WAVESTONE

Introduction à la Sécurité des Systèmes d'Information en entreprise

Attaques et bonnes pratiques concrètes

25/09/2019

Carole CORDIER
Carole.cordier@wavestone.com

Cyril MANSOUR
cyril.mansour@wavestone.com
@MansourCyril

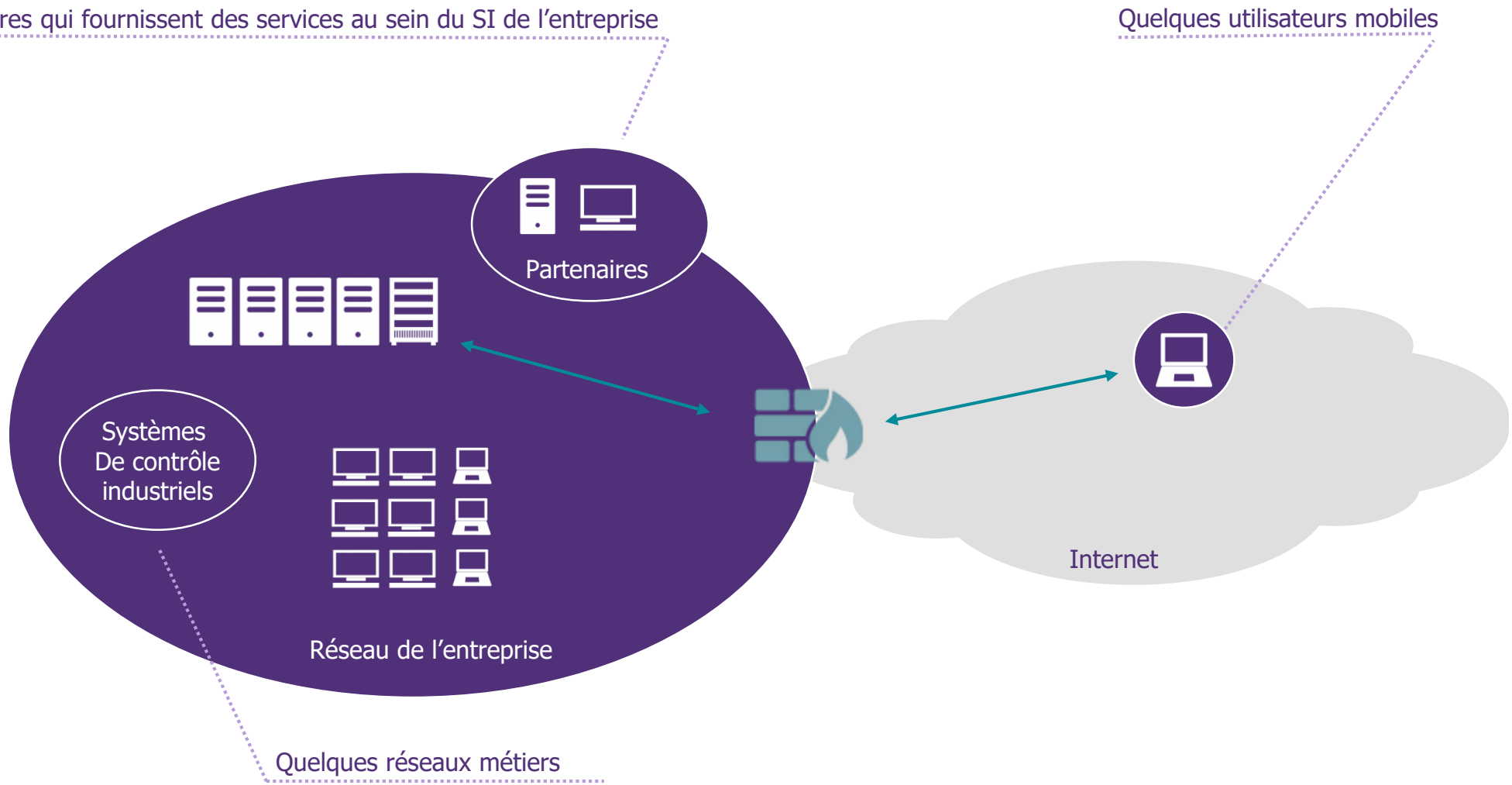
AGENDA


C’est quoi un SI ?

Pour vous, c’est quoi un SI ?

Qu'est-ce *nous avons fait* **jusqu'à maintenant ?**

Un Système d'Information centralisé



Modèle du Château fort

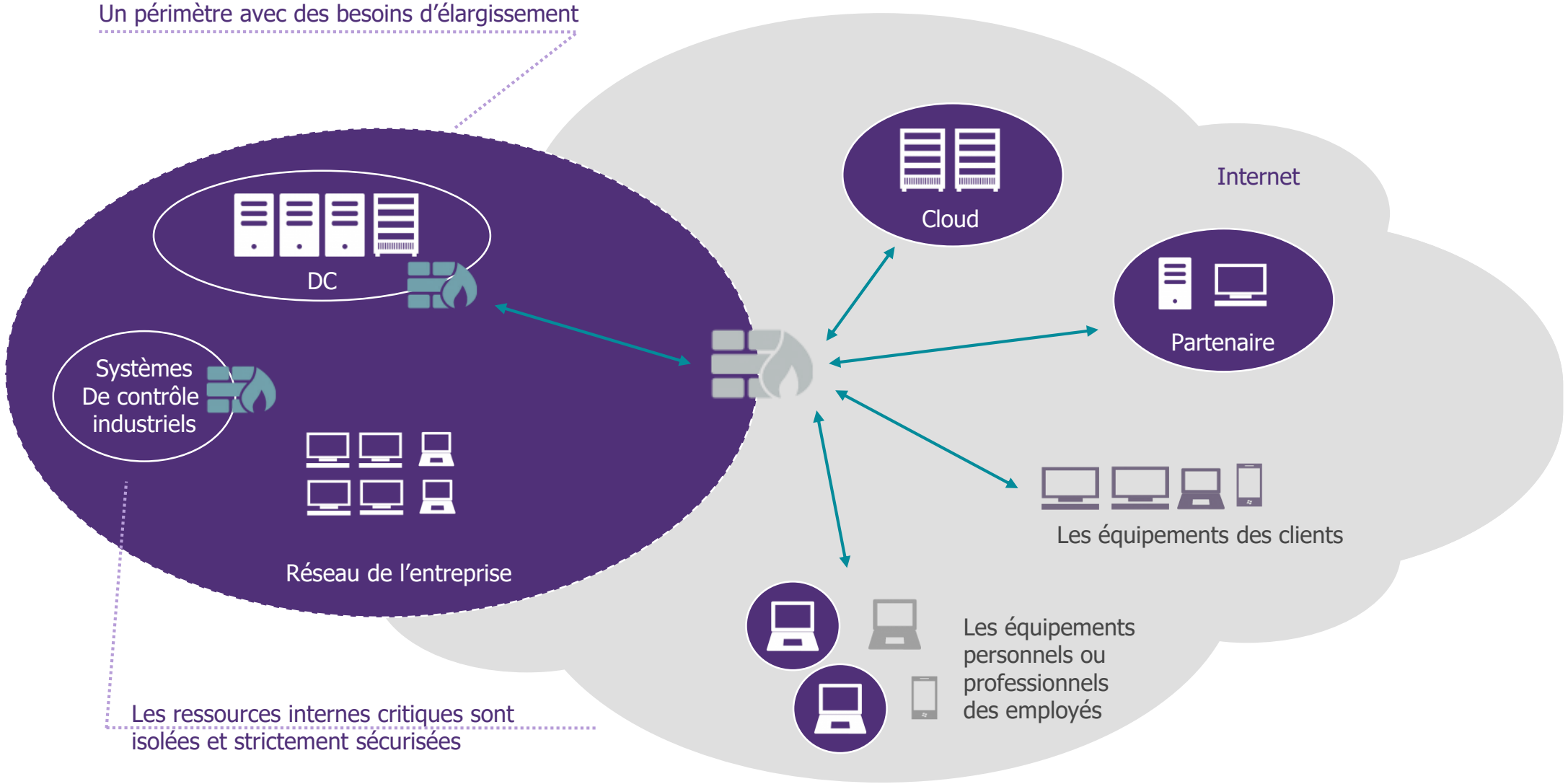
Un unique point d'entrée sécurisé

Libre circulation au coeur de la ville

Un mur solide

Palmanova Fortress (Italy)

Un SI de plus en plus décentralisé



Modèle de l'Aéroport

Des contrôles supplémentaires au niveau des avions

Les zones critiques sont hautement sécurisées

Des millions de passagers et des milliers de fournisseurs de services se déplacent chaque mois dans l'aéroport

Gatwick Airport (UK)

Pourquoi
nous avons besoin
d' **ÉVOLUER**

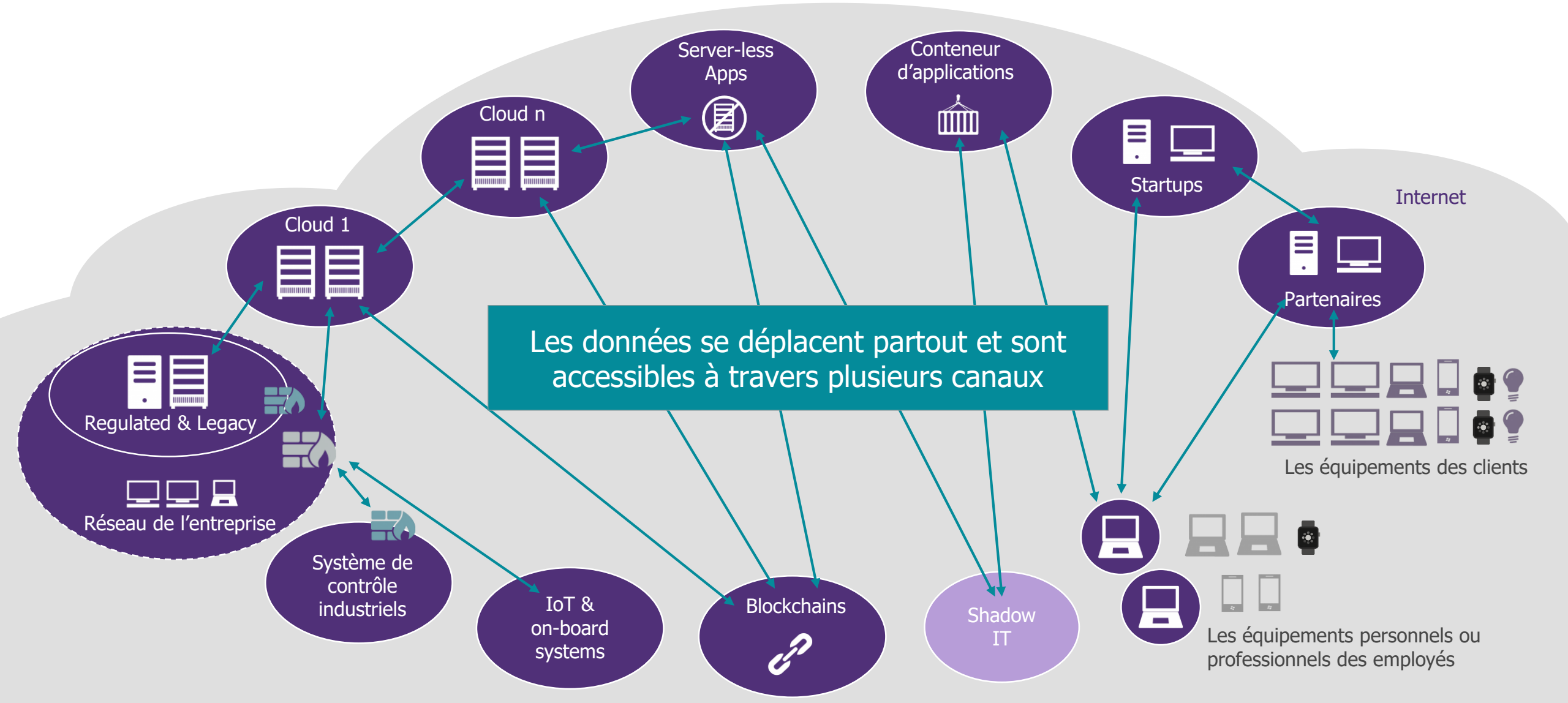
Vers 2020

Le Cloud est une réalité, même pour les applications métiers critiques

Les méthodes agiles et le DevOps sont une réalité

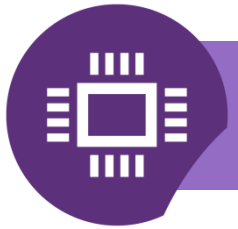
Les méthodes actuelles et les pratiques sécurités n'arrivent pas à suivre le rythme de ce nouveau mode opératoire

Vers 2020 : Un système d'information centralisé



Un nouveau modèle

Avec des données partout



Avec des applications exécutées par plusieurs entités tierces

Où vous êtes responsables de détecter les incidents et de répondre globalement

Un nouveau modèle de sécurité : La compagnie aérienne

Avec des avions et des passagers partout

Où vous faites confiance à un aéroport en ce qui concerne la gestion de vos équipages, vos passagers et vos avions

Où votre centre d'opération suit votre flotte et gère les incidents et les crises


Qu'est-ce qui pourrait poser problème ?

Pour vous, quelles sont les zones critiques d'un SI qui doivent être protégées ?

Exemple d’attaque : *NotPetya*

June 27th

Please note that this is a fictional picture

L'Ukraine *est l'épicentre*

Le Monde Entier *a subi*

Angleterre – Reckitt Benckiser
Plus de 100 M£ de perte de chiffre d'affaire
Perturbation de la production pendant 2 semaines

Danemark – Maersk
Près de 300 M$ de perte de chiffre d'affaire

États-Unis – FedEx (TNT)
300 M$ de perte – Un mois de retard sur certaines expéditions

Ukraine
Plus de 1500 entreprises affectées

États-Unis – Merck
Plus de 600M$, 3 mois d'interruption

France – Saint-Gobain
Près de 250 M€ de perte de chiffre d'affaire
Perturbation de la production et des ventes pendant 2 semaines

Que s'est il *RÉELLEMENT* passé?

Timeline d'une **ATTAQUE MÉTICULEUSEMENT** *préparée*

Avant avril 2017

Les cybercriminels ont **compromis** les serveurs de la société MEDoc

Le 27 juin 2017, 9:12-12:32 UTC

NotPetya se répand à travers les serveurs compromis mis à jour

Le 27 juin 2017, ~12:00 UTC

Diffusion à travers les vulnérabilités de **Microsoft** et les faiblesses des actions **admins**

Le 27 juin 2017, ~13:30 UTC

L'infection des ressources Windows, **chiffrement de fichiers et redémarrage**

Le 27 juin 2017, 19:46 UTC

Les cybercriminels **effacent** le contenu des serveurs utilisés pour l'infection initiale

Plusieurs incohérences dans la théorie du ransomware

Une rançon que vous ne pouvez pas payer

Un canal de distribution très ciblé

Un timing spécifique concernant l'Ukraine

NotPetya, *un acte de* Cyberguerre?

Source: theregister.co.uk & Urkraine army - 2017

Voici
ce que nous avons traversé

Quelle est la situation technique ?

Entre *50%* et *95%* de postes de travail et de serveurs détruits.

Les outils d'admin, les diagrammes de réseaux, les logs… sont soit chiffrés, soit indisponibles.

Les systèmes de restaurations sont inutilisables.

Un chaos organisationnel…

Les applications métiers et les emails ne fonctionnent plus

Les équipes IT sont surchargées

Le Top management demande des comptes

Quelle que soit la localisation

Que s’est-il passé *durant les premières heures ?*

Investiguer
pour bien comprendre la menace

Former une équipe
composées de partenaires
et d'autorités de confiance

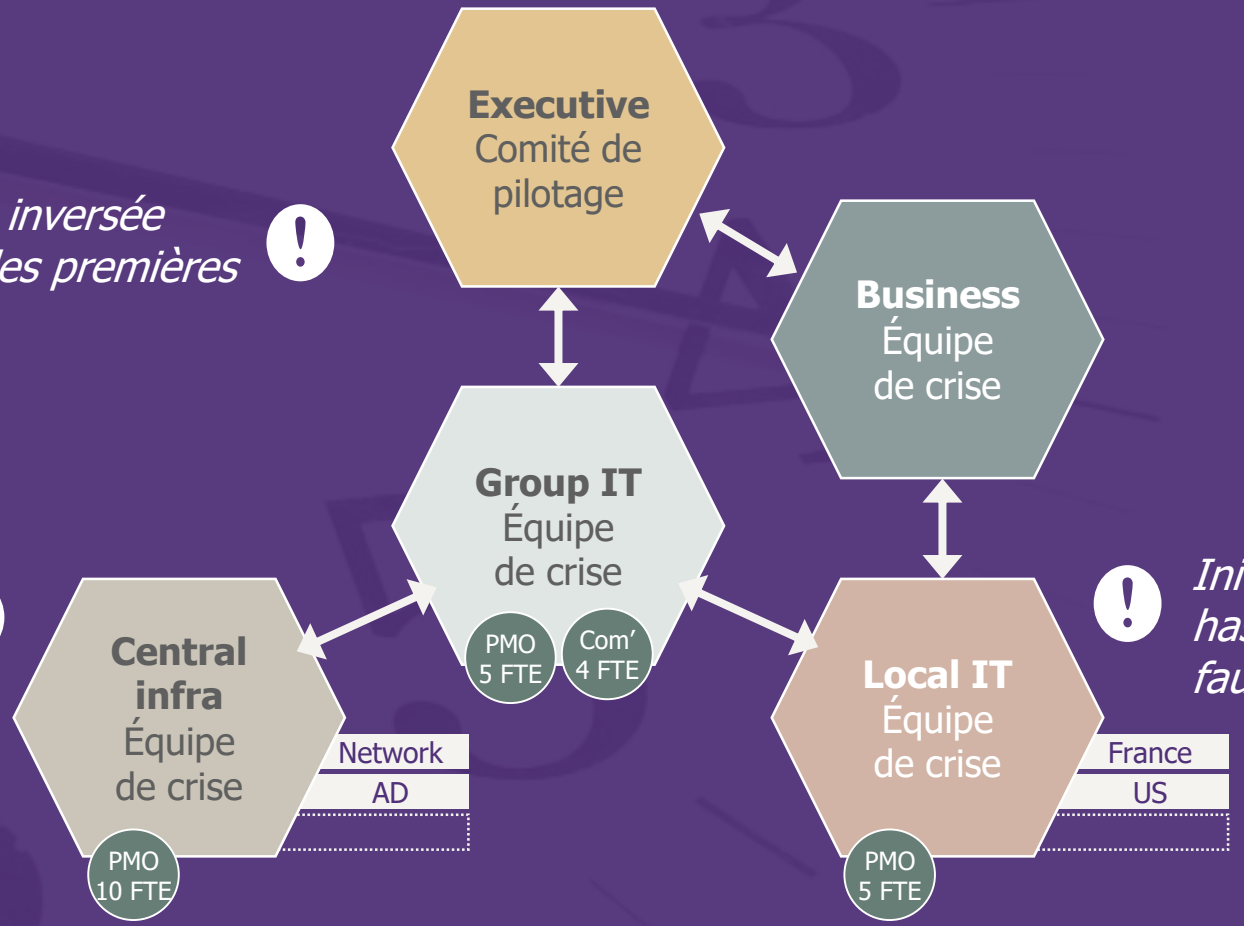
Analyser le malware

Structurer une équipe de crise disponible 24/7

Pyramide inversée pendant les premières heures

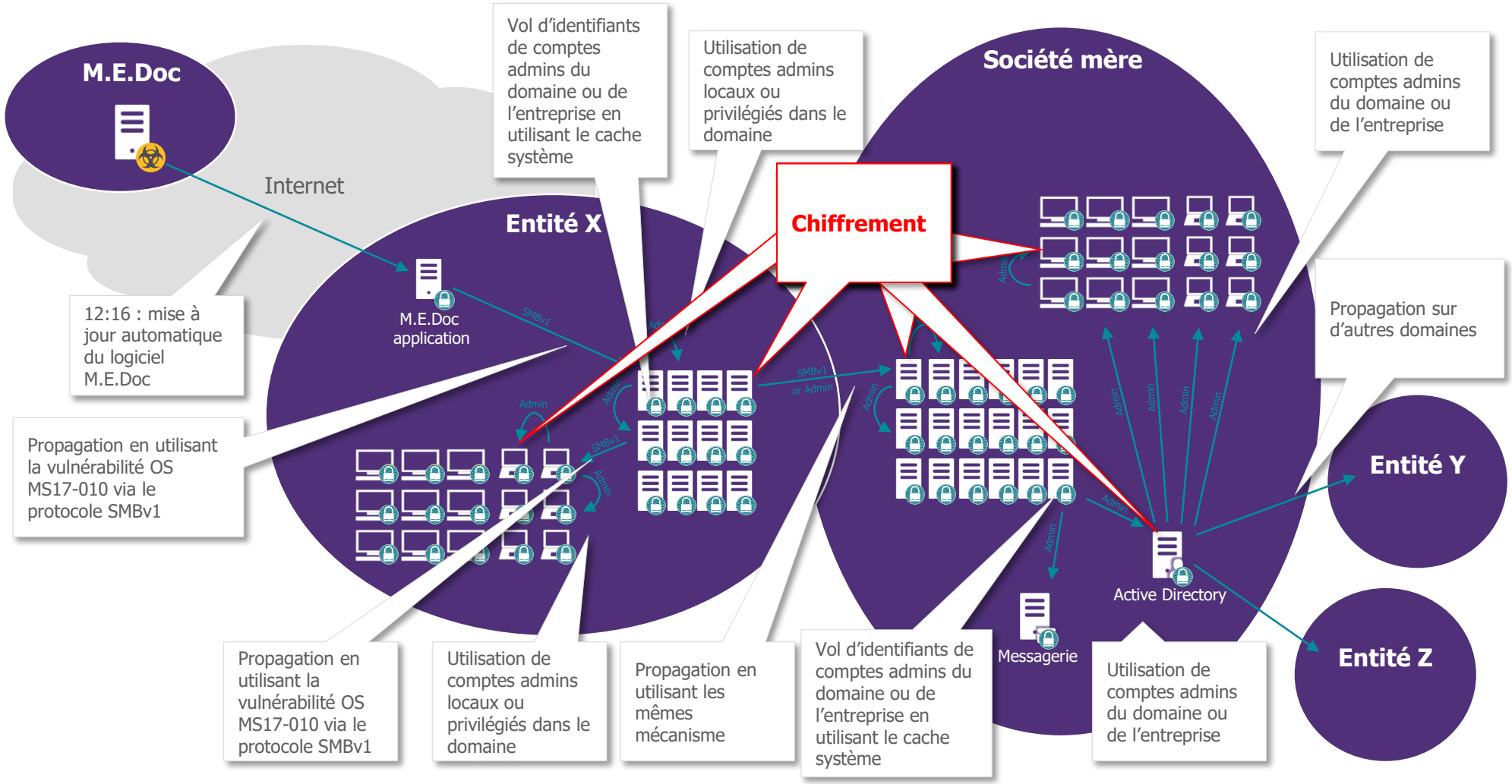
Équipe surinvestie : mauvaise décisions causées par l'épuisement

Initiatives locales hasardeuses causées par de fausses rumeurs



Feedback des investigations du **CERT-W**

Comment NotPetya est entrée et s'est propagée au sein de l'entreprise ?



Tout ça, en moins de deux heures pour certaines entreprises !

Sauver
ce qui peut être sauvé

Débrancher le réseau

Pas d'anticipation d'un pareil cas d'usage et de décision à prendre

Développer un script sanitaire

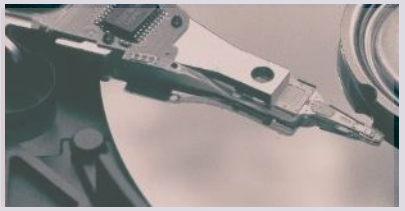
Pas de plateforme pour partager le script, FAQ, chat…

Réaliser une communication
par des moyens non-corporate

Difficulté à distinguer les communications officielles

WannaCry, May 2017

NotPetya, June 2017



Shamoon 2, Jan 2017

Gestion de crise :
essentielle, mais **pas suffisante…**

LA CYBER-RESILIENCE EST INCONTESTABLEMENT LE VRAI SUJET !

1 Introduire de la diversité

2 Être capable d'endiguer une propagation

3 Industrialiser la reconstruction

4 Tester la gestion de sa cyber-crise


Que se passe-t-il durant une attaque ?

Pour vous, quelles sont les grandes étapes d’une attaque ?

NotPetya : un exemple d'attaque complexe et globale

Une attaque qui n'a duré qu'1 jour, mais qui a causé des dégâts considérables avec une portée globale

Étape 1

Vol des informations d'admin pour pénétrer les serveurs de MEDoc (Une compagnie de comptabilité fiscale Ukranienne)

Étape 2

Compromission d'une archive de mise à jour pour du logiciel MEDoc

Étape 3

Intrusion au sein de tous les systèmes d'information des clients de MEDoc à travers l'installation automatique de la mise à jour sur les serveurs clients

Étape 4

Propagation d'une machine à l'autre à travers les vulnérabilités de Microsoft (MS17-010) and et l'utilisation d'un compte admin local ou d'un compte à privilège

Étape 5

Propagation d'une entité à l'autre en utilisant le même mécanisme de l'étape 4 (mouvement latéral) et récupération des informations d'identification de la mémoire cache

Étape 6

Exposition du malware en tant que ransomware et entre-temps supprimer le contenu des serveurs utilisés pour l'intrusion

Étape 7

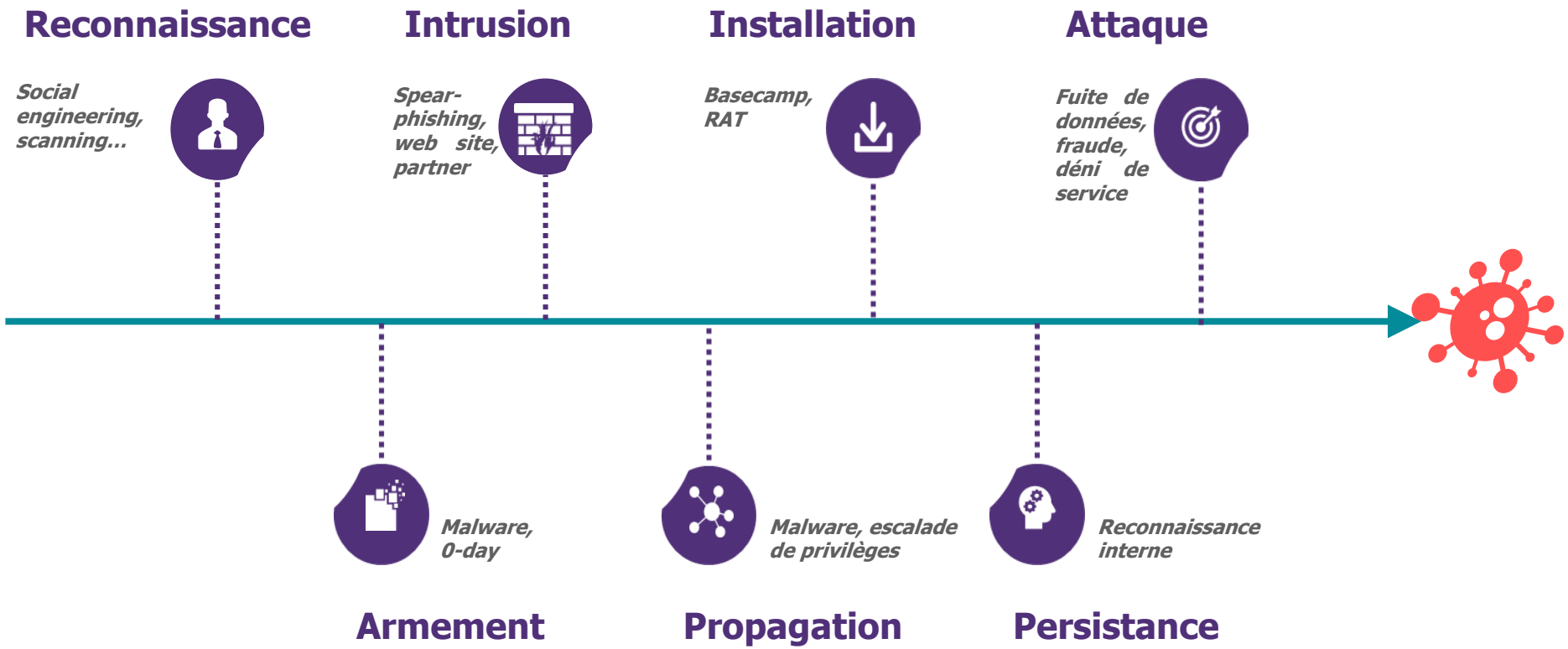
Redémarrage et chiffrement complet des disques ou chiffrement de fichiers spécifiques si les disques sont déjà chiffrés

1 milliard de dollars de perte

De 60 à 95% de destruction des serveurs visés

150+ Pays affectés

Le SI est toujours attaqué de la même façon : *La killchain*




Quelles sont les
bonnes pratiques
de sécurité
dans un SI ?

Pour vous, comment peut-on se protéger d'une attaque ?

Plusieurs **ACTIONS** pour anticiper

1 *Avoir une hygiène simple de cybersécurité (droit d'accès, patch management, administration sécurisée, surveillance, gouvernance…). Simple…mais qui requiert beaucoup d'efforts pour être implémentée*

2 *Connaître ses éléments critiques (crown jewels) en ce qui concerne l'IT et l'exploitation (analyse de risques, régulations…), les sécuriser by design et assurer la continuité d'activité*

3 *Se tester réellement (redteam audit, backup et plan de reprise d'activité) et appliquer les recommendations de l'audit*

4 *Connaître et faire connaître son équipe Cybersécurité (sensibilisation, formation, aide) pour être alerté lorsque cela est nécessaire*

Différents frameworks existent

NIST :
L'américain divisé en 5 parties

ISO 27002 :
La norme avec 114 bonnes pratiques réparties de 14+4 chapitres

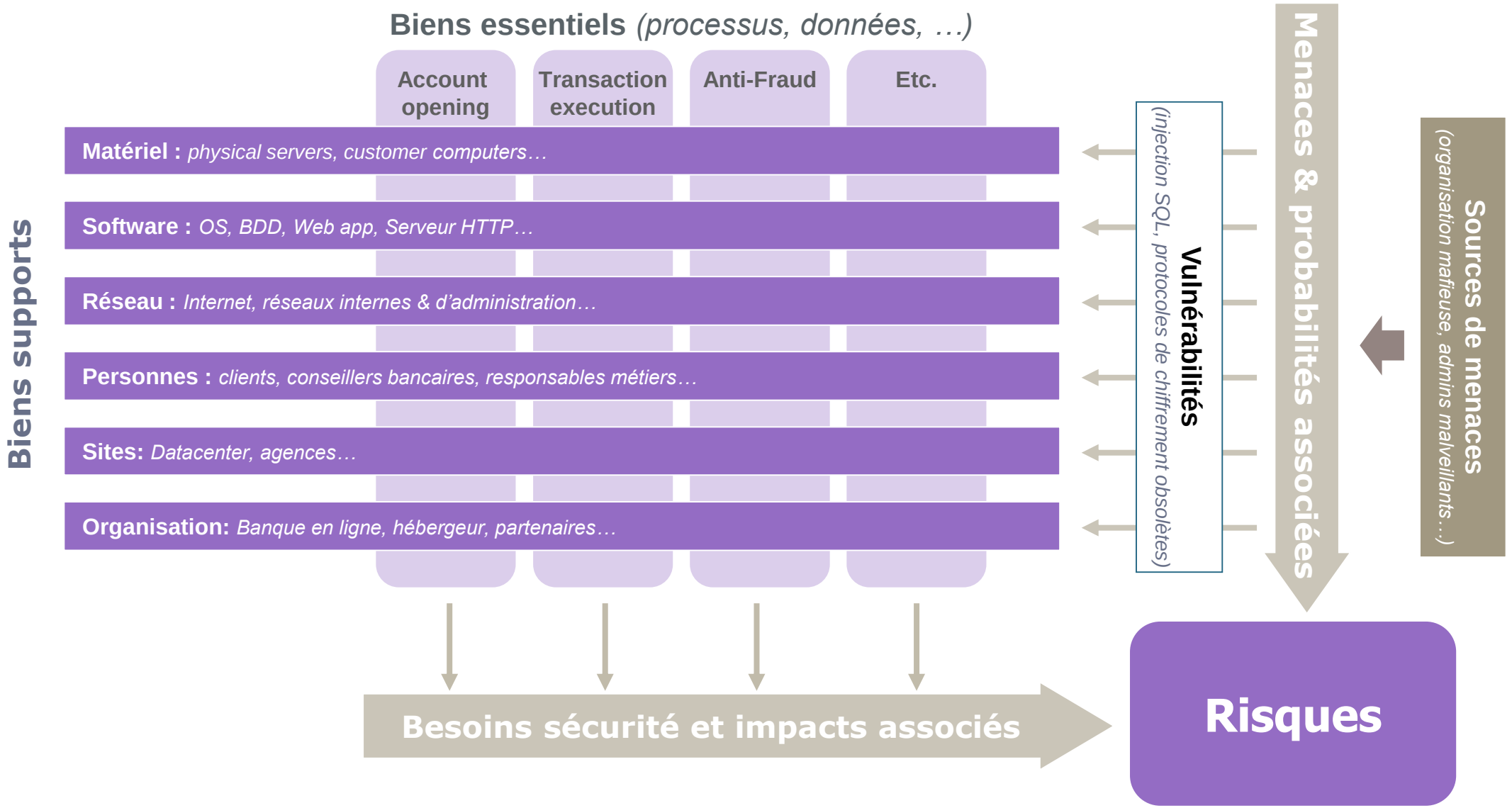
5. Politiques de sécurité de l'information
6. Organisation de la sécurité de l'information
7. La sécurité des ressources humaines
8. Gestion des actifs
9. Contrôle d'accès
10. Cryptographie
11. Sécurité physique et environnementale
12. Sécurité liée à l'exploitation
13. Sécurité des communications
14. Acquisition, développement et maintenance des systèmes d'information
15. Relations avec les fournisseurs
16. Gestion des incidents liés à la sécurité de l'information
17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
18. Conformité

Le guide de l'ANSSI :
Le français composé 42 règles réparties en 10 chapitres

1. Sensibiliser et former
2. Connaître le système d'information
3. Authentifier et contrôler les accès
4. Sécuriser les postes
5. Sécuriser le réseau
6. Sécuriser l'administration
7. Gérer le nomadisme
8. Maintenir le système d'information à jour
9. Superviser, auditer, réagir
10. Pour aller plus loin

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

L'analyse de risques : Un grand mot pour un concept simple



Les Red, Blue and Purple teams

Des audits d'une Purple team sont constitués de **tests d'intrusions** (Red Team) réalisés pour évaluer la **capacité de détection** sur un périmètre donné (Blue Team) et ainsi améliorer son efficacité.

RED TEAM

Approche axé sur un objectif

Les actions d'une Red team sont techniquement les mêmes que lors de tests d'intrusions. Mais leur objectif est de prouvé que leur objectif peut être atteint et non pas de remonter toutes les vulnérabilités

- Accès à des informations sensibles : nouveau projet, ventes, liste de clients, emails du comité de direction, …
- Prendre le contrôle d'une machine spécifique : application financière, …
- Information réglementée.

Se comporter comme un réel attaquant

- Social engineering.
- Intrusion physique.
- Exfiltration.de données

Pentests à différents niveaux

BLUE TEAM

Gestions des évènements

Chercher et collecter les éléments techniques permettant la détection d'incidents de sécurité

Gestions des incidents

Identification et qualification des incidents de sécurité basés sur les évènements collectés

Gestion de management

Signalement au responsable des incidents de sécurité qui menacent le système

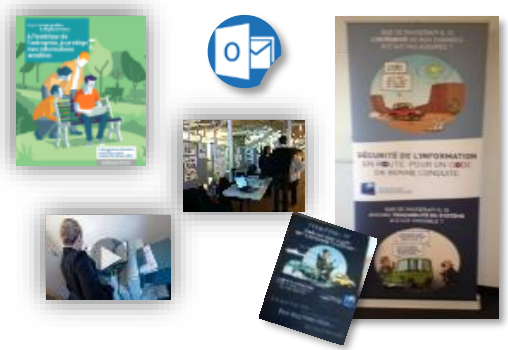
Les tests sont accompagnés par des **ateliers** entre la Red Team et la Blue Team pour **échanger sur les tests effectués** et les résultats obtenus par la Red Team tout comme les évènements de sécurité **identifiés avec succès** par la Blue Team

Les actions de sensibilisation

Information

Provoquer une prise de conscience des risques

Informer sur les mesures de sécurité



Communications ciblées

Changer les habitudes

Donner des bonnes pratiques et créer des réflexes

Formations

Augmenter le niveau de connaissance des outils de sécurité

Améliorer les compétences clés

8 questions simples : Qui ? Pourquoi ? Quoi ? Quand ? Par qui ? Comment ? Quel intérêt ? À quel prix ?

Mais **les attaques** sont inévitables

Soyons donc prêt !

5 *Se préparer à des **crises à long terme** (plusieurs semaines) **silencieuses** et généralement confidentielles **contre un être humain** qui a pris le temps d'apprendre les rouages internes*

6 *Travailler en collaboration avec les métiers puisqu'ils sont la réelle cible de l'attaque, **le département IT et les experts externes** pour identifier les cibles et comprendre les raisons de l'attaque*

7 *Assurer des méthodes de travail de secours ou dégradés dans le but d'assurer la continuité des opérations dans le cas d'une destruction ou d'une perte de confiance (papier, plusieurs systèmes d'information...)*

8 *Savoir comment faire face **à ces crises sur tous les niveaux**, media, RH ... Et s'entraîner à travers un exercice de crise*


Et vous
dans tout ça?

Quel est votre rôle en tant qu'utilisateur ?

« L’hygiène informatique c’est se laver les mains et le clavier ? »

En tant qu’utilisateur du SI :

/ Vous avez accès à des ressources de l’entreprise

Par conséquent, il est de votre responsabilité de :

/ Respecter les bonnes pratiques et guide d’hygiène informatique

Quel est votre rôle en tant que super-utilisateur ?

« De grands pouvoirs impliquent de grandes responsabilités »

En tant que développeur/administrateur :

/ Vous êtes des utilisateurs privilégiés

/ Vous avez accès au cœur même de l'entreprise : le code source des applications, les bases de données, les accès aux serveurs…

Par conséquent, il est de votre responsabilité de :

/ Vous assurer de la sécurité :

De votre environnement de développement

Dans les développements que vous produisez

/ Respecter les bonnes pratiques et la norme de développements sécurisés

/ Suivre et appliquer les cours de cette année


Et Wavestone
dans tout ça ?

Dans un monde où la capacité à se transformer est la clé du succès,
nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders
dans leur secteur

2 800 collaborateurs
dans 8 pays

Parmi les leaders du conseil
indépendant en Europe,
n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milan* | Bruxelles | Genève | Casablanca | Istanbul* | Edimbourg
Lyon | Marseille | Nantes

* Partenariats

Une capacité unique à combiner expertise sectorielle, connaissance des fonctions de l'entreprise et maîtrise des technologies

FONCTIONS

Stratégie

Management & financement de l'innovation

Marketing, ventes & expérience client

People & change

Finance, risques & achats

Operations & logistique

SECTEURS

Banque & assurance

Télécoms & média

Biens de consommation & distribution

Industrie

Énergie & utilities

Transport & voyages

Immobilier

Secteur public & institutions internationales

TECHNOLOGIES

Stratégie digitale & SI

Technologies digitales & émergentes

Architecture SI & data

Cybersécurité & confiance numérique

Réussir sa **transformation numérique** grâce à la **confiance numérique**

500+
Consultants & Experts

1,000+
Missions par an dans plus de **20** pays

Nos clients
COMEX, Métier, CDO, CIO, CISO, BCM

UNE EXPERTISE EPROUVEE

- Stratégie et Conformité
- Transformation métier sécurisée
- Architecture et programme sécurité
- Identité, Fraude et Services de Confiance
- Tests d'intrusion & Réponse à incident
- Continuité d'Activité & Résilience
- SI Industriel

NOS DIFFERENCIATEURS

- Connaissance des risques métier
- Méthodologie AMT pour les schémas directeurs
- Radars Innovation et Start-ups
- CERT-W
- Bug Bounty by Wavestone

Des références de tout premier plan, et un retour d'expérience unique

SOCIETE GENERALE
Stratégie cybersécurité du groupe

BARCLAYS
Programme de remédiation cybersécurité

ALLIANZ - WORLDWIDE PARTNERS
Mise en conformité RGPD à l'échelle internationale

SANOFI
Programme de sécurisation des SI industriels

SAINT-GOBAIN
Réponse à incident sur crise cyber

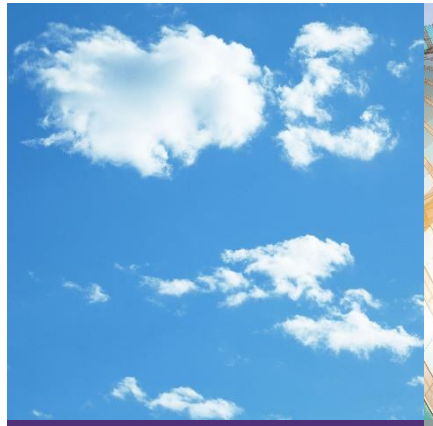
SOWEE - EDF GROUP
Audit et architecture sécurisée cloud & IoT

EDF
Stratégie Customer IAM et déploiement

SOCIETE GENERALE
Lutte contre la fraude grâce au Machine Learning

ENISA - EUROPEAN SECURITY AGENCY
Promotion des start-ups sécurité en Europe

Nous anticipons les tendances pour guider vos réflexions



CLOUD

Adopter un nouveau modèle de sécurité pour prendre en compte la réalité des déploiements

INFRASTRUCTURES CRITIQUES
(LPM/NIS, NYDFS…)

Identifier le périmètre adéquat pour limiter les impacts tout en garantissant la sécurité nationale

PROGRAMMES CYBERSECURITE

Définir son propre Framework inspiré des standards internationaux (NIST, ISO…) pour reporter de manière homogène au Board et régulateurs

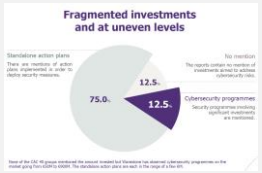
SURVEILLANCE & ANTI-FRAUDE

Rendre disponible le socle technique du SOC aux métiers pour compléter leur anti-fraude sur les chaines transactionnelles critiques

CYBER RESILIENCE

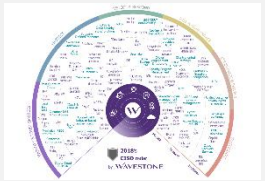
Inclure un scenario d'attaque du SI à grande échelle dans le PCA, et se tester régulièrement

Nos différenciateurs uniques pour vos enjeux cybersécurité



Benchmark maturité cybersécurité

Comment vous situez-vous par rapport au reste du marché sur le volet cyber ?



Radar du RSSI

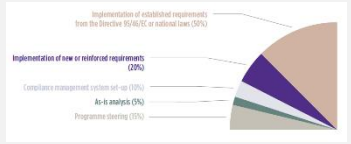
Identifiez les sujets d'actualité pour vous les approprier

Radar des Start-ups

Identifiez les pépites de la cybersécurité et de la confiance numérique

Benchmark des tests d'intrusion web

Qu'apprend-on de 150+ audits et quelles actions doivent être entreprises?



Benchmark RGPD

Découvrez les priorités et les budgets alloués au sein des grandes organisations

MACHINE LEARNING by WAVESTONE & DATA LAB

Machine Learning Data Lab

Concrétisez vos besoins en matière de lutte contre la fraude en s'appuyant sur notre équipe de data scientists

Awareness and training models

Sensibilisez vos équipes sur la sécurité par une approche concrète (SI industriel, objets connectés, véhicule autonome etc.)

CERT W

CERT-Wavestone

Tirez parti de nos outils internes d'APT Hunting et de gestion de crise

Nous accélérons les start-ups cybersécurité pour construire et animer un écosystème d'open-innovation

ALSID

Une solution de cyberdéfense conçue pour les décideurs afin de détecter les failles des entreprises avant les hackers

Citalid CYBERSÉCURITÉ

Une solution de cyber threat intelligence tirant parti de marqueurs techniques, géopolitiques, économiques et sociaux pour anticiper les cyber menaces et quantifier les risques

SKEY3CODE

Proposition d'une solution d'authentification forte pour les transactions et de sécurisation des applications.

sqreen

Sqreen renforce la sécurité des applications web de façon robuste, continue et transparente.

WAVESTONE

Cyril MANSOUR
Consultant

M +33 (0)6 61 34 56 69
cyrill.mansour@wavestone.com

Carole CORDIER
Consultant

M +33 (0)6 67 78 71
carole.cordier@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

EDIMBOURG

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE