



Digital Risk Management during the Confinement

Analysis of Uber Eats

Thanh Tung TRINH
thanh-tung.trinh@epita.fr
Msc Data Science



What is a Risk?

A risk is constituted everytime a threat is able to access a valuable asset by exploiting a vulnerability and circumventing existing security controls.

“Một nguy cơ hiểm nguy được tạo thành từ một mối đe dọa có thể thâm nhập vào những tài sản giá trị mà kẻ xấu có thể lợi dụng kẻ hở của hệ thống và bỏ qua những phương thức bảo mật.”

Summary

1. Uber Eats is an online food ordering application on mobiles (iOS and Android) with the headquarter based in US. Uber Eats France.
2. During the confinement of corona virus, the increasing of food delivery is up to + 700% and Uber Eats has a huge demand at the moment.
3. Uber Eats utilizes the algorithm of mapping with massive motor bike and bicycle users in order to navigate the food delivery path.
4. As one of the most consuming service at the moment, Uber Eats is an ideal application for the hackers to execute the crimes.
5. The case of Uber Eats in this analysis is about France territory only, however other EU countries would have the similarities in terms of digital risk scenarios.

















Assumption

1. This analysis focuses on France Market.
2. Uber Eats using SFR and Telco as the provider for internet and LPWAN infrastructure.
3. Uber Eats has the AWS service to synchronize the users' data.
4. Uber Eats uses AWS to host their cloud platform.
5. Both Uber Eats Server and AWS server hosting are based in France.
6. Payment service is included within the Uber Eats application.
7. Restaurant connects with Uber Eats via the cloud platform of AWS back-end service.

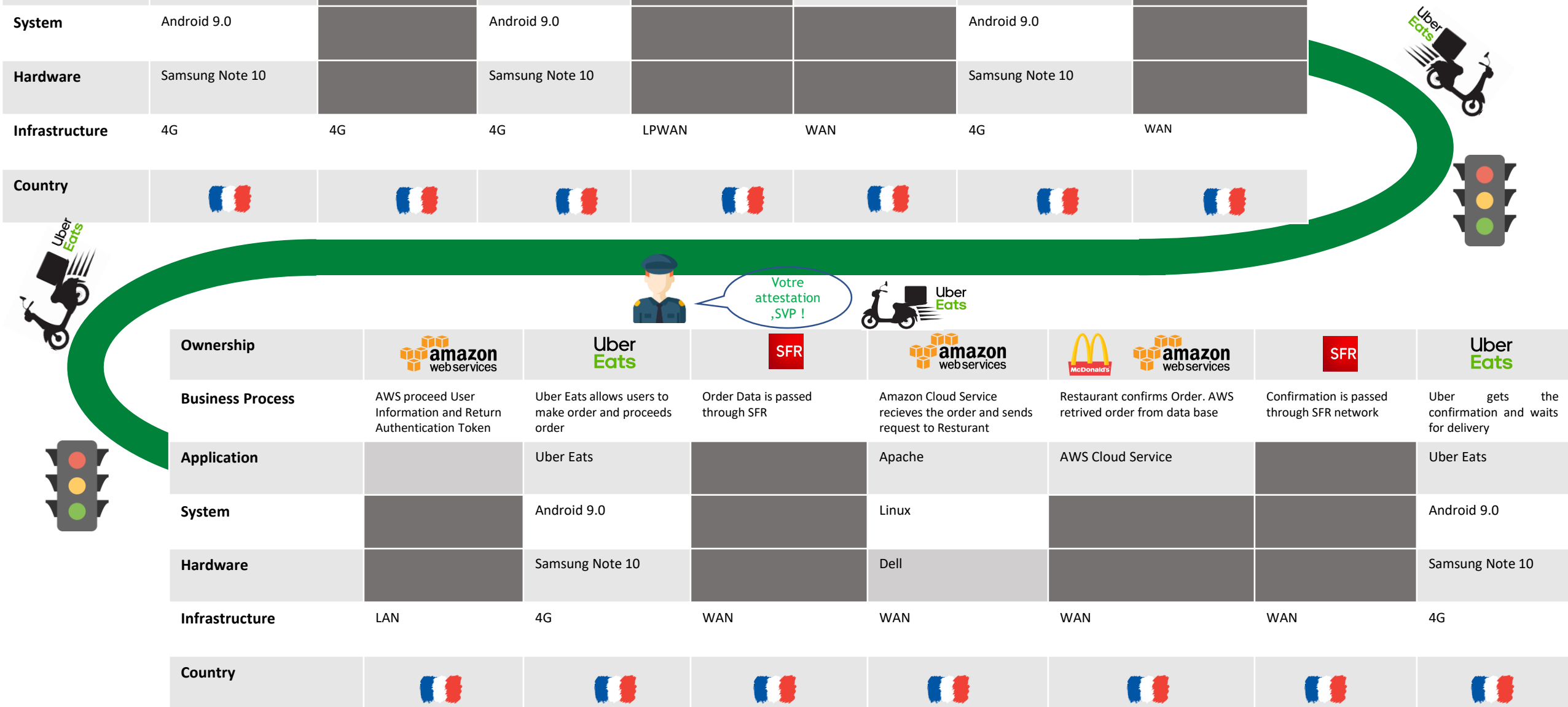


Uber
Eats
App Creator



Ownership	 				 		
Business Process	User taps on the Uber Eats App to start ordering Food	Uber Eats checks the internet connection of the phone	Uber Eats checks the User Authentication	SFR asks for Amazon IP Address to Telco France	SFR DNS returns with IP Address of Amazon	Uber Eats checks User Synchronizing and Location	SFR sends the Encrypted User Information to AWS Cloud Service
Application	Uber Eats		Uber Eats		DNS Server	Uber Eats	
System	Android 9.0		Android 9.0			Android 9.0	
Hardware	Samsung Note 10		Samsung Note 10			Samsung Note 10	
Infrastructure	4G	4G	4G	LPWAN	WAN	4G	WAN
Country							

What happens when you order food on Uber Eats during the Confinement?





Hacker Stories

Uber
Eats



HS1: As a hacker of from X-File, I want to follow the users in order to have the right place for advertising.

HS2: As a hacker sponsored by Delaware, I want to disrupt the proper function of the Uber Eats with a trojan so that the trustworthy of Uber Eats decreases.

HS3: As a hacker from Mafia Dark Web, I want to track the location of Kid through Uber Eats in order to execute the Kidnapping.

HS4: As a Uber Eats ex-employee, I want to access to customers email addresses, in order to destroy company's image.

HS5: HS5: As a hacker sponsored by a mapping company GALA, I want to make the wrong mapping on Uber Eats, so that Uber Eats can not function and will change to use the mapping of GALA.

HS6 : As a hacker with intention of a thief, I want to access the information on the Uber Eats app on a user, in order to know the absence time at home, so that I could guess the best time to execute the stealing.



HS7: As a hacker of ex-employer, I want to get the user data of Uber Eats and sell it to competitors.

HS8: As a hacker with intention of a robber, I want get the location of delivery man to rob his motor bike.

HS9: As a hacker of Grab X, I want to control the Uber Eats app by attack its server and ask Uber Eats for money.

HS10: As a hacker sponsored by a competitor, I want to launch a distributed denial of service attack to bring down the application servers of Uber Eats for 7 days, in order for the app to lose the customer

HS11: As a bad intentioned hacker, during the confinement, I want to put the fake news on Uber Eats app that people can go out to get free food so that the spreading of virus Covid 19 increases.

HS12: As a hacker from Aka - a competitor of AWS, I want to disrupt AWS infrastructure so that its partner's services such as Uber Eats will be stopped and they would switch to Aka's service

Risk Assessment

Uber
Eats



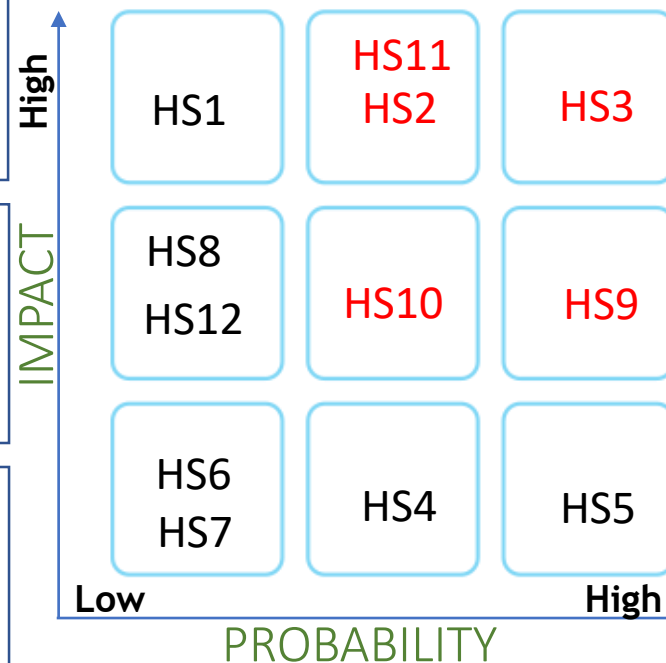
HS7: As a hacker of ex-employer, I want to get the user data of Uber Eats and sell it to competitors.

HS8: As a hacker with intention of a robber, I want get the location of delivery man to rob his motor bike.

HS9: As a hacker of Grab X, I want to control the Uber Eats app by attack its server and ask Uber Eats for money.

HS1: As a hacker of from X-File, I want to follow the users in order to have the right place for advertising.

HS4: As a Uber Eats ex-employee, I want to access to customers email addresses, in order to destroy company's image.



HS2: As a hacker sponsored by Delaware, I want to disrupt the proper function of the Uber Eats with a trojan so that the trustworthy of Uber Eats decreases.

HS5: As a hacker sponsored by a mapping company GALA, I want to make the wrong mapping on Uber Eats, so that Uber Eats can not function and will change to use the mapping of GALA.

HS10: As a hacker sponsored by a competitor, I want to launch a distributed denial of service attack to bring down the application servers of Uber Eats for 7 days, in order for the app to lose the customer

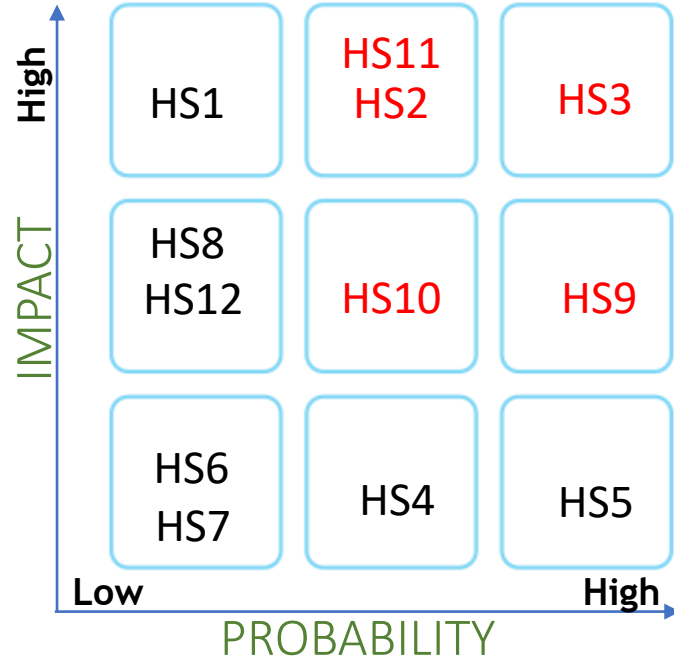
HS11: As a bad intentioned hacker, during the confinement, I want to put the fake news on Uber Eats app that people can go out to get free food so that the spreading of virus Covid 19 increases.

HS12: As a hacker from Aka - a competitor of AWS, I want to disrupt AWS infrastructure so that its partner's services such as Uber Eats will be stopped and they would switch to Aka's service

HS3: As a hacker from Mafia Dark Web, I want to track the location of Kid through Uber Eats in order to execute the Kidnapping.

HS6: As a hacker with intention of a thief, I want to access the information on the Uber Eats app on a user, in order to know the absence time at home, so that I could guess the best time to execute the stealing.

Risk Analysis



HS1: As a hacker of from X-File, I want to follow the users in order to have the right place for advertising.

Low Probability - the hacker wants the information of the user which can happen to any application. The intention for commercial purpose which can be replaced by other channels.

High Impact - If this happens, the security system of Uber Eats got the big problem. And it can also leak the payment information of users.

HS2: As a hacker sponsored by Delaware, I want to disrupt the proper function of the Uber Eats with a trojan so that the trustworthiness of Uber Eats decreases.

Medium Probability - The intention of the hacker was clear and he knew how to inject the trojan into the Uber Eats system.

High Impact - If this happens, the whole application will not function and users immediately aware of the problem. Users would highly remove Uber Eats out of the phone.

HS3: As a hacker from Mafia Dark Web, I want to track the location of Kid through Uber Eats in order to execute the Kidnapping.

High Probability - The hacker knows what he wants with a strong plan. As a widely used application, Uber Eats is a perfect target for those bad intentioned mafias. They could attack and steal the location information during the transaction between Uber Eats server and Mobile device via 4G internet.

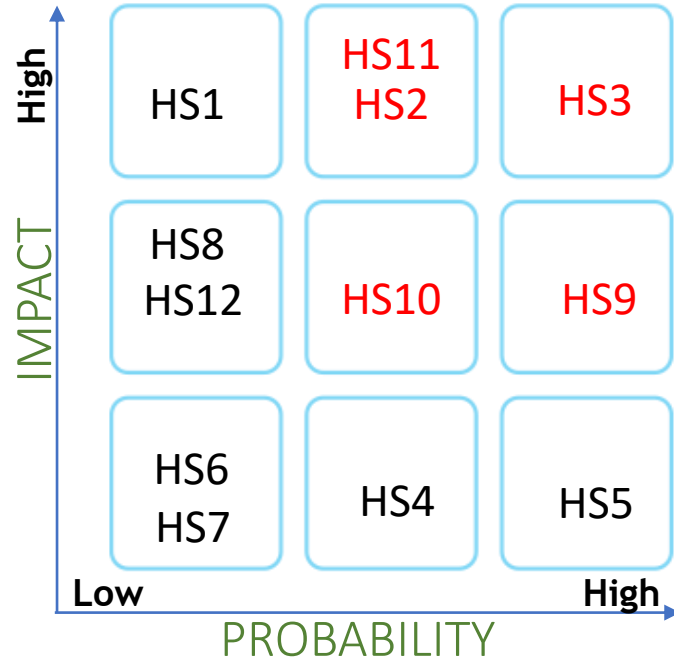
High Impact - This could impact to the lives of user and destroy the whole company trust. It will be a big crisis for Uber Eats which could lead to shut down the whole company.

HS4: As a Uber Eats ex-employee, I want to access to customers email addresses, in order to destroy company's image.

Medium Probability - The hacker was an employee before, so he would know how to enter the user's storage data.

Low Impact - Uber Eats can manage the media crisis by public relation.

Risk Analysis



HS5: As a hacker sponsored by a mapping company GALA, I want to make the wrong mapping on Uber Eats, so that Uber Eats can not function and will change to use the mapping of GALA.

High Probability - The hacker know how the mapping system works so he could easily break the security defense of mapping on Uber Eats

Low Impact - Changing supplier of mapping on Uber Eats will not impact much on the business operation. Just to make sure the user's experience will not be change so much.

HS6: As a hacker with intention of a thief, I want to access the information on the Uber Eats app on a user, in order to know the absence time at home, so that I could guess the best time to execute the stealing.

Low Probability - Uber Eats has the security system to preventing leaking user's information, the motivation of hacker is simple and it would rarely to happen.

Low Impact - Leaking user's information is a problem, but it can be quickly fixed the issue by implementing the fixing bug on system and create higher security defense.

HS7: As a hacker of ex-employer, I want to get the user data of Uber Eats and sell it to competitors.

Low Probability - The hacker knows how to access the system of user's information storing, but the motivation of competitor is low since data users can not help to increase switching immediately.

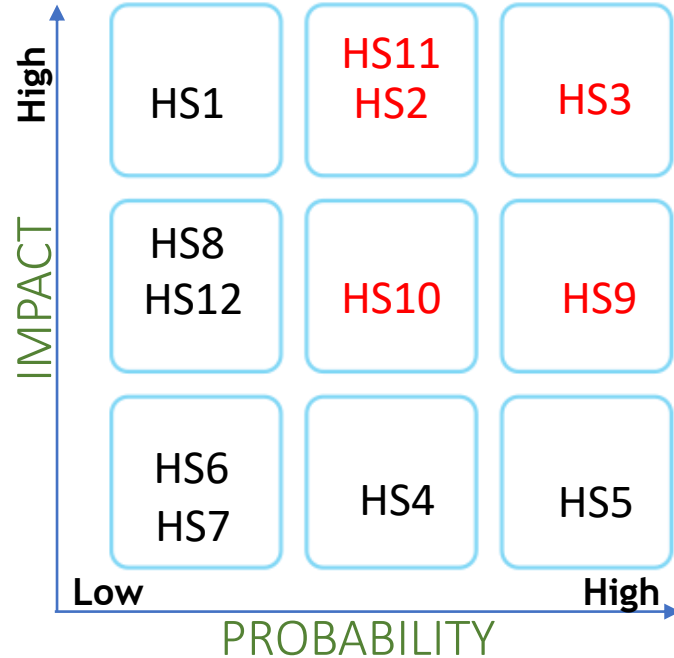
Low Impact - The user's information is useful for the commercial purpose. It may also impact to the company reputation.

HS8: As a hacker with intention of a robber, I want to get the location of delivery man to rob his motor bike.

Low Probability - This is a bad intentioned hacker, however he would not execute the crime for such a complicated hacking with only for stealing normal value thing.

Medium Impact - It could impact to the trust of the app to delivery staffs.

Risk Analysis



HS9: As a hacker of Grab X, I want to control the Uber Eats app by attack its server and ask Uber Eats for money.

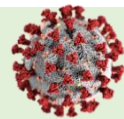
High Probability - the hacker could possibly attack to the security system of Uber Eats and control the application. From that, we would ask money from Uber Eats as a deal to give back the controlling right.

Medium Impact - it will impact to the whole application, and users will aware of the problem. It could impact to business in short term.

HS10: As a hacker sponsored by a competitor, I want to launch a distributed denial of service attack to bring down the application servers of Uber Eats for 7 days, in order for the app to lose the customer.

Medium Probability - The hacker is sponsored with strong support behind in term of finance and technology. They can shut down the application and the server of Uber Eats. The server can be taken down during the transaction between Uber Eats and restaurant, there is also a risk at this stage.

High Impact - if it happens, it would be a big impact to the system and consequently, user will switch to other competitor's applications.



HS11: As a bad intentioned hacker, during the confinement, I want to put the fake news on Uber Eats app that people can go out to get free food so that the spreading of virus Covid 19 increases.

Medium Probability - The ill-intentioned hacker has the criminal intention to spread out the virus by using fake news. This could happen during the confinement since users utilize the online food order really much.

High Impact - If it happens, it could be not only crisis to the Uber Eats but also to the lives of million people. This is an extrem criminal.

HS12: As a hacker from Aka - a competitor of AWS, I want to disrupt AWS infrastructure so that its partner's services such as Uber Eats will be stopped and they would switch to Aka's service

Low Probability - The company would rarely sponsor to a hacker to attack a server supplier. However, it still would happen.

Medium Impact - Uber Eats can change the supplier by another, just to make sure the performance of the app and user's experience won't change much. It could be a risk on taking time to harmonize the new supplier to the business.

Mitigation

- Reduce
- Transfer
- Accept
- Avoid

HS2: As a hacker sponsored by Delaware, I want to disrupt the proper function of the Uber Eats with a trojan so that the trustworthiness of Uber Eats decreases.

Rule 23 - Systematically use secure application and protocols
Rule 26 - Clearly define the objectives of system and network monitoring
Rule 25 - Secure the dedicated network interconnections with partners

HS3: As a hacker from Mafia Dark Web, I want to track the location of Kid through Uber Eats in order to execute the Kidnapping.

Rule 23 - Systematically use secure application and protocols
Rule 26 - Clearly define the objectives of system and network monitoring
Rule 27 - Define event log analysis methods
Rule 40 - Carry out a security audit

HS9: As a hacker of Grab X, I want to control the Uber Eats app by attack its server and ask Uber Eats for money.

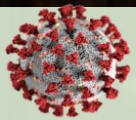
The rules also applies to AWS service
Rule 18 - Encrypted sensitive data sent through the internet
Rule 26 - Clearly define the objectives of system and network monitoring
Rule 27 - Define event log analysis methods

Mitigation

- Reduce
- Transfer
- Accept
- Avoid

HS10: As a hacker sponsored by a competitor, I want to launch a distributed denial of service attack to bring down the application servers of Uber Eats for 7 days, in order for the app to lose the customer.

Rule 23 - Systematically use secure application and protocols
Rule 26 - Clearly define the objectives of system and network monitoring
Rule 27 - Define event log analysis methods
Rule 8 - Identify each individual accessing the system by name and distinguish the user/admin roles



HS11: As a bad intentioned hacker, during the confinement, I want to put the fake news on Uber Eats app that people can go out to get free food so that the spreading of virus Covid 19 increases.

The Rule also applies to AWS Service
Rule 23 - Systematically use secure application and protocols
Rule 26 - Clearly define the objectives of system and network monitoring
Rule 27 - Define event log analysis methods
Rule 40 - Carry out a security audit



Reference:

<https://www.ubereats.com/fr-en>

<https://www.shutterstock.com/>

<http://www.leparisien.fr/societe/coronavirus>