DIGITAL RISK MANAGEMENT
Analysis of
GATOR SMART WATCH

BY,
SOUMYA GUDURU

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.

ప్రమాదం అంటే ఏమిటి ?

ముప్పును విశ్లేషించడిం మరియు ఇప్ంటికే ఉన్న భద్రతా చర్యలను ప్రిమితిం చేయడిం ద్వారా ఒక ఆస్తిని యాక్సెస్ చేయగలగడిం వలన్ ద్వారిం ఏర్ండుతిందిి.

SUMMARY

Gator watch is a wearable mobile phone designed especially for 5-12-year-olds. It uses GPS, two-way calling, works across multiple networks and has an SOS feature for peace of mind.

In this analysis, We are looking at the possible risks that arises from the using Gator Smart watch for kids.

ASSUMPTION:

A mother buys the Gator smart watch for her kid and download the Gator App on her Samsung mobile using Google Playstore.

Mother opens the App to check the current location of the kid when the kid goes out for playing.

FEATURES OF GATOR

- SOS BUTTON FOR THE KIDS. STARTS CALLING ALL EMERGENCY NUMBERS IN LOOP.
- 4 DAY STANDBY BATTERY
- EASY TO CALL AND RECEIVE CALLS
- REALTIME TRACKING IF YOUR KIDS LOCATION
- GLOBAL RANGE. WITHOUT ANY RANGE LIMITATION. WORKS WORLD-WIDE

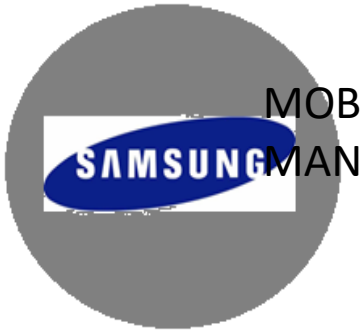
CREATORS OF GATOR WATCH

ACTORS

DNS PROVIDER

WATCH USER

APP
DISTRIBUTER



MOBILE DEVICE
MANUFACTURE

INTERNET PROVIDER
OF CHINA

APP SERVER &
DATACENTER

WBSITE HOSTING
SERVER

OWNERSHIP	SAMSUNG	GATOR KIDS GPS WATCH	NEWWAVE COMMUNICATIONS	GoDaddy	西部数码 www.west.cn
BUSINESS PROCESS	A Mother downloads the Gator App from the Google play store	Mother tries to use the Gator mobile App to check the location of her child	Mobile connects to the internet using NEWWVAE internet service provider	DNS provider for the Gator service is GoDaddy.	Chengdu West Dimension Digital Technology Co.LTD cloud server hosts the gator FE server . It receives the request.
APPLICATION	Gator App for Android	Gator App for Android			Gator Application Server
SYSTEM(OS)	Android 8.0 Oreo	Android 8.0 Oreo			
HARDWARE	Samsung Galaxy A9 Pro	Samsung Galaxy A9 Pro			
INFRASTRUCTURE	4G	4G			
COUNTRY	CHINA	CHINA	CHINA	CHINA	CHINA

OBASHI

OWNERSHIP	西部数码 www.west.cn	西部数码 www.west.cn	NEWWAVE COMMUNICATIONS	SAMSUNG
BUSINESS PROCESS	CWDDTechnology Co.LTD sends the request to the backend server	Chengdu West Dimension Digital Technology Co.LTD Data Center retrieves the updataed location from the DATABASE	Respond is passed through NewWave Network	Mother views the current location of her child in the App
APPLICATION	Gator Application Server	Gator DataBase server		Gator App for Android
SYSTEM(OS)				Android 8.0 Oreo
HARDWARE				Samsung Galaxy A9 Pro
INFRASTRUCTURE				4G
COUNTRY	CHINA	CHINA	CHINA	CHINA

HACKER STORIES

HS1	As a hacker sponsored by a competitor I want to hack the server put the denial of service attack to bring down the Application servers of Gator for an hour in order for the app deemed unreliable
HS2	As a hacker sponsored by the competitor I want to hack the server to know their Business model of the company
HS3	As a self employed hacker, I want to hack Volusion Data Center where Gator stores the credit card details of the payments, to steel the credit card details of the users and misuse them.
HS4	As a self employed hacker I want to hack the DB to know the email ids of all the users registered and sell the data to a third party which uses the details for sending promotional messages.
HS5	As a hacker in a partnership with a thief, I want to hack the user mobile and to stalk the kids location to kidnap and ask for money

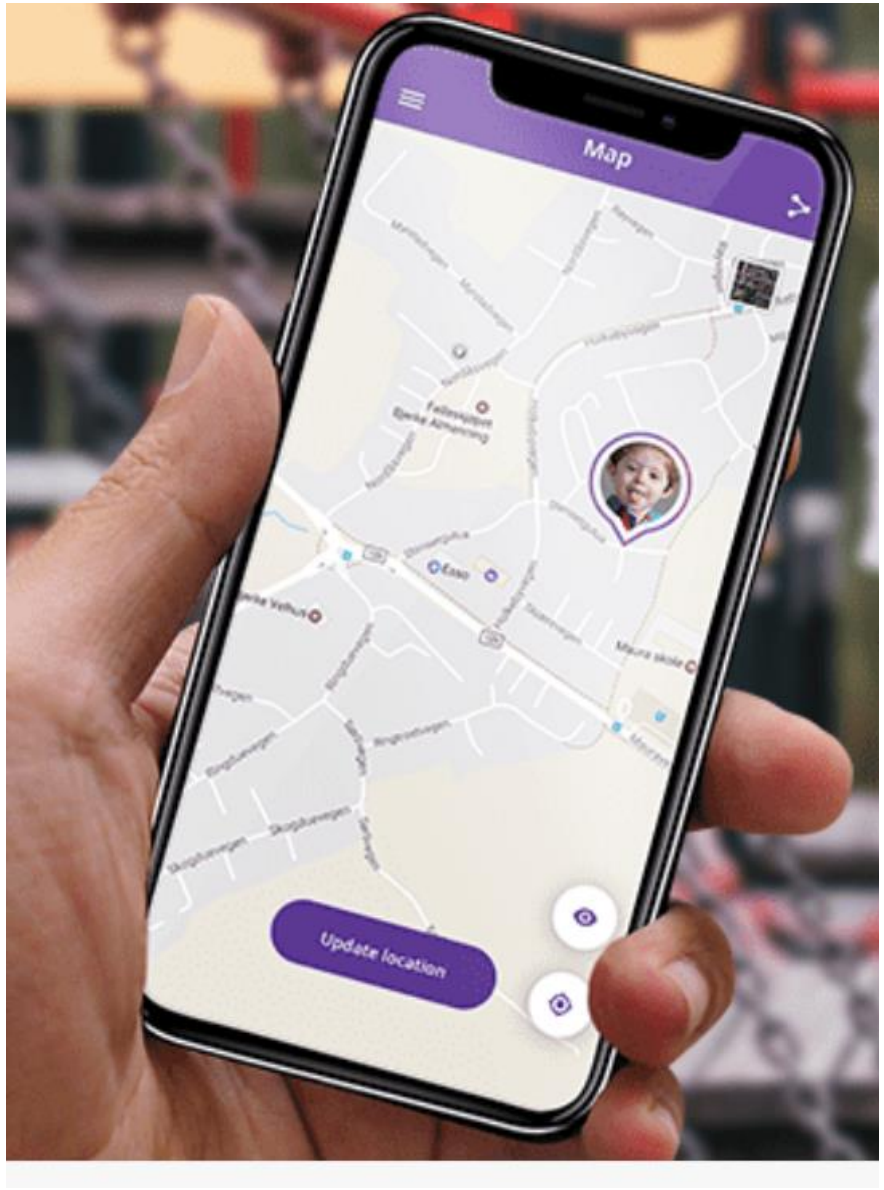
HS6	As a hacker sponsored by competitor, I want to hack the server and put malicious code in the application so the app always shows one constant location for all the users, so users feel Gator is not reliable
HS7	As a teen neighbor with hacking skills I want to jam the signals of the mobile so the call gets disconnected
HS8	As an ill intention employee of Chengdu, I want to sniff the data received to Gator App server and find the location of a children and sell the data to mafia
HS9	I want to hack the Gator watch and stop its location tracking functionality by tampering with its GPS module.
HS10	As a hacker of the Tesco mobile network company, I want to hack the base station, to disturb the calls , so that Gator leaves partnership with EE, Vodaphone & O2 in Uk and switches to my network which is in loss
HS11	As a hacker I want to hack the DB to know a particular child's location to kidnap the kid
HS12	As an existing smart watch company in the market for a decade, I want to hack Volusion Data Center , go get all the user credit card details and air it online, so Gator will be sued under GDPR
HS13	As a designer of Gator who is coerced by the sales manager of the company, I want to replace the batteries of gator1 watch with some low potential batteries which function for 1 year , inorder to boost users to switch to Latest Gator3 watch
HS14	As an employee of Gator Manufactures, who is bribed by the Competitors, I want to temper with the GPRS module during the manufacturing process, inorder to cause visible malfunction while location tracking

RISK ASSESSMENT

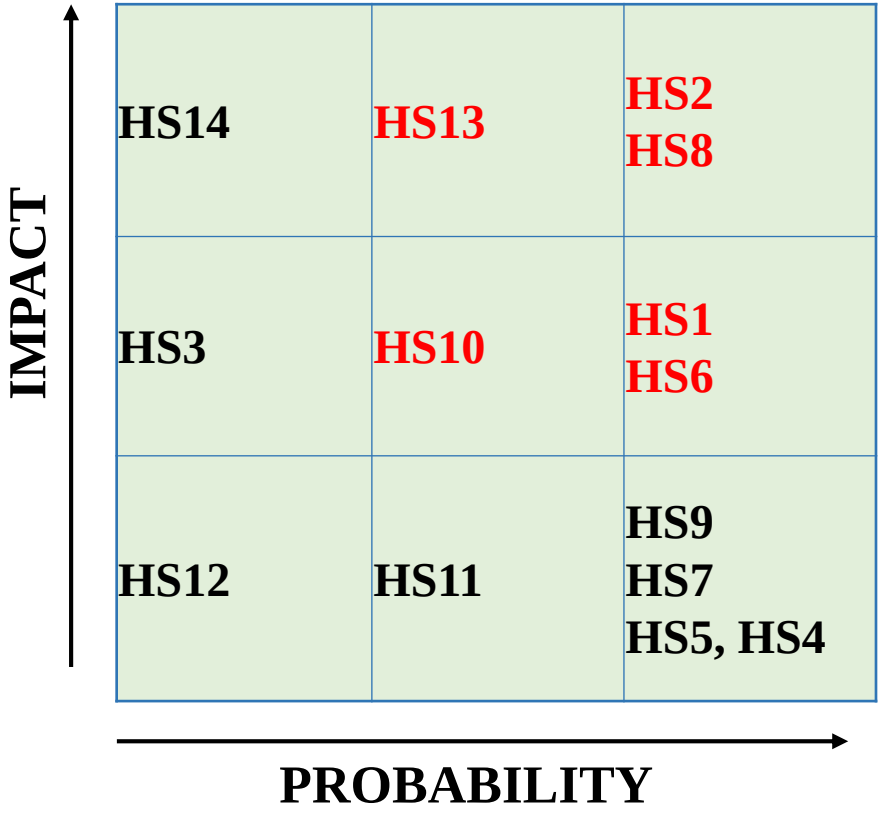
IMPACT

HS14	HS13	HS2 HS8
HS3	HS10	HS1 HS6
HS12	HS11	HS9 HS7 HS5, HS4

PROBABILITY

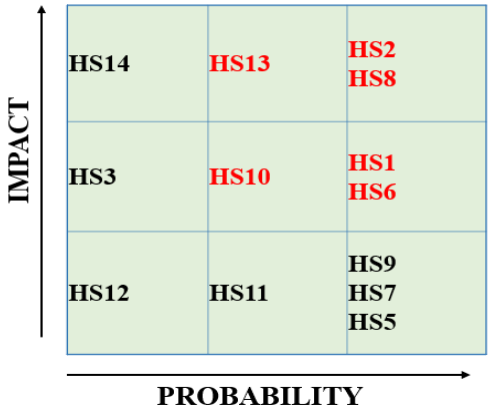


ANALYSIS



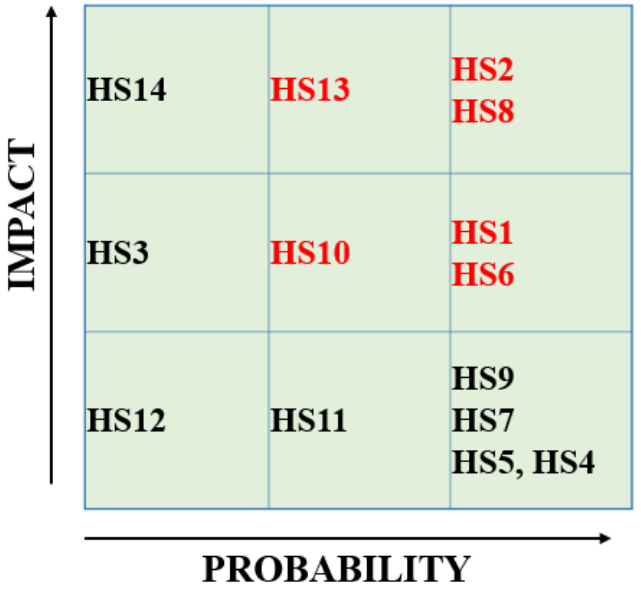
HS1	As a hacker sponsored by a competitor I want to hack the server put the denial of service attack to bring down the Application servers of Gator for an hour in order for the app deemed unreliable	**High Probability** - Gator competitors will have a strong intention to take the company down as Gator pose a big threat for their existing products or services. There are many means to perform a DDoS attack, and there are also tools readily accessible for low skilled hackers to use.
		Medium impact - as the attack may go unnoticed because of the 1 hour duration. All the bank applications or any other dynamic website may have service unavailable for a day which is totally understandable
HS2	As a hacker sponsored by the competitor I want to hack the server to know their Business model of the company	**High Probability** - as hacker is sponsored by the competitor so they can afford all the resources
		High Impact - if the business model gets leaked, competitor's can implement the same product with same features, and if they sell it for low price than gator, Gator will its market completely
HS3	As a self employed hacker, I want to hack Volusion Data Centre where Gator stores the credit card details of the payments, to steel the credit card details of the users and misuse them.	**Low Probability** - as Volusion Datacenter stores the Data in encrypted form. So even if the hacker gets his hands on the Data it will near it impossible to decrypt them
		Medium Impact on Gator, as they outsourced a third party for the Website hosting. Gator can sue Volusion for any Data loss form their side, But gator may lose its customer belief and it may state that it is cancelling the partnership with Volusion ,so impact is medium

ANALYSIS



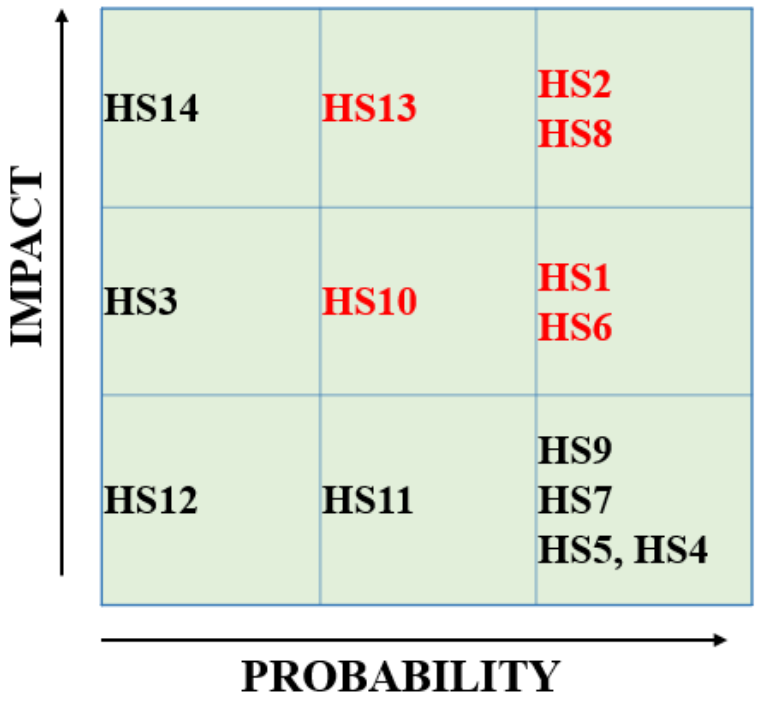
HS4	As a self employed hacker I want to hack the DB to know the email ids of all the users registered and sell the data to a third party which uses the details for sending promotional messages.	**High Probability** as it is easy to do so by a skill full individual hacker
		Low Impact on Gator as the users will not be bothered much by the promotional messages
HS5	As a hacker in a partnership with a thief, I want to hack the user mobile and to stalk the kids location to kidnap and ask for money	**High Probability** as it is easy to hack a users mobile
		Low impact on Gator as the hacking is done on users mobile phone
HS6	As a hacker sponsored by competitor, I want to hack the server and put malicious code in the application so the app always shows one constant location for all the users, so users feel Gator is not reliable	**Medium Probability** Gator transmitted the data without any encryption and to tamper with GPS module user should first know the all technical details of gator
		Medium Impact, because QA team may that perform regular test on the server code will recognize the defect within a day and remove the malicious code
HS7	As a teen neighbor with hacking skills I want to jam the signals of the mobile so the call gets disconnected	**High probability-** It is very easy to jam the signals with open source education available today. Youngsters would be amused and thrilled to tamper with the technology
		Low impact on Gator as the user may think it is the network problem because the mobile device will have zero signal
HS8	As an ill intention employee of Chengdu, I want to sniff the data received to Gator App server and find the location of a children and sell the data to mafia	**High Probability** as the Gator stores and transmits its data without encryption
		High Impact if this news gets publicized as the children wearing the gator watches are prone to security issues then no parents would prefer this product

ANALYSIS



HS9	I want to hack the Gator watch and stop its location tracking functionality by tampering with its GPS module.	**High Probability** as it is easy to hack a device
		Low impact on Gator, as gator watch has 4 different types of location tracking modules . If GPS module is not working location will be traced by mobile network.
HS10	As a hacker of the Tesco mobile network company, I want to hack the base station, to disturb the calls , so that Gator leaves partnership with EE, Vodaphone & O2 in Uk and switches to my network which is in loss	**Medium Probability**, as a network company which is in loss, it may not be able to afford to disturb lines of three major networks of UK
		Medium impact on Gator, as the calls may be disturbed but the user can still view the exact location of their child on the APP , which gives little piece of mind to the parents
HS11	As a hacker I want to hack the DB to know a particular child's location to kidnap the kid	**Medium Probability** as the datacenters network administration will be very cautious regarding any intrusions
		low impact as the Kidnapper planned to kidnap a child to ask money from the parents and nobody will ever that how kidnapper got the location
HS12	As an existing smart watch company in the market for a decade, I want to hack Volusion Data Centre , go get all the user credit card details and air it online, so Gator will be sued under GDPR	**Low Probability** as Volusion Data center stores the Data in encrypted form. So even if the hacker gets his hands on the Data it will near it impossible to decrypt them
		Low Impact as users will have the right to sue Gator for lack of protection of data, but as the data is encrypted if they publish the data online ,it will be just some random Alphanumeric digits

ANALYSIS



HS13	As a designer of Gator who is coerced by the sales manager of the company, I want to replace the batteries of gator1 watch with some low potential batteries which function for 1 year , inorder to boost users to switch to Latest Gator3 watch	
	Medium Probability - There is a strong intention for the sales manager to do so, as it is vital for sales to ensure that users always buy new devices. But the team may not accept to this practice or even if 1 person whom they discussed with did not agree, they will not be able to implement it, as there is a risk this person may whistleblowing	**High Impact** - Assuming that Gator gets caught, or the whistle-blower leaked the wrong ideas Gator had, it is terrible publicity. As a start-up, Gator will lose all its investors for any further funding

HS14	As an employee of Gator Manufacture Bribed by the Competitors, I want to temper with the GPRS module during the manufacturing process, inorder to cause visible malfunction while location tracking	**Low Probability**: There would be QA efforts performed regorsly before any module application going into production
		High Impact: Assuming if the employee manages to temper with a full batch of the product , it could be very costly for the Company to investigate and remanufacture the devices

MITIGATION

HS1	RULES THAT APPLY	MITIGATION
As a hacker sponsered by a competitor I want to hack the server put the denial of service attack to bring down the Application servers of Gator for an hour in order for the app deemed unreliable	RULE 21: Use secure Network protocols when they exist RULE 36: Activate and configure the most important component logs Rule 7: Only allow controlled devices to connect to the network of the organization	Rule 21 would ensure that the servers are developed with the concept of security by design Rule 36 is required in order to be able to detect possible malfunctions and illegal access attempts to the components of the information system. Rule 7 will help in dectecting the any unauthorised devices trying to connect to the network

HS13	RULES THAT APPLY	MITIGATION
As a designer of Gator who is coerced by the sales manager of the company, I want to replace the batteries of gator1 watch with some low potential batteries which function for 1 year , inorder to boost users to switch to Latest Gator3 watch	**RULE 21: Use secure Network protocols when they exist** **Rule 26 - Clearly define the objectives of system and network monitoring Rule 36 - Activate and configure the most important component logs** **Rule 38 - Undertake regular controls and security audits then apply the associated corrective actions**	**Rule 21 would ensure that the Base stations are developed with the concept of security by design** **Rule 26 and 27 would ensure that the parameters of a host-based intrusion detection system is in place, to enable the detection of an unauthorized execution of a software update. Rule 36 is required in order to be able to detect possible malfunctions and illegal access attempts to the components of the information system.** **Rule 38 would ensure that a security audit is conducted atleast once in a year**

HS8	RULES THAT APPLY	MITIGATION
As an ill intention employee of Chindon, I want to sniff the data received to Gator App server and find the location of a children and sell the data to mafia	Rule 26: Control and protect access to the server rooms and technical areas Rule 7: Only allow controlled devices to connect to the network of the organization Rule 18: Encrypt sensitive data sent through the Internet RULE 28: would ensure that non privileged users will not be able to see the machines used for system administration on their current network, and even if they do, they will not have privilege access to these machines. RULE 29: Reduce administration rights on workstations to strictly operational needs	Rule 26 achieves Physical security mechanisms must be a key part of information systems security and be up to date to ensure that they cannot be bypassed easily Rule 7 will help in detecting the any unauthorized devices trying to connect to the network RULE 18 would ensure that even if the hacker successfully intercepts the data in transit, he/she will not be able to decrypt the information Rule 28 and Rule 29 would ensure that non privileged users will not be able to see the machines used for system administration on their current network, and even if they do, they will not have privileged access to these machines.

HS10	RULES THAT APPLY	MITIGATION
As a hacker of the Tesco mobile network company, I want to hack the base station, to disturb the calls , so that Gator leaves partnership with EE, Vodaphone & O2 in Uk and switches to my network which is in loss	RULE 21: Use secure Network protocols when they exist Rule 36 - Activate and configure the most important component logs Rule 38 - Undertake regular controls and security audits then apply the associated corrective actions	Rule 21 would ensure that the Base stations are developed with the concept of security by design, inorder to stop the adversies break into the base stations. The cell-site vault is a secure processing environment designed to resist such tampering and to protect the sensitive functions associated with cellular processing. Rule 36 is required in order to be able to detect possible malfunctions and illegal access attempts to the components of the information system. Rule 38 would ensure that a security audit is conducted atleast once in ayear

HS2	RULES THAT APPLY	IMITIGATION
As a hacker sponsered by the competitor I want to hack the server to know their Business model of the company	Rule 7: Only allow controlled devices to connect to the network of the organization Rule 19: Segment the network and implement a partitioning between these areas Rule 4: Identify the most sensitive information and servers and maintain a network diagram	Rule 7 will help in dectecting the new devices trying to connect to the network Rule 19 will help in reducing the damage as not all the information of the company is placed on one server Rule 4: will help to help to resolve the part of the server through ehich the hacker is trying to enter the network

HS6	RULES THAT APPLY	MITIGATION
As a hacker sponsered by competitor, I want to hack the server and put malicious code in the application so the app always shows one constant location for all the users, so users feel Gator is not reliable	RULE 21: Use secure Network protocols when they exist Rule 36 - Activate and configure the most important component logs Rule 4: Identify the most sensitive information and servers and maintain a network diagram Rule 7: Only allow controlled devices to connect to the network of the organization Rule 19: Segment the network and implement a partitioning between these areas	Rule 21 would ensure that the Base stations are developed with the concept of security by design Rule 36 is required in order to be able to detect possible malfunctions and illegal access attempts to the components of the information system. Rule 4: will help to help to resolve the part of the server through which the hacker is trying to enter the network Rule 7 will help in detecting the new devices trying to connect to the network Rule 19 will help in reducing the damage as not all the information of the company is placed on one server

THANK YOU