Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère
éducation
nationale
jeunesse
vie associative

PNF
21 janvier
2020

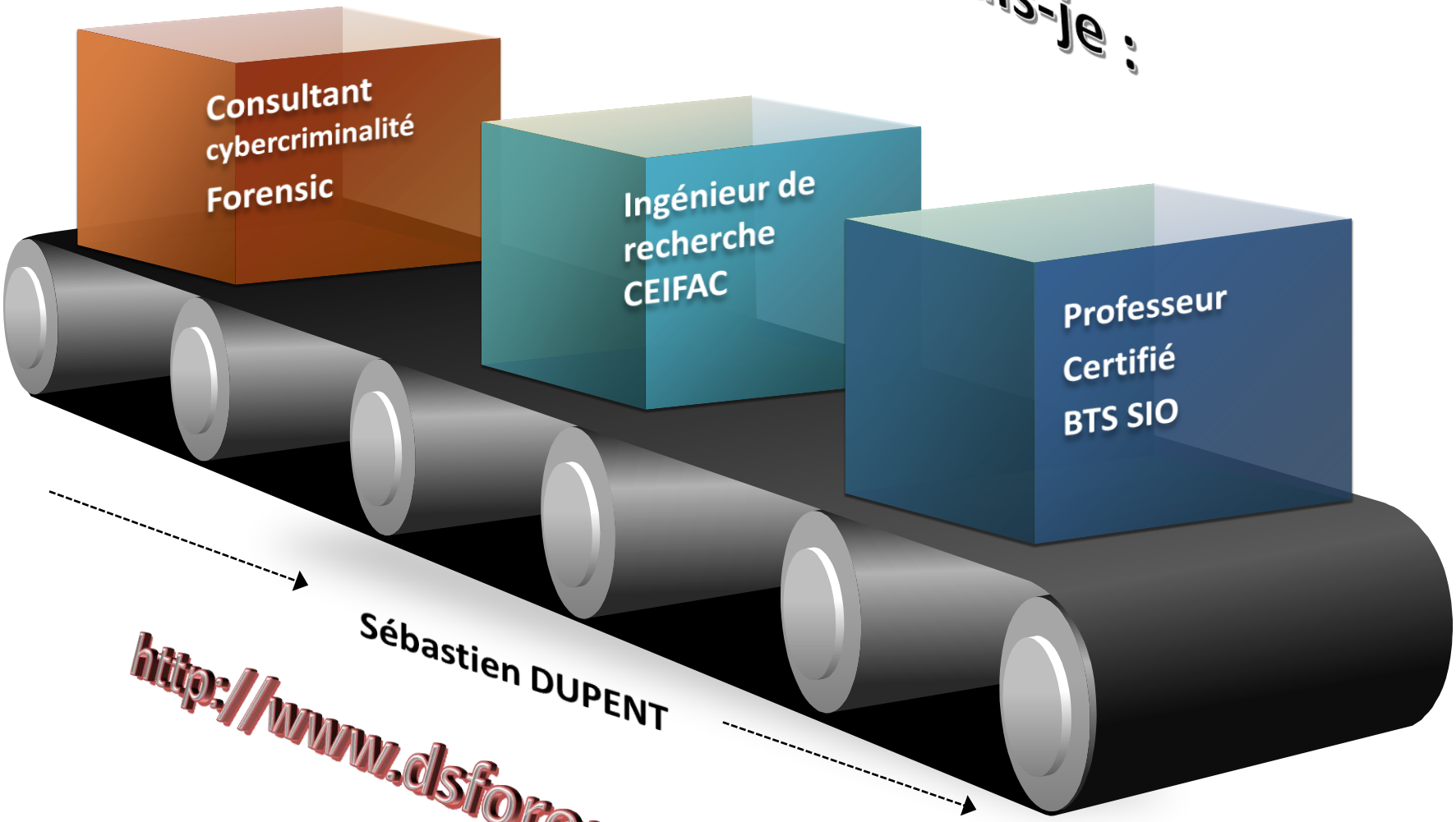
Domaine d'activité 3

Cybersécurité des services informatiques

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale jeunesse vie associative

Qui suis-je :



Sébastien DUPENT

http://www.dsforensic.fr

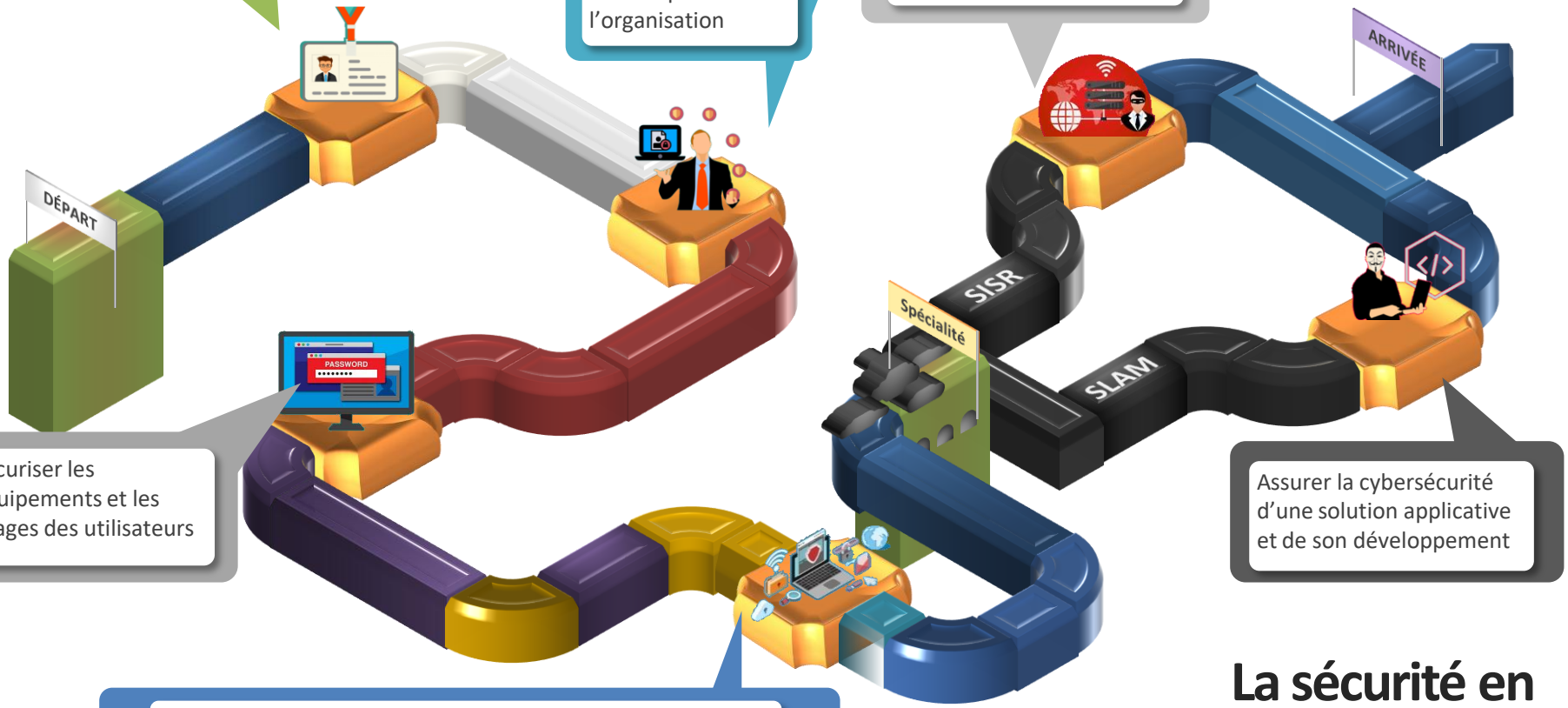
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère
éducation
nationale
jeunesse
vie associative

Protéger les données à caractère personnel

Préserver l'identité numérique de l'organisation

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service



Sécuriser les équipements et les usages des utilisateurs

Assurer la cybersécurité d'une solution applicative et de son développement

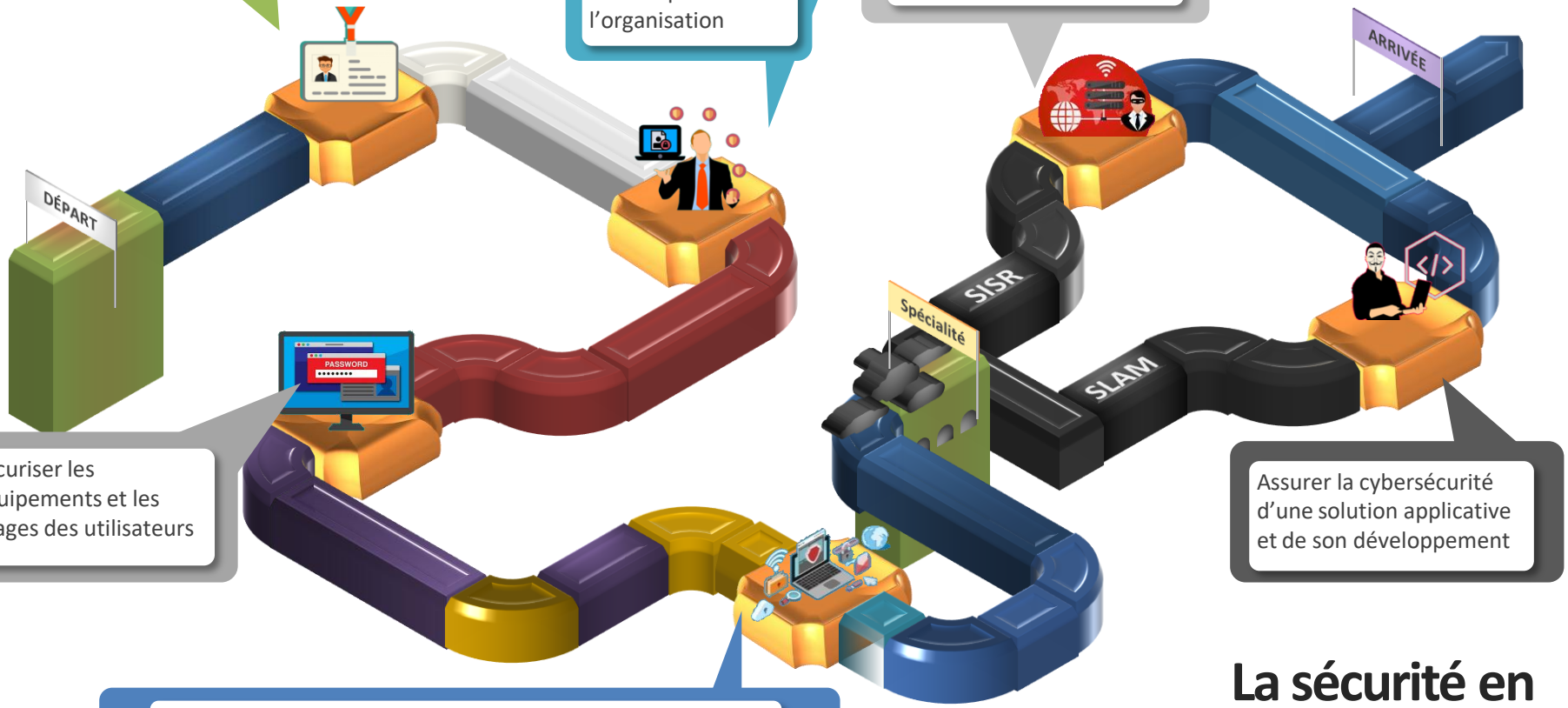
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

La sécurité en BTS SIO

Protéger les données à caractère personnel

Préserver l'identité numérique de l'organisation

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service



Sécuriser les équipements et les usages des utilisateurs

Assurer la cybersécurité d'une solution applicative et de son développement

Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

La sécurité en BTS SIO

LES BONS RÉFLEXES DE LA PROTECTION DES DONNÉES PERSONNELLES

Ne collecter que les données vraiment nécessaires

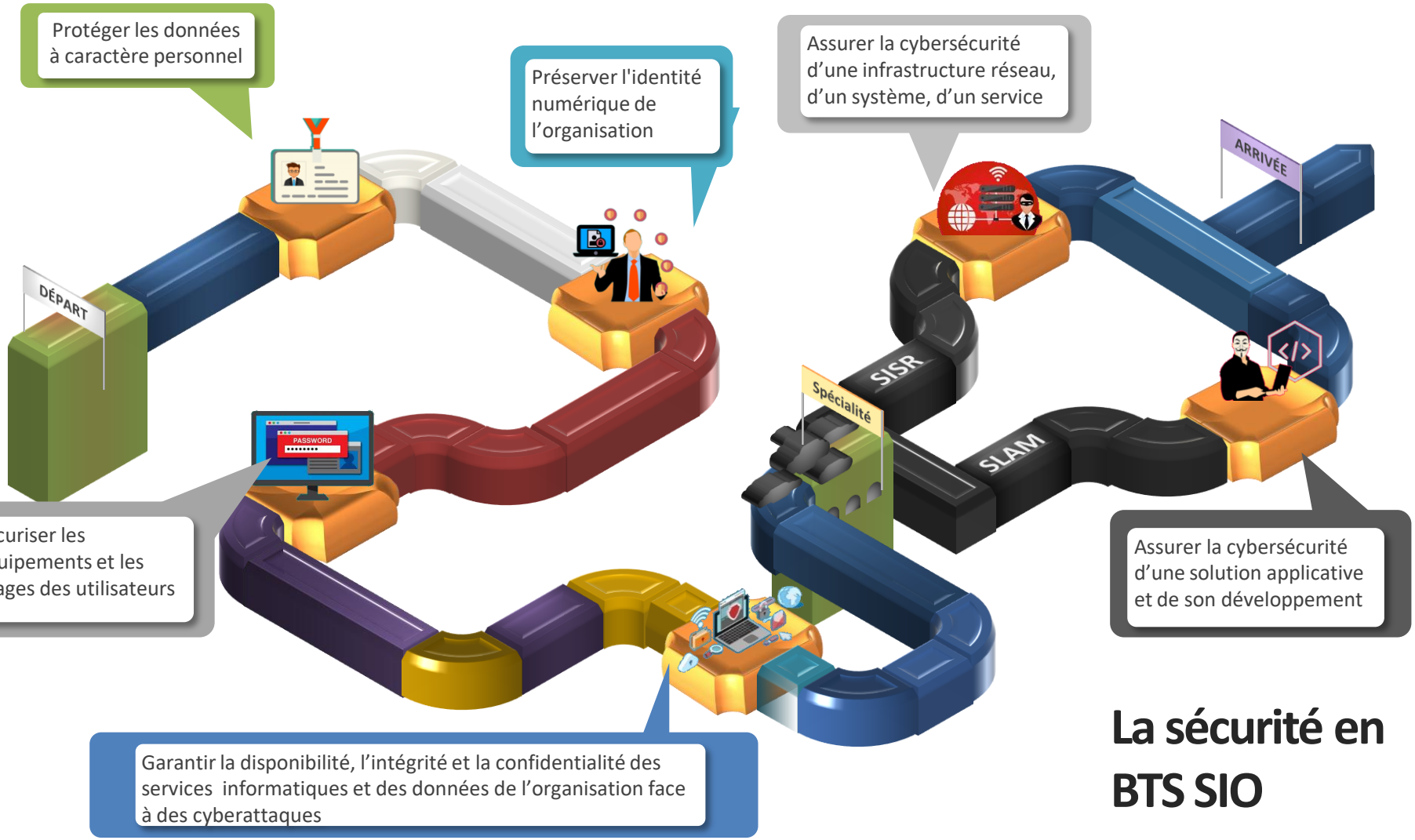
Information claire et complète

Répondre dans les meilleurs délais aux demandes de consultation, de rectification ou de suppression des données

Le partage et la circulation des données personnelles doivent être encadrés et contractualisés

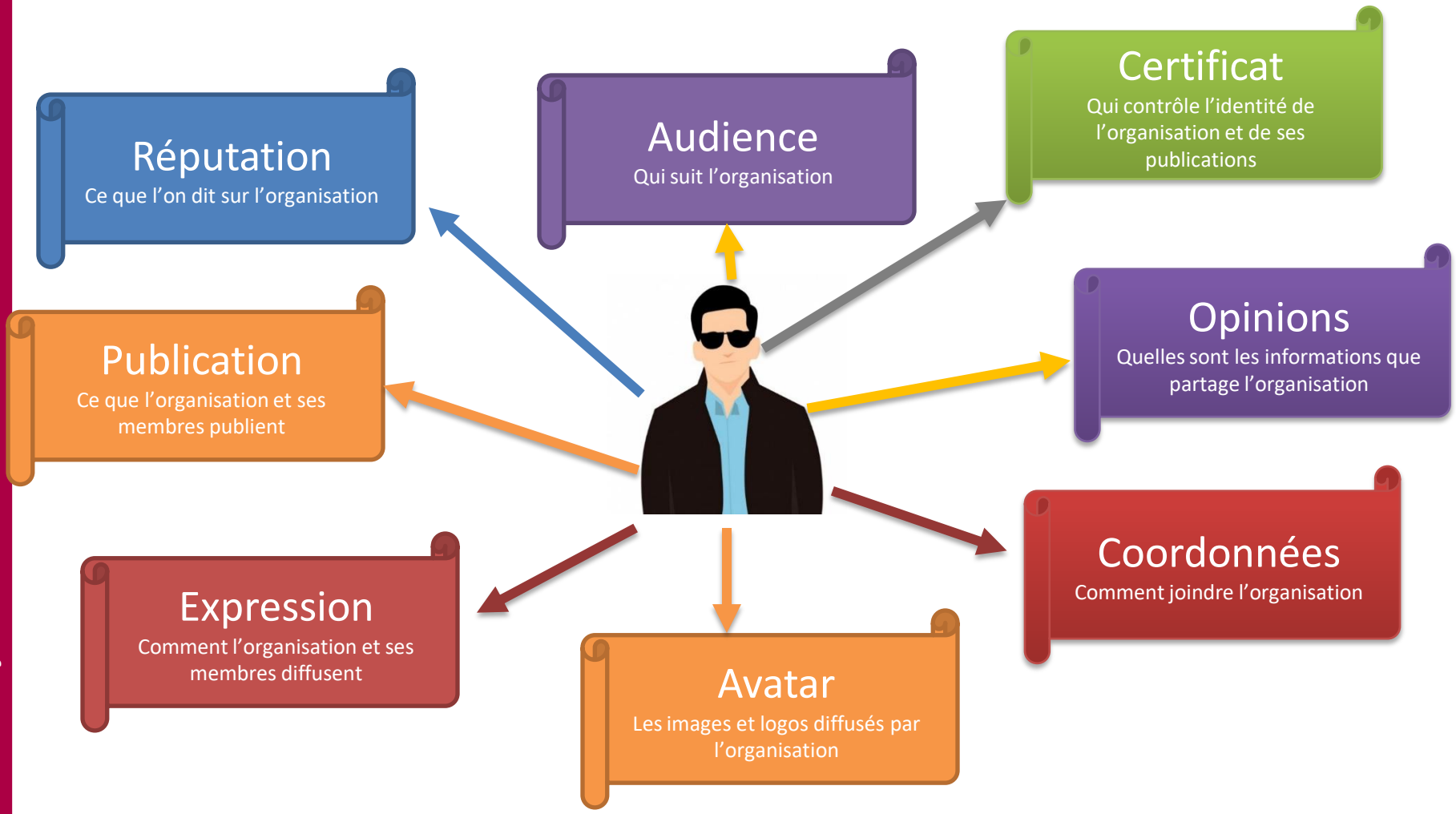
Mise en place de mesures spécifiques

Adapter en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

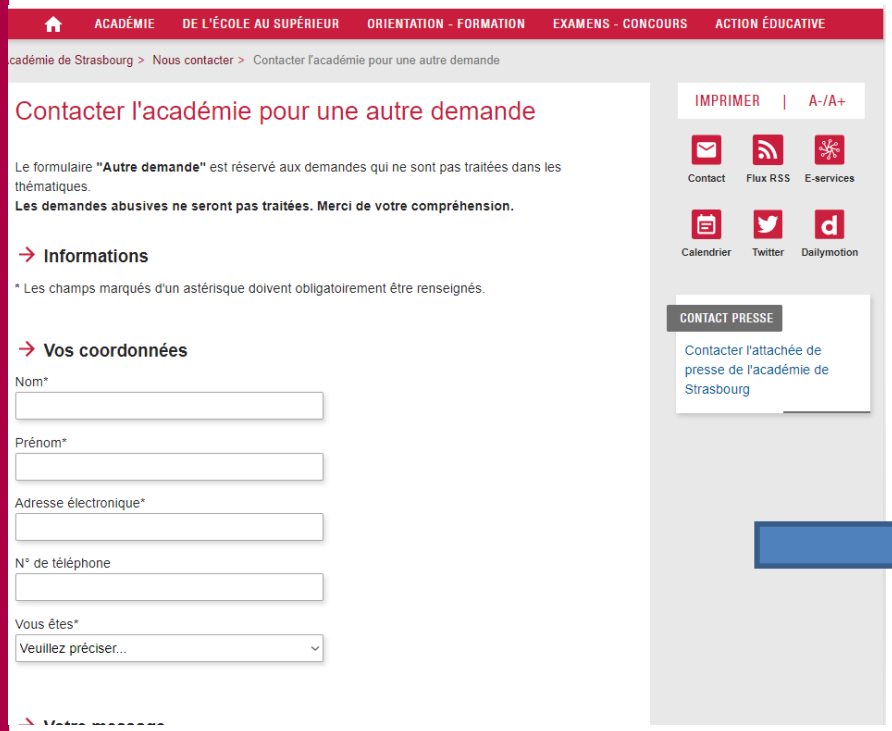


La sécurité en BTS SIO

L'identité numérique



Exemple par le plagiat → phishing

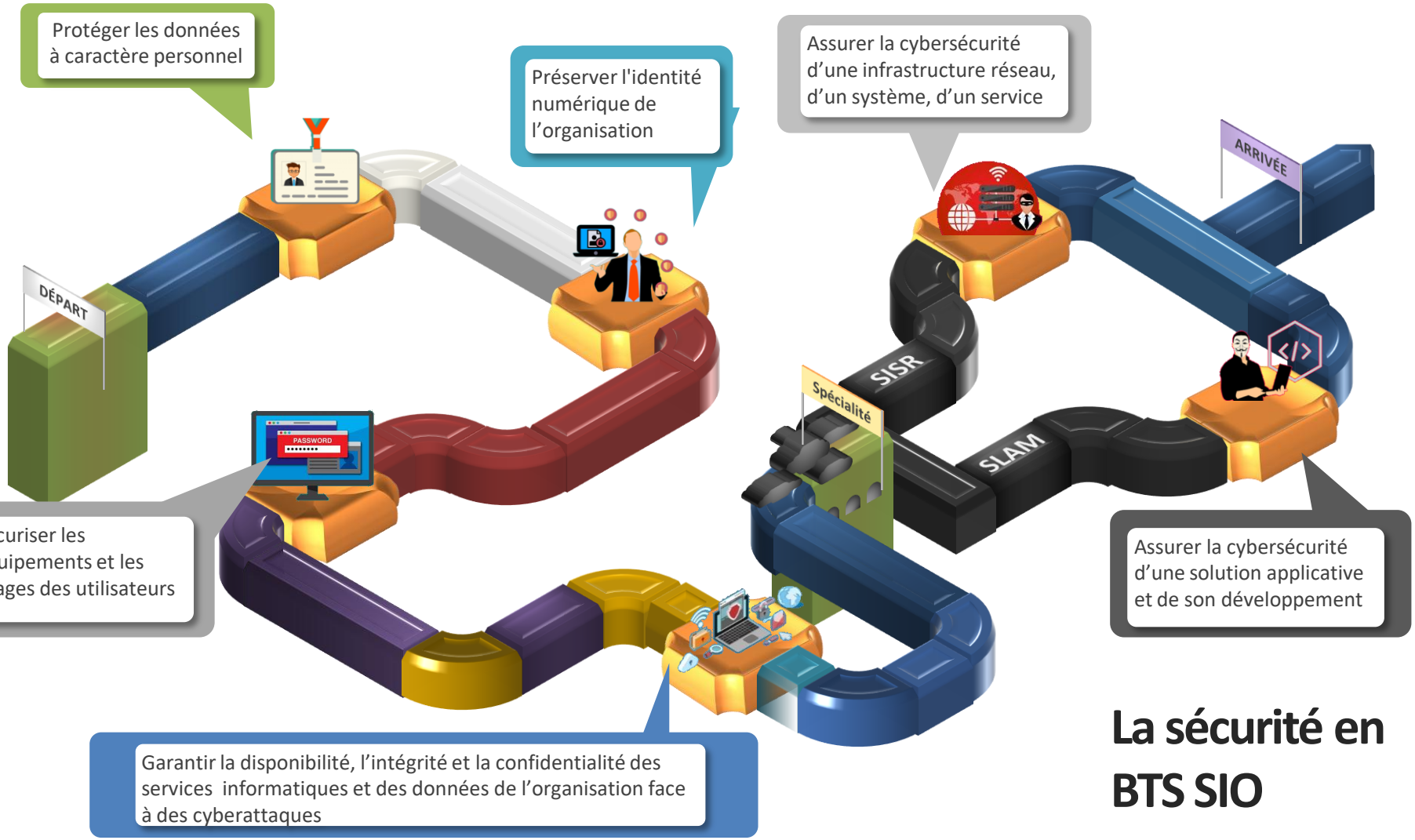


LES TYPOSQUATTAGES

acstrasbourg.**com**	DISPONIBLE	1 an	19,90 €/an
ac-strasbourg.**paris**	DISPONIBLE	1 an	49,90 €/an
acstrasbourg.**paris**	DISPONIBLE	1 an	49,90 €/an
ac-strasbourg.**net**	DISPONIBLE	1 an	19,90 €/an
acstrasbourg.**net**	DISPONIBLE	1 an	19,90 €/an
ac-strasbourg.**eu**	DISPONIBLE	1 an	19,90 €/an
ac-strasbourg.**alsace**	DISPONIBLE	1 an	75,00 €/an
acstrasbourg.**alsace**	DISPONIBLE	1 an	75,00 €/an

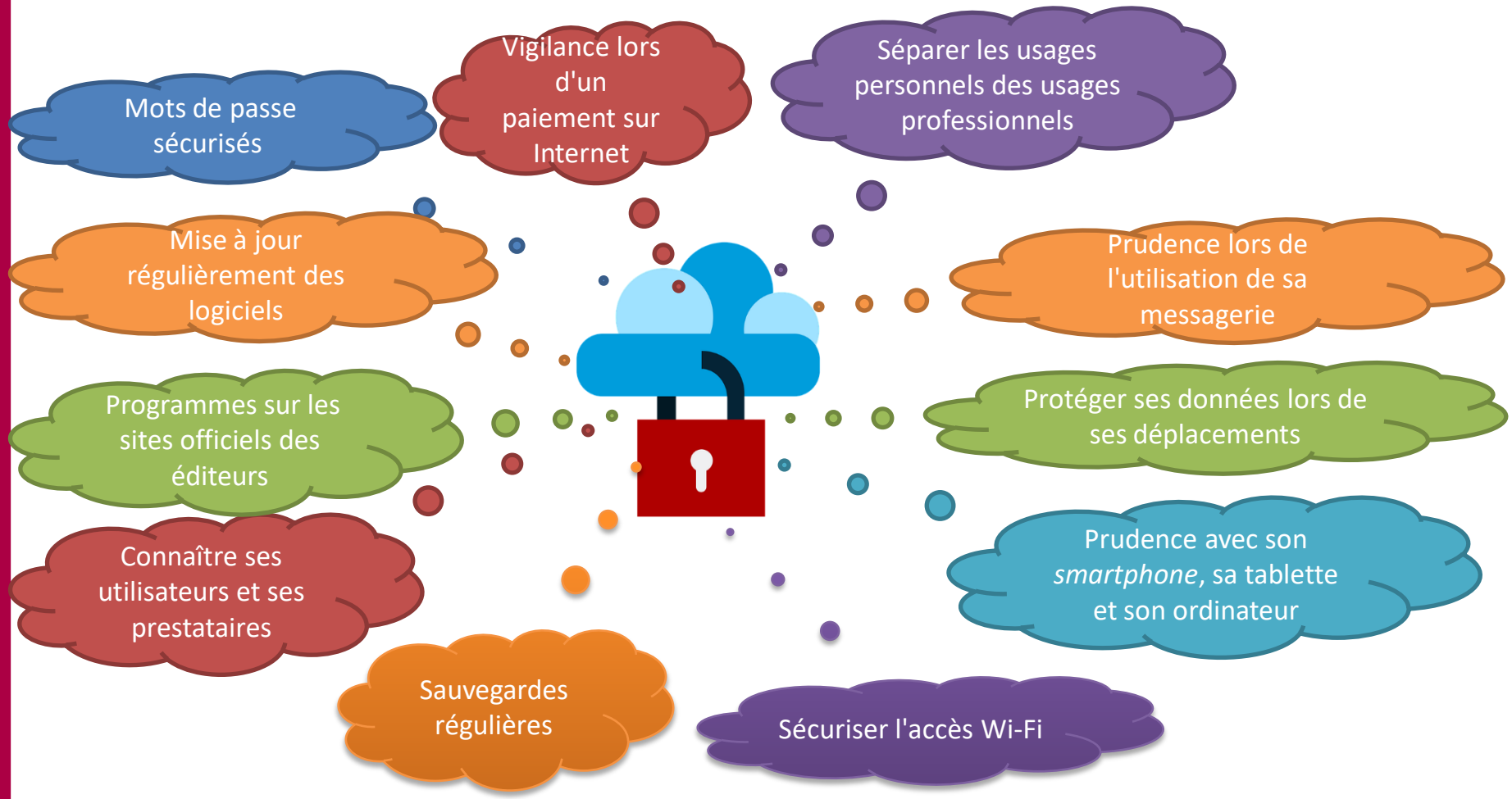
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale jeunesse vie associative



La sécurité en BTS SIO

Les recommandations



Les mots de passe

12345
1234567
12345678
123456789 123123 555555
7777777
111111
654321
abc123
1q2w3e4r
qwerty
qwerty123
qwertyuiop admin
password princess
iloveyou
1q2w3e4r
password1 888888
lovely

Faire tester leur mot de passe aux élèves

http://www.passwordmeter.com

Test Your Password		Minimum Requirements
Password:	•••••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 28
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 16
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	6	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

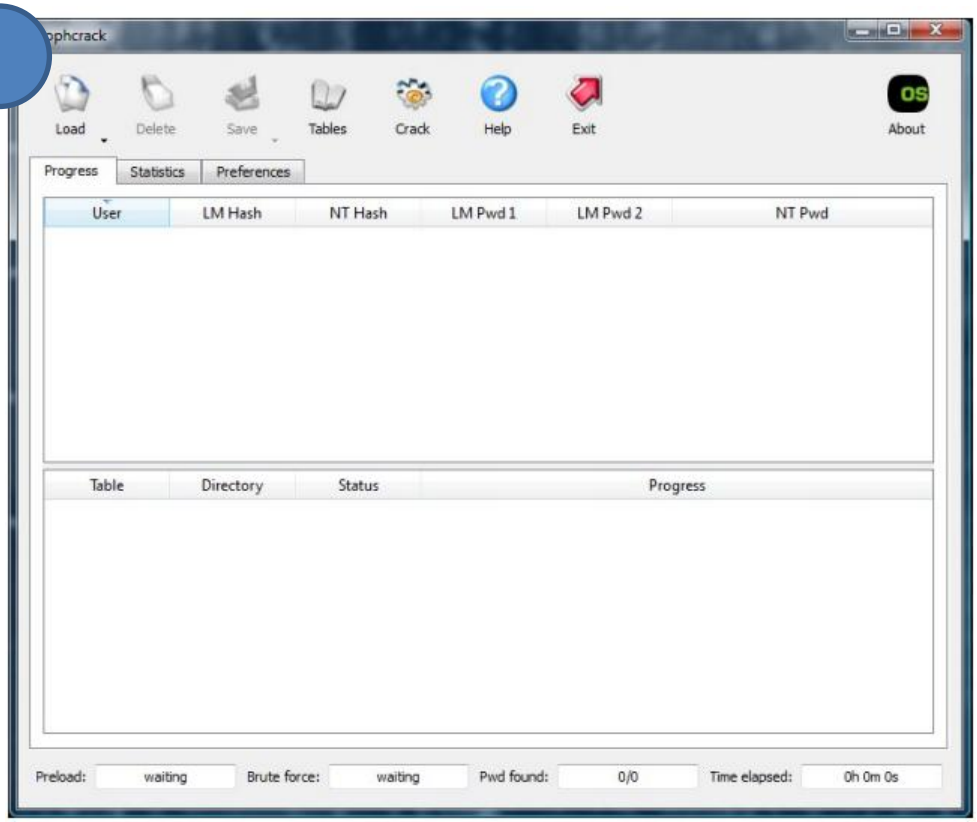
Craquer des mots de passe

Demander aux élèves de craquer le mot de passe d'une machine virtuelle sous Windows

Avec par exemple Ophcrack

http://pignon.camille.free.fr/save/Ophcrack%20tutorial.pdf

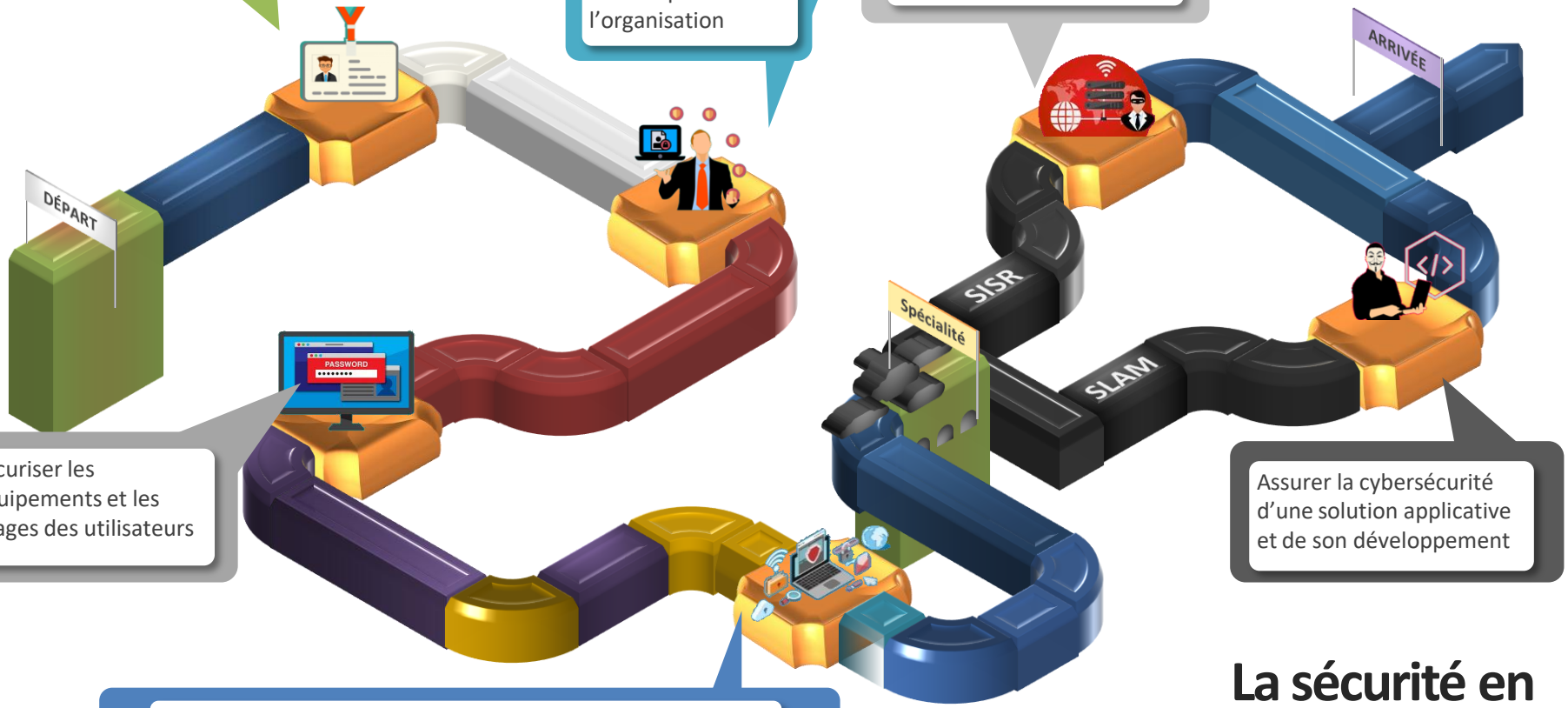
(autre logiciel possible : John the Ripper, Cain and Abel, THC Hydra)



Protéger les données à caractère personnel

Préserver l'identité numérique de l'organisation

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service



Sécuriser les équipements et les usages des utilisateurs

Assurer la cybersécurité d'une solution applicative et de son développement

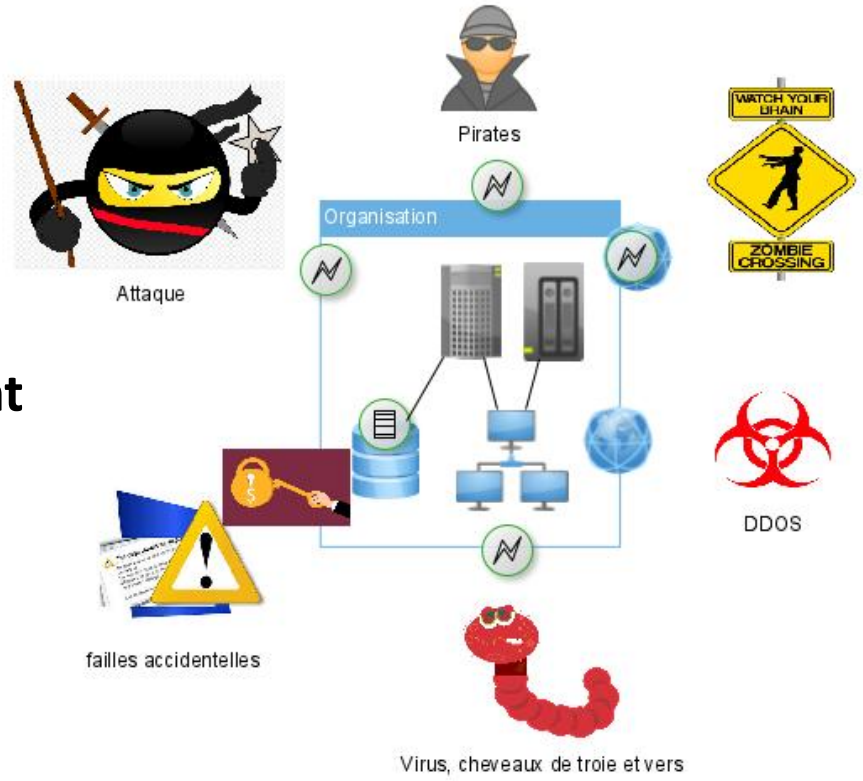
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

La sécurité en BTS SIO

Modélisation / Cartographie des risques

Identification des menaces potentielles telles que les vulnérabilités structurelles qui peuvent être identifiées.

Celles-ci doivent être énumérées et classées par priorité

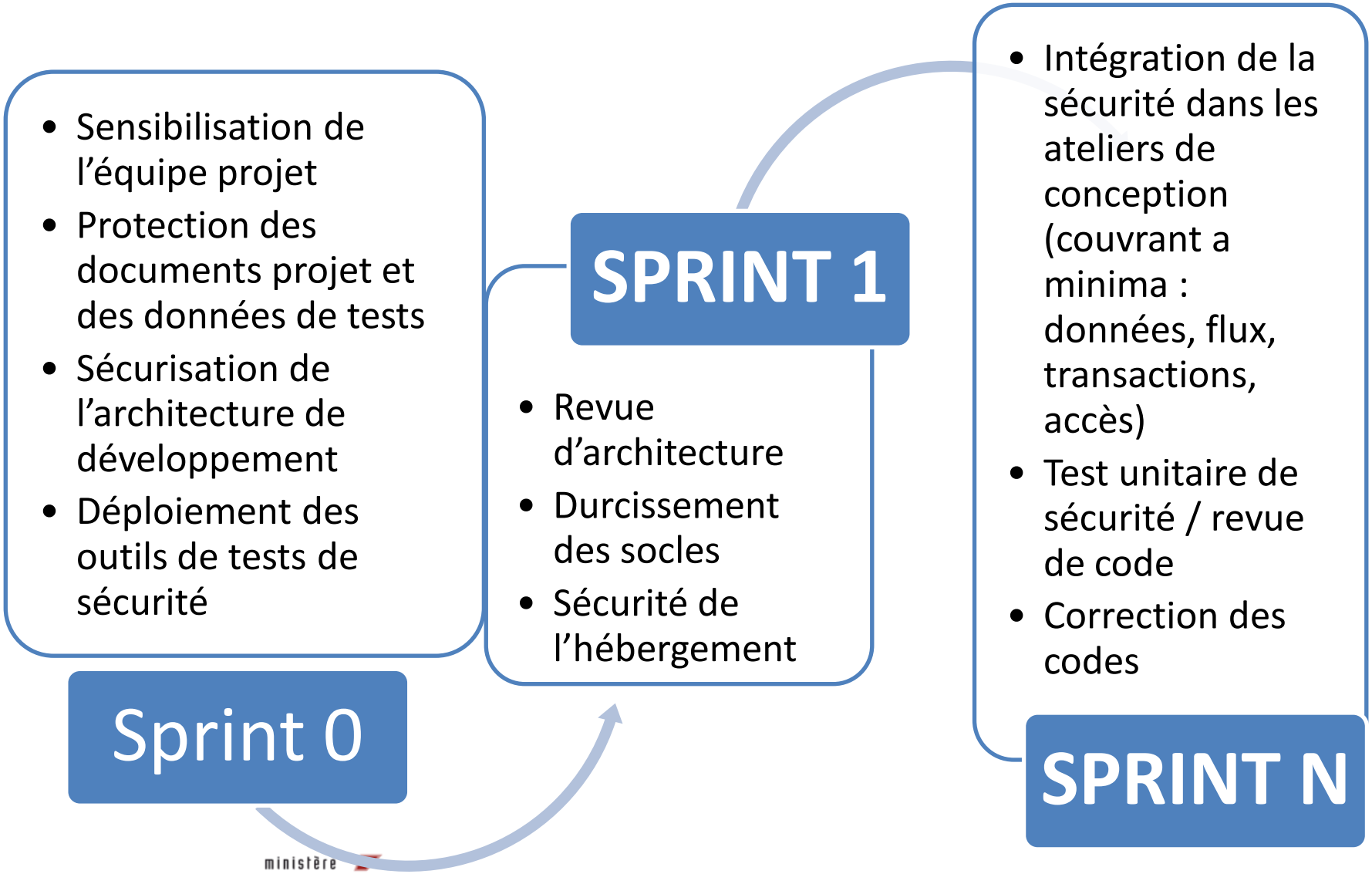


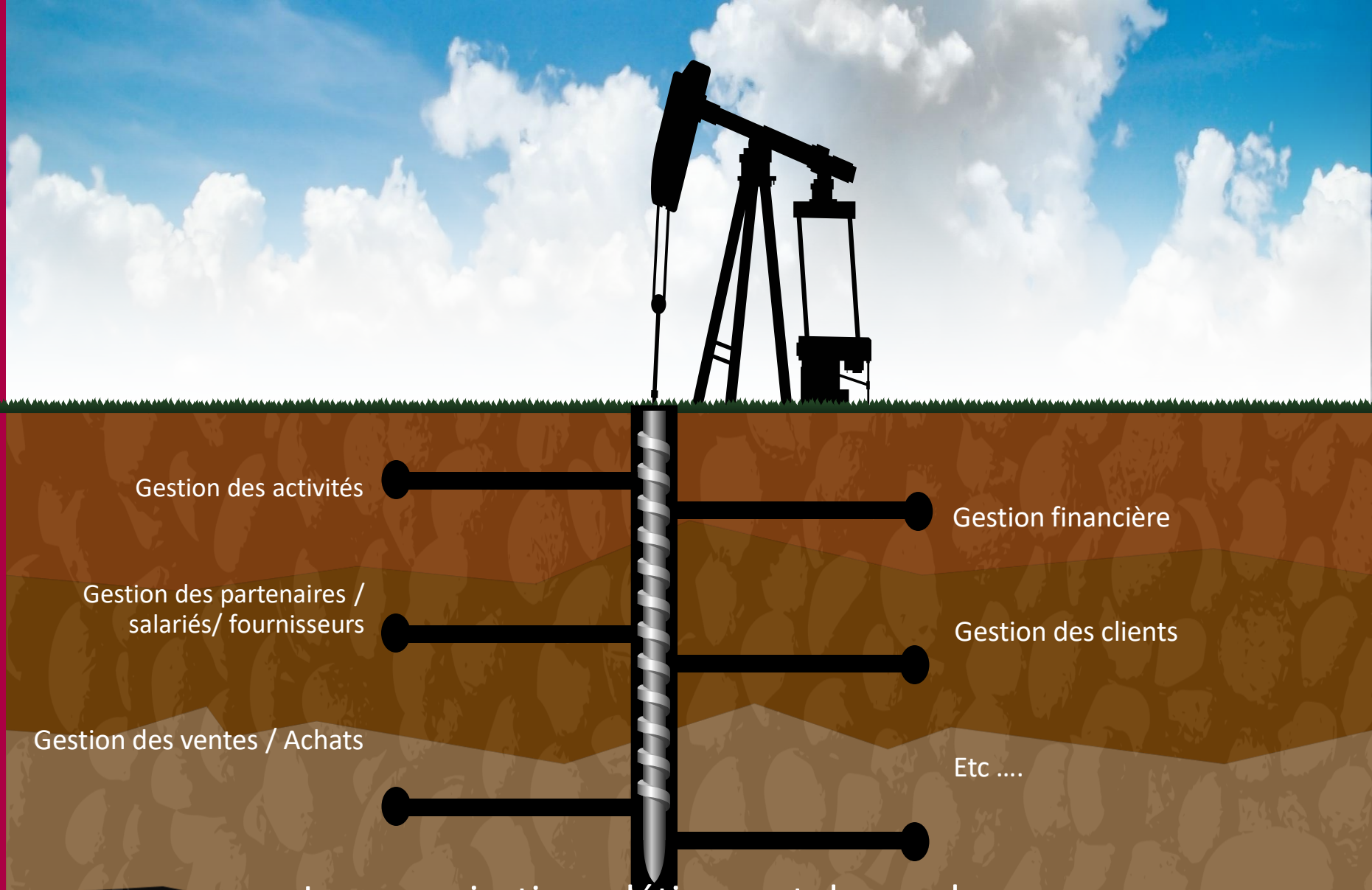
Modélisation / Cartographie des risques

Les différentes méthodes

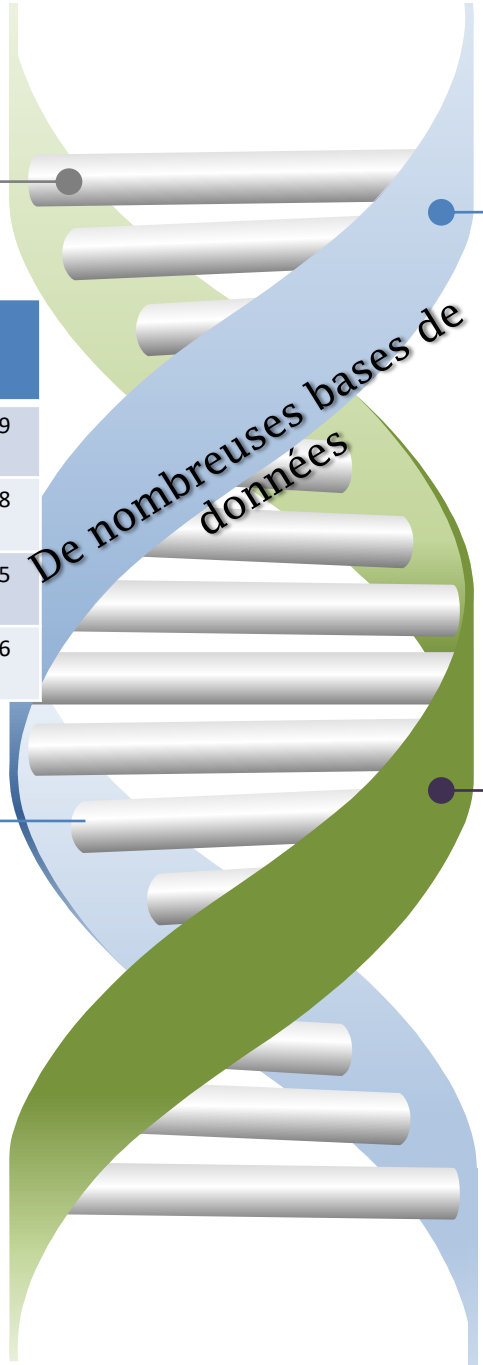
- STRIDE
- P.A.S.T.A
- TRIKE
- VAST
- ISO/CEI 27005

sécurité en mode agile





Les organisations détiennent de nombreuses données



Reservation

Id	Nom	Prénom	Événement	Nb Place	N°Carte
1	DURAND	Jean	St lucie	5	5857587289
2	DAMIENS	David	Poterie	2	8668668768
3	LAMBERT	Thierry	Waldfescht	10	9667518685
4	SCHMITT	Stephane	Thé dansant	4	2986521486

Visiteur

Id	Nom	Prénom	Mail	Adresse	Dernier cnx
1	DURAND	Jean	J_durand85@gmail.com	10 Rue de la paix	08/12/15
2	DAMIENS	David	Dam_dav@outlook.fr	2 Rue de l'Eglise	01/09/19
3	LAMBERT	Thierry	Lambert_th80@yahoo.fr	45, rue du poisson	15/10/19
4	SCHMITT	Stephane	Steph-schm@orange.fr	70, rue de l'espace	10/06/19

Événement

Id	Libelle	Date	Association
1	St Lucie	15/12/15	OMACL
2	Poterie	10/08/19	OMACL
3	Waldfescht	21/08/19	ANO
4	Thé dansant	20/01/19	BRUNEBARRI

Association

Id	Nom	Président	Adresse
1	OMACL	David Legrand	Mairie de soufflenheim
2	ANO	Patrick Muller	Chalet de la forêt
3	BRUNEBARRI	Eric Kauffman	Ancienne gendarmerie
4	Foot	Fabrice Martin	Stade de Foot

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale jeunesse vie associative

Mise en conformité

Authentifier les utilisateurs
Gérer les habilitations

Réplication

Optimisation

Confidentialité

Anonymisation

Intégrité

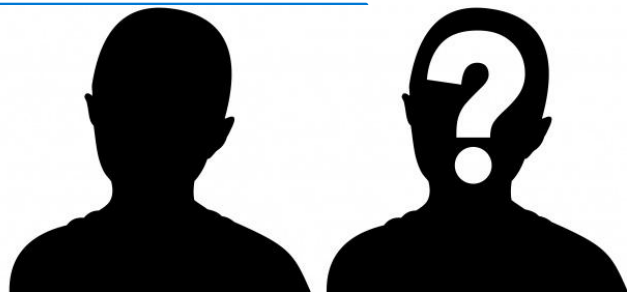
Disponibilité

Forme normale

Pseudonymisation
le chiffrement
Anonymisation
floutage

Sauvegarde

Anonymisation



Les informations d'identification ou critiques ne doivent pas être consultables ou utilisées hors des traitements pour lesquelles elles sont destinées

Anonymisation ou masquage

Permet de transformer les données personnelles de façon à ce que l'on ne puisse pas identifier des personnes.
On utilise ce procédé généralement lors de l'externalisation des informations pour des buts statistiques.
Cette technique permet de s'affranchir du RGPD.

Pseudonymisation

C'est le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires.

Floutage

C'est le traitement qui consiste à rendre invisibles les informations nominatives des bases de données et fichiers clients.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale jeunesse vie associative

Les vulnérabilité du site

Base de données

Injection SQL

Publication commentaire

Attaque XSS

Connexion

Mots de passe et protection

Données

Failles de sécurité des identifiants de données visualisées

Mauvaise configuration de la sécurité

Failles de configuration liées aux serveurs *Web*

Fonctionnalité

Failles de sécurité liées aux accès de fonctionnalité

Composant vulnérable

Failles liées à l'utilisation de composants tiers

Redirections et contrats à terme non validés

Failles liées aux redirections et transmission générique des applications.

Archive et suivi des utilisateurs

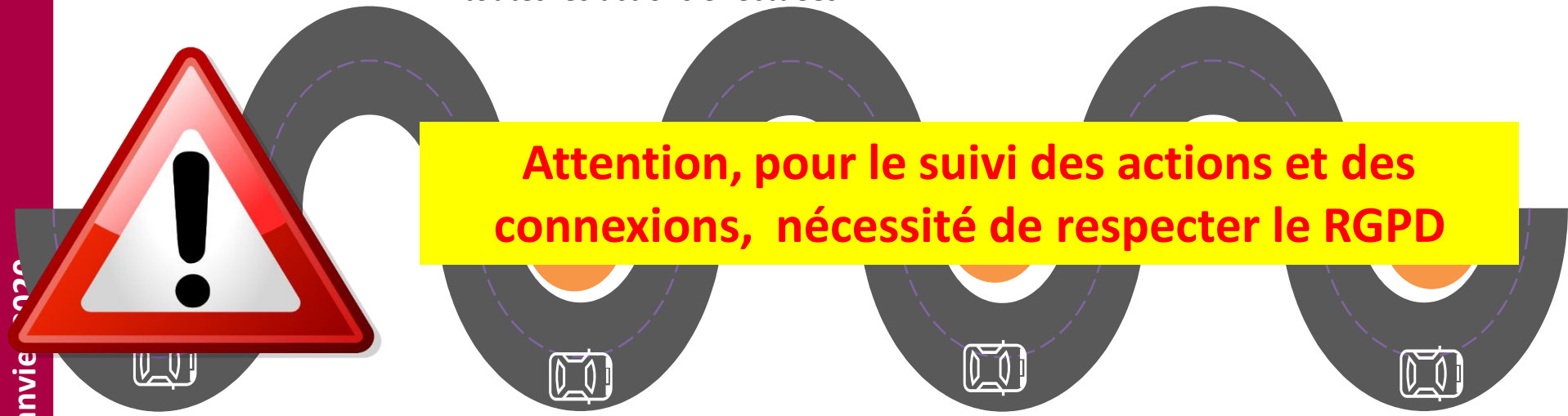
Du fait des données de gestion, mais aussi du nombre important d'utilisateurs, il est essentiel d'effectuer des sauvegardes et des suivis

Archive

- Il faut créer pour chaque table sensible une table qui contient toutes les actions effectuées

Log

- Mettre en place dans le programme des logs



Attention, pour le suivi des actions et des connexions, nécessité de respecter le RGPD

Sauvegarde

- Il faut mettre en place une sauvegarde régulière de la base de données et aussi du site

Suivi des actions

- Dans toutes les tables, mettre des champs création, modification avec l'utilisateur et la date/heure

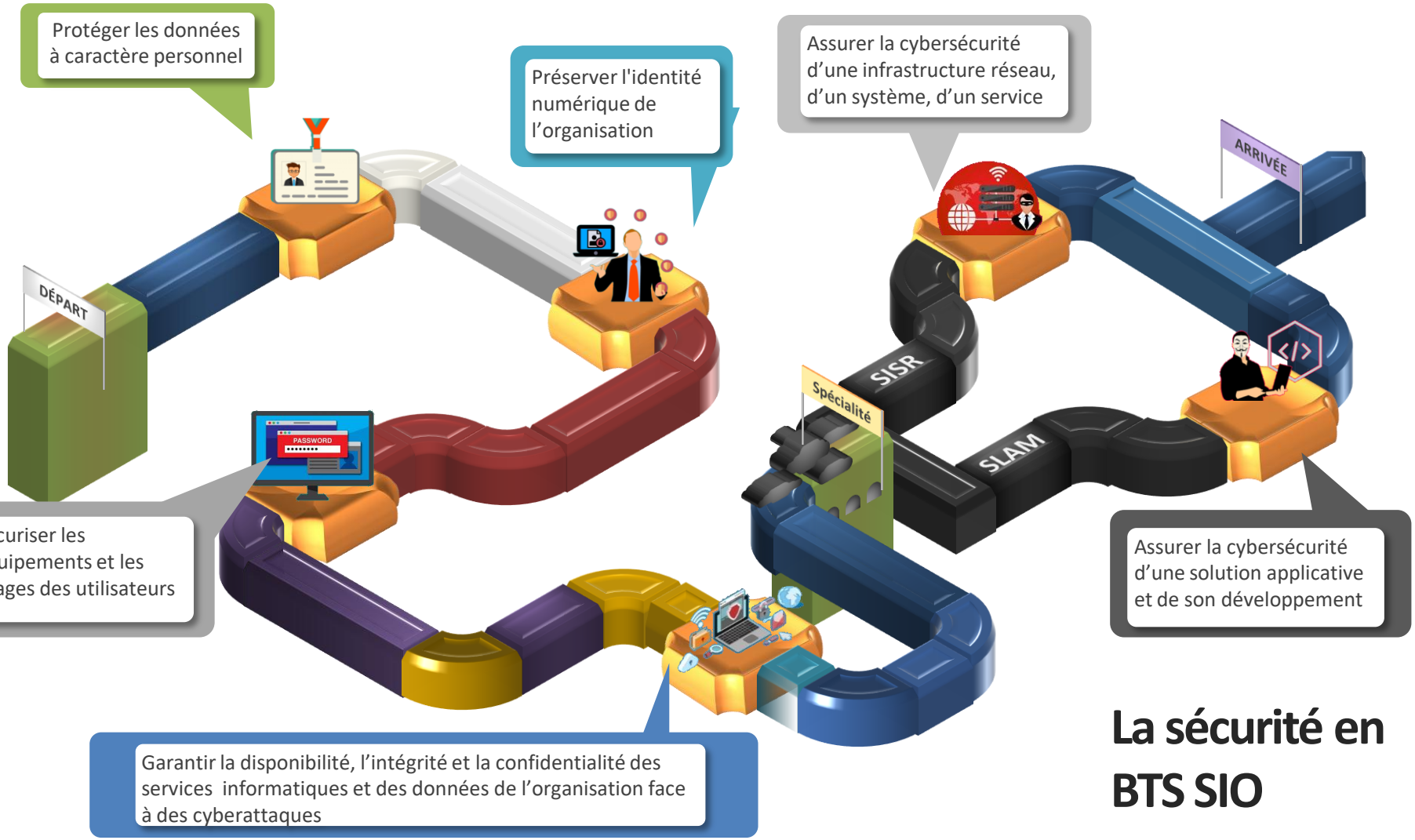
Redondance des informations

Atout

- mesures de protection et de prévention d'atteinte à l'intégrité des données, la perte irrécupérable d'informations

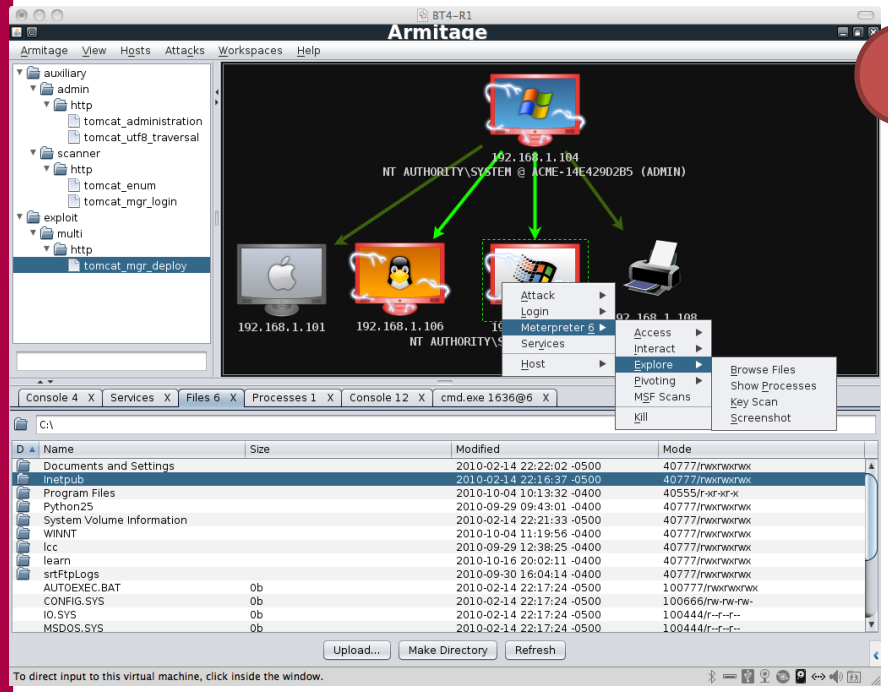
Risque

- données stratégiques éparpillées
- données non cohérentes



La sécurité en BTS SIO

Exploiter les vulnérabilités des systèmes informatiques



L'utilisation de l'outil Metasploit, en particulier à l'aide de l'interface Armitage, est un très bon moyen de démontrer les différentes vulnérabilités des systèmes informatiques par l'analyse des attaques d'hameçonnage : trace réseau, analyse des postes, détection de l'attaquant, tests d'intrusion.

Exploitation des erreurs de développement

Explorer les problèmes des informations révélées à la suite d'une gestion des erreurs mal implémentée.

Par exemple : Un algorithme d'authentification de mot de passe qui vérifie la saisie de façon séquentielle. Cela veut dire qu'il analyse le séquencement des échecs permettant d'identifier à quel moment dans la chaîne du mot de passe l'échec s'est produit. Il est alors possible de deviner le mot de passe une lettre à la fois.

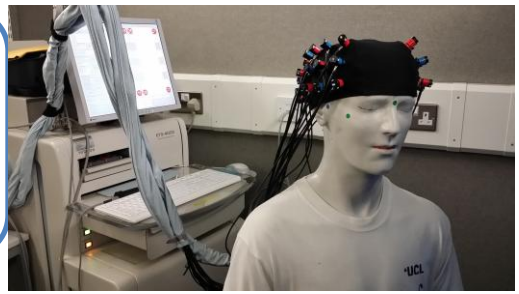
test de pénétration

Pentesting Black-Box

- Simulation d'une attaque externe, donnant un tout petit peu d'informations sur les systèmes à tester (à l'exception des intervalles d'adresses IP ou le nom de domaine).

Pentesting White-Box

- Simulation d'une attaque interne, connaissance complète sur le réseau/système cible, incluant le schéma d'adresses IP, code source, détails des systèmes d'exploitation.



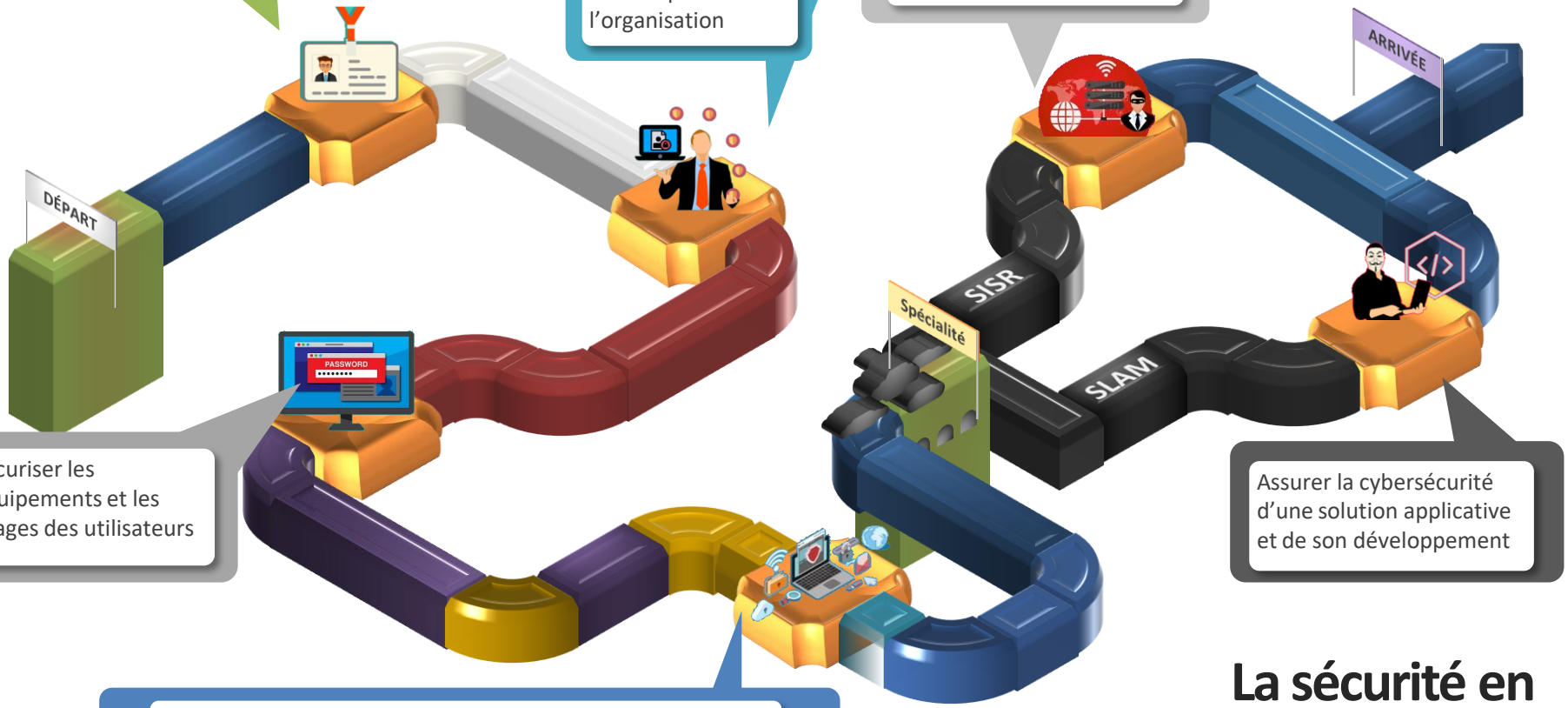
Pentesting Gray-Box

- approche hybride : le testeur dispose normalement d'informations limitées à propos du réseau/système cibles

Protéger les données à caractère personnel

Préserver l'identité numérique de l'organisation

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

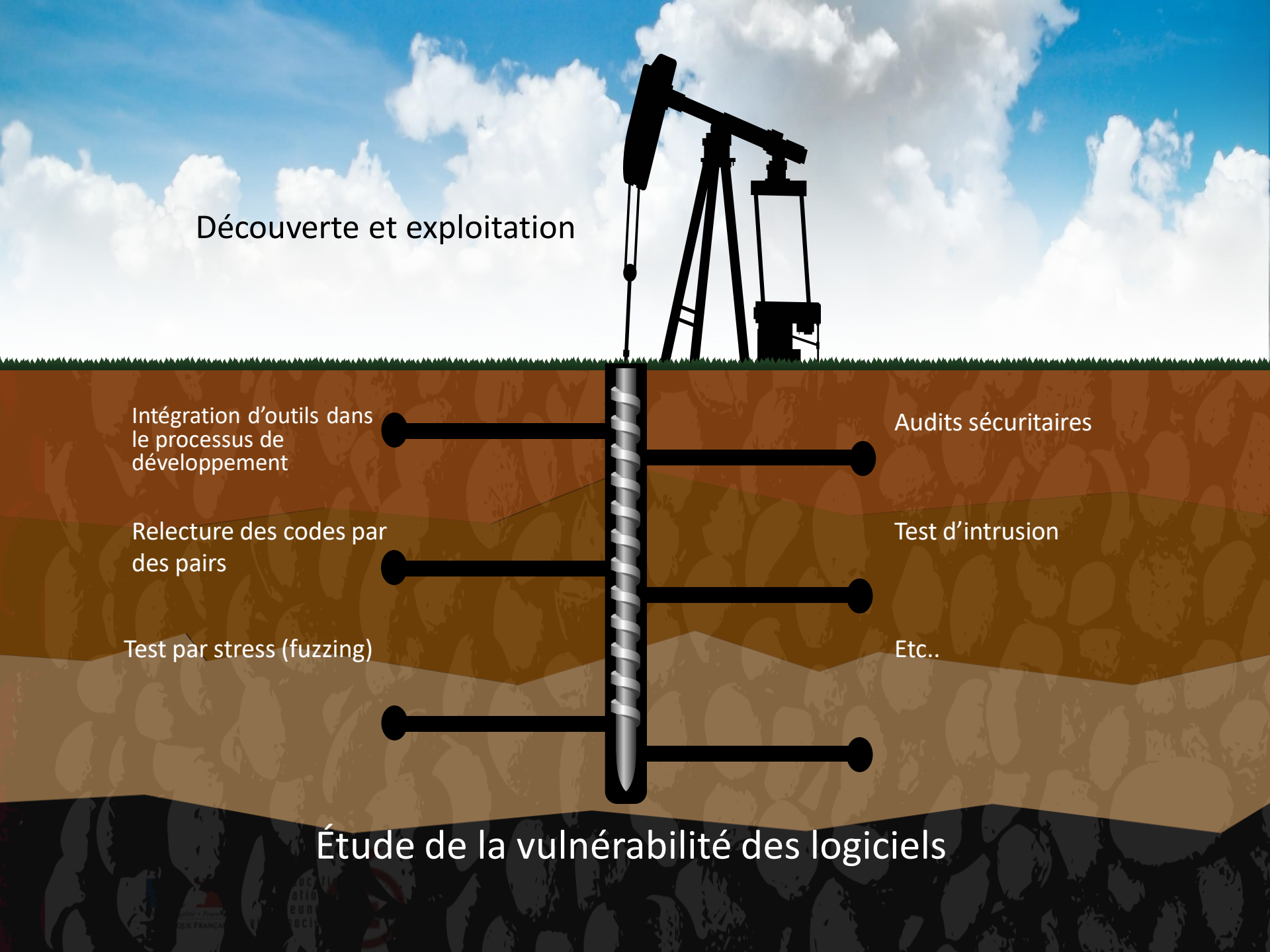


Sécuriser les équipements et les usages des utilisateurs

Assurer la cybersécurité d'une solution applicative et de son développement

Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

La sécurité en BTS SIO


Découverte et exploitation
Intégration d'outils dans le processus de développement
Relecture des codes par des pairs
Test par stress (fuzzing)
Audits sécuritaires
Test d'intrusion
Etc..
Étude de la vulnérabilité des logiciels

Utilisation des bogues (bugs) logiciels

Techniques utilisées pour la recherche de vulnérabilité. Son principe est simple, on vérifie toutes les entrées possibles pour l'application.

Utilisation de la méthode fuzzing pour trouver des vulnérabilités logicielles, par exemple à l'aide de logiciels tels que SCRATCH (http://packetstormsecurity.org/UNIX/misc/scratch.rar)

puis, utiliser ces erreurs pour contrôler l'exécution d'un logiciel et effectuer des modifications, par exemple, dans une base de données ou accéder à des données confidentielles

Utilisation du Forensic computer

Utilisation du logiciel Autopsy pour identifier des problèmes de sécurité dans les implémentations des logiciels, en particulier dans les cas où les programmeurs ne prennent pas en compte le fonctionnement des fichiers des systèmes d'exploitation lorsqu'ils tentent de supprimer des informations critiques.

Étude de la vulnérabilité des logiciels

Les ressources risquées

Limitation erronée de chemin

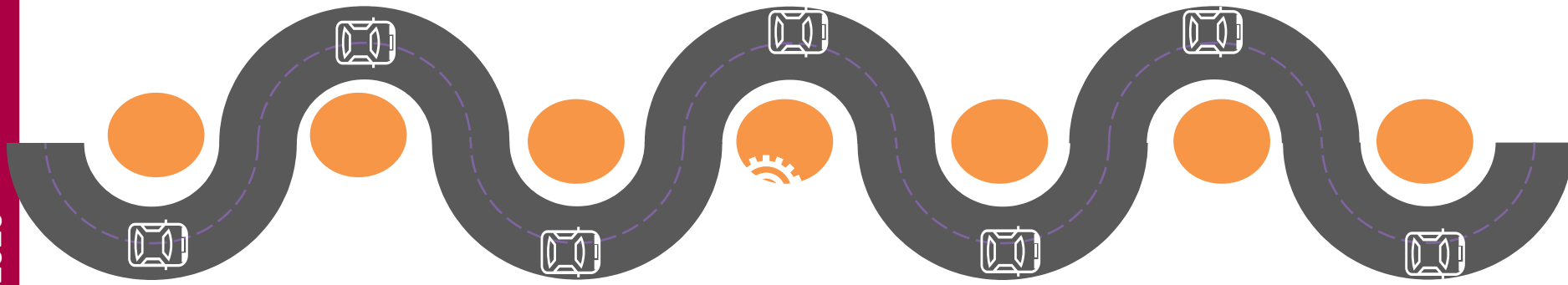
- Un utilisateur peut accéder à des données se situant dans des répertoires qui lui sont interdits

Inclusion d'une fonctionnalité corrompue

- Utilisation d'une bibliothèque corrompue

Débordement d'un entier

- Vulnérabilité touchant OpenSSH (versions 2.9.9 à 3.3)



Débordement de tampons

- Exemple vulnérabilité dans la pile de fonction getaddrinfo bibliothèque glibc

Téléchargement sans contrôle d'intégrité

- Virus suite fausse mise à jour Firefox

Calcul incorrect de la taille d'un tampon

- Exemple d'ariane 5

Chaîne de formatage incontrôlée

- https://www.cgsecurity.org/Articles/SecProg/Art4/index-fr.html

Étude de la vulnérabilité des logiciels

Défense poreuse

- Mauvaise authentification
- Aucun mécanisme d'autorisation
- Mise en place d'un profil de connexion figé dans le code
- Absence de chiffrement
- Décision basée sur des données non fiables
- Mauvais contrôle d'accès
- Demandes d'authentification répétées
- Algorithme cryptographique non fiable
- Mécanismes inappropriés pour prévenir les demandes d'authentification répétées
- Fonction de hashage sans « salt »

Les Rendez-vous

FIC 2020
28, 29 et 30 janvier 2020
Lille

Conférence / Table ronde du CEIFAC sur la cybercriminalité le 2 avril 2020 Université de Strasbourg
(Approche légale/panorama/typologie
Approche technique
Protection des victimes)