
Guillaume Malbrand | Sales Engineer
Romain Testu | Sales Engineering Manager
Matthias Maier | Product Marketing Director

# GUILLAUME MALBRAND

Sales Engineer
Splunk France

splunk> .conf18

# ROMAIN TESTU

Sales Engineering Manager
Splunk France

# MATTHIAS MAIER

Director, Product Marketing - Security
Splunk EMEA

splunk> .conf18

# What is the Lord of the SOC Dashboard?

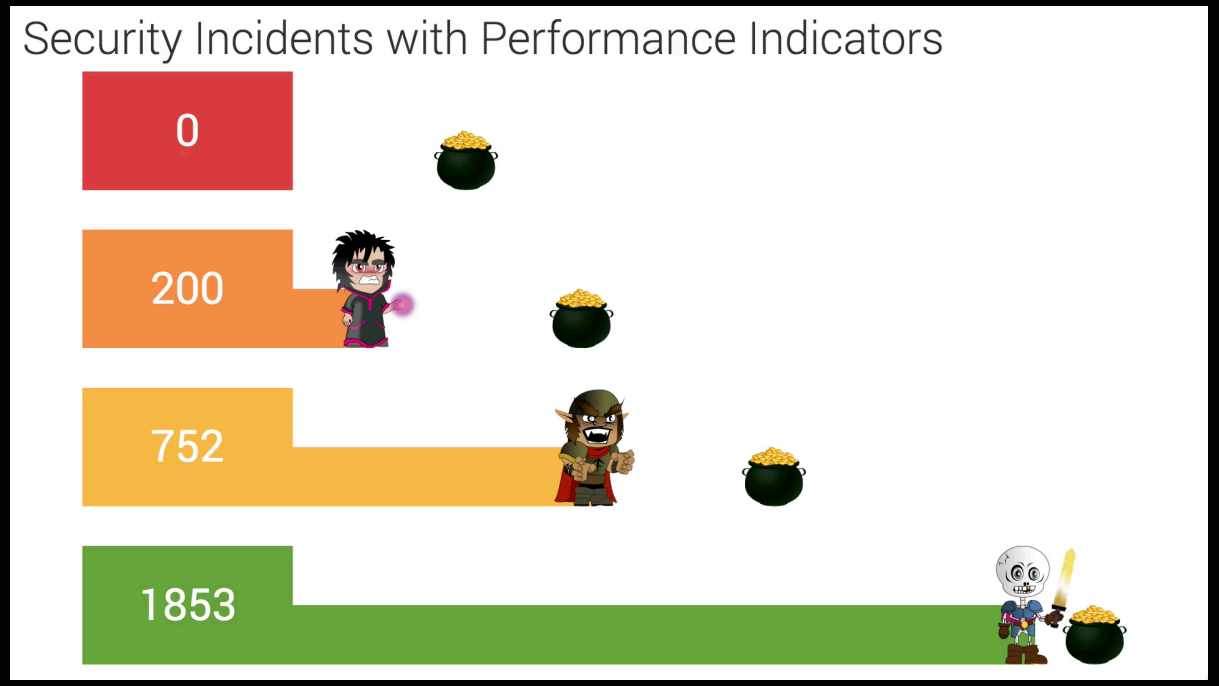
**Competition**

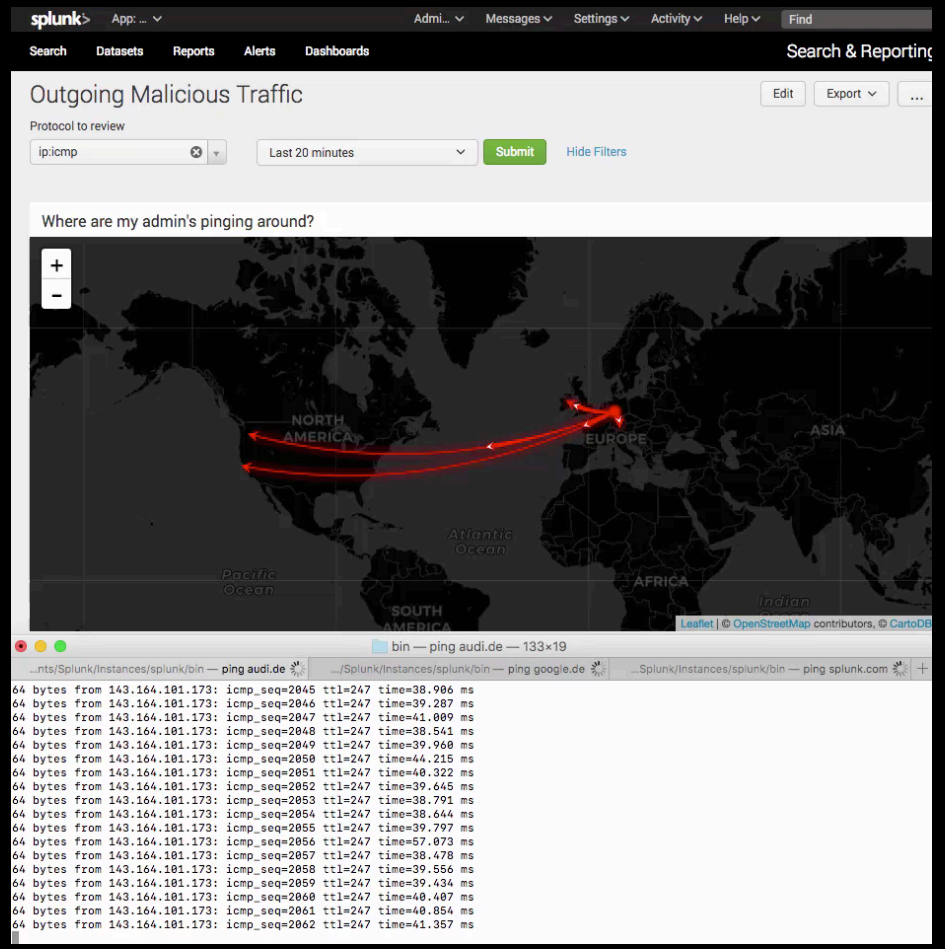
splunk> .conf18

# What Would You Show Them?

splunk> .conf18

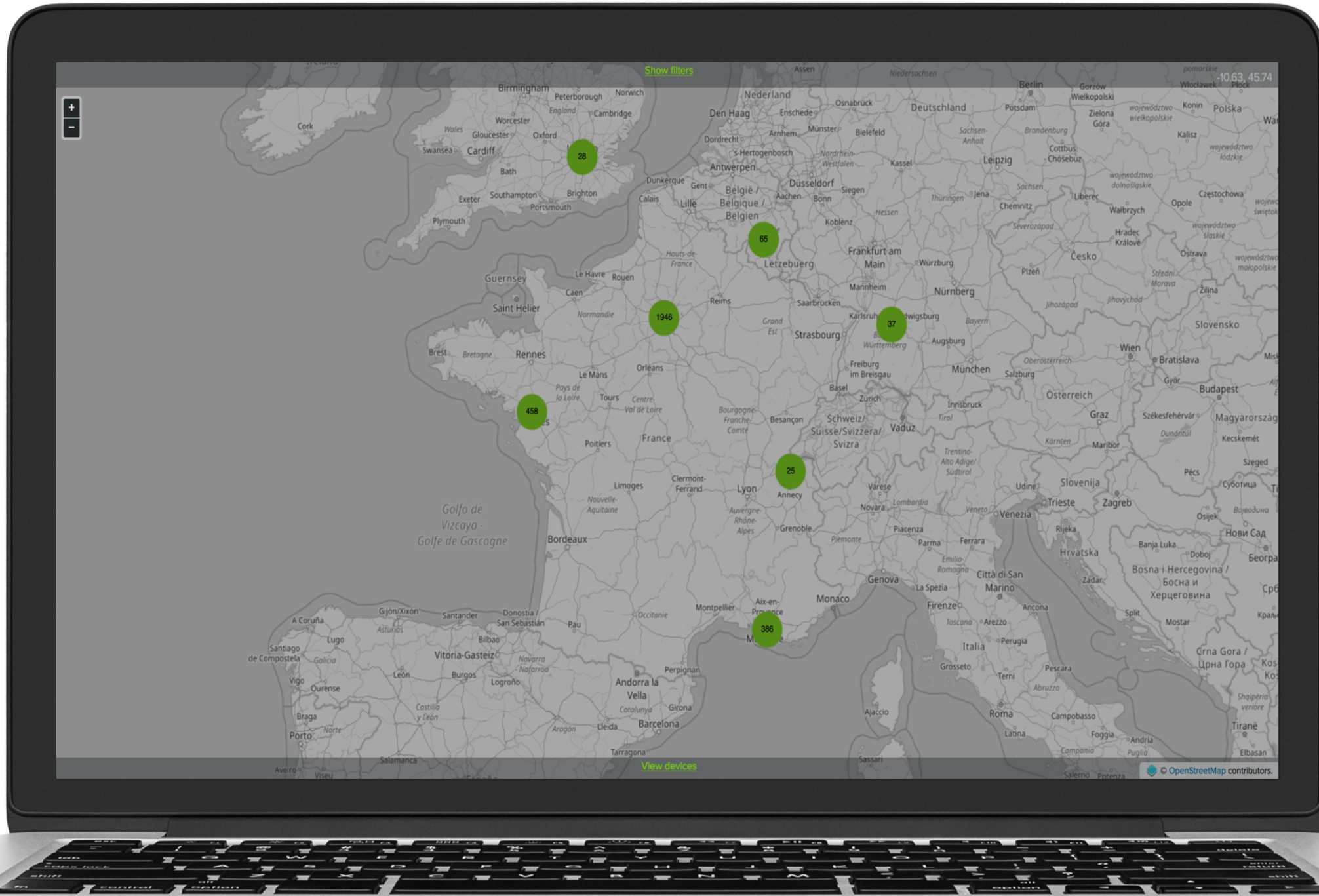
# Submissions

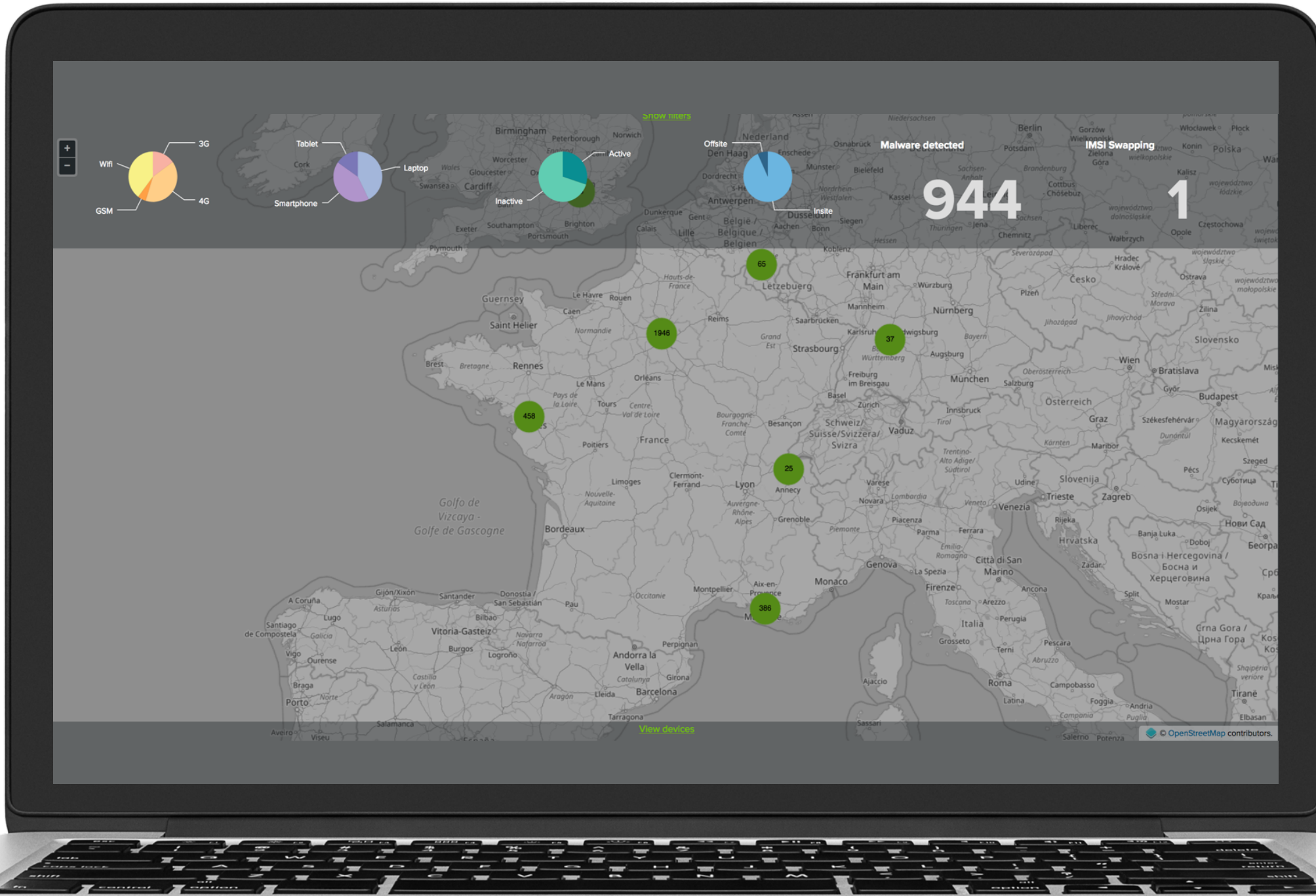


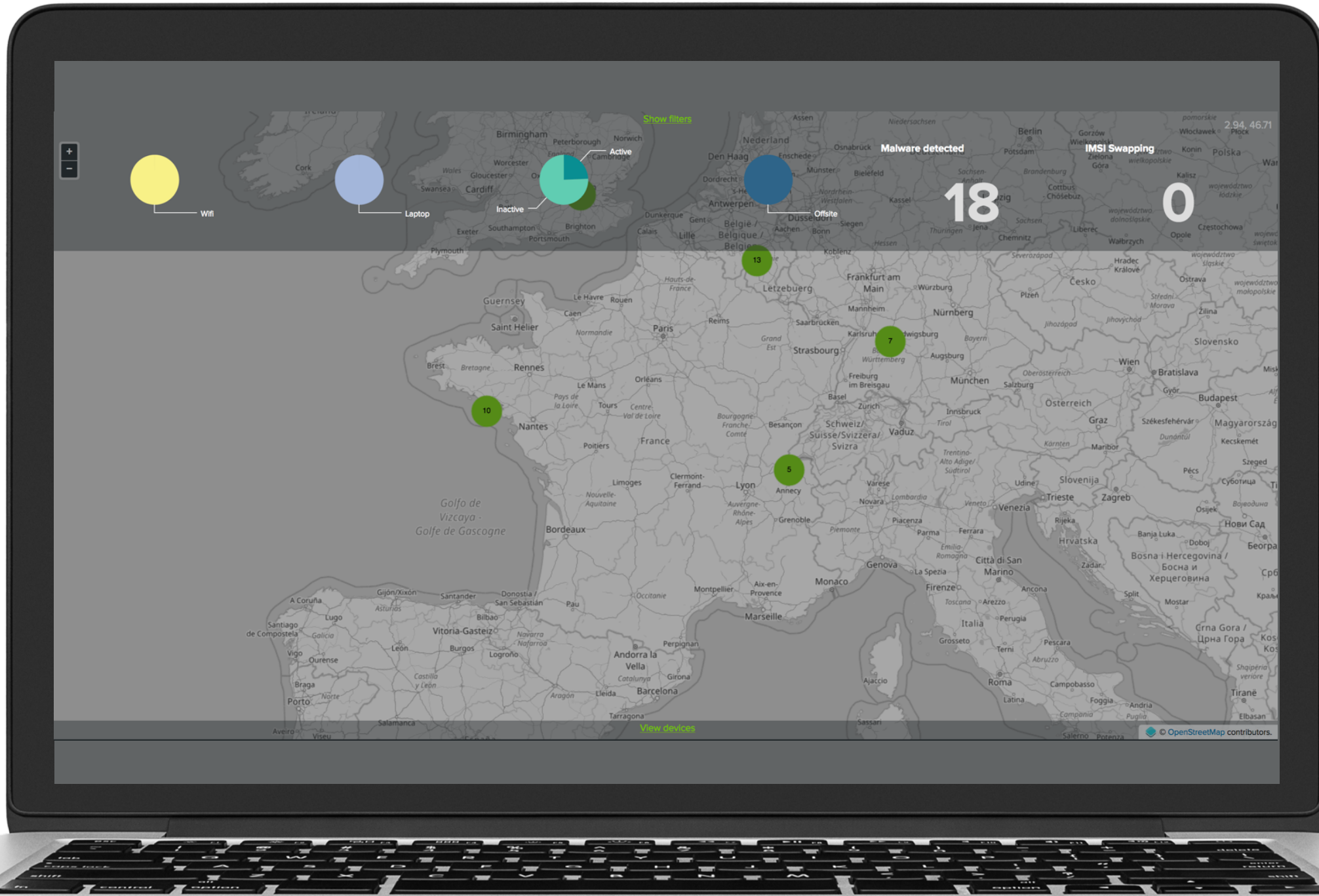



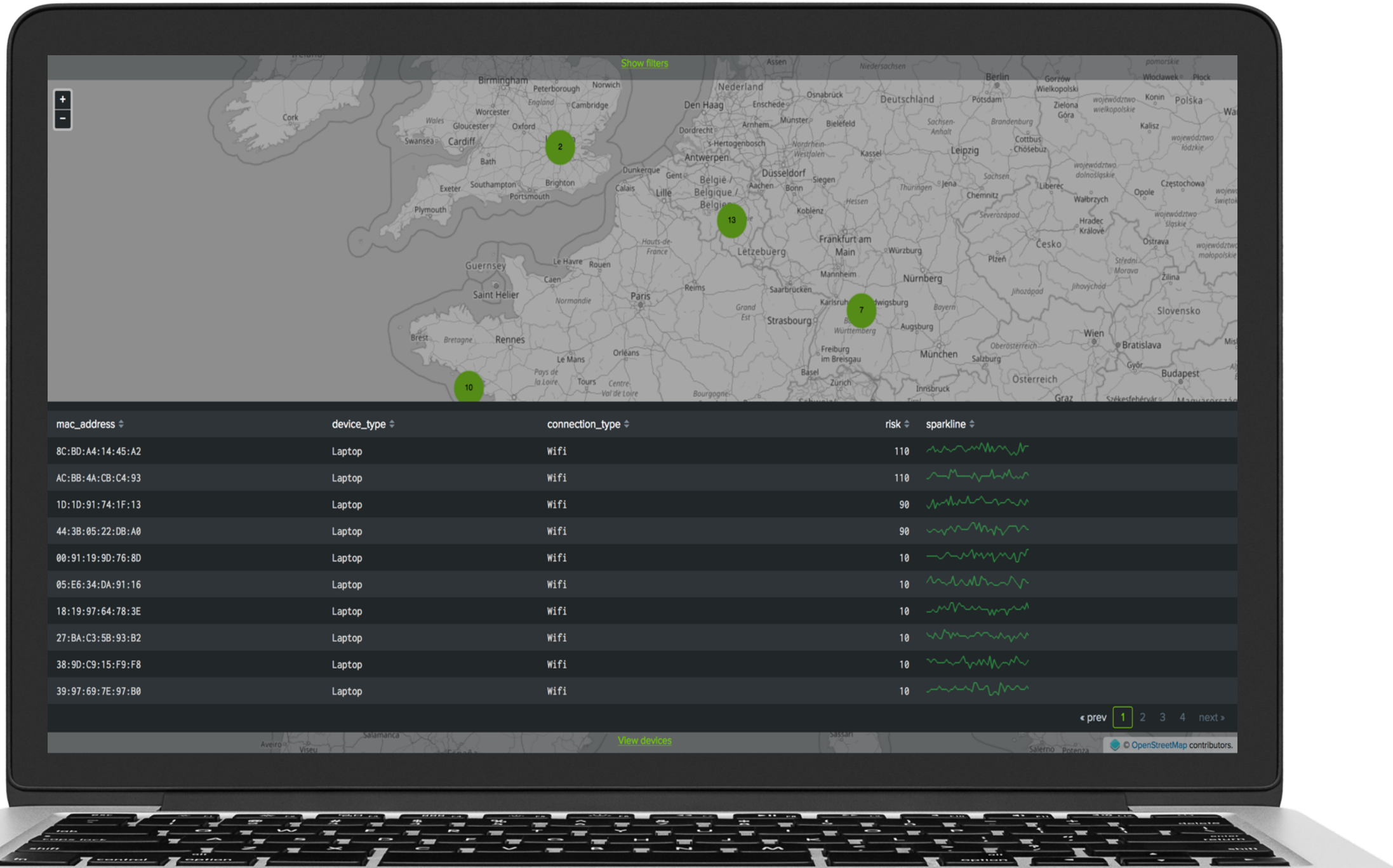
# Mobile Security App

splunk> .conf18


Show filters
-10.63, 45.74
28
65
1946
37
458
25
386
View devices
© OpenStreetMap contributors.

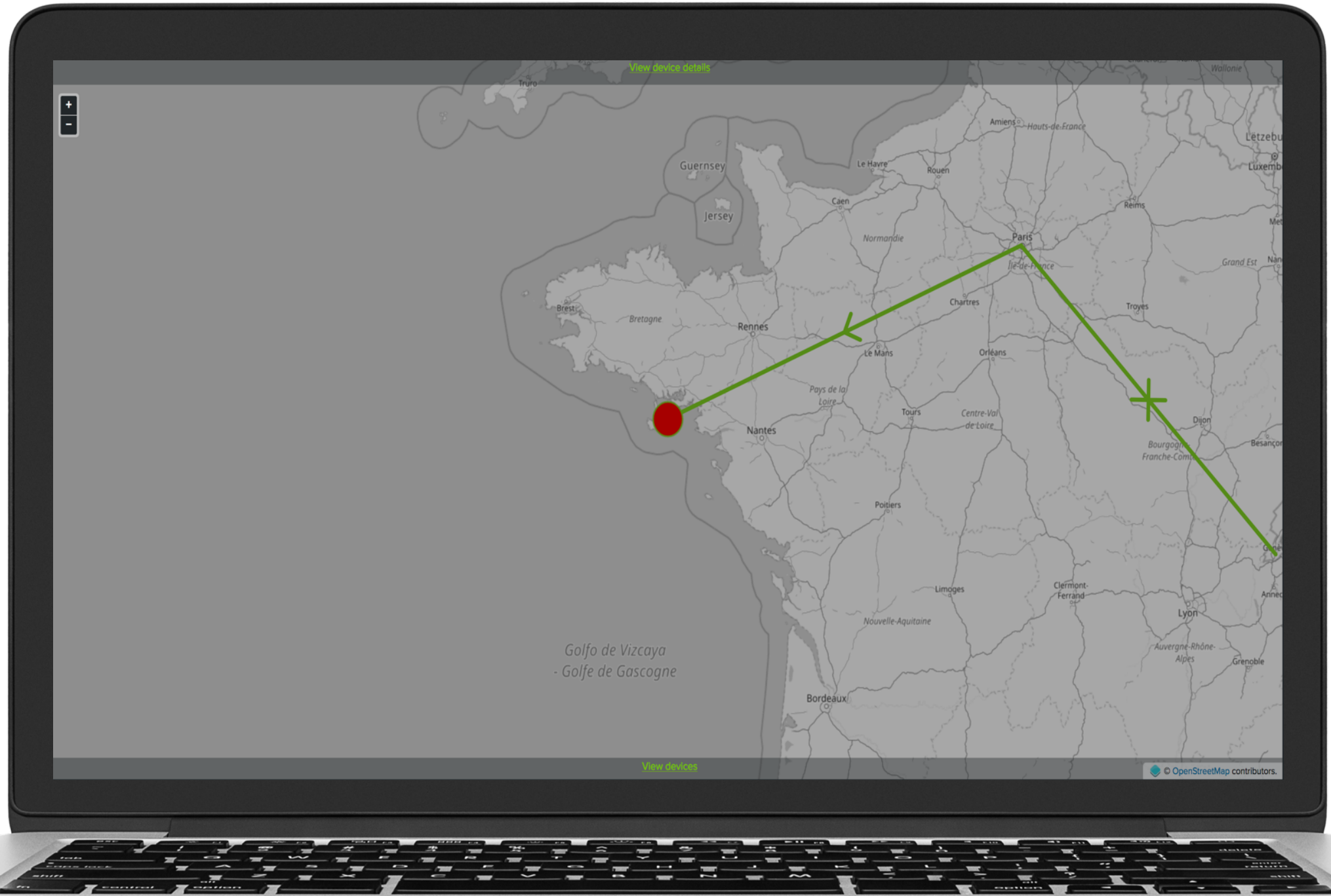

Show filters
3G
Wifi
4G
GSM
Tablet
Laptop
Smartphone
Active
Inactive
Offsite
Insite
Malware detected
944
IMSI Swapping
1
65
1946
37
458
25
386
View devices
© OpenStreetMap contributors.

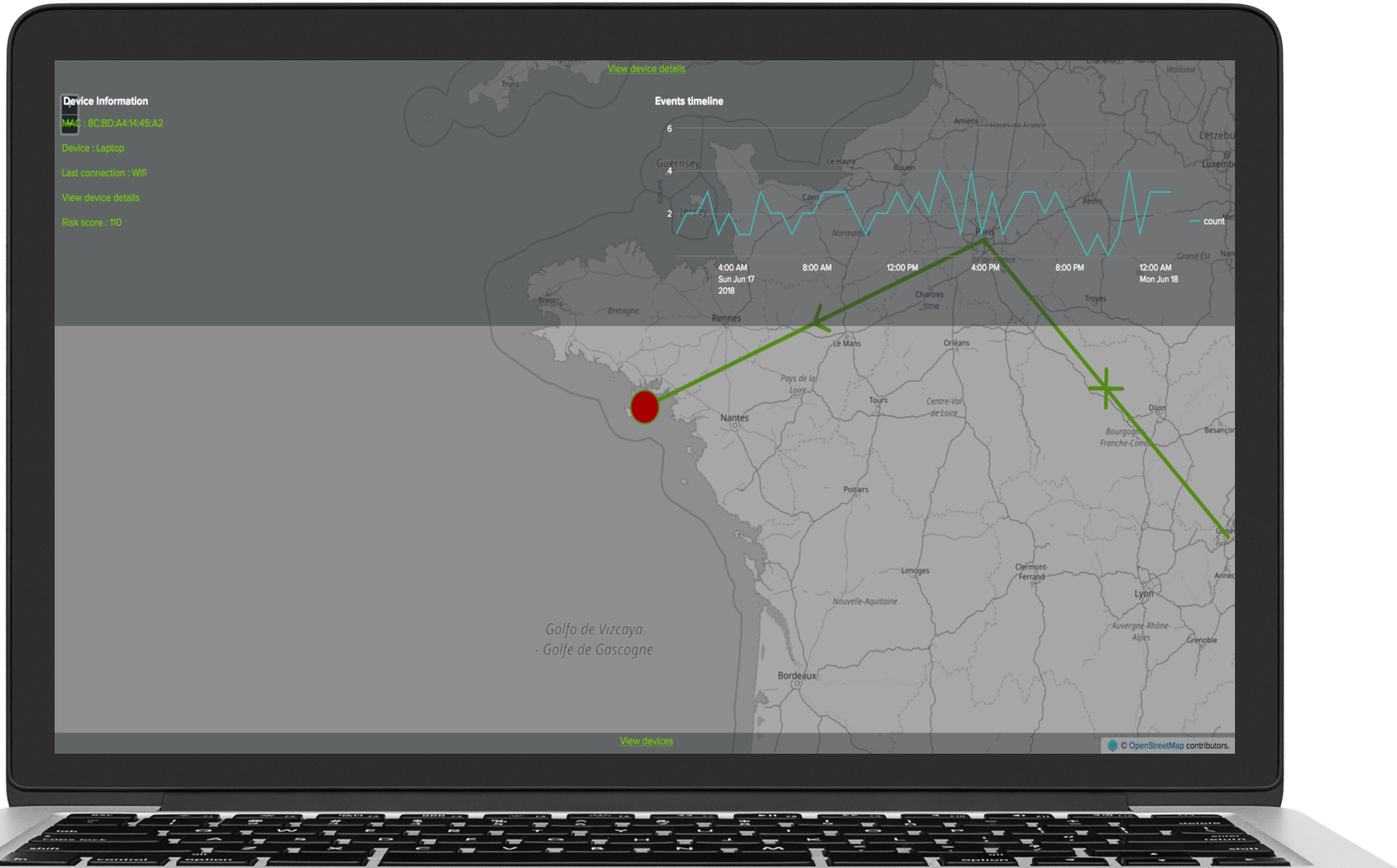

Show filters
2.94, 46.71
Wifi
Laptop
Active
Inactive
Offsite
Malware detected
18
IMSI Swapping
0
13
7
10
5
View devices
© OpenStreetMap contributors.




| mac_address | device_type | connection_type | risk | sparkline |
|---|---|---|---|---|
| 8C:BD:A4:14:45:A2 | Laptop | Wifi | 110 | |
| AC:BB:4A:CB:C4:93 | Laptop | Wifi | 110 | |
| 1D:1D:91:74:1F:13 | Laptop | Wifi | 90 | |
| 44:3B:05:22:DB:A0 | Laptop | Wifi | 90 | |
| 00:91:19:9D:76:8D | Laptop | Wifi | 10 | |
| 05:E6:34:DA:91:16 | Laptop | Wifi | 10 | |
| 18:19:97:64:78:3E | Laptop | Wifi | 10 | |
| 27:BA:C3:5B:93:B2 | Laptop | Wifi | 10 | |
| 38:9D:C9:15:F9:F8 | Laptop | Wifi | 10 | |
| 39:97:69:7E:97:B0 | Laptop | Wifi | 10 | |

« prev 1 2 3 4 next »


View device details
+
−
Truro
Guernsey
Jersey
Le Havre
Rouen
Amiens
Hauts-de-France
Caen
Normandie
Paris
Reims
Grand Est
Île-de-France
Chartres
Troyes
Brest
Bretagne
Rennes
Le Mans
Orléans
Pays de la Loire
Tours
Centre-Val de Loire
Nantes
Dijon
Poitiers
Limoges
Clermont-Ferrand
Lyon
Nouvelle-Aquitaine
Auvergne-Rhône-Alpes
Grenoble
Golfo de Vizcaya
- Golfe de Gascogne
Bordeaux
View devices
© OpenStreetMap contributors.

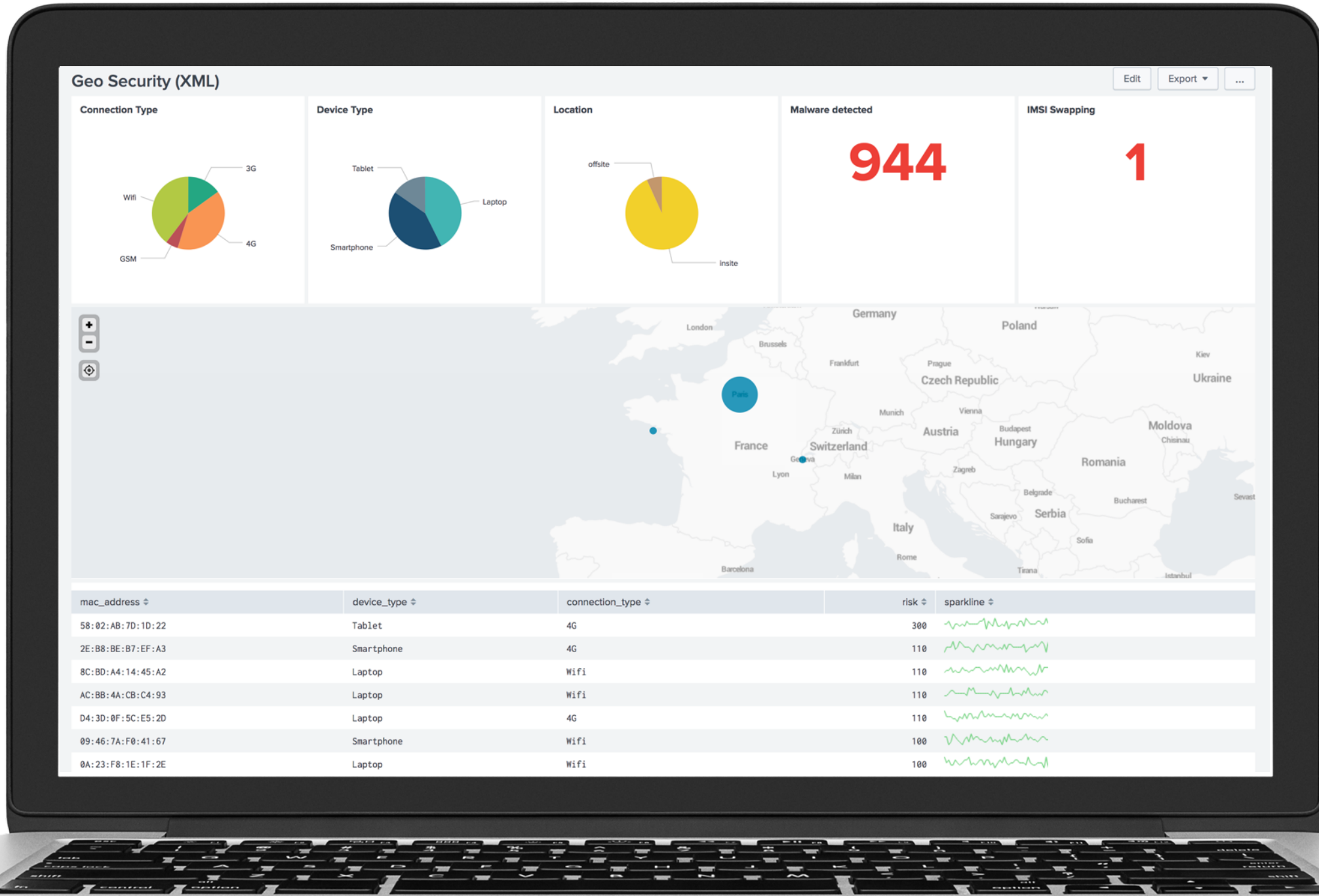

View device details
Device Information
MAC : 8C:BD:A4:14:45:A2
Device : Laptop
Last connection : Wifi
View device details
Risk score : 110
Events timeline
6
4
2
count
count
4:00 AM
Sun Jun 17
2018
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Mon Jun 18
Truro
Guernsey
Amiens
Le Havre
Rouen
Caen
Reims
Paris
Brest
Bretagne
Rennes
Chartres
Troyes
Le Mans
Orléans
Pays de la Loire
Tours
Centre-Val de Loire
Nantes
Dijon
Poitiers
Limoges
Clermont-Ferrand
Lyon
Nouvelle-Aquitaine
Auvergne-Rhône-Alpes
Grenoble
Golfo de Vizcaya
- Golfe de Gascogne
Bordeaux
View devices
© OpenStreetMap contributors.

# How Can You Do this with Splunk ?

splunk> .conf18

# Creating Your Dashboard

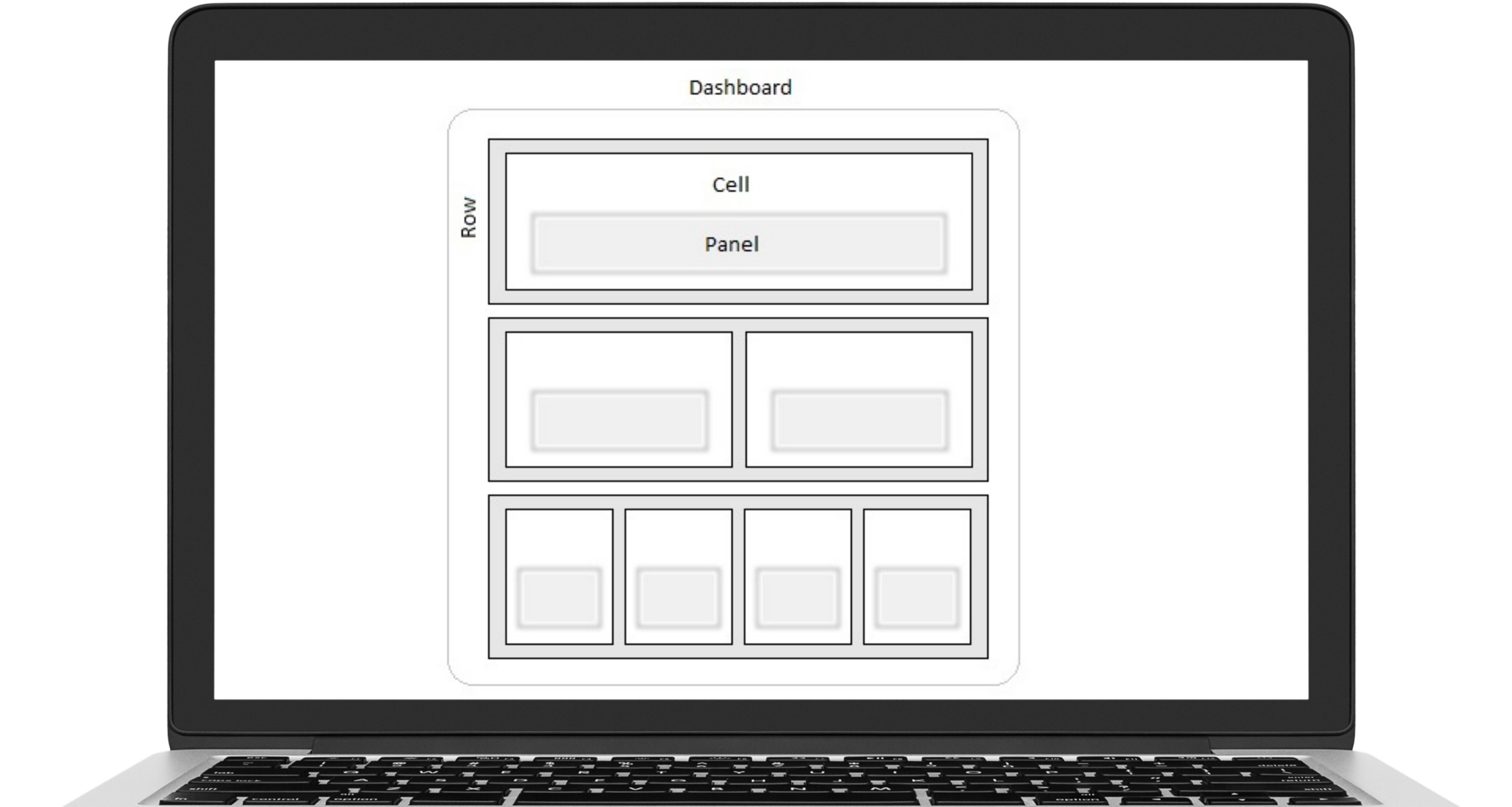
1. The raw dashboard was built 100% with Splunk Web
2. All you need is covered in the Splunk Fundamentals 1 Training Course
3. The key is to understand how it's shaped


Geo Security (XML)
Edit
Export
...
Connection Type
3G
Wifi
4G
GSM
Device Type
Tablet
Laptop
Smartphone
Location
offsite
insite
Malware detected
944
IMSI Swapping
1
Germany
Poland
London
Brussels
Frankfurt
Prague
Czech Republic
Kiev
Ukraine
Paris
Munich
Vienna
Zürich
Austria
Budapest
Hungary
Moldova
Chisinau
France
Switzerland
Romania
Lyon
Milan
Zagreb
Belgrade
Bucharest
Sevast
Sarajevo
Serbia
Italy
Sofia
Rome
Barcelona
Tirana
Istanbul
mac_address
device_type
connection_type
risk
sparkline
58:02:AB:7D:1D:22 Tablet 4G 300
2E:B8:BE:B7:EF:A3 Smartphone 4G 110
8C:BD:A4:14:45:A2 Laptop Wifi 110
AC:BB:4A:CB:C4:93 Laptop Wifi 110
D4:3D:0F:5C:E5:2D Laptop 4G 110
09:46:7A:F0:41:67 Smartphone Wifi 100
0A:23:F8:1E:1F:2E Laptop Wifi 100

# Dashboard Structure

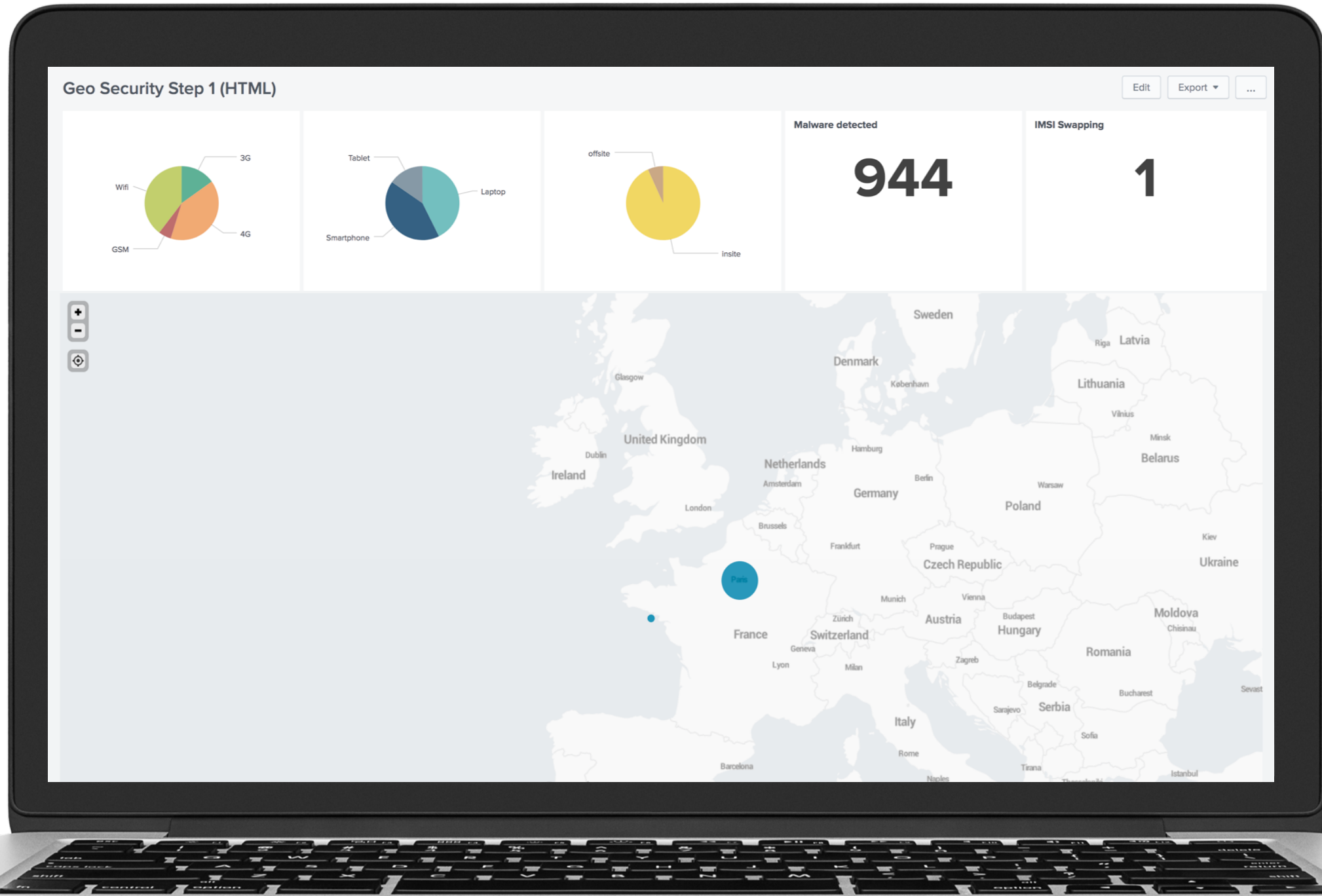
All Splunk dashboards have a structure:

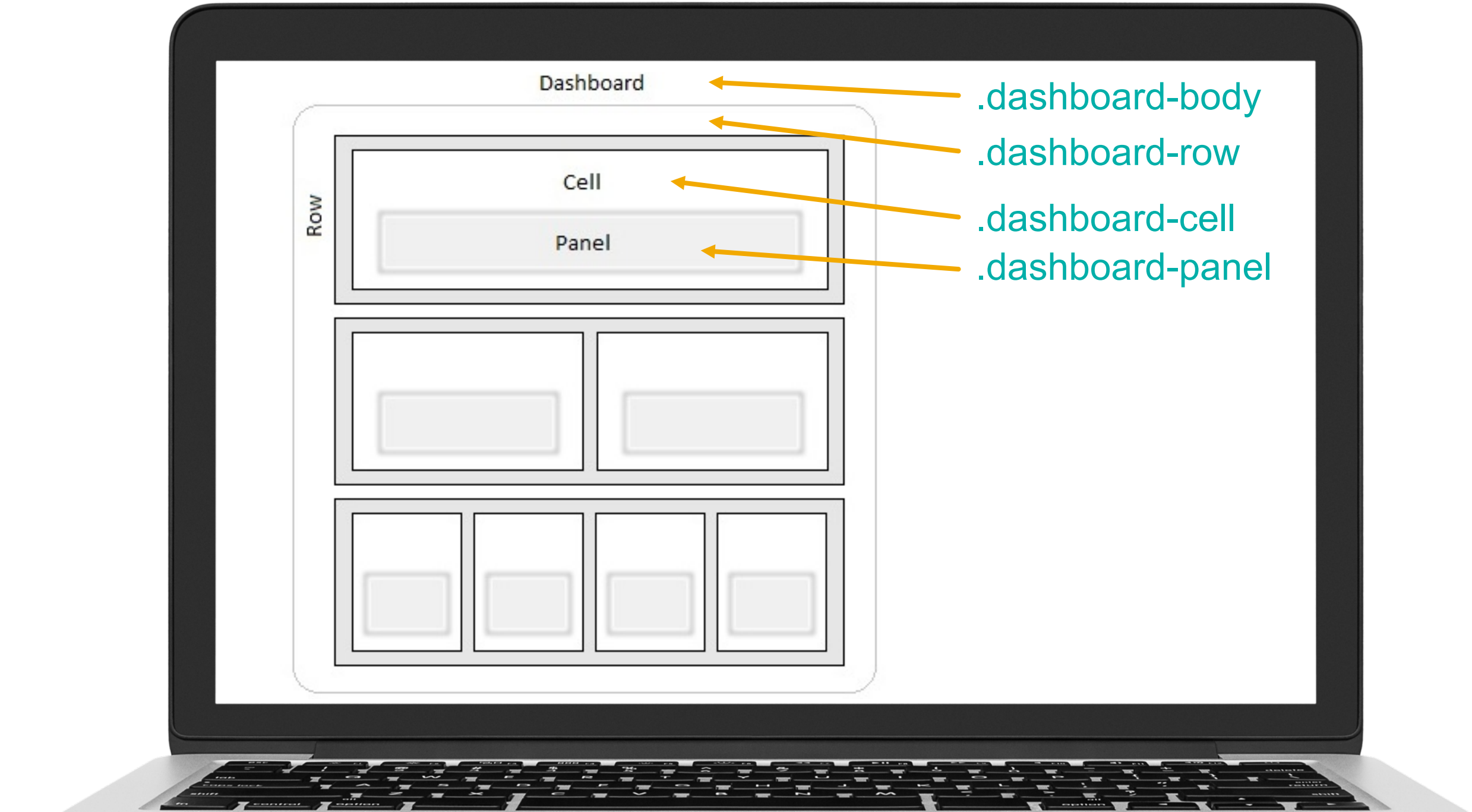
- A dashboard is made of a body
- A body is made of rows
- A row is made of cells
- And a cell is made of panels


Dashboard
Row
Cell
Panel

# Play with HTML / CSS

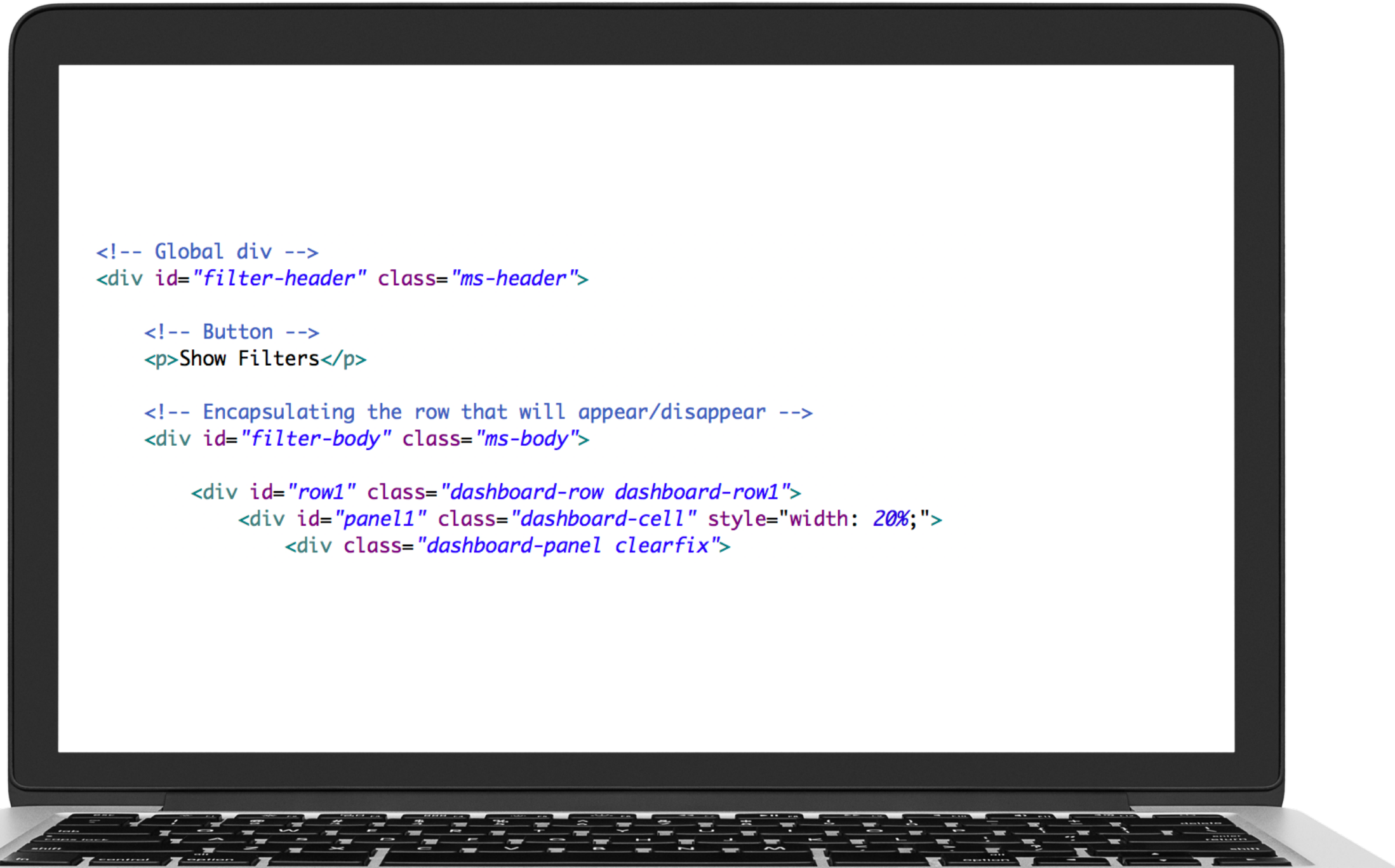
1. Convert your dashboard to HTML
2. Identify the CSS classes for dashboard, rows, panels and cells


Geo Security Step 1 (HTML)
Edit
Export
...
3G
Wifi
4G
GSM
Tablet
Laptop
Smartphone
offsite
insite
Malware detected
944
IMSI Swapping
1
Sweden
Latvia
Riga
Denmark
København
Lithuania
Vilnius
Minsk
Belarus
Glasgow
United Kingdom
Dublin
Ireland
Hamburg
Netherlands
Amsterdam
Berlin
Germany
Warsaw
Poland
London
Brussels
Frankfurt
Prague
Czech Republic
Kiev
Ukraine
Paris
Munich
Vienna
Zürich
Austria
Budapest
Hungary
Moldova
Chisinau
France
Switzerland
Geneva
Lyon
Milan
Zagreb
Romania
Belgrade
Bucharest
Sevast
Sarajevo
Serbia
Italy
Sofia
Rome
Barcelona
Tirana
Istanbul
Naples


Dashboard
Row
Cell
Panel
.dashboard-body
.dashboard-row
.dashboard-cell
.dashboard-panel

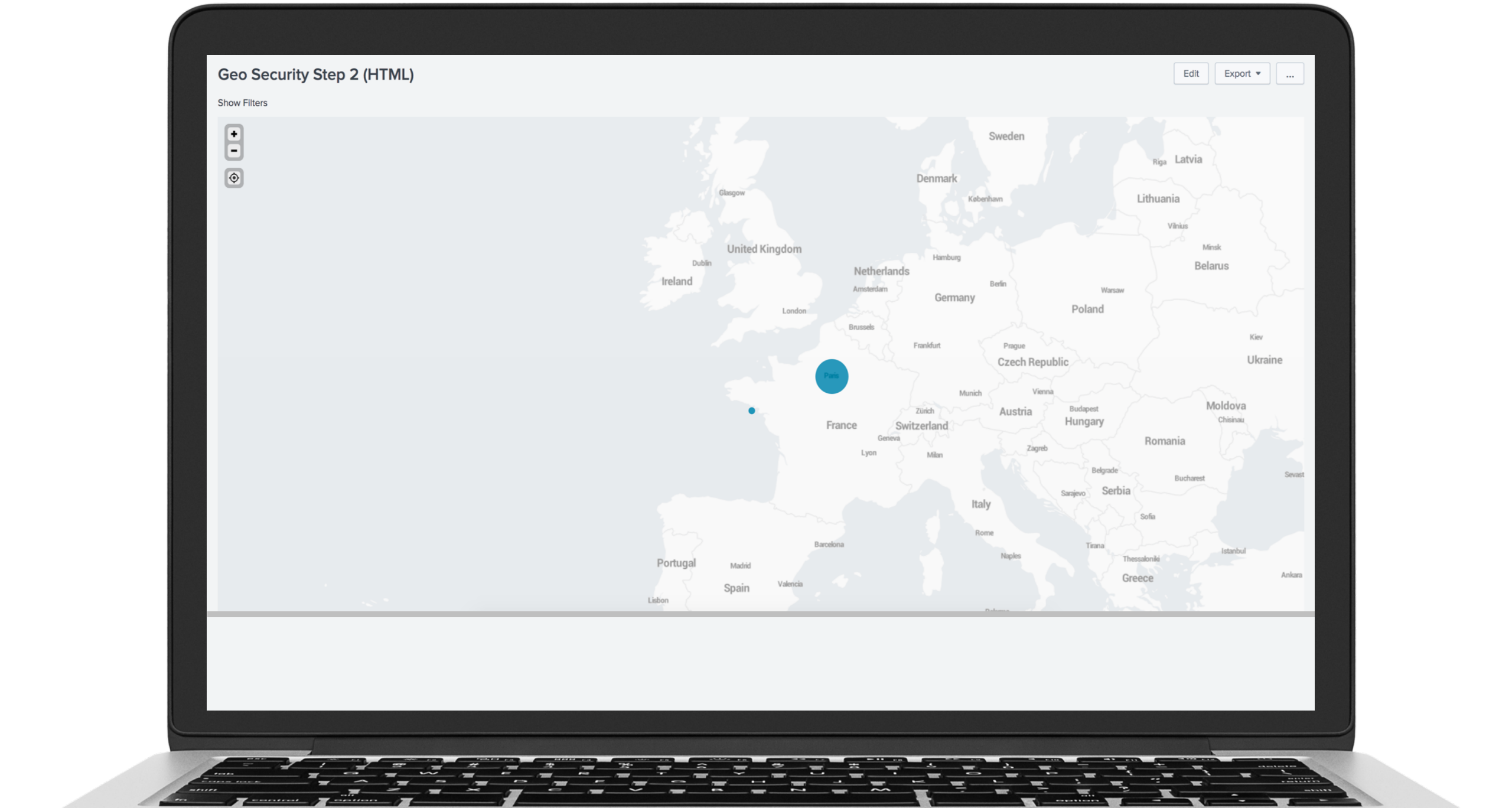
# Play with HTML / CSS

3. Add the custom part
4. Add button actions to show / hide some parts


<!-- Global div -->

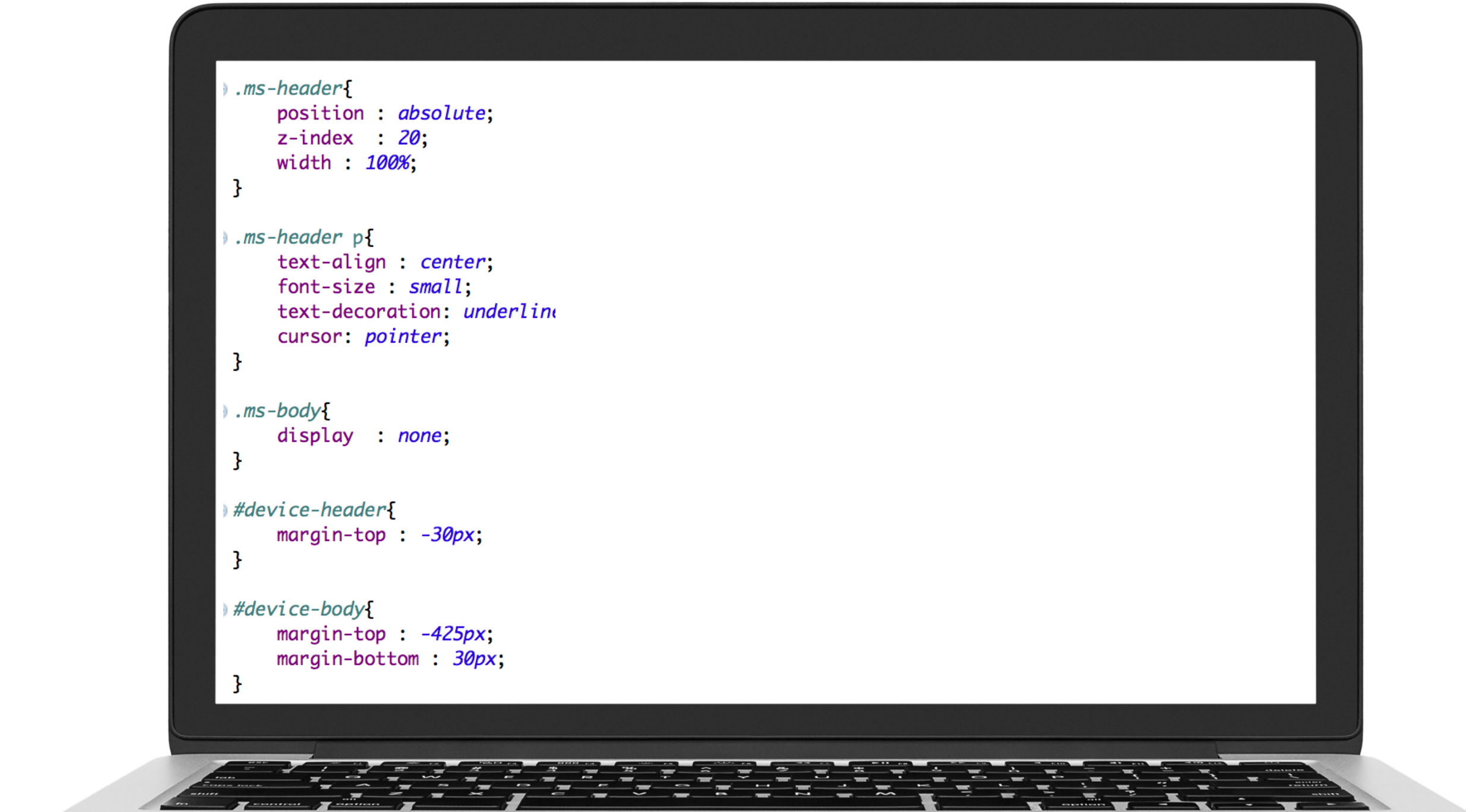
<!-- Button -->
Show Filters
<!-- Encapsulating the row that will appear/disappear -->

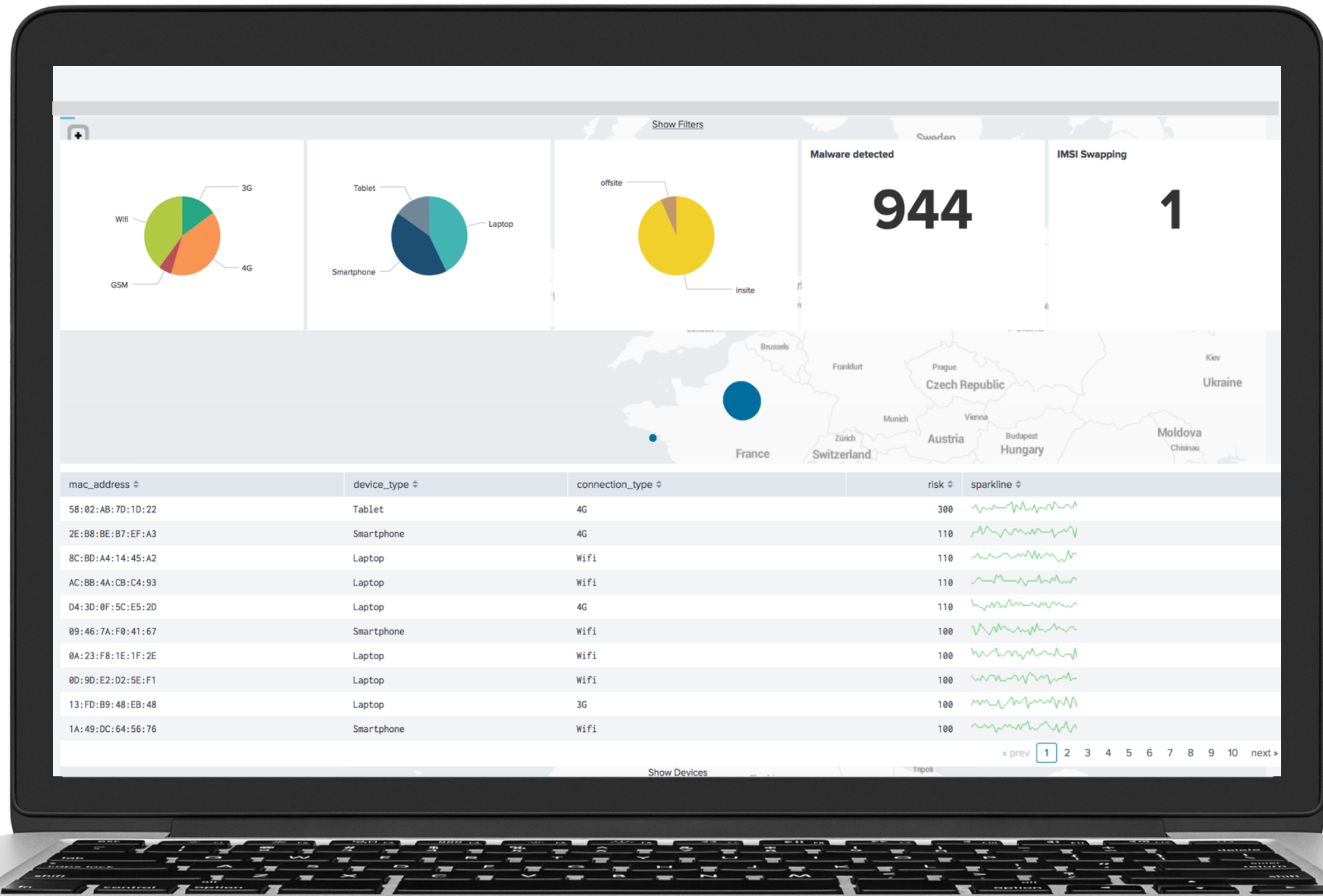

$(document).ready(function(){
$("#filter-header p").click(function(){
$("#filter-body").toggle();
});
$("#device-header p").click(function(){
$("#device-body").toggle();
});
});

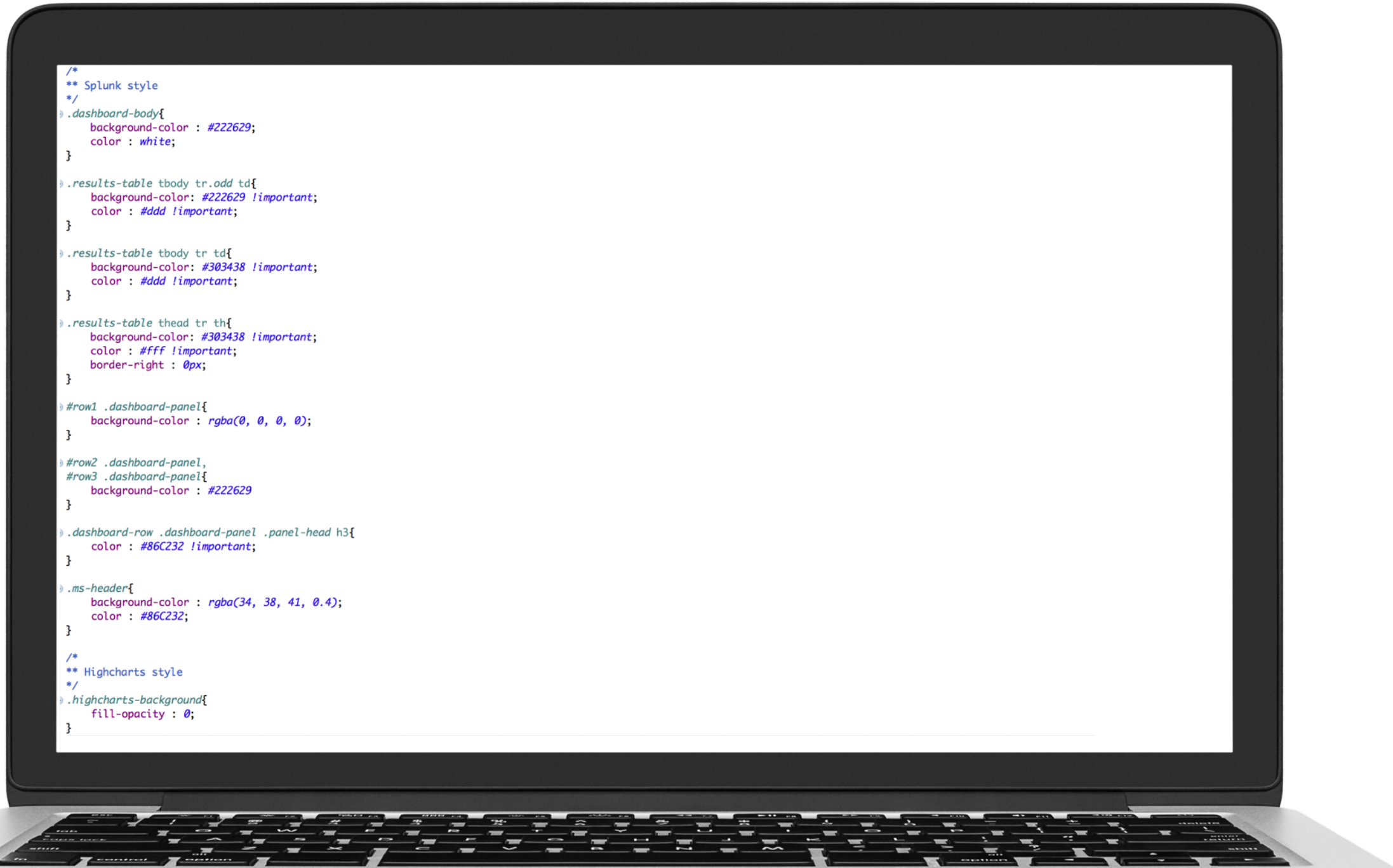

Geo Security Step 2 (HTML)
Edit
Export
...
Show Filters
Sweden
Latvia
Riga
Denmark
Lithuania
Glasgow
København
Vilnius
Minsk
United Kingdom
Hamburg
Belarus
Dublin
Netherlands
Ireland
Berlin
Amsterdam
Warsaw
Germany
Poland
London
Brussels
Kiev
Frankfurt
Prague
Ukraine
Czech Republic
Paris
Munich
Vienna
Moldova
Austria
Budapest
Zürich
Chisinau
Hungary
France
Switzerland
Romania
Geneva
Zagreb
Lyon
Milan
Belgrade
Bucharest
Sevast
Sarajevo
Serbia
Italy
Sofia
Rome
Barcelona
Tirana
Istanbul
Portugal
Madrid
Naples
Thessaloniki
Spain
Valencia
Greece
Ankara
Lisbon

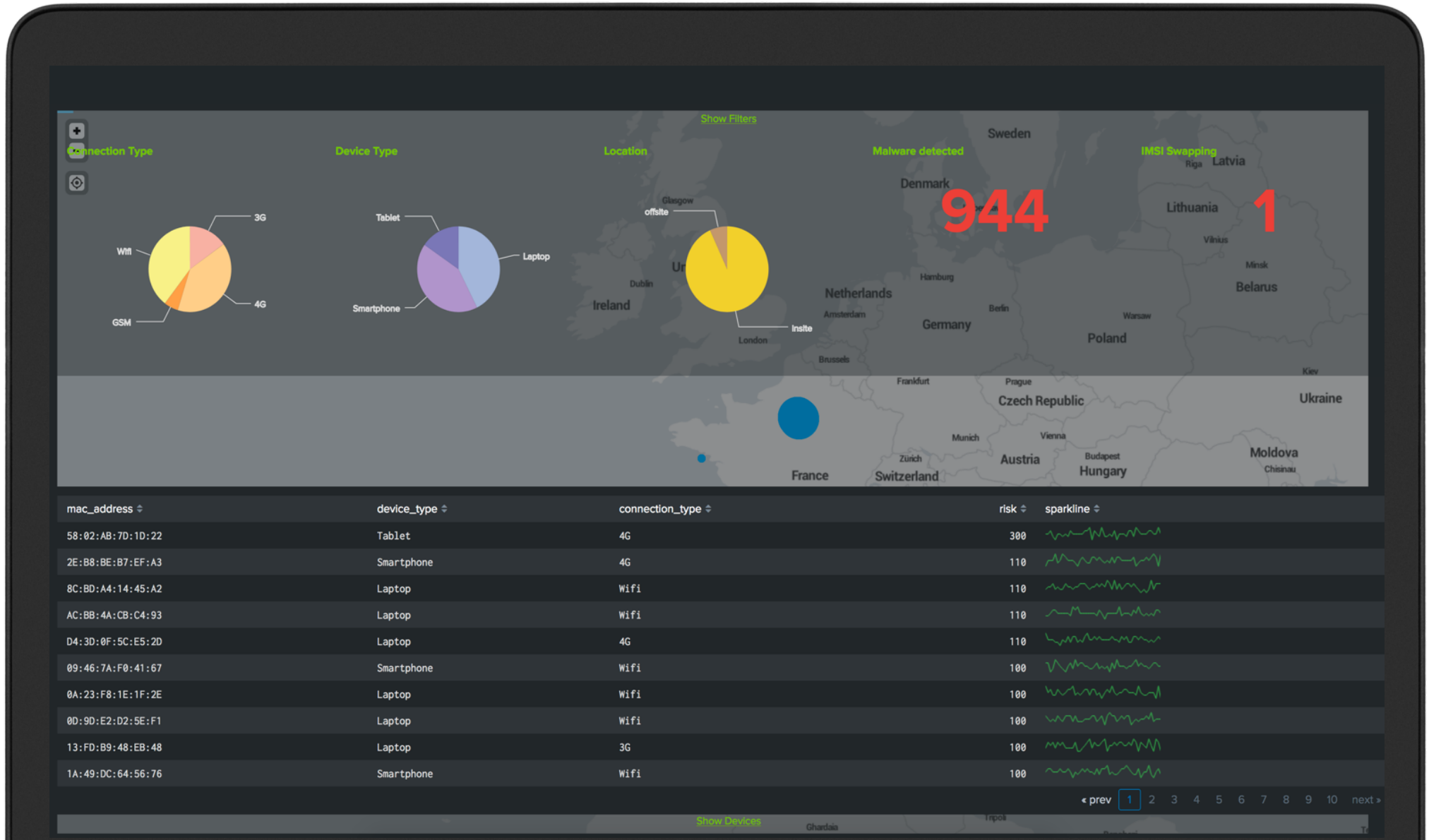
# Play with HTML / CSS

5. Play with the drill-down
6. Add colors and transparency


.ms-header{
position : absolute;
z-index : 20;
width : 100%;
}
.ms-header p{
text-align : center;
font-size : small;
text-decoration: underlin
cursor: pointer;
}
.ms-body{
display : none;
}
#device-header{
margin-top : -30px;
}
#device-body{
margin-top : -425px;
margin-bottom : 30px;
}


Show Filters
3G
Wifi
4G
GSM
Tablet
Laptop
Smartphone
offsite
insite
Malware detected
944
IMSI Swapping
1
Brussels
Frankfurt
Prague
Czech Republic
Kiev
Ukraine
Munich
Vienna
Austria
Budapest
Hungary
Moldova
Chisinau
Zürich
Switzerland
France
mac_address
device_type
connection_type
risk
sparkline
58:02:AB:7D:1D:22 Tablet 4G 300
2E:B8:BE:B7:EF:A3 Smartphone 4G 110
8C:BD:A4:14:45:A2 Laptop Wifi 110
AC:BB:4A:CB:C4:93 Laptop Wifi 110
D4:3D:0F:5C:E5:2D Laptop 4G 110
09:46:7A:F0:41:67 Smartphone Wifi 100
0A:23:F8:1E:1F:2E Laptop Wifi 100
0D:9D:E2:D2:5E:F1 Laptop Wifi 100
13:FD:B9:48:EB:48 Laptop 3G 100
1A:49:DC:64:56:76 Smartphone Wifi 100
« prev 1 2 3 4 5 6 7 8 9 10 next »
Show Devices


/*
** Splunk style
*/
.dashboard-body{
background-color : #222629;
color : white;
}
.results-table tbody tr.odd td{
background-color: #222629 !important;
color : #ddd !important;
}
.results-table tbody tr td{
background-color: #303438 !important;
color : #ddd !important;
}
.results-table thead tr th{
background-color: #303438 !important;
color : #fff !important;
border-right : 0px;
}
#row1 .dashboard-panel{
background-color : rgba(0, 0, 0, 0);
}
#row2 .dashboard-panel,
#row3 .dashboard-panel{
background-color : #222629
}
.dashboard-row .dashboard-panel .panel-head h3{
color : #86C232 !important;
}
.ms-header{
background-color : rgba(34, 38, 41, 0.4);
color : #86C232;
}
/*
** Highcharts style
*/
.highcharts-background{
fill-opacity : 0;
}



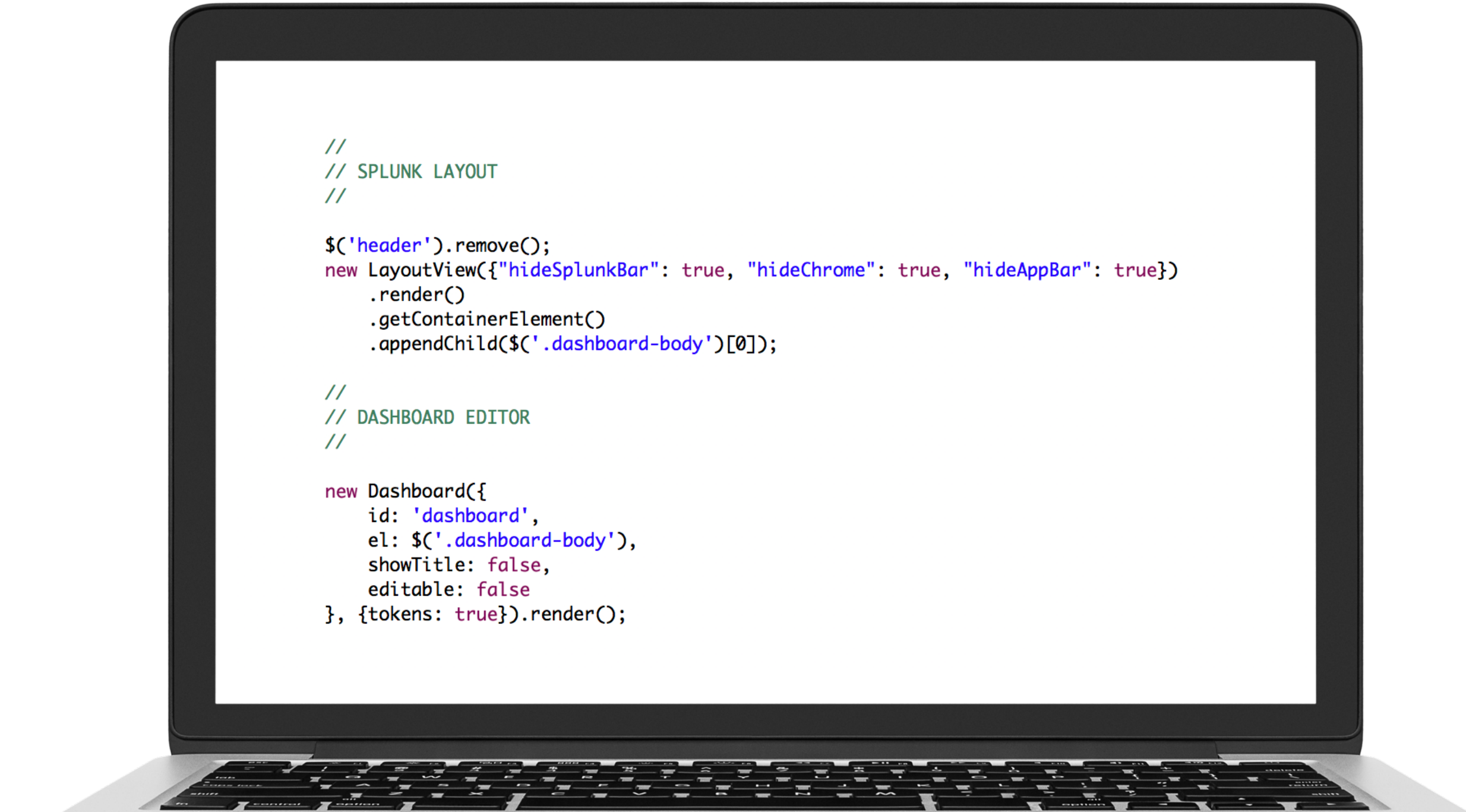

| mac_address | device_type | connection_type | risk | sparkline |
|---|---|---|---|---|
| 58:02:AB:7D:1D:22 | Tablet | 4G | 300 | |
| 2E:B8:BE:B7:EF:A3 | Smartphone | 4G | 110 | |
| 8C:BD:A4:14:45:A2 | Laptop | Wifi | 110 | |
| AC:BB:4A:CB:C4:93 | Laptop | Wifi | 110 | |
| D4:3D:0F:5C:E5:2D | Laptop | 4G | 110 | |
| 09:46:7A:F0:41:67 | Smartphone | Wifi | 100 | |
| 0A:23:F8:1E:1F:2E | Laptop | Wifi | 100 | |
| 0D:9D:E2:D2:5E:F1 | Laptop | Wifi | 100 | |
| 13:FD:B9:48:EB:48 | Laptop | 3G | 100 | |
| 1A:49:DC:64:56:76 | Smartphone | Wifi | 100 | |

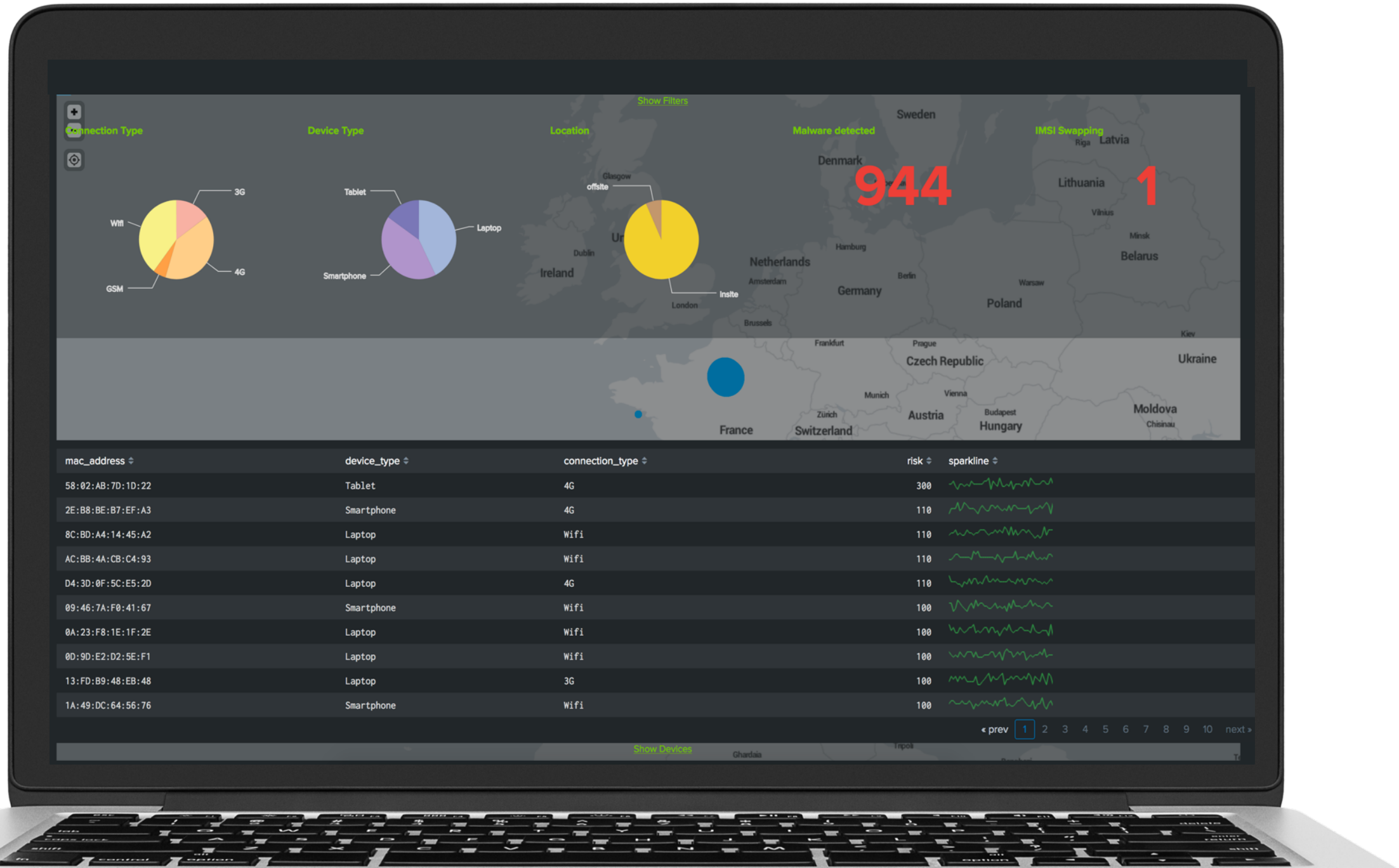
« prev 1 2 3 4 5 6 7 8 9 10 next »

# Play with HTML / CSS

7. Remove what we don’t need to show (like Splunk’s application bar)

8. Make it a full-screen dashboard


//
// SPLUNK LAYOUT
//
$('header').remove();
new LayoutView({"hideSplunkBar": true, "hideChrome": true, "hideAppBar": true})
.render()
.getContainerElement()
.appendChild($('.dashboard-body')[0]);
//
// DASHBOARD EDITOR
//
new Dashboard({
id: 'dashboard',
el: $('.dashboard-body'),
showTitle: false,
editable: false
}, {tokens: true}).render();




| mac_address | device_type | connection_type | risk | sparkline |
|---|---|---|---|---|
| 58:02:AB:7D:1D:22 | Tablet | 4G | 300 | |
| 2E:B8:BE:B7:EF:A3 | Smartphone | 4G | 110 | |
| 8C:BD:A4:14:45:A2 | Laptop | Wifi | 110 | |
| AC:BB:4A:CB:C4:93 | Laptop | Wifi | 110 | |
| D4:3D:0F:5C:E5:2D | Laptop | 4G | 110 | |
| 09:46:7A:F0:41:67 | Smartphone | Wifi | 100 | |
| 0A:23:F8:1E:1F:2E | Laptop | Wifi | 100 | |
| 0D:9D:E2:D2:5E:F1 | Laptop | Wifi | 100 | |
| 13:FD:B9:48:EB:48 | Laptop | 3G | 100 | |
| 1A:49:DC:64:56:76 | Smartphone | Wifi | 100 | |

« prev 1 2 3 4 5 6 7 8 9 10 next »

# Download Example

**Download the Splunk App**
https://splunk.box.com/s/z13oymagtwtgtuf7f8keuuy5n7epuyua


**More documentation on Splunk customization**
https://docs.splunk.com/Documentation/Splunk/7.1.2/AdvancedDev/UseCSS

**Highcharts CSS references**
https://www.highcharts.com/docs/chart-design-and-style/style-by-css

# Questions?

splunk> .conf18

# Thank You

**Don't forget to rate this session in the .conf18 mobile app**