

|  |  |  |  |
| --- | --- | --- | --- |
| DEPARTMENT | **MCA** | SEMESTER | **SUMMER SEM. I 2021-2022** |
| **COURSE** | **CLOUD COMPUTING** | **CODE** | **ITA-6009** |
| FACULTY | Prof. NEELNARAYANAN V | SLOT | AB1/AB2 |
| STUDENT NAME **:** | **DINESH YOGESH PAREKH** | REG NO | **20MCA1013** |

**Detecting insider based attacks in cloud**

we gonna talk about the threat modeling so we're going to see what are the threats that the attacker can exploit to get into the SAS systems or network and then we're going to focus mainly on the cloud computing threats because those are the main threats that I guess people are more curious about learning nowadays like using the old data centers and then like you know everything every data is on one from Isis the days are gone now so we focus more on the under cloud computing threat but let's see Enchant-ix like what are the other threats that we have in common right so of course one of the main thing is the cloud computing crash we will dive into those the other thing is about the advanced persistent threats if you are interesting interested to know about more in details let me know then the viruses and warm so these are very common and like you know this is one of the biggest threat not just for the enterprise but also for the personal computers as well then we have

ransomware we have seen enough examples of this in the recent times where large and larger enterprise gets attacked by the ransomware and then they have to like them big to get rid of it so these are another most recent and very popular threat then we have mobile threats of course this is very common as well because nowadays everything is on worldwide smartphones and I will imagine how with someone like you know and not just the mobile devices but but imagine if someone gets hold of him evaluates how much data can can attacker can get like people do not care about this a lot and they don't think about it but it is a lot it's as big and as I would say as as more risk as someone could get the laptops oh man this is a big threat as well then we have botnets of course by using computing cloud computing but there are a lot of botnets and don't all over that that's been happening as well then we have insider attack this is this has never gone off the list ever since we have the internet or ever.

Since we have this enterprises and there's always an insider threat and that's why companies are investing or I would say like you know utilizing more and more or the security awareness training and stuff like that then we are fishing again how sort of like early security awareness people should be aware like how can they get fished but again this is one of the kevin Mitnick if you know her name of the person he is the famous I guess person who would conduct this sort of like you know phishing attack so it's also very common then we have our application to us we talk about this all the time we have a separate playlist of all the application text so if you are curious to know just go and check it out but there are just thousands of application threads we have and nonetheless IOT threats because there are things like smart refrigerator right so that's an internet of things we have smart speakers we have Alexa we have Google home I don't know like we have just tons of smart devices into our home and then every every device is suspect about to the to the attack now imagineone scenario it's a home network and your home router iPad like you know 50% of people are not patching their home router regularly so of course that's a like you know basic attack or basic .

I would say target for any attacker so if someone gets into the home network now home network is connected now with the multiple devices so your refrigerator is connected your let's say thermostat is connected your mobile devices are connected your PCs your kid species and everything is connected now once the attacker gets into the home router now they have access to pretty much every device did the home like it's controlled using the home router or modem now once they get into let's say one of your cell phone right so that through that they can now see all the traffic although it's encrypted but attacker can still see which sites are being visited and all those things so they're still gonna see all those details now they get into this home network and then now they also got into this mobile device now imagine you took the same phone to your to your place like work work place or anywhere now you're switching the Wi-Fi network but now since attacker has access to your phone mobile phone mobile device now they can now your entire network the workplace network is exposed because of your wonder wall device is your mobile device and imagine how how long it this could go so I have the threats are big nowadays have they're just new a new device is coming like the watch and they just count these devices we have for the Internet of Things and all of them are of course a big threat if we are not securing it properly .

Now yeah these are like you know so many threats out there and that there are few more as well I'm sure I've not like you know consolidate all of them but still deserve this a few high ones that I thought like you know might be useful to talk about now let's take a deep dive into the cloud computing threats one of the I guess benefit of moving on to the cloud computing is you do not someone who wants the large computing power doesn't have to buy all the equipments they can just of course it it cost you a lot but as long as you have your credit card you can pay it you can get as much complete power as you want by just logging in to the website and then subscribe to whatever the computing power you want and use it right so that's a benefit as well as the threat so because the attacker can use this the same service to attack against the other organization so one of the first things going to talk about is the company's power to crack the password now imagine back in the days where you had like a CPU where you could fire maybe like you know let's say 100,000 150,000 correct passwords per second now using the cloud computing they have like so man virtual machines you can subscribe to millions of device like millions o systems and then spin up spun up all those devices and then use that company power to crack the password so that's quite possible and that's why every fact has to have some controls around readwrite so the controls that we highly recommend to everyone is of course you should have detection for the brute forcing you should also make sure your passwords are complex because even though your passwords are let's say very complex and is let's say 16 characters with alphanumeric and everything then even even like the millions of computing power like even someone tries to crack like with a million password seconds they're not able to crack it because of course your password secure the chances of creating the part that complex password is is literally a 50-50 possibility at that point so of course there's a big thread but then we also have control around it and and that's something everyone should consider .

So let's talk about the data loss threat so data loss threat is imagined back in the days we had like a big data center where only one company would have their own signal systems and storing all the data

so all the other tenants had like no physical separation and also there's a

of course logical separation as well now in the cloud computing there was your machines and there are chances that your data might be hosts on the same device or same system where the other kind of data I located so it's just logically separate not the physical separation is anymore there now the data loss is a bit of threat here because I someone goes wrong then you're just losing data to one customer you're just losing bid off all the customers who are hosting or using that particular systems or cell systems or region of course there is a way like

attacker would be more focused on stealing this data because if they deploy like perfectly well-crafted virus or malware or something they can delete like you know change the integrity of the data they can destroy the data they can also steal the data so you can do whatever you want so that's that's a big big threat here of course this is a sort of like a shared responsibility between the top provider and the client customers who are using this cloud computing they have to configure the services such a way that it doesn't get affected oh no it doesn't get like you know don't have everything in plain text and all those things so you don't you have some some power of limiting the data loss here the next one is the stealing information from other resources now imagine in the data center you have like a lesson to people and the system administrator with limited access to certain things now in the cloud computing if someone has access to your cloud account and they they have access to all the resources when they log in that they'll be a very scenario because that's just impossible to imagine that one people having access to everything and then there is no accountability on what the person can do and that's why we have this cloud provider provides with the policies and other controls like a logging and roles and all those things which which administrator can use and restrict the employees to use what kind of things they can do after having access to the cloud or counseling if you need access let's say if the HR person need access to be some of the data like the employee we'll only be able to access that particular data and not anything more than that so you can have these roles and policies defined to cover control this threat and the last one is the data tag so are we we pretty much talks about this by discussing about like you know how much computing power one can have so if I can I can let you know subscribe to let's say millions of easy to devices and then I use those computing power to attack against one of the system .

I can absolutely do that and and that's that's so easy to carry out like if if that cloud provider is not fast enough to understand and react to the situation and also the defender all the audio victim is no does not have any control in place like the introduction or prevention sort of systems firewalls and all those things then of course this attack could be successful but then again we have this controls in place and if you are not using these controls in the right way you could be suspect evolve to this threats as well so there are so many other threats out there like once we go into more depth I guess we'll will talk about those but these are some time editors that you should always consider when you are using cloud or when you are moving to the cloud and make sure your customers also understand this very well so that's all from this particular week and yeah if you have any questions yeah keep them coming I know that tons of questions coming down on the various different stuff and I try to get on top of it as much as I can but please bear with me if I don't respond very quickly but I'll try to get you as soon as I can and let me know if you have any other suggestions for the next week I'll try to implement that I'll try to provide you some more information on whatever topic you need help it until the English (auto-generated) we are going to be talking about something very fundamental and at the same time very very critical to an organization what usually gets overlooked but what needs a high priority of detection and follow-up on that specific case so we're talking about insider threats through today's webinar I'm also going to be giving you pointers on how to detect insider threats what sort of signs to look for when we are talking about insider threats and how do you effectively mitigate and potential insider threat or how do you retaliate when something of that sort happens all right for those who want a copy of the webinar that's going to be available all you have to do is leave your email ID towards the end of the session and I'd be able to send you over the video and the presentation deck as well so that being said let's quickly get into the topic when it comes to fraud prevention especially many organizations tend to overlook the idea of insider threats it could be both malicious or it could be probably accidental many times insider threats aren't accidental but malicious so that being the case administrators are very much equipped with tools I'd say probably your sim solution that can detect a potential data breach or a potential external attack and give you real-time updates on what's going wrong but when it comes to office 365 who would expect our security outage that's happening from the inside not not many of us right in fact we'd be absolutely certain about the fact that our users are going to not try to do anything crazy but on the contrary we've got statistics that prove otherwise they is a huge shift in how the at tack landscape is evolving and much to our concern it is essentially the insiders who caused majority of the attacks in the organization mostly knowingly and few accidentally you know we still have employees writing their passwords on a piece of sticky note and sticking them right on top of their desktop how are we going to save our organization with probably advanced machine learning and user behavior analytics and things like that so is fundamentally starts with having practices in place that are going to help you certain or a certain the fact that there's no potential loophole that an attack either with a malicious intent

or someone unknowingly does something

wrong to your organization so we dissect

how insider activities work we'll

understand what could potentially lead

to a threat we'll also then go forward

talking about what kind of attacks do

insiders pull off and what signs you

need to look for when you are talking

about insider threats and finally I'll

give you five easy tips that you can

implement right away when you know

something's gone wrong so I'll be giving

you real-time insights data numbers

please do to pay close attention I'll

also be giving you action items to go

back and perform and towards the end of

the session I'm also going to be sharing

a couple of ebooks that we have put

together to help you secure your office

365 better to start off with we'll

understand what insider threats are so

insiders are not basically a employees

working in your organization's with the

growing roles of accidental insider and

fraud schemes it's high time that we

understand and we stand up to an insider

threat by probably having a program to

stop a malicious intent that is pretty

much the idea so when it comes to

critical assets in the organization it's

probably going to be the people the most

important asset it could be information

which again is vital to your

organization now that there are so many

complex regulations that are in place

that require you to secure your

information to trap your

to audited and ensure that you have a

system in place that tells you if any

probable personally identifiable

information goes out of the system quite

a lot around information and obviously

facilities are also quite an important

critical asset many a times what happens

is a potential individual who has

authorized access is the one who turns

out to be the one causing access I mean

all the losses so inside us a couple of

times they're not with malicious intent

and it could basically be because of

quite a few reasons they could be

regular employees in the organization

who are disgruntled with how the system

works so they go on and die except what

Allah they go on and transfer data from

inside the organization to someone

outside the organization or probably

have some confidential information of

the organization displayed on the

internet have it out for the public so

that is something that you would need to

check every now and then so how do you

do it especially when it's office 365

when all of it is online how are you

going to stop anything of that sort from

happening we would not want users to do

something of that sort but the problem

is when it comes to systems that are on

the cloud the variables that are

involved are quite exhaustive and

unpredictable as well so if you're

talking about a identity access

management system like Active Directory

and on from my system essentially you

would be able to be in complete control

of the entire file integrity you would

have systems to tell you who is

accessing what what's happening or is

there any suspicious access is there any

escalation of privilege and all of that

but what about cloud do we have the

know-how that is essential to prevent

all this so it all starts with people

with privileged access and them being

probably this disgruntle or have a bad

and at times you should also consider

the fact that bringing in new employees

are probably a temporary workforce of

contract employees or service providers

or giving them access to your network

can at times to try a turn out to be the

problem so the first thing that a

outsider would try to do is probably

have a backdoor entry or leave a

backdoor entry when they get the chance

so they try to get hold of some vital

information that could be useful for

their business or it could even bring

your business down we need to take that

into consideration the kind of

information that gets lost usually is

confidential information which is very

obvious

it could be financials it could be data

pertaining to your customers probably

that's a very big problem and the worst

one would be employee data details of

bank accounts details of credit card

details like Social Security number all

that gets lost and this is just one side

of things - how information gets lost

what about organization that deals with

healthcare what about health records of

people that again is a very very big

problem in fact much to my surprise I

recently stumbled upon an article and

understood that the personally

identifiable information is details like

your name your telephone number your

email ID and other basic details get

sold for about two three dollars in the

black market or the dark web as they

call it but your health record the one

that has your details put in to your

insurance insured or what medical

history you have and all that gets sold

up to $50 per user record on the dark

web so how disturbing is that so there

are quite a lot of motivation and

attacker would have beat insider or the

next external attacker they have a lot

of motivation because there's a lot of

money associated with it we need to be

very very sure that all intellectual

property in the organization like trade

secrets or probably product design

statements all of them are number one

secured and number two monitored and

tracked for access at every point in

time so you will need to have processes

that intimate you when someone's trying

to add

a specific intellectual property you

will need to have in fact workflows or I

would say an approval mechanism if it's

highly confidential and critical someone

needs to give you approval to access

data that can very much be done and

privileged account information like

credentials and passwords should at no

point in time be saved as plain text so

I'll be talking or walking you through

quite a few options to stop all of this

and ensure that all best practices

required are in place for that we'll

start off by understanding what

essentially would an insider do it's

usually want to flood the organization

steal some important customer data and

this usually happens during the normal

working us because no one is really

going to notice they are already inside

the organization they have access to

customer data they very much can copy it

to a flashdrive or probably uploaded to

their cloud because there's no system to

monitor all of that so again there's a

problem they are already pre authorized

to do all of this and the thing is you

would not really be having a system to

monitor all of this and fraud becomes

absolutely easy so this doesn't also

require quite a lot of technical

knowledge it could very much be

transferred so that's one thing I t's a

potage is a problem of another level so

they try to get access to your system

they probably did not have access

earlier but then somehow sneaked in and

got some maxes or added themselves to

some administrator group and now they

want to bring the system down or

probably install a potentially malicious

system or a malware in the system and

gain access so when this happens they

are mostly not at work and they're

mostly not at work and operate this

whole scam probably in the middle of the

night when it's non-business Horstman

nobody would probably be looking that's

exactly when they pull an ID sabotage

where they'd have a malicious program

being installed in the network or get

the system down or crash it or cause a

denial of service basically to hinder

business basically to cause damage to

the reputation and quite a lot and the

last one is going to be theft of

intellectual property it usually happens

when it's time for an employee to leave

so I am recruited by a competitor I have

a job offer I have a 30-day notice

period to leave the organization so what

I also do have is access to all

corporate data why not have a provision

to send across all corporate data in

real time to a personal email ID even

after I leave my organization okay

that's something that I can't adjust

that's something that I would not want

an environment to be open to or

vulnerable to so we would need processes

that check if there are any unnecessary

access or modifications to mailbox

settings or if there are any forwarding

that are set to personal email accounts

or the ones that are not a part of the

domain we will need that as well and for

this again they'll need to have a bit of

technical expertise what they do is

probably try and share trade secrets and

most of the times when they're doing it

they're authorized and this can very

much happen during normal working us

because nobody is going to check for the

changes that are happening right here so

you'd need to have an upper hand

basically by understanding attackers

mindset so that's where it all starts so

for you to detect easy things that you

can probably look into is access during

non-working horse beyond business horse

access or modification of data for which

they are not supposed to be messing with

you need to have a provision to track

that and the last one is a very useful

functionality from office 365 which is

mailbox content search so you have

certain key words you have certain

intellectual you have a patent let's say

you have a patent so you would not want

any of that document being attached or

shared either expectedly or unexpectedly

so what you could probably do is set the

mailbox content search to work your way

let you know if there's something of

that sort data containing personal

information or patron corporate identity

or some intellectual property being

shared attached or copied you get an

immediate

if it's happening over the office 365

mailing system we'd be looking into

these three aspects to start with we

will take a look at a report a straight

out of the box that the poll that is

going to give you access to logon

activity that's happening during

non-business hours so you will be able

to audit such activity I've got about

four five reports around auditing logon

activity I also have real-time reports

like quite a lot on business hours and

non-business arson what exactly they're

trying to pull off right here I'm going

to take a quick second and show you that

specific report so what we have right

here is a report for activities during

non-business horse here you go

I've got an out-of-the-box report that

is going to tell me and give me insights

into all those users who are accessing

from a specific IP all from a specific

device during non distance ours it gives

me a list of successful log ons it gives

me a list of failed logins and this is

going to be phenomenally helpful when I

am trying to go on and perform a root

cause analysis to check if someone's

being intruded into my data at the wrong

point in time so I can start off with a

very simple report accepting who's

logging in beyond business arts

straightforward report that's quite

helpful next one is going to be

unauthorized modification of data so I

can have out-of-the-box reports that

give me insights into how my onedrive is

being handled let's say this important

corporate data maybe patron documents in

my onedrive and then a specific set of

users who should be accessing it that's

okay I'm a user who has access to the

data but then I don't usually access at

many a times because that doesn't really

pertain to me but all of a sudden one

day I access the file a hundred times

that's a deviation in my usual behavior

then I probably perform some

modification on it on some critical

aspect of the file that again is a

deviation of behavior I've probably

copied it to a USB flash drive or I've

uploaded it to the cloud I would need

processes basically the admin

processes and systems to notify when

anything of this sort happens especially

when this is happening with an external

user you would need to be all the more

vigilant and all the more careful and

try and stop this so we're talking about

unauthorized modification of data and

having a provision to keep tab on all of

that and get real-time alerts when

something's going wrong you'd get a mail

you'd get a push notification get a text

notification you can even configure an

alarm to go on your phone when something

of this sort happens you'd get notified

the next one is the content search

functionality that comes with office 365

this is already available for you you

can go on configure the content search

key in those important keywords that you

don't want your users to be sharing over

an email it could be on the subject it

could be on the body you would get

notified and in fact you could do a

search to check if someone's already

done it you could do it two way but what

we've observed is this functionality is

quite restricted and it's rudimentary in

terms of its functionality and the reach

that it's got so what we've done is

we've kind of topped it up with a few

more functionalities from manage engine

we call it the advanced office 365

mailbox content search we've included a

provision for having a condition based

search so you can have predefined

conditions you can check for specific

set of users especially let's say users

pertaining to an administrative group

you can very much keep track of them and

means they're being sent and received

and check for any specific keywords

essentially passwords and credentials

should not be shared over email that's

something that you can look into and

again you can train the system to work

in your favor

with the pattern based search that's

available when someone's trying to

attach a file with PII or when someone's

trying to attach a file that's called

credit card information let's say or

when someone's trying to attach a file

that has information pertaining to an

organisation's confidential data that

has a specific pattern maybe numbers

maybe algorithms maybe code may be quite

a lot of different

additions and combinations that are

available on which you can train the

solution to look into and when that

specific word or pattern or string gets

used or something similar that also gets

used in an email or appears in an email

and in the subject or in the body you

get an instant notification what's best

is the functionality that lets you

automate the whole thing so you can

schedule it to run probably every half

an hour or probably once in a day if you

trust your users and then get notified

if there's some anomalous not expected

activity going on so this is very simple

this is very straightforward but when it

has the functionality to be automated

and then it has the functionality to be

pattern based it becomes all the more

simple for organizations to go on and

pinpoint if something from where it all

started root cause analysis is going to

be quite easy in this specific format so

how do you tackle all this in the first

place you get the privileged management

done right that's the whole deal so the

right users lead write accesses you

necessarily need to have an user

activity monitoring solution in place a

UAM that's what we say a UAM to check if

it's a suspicious event or a normal

activity you would need to also look

into these signs of compromise let's say

one common sign of compromise is the

user being continuously locked out of

their account or them receiving a mail

for a password reset so these are

essentially how it starts and again when

we are talking about Wow let me let me

let me get to this case I've got a cool

question from Jason as a school we would

like to be able to see if there are

files containing malicious content yes

that is a wonderful case you dream us be

able to do that Jason quickly getting

back to the topic that we will

discussing a while back this is quite

helpful for you to prevent a cyber

bullying case the product would be able

to look into hate words

slander terms in the body of the mail or

probably other collaboration

applications that the students are using

since its office 365 many education

institutions are using it and the

product can very much help you stop

cyberbullying or reduce the extent of

cyberbullying thank you so much for the

question Jason there are quite a lot of

cases not necessarily at enterprise

level but also even at a school at an

educational institution you might as

well use this and so the question so

well forward we're talking about cases

of account compromised here we're

talking about a specific set of things

that you can look out for if there is

any unusual change in the name of the

user probably the password gets changed

or there's a request for password

changing or another critical thing that

you should be looking out for is

changing in the mail forwarding rules so

if there is anything suspicious

happening in the mail forwarding loose

any activity that points to the user's

mail forwarding including an external

email id that's something that you

should note you could interview should

have your users educated basically tell

them what signs to look for and then go

on and immediately act upon them so

these are basic signs unusual account

logins from a different IP address so in

fact we are working on a current module

called the user behavior analytics

module and this module is going to

essentially help you administrators to

use a machine learning power algorithm

to check how a user interacts with your

office 365 target system so when a user

deviates from the existing behavior it

could be basically because they are

operating from a different geography

that could be a case it could be because

they are operating from a device that is

not registered in your system it could

basically be because of IP address that

has a bad reputation score so we've got

quite a few parameters against which we

peg a user every single time when they

are logging in and when the risk profile

that we drew off shoots the baseline you

get a notification and

you probably would need to authenticate

yourself once more through the

multi-factor authentication algorithm

that will kick in so we are talking

about an intelligent system to help you

secure your office 365 environment and

in this case it's going to be a lot more

sensible preventing any possible false

positives coming in many times the

problem is you have a system that is

condition based all it does is something

is violating the condition it just keeps

you giving out false positives but sure

what we're talking about is an

intelligent system that drafts a user

behavior and profiles every single users

action based on historical data and then

it goes on to give you an alert so this

is a lot more informed decision that we

are talking about in fact in this case

account logins there could be quite a

few employees who are traveling warrior

who are on the go or remote employees or

belong to the sales department and they

are required to go on site to go to a

different geographical location so at

that point in time the system already

knows that they have said the pattern or

a set trend of them traveling and you

don't really get a false positive at

that point in time so we're talking

about two things making it more usable

for the users and at the same time

keeping it secure for the organization

so that's one thing that you can look

into and the next one is the altered

email settings so if there is any

additional changes to the inbox or

outbox forwarding rules that you should

be noting if there are any unauthorized

access from devices that are not there

in your list of devices that are

attached to your system you should get

notified and you should have a process

and that's going to be available so we

call it device footprint things so if

there's any deviation you'd get notified

there as well and most of the times this

is the easiest pointer to find if

someone gets this message saying that

they are locked out of the account quite

frequently that means someone else is

trying to access their account probably

they fail multiple times with a bad

login and the account got locked out so

that's one sign that you could look out

for but what could be all the more

better is to have a dashboard it's

called the secure score dashboard okay

what am

do is I'm going to quickly share the

link to you on chat right now this is

quite an effective dashboard for you to

make use of essentially when you are

trying to evaluate your existing

security in your organization the score

is absolutely free you can derive your

own score so I'm going to quickly ask

you to access this link I'm pretty sure

you're connected to your office 365

right now quickly access this dashboard

and tell me what is your score I have a

pathetic school my score is 51 but I'll

tell you why and how to increase the

score in a while let's see who's got the

highest score today

oK we've got Steve who's got a hundred

twenty-eight that's good that's good

that's a good start

Raj says he's got a 215 okay that's the

highest so far

what's your secure score let's see who's

got the highest secure score the link is

absolutely available for everybody to

access if you are already on your office

365 set up this is from Microsoft and

you'd be able to use it if you have not

used it before please do right now and

tell me your secure score let's let's go

about making your secure score better

all right mark has the highest so far he

says he's got a 312 Wow that is a huge

leap from the previous people I mean

that's that's a good score mark I think

mark stands to be the clear winner right

now but what about me I have a pathetic

score and why is that there are quite a

lot of actions that are pending from my

side I will need to do a lot more to

increase my secure score so this

dashboard

gives me a real-time see through into

how my organization is structured with

respect to basic things it could be

something as simple as enabling

multi-factor authentication it could be

something as simple as turning on

Auditing it could be something as simple

as having password hash sync in place

quite a lot when you're in an hybrid

environment you would want to consider

password hash Jeff says he's got 83 no

problem Jeff this is gonna be quite easy

and straightforward what you could do is

you could get into this dashboard all

right you have very easy action items to

do it would take you probably one days

time to do all these action items or

enable most of them it's going to be

very easy and for it to reflect it takes

about 24 hours and you'd be having a

very clear-cut picture as to where you

currently stand and how you've improved

in fact Microsoft goes on to give you

how you're securing your organization by

enabling that specific requirement and

what compliance requirements are you

meeting by doing so this is exactly what

someone would

it makes it easy for every users and

blocking jailbroken devices are routed

mobile devices so there could be

potential entrance or entry points for

an attacker jailbroken device or a

rooted mobile device they have con

control and that could possibly be the

reason of a potential malware entry or

probably the event on to install some

apk file on their Android device that

was routed and that instead that got a

mile away splitting across the

organization lots and lots of cases very

easy to do this go for it figure out

what's your secure score and as a

practice come back to your secure score

dashboard once in a month assess your

existing standard check if there are any

new action items that you can do and

it's quite easy to do and keep improving

your secure school and then after a

point once you have like a really cool

secure score you can be very sure that

your organization's Office 365 is a lot

more secure so why exactly are we

discussing this we'd want to keep a

potential insider or probably someone

who had a malicious instance on check

and number two we do not want any user

to accidentally cause damage to the

organization someone has a rooted device

you do not know that could be the reason

for your entire network coming down who

do you want that not necessarily simple

is to use the secure score dashboard

going beyond I've given you ways to

detect I've given you ways to secure

your organization now the last step is

going to be just in case if something

bad went down how do you react to it how

do you retaliate how do you minimize the

damage damage control is what we're

going to be talking about right now and

I have five points for you we start off

with something as simple as password

resets go on and do an organization-wide

password reset alright and in fact I'd

ask you to set random passwords for

users and have them notified personally

do that it's going to be quite an effort

but if you do it through the tool it's

going to be quite easy

select all the users have them notified

on their mobile phones with your new

password you can do that or have them

personally the email you could do that

as well

random passwords are going to help you

stop compromised accounts so that's

something that is very fundamental but

can help you big time and again enabling

multi-factor authentication if you

remember on the secure score dashboard

enabling multi-factor authentication was

an action item please do that enforcing

multi-factor authentication on users is

going to be quite easy and in fact

Microsoft makes it very very easy for

you to enable MFA you can have the

Microsoft Authenticator app installed on

your users device it works with touch ID

it works with face recognition how easy

could it get this is this is quite

simple it's not going to be complicated

for the users as well and they'd not

have a problem doing this so please go

on and reset passwords and enable

multi-factor authentication as the first

first aid measure all right the next one

is to quickly check if there are any

unnecessary delegations on the mailbox

that's something that an Insider would

be doing if they want to exfiltrate data

if they want to do an espionage this is

what they do do check for any malicious

delegations check for permissions in the

tool lets you quickly go through all

delegations and also from the report

from the same dashboard you'd be able to

modify permissions if there are any

unnecessary permissions right there all

right the next one is to remove

suspicious mail forwarding that you

could do very easily

you can check if there are any external

forwarding addresses the tool has a

dedicated report to check if there are

any external forwarding addresses that's

a quite a useful functionality that's

most of the time the reason for data

being lost and when an Insider is

planning to leave the organization

they'd set forwarding to their personal

personal email address that you could

very much stop so there are quite a lot

of extensive reports that come pre built

into the product and one such report is

mailboxes with external mail forwarding

I'm gonna show you the dashboard right

here here you go I have a mailbox with

external email forwarding report and it

gives me all those users with external

forwarding set and it works across

domains since the tool is capable of

managing

multiple tenants and multiple domains it

is going to be effective for you to get

all of those information under one

single console straightforward that's

what we are talking about just a second

just a second getting back to the

presentation so we were talking about

removing any suspicious mail forwarding

rules that are set just one second a

PowerPoint deck hung all right perfect

okay go the next one is going to be a

prohibition to go beyond the native

limitation what is again the native

limitation a quick question for you

how long can you office 365 save your

audit logs that's a quick question for

you how long by default does your

Microsoft Office 365 save your audit

logs let's see who gets the answer right

Mario says it's 120 days that's almost

close that's almost close jason says

it's 90 days okay 90 days does anybody

have another answer Mario says it's 120

days it's almost close jason says it's

90 days and the answer is 90 days Jason

got it right so three months of audit

logs is that going to be good enough is

your auditor going to be happy with that

data or will you even be able to do any

proper root-cause analysis if the FN

attack went on because many a times for

an organization to detect that they

underwent an attack it takes up to four

or five months after the damage is made

coming back and checking to have no

other data snot something that is

appreciated so what you could do is you

could make use of the tool and extend it

however long you want very simple

extended for a year

in fact I'd recommend doing it for 13

months that helps in most of the

auditing cycles go on have it for 500

days

that's quite a useful bit of audit logs

being archived and the best part is the

whole thing gets archived it gets

password-protected and also you could

very well get into the system and check

any time for any critical activity going

on around the account or derive any

insights from the audit logs that are

available or get reports because the

product lets you do that audit logs

check for reports exhaustive set of

reports around compliance around

security around onedrive licensing quite

a lot that you could use off and set

real-time alerts for any changes that

are happening so if there is any

activity happening on your Active

Directory like some admin level role

changes or some group membership

modification happens any privilege

escalation essentially gets reported and

alerted right here it tells you based on

the level of criticality you would get

hold of any intruder trying to access

your file and folder system or any

insider trying to unnecessarily modify

any data so someone deleted an important

file intending to disrupt business you

get a notification right here you got

all of that right here so what I would

recommend you to do is to get back to

your environments start off with the

secure score dashboard that's the

easiest one to do ensure that you have

all these items on the checklist in

place and get back to me tell me how

your secure score improved and I'd like

to be by your side when you do this

right because we have this solution that

essentially empowers administrators and

we'd like to interact with you to

understand what specific challenges that

you're facing and see if we could

possibly