



PERCONA
LIVEONLINE
MAY 12 - 13th
2021

OSINT - Do you really know what
data you're leaking?

Hello!

I am David Busby

Information Security Architect @ Percona LLC

@icleus 

@oneiroi  



Precepts

Let's jump right in and set expectations for this talk.

Precepts

This talk is

- Not a comprehensive list on personal safety.
- Not a guide on how to stalk someone.
 - Seriously do not stalk people!
- Full of memes ...
 - Ok I maybe it is ...
- Draws on many, many, many, etc. others' research, without which this talk would not be possible.

Terminology

Let's define some of the acronyms we'll be using.



Terminology

OSINT

Open Source Intelligence

OPSEC

Operational Security

PERSEC

Personal Security

COMSEC

Communication Security

INFOSEC

Information Security

Importance

Let's define why these topics are important.



Homicide Offender vs. Victim demographics

View by: **#** %

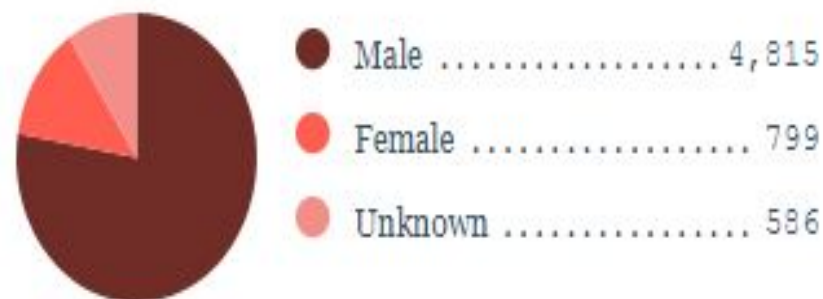
Sex

Race

Ethnicity

Age

Offender Sex

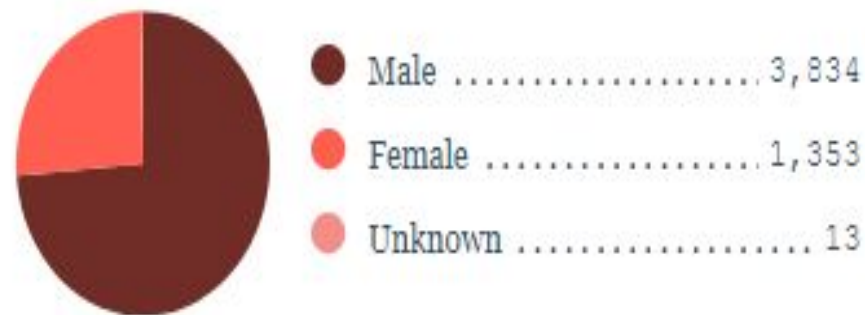


Offenders w/ reported sex

6,200

 Download

Victim Sex



Victims w/ reported sex

5,200

 Download

Importance

Improving individual safety through awareness.

Using US Crimes Statistical Data ...

- Homicides
 - 77.7% Male offender
 - 12.8% Female offender
 - 73.7% Male victim
 - 26% Female victim
- Sexual Assault
 - 92.5% Male offender
 - 4.2% Female offender
 - 10.7% Male victim
 - 89.17% Female victim

Importance

Protection of human life should be everyone's first priority!

- This includes (but is not limited to):
 - Protection of quality of life.
 - Includes protection from abuse, fraud, malicious behaviours, malevolent threats, and threat actors.

bUt tHe sTaTs
aRe blaSed ...



Real Cases

Let's cover some examples of where data exposure has lead to concerning consequences.



Stalker used
corneal reflection to
locate female singer
...

Data exposure is a problem

- The [BBC reports](#): **Stalker 'found Japanese singer through reflection in her eyes'**
 - October 2019
 - Identified train station from corneal reflection
 - Used google street view to further confirm angle to station and approximate location.
- [2013 Academic Research Article](#)
 - Peer reviewed

a

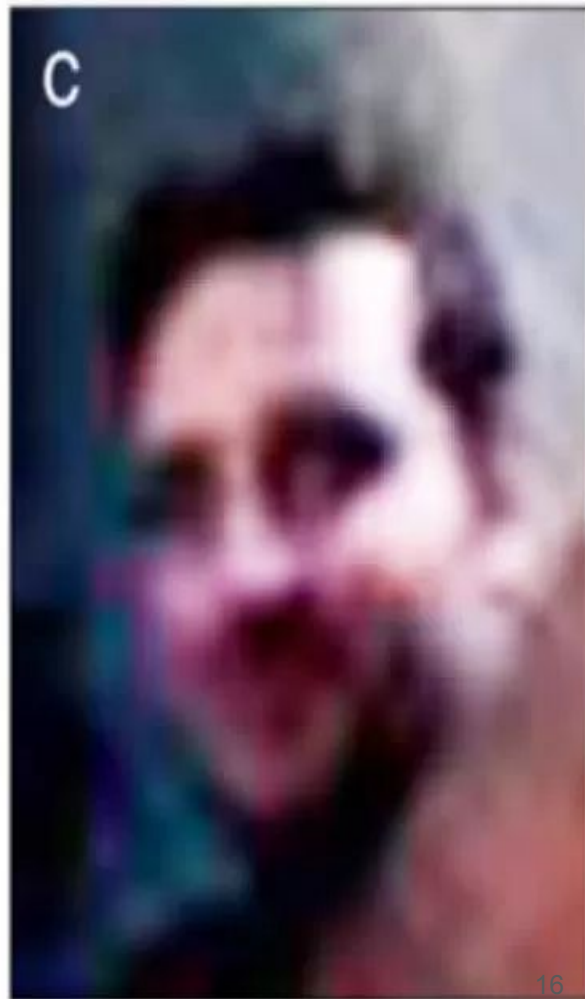
Zoom and
enhance ...



b



c



But it's still an edge case ... right ?!

- Alright let's not focus on corneal reflections, and instead focus on actual data in your images ...
- Images taken on modern devices will contain EXIF data:
 - Which may include:
 - GPS (inc. timestamp, elevation, lat:long, direction facing, etc...)
 - Date & time
 - Device type
 - and more

```
exiftool /Volumes/JetDrive/IMG_20160707_192748.jpg | egrep -i 'GPS|Software|Model'
```

```
GPS Date Stamp : 2016:07:07
```

```
GPS Altitude : Unknown (2)
```

```
GPS Longitude : West
```

```
GPS Latitude : North
```

```
GPS Time Stamp : 18:20:38
```

```
Camera Model Name : ONEPLUS A3003
```

```
Software : OnePlus3-user 6.0.1 MMB29M 4 dev-keys
```

```
GPS Altitude : 0 m Above Sea Level
```

```
GPS Date/Time : 2016:07:07 18:20:38Z
```

```
GPS Latitude : 32 deg 58' 3.12" N
```

```
GPS Longitude : 12 deg 40' 43.88" W
```

```
GPS Position : 62 deg 18' 7.61" N, 2 deg 40' 43.88" W
```

You should strip exif
data from images
before making them
public ...

What is wrong with you?!

Why are you even aware of this ?!?!

- By thinking like the “enemy”

- “I am your enemy, the first one you've ever had who was smarter than you. There is no teacher but the enemy. No one but the enemy will tell you what the enemy is going to do. No one but the enemy will ever teach you how to destroy and conquer. Only the enemy shows you where you are weak. Only the enemy tells you where he is strong. And the only rules of the game are what you can do to him and what you can stop him from doing to you. I am your enemy from now on. From now on I am your teacher. I will devise the strategy of your army, and you will learn to be quick and discover what tricks the enemy has for you. Remember, boy. From now on the enemy is more clever than you. From now on the enemy is stronger than you. From now on you are always about to lose.”
 - ” - Orson Scott, Ender’s Game
- “to defeat your enemy you must become your enemy”
 - - Sun Tzu, Art of War

Sun Tzu quotes and
CISSP talks are like
some unwritten rule

...

To know your enemy, you
must become your enemy.

Sun Tzu



There's also...

Yes, there is plenty more, so let's take a brief look at 802.11 standards and what they may be “leaking”.



Let's look at 802.11 ...

The amount of data we “leak” into our surroundings is concerning ...

Ever lost a bluetooth device? If only you could ...

- FIND IT (WITH ACCURACY) by looking at the Received Signal Strength Indication data
 - This is used in commercial products, such as Tile, Trackr.
 - Used by marketing agencies to track population density of an area, where patrons move throughout a shopping center.

Let's look at 802.11 ...

WiFi

Wireless beacons will broadcast every single wireless access point your device has ever connected to.

Commercial applications again look to capture this information (which is broadcasted in the clear).

Even \$gov
applications
collect this data ...



Wi-Fi data collection

We collect Wi-Fi connection data at this station to better understand journey patterns and improve our services

We will not identify individuals

You can opt out by turning off your device's Wi-Fi

For more information visit
tfl.gov.uk/wifi-data-collection

But wait ...

There's more ...



A little knowledge
can be a powerful
thing ...



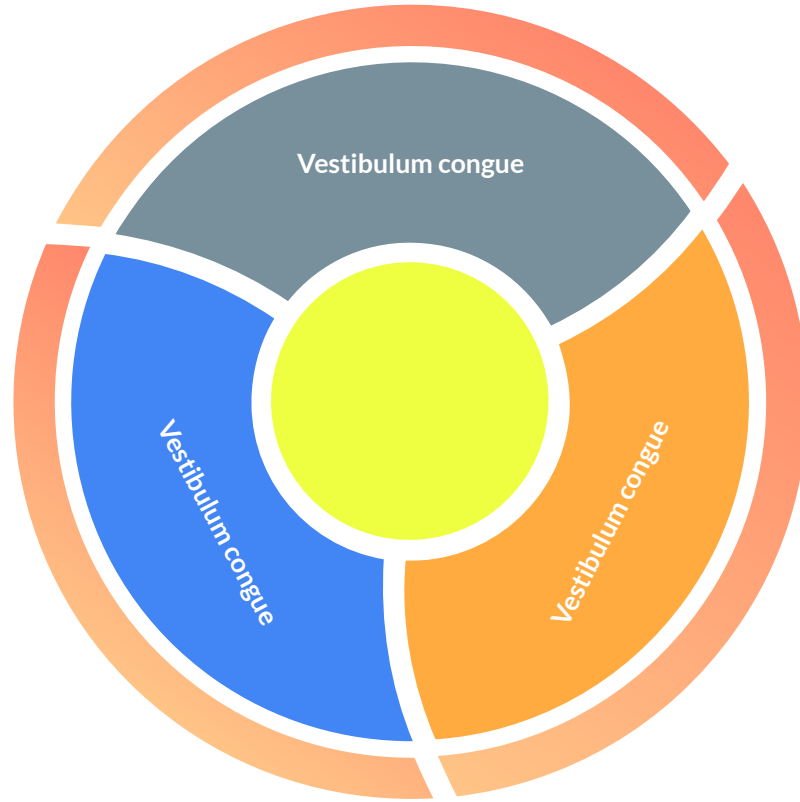
You're in control



You are in control of what data is leaking from your devices!

- Disable services when not required / not used
 - WiFi, Bluetooth (Saves battery too ...)
- Use a tunneling VPN service for “public wifi”
 - Encrypts traffic, makes interception more difficult
- Tailor your conversations for your surrounding audience.
 - Maybe you shouldn't discuss 2020, 2021 plans in a public setting.
- Trust BUT verify
 - You are all part of the “human firewall” at your organizations.

Use diagrams to
explain your
ideas



And tables to compare data

| | A | B | C |
|--------|-----------|-----------|-----------|
| Yellow | 10 | 20 | 7 |
| Blue | 30 | 15 | 10 |
| Orange | 5 | 24 | 16 |

Maps



89,526,124

Whoa! That's a big number, aren't you proud?



89,526,124\$

That's a lot of money



185,244 users

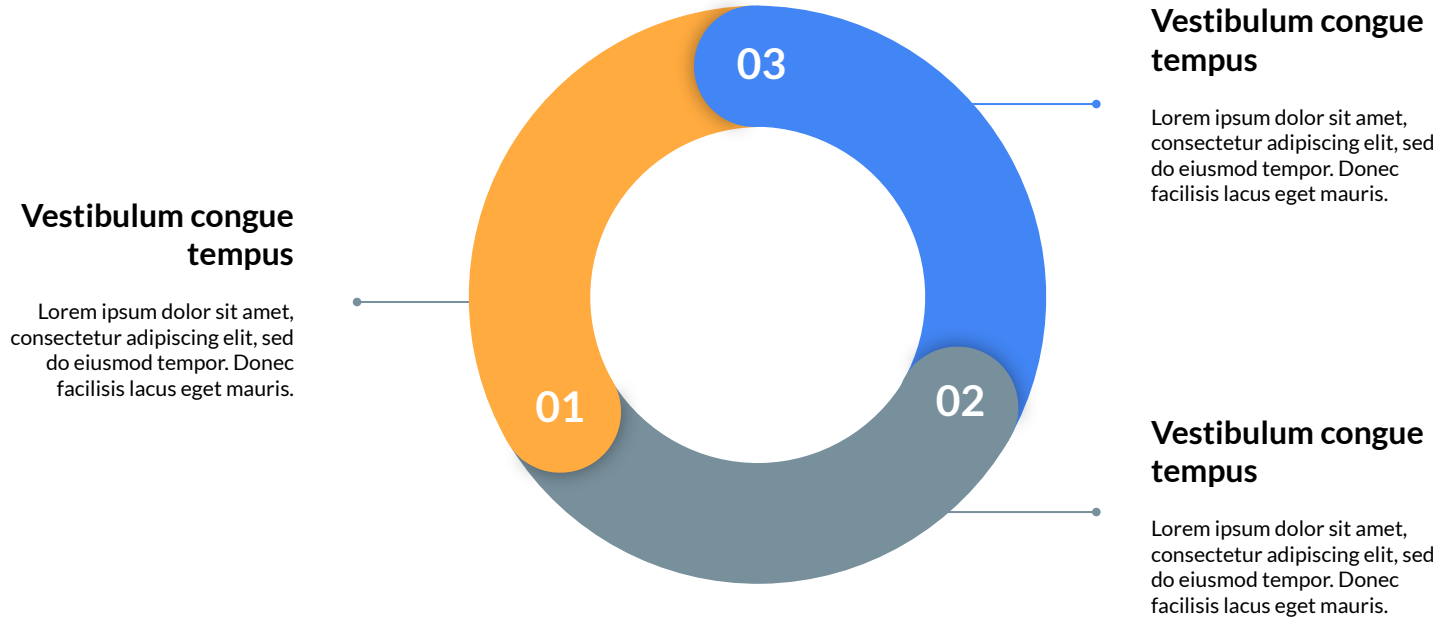
And a lot of users



100%

Total success!

Our process is easy



Let's review some concepts

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

Yellow

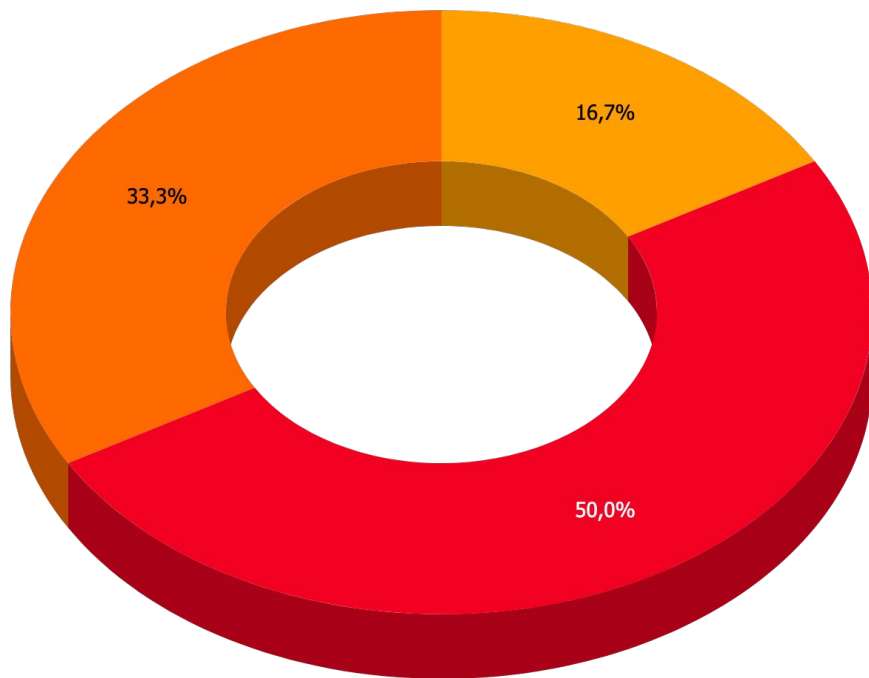
Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.



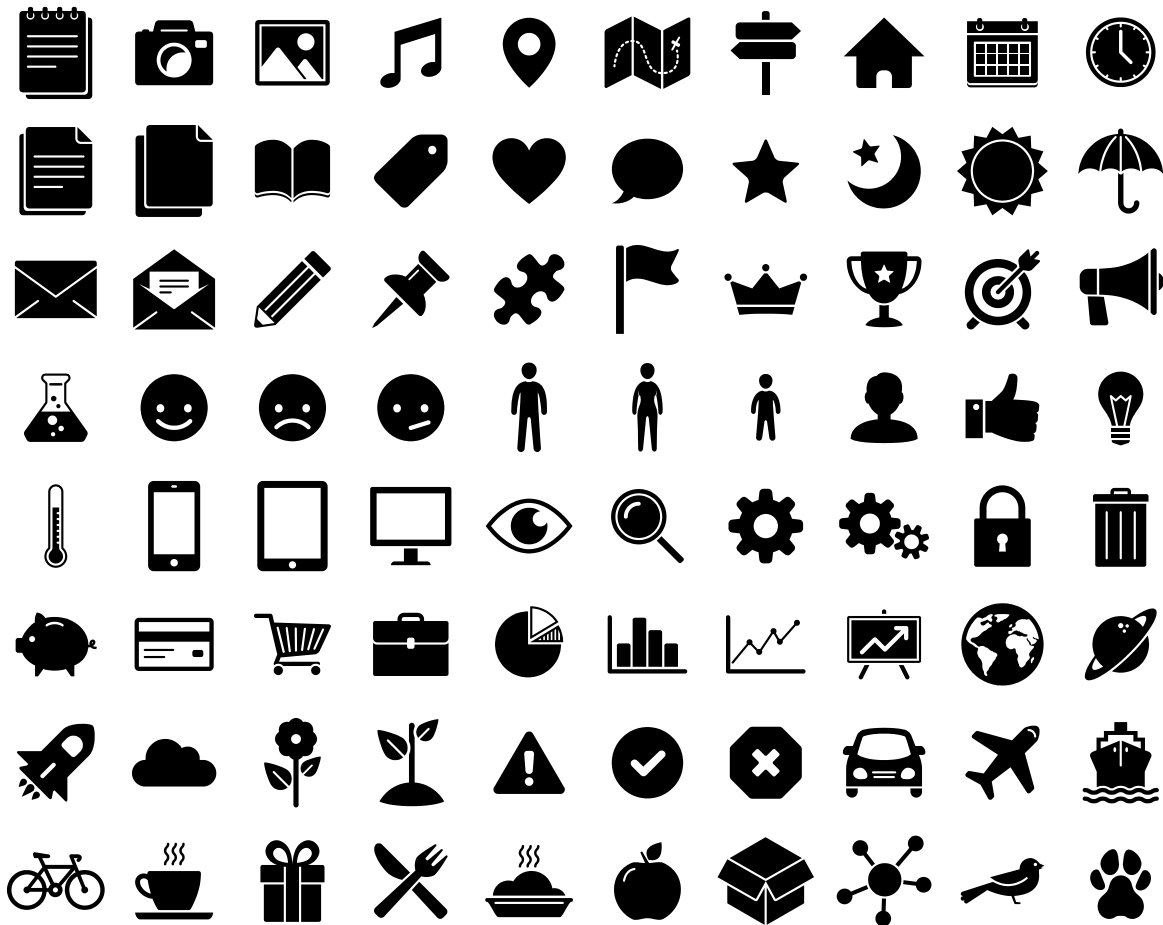
You can insert graphs from [Google Sheets](#)

Thanks!

Any questions?

You can find me at:

- david.busby@percona.com



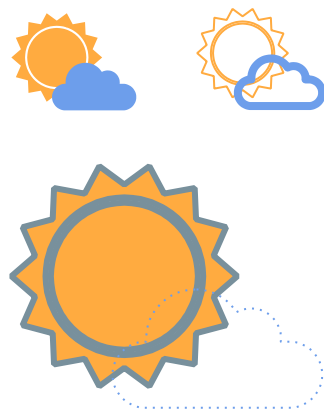
SlidesCarnival icons are editable shapes.

This means that you can:

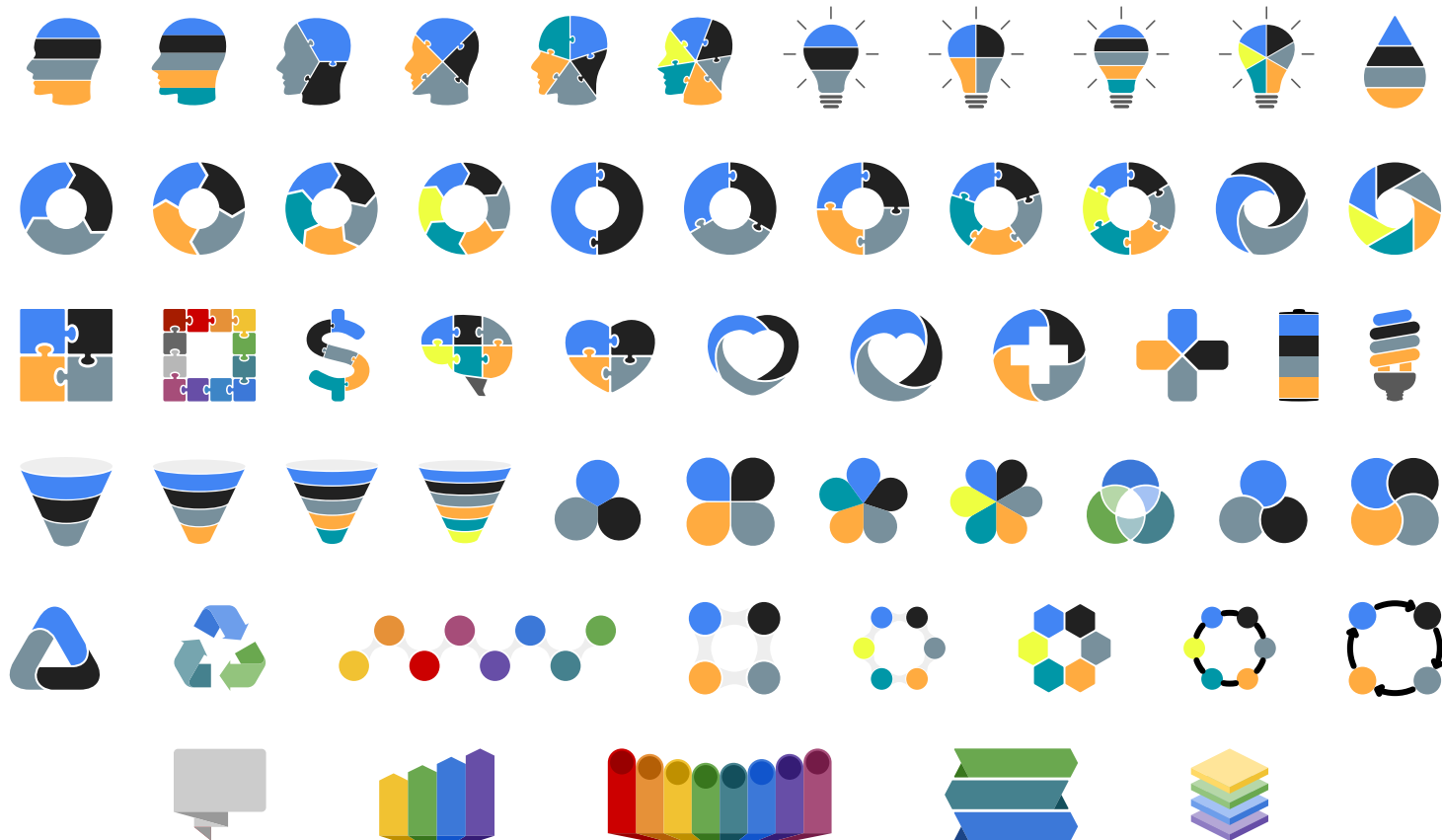
- Resize them without losing quality.
- Change fill color and opacity.
- Change line color, width and style.

Isn't that nice? :)

Examples:



Diagrams and infographics





THANK YOU !



PERCONA
LIVEONLINE
MAY 12 - 13th
2021