MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

Voyage professionnel à l'international

qu'advient-il de vos périphériques lors d'un contrôle à l'étranger ?

TLP:CLEAR

Histoire tirée de faits réels

TLP:CLEAR

Présentation du contexte (1)

Frodon Sacquet

Ingénieur de l'entreprise française Cul-de-sac

Téléphone personnel – Android – Huawei

Téléphone professionnel – Android – Samsung

Sam Gamegie

Ingénieur de l'entreprise française Cul-de-sac

Téléphone personnel – Android – Oppo

TLP:CLEAR

Présentation du contexte (2)


Voyage professionnel

But : échanger sur des technologies de pointe

Gondor

Passage dans le pays du Gondor
Contrôle frontière

Faramir

Interrogatoire poussé de plusieurs heures par Faramir

TLP:CLEAR

Sommaire

TLP:CLEAR

Déroulement des faits (1)

Environnement

- Salle d'interrogatoire - Seul
- Récupération des appareils électroniques
- Pression et questions
- Durée : 3h30

Diverses questions

- Codes de déverrouillage
- Raisons de la venue au Gondor
- Entreprise Cul-de-sac
- Informations personnelles

TLP:CLEAR

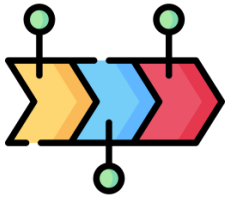
Déroulement des faits (2)

Sam et Frodon après l'interrogatoire

Entreprise sensible

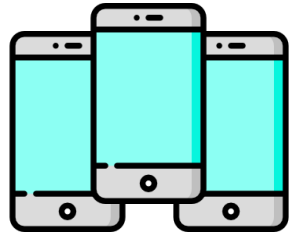
Contacte l'Officier de Sécurité

Contacte notre service



Création d'une chronologie

Copie des données pour analyse



Remise des supports

TLP:CLEAR

Analyse des téléphones – Déverrouillage

Les codes de déverrouillage ont-ils été utilisés ?

Déverrouillage du téléphone

timestamp	package_name	type
2023-01-28 17:43:49	android	18

*Sam perso – Table **events***
/data/data/com.google.android.apps.wellbeing/databases/app_usage

Type : 18
———
Déverrouillage du téléphone

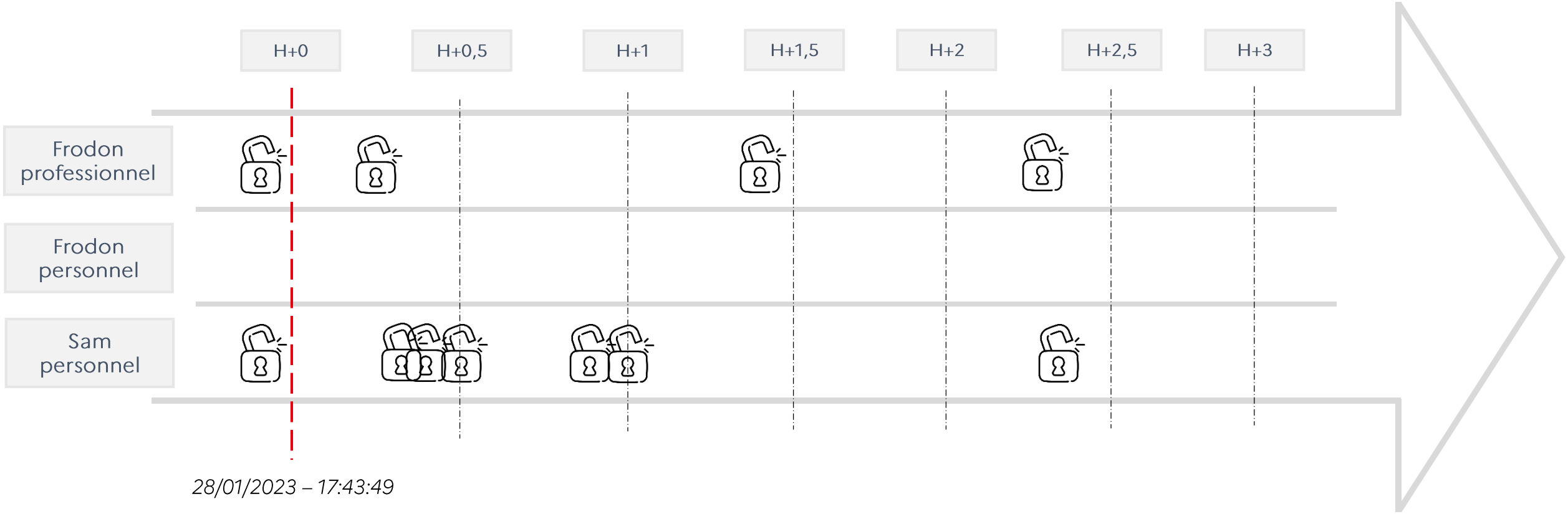
Déverrouillage du téléphone

timestamp	eventType	className
2023-01-28 17:43:32	18	NULL

*Frodon pro – Table **usageEvents***
/data/data/com.samsung.android.forest/databases/dwbCommon.db

TLP:CLEAR

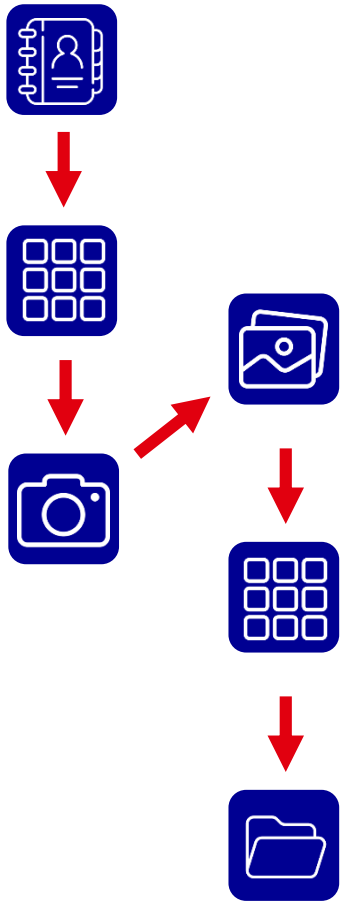
Analyse des téléphones – Déverrouillage



TLP:CLEAR

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Analyse des téléphones – Consultation



Que s'est-il passé après le déverrouillage ?

Contacts, photos

timestamp	package_name	type
2023-01-28 20:29:04	com.android.contacts	23
2023-01-28 20:29:06	com.oppo.launcher	2
2023-01-28 20:29:06	com.oppo.camera	1
2023-01-28 20:29:06	com.oppo.launcher	23
2023-01-28 20:29:07	com.oppo.camera	2
2023-01-28 20:29:07	com.coloros.gallery3d	1
2023-01-28 20:29:08	com.oppo.camera	23
2023-01-28 20:29:11	com.coloros.gallery3d	2
2023-01-28 20:29:11	com.oppo.launcher	1
2023-01-28 20:29:11	com.coloros.gallery3d	23
2023-01-28 20:29:12	com.oppo.launcher	2
2023-01-28 20:29:12	com.coloros.filemanager	1

*Sam perso – Table **events***
/data/data/com.google.android.apps.wellbeing/databases/app_usage

Type : 2
—
Activité passée au 2nd plan

Type : 1
—
Activité passée au 1er plan

Type : 23
—
Activité invisible sur l'UI

TLP:CLEAR

Analyse des téléphones – Consultation

Type : 2

Activité passée au 2nd plan

Type : 1

Activité passée au 1er plan

Type : 23

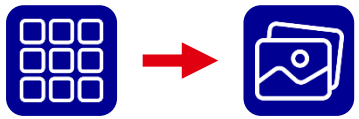
Activité invisible sur l'UI

Conversations

timestamp	eventType	className
2023-01-28 18:12:06	1	com.whatsapp.Conversation
2023-01-28 18:12:07	23	com.whatsapp.HomeActivity
2023-01-28 18:12:08	2	com.whatsapp.Conversation
2023-01-28 18:12:09	1	com.whatsapp.HomeActivity
2023-01-28 18:12:09	23	com.whatsapp.Conversation
2023-01-28 18:12:11	2	com.whatsapp.HomeActivity

Photos

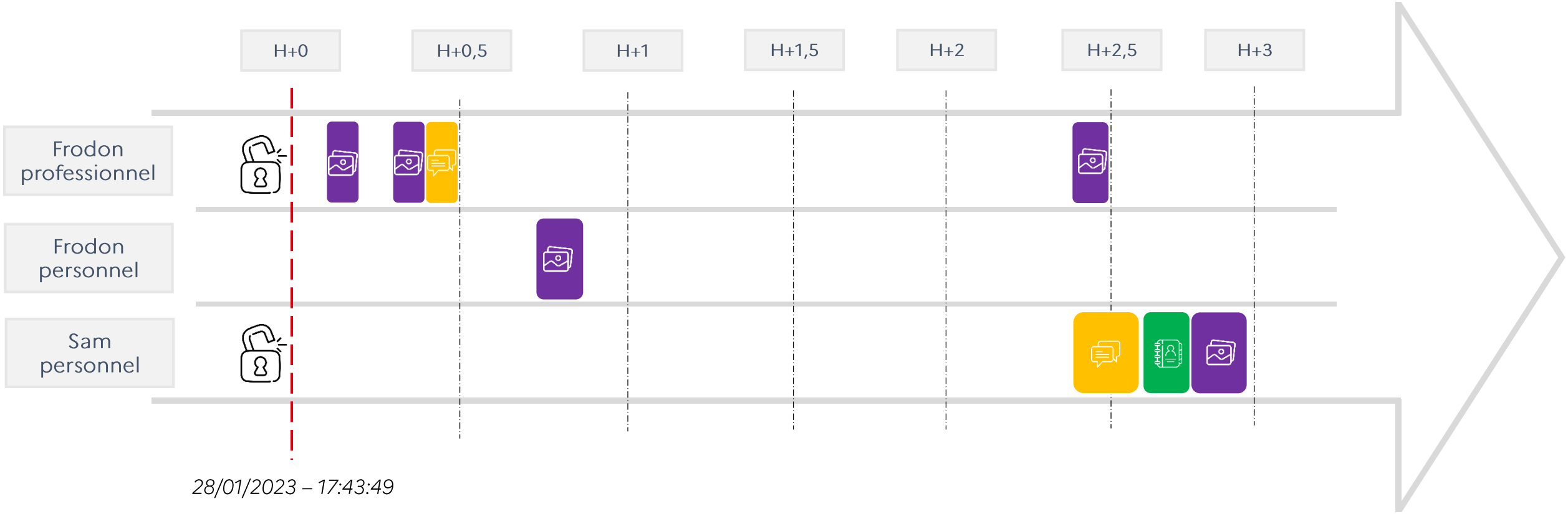
timestamp	eventType	className
2023-01-28 18:06:17	23	com.samsung.android.gallery.app.activity.GalleryActivity
2023-01-28 18:06:19	2	com.android.launcher3.uioverrides.QuickstepLauncher
2023-01-28 18:06:19	1	com.samsung.android.gallery.app.activity.GalleryActivity
2023-01-28 18:06:20	23	com.android.launcher3.uioverrides.QuickstepLauncher
2023-01-28 18:06:21	2	com.samsung.android.gallery.app.activity.GalleryActivity
2023-01-28 18:06:21	1	com.android.launcher3.uioverrides.QuickstepLauncher
2023-01-28 18:06:21	23	com.samsung.android.gallery.app.activity.GalleryActivity



Frodon pro – Samsung Digital Wellbeing - Table usageEvents
/data/data/com.samsung.android.forest/databases/dwbCommon.db

TLP:CLEAR

Analyse des téléphones – Consultation



TLP:CLEAR

Analyse des téléphones – Paramètres

Le téléphone a-t-il été modifié ?

Paramètres

timestamp	package_name	type
2023-01-28 18:13:43	com.android.settings	23
2023-01-28 18:13:45	com.android.settings.intelligence	2
2023-01-28 18:13:45	com.android.settings	1
2023-01-28 18:13:46	com.android.settings.intelligence	23
2023-01-28 18:13:50	com.android.settings	2
2023-01-28 18:13:51	com.android.settings	1
2023-01-28 18:13:51	com.android.settings	23
2023-01-28 18:13:59	com.android.settings	2
2023-01-28 18:13:59	com.android.settings	1
2023-01-28 18:14:00	com.android.settings	23

*Sam perso – Table **events***
/data/data/com.google.android.apps.wellbeing/databases/app_usage

Type : 2
—
Activité passée au 2nd plan

Type : 1
—
Activité passée au 1er plan

Type : 23
—
Activité invisible sur l'UI

TLP:CLEAR

Type : 5
———
Modification des paramètres

Analyse des téléphones – Paramètres

Paramètres

timestamp	eventType	className
2023-01-28 17:55:49	23	com.android.launcher3.uioverrides.QuickstepLauncher
2023-01-28 17:55:52	2	com.android.settings.homepage.SettingsHomepageActivity
2023-01-28 17:55:52	1	com.samsung.android.samsungaccount.setting.ui.main.SettingMainPreference
2023-01-28 17:55:53	2	com.samsung.android.samsungaccount.setting.ui.main.SettingMainPreference
2023-01-28 17:55:53	1	com.android.settings.homepage.SettingsHomepageActivity
2023-01-28 17:55:53	23	com.samsung.android.samsungaccount.setting.ui.main.SettingMainPreference
2023-01-28 17:56:04	2	com.android.settings.homepage.SettingsHomepageActivity
2023-01-28 17:56:04	1	com.android.settings.SubSettings
2023-01-28 17:56:05	23	com.android.settings.homepage.SettingsHomepageActivity
2023-01-28 17:56:17	2	com.android.settings.SubSettings
2023-01-28 17:56:17	1	com.android.launcher3.uioverrides.QuickstepLauncher
2023-01-28 17:56:18	23	com.android.settings.SubSettings

Modification de paramètres

timestamp	eventType	
2023-01-28 18:04:58	5	NULL
2023-01-28 18:05:25	5	NULL

Frodon pro – Samsung Digital Wellbeing - Table usageEvents
/data/data/com.samsung.android.forest/databases/dwbCommon.db

TLP:CLEAR

Analyse des téléphones – Paramètres

Recherche dans les settings du téléphone

query	timestamp
numero bui	2023-01-28 18:29:54
de	2023-01-28 18:30:39
numéro de build	2023-01-28 18:30:41
option dev	2023-01-28 18:37:28
lagnu	2023-01-28 19:11:45
lang	2023-01-28 19:47:16

Frodon perso – Table saved_queries
/data/user_de/0/com.android.settings/databases/search_index.db

Activation USB debugging

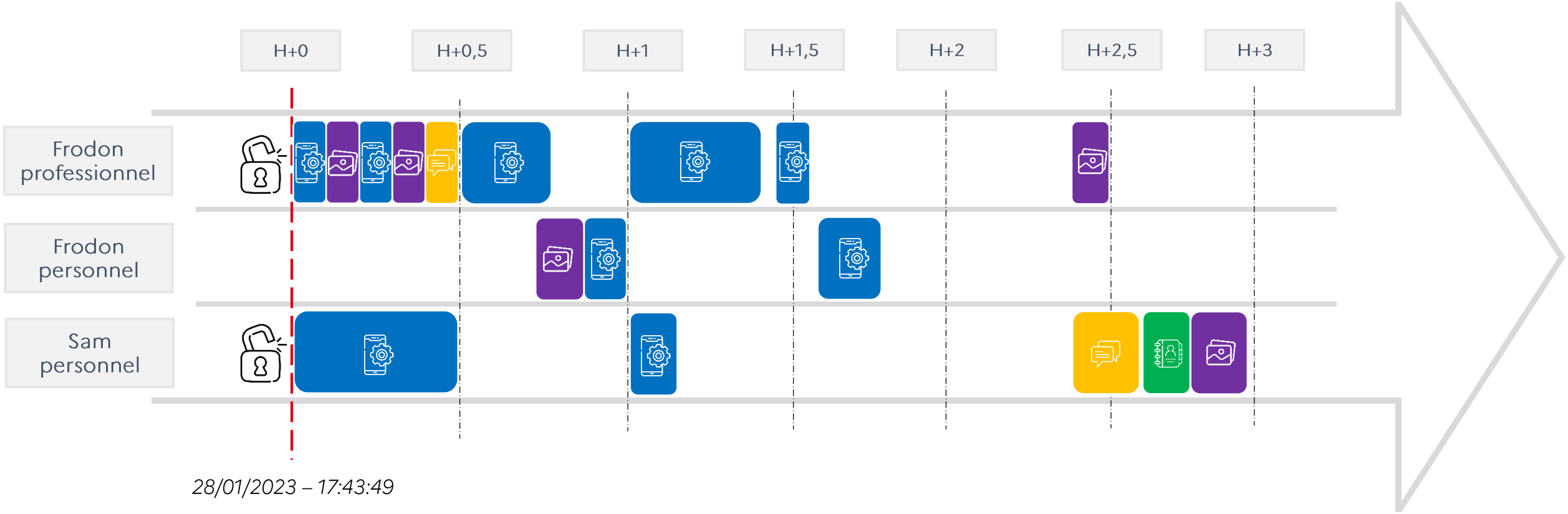
/data/system_ce/0/launch_params/com.android.systemui_.usb.HwUsbDebuggingActivity.xml

Frodon perso
Date de modification : 25/01/2023 19:37

Langue | Numéro de version | Option développeurs | Débug USB

TLP:CLEAR

Analyse des téléphones – Paramètres



28/01/2023 – 17:43:49

TLP:CLEAR

Analyse des téléphones – Application Terre du Milieu

Est-ce qu'un élément a été installé ?

Installation d'une application

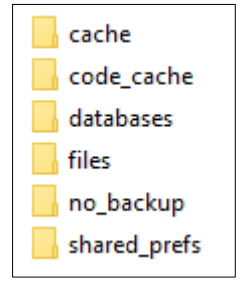
```
<package name="com.terre.milieu" codePath="/data/app/~~SGVsbG8gVGhlcmU=/com.terre.milieu-R2VuZXJhbCBLZW5vYmk=
    <sigs count="1" schemeVersion="2">
        <cert index="5" key="4d617920746865206666f726365206265207769746820796f754d617920746865206666f7263652062
    </sigs>
    <perms>
        <item name="android.permission.BLUETOOTH" granted="true" flags="0" />
        <item name="android.permission.AUTHENTICATE_ACCOUNTS" granted="true" flags="0" />
        <item name="android.permission.INTERNET" granted="true" flags="0" />
        <item name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" granted="true" flags="0" />
        <item name="android.permission.ACCESS_NETWORK_STATE" granted="true" flags="0" />
        <item name="android.permission.READ_USER_DICTIONARY" granted="true" flags="0" />
        <item name="android.permission.ACCESS_WIFI_STATE" granted="true" flags="0" />
    </perms>
    <proper-signing-keyset identifier="148" />
</package>
```

Sam perso – packages
/data/system/packages.xml

Application toujours installée

/data/data/com.terre.milieu
/data/app/~~xxxxxxxxxx/com.terre.milieu/base.apk

Sam perso



TLP:CLEAR

Analyse des téléphones – Application Terre du Milieu

Log d'erreur

```
PID = 0
UID = 0
PackageName = com.terre.milieu
KeyMsg = AppBootFail:com.terre.milieu
```

Frodon perso – Log
/data/log/faultlog/xxxxx-xxxxxxxxxxxxxxx.log

Log

C4com.terre.milieuD

Frodon perso – Log de l'application
/data/system/usagestats/0/yearly/xxxxxxxx

Analyse des téléphones – Application Terre du Milieu

Utilisation de l'application

timestamp	package_name	type
2023-01-28 18:18:04	com.terre.milieu	2
2023-01-28 18:18:04	com.google.android.permissioncontroller	1
2023-01-28 18:18:04	com.google.android.permissioncontroller	23
2023-01-28 18:18:05	com.google.android.permissioncontroller	2
2023-01-28 18:18:05	com.terre.milieu	1
2023-01-28 18:18:05	com.google.android.permissioncontroller	23
2023-01-28 18:18:05	com.terre.milieu	2

*Sam perso – Table **events***
/data/data/com.google.android.apps.wellbeing/databases/app_usage

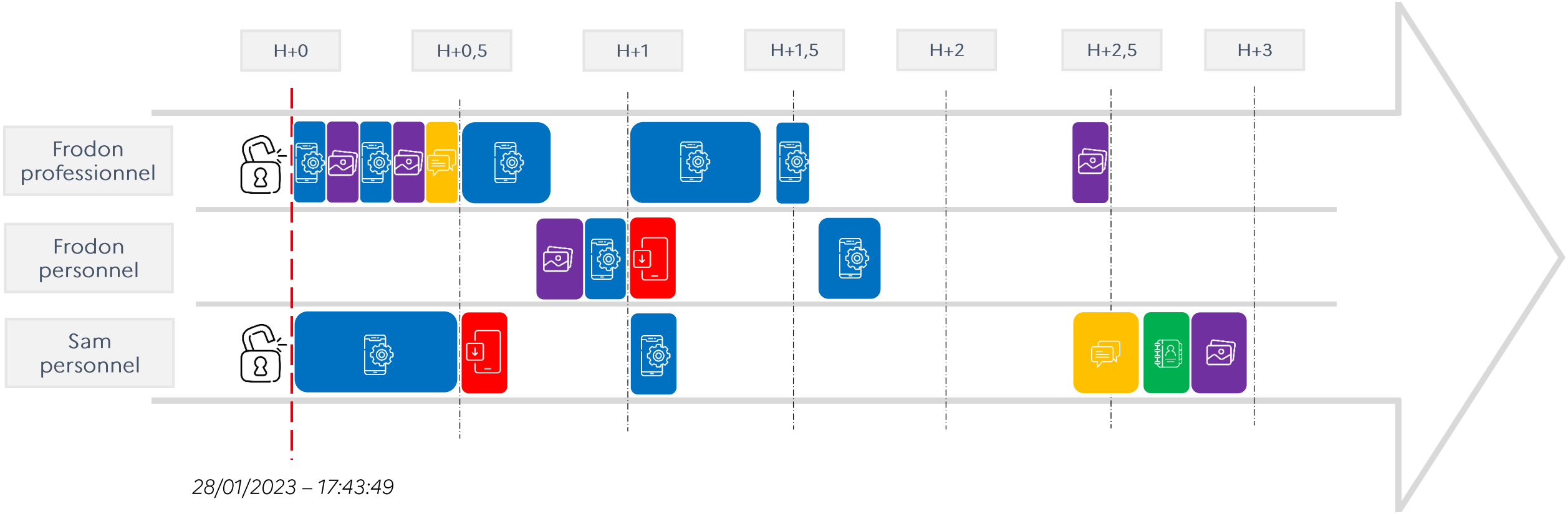
Trace de l'application

Fichier de configuration

Frodon perso – Log de l'application
/data/user_de/0/com.huawei.hwid/shared_prefs/HiAd_sp_com.terre.milieu.xml

TLP:CLEAR

Analyse des téléphones – Application Terre du Milieu



28/01/2023 – 17:43:49

TLP:CLEAR

Analyse des téléphones – Application Terre du Milieu

MDM

Mobile Device Management

- Gestion des terminaux mobiles
- Harmonise et sécurise la flotte de la société
- Installé sur le téléphone professionnel

Téléphone professionnel

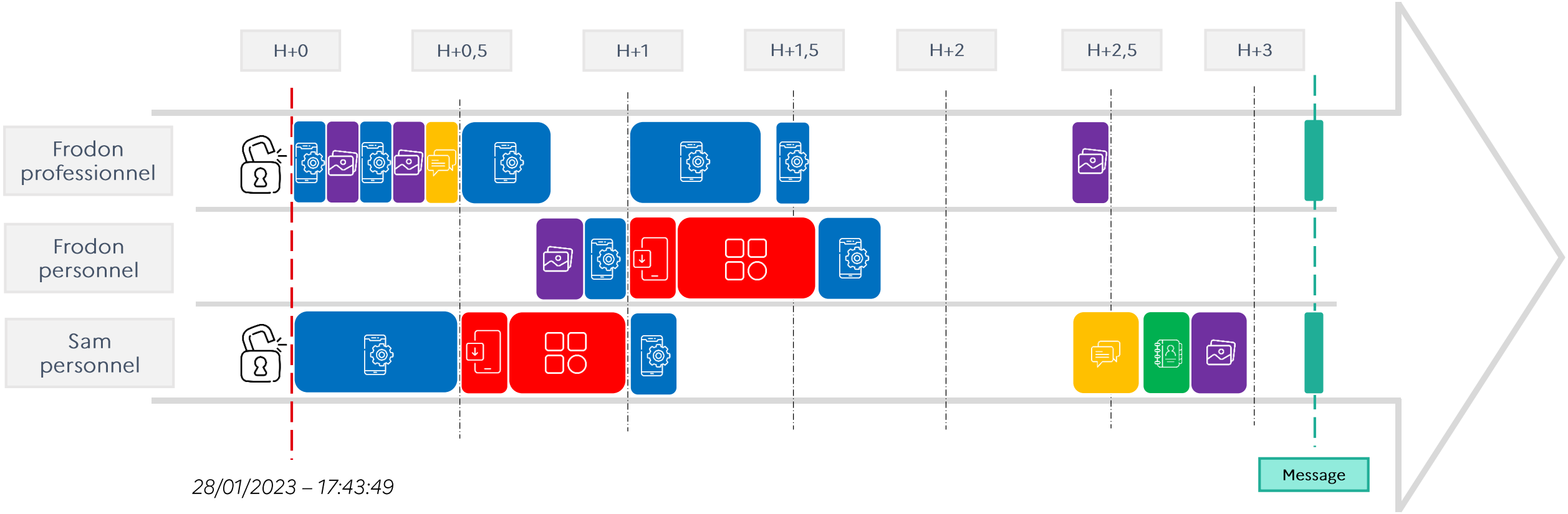
de Frodon

- Mot de passe spécifique pour accéder à la partie pro
- Accès aux paramètres limités
- Impossibilité de modifier certains paramètres

Bien configuré : permet l'ajout d'une couche de sécurité au téléphone

TLP:CLEAR

Analyse des téléphones – Application Terre du Milieu



TLP:CLEAR

Présentation de l'application retrouvée

Terre du Milieu

com.terre.milieu

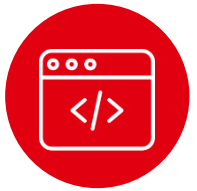
Installation durant l'interrogatoire

Non disponible sur les boutiques logicielles Android

Installation via l'activation de paramètres du téléphone

Permissions demandées

- android.permission.READ_CONTACTS
- android.permission.READ_CALL_LOG
- android.permission.INTERNET
- android.permission.READ_SMS
- android.permission.RECEIVE_SMS
- android.permission.READ_PHONE_STATE
- android.permission.READ_CALENDAR
- android.permission.ACCESS_WIFI_STATE
- com.android.voicemail.permission.READ_VOICEMAIL
- android.permission.BLUETOOTH



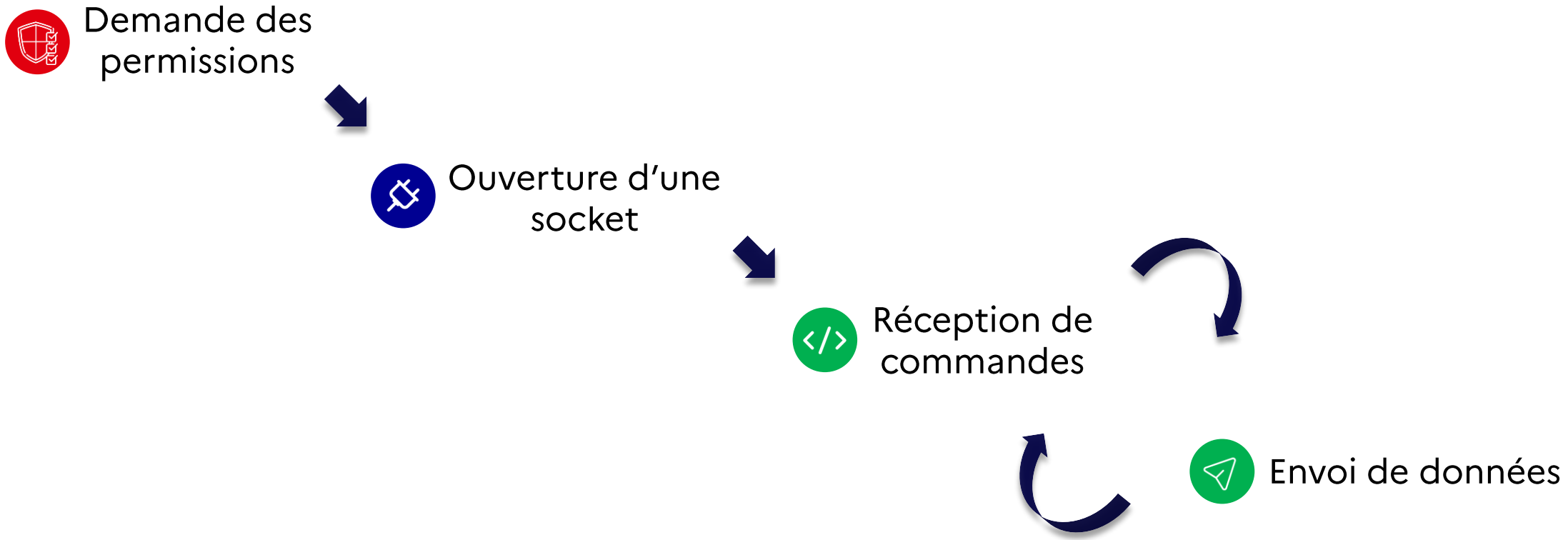
Camouflage du code de l'application

TLP:CLEAR

Présentation de l'application retrouvée

Terre du Milieu
com.terre.milieu

Structure globale



TLP:CLEAR

Présentation de l'application retrouvée

Protocole de transport via TCP

Terre du Milieu
com.terre.milieu

taille de la **charge utile**
uint32

charge utile
n *octets*

TLP:CLEAR

Présentation de l'application retrouvée

Structure des charges utiles de requêtes

Terre du Milieu
com.terre.milieu

taille de la **charge utile**
uint32

Code requête *1 octet*

Argument (optionnel, dépend de la requête) *1 octet*

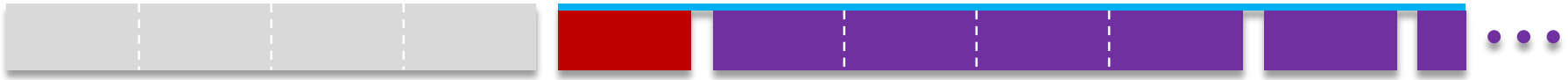
Possibilité de chainer les commandes

TLP:CLEAR

Présentation de l'application retrouvée

Structure des charges utiles de réponse

Terre du Milieu
com.terre.milieu



taille de la **charge utile**
uint32

Code réponse *1 octet*
Généralement le code requête + 1, ou code d'erreur

Réponse sérialisée taille dépendant du **code réponse**
Composé de byte, int32, int64, string, bool, blob

TLP:CLEAR

Présentation de l'application retrouvée

Terre du Milieu
com.terre.milieu

Commandes possibles

- Informations générales (opérateur, SIM, langue, build infos, MAC wifi & bluetooth, Ad ID, Android ID)
- Ping
- Comptes enregistrés
- Version du SDK Android
- Version de la release Android
- Activer/désactiver le mode verbeux
- **Requêter des données** (*cf.* diapo suivante)

TLP:CLEAR

Terre du Milieu
com.terre.milieu

Présentation de l'application retrouvée

Données requêtables

- **Contacts** (noms, numéros, emails, organisations, photos)
- **Historique d'appels** (correspondant et durée)
- **SMS** & **MMS** (stockés sur le téléphone et la carte SIM)
- **Calendrier** (détail des rendez-vous, participants)
- **Marque-pages** Google Chrome
- Historique de **recherche** Google Chrome
- Mots spécifiques au **dictionnaire** de l'utilisateur (clavier)
- **Emails** (contenu et pièces jointes de mails)
- **Applications** installées
- Wi-Fi ? *Non implémenté*

TLP:CLEAR

Terre du Milieu
com.terre.milieu

Présentation de l'application retrouvée

Bilan de la rétro-conception

- Levée de doute sur le type d'implant
  - Pas de **persistance**
  - Pas de **poterne logicielle**
- Liste exhaustive des données accédées
  - Très **intrusif**
  - Possible accès à des **données professionnelles sensibles**
  - Possibilité de **suivi *a posteriori*** via les identifiants publicitaires
- Ré-implémentation d'un client

TLP:CLEAR

Conclusion

Consultation

Du téléphone

Modification

Installation d'une application

Suivi de personne

Grâce aux informations récupérées

Attention

Perte du téléphone
Contrôle de police
Éloignement de ses appareils

Commanditaire

Tous types de pays

Tout type de supports

Ordinateurs
Téléphones
Objets connectés

TLP:CLEAR

Conclusion – Bonnes pratiques

MDM

Durcissement
du téléphone

BYOD

Séparation des utilisations
professionnelles / personnelles

Vigilance

Lorsque l'on n'est pas en
possession de son téléphone

Batterie

70% → 100% ??
70% → 40% ??
Éteindre son téléphone

Enveloppe sécurisée
scellée

Bonnes personnes
informées

TLP:CLEAR

Merci pour votre attention

Questions ?

Pour nous rejoindre

recrutement-cyber@interieur.gouv.fr

TLP:CLEAR