inject malicious inputs into an API and affect downstream processes',
'An adversary may spoof Message Queue and gain access to Web API', 'Attacker can deny a malicious act on an API
leading to repudiation issues', "An adversary can gain access to sensitive data stored in Web API's config files
", 'An adversary can gain access to sensitive data by sniffing traffic to Web API', 'An adversary can gain acces
s to sensitive information from an API through error messages', 'An adversary may gain unauthorized access to We
b API due to poor access control checks', 'An adversary can gain access to sensitive data by performing SQL inje
ction through Web API', 'An adversary may inject malicious inputs into an API and affect downstream processes',
'An adversary may spoof Message Queue and gain access to Web API', 'Attacker can deny a malicious act on an API
leading to repudiation issues', "An adversary can gain access to sensitive data stored in Web API's config files
", 'An adversary can gain access to sensitive data by sniffing traffic to Web API', 'An adversary can gain acces
s to sensitive information from an API through error messages', 'An adversary may gain unauthorized access to We
b API due to poor access control checks', 'An adversary can gain access to sensitive data by performing SQL inje
ction through Web API', 'An adversary may inject malicious inputs into an API and affect downstream processes',
'An adversary may spoof Message Queue and gain access to Web API', 'Attacker can deny a malicious act on an API
leading to repudiation issues', "An adversary can gain access to sensitive data stored in Web API's config files
", 'An adversary can gain access to sensitive data by sniffing traffic to Web API', 'An adversary can gain acces
s to sensitive information from an API through error messages', 'An adversary may gain unauthorized access to We
b API due to poor access control checks', 'An adversary can deny actions on Cloud Gateway due to lack of auditin
g', 'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An adversary
may inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof Order Service
and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation issues', "An ad
versary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain access to se
nsitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information from an API
through error messages', 'An adversary may gain unauthorized access to Web API due to poor access control checks
', 'An adversary can gain access to sensitive data by performing SQL injection through Web API', 'An adversary m
ay inject malicious inputs into an API and affect downstream processes', 'An adversary may spoof Payment Service
and gain access to Web API', 'Attacker can deny a malicious act on an API leading to repudiation issues', "An ad
versary can gain access to sensitive data stored in Web API's config files", 'An adversary can gain access to se
nsitive data by sniffing traffic to Web API', 'An adversary can gain access to sensitive information from an API
through error messages', 'An adversary may gain unauthorized access to Web API due to poor access control checks
']
```

In [ ]:

```python
threats = [
    'Cloud Gateway Auditing Lacking',
    'Poor Access Control Checks',
    'Sensitive Info From Error Messages',
    'Sniffing Web API Traffic',
    'Sensitive Data in Config Files',
    'Repudiation Issues in API',
    'Spoof Generic Data Store',
    'Malicious Input Injection',
    'SQL Injection Through Web API',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Generic Data Store',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Generic Data Store',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Generic Data Store',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'Malicious Input Injection',
    'Spoof Generic Data Store',
    'SQL Injection Through Web API',
    'Cloud Gateway Auditing Lacking',
    'Cloud Gateway Auditing Lacking',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof API Gateway',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof API Gateway',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof API Gateway',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof API Gateway',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'Cloud Gateway Auditing Lacking',
    'Cloud Gateway Auditing Lacking',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Message Queue',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Message Queue',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Message Queue',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'Cloud Gateway Auditing Lacking',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Order Service',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks',
    'SQL Injection Through Web API',
    'Malicious Input Injection',
    'Spoof Payment Service',
    'Repudiation Issues in API',
    'Sensitive Data in Config Files',
    'Sniffing Web API Traffic',
    'Sensitive Info From Error Messages',
    'Poor Access Control Checks'
]


df["Summary abbv"] = threats
df.head()
```

Out[ ]:

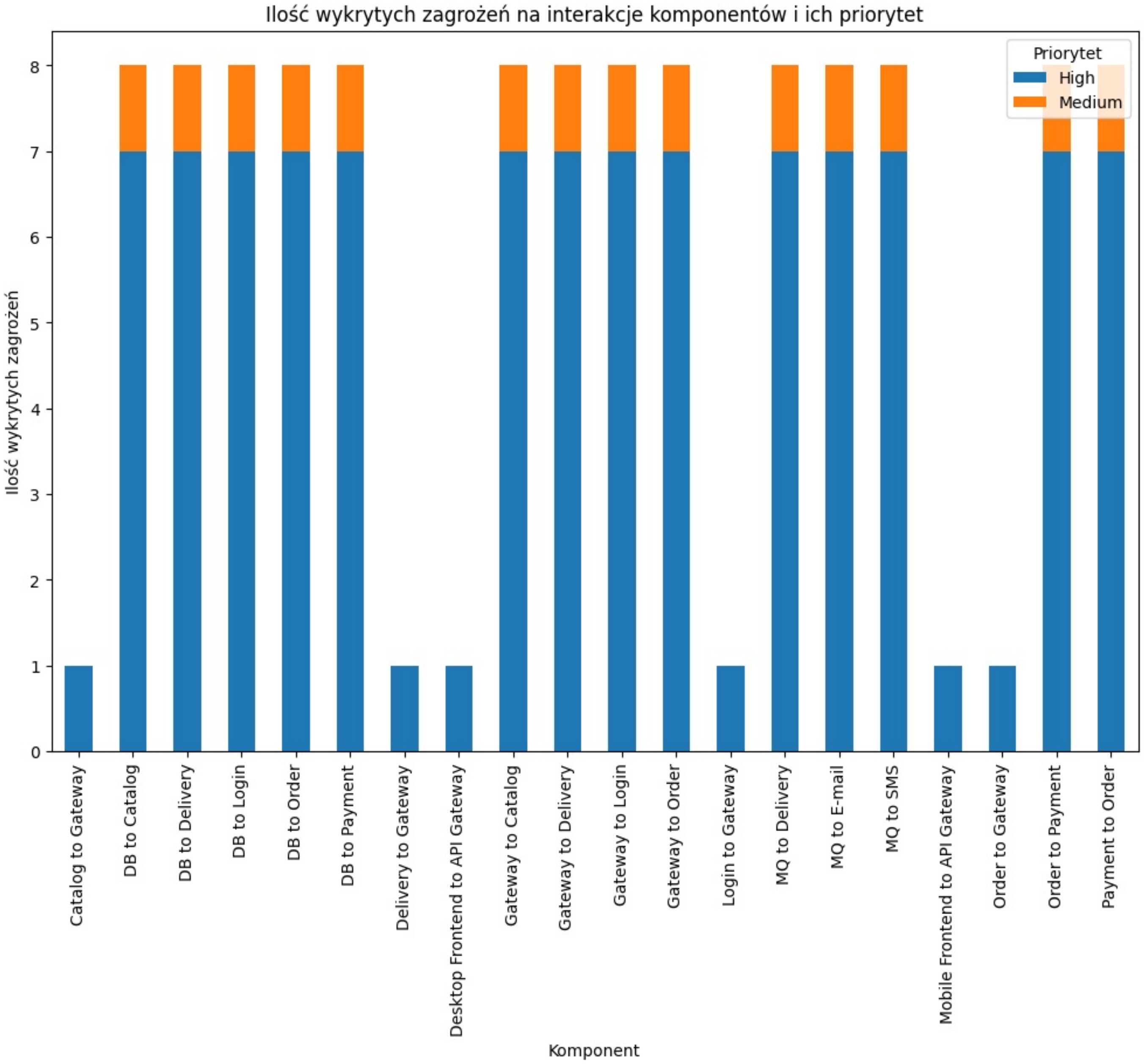
	Interaction Name	Threat Number	Summary	Priority	State	Category	Description	SDL Phase	Mitigations	Summa ab
0	Catalog to Gateway	1	An adversary can deny actions on Cloud Gateway...	High	Not Started	Repudiation	An adversary may perform actions such as spoof...	Design	Ensure that appropriate auditing and logging i...	Clo Gatev Audit Lack
1	DB to Catalog	2	An adversary may gain unauthorized access to W...	High	Not Started	Elevation of Privileges	An adversary may gain unauthorized access to W...	Implementation	Implement proper authorization mechanism in AS...	P Acc Con Che
2	DB to Catalog	3	An adversary can gain access to sensitive info...	High	Not Started	Information Disclosure	An adversary can gain access to sensitive data...	Implementation	Ensure that proper exception handling is done ...	Sensit Info Fr Er Messag
3	DB to Catalog	4	An adversary can gain access to sensitive data...	High	Not Started	Information Disclosure	An adversary can gain access to sensitive data...	Implementation	Force all traffic to Web APIs over HTTPS conne...	Sniff Web Tra
4	DB to Catalog	5	An adversary can gain access to sensitive data...	Medium	Not Started	Information Disclosure	An adversary can gain access to the config fil...	Implementation	Encrypt sections of Web API's configuration fi...	Sensit Data Cor Fi

Threats + risk per component

In [ ]:

```
grouped_df = df.groupby(['Interaction Name', 'Priority']).size().unstack(fill_value=0)

grouped_df.plot(kind='bar', stacked=True, figsize=(12, 8))
```

```python
plt.title('Ilość wykrytych zagrożeń na interakcje komponentów i ich priorytet')
plt.xlabel('Komponent')
plt.ylabel('Ilość wykrytych zagrożeń')
plt.legend(title='Priorytet')
plt.show()
```



In [ ]:

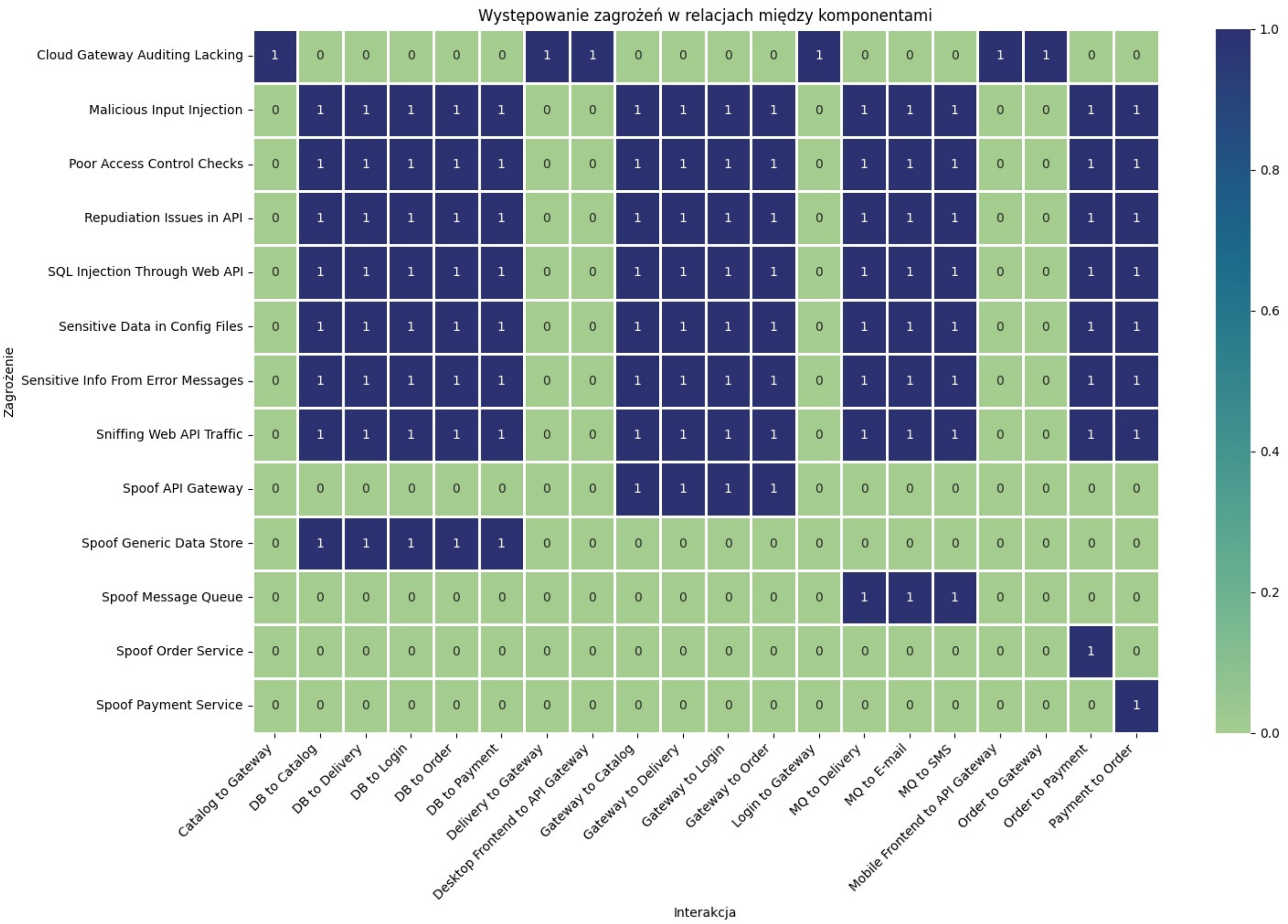
```python
# threats_shortened = [
#     "Zagrożenie niezaprzeczalności danych w API Gateway",
#     "Dostęp do wrażliwych danych przez SQL Injection",
#     "Możliwość podsłuchu ruchu sieciowego",
#     "Sensitive Data Exposure konfiguracji",
#     "Sensitive Data Exposure poprzez komunikaty błędów",
#     "Broken Access Control w API",
#     "Wpływ API Injection powiązane procesy",
#     "Spoofing serwisu API Gateway",
#     "Spoofing bazy danych",
#     "Spoofing Message Queue",
#     "Spoofing Serwisu Order",
#     "Spoofing Serwisu Payments",
#     "Zagrożenie niezaprzeczalności danych w API"
# ]

# threat_mapping = dict(zip(df["Summary"].unique(),threats_shortened))

# df["Summary"] = df["Summary"].map(threat_mapping)
# df["Summary abbv"] =
```

Threats in components

In [ ]:

```python
relations_threats_heatmap = df.groupby(["Summary abbv","Interaction Name"]).size().unstack(fill_value=0)

plt.figure(figsize=(16, 10))
```

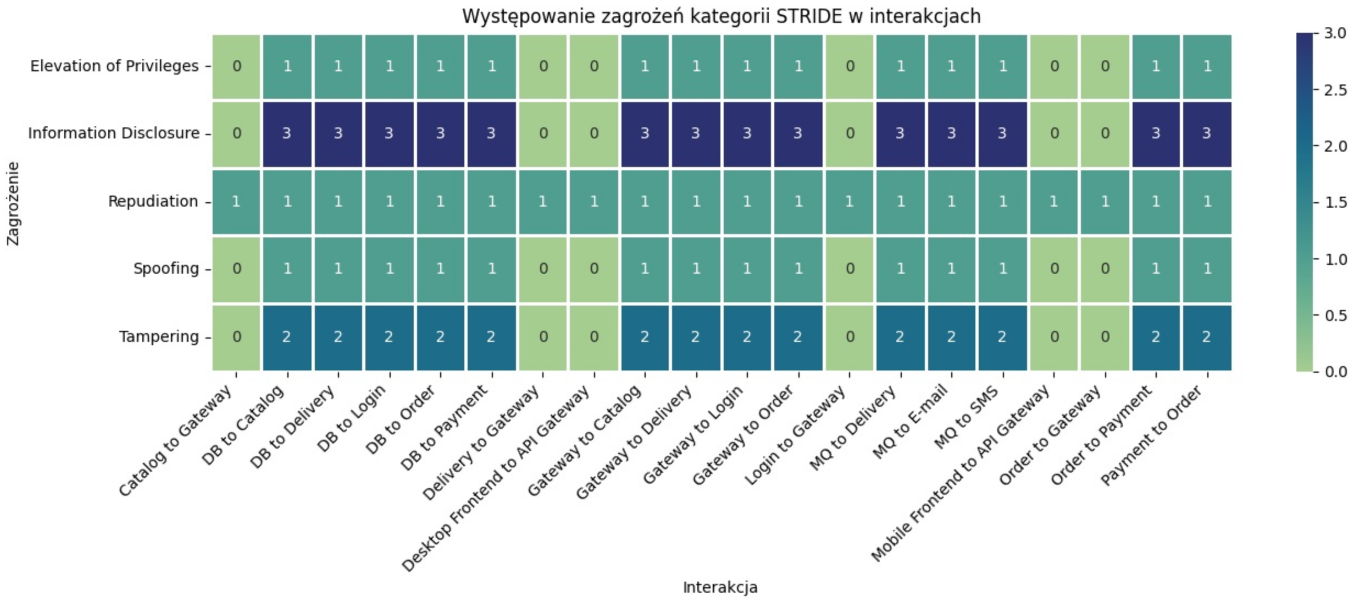
```
sns.heatmap(relations_threats_heatmap,annot=True,linewidth=1, fmt="d", cmap="crest")
plt.title('Występowanie zagrożeń w relacjach między komponentami')
plt.xlabel('Interakcja')
plt.ylabel('Zagrożenie')
plt.xticks(rotation=45,ha="right")
plt.show()
```



STRIDE Categories in Components

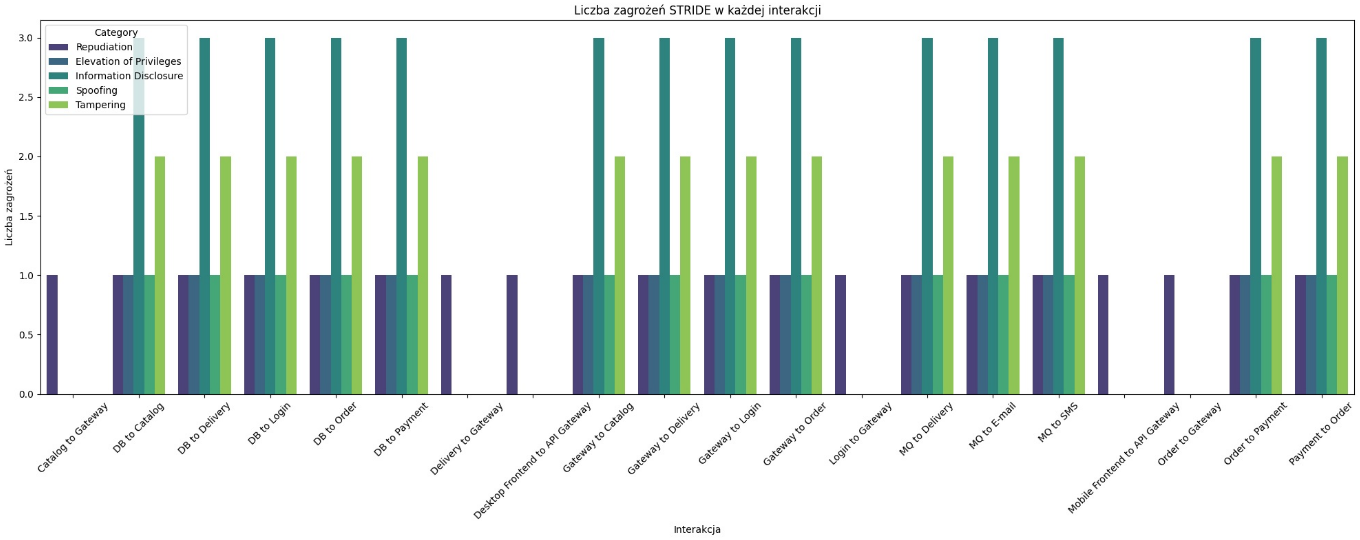
In [ ]:

```
summary_and_category = df.groupby(["Interaction Name","Category"])

summary_and_category_heatmap = summary_and_category.size().unstack(fill_value=0)

# sns.barplot(df["Interaction Name","Category"],x="Interaction Name",y="Category", cmap="YlGnBu")
# plt.title('Występowanie zagrożeń w relacjach między komponentami')
# plt.xlabel('Interakcja')
# plt.ylabel('Zagrożenie')
# plt.xticks(rotation=45,ha="right")
# plt.show()

interaction_category = df[["Interaction Name","Category"]]
category_counts = interaction_category["Category"].value_counts()

# plt.figure(figsize=(10, 6))
# sns.barplot(x=category_counts.index, y=category_counts.values, palette='viridis')
# plt.title('Count of Categories')
# plt.xlabel('Category')
# plt.ylabel('Count')
# plt.xticks(rotation=45)
# plt.show()


interaction_category_heatmap = df.groupby(['Category','Interaction Name']).size().unstack(fill_value=0)
plt.figure(figsize=(15, 4))
sns.heatmap(interaction_category_heatmap, annot=True,linewidth=1,cmap="crest")
plt.title('Występowanie zagrożeń kategorii STRIDE w interakcjach')
plt.xlabel('Interakcja')
plt.ylabel('Zagrożenie')
plt.xticks(rotation=45,ha="right")
plt.show()
```



In [ ]:

```python
# Grouping by 'Interaction Name' and 'Category' and counting occurrences
interaction_category_counts = df.groupby(['Interaction Name','Category']).size().reset_index(name='Count')

# Plotting the data
plt.figure(figsize=(20, 8))
sns.barplot(x='Interaction Name', y='Count', hue='Category', data=interaction_category_counts, palette='viridis
plt.title('Liczba zagrożeń STRIDE w każdej interakcji')
plt.xlabel('Interakcja')
plt.ylabel('Liczba zagrożeń')
plt.xticks(rotation=45)
plt.legend(title='Category')
plt.tight_layout()
plt.show()
```



Loading [MathJax]/jax/output/CommonHTML/fonts/TeX/fontdata.js