OMEGA SECURITY

Omega Security Findings

Business Confidential

Date : 8/10/2024
Project: 123-45
Version: 1.0

OMEGA SECURITY

TABLE OF CONTENTS

Confidentiality Statement -

Omega Security operates on an above board security based platform that ethically penetrates known organizations for many purposes including Governance, Risk, Compliance, etc. When authorized to do so we operate with the understanding that all information & data that has been collected during the penetration test will be held under confidential highly secure documentation to keep peace of mind for customers. All informational databases that we use follow NIST regulations and are consecutively checked by third party companies to confirm the validity of our security. All information gathered will not be publicly disclosed, following that it will only be disclosed to personnel that the customer sees fit to handle confidential information/data. All of this requires close care and consideration when dealing with any company, since we value customer satisfaction above all we only intend to remediate and give solutions as soon as possible with any information gathered.

Disclaimer -

Although we do our utmost at Omega Security to keep information secure and to never disclose information and data found during penetration tests (within lawful parameters); We are still bound by U.S. law. Under the circumstance of specific

information and data found we must still make certain judgment calls when it comes to reporting information to public response agencies that the U.S. Government is in action to pursue types of illegal activities.

Keep in mind when hiring Omega Security that any information that crosses lawful and moral obligation to upholding a strictly run and law abiding business will not be tolerated, and will instantly be reported to local Government agencies and is no longer under our jurisdiction of Omega Security to secure this kind of information.

Contact Information -

U.S. Locations -

- California, Los Angeles, 90014, 822 W.8th St. , 1-800-999-9999.
- New York, New York, 10011, 856 N. Ave., 1-800-998-9998
- FL, Miami, 33101, 1942 Pineapple Lane, 1-800-996-9992
- FL, Fort Myers, 59027, 7590 Omni Lane, 1-800-877-8989

EU / Australian Locations on Website

Assessment Overview -

Omega Security has a standard and thorough practice that we continue to tighten and further build upon over the years. Once given approval we operate in multiple areas of service to give our customer their most insightful outcome of valid security options for their personal needs.

We operate in 5 different regions including finding general severity of needs based off customers scope of operations, then once scope and severity is determined we continue to prong for gaps in security which we can determine as areas of vulnerability, then leading to 2 major components is said companies current daily strengths and weaknesses, as most of said companies need a description and formal presentation for C - Suite employees we offer specific guidance and reasoning for any kinds of changes to current security that we find necessary, then finally we then give a deductive reasoning of what the external penetration test found and how the ideas we have to implement new changes in security will find answers for multiple current issues involving data loss, encryption issues, employee awareness, not enough SIEM in place to see multiple avenues that bad actors come from, etc.

We operate in a quick and efficient fashion, attempting to give the clearest and digestible answers for quick security solutions potentially saving millions of dollars in court fees, data loss, overhead operation cost, software fees, etc.

To add the icing to the cake we will make sure that your business has the current needed levels of compliance to follow GRC standards in your area, leaving you completely free and clear of making issues in compliance to state and government laws.

Assessment Components -

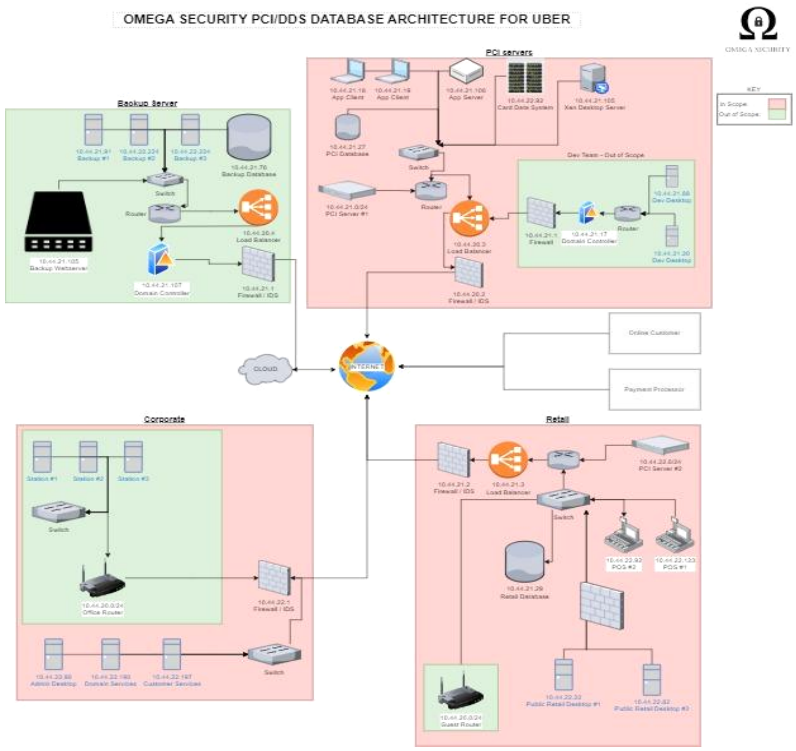
- ***External Penetration Test***
- ***Determining Severity***
- ***Defining what's in scope***
- ***Understanding budget needs if applicable***
- ***Executive Summary***
- ***Strengths / Weakness'***
- ***Vulnerability***
- ***External Penetration Test findings***
- ***Solution Implementation***

Finding Severity Ratings -

General consensus and analysis of Uber since its inception shows that its largest security issue has always been data breaches. More recently even they had a cyber attack happen through multiple employees during a social engineering campaign. Overall its the vast amount of information that Uber has access to from the public that makes it enticing for bad actors, but also very dangerous to hold on to when there is not proper security protocols being followed.

Omega Security has found that unfortunately many of the situations that have happened in the past have been preventable with a change to employee interaction with information. This deems the severity rating at **Medium** level, with these changes being implemented to counteract the information / data leak caused by employees in a timely manner, most upfront security concerns will be handled.

Scope -



This is the Network outlay of an anonymous Uber location that we changed to fit implementation needs. Given the set up we can see it clearly defines the scope of the portions of the Network that we had

access to during the external penetration test. This location was the primary access point when it comes to the location targeted during this external penetration test. We had to have an idea of what the general network outlay of Uber consists of, and with direct contact with Uber we were given this location as a prime example of how business networking should work once Omega Security implementations have been applied (We used Retail as a way to describe the general physical locations that Uber has spread across the country).

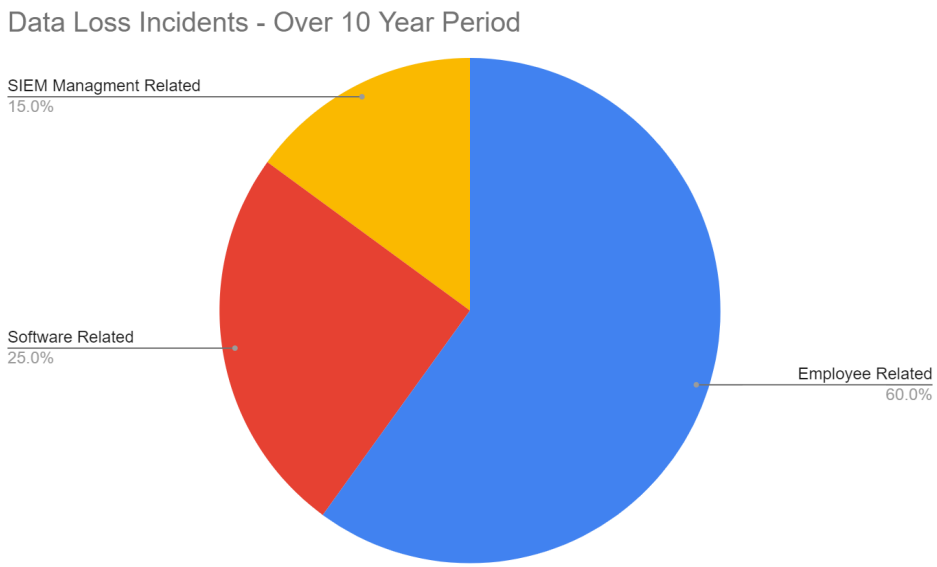
Executive Summary -

- **Security Findings Summary**

  Omega Security has found that although Uber is well rounded, one of their main flaws is the employees interaction with important information/data that customers in all confidence share. This puts distrust in the day to day customer that finds themself in a situation to use transportation, and may find themselves looking for alternative methods of travel due to past history of information/data leaks within Uber Headquarters, to mobile Uber workers getting breached while on the go. Overall employee interaction with information

has always had a huge effect on the company itself, even during events when there may have been a bad actor gaining information when stored on the cloud via third party (this mishap was in 2016), the employee interaction with this altercation was CISO attempting to cover his tracks of the mishap was adamantly fired and eventually brought before court to answer for the severe breach in information/data of 57 million customers. We are trying to avoid having any future incidents within

-This chart gives the general vision of the incidents that have led to leaking of information/data of customers/users -



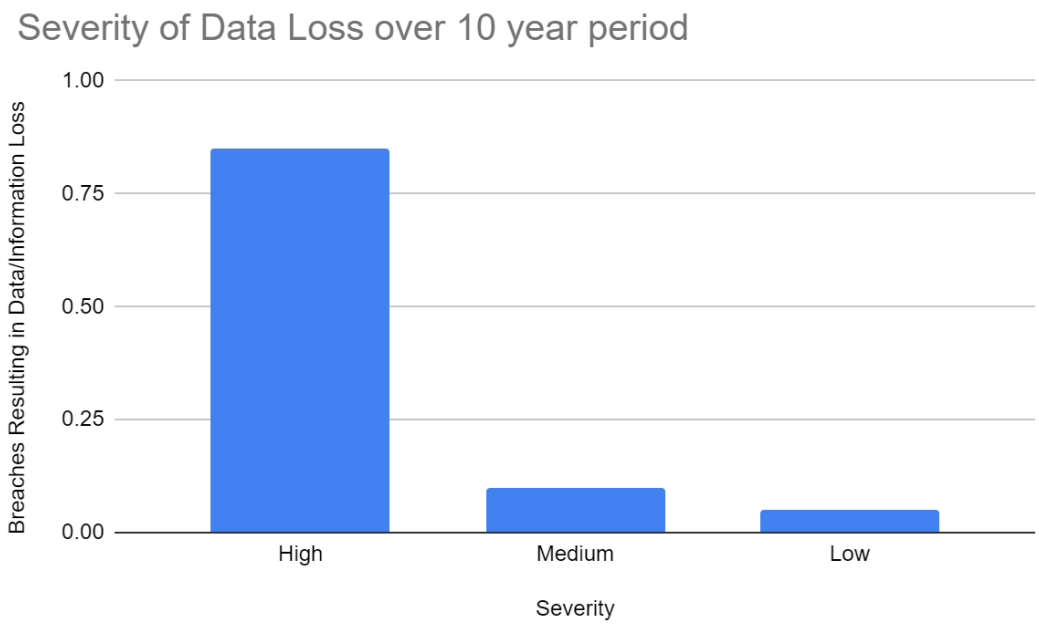
- **Solutions / Attack Summary**

Utilize Netcat, SSH, Brute Force entry etc. we have found that overall Uber has tight security when it comes to being able to extract data & breach during most scenarios. What we find is lack of training and awareness. We find employees giving out information to simply stop the constant berating of messages (2016 incident), or allow access because of emails that seem to be from a friendly employee of the company when they are truly a bad actor looking to get access to important financial information or to get access to passwords and username information

The general solution is highly trained individuals being dispersed to each branch location to train employees to operate with discretion when it comes to handling customer data/information. Also we would implement smaller key features such as highly advanced password options, mandatory restarts for systems to keep updated, very tight monitoring of individuals that have root level access to highly confidential information, heavily encrypted password directory files, constant monitoring of users, heavily engaged SIEM monitoring employees, improvements to current SIEM software, utilization of honey pots, transitioning network setup to enforce security

for traveling employees, lastly is to implement network structures at all static locations and virtual locations to have traffic heavily monitored through the use of Switches and Routers that tie directly into the Operating Systems that have personal/financial information onboard that we are trying to protect and secure.

Many of these solutions must be implemented ASAP due to the severity of the losses that Uber has faced over the last 10 years, here is a chart showing the severity & percentage of event severity that has taken place over the last 10 year period. The Y axis is the percentage of Breaches Resulting in Data/Information Loss.



Security Strengths -

After thorough evaluation of our team we can find that the amount of gaps in security for Uber are very few. In an attempt to gather information from Netcat, SSH, simple asset discovery all finds that there are not many open pockets in security that can be taken advantage of. They have a great setup for online security, and overall have good hashing algorithms for their customers personal/financial information and data that's stored via cloud.

Security Weaknesses -

Uber's largest weakness is in the physical locations, and in the employees especially when traveling abroad, and lastly in the upkeep and circulation of new usernames and passwords for the static locations and networks used at these locations. Some of the best implementations of security need to be on an individual level for employees, and an networking level for the physical locations where data/information of customers is stored. This is highly vital for the continuation of Uber because when the public sees that their personal information is not

safe with a company, the pattern we see is massive financial losses for that company.

Vulnerability by Impact -

Vulnerability for Uber comes from multiple different sources, though keep in mind as previously mentioned these aren't all going to be pressing matters in the overall broad view of company security.

Foremost with just a little online investigation we can find answers to questions like how many different APIs Uber uses (this is important because application platforms thats Uber uses are heavily tied into what kind of process needed to take advantage of these API’s, and with simple google searches we can find these answers), you can use google or Linux to find lists of IP addresses that Uber uses, also easily find who hosts Uber’s DNS (Domain Name Server). The risk of having public information so readily available is that processes done by bad actors always start with gathering information and doing recon, while not all recon gives valuable information, it gives insight to a company's potential weak points which in turn gives more ammunition for potential bad actors. There are even more resources out there for Uber recon such as finding publicly known email addresses for employees, what kind of naming process they use for Active Directory Domain accounts, and many more public resources.

All these examples are known resources used by bad actors to gain access to information/data. Though there are more pressing issues that could be addressed that are beyond even employee/networking issues such as gaining access to AWS servers (since Uber like many business' use AWS), gaining unauthorized access to firewall through brute force entry or even through recon work done about current firewall versions used, access to VPN (which has been an issue for Uber back in the 2016 incident), and this one isn't as pressing of an issue but if a bad actor was to find the encryption practices found for Uber that could open up so much potential for information/data to be leaked.

External Penetration Test Findings -

Uber has a strong security when looking at the level of basic recon from bad actors, when getting to levels such as using Nessus these outcomes can change due to the level of data/information you can receive from using a purchased service.

Overall Uber has the biggest weakness residing in the employees of the company, and not being able to properly secure VPN connections when employees are working away from a static location. Most of these concerns can be addressed from proper training to handle outside threats when attempting phishing and to train employees to look through users constantly while

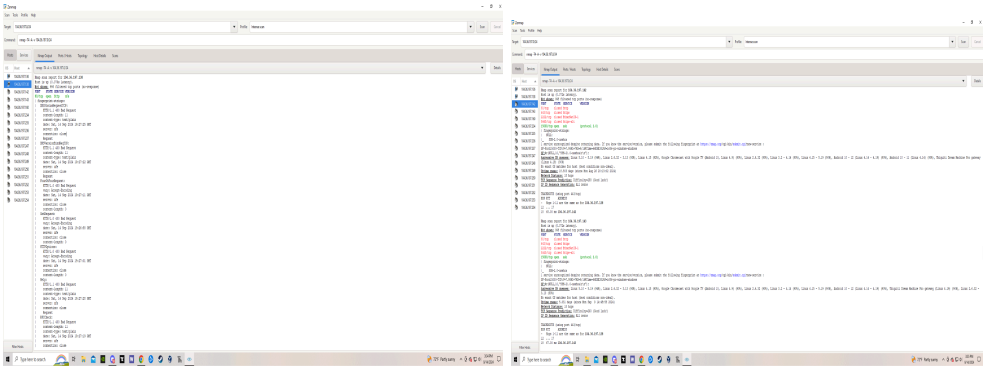
becoming comfortable with thorough investigation of what users are interacting with sensitive and important data.

We also found that Uber has Insufficient records when it comes to Lookout Compliant Policy that holds all businesses in contempt with laws and regulations of records with public data/information and private data/information. Due to there only being a few minor adjustments to being made (records of documents/files of private/public data dating back only 2 years, instead of 3), this is a small issue to fix, and again falls back unto the employees of Uber being trained properly.

This is an example of an Intense Nmap scan on U.S IP address 104.36.197.0/24.

This shows how available information is to find, and with a free application we found 256 hosts, 17 active and scanned.

(There is a ton of pages so just putting a couple screenshots)



Bibliography -

- **Dark Reading, 2024, London.**

  https://www.darkreading.com/cyberattacks-data-breaches/uber-breached-again-attackers-compromise-third-party-cloud

- **UpGuard, 2024, UpGuard Inc.**

  https://www.upguard.com/blog/what-caused-the-uber-data-breach

- **United States Attorneys Office, NDCA, 2024, San Francisco.**

  https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach