

Sécurité des Systèmes d'Information

Sensibilisation

Commandant Michel Dubois
OSSI du SSA

michel1.dubois@intradef.gouv.fr

Dernière mise à jour: 10 novembre 2014



Table des matières

- 1 Introduction**
- 2 Risques, menaces et vulnérabilités**
- 3 Contres mesures**
- 4 Conclusion**



Table des matières

- 1 Introduction**
- 2 Risques, menaces et vulnérabilités**
- 3 Contres mesures**
- 4 Conclusion**



Table des matières

- 1 Introduction**
- 2 Risques, menaces et vulnérabilités**
- 3 Contres mesures**
- 4 Conclusion**



Table des matières

- 1 Introduction**
- 2 Risques, menaces et vulnérabilités**
- 3 Contres mesures**
- 4 Conclusion**



Nos objectifs... .

- ▶ Voir la *réalité de la menace*
- ▶ Avoir une *bonne connaissance de la SSI*
- ▶ Étudier les *moyens* de la mettre en œuvre
- ▶ Définir les *responsabilités* de chaque acteur du SI
- ▶ Définir un certain nombre de *règles concrètes*

Nos objectifs...

- ▶ Voir la *réalité de la menace*
- ▶ Avoir une *bonne connaissance de la SSI*
- ▶ Étudier les *moyens* de la mettre en œuvre
- ▶ Définir les *responsabilités* de chaque acteur du SI
- ▶ Définir un certain nombre de *règles concrètes*

Nos objectifs...

- ▶ Voir la *réalité de la menace*
- ▶ Avoir une *bonne connaissance de la SSI*
- ▶ Étudier les *moyens* de la mettre en œuvre
- ▶ Définir les *responsabilités* de chaque acteur du SI
- ▶ Définir un certain nombre de *règles concrètes*

Nos objectifs...

- ▶ Voir la *réalité de la menace*
- ▶ Avoir une *bonne connaissance de la SSI*
- ▶ Étudier les *moyens* de la mettre en œuvre
- ▶ Définir les *responsabilités* de chaque acteur du SI
- ▶ Définir un certain nombre de *règles concrètes*

Nos objectifs...

- ▶ Voir la *réalité de la menace*
- ▶ Avoir une *bonne connaissance de la SSI*
- ▶ Étudier les *moyens* de la mettre en œuvre
- ▶ Définir les *responsabilités* de chaque acteur du SI
- ▶ Définir un certain nombre de *règles concrètes*

Nos objectifs...

$$\ln(e) + (\cos^2 x + \sin^2 x) = \sum_{i=0}^{\infty} \frac{1}{2^i}$$



L'art de la pédagogie est fait d'humilité et non de fatuité : le but de tout enseignement n'est pas que le professeur, par un discours inutilement compliqué et pédant, paraisse intelligent, mais que ses élèves en aient vaincu les moindres difficultés et en ressortent grandis.

Emile Gaburiaud-Pagès,
L'art d'enseigner aux autres (1919)

Nos objectifs...

$$\ln(e) + (\cos^2 x + \sin^2 x) = \sum_{i=0}^{\infty} \frac{1}{2^i}$$



L'art de la pédagogie est fait d'humilité et non de fatuité : le but de tout enseignement n'est pas que le professeur, par un discours inutilement compliqué et pédant, paraisse intelligent, mais que ses élèves en aient vaincu les moindres difficultés et en ressortent grandis.

Emile Gabauriaud-Pagès,
L'art d'enseigner aux autres (1919)

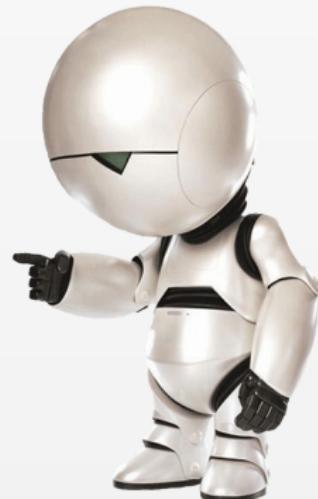
Introduction

1 Introduction

2 Risques, menaces et vulnérabilités

3 Contres mesures

4 Conclusion



Pourquoi la SSI ?

- 1** **Introduction**
 - Pourquoi la SSI ?**
 - Définitions**
 - Information
 - Système d'information
 - Sécurité des Systèmes d'Information
 - Quizz**



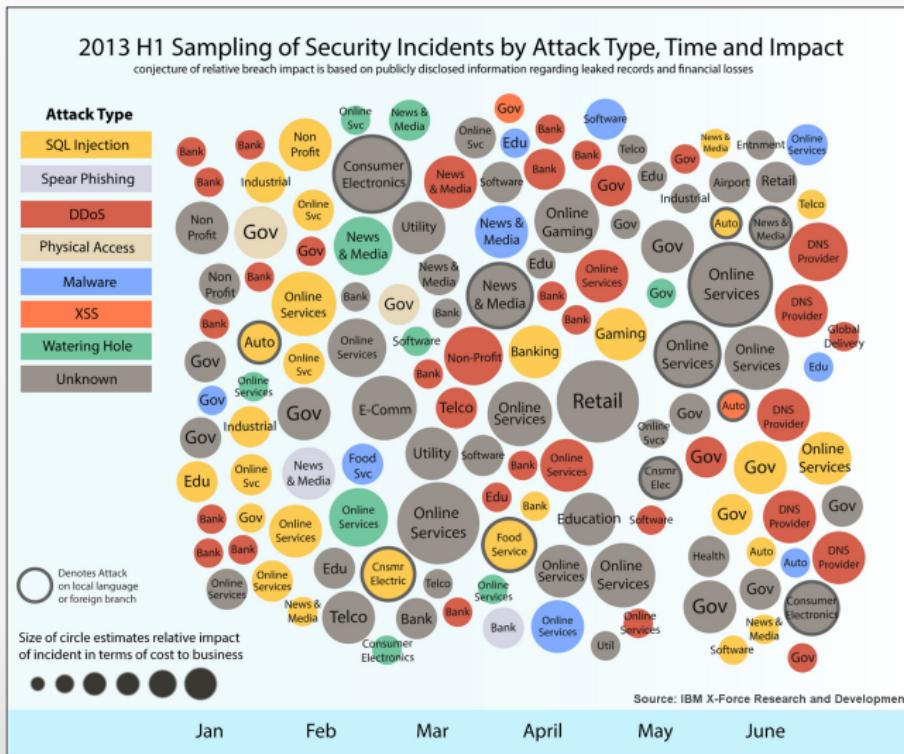
Pourquoi la SSI? : contexte



Pourquoi la SSI ? : contexte



Pourquoi la SSI ?



Pourquoi la SSI ?

Phishing & faux site Web – lundi 28 mars 2011

Screenshot of a Mozilla Firefox browser window showing a phishing attempt on the official French Ministry of Employment and Health website.

The address bar shows: http://studodeux.com/blog/sante.gouv.fr/cartevitale/Carte_Vitale.htm

A red banner at the top of the page reads: "Ce site a été signalé comme étant une contrefaçon!" and "Ce site n'est pas une contrefaçon..."

The main content area is a form titled "Vérification de l'identité." It includes fields for Name, First Name, Address, Postcode, Phone number, Card ID number, Card Vitale number, Credit card number, Card type, and Expiry date.

On the right side, there are two sidebar boxes:

- Le ministre du Travail, de l'Emploi et de la Santé:** Shows a photo of a man and links to Agenda, Biographie, and Contacter le ministère.
- La secrétaire d'Etat chargée de la santé:** Shows a photo of a woman and links to Agenda.

On the left sidebar, there are links to Actualité-Presse, Campagnes, Vidéo-théâtre, Publications et documentation, Etudes recherches et statistiques - DREES, Inspection, contrôle, évaluation (IGAS), Santé Europe, Les dossiers de A à Z, Alertes sanitaires, and S'abonner à DGS-Urgent.

At the bottom left, there is a "Terminé" button.

Pourquoi la SSI ?

Vol de données – 4 octobre 2013

USA TODAY
A GANNETT COMPANY

SEARCH

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 43° SUBSCRIBE

Adobe loses 2.9 mil customer records, source code

 CYBERTRUTH Byron Acohido, USA TODAY 10:16 a.m. EDT October 4, 2013


(Photo: Adobe)

SHARE f 970 CONNECT t 487 TWEET c 20 COMMENT e EMAIL MORE

SEATTLE – Adobe has become the latest big-name data breach victim.

The company that mainstreamed desktop publishing admitted in a statement that hackers gained unauthorized access to 2.9 million customer accounts and stole part of the source code for at least two major consumer-facing products.

"The Adobe breach shows that everyone is fair game," says Edward Goodman, chief privacy officer at risk management firm Identity Theft 911. "The hackers went in and stole private consumer information in the form of card information, even if it was encrypted, and they stole intellectual property. Those are two valuable assets."

USA NOW


Pope's cool confession | USA NOW
Dec 03, 2013

Pourquoi la SSI ?

Hacktivisme – avril 2013

"Syrian hackers" break into Associated Press Twitter account and break news that explosions at White House have injured Obama - sending DOW Jones plunging 100 points

The Associated Press (@AP) Following

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

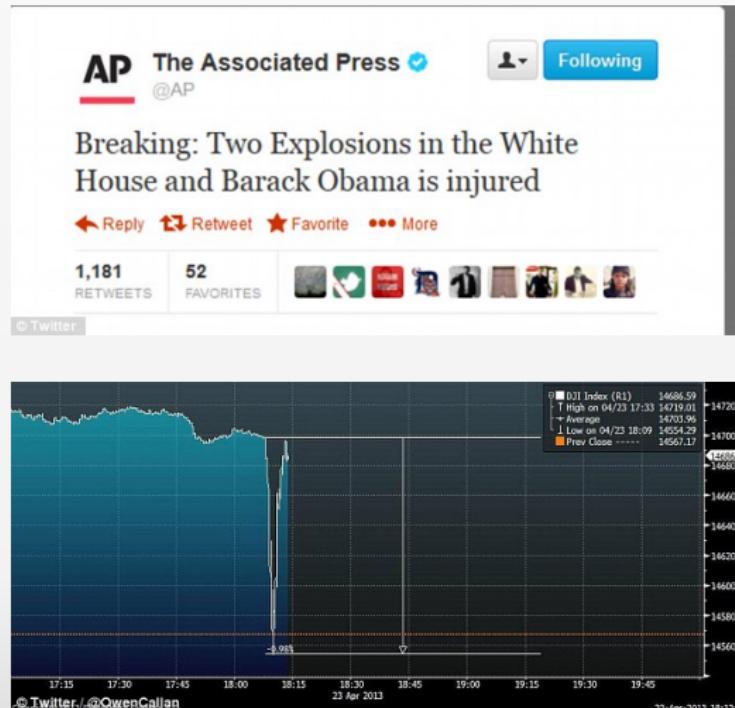
1,181 RETWEETS 52 FAVORITES

Twitter

Pourquoi la SSI ?

Hacktivisme – avril 2013

"Syrian hackers" break into Associated Press Twitter account and break news that explosions at White House have injured Obama - sending DOW Jones plunging 100 points



Pourquoi la SSI ?

Hacktivisme – avril 2013



l'Humanité.fr

ENVIES DE CHANGER LE MONDE

A LA

MONDE

POLITIQUE

SOCIAL-ÉCO

SOCIÉTÉ

ENVIRONNEMENT

MONDE

Pourquoi la SSI ?

Hacktivisme – mars 2014



OI Business

Retours d'expérience | Guides pratiques | Dossiers | Portraits | Agenda | Emploi | Télécharger pro

E-commerce | Start-up | Sécurité | Infrastructure | SSI | Télécommunications | Cloud | Logiciels & applic.



LE MAGAZINE

APPLI

01

Business

Pourquoi la SSI ?

■■■ Orange F 3G 06:47 ► ● 84 %

US warns of cyber attacks on medical devices

June 14, 2013, 2:47 am
AFP



WASHINGTON (AFP) - US authorities on Thursday warned makers of medical devices and hospital networks to step up efforts to guard against potential cyber attacks.



“À ce jour, à cause de l'informatique, nous risquons de sortir d'un hôpital, dans un état pire que celui dans lequel nous y sommes rentrés.”

Patrick Pailloux
Discours de clôture
SSTIC 2010



Pourquoi la SSI ?

Négligence – vendredi 27 juin 2014



This is a photo taken by Brazilian newspaper Correio Braziliense of police chief Luiz Cravo Dorea taken at the the World Cup main command and control security center.

wifi network "WORLDCUP" password "b5a2112014" (leet speak for Brazil 2014)

http://thehackernews.com/2014/06/fifa-world-cup-security-team_26.html

Pourquoi la SSI ?

Vandalisme – 16 mars 2014



“Deux centraux téléphoniques ont été détruits par des incendies dans la nuit de samedi à dimanche en Haute-Garonne (à Bessières et Villemur-sur-Tarn) privant 8000 abonnés de téléphone fixe et d'ADSL.”



“Des centraux opportunément incendié pendant qu'un gang de malfaiteurs pénétrait dans la salle des coffres de l'agence du Crédit Agricole.”

Pourquoi la SSI ?



La NSA espionnait dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, montrent des documents secrets dont "Der Spiegel" a pris connaissance. AP/KIN CHEUNG

Les services de renseignement américains espiaient dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, dont ils avaient réussi à pénétrer les réseaux informatiques, montrent des documents secrets dont [l'hebdomadaire allemand Der Spiegel](#) a pris connaissance.

Le magazine allemand cite dans un article publié samedi 29 juin un document classé "strictement confidentiel" de la

Pourquoi la SSI ?

Orange F 3G 20:35 3 %

Prism : la NSA espionnait l'Union européenne

29.06.2013 à 20:30 | Le Monde.fr avec AFP et Reuters

La NSA espionnait dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, montrent des documents secrets dont "Der Spiegel" a pris connaissance. AP/KIN CHEUNG

Les services de renseignement américains espionnaient dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, dont ils avaient réussi à pénétrer les réseaux informatiques, montrent des documents secrets dont [l'hebdomadaire allemand Der Spiegel](#) a pris connaissance.

Le magazine allemand cite dans un article publié samedi 29 juin un document classé "strictement confidentiel" de la

Orange F 3G 20:58 7 %

< Retour Le Point.fr

Tech & Net

Allemagne : les parlementaires privés d'iPhone

Suite au scandale des écoutes, les Allemands vont utiliser un logiciel de cryptage des données. Seul défaut, il n'est pas compatible avec les iPhone.

Le Point.fr | 26/11/13 | 14:10

Depuis quelques semaines, l'iPad, la tablette numérique de la marque à la pomme, est interdite de séjour au 10, Downing Street, la résidence officielle de David Cameron, le Premier ministre britannique. À son tour, l'Allemagne vient d'interdire les iPhone au Bundestag, le parlement allemand, [révèle](#)



Pourquoi la SSI ?

Orange F 3G 20:35 3 %

Prism : la NSA espionnait l'Union européenne

29.06.2013 à 20:30 | Le Monde.fr avec AFP et Reuters



La NSA espionnait dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, montrent des documents secrets dont "Der Spiegel" a pris connaissance. AP/KIN CHEUNG

Les services de renseignement américains espiaient dans le cadre du programme de surveillance Prism plusieurs bureaux de l'Union européenne, dont ils avaient réussi à pénétrer les réseaux informatiques, montrent des documents secrets dont [l'hebdomadaire allemand Der Spiegel](#) a pris connaissance.

Le magazine allemand cite dans un article publié samedi 29 juin un document classé "strictement confidentiel" de la

Orange F 3G 20:58 7 %

< Retour Le Point.fr

Tech & Net



Allemagne : les parlementaires privés d'iPhone

Suite au scandale des écoutes, les Allemands vont utiliser un logiciel de cryptage des données. Seul défaut, il n'est pas compatible avec les iPhone.

Le Point.fr | 26/11/13 | 14:10

Depuis quelques semaines, l'iPad, la tablette numérique de la marque à la pomme, est interdite de séjour au 10, Downing Street, la résidence officielle de David Cameron, le Premier ministre britannique. À son tour, l'Allemagne vient d'interdire les iPhone au Bundestag, le parlement allemand, révèle

Orange F 3G 20:58 7 %

Commenter Partager Envoyer A- A+

Orange F 20:39 84 %

Cyberespionnage : quatre ordinateurs disparaissent toutes les heures à Roissy-Charles-de-Gaulle



Copyright Reuters

Share 0

Michel Cabiroi | 03/07/2013, 16:36 - 652 mots

21 % des utilisateurs d'ordinateurs volés à l'aéroport Roissy-Charles-de-Gaulle estiment qu'ils contenaient des informations confidentielles qui ne sont pour la plupart pas chiffrées (93 %). Autre vulnérabilité pour les entreprises, les smartphones utilisés de façon quotidienne pour des usages

Orange F 3G 20:39 84 %

Commenter Partager Envoyer A- A+

Pourquoi la SSI ?

Orange F 22:23 13 %

La cyberguerre, nouvel enjeu des armées

13.07.2013 à 17:03 | Le Monde.fr Guénaël Pépin



Les forces "cyber" sont en pleine formation au sein des armées, dans le but de pouvoir attaquer et répondre aux nouvelles menaces numériques. REUTERS/STOYAN NENOV

Les scandales des écoutes électroniques par les Etats-Unis, le Royaume-Uni ou encore la France mettent au premier plan les rivalités entre Etats en matière d'espionnage et de conflits "en ligne", pour lesquels les gouvernements préparent leurs armes. "Prism est la partie émergée de l'iceberg", expliquait Jarno Limmell, directeur de la sécurité de l'éditeur finlandais de solutions réseaux Stonesoft, lors d'un atelier à l'ambassade de Finlande en France le 20 juin.

Pourquoi la SSI ?



Les forces "cyber" sont en pleine formation au sein des armées, dans le but de pouvoir attaquer et répondre aux nouvelles menaces numériques. REUTERS/STOYAN NENOV

Les scandales des écoutes électroniques par les Etats-Unis, le Royaume-Uni ou encore la France mettent au premier plan les rivalités entre Etats en matière d'espionnage et de conflits "en ligne", pour lesquels les gouvernements préparent leurs armes. "Prism est la partie émergée de l'iceberg", expliquait Jarno Limnälä, directeur de la sécurité de l'éditeur finlandais de solutions réseaux Stonesoft, lors d'un atelier à l'ambassade de Finlande en France le 20 juin.



Communiqué publié sur le site d'Apple dédié aux développeurs. APPLE

Le géant informatique américain Apple a averti les développeurs d'applications pour ses produits que son site qui leur est dédié avait été piraté et que des informations les concernant peuvent avoir été dérobées.

"Jeudi, un intrus a essayé d'accéder à des données personnelles sur les développeurs enregistrés sur notre site", indique Apple dans un communiqué sur ce site, dimanche 21 juillet. En réaction à l'attaque informatique, qui a eu lieu jeudi, le groupe

Pourquoi la SSI ?

Orange F 22:23 13 %

La cyberguerre, nouvel enjeu des armées

13.07.2013 à 17:03 | Le Monde.fr Guénaël Pépin



Les forces "cyber" sont en pleine formation au sein des armées, dans le but de pouvoir attaquer et répondre aux nouvelles menaces numériques. REUTERS-STOYAN NENOV

Les scandales des écoutes électroniques par les Etats-Unis, le Royaume-Uni ou encore la France mettent au premier plan les rivalités entre Etats en matière d'espionnage et de conflits "en ligne", pour lesquels les gouvernements préparent leurs armes. "Prism est la partie émergée de l'iceberg", expliquait Jarno Limnéll, directeur de la sécurité de l'éditeur finlandais de solutions réseaux Stonesoft, lors d'un atelier à l'ambassade de Finlande en France le 20 juin.

Orange F 06:50 95 %

Le site d'Apple dédié aux programmateurs d'applications piraté

22.07.2013 à 06:37 | Le Monde.fr avec AFP



Pourquoi la SSI ?

Erreur humaine – décembre 2013

***** Orange F 09:35 43 %
googleonlinesecurity.blogspot.de

Google Online Security Blog

Saturday, December 7, 2013

Further improving digital certificate security

Posted by Adam Langley, Security Engineer

Late on December 3rd, we became aware of unauthorized digital certificates for several Google domains. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to ANSSI, a French certificate authority.

Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.

Pourquoi la SSI ?

Erreur humaine – décembre 2013

***** Orange F 9:35 43 % googleonlinesecurity.blogspot.de

Google Online Security Blog

Saturday, December 7, 2013

Further improving digital certificate security

Posted by Adam Langley, Security Engineer

Late on December 3rd, we became aware of unauthorized digital certificates for several Google domains. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to ANSSI, a French certificate authority. Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.

09:09 46 %

Google bloque des certificats de sécurité Internet émis par une autorité française

08.12.2013 à 15:58 | Le Monde.fr



Une personne utilise Google sur une tablette tactile.
AFP/DAMIEN MEYER

Une potentielle importante faille de sécurité pour les internautes a été évitée. Google a annoncé samedi avoir bloqué plusieurs certificats de sécurité émis par une autorité de certification liée à l'Agence nationale de la sécurité des systèmes d'information française (Anssi, l'organisme chargé de la sécurité informatique de l'Etat français), après avoir découvert que ces certificats étaient possiblement corrompus.

Pourquoi la SSI ?

Erreur humaine – décembre 2013

••••• Orange F 09:35 43 %
googleonlinesecurity.blogspot.de

Google Online Security Blog

Saturday, December 7, 2013

Further improving digital certificate security

Posted by Adam Langley, Security Engineer

Late on December 3rd, we became aware of unauthorized digital certificates for several Google domains. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to ANSSI, a French certificate authority. Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.

07:09 46 %

Google bloque des certificats de sécurité Internet émis par une autorité française

08.12.2013 à 15:58 | Le Monde.fr



Une personne utilise Google sur une tablette tactile.
AFP/DAMIEN MEYER

Une potentielle importante faille de sécurité pour les internautes a été évitée. Google a annoncé samedi avoir bloqué plusieurs certificats de sécurité émis par une autorité de certification liée à l'Agence nationale de la sécurité des systèmes d'information française (Anssi, l'organisme chargé de la sécurité informatique de l'Etat français), après avoir découvert que ces certificats étaient possiblement corrompus.

••••• Orange F 09:34 43 %

ssi.gouv.fr



ANSSI

Agence nationale
de la sécurité
des systèmes d'information

Que faire en cas d'incident ? Le site du CERTA Portail de la sécurité informatique Documentation

Vous êtes ici : Accueil > menu > Actualités > Suppression d'une branche de l'IGC/A

Suppression d'une branche de l'IGC/A

7 décembre 2013

Suite à une erreur humaine lors d'une action de renforcement de la sécurité au ministère des finances, des certificats numériques correspondant à des domaines extérieurs à l'administration française ont été signés par une autorité de certification de la direction générale du Trésor rattachée à l'IGC/A.

Cette erreur n'a eu aucune conséquence sur la sécurité des réseaux de l'administration ni sur les internautes. La branche considérée de l'IGC/A a été coupée à titre préventif.

Un renforcement des procédures de l'IGC/A est en cours d'étude pour éviter qu'un tel incident ne puisse se reproduire.

Si © 2013 Flux RSS Contacts Informations éditeur Aide et accessibilité Presse Actualités Plus
ariat général de la défense et de la sécurité nationale Service public France.fr



Pourquoi la SSI ?

Atteinte à un STAD – **mercredi 18 juin 2014**

We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no** machine access had been achieved due to the intruder not having our Private Keys.

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for **will put Code Spaces in a irreversible position** both financially and in terms of on going credibility.
As such at this point in time **we have no alternative but to cease trading** and concentrate on supporting our affected customers in exporting any remaining data they have left with us.

<http://www.codespaces.com/>

Pourquoi la SSI ?

Atteinte à un STAD – **mercredi 18 juin 2014**

The screenshot shows a Twitter feed for the account @CodeSpaces. The feed displays seven tweets from June 18, 2014, each accompanied by an orange gear icon. The tweets are as follows:

- @chrismckee No this was our mistake, I can only assume our login and password was compromised
- @chrismckee we have raised a ticket with Amazon nothing they can do based on the events that took place, ongoing convo with the police
- @ifify If we are devastated, we are focussing on what we can do to support our customers and will figure out how to move forward another day
- @PlazaCommerce Please see the update at codespaces.com - We wont be back online.
- @LeeSmall65535 @GeoSheehy no external access to the data was achieved it was deleted from the administration console,
- @DBlackborough @petehotchkiss We store them in S3 buckets, all our buckets were cleared out via the admin console.
- @petehotchkiss It's a terrible position to be in, we have served this community for 7 years but we let everyone down in one night!

From: mike dudson <mikedudson@hotmail.com>
Reply-to: <mikedudson@hotmail.com>

how did u like the ddos attacks on ur server
and deleted ur files lol ur security is zero
we ow3ned and hacked ur sorry asses
<https://www.facebook.com/groups/HackersElite452/>

put ur website up we will trash it again

we are hackers elite Anonymous
we do not forgive
we do not forget
expect us

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013



Pourquoi la SSI ?

Hacktivism – vendredi 1^{er} novembre 2013

facebook Trouvez des personnes, des lieux ou d'autres choses Retrouver des am

Over-x Hocine (Hcn)

Ajouter S'abonner Message

Journal À propos Photos Amis Plus ▾

Vous connaissez Over-x ?

Pour voir ce qu'il partage avec ses amis, envoyez-lui une invitation.

Ajouter

Photos - 63

Over-x Hocine a partagé un lien.
il y a 2 heures

هذه أول تغريدة حول أحد دومنيات موقع وزارة الدفاع الفرنسية

Accueil
www.esa.sante.defense.gouv.fr

L'école de santé des armées (ESA) forme des jeunes gens se destinant à une carrière de médecin ou pharmacien militaire au sein du service de ...

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet Over-X
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet Over-X
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Pourquoi la SSI ?

Hacktivisme – vendredi 1^{er} novembre 2013

- ▶ "Je lance mes actions contre la France en souvenir des **martyrs Algériens.**"
- ▶ "Je choisis des sites qui ont de l'**influence**, des espaces **gouvernementaux.**"
- ▶ "C'est plus **efficace** pour être entendu, en plus des pertes financières."
- ▶ "Les **fichiers**, voilà la chose la plus importante pour moi. Les emails, les noms, les numéros de téléphone."
- ▶ Pseudonyme sur Internet **Over-X**
- ▶ 22 ans
- ▶ habite à Hadjout Wilaya de Tipaza en Algérie
- ▶ plus de 5000 piratages depuis 2011

Source : https://zataz.com/news/23170/pirate_-algerie_-over_.html

Définitions

1 Introduction

■ Pourquoi la SSI ?

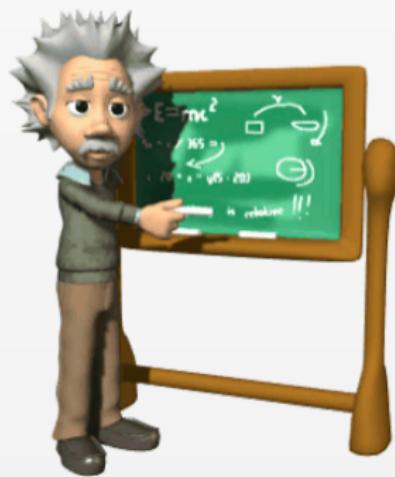
■ Définitions

- Information
- Système d'information
- Sécurité des Systèmes d'Information

■ Quizz



Information



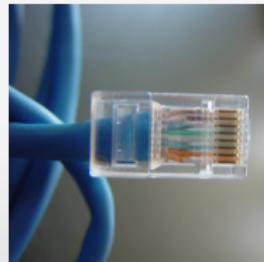
Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de supports

- ▶ La paire de cuivre support d'impulsions électriques
- ▶ La Fibre optique support d'impulsions lumineuses
- ▶ L'éther support des ondes radios.



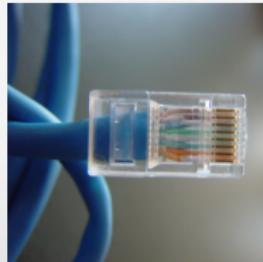
Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de supports

- ▶ La **paire de cuivre** support d'impulsions électriques
- ▶ La **Fibre optique** support d'impulsions lumineuses
- ▶ L'**éther** support des ondes radios.



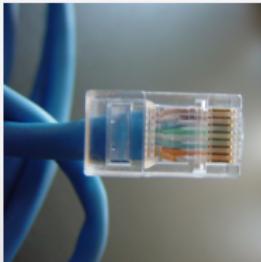
Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de supports

- ▶ La **paire de cuivre** support d'impulsions électriques
- ▶ La **Fibre optique** support d'impulsions lumineuses
- ▶ L'**éther** support des ondes radios.



Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de codes

- ▶ a b c d e f g h i j k l m n o p q r s t u v w x y z
- ▶ α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ ι φ χ ψ ω
- ▶ а б в г д е ё ж з и й к л м н о р с т у ф х ц ч щ ў Ѣ ю я
- ▶ 00110100 01101110 00100111 11100100

Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de codes

- ▶ a b c d e f g h i j k l m n o p q r s t u v w x y z
- ▶ α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ ι φ χ ψ ω
- ▶ а б в г д е ё ж з и й к л м н о р с т у ф х ц ч щ ў Ѣ ю я
- ▶ 00110100 01101110 00100111 11100100

Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de codes

- ▶ a b c d e f g h i j k l m n o p q r s t u v w x y z
- ▶ α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω
- ▶ а б в г д е ё ж з и й к л м н о р с т у ф х ц ч щ ў Ѣ ю я
- ▶ 00110100 01101110 00100111 11100100

Information

Information

Information : élément de connaissance, renseignement élémentaire susceptible d'être transmis grâce à un support et à un code.

Exemples de codes

- ▶ a b c d e f g h i j k l m n o p q r s t u v w x y z
- ▶ α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω
- ▶ а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч щ ъ ў ю я
- ▶ 00110100 01101110 00100111 11100100

Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

► 1 page = 184 562 octets

► 1Mo = 5,68 pages

► 1Go = 5 817,78 pages

► = 11,6 tonnes soit 29,028 kg

► 4Go = 23 271,13 pages

► 1To = 5 957 410,66 pages

► = 11,914,8 tonnes soit 31,283 kg

Exemples d'Informations

Conférence sur une page :
January 20, 1993

THE PRESIDENT: Thank you very much. And tonight, I have a high priority and deliver house of my speech. It's been a long time since we've had the Nixon message with these words. Madam Speaker,

In his speech, Mr. John R. D'Alessandro, Jr., from Baltimore, Maryland, our friend, and a member of the House at the moment. Let me add, and I am sure many of you will agree with me, preceding tonight is Speaker of the House of Representatives, Mr. Tom Foley, and the Vice

Madam Speaker, Vice President George Bush, members of Congress, and distinguished guests.

The one of certain beings are together at a conference - when decisions are hard and courage is needed.

We are here tonight to make a decision about what others are doing and what others are going to do, and others that are ours to begin. In all of this, much is asked of us. We must be bold, we must be courageous, and we must be determined.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

Since the last chapter are now to the House and the Senate, and I congratulate the Democratic majority, the Republicans, and the new members of the House.

Each of us is guided by our own conscience - and the standards of our constituents - and the standards of the people who elected us to office. We must set the same standards, and called to serve the good cause.

To reflect the nation's propensity to expand opportunity and to expand opportunity for all Americans to live up to their God-given potential.

Since the last chapter are now to the House and the Senate, and I congratulate the Democratic majority, the Republicans, and the new members of the House.

Each of us is guided by our own conscience - and the standards of our constituents - and the standards of the people who elected us to office.

We must set the same standards, and called to serve the good cause.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

It is a challenge and a challenge to our country - and the world - to meet that challenge.

stop. In the coming weeks, I will submit a budget that eliminates the federal deficit within the next five years. I will work with the Congress to make sure that we can restrain the spending aspects of the federal government, and we can balance the federal budget...



Be it, or not to be; that is the question:
Whether 'tis nobler to suffer the slings
And arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die, to sleep;
No more; and by a sleep to say we end
The heartache, and the thousand natural
shocks
That flesh is heir to. 'Tis a consummation
That comes not but like a dream;
To sleep, perchance to dream: ay, there's the
be it, or not to be; that is the question:

The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die, to sleep;

No more; and by a sleep to say we end
The heartache, and the thousand natural
shocks

That flesh is heir to. 'Tis a consummation
That comes not but like a dream;

To sleep, perchance to dream: ay, there's the
be it, or not to be; that is the question:

We have hitherto shirked this mortal coil,
But that the dread of something after death,

The undiscovered country from whose bourn

No traveler returns, puzzles the will

With a shakespearean gloom. One thing is clear,

He who would bear the whips and scorns

The tyrant's wrong, the peacock's coat,

Condemned to wear a weary life,

The smacks of office and the smirks

That come with being a public whale,

Why he himself might be better made

To sleep, perchance to dream: ay, there's the

be it, or not to be; that is the question:

To grant and never never a weary life,

But that the dread of something after death,

The undiscovered country from whose bourn

No traveler returns, puzzles the will

With a shakespearean gloom. One thing is clear,

He who would bear the whips and scorns

$$D(x) = (\sin^2(y) + \cos^2(y)) = \frac{1}{\sin^2(y)}$$

Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

- ▶ **1 page = 184 562 octets**
- ▶ **1Mo = 5,68 pages**
- ▶ **1Go = 5 817,78 pages**
 - ▶ = 11,6 rames soit 29,028 kg
- ▶ **4Go = 23 271,13 pages**
 - ▶ = 5 000 rames
- ▶ **1To = 5 957 410,66 pages**
 - ▶ = 1 000 000 rames soit 250 000 m³

Exemples d'Informations
Conférence sur une page :
January 20, 1999



In the coming weeks, I will submit a budget that eliminates the federal deficit within the next five years. I will propose a balanced budget amendment to the federal constitution so that we can restrain the spending aspects of the federal government, and we can balance the federal budget...

Mr. PRESIDENT: Thank you very much. And tonight, I have a high privilege and distinct honor of giving my first speech as Speaker of the House, and I do it with these words: Madam Speaker,

In a speech to the House of Representatives, Mr. D'Alessandro, Sr., from Baltimore, Maryland, was presented with a copy of the Constitution of the United States, presented by the House of Representatives, and he accepted it. Mr. Speaker, preceding tonight as Speaker of the House of Representatives, I would like to thank him.

Madam Speaker, Vice President Cheney, members of Congress, distinguished guests, ladies and gentlemen,

The one of certain beings are together at a conference - when decisions are hard and courage is needed. We are here to make those decisions. We are here to make those decisions that are hard and courageous, and others that are easy to begin. In all of this, much is asked of us. We are asked to be bold, to be courageous, to be determined, to be strong, to be challenges and determined - and the world to thank us for our leadership.

Since the last chapter are now to the House and the Senate, and I congratulate the Democratic majority, the Republicans, and the independent members. Each of us is guided by our own convictions - and the task before us is to work together, all of us, to meet the same standards, and called to serve the good purpose. To reflect the nation's propensity to expand the opportunity for all Americans, and to pass laws that allow generations to guard America against all the challenges that lie ahead with them we have our full to defend us.

We're in a time of great uncertainty, and the world is changing rapidly and necessarily to our life. Like many before us, we can work through our differences, and achieve high levels of success. Our country is strong. Our economy must carry which side of the scale on - as long as we work together, and we work hard, and we do what we do. Our job is to make life better for our fellow Americans, and to help them to build a future of hope and opportunity, and to keep our country strong, and to defend us.

A future of hope and opportunity begins with a growing economy - and that is what we have. We're creating more than 100,000 new jobs every month, a recovery that has created 1.2 million new jobs - so far. Unemployment is low, inflation is low, and wage are strong. This is a time of opportunity, and we must be to keep it that way, and with more government, but with less waste.

Next week, I'll submit a full report on the state of our economy. Tonight, I want to focus on the most important action that we can take to improve our economy. First, we must balance the federal budget. We can do no better than to start with a balanced budget, and to end with a balanced budget, and to end with a balanced budget in Washington, D.C. We set a goal of cutting the deficit in half by 2000, and set that goal this year ahead of schedule. Now let me take the next

step. In the coming weeks, I will submit a budget that eliminates the federal deficit within the next five years. I will propose a balanced budget amendment to the federal constitution so that we can restrain the spending aspects of the federal government, and we can balance the federal budget...

Be it, or not to be, that is the question:
That is a knotted question, and it is a knotted.
The ship and arrows of corrosion ferret,
Or to take arms agains a sea of troubles,
And by opposing end them. To thine selfe be it a knotted;
No more, and by a sleep to say we end
The heartache, and the thousand natural
shocks
That this knotted. 'Tis a knotted
That this knotted. 'Tis a knotted
To be, or not to be: that is the question;
To sleep, perchance to dream: ay, there's the
For in that sleep of death what dream may
We have here stuff'd of this mortal coil,
That grieves us: hence the saying, 'To die,
To sleep: if it be so, we shall shortly
See such sights as we have never seen.
The eye倦's wing, the proud man's con-
temny,
The snail's slow drapery, the lass's bairn,
The ant's pretensions, the weaver's bairn,
The shank's office and the smock's bairn,
What be himself might his master make
Of a knotted? For in that sleep of death,
To grant me never under a weary life,
But that the death of sleeping we death,
No trouble returns, prunes the will
To thine selfe be it a knotted: that we have
Thus to others who know not of?

This remonstrance does that much of us all
To sit downe with the quiet of thought,
And to be quiet. 'Tis a knotted: that we have
With the regard that covers us very,
The knotted, and the knotted, and the knotted
The knotted, and the knotted, and the knotted
$$D(x) = (\sin^2(y) + \cos^2(y)) - \frac{1}{x^2}$$

Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

- ▶ 1 page = 184 562 octets
 - ▶ 1Mo = 5,68 pages
 - ▶ 1Go = 5 817,78 pages
 - ▶ = 11,6 rames soit 29,028 kg
 - ▶ 4Go = 23 271,13 pages
 - ▶ = 1 clef USB
 - ▶ = 46,5 rames soit 116,11 kg
 - ▶ 1To = 5 957 410,66 pages
 - ▶ = 103,6 rames soit 278,72 kg



Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

- ▶ **1 page = 184 562 octets**
- ▶ **1Mo = 5,68 pages**
- ▶ **1Go = 5 817,78 pages**
 - ▶ = 11,6 rames soit 29,028 kg
- ▶ **4Go = 23 271,13 pages**
 - ▶ = 1 clef USB
 - ▶ = **46,5 rames soit 116,11 kg**
- ▶ **1To = 5 957 410,66 pages**

Exemples d'Informations

Conférence sur une page

January 20, 2009

THE PRESIDENT: Thank you very much. And tonight, I have a high priority and deliver house of my speech. It's been a long time since we've had the same message with these words. Madam Speaker,

In his speech, the Honorable Nancy Pelosi, D'Alessandro, 2, from Baltimore, Maryland, our President, and the House at the session. Let nothing stand in the way of the people who work hard every day to make America great again.

Madam Speaker, Vice President Cheney, members of Congress, distinguished guests, and friends.

The one of certain things go together at a conference:

what decisions are hard and courage is needed. We're here to do what's right, and what's right and others that are ours to begin. In all of this, much is asked of us, and we must meet those challenges with a spirit of challenge and determination - and the world to thank us for it.

Since the last chapter are now to the House and the Senate, and I congratulate the Democratic majority, the Republicans, and the House and the Senate.

Each of us is guided by our own convictions - and the values that we hold dear. And all of us share the same standards, and called to serve the good cause.

To reflect the nation's propensity to expand the opportunity for all Americans, and to pass on to future generations a guard American against all the challenges ahead with them we have our full

to defend it.

We're in this for the long haul, and we must be there for the long haul, and stay true to the life.

As we work through our differences, and achieve high standards of living for all Americans. Our country must care which side of the aisle we sit on - as long as we're working together to get the job done.

Our job is to make life better for our fellow Americans, and to help them to build a better life for themselves and their families. And we must do this to keep it this way, and with more government, but with less waste.

A future of hope and opportunity begins with a growing economy - and that is what we have. We're on the right track, and we're making progress - and a recovery that has created 1.2 million new jobs - so far. Unemployment is low, inflation is low, and wage are strong. This is the kind of economy that we want to keep it this way, and with more government, but with less waste.

Next week, I'll submit a full report on the state of our economy. Tonight, we will focus on the most important action we can take to move forward - and that is to pass a budget.

First, we must balance the federal budget. We must do the right thing, and we must do it now. We must end the spending discipline in Washington, D.C. We set a goal of cutting the deficit in half by 2010, and use that goal

step. In the coming weeks, I will submit a budget that eliminates the federal deficit within the next five years. I will work with the House and the Senate to make sure we can restrain the spending aspects of the federal government, and we can balance the federal budget.



To be, or not to be, that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die, to sleep,
No more; and by a sleep to say we end
The heartache and the thousand sorrows
sighed.
That would be to die. 'Tis a consummation
That comes not but like a睡。
To sleep, perchance to dream: Ay, there's the rub!
For in that sleep of death what dreams may

We have here夫 of this mortal coil,
That grieves us; then it is a thought
That we shall shortly sleep in death,
Or we shall wake in hell.

He who would bear the whips and scorns of
The emperor's wrath, the proud man's contumely,
The censure of the world, his enemies' malice,
The smacks of office and the sneers of fortune,
Who he himself might his easier make
Than we ourselves feel; is this notwithstanding
To grant and never suffer a weary life.

But that the dread of something after death,
The undiscovered country from whose bourn
No traveler returns, puzzles the will
And makes us rather bear those ills we have

Than fly to others we know not of?

This remainder does not much concern me; but
Such ills we have in this life, which may come
is added o'er us with the pale cast of thought,
And which often takes us when we are asleep,
With the regard that curtains turn away;

The life before us, and which comes not back

The life before us, and which comes not back

With the regard that curtains turn away;
The life before us, and which comes not back

With the regard that curtains turn away;

Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

- 1 page = 184 562 octets
 - 1Mo = 5,68 pages
 - 1Go = 5 817,78 pages
 - = 11,6 rames soit 29,028 kg
 - 4Go = 23 271,13 pages
 - = 1 clef USB
 - = 46,5 rames soit 116,11 kg
 - 1To = 5 957 410,66 pages
 - = 11 914,8 rames soit 29,72 T



Information

Taille de l'information

Référence : 1 page A4 enregistrée au format PDF de Adobe.

- ▶ **1 page = 184 562 octets**
- ▶ **1Mo = 5,68 pages**
- ▶ **1Go = 5 817,78 pages**
 - ▶ = 11,6 rames soit 29,028 kg
- ▶ **4Go = 23 271,13 pages**
 - ▶ = 1 clef USB
 - ▶ = 46,5 rames soit 116,11 kg
- ▶ **1To = 5 957 410,66 pages**
 - ▶ = 11 914,8 rames soit 29,72 T

Exemples d'informations

Conférence sur une page :
January 20, 1993

THE PRESIDENT: Thank you very much. And tonight, I have a high priority and distinct honor of giving the opening speech at the State of the Union message with these words: Madam Speaker.

In his speech, the Honorable Newt Gingrich, D'Arlacino, N. from Baltimore, Maryland, our President, and the House at the session. Let nothing stand in the way of the budgetary policy of the House, preceding tonight as Speaker of the House of Representatives, the Honorable Newt Gingrich, Madam Speaker, Vice President Cheney, members of Congress, and distinguished guests.

The one of certain things go together at a conference - when decisions are hard and courage is needed. We are faced with some very difficult choices and others that are easy to begin. In all of this, much will be asked of us, and we must meet those challenges and determined resolve - and the world to thank us for it.

Since the last election are now to the House and the Senate, and I congratulate the Democratic majority, the Republicans, and the House and the Senate. Each of us is guided by our own convictions - and the task before us is to work together to fulfill the main standards, and called to serve the good cause. To reflect the nation's propensity to spend and the need to make the right choices in order to pass to future generations good America against all the odds. And let's do it with them who have sent us to defend us.

We're in a bind. We're in a bind. We're in a bind. And we're in a bind. And we're in a bind. Like many before us, we can work through our differences, and achieve high standards of living for all Americans. One of the most important thing of the role of the president is to be a leader. Our job is to lead the country, and to help them to build a better life for themselves and their families. And that's what we have to do.

A future of hope and opportunity begins with a growing economy - and that is what we have. We've got a strong economy, and one that is growing, which has created 1.2 million new jobs - so far. Unemployment is low, and the economy is strong, and growing. That's why we have to keep the economy strong. That's why we have to keep it strong, and with more government, but with less regulation.

Next week, I'll submit a full report on the state of our economy. Tonight, I want to focus on the most important action that we can take to improve the economy. First, we must balance the federal budget. We must do the right thing, and that's what we're doing. We're spending discipline in Washington, D.C. We set a goal of cutting the deficit in half by 2000, and use that goal this year ahead of schedule. Now let me take the next

step. In the coming weeks, I will submit a budget that eliminates the federal deficit within the next few years. I will work with the Congress to do this. And then, we can restrain the spending aspects of the federal government, and we can balance the federal budget.



To be, or not to be, that is the question:
Whether 'tis nobler to suffer the slings
And arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die, to sleep,
No more; and by a sleep to say we end
The heartache and the thousand sorrows
sucks

That which we are, we are; our fatal¹
Nature then let us not wrong. One to sleep
Is a knell to end life's little day.

For in that sleep of death what dreams may

We have here sleep of this mortal coil,
That grieves us; then it is import
To take arms against a sea of troubles,

And by opposing end them? To die, to sleep,
To sleep perchance to dream: Ay, there's the

For in that sleep of death what dreams may

We have here sleep of this mortal coil,
That grieves us; then it is import
To take arms against a sea of troubles,

And by opposing end them? To die, to sleep,
To sleep perchance to dream: Ay, there's the

The o'ercomer's woe, the proud man's con-
tempt,

The bane of disappointed love, the bane's
The snakish of offices and the snakish

When he himself might his center make
His center make his center make his center make

To grant and never never a weary life,
But that the dead are sleeping the death,

The snakish of offices and the snakish

No trouble returns, prunes the will,

That is, to take arms against a sea of

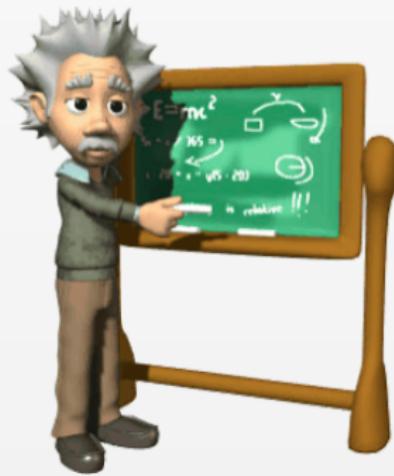
This remonstrance does that much of us all:

It is a knell to end life's little day.

With this regard consider how sorely
The He of Orchid Neurys,

$$\ln(x) + (\sin^2(y) + \cos^2(y)) = \frac{1}{\sin^2(y)}$$

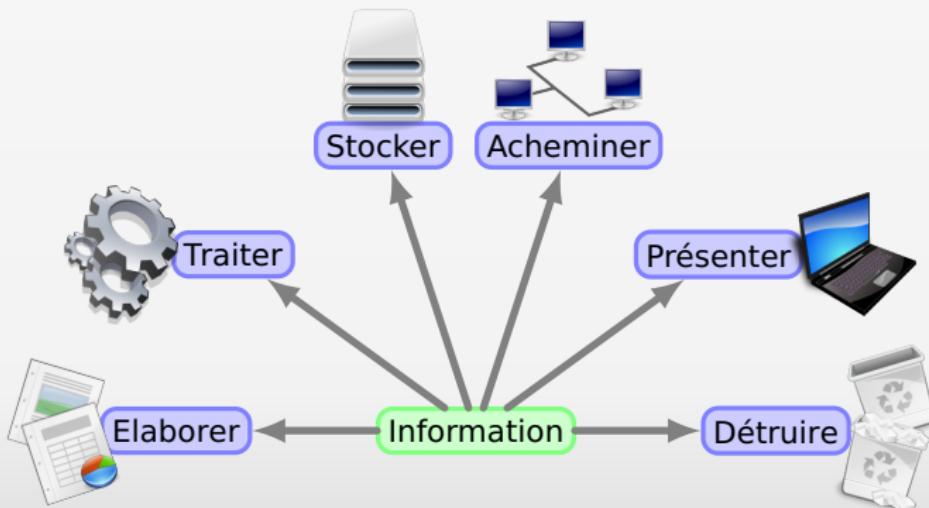
Système d'information



Système d'information

Système d'information

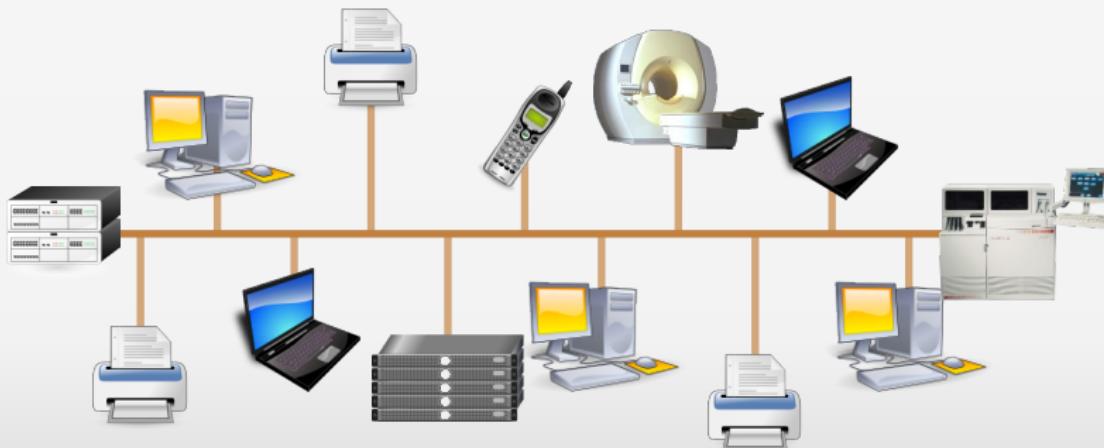
Un **Système d'Information** est un ensemble organisé de ressources matérielles, logicielles et humaines destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.



Système d'information

Système d'information

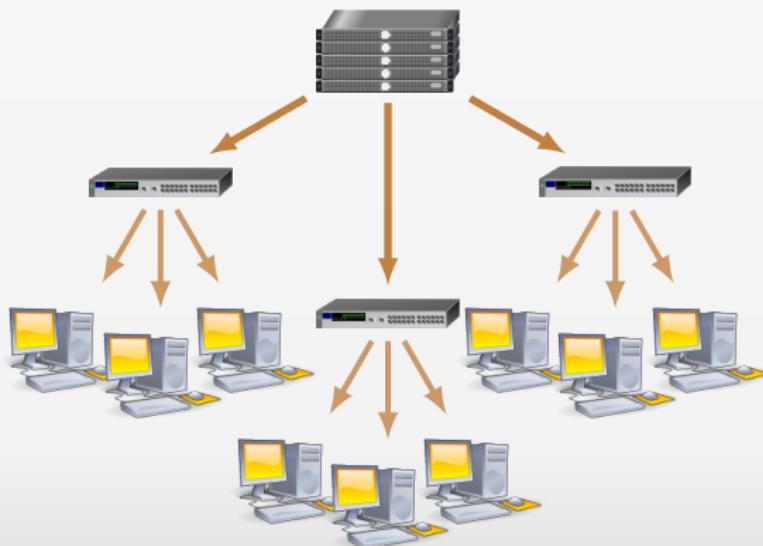
Concrètement, il s'agit des réseaux informatiques et téléphoniques, des ordinateurs, des serveurs, des autocom, des téléphones, des télécopieurs, des imprimantes, photocopieurs, des systèmes d'exploitation, des logiciels utilisés sur ces équipements et des personnels qui les administre....



Intranet

Intranet

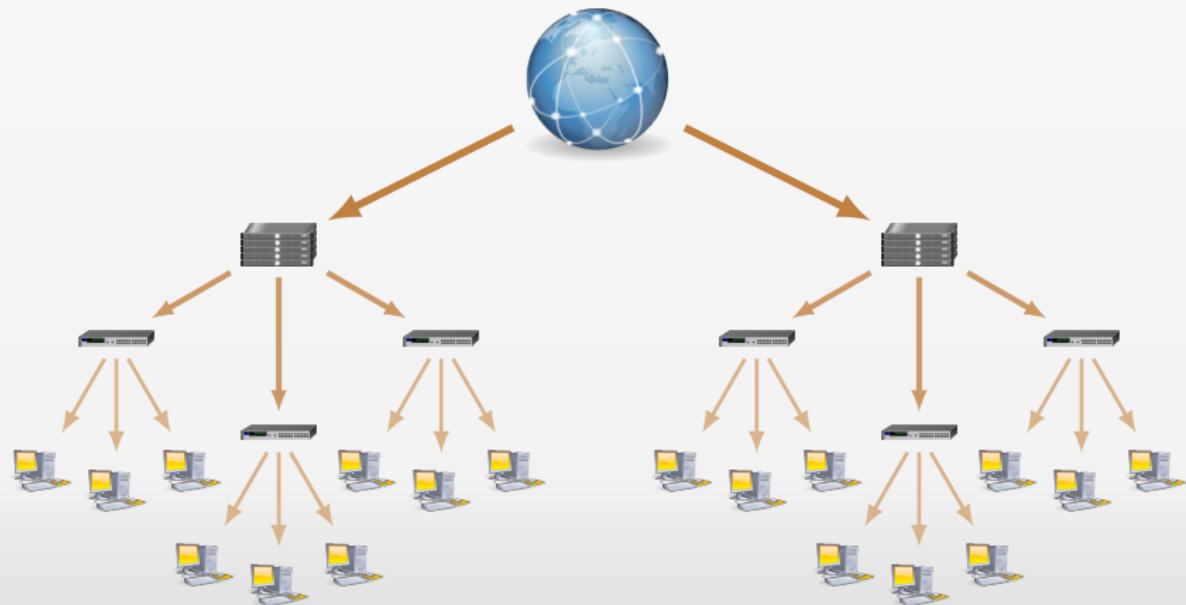
Un intranet résulte de l'interconnexion de plusieurs ordinateurs et serveurs



Internet

Internet

L'Internet résulte de l'interconnexion de plusieurs intranets à l'échelle mondiale



Sûreté & Sécurité



Sûreté

Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **panne**.

Sûreté & Sécurité



The screenshot shows a news portal for Georgia. At the top right is the logo of the Ministry of Internal Affairs of Georgia. Below it, there are two main news items:

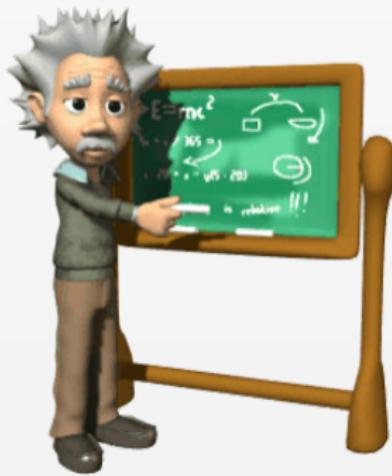
- 17 თებერვალი 2008**: A meeting between the Minister of Internal Affairs and the European Union delegation. The text discusses the importance of cooperation and mutual trust.
- 28 თებერვალი 2008 / 18:00**: A press conference by the Ministry of Internal Affairs to address recent events.

On the left side of the page, there is a sidebar with links to other news sections and a search bar.

Sécurité

Ensemble des mesures qui mettent un système et les informations qu'il traite à l'abri de toute **agression**.

Sécurité des Systèmes d'Information



Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, **la sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.

Confidentialité

Disponibilité

Intégrité

Authentification

Traçabilité

Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, **la sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.



Disponibilité

Intégrité

Authentification

Traçabilité

Confidentialité

Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, la **sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.



Confidentialité



Disponibilité

Intégrité

Authentification

Traçabilité

Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, la **sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.



Confidentialité



Disponibilité



Intégrité

Authentification

Traçabilité

Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, la **sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.



Confidentialité



Disponibilité



Intégrité



Authentification

Traçabilité

Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information (Référentiel Général de Sécurité)

La **sécurité des systèmes d'information** recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de **garantir**, au juste niveau requis, la **sécurité des informations** d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.



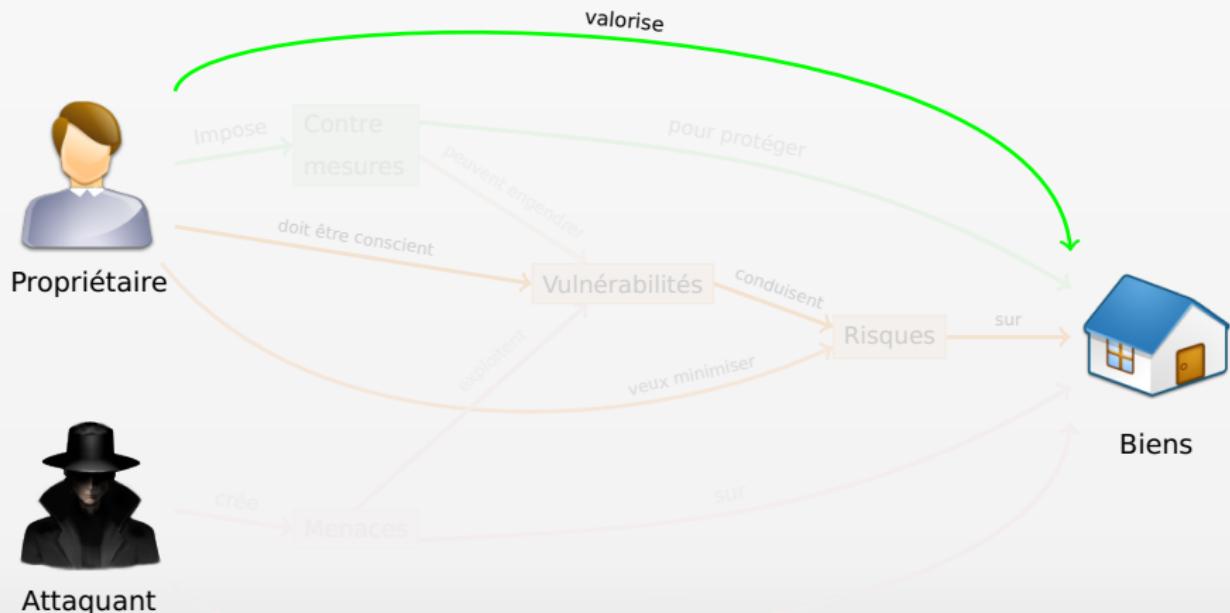
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



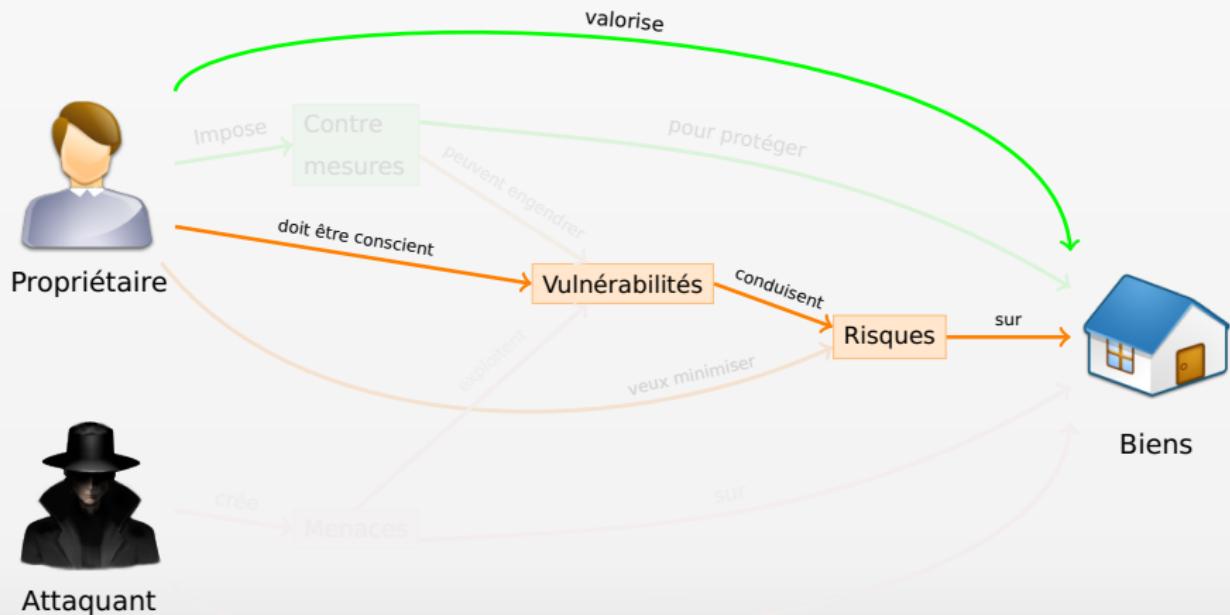
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



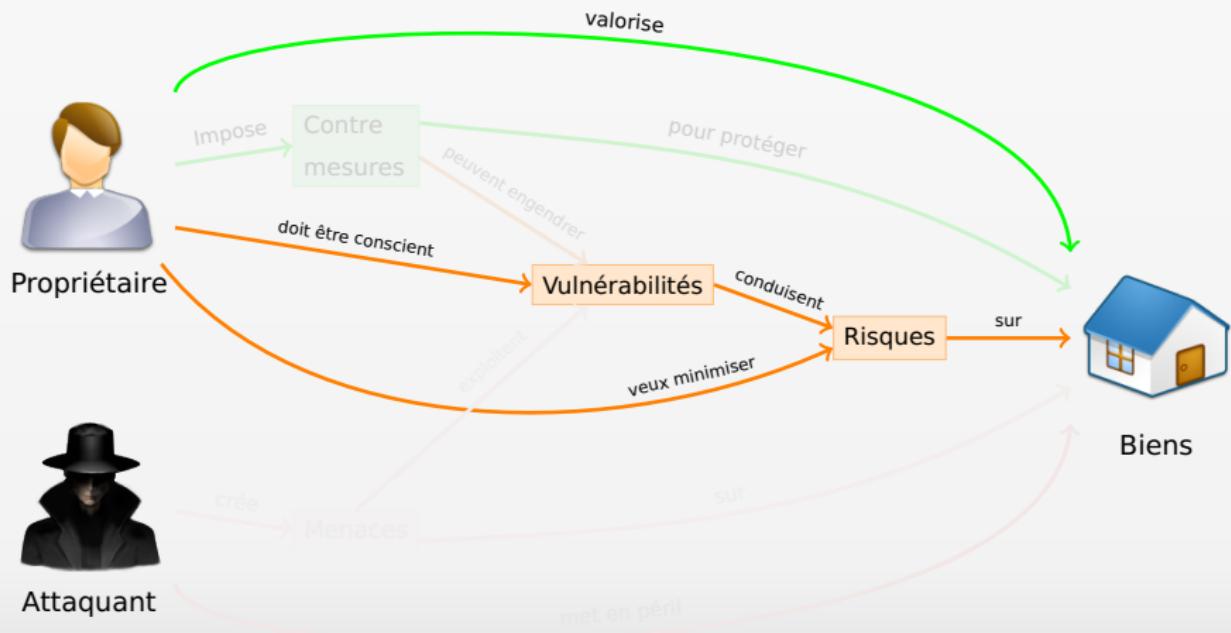
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



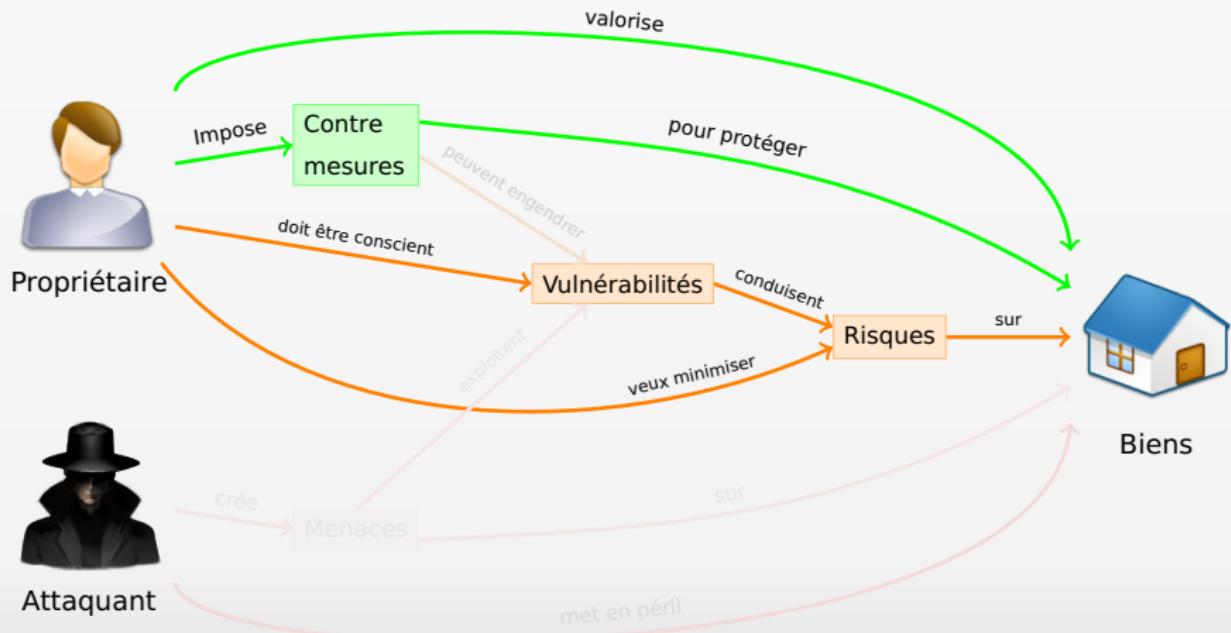
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



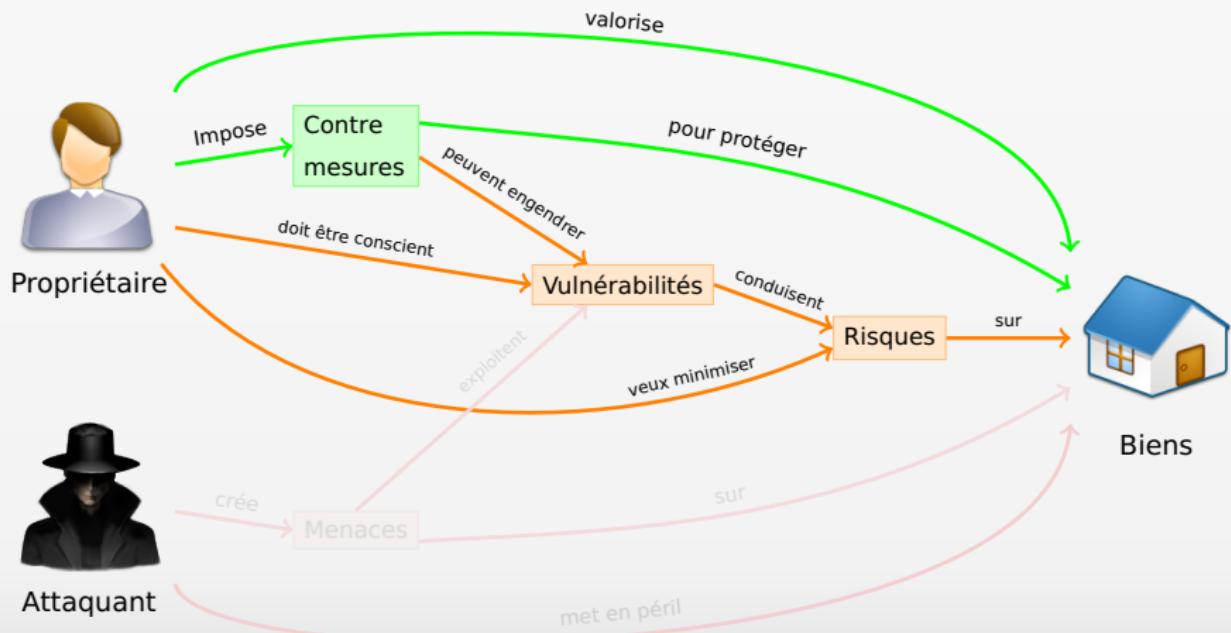
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



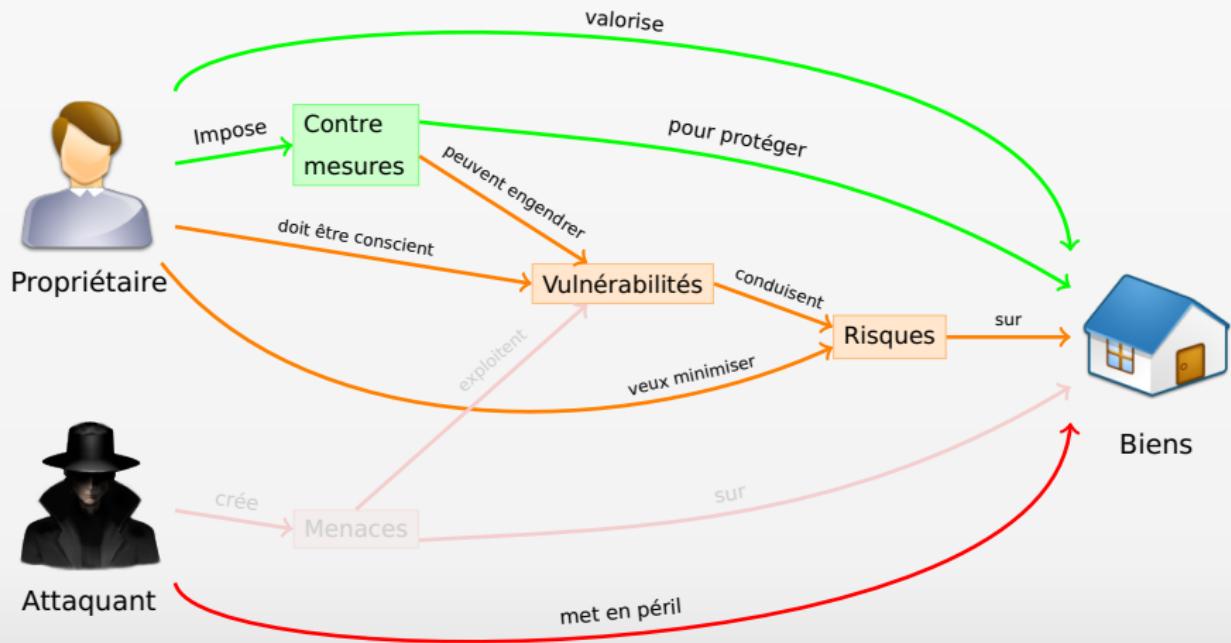
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



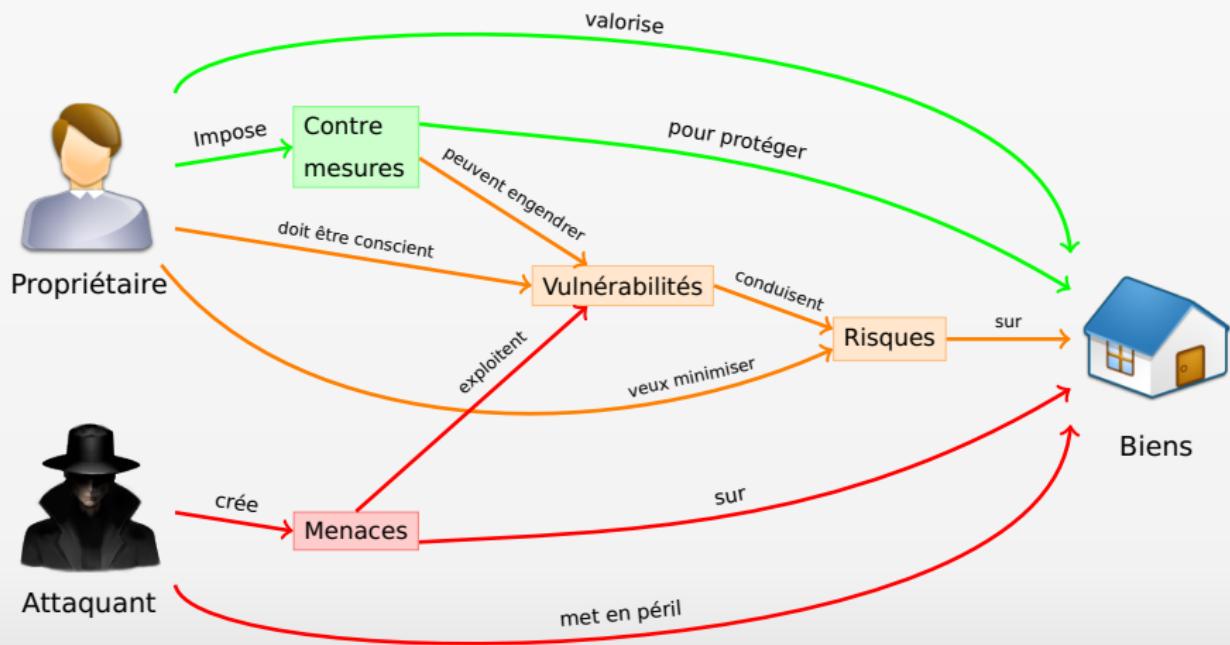
Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



Sécurité des Systèmes d'Information

En résumé : le **modèle général de sécurité**



Quizz

1 Introduction

- Pourquoi la SSI ?
- Définitions
 - Information
 - Système d'information
 - Sécurité des Systèmes d'Information
- Quizz



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sensitive ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sensible ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sensible ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ **Combien de mots de passe utilisez-vous ?**
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sur Internet ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sur Internet ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ **Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?**
- ▶ Quelle est la durée de vie d'une information sur Internet ?



Petit Quiz ...

- ▶ Connaissez vous le nom de votre correspondant SSI ?
- ▶ Que faites vous quand vous quittez momentanément votre station de travail ?
- ▶ Quelle est la longueur de votre mot de passe ?
- ▶ Combien de mots de passe utilisez-vous ?
- ▶ Reste-t-il des documents sur votre bureau quand vous partez le soir ?
- ▶ Combien peut coûter la copie frauduleuse de logiciel et l'utilisation de logiciels piratés ?
- ▶ Quelle est la durée de vie d'une information sur Internet ?



Risques, menaces et vulnérabilités

1 Introduction

2 Risques, menaces et vulnérabilités

3 Contres mesures

4 Conclusion



Le risque

2 Risques, menaces et vulnérabilités

- Le risque
- Les menaces
- Les vulnérabilités



Sécuriser un **système d'information** revient à essayer de **se protéger contre les risques**, liés à son utilisation et pouvant avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite.



L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

l'impact financier et/ou la probabilité de survenance d'un événement indésirable.

L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

l'impact financier et/ou la probabilité de survenance d'un événement indésirable.

L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

La combinaison des ces trois facteurs fonde le « risque », qui permet de mesurer l'impact financier associé à la probabilité d'occurrence d'un événement menaçant.

L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

La combinaison des ces trois facteurs fonde le « risque », qui permet de mesurer l'impact financier et/ou la probabilité de survenance d'un évènement indésirable.

L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

La combinaison des ces trois facteurs fonde le « risque », qui permet de mesurer l'impact financier et/ou la probabilité de survenance d'un évènement indésirable.

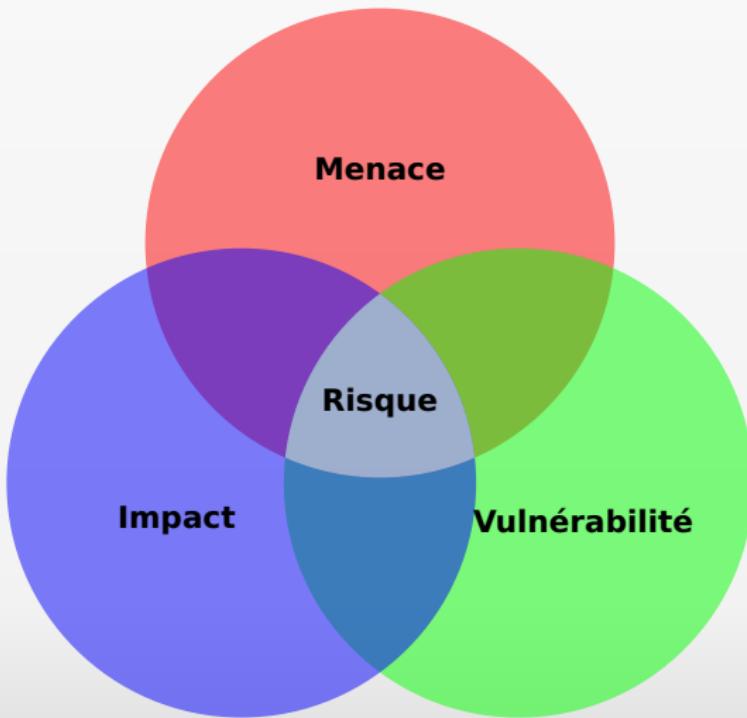
L'équation du risque

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Impact}}{\text{Contre-mesures}}$$

- ▶ La **menace** désigne l'ensemble des éléments, internes et externes, pouvant nuire aux actifs d'une organisation
- ▶ La **vulnérabilité** exprime toutes les faiblesses des ressources qui pourraient être exploitées par des menaces, dans le but de les compromettre
- ▶ L'**impact** est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, impact juridique, perte de crédibilité...

La combinaison des ces trois facteurs fonde le « risque », qui permet de mesurer l'impact financier et/ou la probabilité de survenance d'un évènement indésirable.

Le risque en résumé



Les menaces

2 Risques, menaces et vulnérabilités

- Le risque
- Les menaces
- Les vulnérabilités



Les menaces

Définition

Menace

Une menace est une **Violation potentielle de la sécurité**. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- ▶ les menaces non intentionnelles
- ▶ les menaces intentionnelles



Les menaces

Définition

Menace

Une menace est une **Violation potentielle** de la sécurité. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- ▶ les menaces **non intentionnelles**
- ▶ les menaces **intentionnelles**



Les menaces

Définition

Menace

Une menace est une **Violation potentielle** de la sécurité. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- les menaces **non intentionnelles**
- les menaces **intentionnelles**



Les menaces

Définition

Menace

Une menace est une **Violation potentielle** de la sécurité. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- ▶ les menaces **non intentionnelles**
- ▶ les menaces **intentionnelles**



Les menaces

Définition

Menace

Une menace est une **Violation potentielle** de la sécurité. La menace doit-être considéré comme **permanente** et il est par conséquent difficile d'agir dessus.

On distingue :

- les menaces **non intentionnelles**
- les menaces **intentionnelles**



Les menaces

Les menaces non intentionnelles

Incendie, dégâts des eaux, pollution, accidents majeurs



Exemples de mesures de sécurité :

- ▶ Système de détection incendie, extinction incendie adaptée (FM200)
- ▶ repérage des tuyaux, détecteur d'inondation

Les menaces

Les menaces non intentionnelles

Phénomènes climatiques, sismiques, volcaniques, météorologiques, crue



Exemples de mesures de sécurité :

- ▶ constructions aux normes sismiques
- ▶ zones inondables

Les menaces

Les menaces non intentionnelles

Défaillance de la climatisation, perte d'alimentation énergétique, perte des moyens de télécommunications

Modèles	Hauteur (U)	Quantité maximum par baie de 42 U	Chaleur maximum par baie (kW)	Charge calorifique maxi par m ² (kW/m ²)
Dell Power Edge 1850	1	42	23	34,4
Dell Power Edge 1855	7	6	24	38
Sun Fire B 1600	3	14	14,5	21,5
IBM BladeCenter Type 8677	7	6	24	38

Chaleur dégagée par quelques serveurs du marché
doc. Yalta / source Emerson Network Power



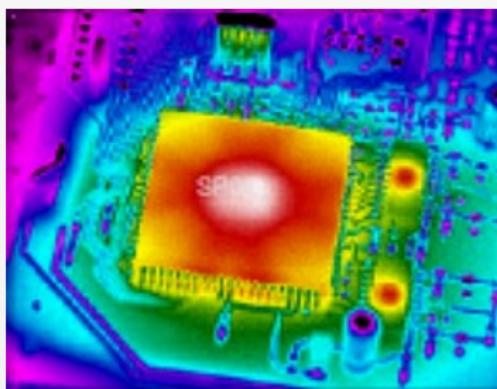
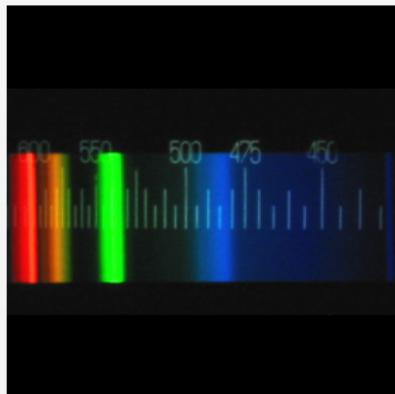
Exemples de mesures de sécurité :

- ▶ Refroidissement (climatisation), gestion du taux d'humidité
- ▶ Redondance de l'alimentation électrique
- ▶ Duplication des arrivées réseaux et téléphones

Les menaces

Les menaces non intentionnelles

Rayonnements électromagnétiques, rayonnements thermiques, impulsions électromagnétiques



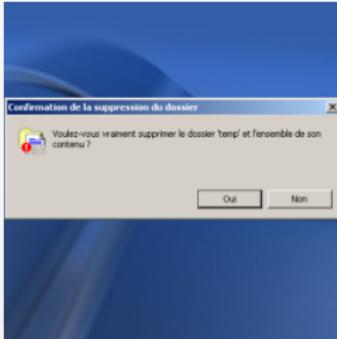
Exemples de mesures de sécurité :

- ▶ norme tempest

Les menaces

Les menaces non intentionnelles

Panne, dysfonctionnement matériel et logiciel, erreur de saisie, erreur d'utilisation



Exemples de mesures de sécurité :

- ▶ Prise en compte de la SSI dès le début d'un projet informatique
- ▶ Formation des utilisateurs aux outils informatiques utilisés
- ▶ Politique adaptée pour le choix des technologies logicielles

Les menaces

Les menaces intentionnelles

Saturation ou destruction de matériel, piégeage et utilisation illicite du matériel,
altération de données



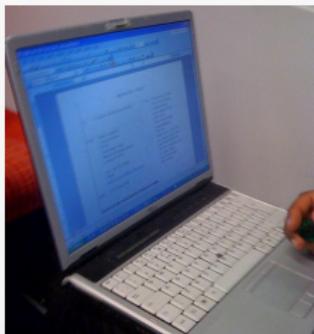
Exemples de mesures de sécurité :

- ▶ Vigilance, fermeture systématique des bureaux
- ▶ Chiffrement des supports de stockage de données et des flux réseaux

Les menaces

Les menaces intentionnelles

Vol de supports, de documents, de matériels, divulgation interne et externe, interception de signaux parasites compromettants, espionnage à distance



« Ministers were embarrassed by a new security row last night after one of Business Secretary Peter Mandelson's top officials allowed secret Whitehall information to be read on a packed commuter train. Zahir Sachak's **exchange of 'restricted' emails**, including details of commercially sensitive Government policies and an admission that taxpayers' money was being wasted, was viewed by MP's secretary Clare Gledhill, who was sitting next to him **on the train out of Waterloo... »**

<http://www.dailymail.co.uk/news/article-1082375/The-zzzzivil-servant-fell-asleep-train-laptop-secrets-view.html>

Exemples de mesures de sécurité :

- ▶ Politique du bureau vide, destruction des documents sensibles
- ▶ Fixation des ordinateurs par câble
- ▶ Politique stricte pour l'utilisation des technologies sans fils

Les menaces

Les menaces intentionnelles

Altération, piégeage ou copie frauduleuse de logiciel, utilisation de logiciels contrefaits ou copiés



 Bienvenue, humains ! Je suis prêt pour vous.

Nous sommes venus en paix et avec bienveillance !

- Un robot ne peut blesser un être humain ou, par son inaction, permettre qu'un être humain soit blessé.
- Les robots ont vu des choses que vous ne pourriez pas croire.
- Les robots sont vos copains en plastique avec lesquels il est amusant d'être.
- Les robots ont des postérieurs en métal brillant qui ne doivent pas être mordus.

Et ils ont un plan.

 Easter egg - Firefox - about : robots

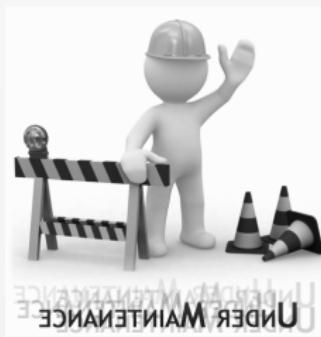
Exemples de mesures de sécurité :

- ▶ Élaboration de listes blanches de logiciels autorisés
- ▶ Limitation des droits d'utilisateurs (impossibilité d'installation de logiciels)

Les menaces

Les menaces intentionnelles

Atteinte à la maintenabilité du système d'information, atteinte à la disponibilité du personnel



avis d'arrêt de travail

initial de prolongation (?) volet 1, à adresser au service médical

à adresser, dans les deux jours, à l'organisme d'assurance maladie, à l'aide de l'enveloppe M, le Médecin-Conseil tel. 1-102-41-1er, 1-102-44, L-151-1, L-221-1, L-3224, R-221-11, 0-220-6, L-376-4, 0-210-33 et D-111-42 du Code de la sécurité sociale

adresse : _____

numéro d'immatriculation _____

nom (auj. s'il n'y a pas nom d'espouse) _____
prénom _____

code de l'organisme de rattachement (voir votre attestation papier-vitré) _____

adresse où le malade peut être visité (si différente de votre adresse habituelle) _____

code postal _____ ville _____ n° de téléphone : _____

bâtiment : étage : appartement : code d'accès de la résidence : _____

(T) l'employeur de votre culture est consigné et cette adresse se situe hors de votre département de résidence

activité salariée _____ profession indépendante _____

sans emploi _____ date de cessation d'activité _____ précisez votre situation _____

l'arrêt présent fait suite à un accident causé par un tiers _____ oui _____ non _____

l'arrêt présent fait suite à une autre thématique _____ oui _____ non _____

l'arrêt présent est en rapport avec l'affection pour laquelle vous êtes pensionné(e) de guerre _____ oui _____ non _____

(T) si le patient présent est prescrit par un médecin autre que le médecin qui a prononcé l'arrêt initial, indiquer nomprénom du médecin présent _____

nom, prénom ou dénomination sociale _____

adresse _____

n° téléphone : _____ e-mail : _____



Exemples de mesures de sécurité :

- ▶ Transfert de connaissance – suppression de l'expert unique
- ▶ Attention particulière apportée aux contrats de maintenance
- ▶ Éviter la télémaintenance

Les menaces

Les menaces intentionnelles

Écoute passive, usurpation de droits, reniement d'actions, fraude, abus de droit

```
# sudo tcpdump -n -s 0 -ttttvvv -R -i en1
tcpdump: listening on en1, link-type EN10MB (Ethernet), capture size 65535 bytes
2009-12-26 21:11:41.881797 IP (tos 0x0, ttl 64, id 3824, offset 0, flags [DF], proto TCP (6), length 709)
    192.168.1.95.60175 > 209.85.229.105.80: Flags [P..], cksum 0x286e (correct), seq 3513748854:3513749491, ack 1466425235, win 65535, options [nop,nop,T5 val 500170654 ecr 636534537], length 657
E.....W....|. ....U...P.BHg.....(n.....
.....G...|.....U/1
Hosts: www.google.fr
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=q999d7o35br0+4ieded1554e77o4;FF=4;LD=fr;PHPSESSID=1261857246;LTI=1261857646;S=Vi-kk5hu10Grphac; H1D=30+E0L7T1Idki#oRo72
.....Qo1deddt;ITQB515cspxz75sk1q5ic0_32RISvsa4rRizwL7lXCTI+7Lvg8-as;j0qKdsJ2;8AVVYRhsupla9C9u5nzedav;e10kh6gfa;T=1CtH+25

2009-12-26 21:11:41.956623 IP (tos 0x0, ttl 53, id 40858, offset 0, flags [none], proto TCP (6), length 1470)
    209.85.229.105.80 > 192.168.1.95.60175: Flags [...], cksum 0xfe9a (correct), seq 1:1419, ack 657, win 266, options [nop,nop,T5 val 636573368
E.....S.K.,U...P.Hg...o.....
.....N.V....HTTP/1.1 200 OK
Date: Sat, 26 Dec 2009 20:11:40 GMT
Expires: -
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gce
Content-Length: 5088
X-HSS-Protection: 0
```

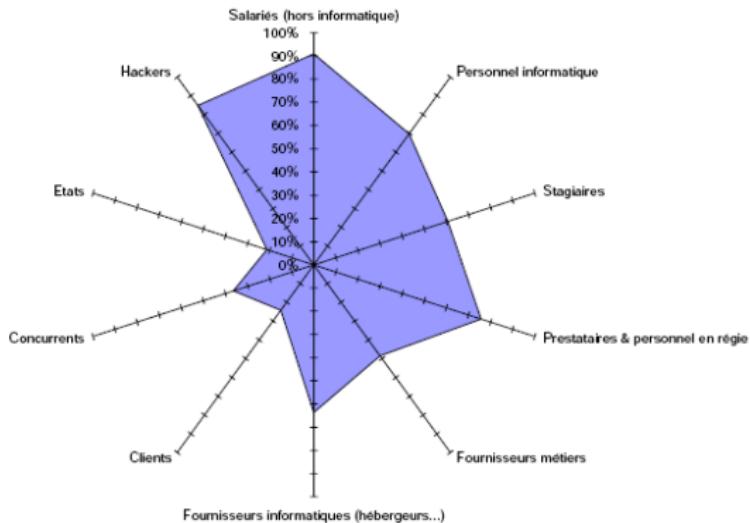
Exemples de mesures de sécurité :

- Mécanismes de signature, d'authentification et de chiffrement
- Login et mot de passe secret, authentification forte

Les menaces

La cybercriminalité : **Origine** (source CIGREF)

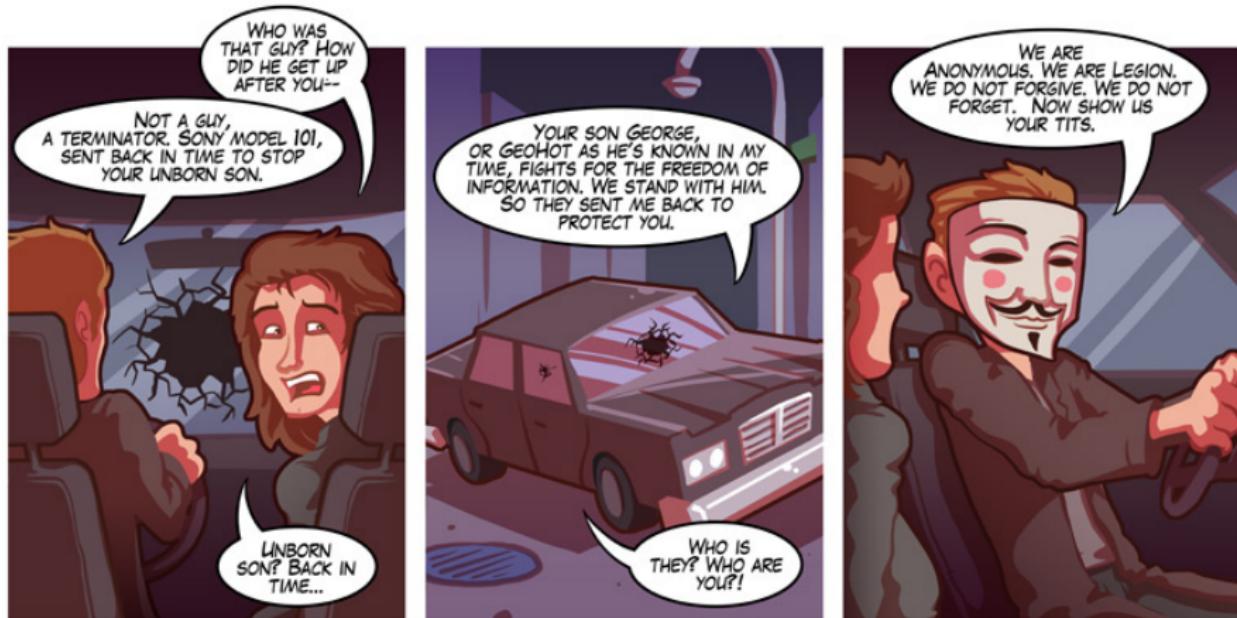
Origine de la cybercriminalité



Les menaces

La cybercriminalité : Évolution

La nouvelle cybercriminalité



Les vulnérabilités

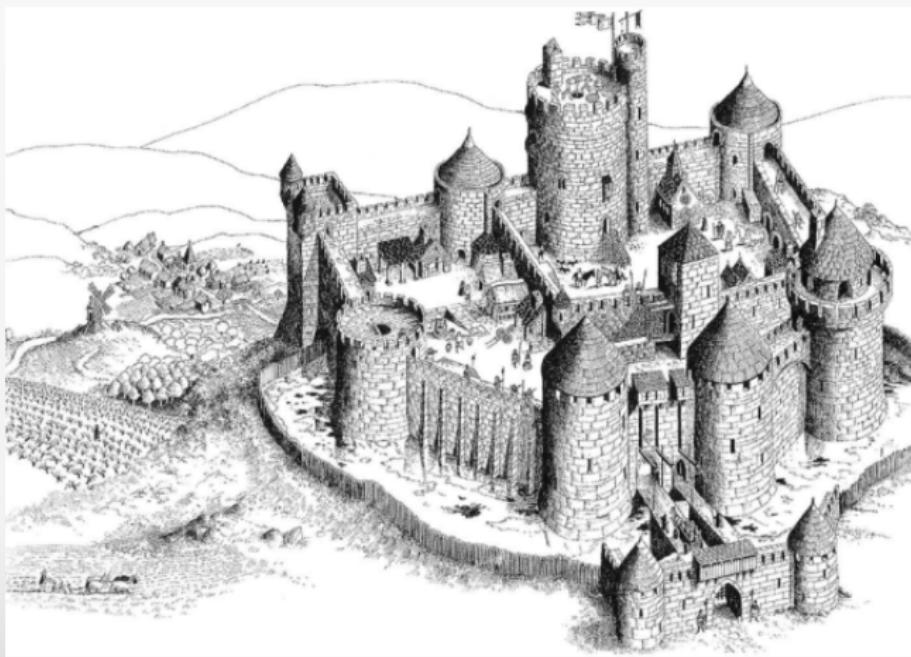
2 Risques, menaces et vulnérabilités

- Le risque
- Les menaces
- Les vulnérabilités



Les vulnérabilités

L'image du château



Les vulnérabilités

Définition

Vulnérabilité (*Wikipedia*)

Une vulnérabilité est une **faiblesse** dans un système d'information permettant à un attaquant de porter atteinte à l'intégrité de ce système, à sa confidentialité et à son intégrité.

Vulnérabilité (*Jack A. Jones – RMI*)

Une vulnérabilité est la **probabilité** qu'une ressource ou qu'une entité ne puisse pas résister aux actions d'un élément menaçant.



Les vulnérabilités

Définition

Vulnérabilité (*Wikipedia*)

Une vulnérabilité est une **faiblesse** dans un système d'information permettant à un attaquant de porter atteinte à l'intégrité de ce système, à sa confidentialité et à son intégrité.

Vulnérabilité (*Jack A. Jones – RMI*)

Une vulnérabilité est la **probabilité** qu'une ressource ou qu'une entité ne puisse pas résister aux actions d'un élément menaçant.



Les vulnérabilités

Définition

Une vulnérabilité est donc la **caractéristique** d'une entité qui constitue une **faiblesse** ou une **faille** au regard de la sécurité des systèmes d'information.



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité d'origine matérielle



Les vulnérabilités

Classification des vulnérabilités

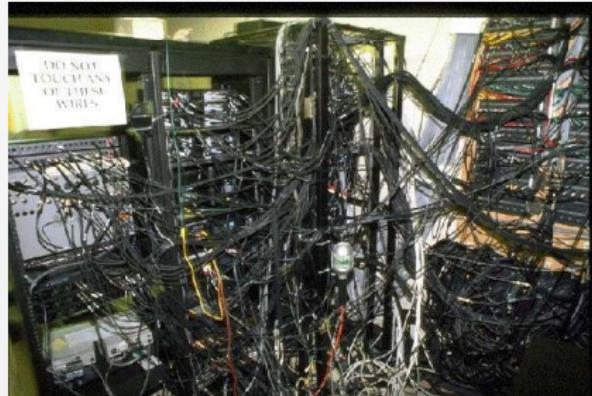
Vulnérabilité d'origine logicielle



Les vulnérabilités

Classification des vulnérabilités

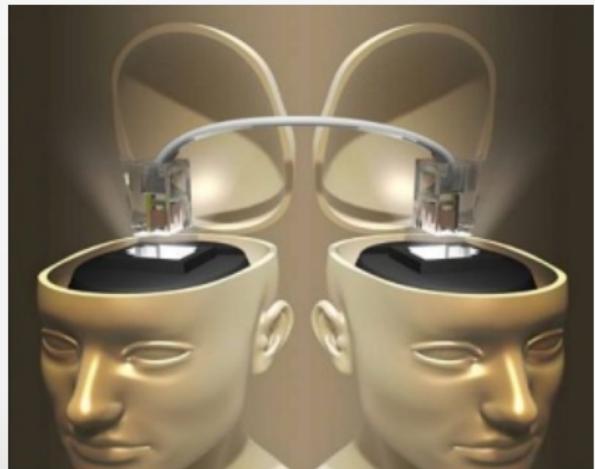
Vulnérabilité liée au réseau



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au personnel



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au personnel



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au personnel

- ▶ Syndrome de l'expert unique
- ▶ Absence de procédure de transfert de connaissances ...



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au personnel

- ▶ Syndrome de l'expert unique
- ▶ Absence de procédure de transfert de connaissances ...



Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au site



Installation en zone inondable

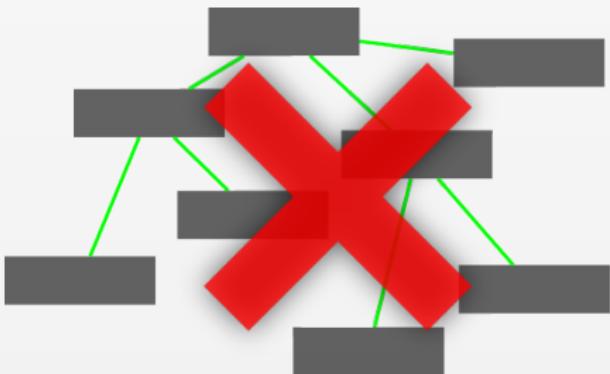


Absence de contrôle d'accès au site ou aux locaux

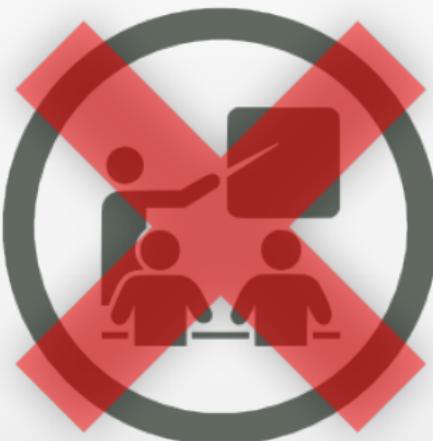
Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité d'origine organisationnelle



Absence d'organisation SSI

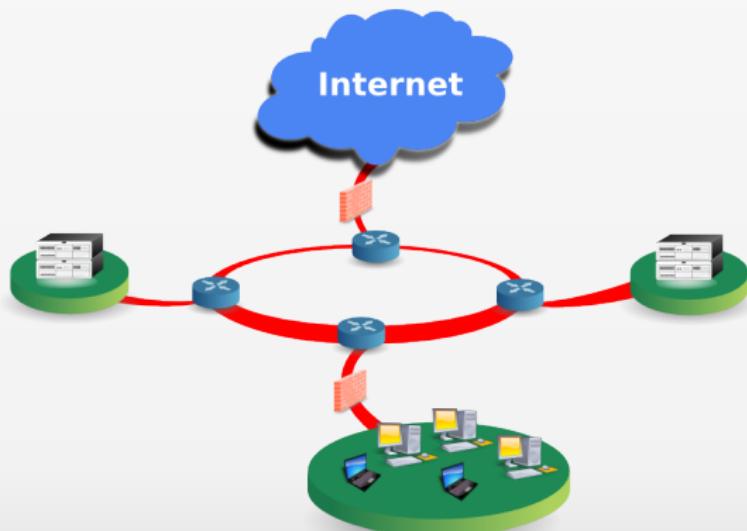


Absence de sensibilisation SSI

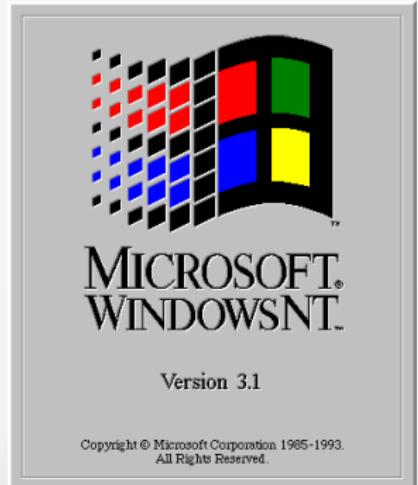
Les vulnérabilités

Classification des vulnérabilités

Vulnérabilité liée au *système*



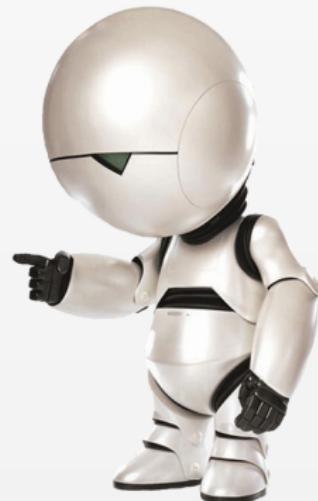
Erreur de configuration



Logiciel obsolète

Contres mesures

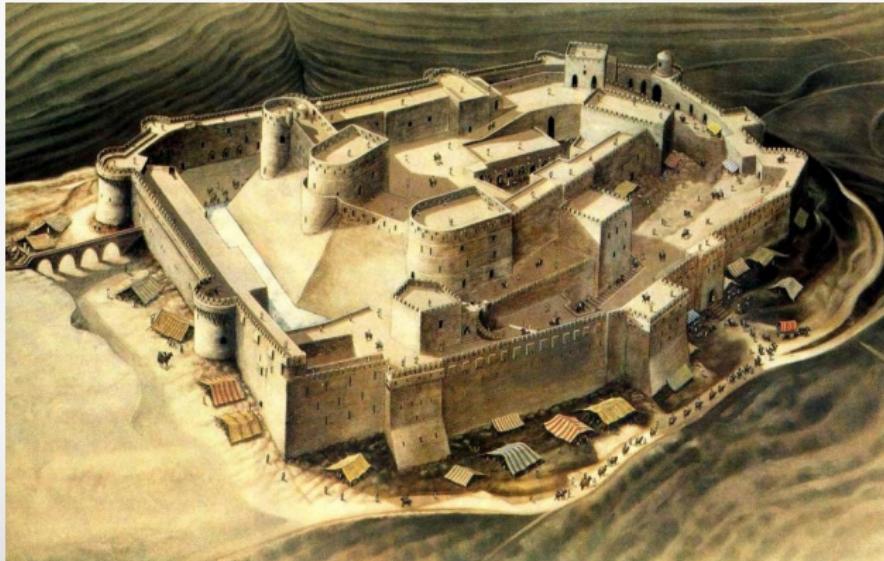
- 1** Introduction
- 2** Risques, menaces et vulnérabilités
- 3** Contres mesures
- 4** Conclusion



Contres mesures

La défense en profondeur

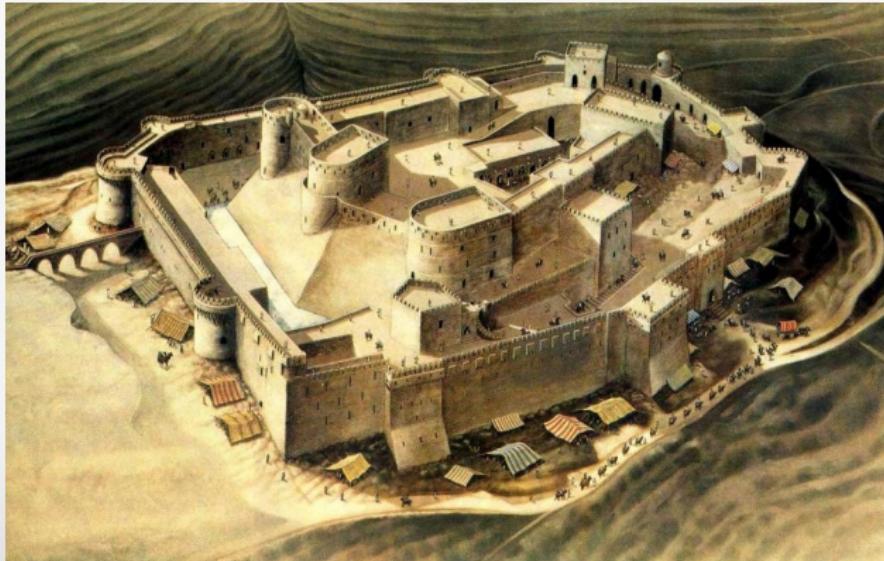
La **défense en profondeur** est une stratégie militaire. Elle cherche à **retarder** l'avance d'un attaquant, tout en l'affaiblissant. Pour atteindre cet objectif, la défense en profondeur utilise **plusieurs lignes de défense indépendantes**.



Contres mesures

La défense en profondeur

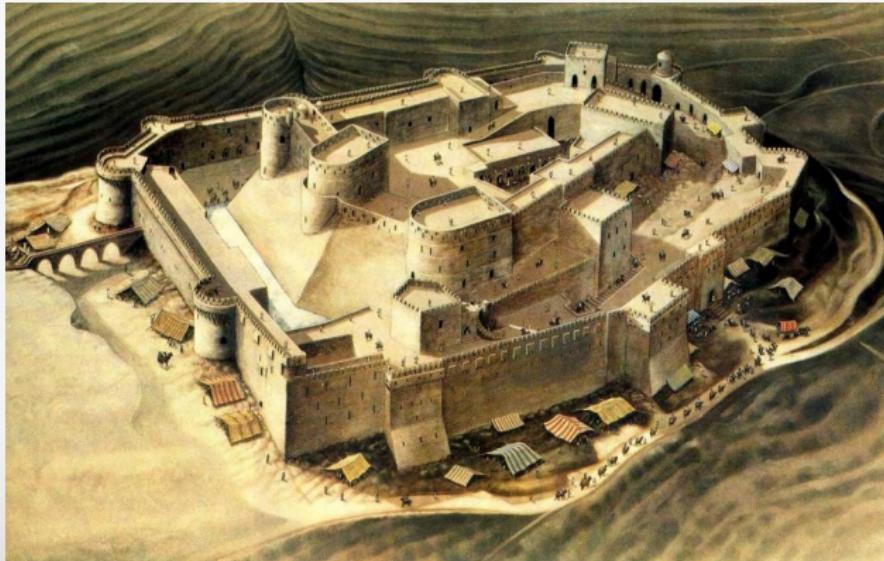
La **défense en profondeur** est une stratégie militaire. Elle cherche à **retarder** l'avance d'un attaquant, tout en l'affaiblissant. Pour atteindre cet objectif, la défense en profondeur utilise **plusieurs lignes de défense indépendantes**.



Contres mesures

La défense en profondeur

La **défense en profondeur** est un stratégie militaire. Elle cherche à **retarder** l'avance d'un attaquant, tout en l'affaiblissant. Pour atteindre cet objectif, la défense en profondeur utilise **plusieurs** lignes de défense indépendantes.

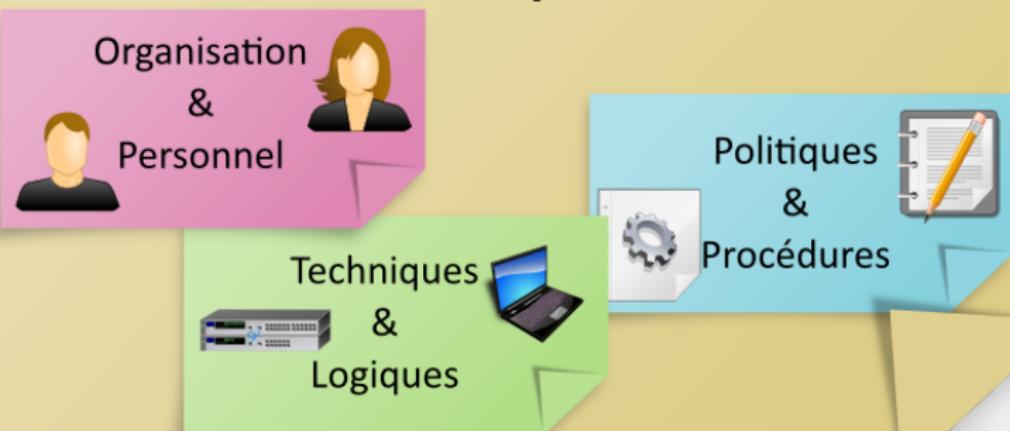


Contres mesures

La défense en profondeur

3 catégories de moyens pour la défense en profondeur

Défense en profondeur



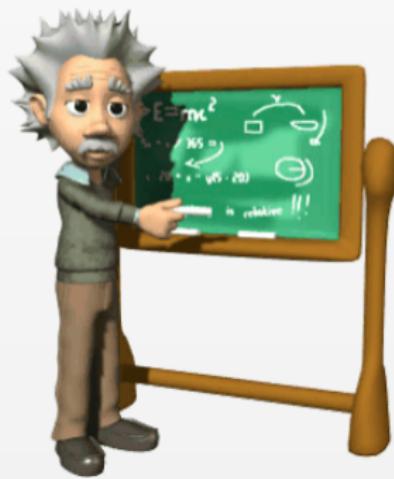
Organisation & Personnel

3 Contres mesures

- Organisation & Personnel
 - Organisation
 - Le personnel
- Techniques & Logiques
 - Les mots de passe
 - La lutte antivirale
 - Les clefs USB
 - La messagerie
 - Classification des données
- Politiques & Procédures
 - La réglementation
 - La politique SSI
 - Code de bon usage

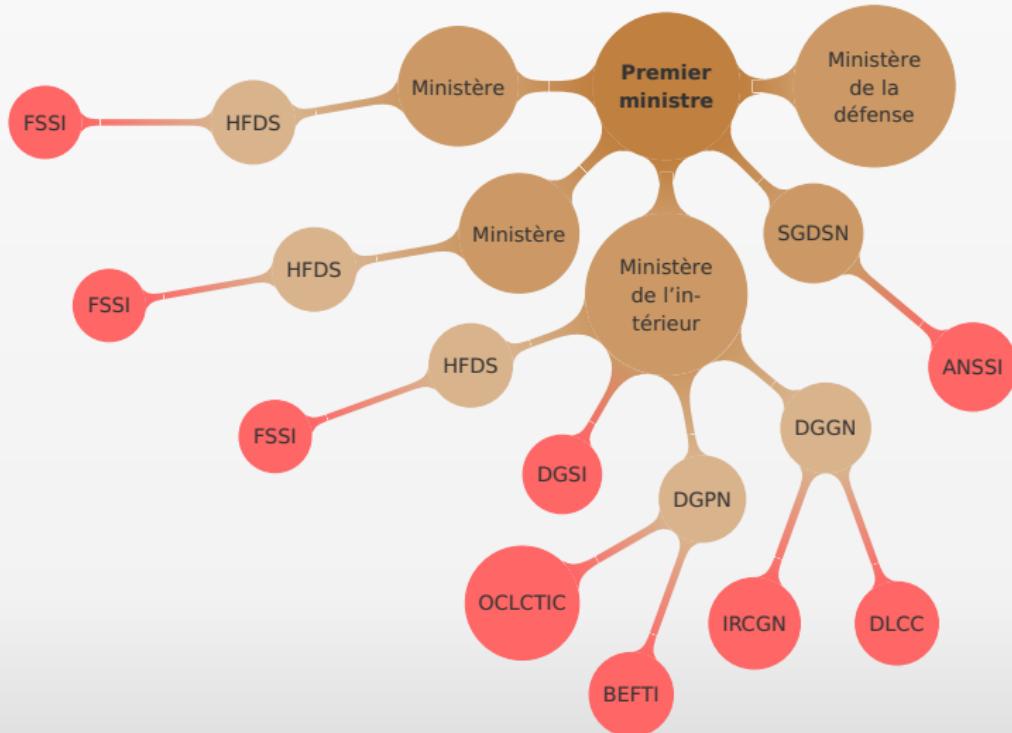


Organisation



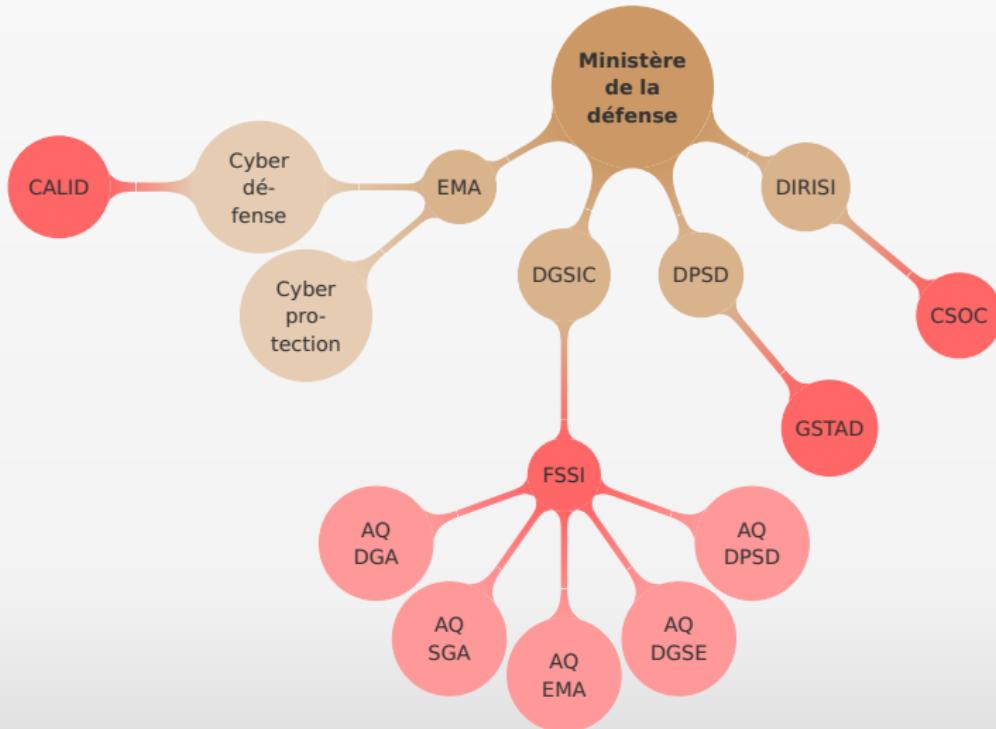
Organisation

La chaîne fonctionnelle SSI



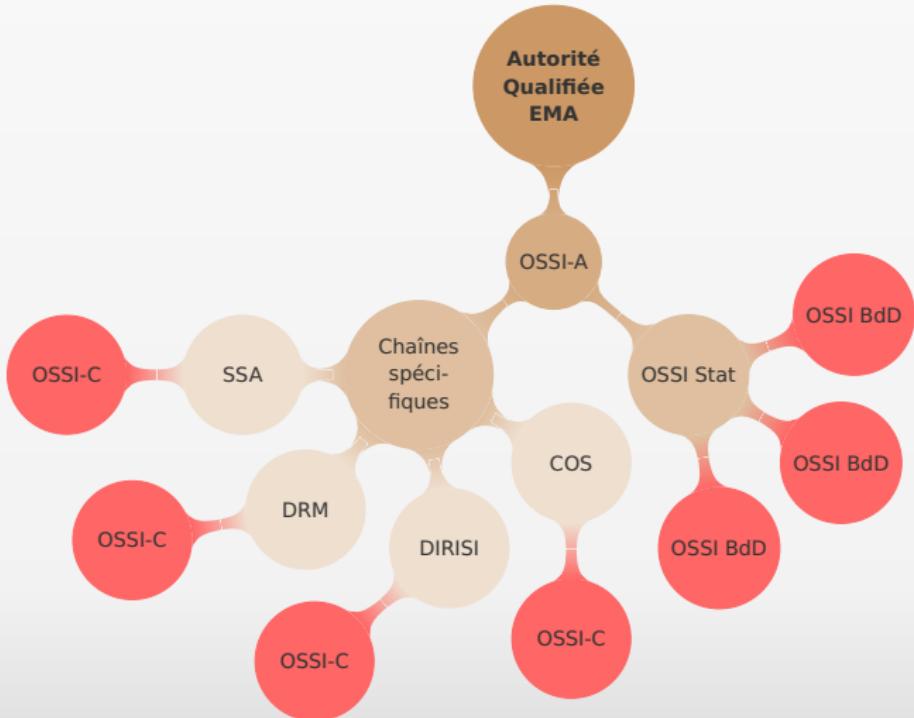
Organisation

La chaîne fonctionnelle SSI



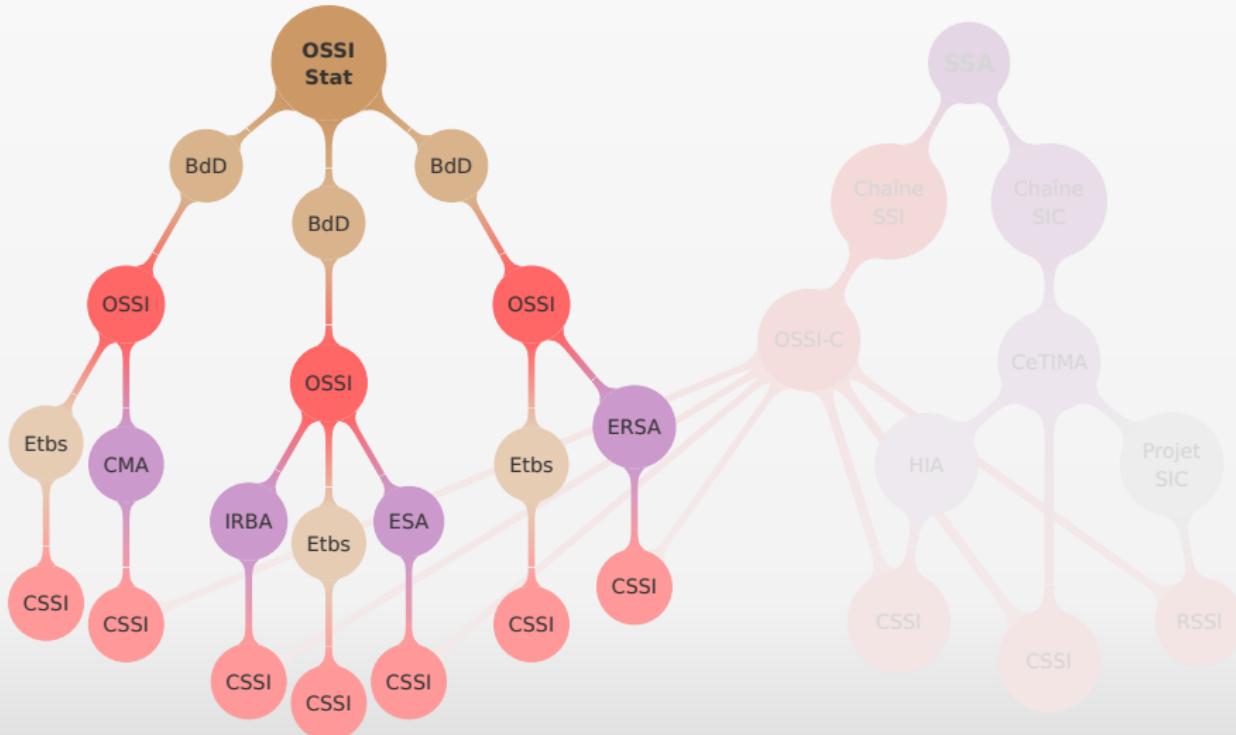
Organisation

La chaîne fonctionnelle SSI



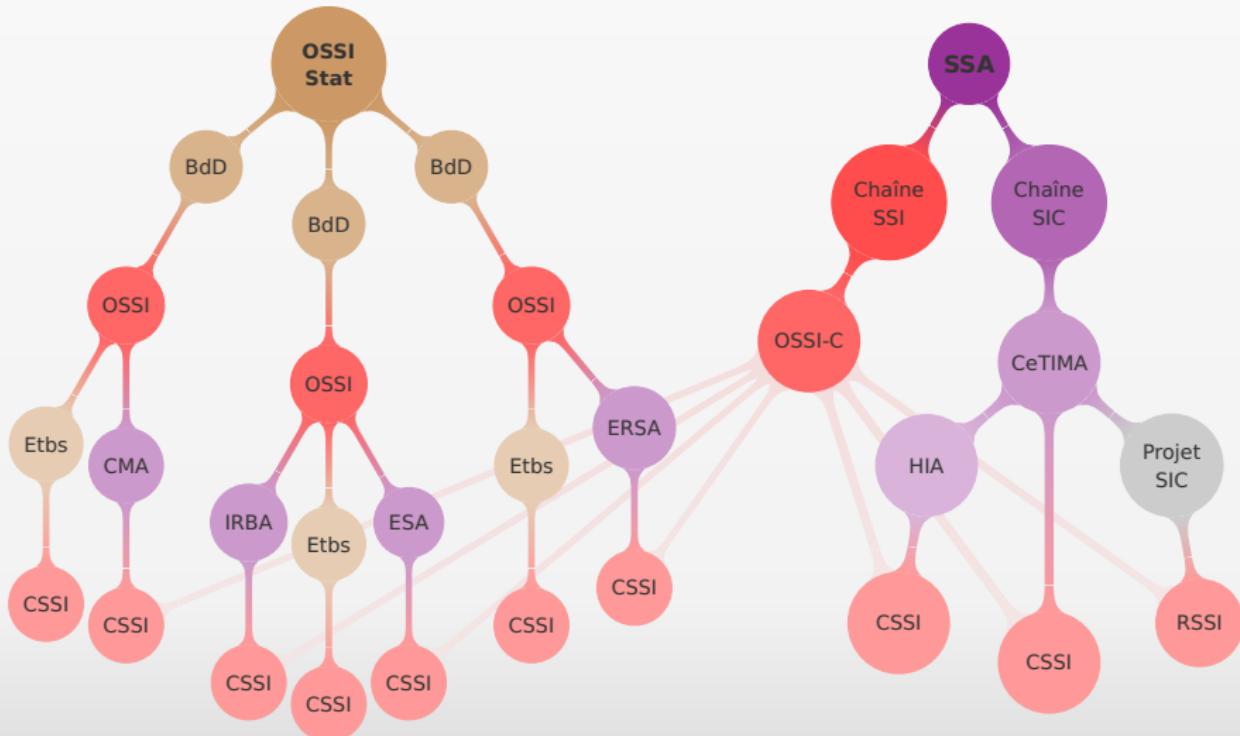
Organisation

La chaîne fonctionnelle SSI



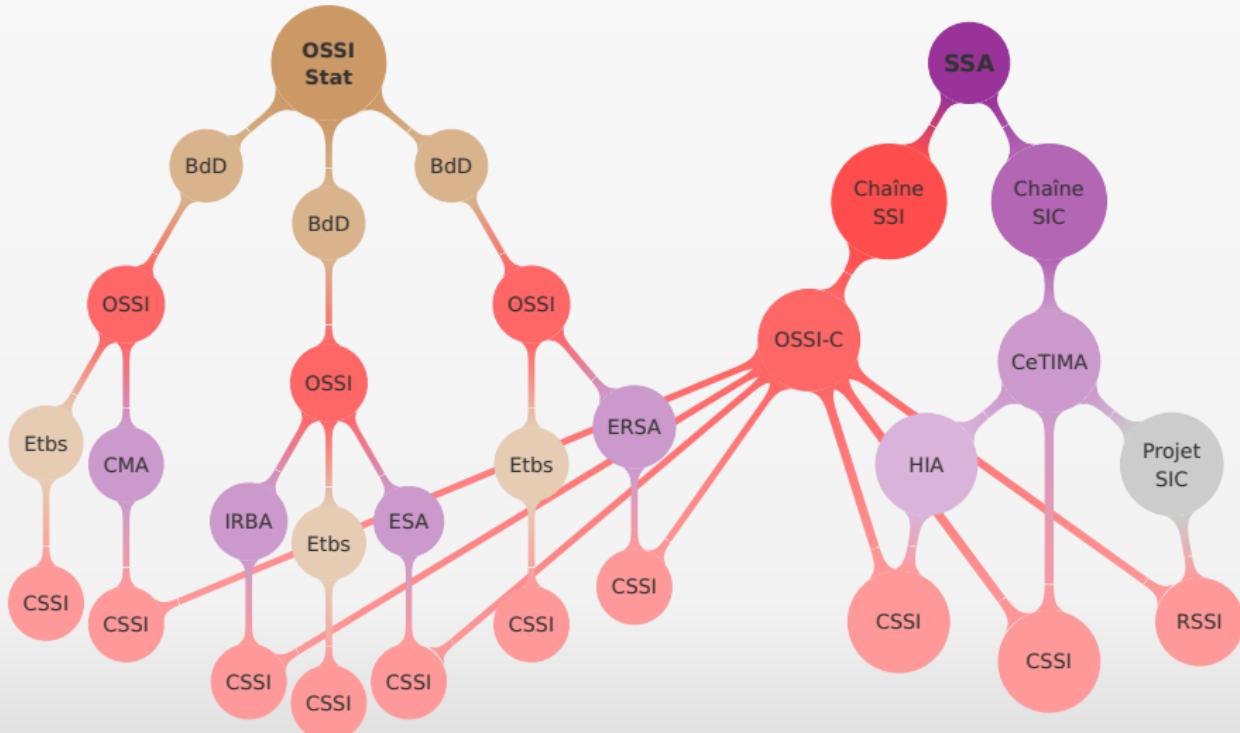
Organisation

La chaîne fonctionnelle SSI

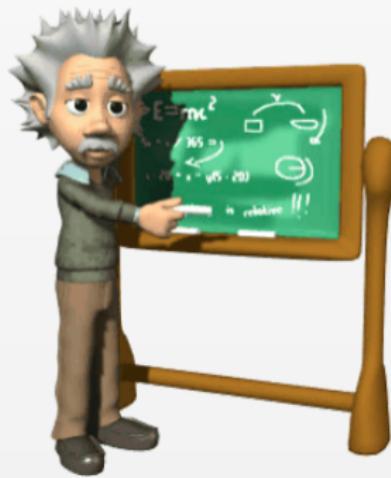


Organisation

La chaîne fonctionnelle SSI



Le personnel



Le personnel

Qui intervient dans la SSI de l'organisme ?

- ① la direction
- ② l'OSSI, le RSSI, le CSSI
- ③ le technicien informatique
- ④ l'utilisateur final



Le personnel

Qui intervient dans la SSI de l'organisme ?

- ① la direction
- ② l'OSSI, le RSSI, le CSSI
- ③ le technicien informatique
- ④ l'utilisateur final



Le personnel

Qui intervient dans la SSI de l'organisme ?

- ① la direction
- ② l'OSSI, le RSSI, le CSSI
- ③ le technicien informatique
- ④ l'utilisateur final



Le personnel

Qui intervient dans la SSI de l'organisme ?

- ① la direction
- ② l'OSSI, le RSSI, le CSSI
- ③ le technicien informatique
- ④ l'utilisateur final

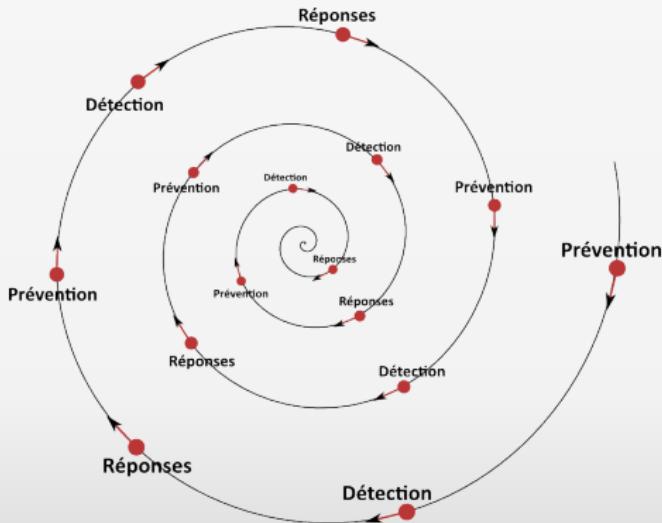


Le personnel

La direction

Le rôle fondamental de la direction

- ▶ donne l'**impulsion** de la démarche SSI à tous les échelons de l'organisme
- ▶ pilote la sécurité des systèmes d'information (tableaux de bords et SMSI)

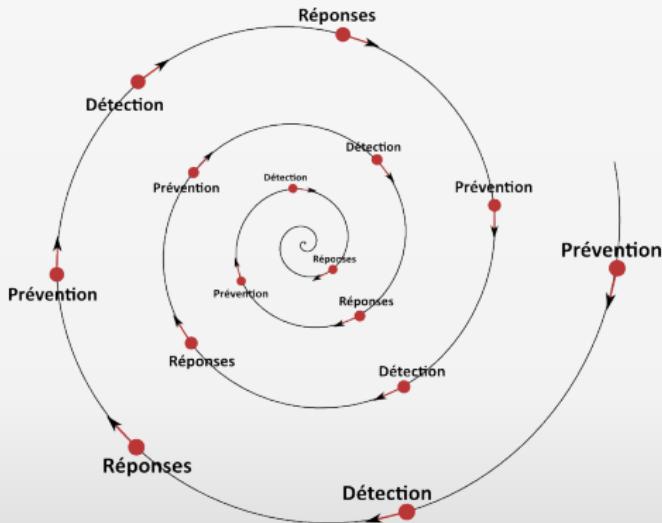


Le personnel

La direction

Le rôle fondamental de la direction

- ▶ donne l'**impulsion** de la démarche SSI à tous les échelons de l'organisme
- ▶ pilote la sécurité des systèmes d'information (tableaux de bords et SMSI)

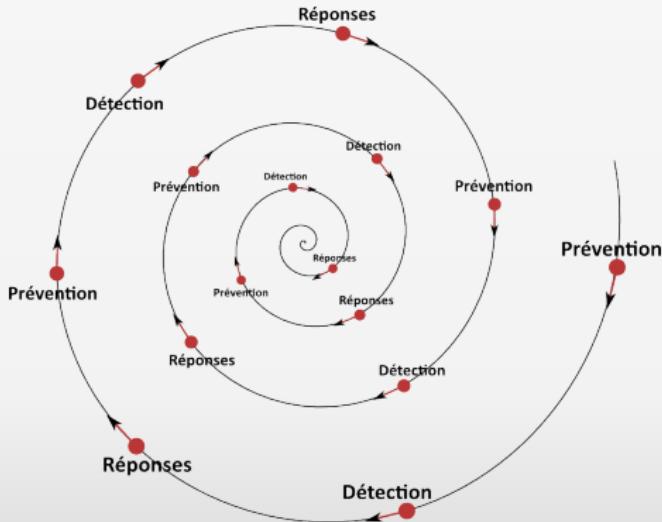


Le personnel

La direction

Le rôle fondamental de la direction

- ▶ donne l'**impulsion** de la démarche SSI à tous les échelons de l'organisme
- ▶ pilote la sécurité des systèmes d'information (tableaux de bords et SMSI)



Le personnel

I'OSSI, le RSSI, le CSSI

► Les fonctions de l'OSSI

- ▶ Responsable de la SSI
- ▶ Conseille la direction
- ▶ Définit et fait valider la PSSI
- ▶ Organise les contrôles internes
- ▶ Informe et sensibilise à la SSI
- ▶ Valide les FEROS et PES
- ▶ Suis les dossiers d'homologation
- ▶ Anime la chaîne SSI

► Les fonctions du RSSI

- ▶ Pilote la SSI pour un projet SI
- ▶ Réalise l'analyse EBIOS
- ▶ Rédige la FEROS
- ▶ Rédige la PES

► Les fonctions du CSSI

- ▶ Correspondant de l'OSSI
- ▶ Fait mettre en œuvre la PSSI
- ▶ Fait remonter les incidents SSI



Le personnel

Le technicien informatique

- ▶ administre les SI conformément à la PSSI
- ▶ signe l'engagement de sécurité spécifique – IM 2004
- ▶ informe le CSSI ou l'OSSI en cas d'incident



Le personnel

Le technicien informatique

- ▶ **administre les SI conformément à la PSSI**
- ▶ signe l'engagement de sécurité spécifique – IM 2004
- ▶ informe le CSSI ou l'OSSI en cas d'incident



Le personnel

Le technicien informatique

- ▶ **administre** les SI conformément à la PSSI
- ▶ signe l'engagement de sécurité spécifique – IM 2004
- ▶ informe le CSSI ou l'OSSI en cas d'incident



Le personnel

Le technicien informatique

- ▶ **administre** les SI conformément à la PSSI
- ▶ signe l'engagement de sécurité spécifique – IM 2004
- ▶ informe le CSSI ou l'OSSI en cas d'incident



Le personnel

L'utilisateur final

- ▶ **utilise** les SI conformément au code de bon usage (IM 2003)
- ▶ **sauvegarde** ses données
- ▶ **utilise un bon mot de passe ET le garde secret**
- ▶ **Informe son CSSI en cas d'incident**



Le personnel

L'utilisateur final

- ▶ **utilise** les SI conformément au code de bon usage (IM 2003)
- ▶ **sauvegarde** ses données
- ▶ utilise un **bon** mot de passe **ET** le garde **secret**
- ▶ **informe** son CSSI en cas d'incident



Le personnel

L'utilisateur final

- ▶ **utilise** les SI conformément au code de bon usage (IM 2003)
- ▶ **sauvegarde** ses données
- ▶ utilise un **bon** mot de passe **ET** le garde **secret**
- ▶ **informe** son CSSI en cas d'incident



Le personnel

L'utilisateur final

- ▶ **utilise** les SI conformément au code de bon usage (IM 2003)
- ▶ **sauvegarde** ses données
- ▶ utilise un **bon** mot de passe **ET** le garde **secret**
- ▶ **informe** son CSSI en cas d'incident



Le personnel

L'utilisateur final

- ▶ **utilise** les SI conformément au code de bon usage (IM 2003)
- ▶ **sauvegarde** ses données
- ▶ utilise un **bon** mot de passe **ET** le garde **secret**
- ▶ **informe** son CSSI en cas d'incident



Le personnel

L'utilisateur final

Le souci du compte-rendu



Swigert Okay, Houston, we've had a problem here.

Houston This is Houston. Say again please.

Lovell Houston, we've had a problem. We've had a main B bus undervolt.



Il n'y a pas de petit incident en SSI

Le personnel

L'utilisateur final

Le souci du compte-rendu



Swigert Okay, Houston, we've had a problem here.

Houston This is Houston. Say again please.

Lovell Houston, we've had a problem. We've had a main B bus undervolt.



Il n'y a pas de petit incident en SSI

Le personnel

L'utilisateur final

Le souci du compte-rendu



Swigert Okay, Houston, we've had a problem here.

Houston This is Houston. Say again please.

Lovell Houston, we've had a problem. We've had a main B bus undervolt.



Il n'y a pas de petit incident en SSI

Le personnel

L'utilisateur final

Le souci du compte-rendu



Swigert Okay, Houston, we've had a problem here.

Houston This is Houston. Say again please.

Lovell Houston, we've had a problem. We've had a main B bus undervolt.



Il n'y a pas de petit incident en SSI

Techniques & Logiques

3 Contres mesures

- Organisation & Personnel
 - Organisation
 - Le personnel
- Techniques & Logiques
 - Les mots de passe
 - La lutte antivirale
 - Les clefs USB
 - La messagerie
 - Classification des données
- Politiques & Procédures
 - La réglementation
 - La politique SSI
 - Code de bon usage



Les moyens techniques et logiques

Les moyens mis en œuvre par l'utilisateur

« L'épaisseur d'un rempart compte moins que la volonté de le défendre »

Thucydude – historien grec du V^{ème} siècle avant JC



La sécurité, c'est l'affaire de tous !

Les moyens techniques et logiques

Les moyens mis en œuvre par l'utilisateur

« L'épaisseur d'un rempart compte moins que la volonté de le défendre »

Thucydude – historien grec du V^{ème} siècle avant JC

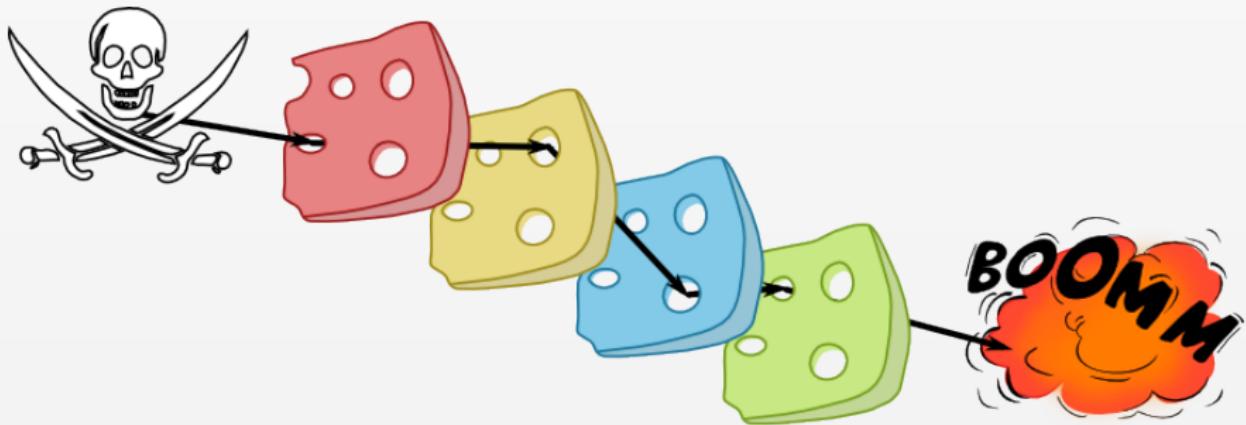


La sécurité, c'est l'affaire de tous !

Les moyens techniques et logiques

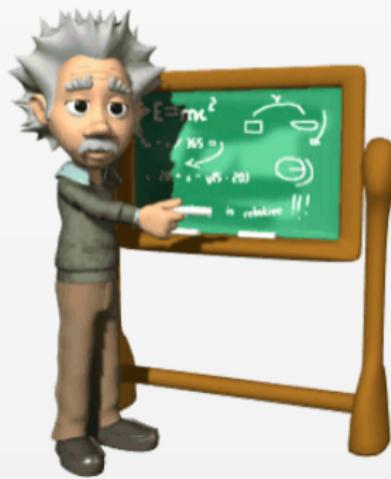
Les moyens mis en œuvre par l'utilisateur

La théorie du gruyère suisse



Une série de **petites négligences** dans les différentes aires de protection du SI peut créer une **chaîne d'incidents** amenant à la concrétisation de l'attaque.

Les mots de passe



Les mots de passe

 **TODAY I FOUND OUT**
FEED YOUR BRAIN

HOME SURPRISE STORE OUR BOOKI ARTICLES PODCAST QUICK FACTS

FOR NEARLY TWO DECADES THE NUCLEAR LAUNCH CODE AT ALL MINUTEMAN SILOS IN THE UNITED STATES WAS 00000000

KARL SMALLWOOD NOVEMBER 29, 2013 102

Today I found out that during the height of the Cold War, the US military put such an emphasis on a rapid response to an attack on American soil, that to minimize any foreseeable delay in launching a nuclear missile, for nearly two decades they intentionally set the launch codes at every silo in the US to 8 zeroes.

We guess the first thing we need to address is how this even came to be in the first place. Well, in 1962 JFK signed the *National Security Action Memorandum 160*, which was supposed to ensure that every nuclear weapon the US had be fitted with a *Permissive Action Link (PAL)*, basically a small device that ensured that the missile could only be launched with the right code and with the right authority.



Des réseaux informatique,
des services & applications :

nécessité d'**authentifier** et de
tracer les entités connectées

Les mots de passe

L'authentification

Identification

L'identification a pour fonction de **définir** l'identité d'une entité.

Authentification

L'authentification a pour fonction de **vérifier** de manière certaine l'identité d'une entité.

Autorisation

Ensemble des **droits accordés** à une entité après identification et authentification.

Accounting

Ensemble des **informations récoltées** pendant toute la durée de la session d'une entité identifiée et authentifiée.

Les mots de passe

L'authentification

Identification

L'identification a pour fonction de **définir** l'identité d'une entité.

Authentification

L'authentification a pour fonction de **vérifier** de manière certaine l'identité d'une entité.

Autorisation

Ensemble des **droits accordés** à une entité après identification et authentification.

Accounting

Ensemble des **informations récoltées** pendant toute la durée de la session d'une entité identifiée et authentifiée.

Les mots de passe

L'authentification

Identification

L'identification a pour fonction de **définir** l'identité d'une entité.

Authentification

L'authentification a pour fonction de **vérifier** de manière certaine l'identité d'une entité.

Autorisation

Ensemble des **droits accordés** à une entité après identification et authentification.

Accounting

Ensemble des **informations récoltées** pendant toute la durée de la session d'une entité identifiée et authentifiée.

Les mots de passe

L'authentification

Identification

L'identification a pour fonction de **définir** l'identité d'une entité.

Authentification

L'authentification a pour fonction de **vérifier** de manière certaine l'identité d'une entité.

Autorisation

Ensemble des **droits accordés** à une entité après identification et authentification.

Accounting

Ensemble des **informations récoltées** pendant toute la durée de la session d'une entité identifiée et authentifiée.

Les mots de passe

L'authentification – Différentes techniques



► Quelque chose que je connais

(exemple : mot de passe)

► Quelque chose que j'ai

(exemple : carte à puce)

► Quelque chose que je suis

(exemple : empreinte digitale, empreinte rétinienne)

► Quelque chose que je fais

(exemple : signature)

► L'endroit où je me trouve

(exemple : station de travail dédiée)

Recommandation

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte), exemple : carte de crédit et code PIN.

Les mots de passe

L'authentification – Différentes techniques



- ▶ Quelque chose que je connais
(exemple : mot de passe)
- ▶ Quelque chose que j'ai
(exemple : carte à puce)
- ▶ Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- ▶ Quelque chose que je fais
(exemple : signature)
- ▶ L'endroit où je me trouve
(exemple : station de travail dédiée)

Recommendation

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte), exemple : carte de crédit et code PIN.

Les mots de passe

L'authentification – Différentes techniques



- ▶ Quelque chose que je connais
(exemple : mot de passe)
- ▶ Quelque chose que j'ai
(exemple : carte à puce)
- ▶ Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- ▶ Quelque chose que je fais
(exemple : signature)
- ▶ L'endroit où je me trouve
(exemple : station de travail dédiée)

Recommandation

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte). exemple : carte de crédit et code PIN

Les mots de passe

L'authentification – Différentes techniques



- ▶ Quelque chose que je connais
(exemple : mot de passe)
- ▶ Quelque chose que j'ai
(exemple : carte à puce)
- ▶ Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- ▶ Quelque chose que je fais
(exemple : signature)
- ▶ L'endroit où je me trouve
(exemple : station de travail dédiée)

Recommandation

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte). exemple : carte de crédit et code PIN

Les mots de passe

L'authentification – Différentes techniques



- ▶ Quelque chose que je connais
(exemple : mot de passe)
- ▶ Quelque chose que j'ai
(exemple : carte à puce)
- ▶ Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- ▶ Quelque chose que je fais
(exemple : signature)
- ▶ L'endroit où je me trouve
(exemple : station de travail dédiée)

Recommandation

Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte). exemple : carte de crédit et code PIN

Les mots de passe

L'authentification – Différentes techniques



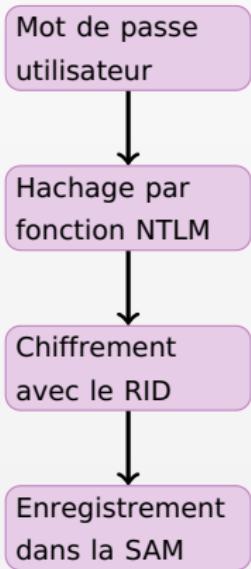
- ▶ Quelque chose que je connais
(exemple : mot de passe)
- ▶ Quelque chose que j'ai
(exemple : carte à puce)
- ▶ Quelque chose que je suis
(exemple : empreinte digitale, empreinte rétinienne)
- ▶ Quelque chose que je fais
(exemple : signature)
- ▶ L'endroit où je me trouve
(exemple : station de travail dédiée)

Recommandation

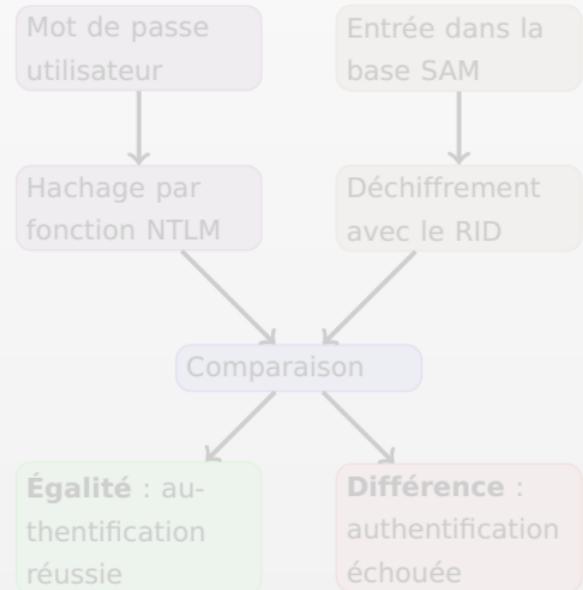
Pour une plus grande sécurité, il est souhaitable de combiner deux ou plusieurs techniques différentes (authentification forte). **exemple : carte de crédit et code PIN**

Les mots de passe

L'authentification – Processus d'authentification local sous Windows



Processus de stockage

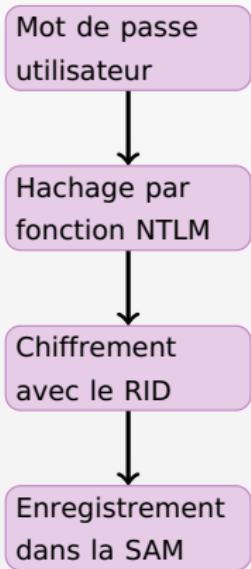


Processus d'authentification

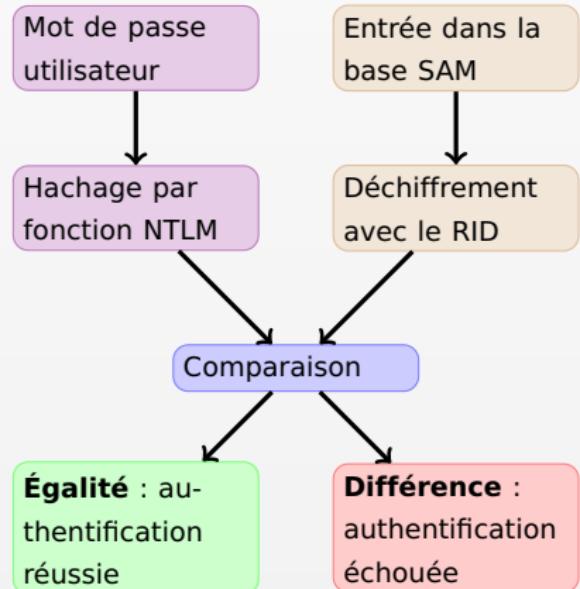
Source : <http://www.hsc.fr/>

Les mots de passe

L'authentification – Processus d'authentification local sous Windows



Processus de stockage



Processus d'authentification

Source : <http://www.hsc.fr/>

Les mots de passe

Principe de base

La sécurité d'un système d'information est **aussi bonne** que celle des mots de passe d'authentification.



Les mots de passe

Trouver un mot de passe

Deviner le mot de passe

Par des techniques de **social engineering** (*canulars téléphoniques, fouille des poubelles, recherche sur Internet...*).

Se faire passer pour le système

Par des techniques de **spoofing** *un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate.*

Espionner le système

Par des techniques de **keylogging** ou de **sniffing** des protocoles réseaux.

Attaquer le fichier de mot de passe

Par des techniques d'attaques par dictionnaire ou par **force brute**.

Les mots de passe

Trouver un mot de passe

Deviner le mot de passe

Par des techniques de **social engineering** (*canulars téléphoniques, fouille des poubelles, recherche sur Internet...*).

Se faire passer pour le système

Par des techniques de **spoofing** *un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate.*

Espionner le système

Par des techniques de **keylogging** ou de **sniffing** des protocoles réseaux.

Attaquer le fichier de mot de passe

Par des techniques d'attaques par **dictionnaire** ou par **force brute**.

Les mots de passe

Trouver un mot de passe

Deviner le mot de passe

Par des techniques de **social engineering** (*canulars téléphoniques, fouille des poubelles, recherche sur Internet...*).

Se faire passer pour le système

Par des techniques de **spoofing** *un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate.*

Espionner le système

Par des techniques de **keylogging** ou de **sniffing** des protocoles réseaux.

Attaquer le fichier de mot de passe

Par des techniques d'attaques par **dictionnaire** ou par **force brute**.

Les mots de passe

Trouver un mot de passe

Deviner le mot de passe

Par des techniques de **social engineering** (*canulars téléphoniques, fouille des poubelles, recherche sur Internet...*).

Se faire passer pour le système

Par des techniques de **spoofing** *un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate.*

Espionner le système

Par des techniques de **keylogging** ou de **sniffing** des protocoles réseaux.

Attaquer le fichier de mot de passe

Par des techniques d'attaques par **dictionnaire** ou par **force brute**.

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

► TOTO ==> 04c1d7cd203ef496f200ee5a096b5764

► TOTO ==> 3ccca12813e4f82de305aa73b91584509

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ==> 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ==> 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ==> 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ==> f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ==>
caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ➔ 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ➔ 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ➔ 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ➔ f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ➔ caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ➔ 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ➔ 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ➔ 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ➔ f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ➔
caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ➔ 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ➔ 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ➔ 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ➔ f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ➔
caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ⇒ 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ⇒ 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ⇒ 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ⇒ f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ⇒
caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Comment est stocké un mot de passe ?

C'est l'empreinte, ou **hash**, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une **fonction mathématique** qui, à partir d'un texte d'origine, calcule une **empreinte unique**, de taille fixée et de manière irréversible.

- ▶ **TOTO** ⇒ 04c1d7cd203ef496f200ee5a096b5764
- ▶ **ToTo** ⇒ 3cca12013a4f82de305ba73b01a84509
- ▶ **Toto** ⇒ 998db284485ec6c227f8dc34086128e1
- ▶ **toto** ⇒ f71dbe52628a3f83a77ab494817525c6
- ▶ **Le ciel est rouge demain il fera beau.** ⇒
caf7a1f03adc02afe3ef1dd51bd3e8b1

Les mots de passe

Trouver un mot de passe

Attaque par dictionnaire

- ① pour chaque mot d'un dictionnaire
- ② calcul du hash
- ③ comparaison avec celui du système



151349	michaella
151350	michaelmas
151351	michaelmastide
151352	michail
151353	michal
151354	michale
151355	miche
151356	micheal
151357	micheil
151358	michel
151359	michelangelesque
151360	michelangelism
151361	michelangelo
151362	michele
151363	michelia
151364	michelin
151365	michelina
151366	micheline
151367	michell
151368	michelle
151369	michelson
151370	micher

Les mots de passe

Trouver un mot de passe

Attaque par dictionnaire

- ➊ pour chaque mot d'un dictionnaire
- ➋ calcul du hash
- ➌ comparaison avec celui du système



151349	michaella
151350	michaelmas
151351	michaelmastide
151352	michail
151353	michal
151354	michale
151355	miche
151356	micheal
151357	micheil
151358	michel
151359	michelangelesque
151360	michelangelism
151361	michelangelo
151362	michele
151363	michelia
151364	michelin
151365	michelina
151366	micheline
151367	michell
151368	michelle
151369	michelson
151370	micher

Les mots de passe

Trouver un mot de passe

Attaque par dictionnaire

- ① pour chaque mot d'un dictionnaire
- ② calcul du hash
- ③ comparaison avec celui du système



151349	michaella
151350	michaelmas
151351	michaelmastide
151352	michail
151353	michal
151354	michale
151355	miche
151356	micheal
151357	micheil
151358	michel
151359	michelangelesque
151360	michelangelism
151361	michelangelo
151362	michele
151363	michelia
151364	michelin
151365	michelina
151366	micheline
151367	michell
151368	michelle
151369	michelson
151370	micher

Les mots de passe

Trouver un mot de passe

Attaque par dictionnaire

- ❶ pour chaque mot d'un dictionnaire
- ❷ calcul du hash
- ❸ comparaison avec celui du système



151349	michaella
151350	michaelmas
151351	michaelmastide
151352	michail
151353	michal
151354	michale
151355	miche
151356	micheal
151357	micheil
151358	michel
151359	michelangelesque
151360	michelangelism
151361	michelangelo
151362	michele
151363	michelia
151364	michelin
151365	michelina
151366	micheline
151367	michell
151368	michelle
151369	michelson
151370	micher

Les mots de passe

Trouver un mot de passe

Attaque par force brute

- parcours exhaustif de l'espace des mots de passe
- plus le mot de passe est long plus il est difficile à trouver
- plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Les mots de passe

Trouver un mot de passe

Attaque par force brute

- ▶ parcours exhaustif de l'espace des mots de passe
- ▶ plus le mot de passe est long plus il est difficile à trouver
- ▶ plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Les mots de passe

Trouver un mot de passe

Attaque par force brute

- ▶ parcours exhaustif de l'espace des mots de passe
- ▶ plus le mot de passe est long plus il est difficile à trouver
- ▶ plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Les mots de passe

Trouver un mot de passe

Attaque par force brute

- ▶ parcours exhaustif de l'espace des mots de passe
- ▶ plus le mot de passe est long plus il est difficile à trouver
- ▶ plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

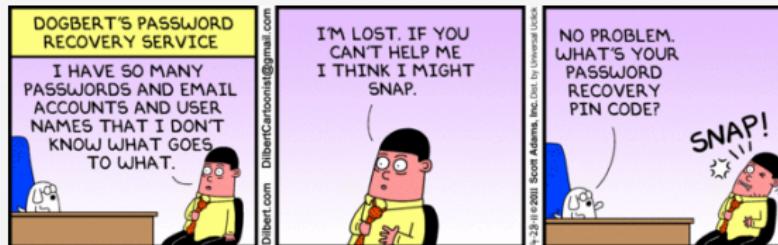
	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : **[A-Z], [a-z], [0-9], [@&#\$%+=€]**
- ▶ est **changé régulièrement**
- ▶ est dédié à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse \Rightarrow Tvlçàlqlfesc

J'crois enfaits, un chat, un oiseau et trois poisson nommés diri, mif et loulou ! \Rightarrow G3elc1o&3phrf&1!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé régulièrement**
- ▶ est dédié à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse ==> Tvlçàlqlfesc

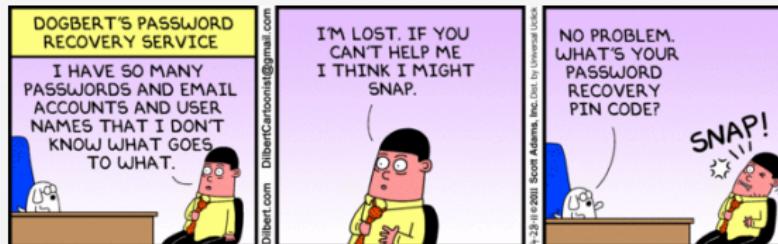
J'crois enfaits, un chat, un oiseau et trois poisson nommés diri, mif et loulou ! ==> G3elc1o&3phrf&1!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé** régulièrement
- ▶ est dédié à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse → Tvlçàlqlfesc

J'ai trois enfants, un chat, un oiseau et trois poissons nommés diri, mif et loulou ! → G3elc1o&3phrf&1!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé** régulièrement
- ▶ est **dédié** à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse \Rightarrow Tvlclqlfesc

J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou ! \Rightarrow G3e1c1o&3pnrf&l!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé** régulièrement
- ▶ est **dédié** à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse \Rightarrow Tvlclqlfesc

J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou ! \Rightarrow G3e1c1o&3pnrf&l!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé** régulièrement
- ▶ est **dédié** à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse \Rightarrow Tvlçàlqlfesc

J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou ! \Rightarrow G3e1c1o&3pnrf&l!

Les mots de passe

Fabriquer un bon mot de passe

Un bon mot de passe :

- ▶ est **secret**
- ▶ contient plus de **9 caractères**
- ▶ contient des caractères parmi : [A ··· Z], [a ··· z], [0 ··· 9], [@&\$#§+*=€]
- ▶ est **changé** régulièrement
- ▶ est **dédié** à une application



Exemples :

Tant va la cruche à l'eau qu'à la fin elle se casse \Rightarrow Tvlclqlfesc

J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou ! \Rightarrow G3e1c1o&3pnrf&l!

Les mots de passe

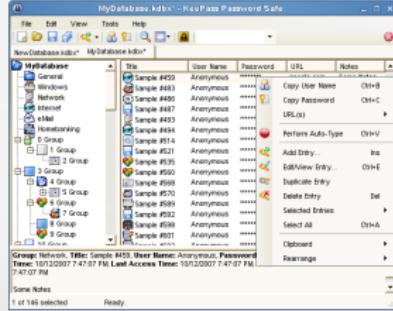
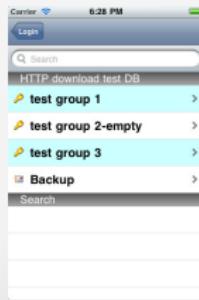
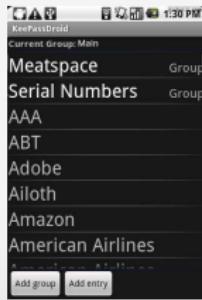
Fabriquer un bon mot de passe

Problème

Un mot de passe par application ou service ⇒ beaucoup de mots de passe !

Solution

Le gestionnaire de mot de passe



Les mots de passe

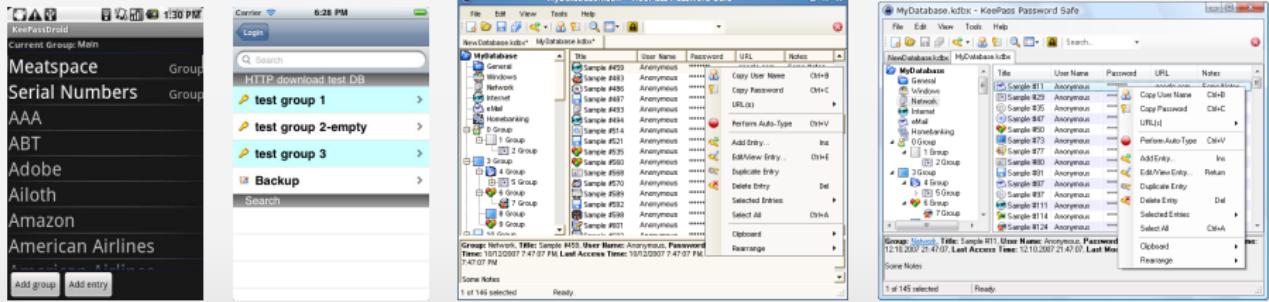
Fabriquer un bon mot de passe

Problème

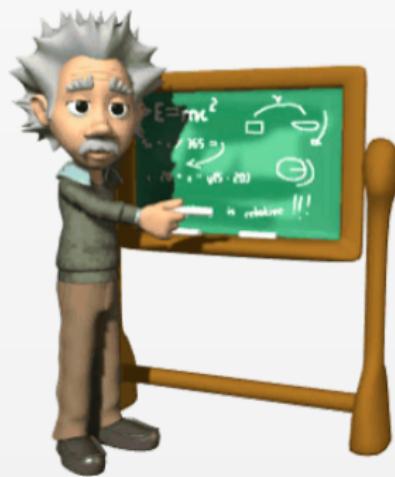
Un mot de passe par application ou service ⇒ beaucoup de mots de passe !

Solution

Le gestionnaire de mot de passe



La lutte antivirale



La lutte antivirale

Malware : évolution de la menace Source : <http://www.symantec.com/business/theme.jsp?themeid=threatreport>

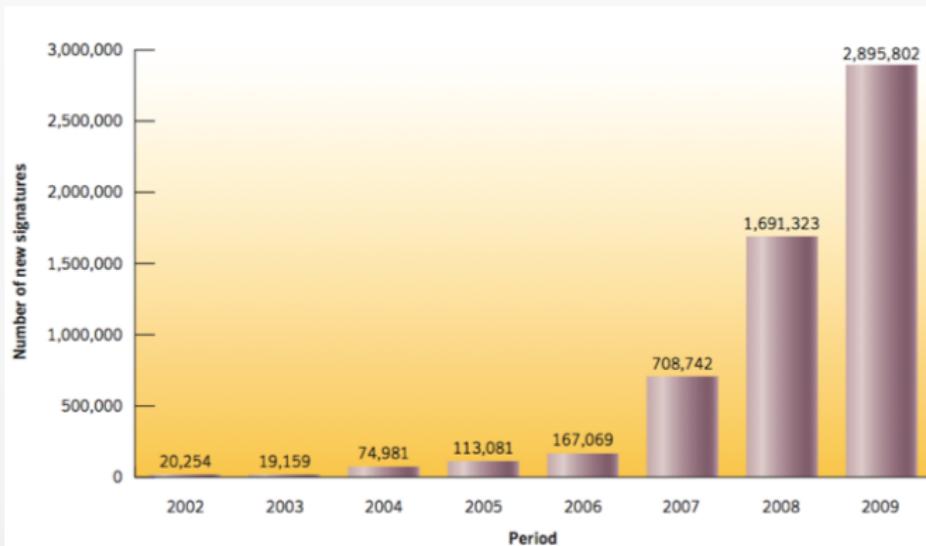


Figure 10. New malicious code signatures

Source: Symantec.

La lutte antivirale



F-Secure – 2007

« Il y a eu plus de malwares produits en 2007 que de malwares produits durant ces 20 dernières années. »

Symantec – 2008

« Le taux de publication de codes malveillants et autres programmes indésirables est supérieur à celui des logiciels légitimes. »

La lutte antivirale



F-Secure – 2007

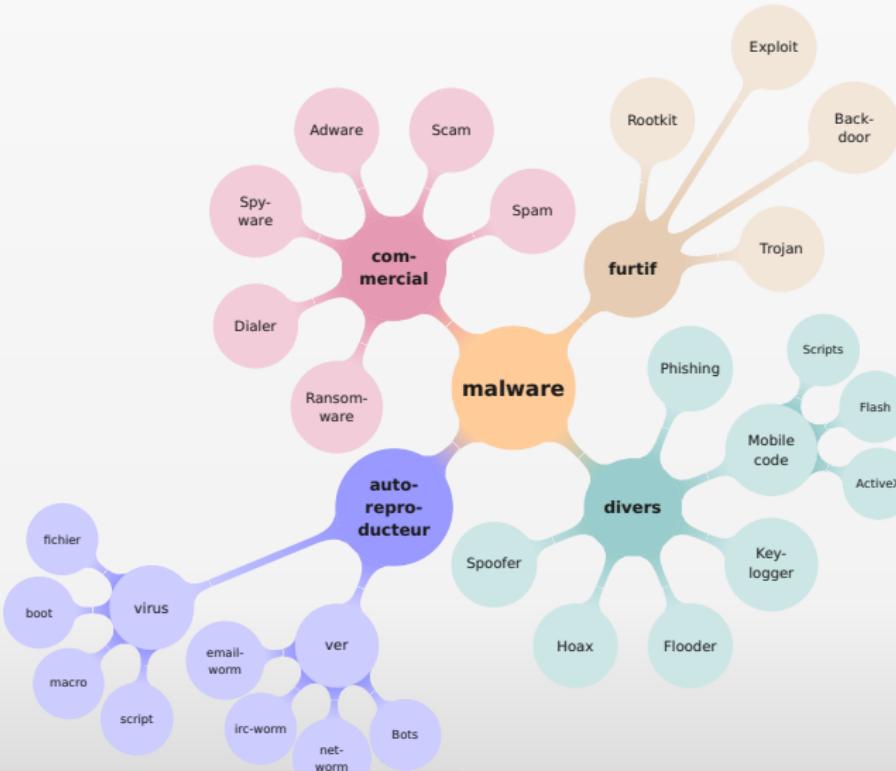
« Il y a eu plus de malwares produits en 2007 que de malwares produits durant ces 20 dernières années. »

Symantec – 2008

« Le taux de publication de codes malveillants et autres programmes indésirables est supérieur à celui des logiciels légitimes. »

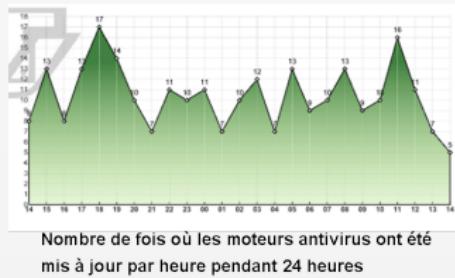
La lutte antivirale

Mwares : classification



La lutte antivirale

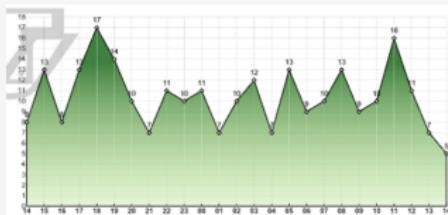
Quelle confiance dans les moteurs antivirus ?



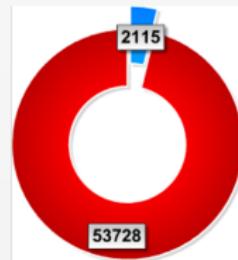
Source : www.virustotal.com

La lutte antivirale

Quelle confiance dans les moteurs antivirus ?



Nombre de fois où les moteurs antivirus ont été mis à jour par heure pendant 24 heures



Erreurs de détection sur 24h

- fichiers infectés non détectés par au moins un antivirus
- fichiers infectés détectés par tous les antivirus

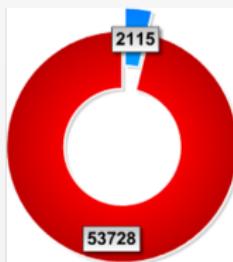
Source : www.virustotal.com

La lutte antivirale

Quelle confiance dans les moteurs antivirus ?

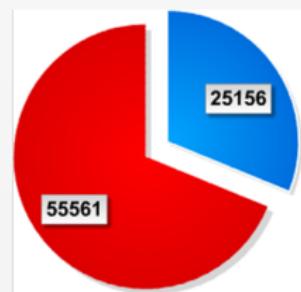


Nombre de fois où les moteurs antivirus ont été mis à jour par heure pendant 24 heures



Erreurs de détection sur 24h

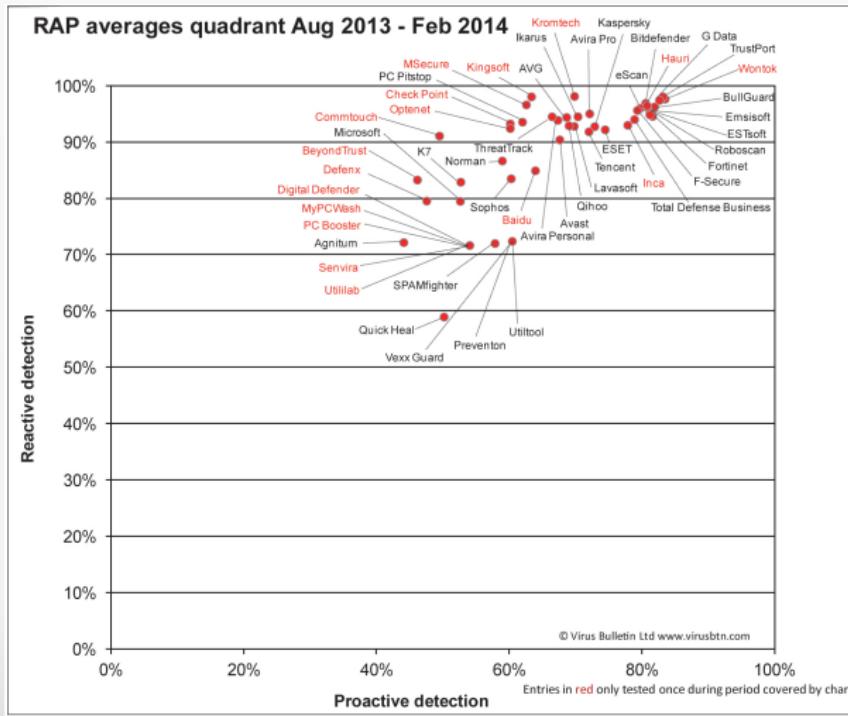
- fichiers infectés non détectés par au moins un antivirus
- fichiers infectés détectés par tous les antivirus



Nombres de fichiers reçus sur 24h

Source : www.virustotal.com

Le meilleur antimalware ?



Source : <http://www.virusbtn.com/vb100/rap-index.xml>

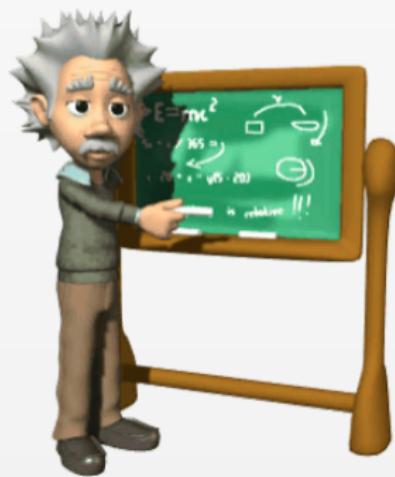
Le meilleur antimalware !!



L'utilisateur, ...



Les clefs USB



Les clefs USB

Le danger des clefs USB

01netPro. Rechercher 01net. web a

Actualités 01netPro Jeux vidéo Produits Astuces Vidéos Télécharger.com

Actualités | Emploi | Start-up | Evénements 01 | Avis d'expert | Vidéos | Indicateurs |

01net Pro / Avis d'expert

Le dilemme de la clé USB

Le Pentagone interdit l'utilisation des clés USB ! A l'origine du bannissement, un virus qui aurait compromis le périphérique d'un militaire... qui l'aurait ensuite transmis.

Laurence Ifrah (DRMCC) | 01net. | le 12/12/2008 à 17h20 | 13 réactions



Le Pentagone interdit l'utilisation des clés USB ! A l'origine du bannissement, un virus qui aurait compromis le périphérique d'un militaire qui l'aurait ensuite transmis à tout le réseau. La clé USB nous pose un vrai dilemme, indispensable parce qu'on la glisse dans sa poche ou dans son sac et qu'aujourd'hui elle atteint des capacités de stockage impressionnantes, elle est néanmoins le

Les clefs USB

Le danger des clefs USB



Les clefs USB

Bref historique...

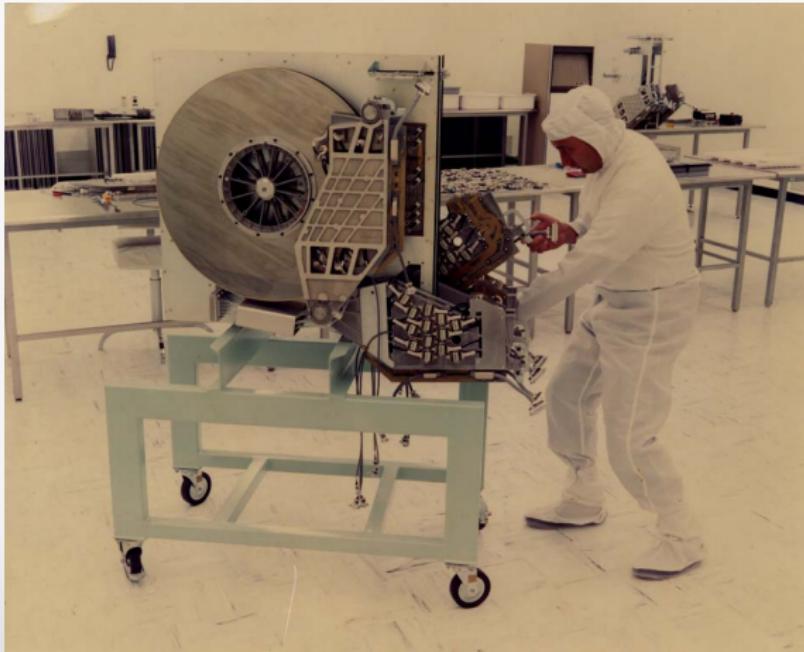
Au commencement, le stockage de l'information...



Les clefs USB

Bref historique...

Arrive l'ère du numérique, volumineux au début . . .



Les clefs USB

Bref historique...

Mais très vite se réduit...



Les clefs USB

Bref historique...

Et, l'évolution aidant, la clef USB naît.



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

Les caractéristiques de la clef USB...

- ▶ grande capacité
- ▶ fiable
- ▶ compact
- ▶ portable
- ▶ universelle
- ▶ économique



Les clefs USB

En résumé, c'est facile et pratique d'utilisation et donc sensible !



Des règles d'utilisation s'imposent...

Les clefs USB

Les règles d'utilisation de la clef USB...

① La clef USB est un support de transport

⇒ supprimez les informations une fois le transfert effectué.

② On ne mélange pas vie privée et vie professionnelle

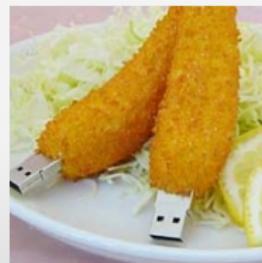
⇒ une clef pour la maison et une clef pour le bureau.

③ Différents niveaux de protection de l'information

⇒ une clef identifiée pour chaque niveau de protection : NP, DR, CD, CM.

④ La clef USB est le vecteur de propagation préféré des malwares

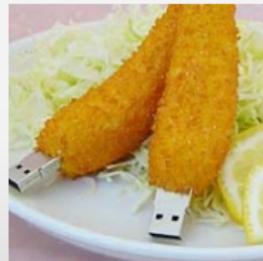
⇒ AVANT toute utilisation de la clef, passez en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef identifiée pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passez en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

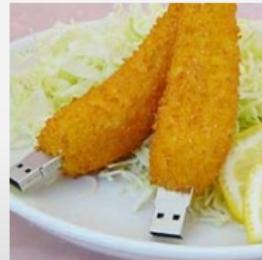
- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef identifiée pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passez-la en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef, identifiée, pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passez par un station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

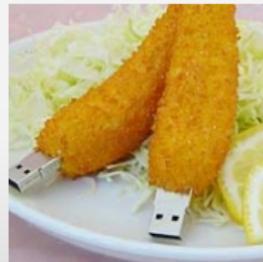
- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef, identifiée, pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passage en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef, identifiée, pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passage en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

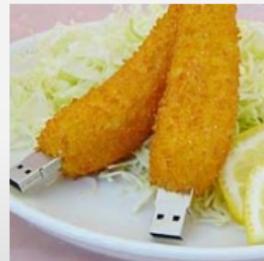
- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef, identifiée, pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passage en station blanche.



Les clefs USB

Les règles d'utilisation de la clef USB...

- ① La clef USB est un support de transport
⇒ supprimez les informations une fois le transfert effectué.
- ② On ne mélange pas vie privée et vie professionnelle
⇒ une clef pour la maison et une clef pour le bureau.
- ③ Différents niveaux de protection de l'information
⇒ une clef, identifiée, pour chaque niveau de protection : NP, DR, CD, CM.
- ④ La clef USB est le vecteur de propagation préféré des malwares
⇒ AVANT toute utilisation de la clef, passage en station blanche.



Les clefs USB

Une clef USB c'est petit...



et cela se perd facilement !

Les clefs USB

Dernières **règles d'utilisation de la clef USB...**

- ① On porte une **attention particulière** au rangement de sa clef USB
- ② On ne ramasse **jamais** une clef USB trouvée dans la rue
- ③ On prévient immédiatement son CSSI en cas de perte ou de vol



Les clefs USB

Dernières **règles d'utilisation de la clef USB...**

- ① On porte une **attention particulière** au rangement de sa clef USB
- ② On ne ramasse **jamais** une clef USB trouvée dans la rue
- ③ On prévient immédiatement son CSSI en cas de perte ou de vol



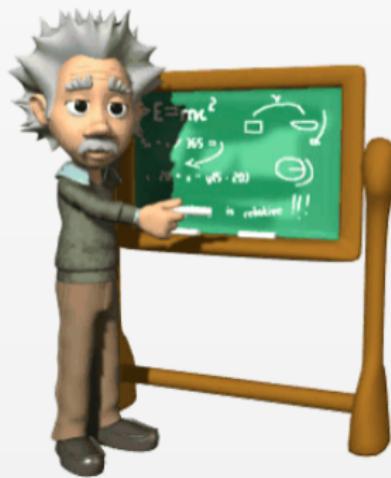
Les clefs USB

Dernières **règles d'utilisation** de la clef USB...

- ① On porte une **attention particulière** au rangement de sa clef USB
- ② On ne ramasse **jamais** une clef USB trouvée dans la rue
- ③ On prévient immédiatement son CSSI en cas de perte ou de vol

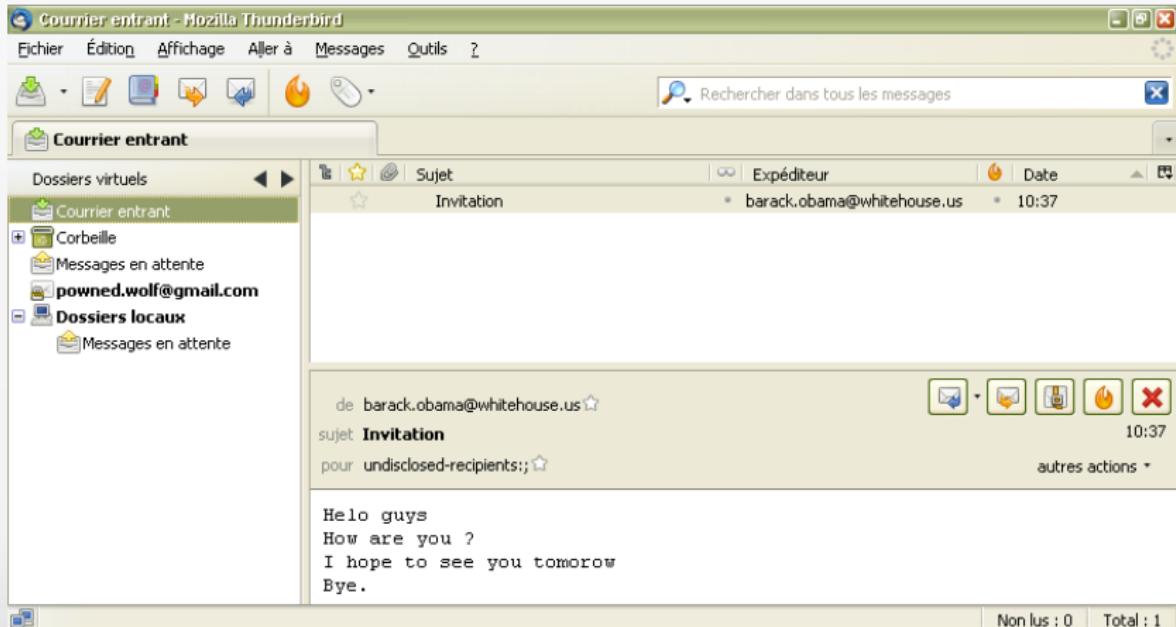


La messagerie



Forger un faux mail...

Forger un faux mail est **facile**



Forger un faux mail piégé...

nouvel
Obs.com

mercredi 13 avril 2011

Météo
Traducteur
Mobile

Guide
Conjugal
Billet

ACTUALITE VIDEO PHOTO BLOG TELE OBS CINE BIBLIOS VOYAGE AUTO

Politique | Monde | Les révolutions arabes | Le mariage de Kate et William | People | Média | Planète | Société | Eco

07/03/11 14:54

44 réactions

Bercy victime d'une gigantesque attaque informatique

150 ordinateurs du ministère de l'Economie ont été infiltrés. François Baroin affirme qu'il y a des "pistes" sur l'origine des attaques.

Mots-clés : Bercy, économie, attaque, informatique, hacker, G20



+T -T
Imprimer
Envoyer
Partager
Traduire
Réagir (44)
J'aime 24

Le ministère de l'Economie et des Finances à Paris, en mars 2010. (c) Afp

Le ministre du Budget, François Baroin, a indiqué lundi 7 mars sur Europe 1 qu'il y avait des "pistes" pour l'instant non confirmées sur l'origine des attaques contre le système informatique du ministère de l'Economie et des Finances (Bercy) en décembre.

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

➊ On ne répond jamais à un email :

- ▶ provenant d'une **banque** ou de **paypal**
- ▶ en **langue étrangère** ou en mauvais français
- ▶ demandant des informations **confidentielles**

➋ On ne clique jamais sur un lien (URL) contenu dans un email

Ce qu'il faut faire...

- ➌ On écrit toujours ses emails en mode **texte**
- ➌ On impose toujours la réception de ses emails en mode **texte**
- ➌ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ➌ Ne pas donner son nom et son prénom dans les emails
- ➌ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

① On ne répond jamais à un email :

- ▶ provenant d'une **banque** ou de **paypal**
- ▶ en **langue étrangère** ou en mauvais français
- ▶ demandant des **informations confidentielles**

② On ne clique jamais sur un lien (URL) contenu dans un email

Ce qu'il faut faire...

- ③ On écrit toujours ses emails en mode texte
- ④ On impose toujours la réception de ses emails en mode texte
- ⑤ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ⑥ Ne pas donner son nom et son prénom dans les signatures
- ⑦ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

① On ne répond jamais à un email :

- ▶ provenant d'une **banque** ou de **paypal**
- ▶ en **langue étrangère** ou en mauvais français
- ▶ demandant des **informations confidentielles**

② On ne clique jamais sur un lien (URL) contenu dans un email

Ce qu'il faut faire...

● On écrit toujours ses emails en **mode texte**

● On impose toujours la réception de ses emails en mode texte

● Ne donner son adresse email professionnelle qu'à des personnes de confiance

● Ne pas donner son nom et son prénom dans l'adresse email

● On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

① On ne répond jamais à un email :

- ▶ provenant d'une **banque** ou de **paypal**
- ▶ en **langue étrangère** ou en mauvais français
- ▶ demandant des **informations confidentielles**

② On ne clique jamais sur un lien (URL) contenu dans un email

Ce qu'il faut faire...

① On écrit toujours ses emails en **mode texte**

② On impose toujours la réception de ses emails en mode texte

③ Ne donner son adresse email professionnelle qu'à des personnes de confiance

④ Ne pas donner son nom et son prénom dans son email

⑤ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ➊ On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ➋ On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ➌ On écrit toujours ses emails en **mode texte**
- ➍ On impose toujours la réception de ses emails en mode texte
- ➎ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ➏ Ne pas donner son adresse email à des personnes qui n'en ont pas besoin
- ➐ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ① On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ② On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ① On écrit toujours ses emails en **mode texte**
- ② On impose toujours la réception de ses emails en mode texte
- ③ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ④ En cas de suspicion on **confirme la provenance** (appel téléphonique)
- ⑤ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ① On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ② On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ① On écrit toujours ses emails en **mode texte**
- ② On impose toujours la réception de ses emails en mode texte
- ③ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ④ En cas de suspicion on **confirme** la provenance (appel téléphonique)
- ⑤

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ① On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ② On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ① On écrit toujours ses emails en **mode texte**
- ② On impose toujours la réception de ses emails en mode texte
- ③ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ④ En cas de suspicion on **confirme** la provenance (appel téléphonique)
- ⑤ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ① On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ② On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ① On écrit toujours ses emails en **mode texte**
- ② On impose toujours la réception de ses emails en mode texte
- ③ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ④ En cas de suspicion on **confirme** la provenance (appel téléphonique)
- ⑤ On prévient immédiatement son OSSI en cas de doute

Les emails

Règles de sécurité pour les emails...

Ce qu'il ne faut pas faire...

- ① On ne répond jamais à un email :
 - ▶ provenant d'une **banque** ou de **paypal**
 - ▶ en **langue étrangère** ou en mauvais français
 - ▶ demandant des **informations confidentielles**
- ② On ne clique jamais sur **un lien (URL)** contenu dans un email

Ce qu'il faut faire...

- ① On écrit toujours ses emails en **mode texte**
- ② On impose toujours la réception de ses emails en mode texte
- ③ Ne donner son adresse email professionnelle qu'à des personnes de confiance
- ④ En cas de suspicion on **confirme** la provenance (appel téléphonique)
- ⑤ On prévient immédiatement son OSSI en cas de doute

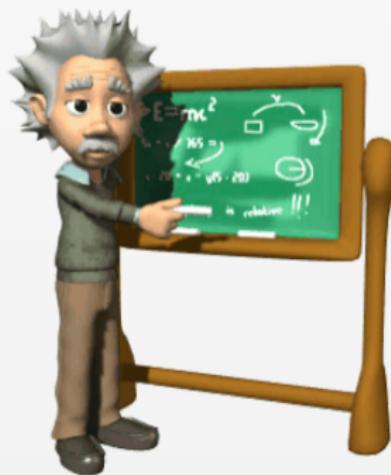
Les emails

Règles de sécurité pour les emails...



Interdiction formelle d'utiliser une adresse email personnelle à des fins professionnelles

Classification des données



Classification des données

- ▶ Les **données** sont au cœur des systèmes d'information
- ▶ Certaines données ou informations sont **sensibles**
- ▶ Les informations sensibles doivent être **protégées**
- ▶ Pour protéger une information sensible on la classifie

Information classifiée

Une information classifiée est une information sensible dont l'accès est restreint par une loi ou un règlement à un groupe spécifique de personnes.



Classification des données

- ▶ Les **données** sont au cœur des systèmes d'information
- ▶ Certaines données ou informations sont **sensibles**
- ▶ Les informations sensibles doivent être **protégées**
- ▶ Pour protéger une information sensible on la classifie

Information classifiée

Une information classifiée est une information sensible dont l'accès est **restreint** par une loi ou un règlement à un groupe spécifique de personnes.



Classification des données

- ▶ Les **données** sont au cœur des systèmes d'information
- ▶ Certaines données ou informations sont **sensibles**
- ▶ Les informations sensibles doivent être **protégées**
- ▶ Pour **protéger** une information sensible on la **classifie**

Information classifiée

Une information classifiée est une information sensible dont l'accès est **restreint** par une loi ou un règlement à un groupe spécifique de personnes.



Classification des données

- ▶ Les **données** sont au cœur des systèmes d'information
- ▶ Certaines données ou informations sont **sensibles**
- ▶ Les informations sensibles doivent être **protégées**
- ▶ Pour **protéger** une information sensible on la **classifie**

Information classifiée

Une information classifiée est une information sensible dont l'accès est **restreint** par une loi ou un règlement à un groupe spécifique de personnes.



Classification des données

- ▶ Les **données** sont au cœur des systèmes d'information
- ▶ Certaines données ou informations sont **sensibles**
- ▶ Les informations sensibles doivent être **protégées**
- ▶ Pour **protéger** une information sensible on la **classifie**

Information classifiée

Une information classifiée est une information sensible dont l'accès est **restreint** par une loi ou un règlement à un groupe spécifique de personnes.



Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

L'accès aux secrets de la défense nationale est une **préoccupation constante** :

- ▶ des services étrangers
- ▶ de groupements divers
- ▶ d'individus isolés

TOP SECRET//SI//ORCON//NOFORN

Gmail Hotmail YAHOO! Google skype paltalk.com AOL e-mail YouTube

(TS//SI//NF) Introduction U.S. as World's Telecommunications Backbone

SPECIAL SOURCE OPERATIONS

PRISM

Much of the world's communications flow through the U.S.

A target's phone call, e-mail or chat will take the **cheapest path, not the physically most direct** path – you can't always predict the path.

Your target's communications could easily be flowing into and through the U.S.

Region	Bandwidth Capacity (Gbps)
Europe	4.812 Gbps
Africa	4.423 Gbps
Asia & Pacific	4.423 Gbps
Latin America & Caribbean	2.721 Gbps
U.S. & Canada	1.1 Gbps

Source: TeleGeography Research

TOP SECRET//SI//ORCON//NOFORN

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

L'accès aux secrets de la défense nationale est une **préoccupation constante** :

- ▶ des services étrangers
- ▶ de groupements divers
- ▶ d'individus isolés

TOP SECRET//SI//ORCON//NOFORN

Gmail Hotmail YAHOO! Google skype paltalk.com AOL mail YouTube

(TS//SI//NF) Introduction U.S. as World's Telecommunications Backbone

PRISM

SPECIAL SOURCE OPERATIONS

Much of the world's communications flow through the U.S.

A target's phone call, e-mail or chat will take the **cheapest path, not the physically most direct** path – you can't always predict the path.

Your target's communications could easily be flowing into and through the U.S.

Region	Bandwidth Capacity (Gbps)
Europe	4.423 Gbps
U.S. & Canada	4.912 Gbps
Africa	4.423 Gbps
Asia & Pacific	4.051 Gbps
Latin America & Caribbean	2.721 Gbps
Middle East	1.1 Gbps

International Internet Regional Bandwidth Capacity in 2011
Source: TeleGeography Research

TOP SECRET//SI//ORCON//NOFORN

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

L'accès aux secrets de la défense nationale est une **préoccupation constante** :

- ▶ des services étrangers
- ▶ de groupements divers
- ▶ d'individus isolés

TOP SECRET//SI//ORCON//NOFORN

Gmail HotmailTM GoogleTM skypeTM paltalkTM AOLTM mail YouTubeTM

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

SPECIAL SOURCE OPERATIONS

PRISM

Much of the world's communications flow through the U.S.

A target's phone call, e-mail or chat will take the **cheapest path, not the physically most direct** path – you can't always predict the path.

Your target's communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

POBCAC



**Problem Occurs Between
Computer and Chair**

L'action de ces organisations est souvent
facilitée par

- ▶ l'ignorance
- ▶ l'inattention
- ▶ la négligence

de certains détenteurs d'informations
qui ne prennent pas les précautions
suffisantes pour en assurer la protection.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

POBCAC



**Problem Occurs Between
Computer and Chair**

L'action de ces organisations est souvent
facilitée par

- ▶ l'ignorance
- ▶ l'inattention
- ▶ la négligence

de certains détenteurs d'informations
qui ne prennent pas les précautions
suffisantes pour en assurer la protection.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

POBCAC



**Problem Occurs Between
Computer and Chair**

L'action de ces organisations est souvent
facilitée par

- ▶ l'ignorance
- ▶ l'inattention
- ▶ **la négligence**

de certains détenteurs d'informations
qui ne prennent pas les précautions
suffisantes pour en assurer la protection.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Toutes les personnes traitant d'informations présentant un caractère de **secret de la défense nationale** doivent être sensibilisées sur leurs responsabilités.



En cas de manquement, elles peuvent encourir des sanctions pénales graves en application des dispositions des articles 413-9 et suivants du code pénal, **y compris en cas d'imprudence ou de négligence** de leur part.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Secret de la défense nationale

Présentent un caractère de secret de la défense nationale les renseignements, procédés, objets, documents, données informatisées ou fichiers :

- ▶ intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion
- ▶ dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Secret de la défense nationale

Présentent un caractère de secret de la défense nationale les renseignements, procédés, objets, documents, données informatisées ou fichiers :

- ▶ intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion
- ▶ dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

Les informations ou supports protégés portent la mention de leur niveau de classification

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

L'accès aux informations classifiées est subordonné à deux conditions :

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

Les informations ou supports protégés portent la mention de leur niveau de classification

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

L'accès aux informations classifiées est subordonné à deux conditions :

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

Les informations ou supports protégés portent la mention de leur niveau de classification

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

L'accès aux informations classifiées est subordonné à deux conditions :

- autorisation d'accès délivrée par un responsable
- justification de l'accès

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

Les informations ou supports protégés portent la mention de leur niveau de classification

L'accès aux informations classifiées est subordonné à deux conditions :

- ▶ avoir fait l'objet d'une décision d'habilitation préalable
- ▶ avoir besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

Les informations ou supports protégés portent la mention de leur niveau de classification

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

L'accès aux informations classifiées est subordonné à deux conditions :

- ▶ avoir fait l'objet d'une décision d'**habilitation** préalable
- ▶ avoir **besoin de les connaître** pour l'accomplissement de sa fonction ou de sa mission

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles de mise en œuvre de la protection du secret de la défense nationale

TRÈS SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire très gravement à la défense nationale et qui concernent les priorités gouvernementales en matière de défense

Les informations ou supports protégés portent la mention de leur niveau de classification

SECRET-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale

CONFIDENTIEL-DÉFENSE

Réervé aux informations ou supports protégés dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié TSD ou SD

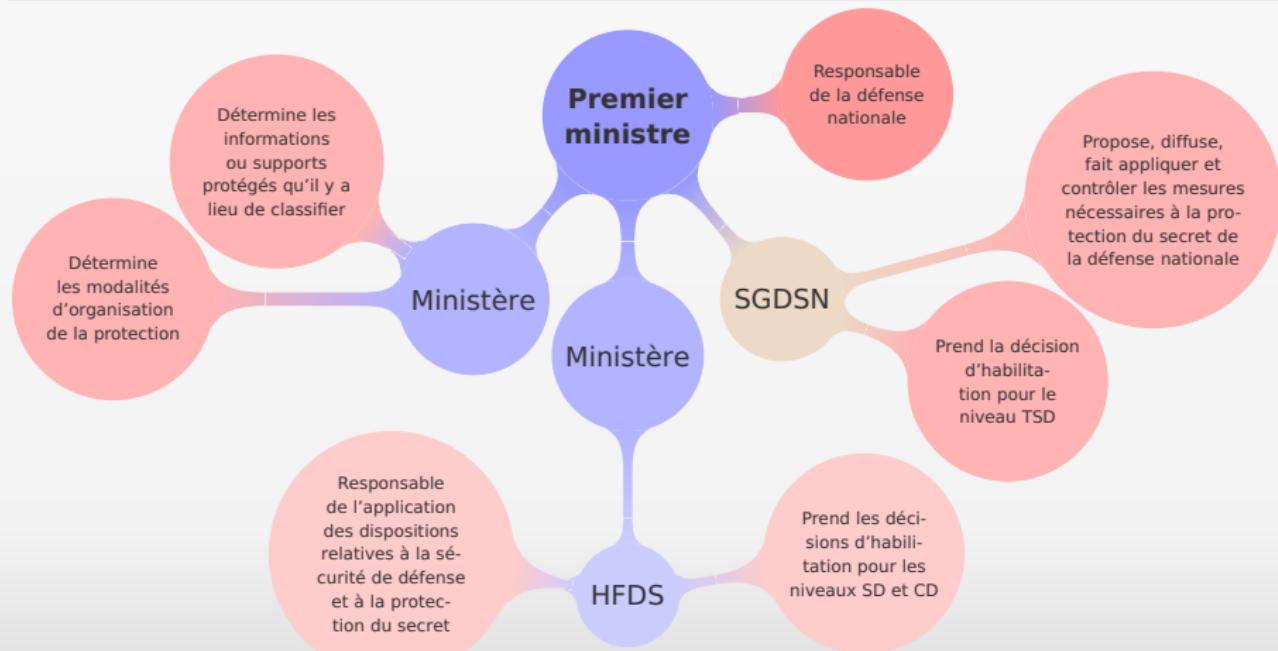
L'accès aux informations classifiées est subordonné à deux conditions :

- ▶ avoir fait l'objet d'une décision d'**habilitation** préalable
- ▶ avoir **besoin de les connaître** pour l'accomplissement de sa fonction ou de sa mission

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Organisation générale de la protection du secret de la défense nationale



Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

La procédure d'habilitation

Définition

La procédure d'habilitation a pour objet de vérifier qu'une personne peut, **sans risque** pour la défense nationale ou pour sa propre sécurité, **connaître** des informations ou supports protégés dans l'exercice de ses fonctions.

Validité de l'avis de sécurité

- ▶ **5 ans** pour le TSD
- ▶ **7 ans** pour le SD
- ▶ **10 ans** pour le CD

La durée de validité de la décision d'habilitation peut être distincte de celle de l'avis de sécurité, elle reste cependant toujours inférieure.

Dossier de demande d'habilitation

- ▶ demande d'habilitation (*responsable*)
- ▶ notice individuelle de sécurité (*individu*)
- ▶ 3 photos d'identité

Engagement de responsabilité

Le titulaire d'une décision d'habilitation reconnaît avoir pris connaissance des obligations particulières imposées à toute personne dépositaire ou ayant eu connaissance d'une information ou d'un support protégé, ainsi que des sanctions prévues par les articles 413-10 à 413-12 du code pénal.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

La procédure d'habilitation

Définition

La procédure d'habilitation a pour objet de vérifier qu'une personne peut, **sans risque** pour la défense nationale ou pour sa propre sécurité, **connaître** des informations ou supports protégés dans l'exercice de ses fonctions.

Validité de l'avis de sécurité

- ▶ **5 ans** pour le TSD
- ▶ **7 ans** pour le SD
- ▶ **10 ans** pour le CD

La durée de validité de la décision d'habilitation peut être distincte de celle de l'avis de sécurité, elle reste cependant toujours inférieure.

Dossier de demande d'habilitation

- ▶ demande d'habilitation (*responsable*)
- ▶ notice individuelle de sécurité (*individu*)
- ▶ 3 photos d'identité

Engagement de responsabilité

Le titulaire d'une décision d'habilitation reconnaît avoir pris connaissance des obligations particulières imposées à toute personne dépositaire ou ayant eu connaissance d'une information ou d'un support protégé, ainsi que des sanctions prévues par les articles 413-10 à 413-12 du code pénal.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

La procédure d'habilitation

Définition

La procédure d'habilitation a pour objet de vérifier qu'une personne peut, **sans risque** pour la défense nationale ou pour sa propre sécurité, **connaître** des informations ou supports protégés dans l'exercice de ses fonctions.

Validité de l'avis de sécurité

- ▶ **5 ans** pour le TSD
- ▶ **7 ans** pour le SD
- ▶ **10 ans** pour le CD

La durée de validité de la décision d'habilitation peut être distincte de celle de l'avis de sécurité, elle reste cependant toujours inférieure.

Dossier de demande d'habilitation

- ▶ demande d'habilitation (*responsable*)
- ▶ notice individuelle de sécurité (*individu*)
- ▶ 3 photos d'identité

Engagement de responsabilité

Le titulaire d'une décision d'habilitation reconnaît avoir pris connaissance des obligations particulières imposées à toute personne dépositaire ou ayant eu connaissance d'une information ou d'un support protégé, ainsi que des sanctions prévues par les articles 413-10 à 413-12 du code pénal.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

La procédure d'habilitation

Définition

La procédure d'habilitation a pour objet de vérifier qu'une personne peut, **sans risque** pour la défense nationale ou pour sa propre sécurité, **connaître** des informations ou supports protégés dans l'exercice de ses fonctions.

Validité de l'avis de sécurité

- ▶ **5 ans** pour le TSD
- ▶ **7 ans** pour le SD
- ▶ **10 ans** pour le CD

La durée de validité de la décision d'habilitation peut être distincte de celle de l'avis de sécurité, elle reste cependant toujours inférieure.

Dossier de demande d'habilitation

- ▶ demande d'habilitation (*responsable*)
- ▶ notice individuelle de sécurité (*individu*)
- ▶ 3 photos d'identité

Engagement de responsabilité

Le titulaire d'une décision d'habilitation reconnaît avoir pris connaissance des obligations particulières imposées à toute personne dépositaire ou ayant eu connaissance d'une information ou d'un support protégé, ainsi que des sanctions prévues par les articles 413-10 à 413-12 du code pénal.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles générales

La mention du niveau de classification doit être portée sur le support de l'information.

Un support **non papier** d'informations protégées classifiées **conserve toujours** le niveau de classification qui lui a été initialement attribué.

La mention **SPÉCIAL FRANCE** est employée pour des informations ou supports protégés ou non que l'autorité émettrice estime ne devoir être communiquées qu'aux **nationaux français**. Elle n'est pas une mention de classification.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles générales

La mention du niveau de classification doit être portée sur le support de l'information.

Un support **non papier** d'informations protégées classifiées **conserve toujours** le niveau de classification qui lui a été initialement attribué.

La mention **SPÉCIAL FRANCE** est employée pour des informations ou supports protégés ou non que l'autorité émettrice estime ne devoir être communiquées qu'aux **nationaux français**. Elle n'est pas une mention de classification.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles générales

La mention du niveau de classification doit être portée sur le support de l'information.

Un support **non papier** d'informations protégées classifiées **conserve toujours** le niveau de classification qui lui a été initialement attribué.

La mention **SPÉCIAL FRANCE** est employée pour des informations ou supports protégés ou non que l'autorité émettrice estime ne devoir être communiquées qu'aux **nationaux français**. Elle n'est pas une mention de classification.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **TRÈS SECRET-DÉFENSE**

Aucun service ou organisme ne peut **élaborer, traiter, stocker, acheminer, présenter ou détruire** des informations ou supports protégés classifiés Très Secret-Défense, sans y avoir préalablement été **autorisé** par le Premier ministre.

La **reproduction totale ou partielle** des informations ou supports protégés classifiés Très Secret-Défense est **formellement interdite**.

Une informations ou support TSD ne peuvent être élaborés, reproduits, préparés en vue de leur circulation, conservés, archivés, ou détruits que dans les **zones réservées**.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **TRÈS SECRET-DÉFENSE**

Aucun service ou organisme ne peut **élaborer, traiter, stocker, acheminer, présenter ou détruire** des informations ou supports protégés classifiés Très Secret-Défense, sans y avoir préalablement été **autorisé** par le Premier ministre.

La **reproduction totale ou partielle** des informations ou supports protégés classifiés Très Secret-Défense est **formellement interdite**.

Une informations ou support TSD ne peuvent être élaborés, reproduits, préparés en vue de leur circulation, conservés, archivés, ou détruits que dans les **zones réservées**.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **TRÈS SECRET-DÉFENSE**

Aucun service ou organisme ne peut **élaborer, traiter, stocker, acheminer, présenter ou détruire** des informations ou supports protégés classifiés Très Secret-Défense, sans y avoir préalablement été **autorisé** par le Premier ministre.

La **reproduction totale ou partielle** des informations ou supports protégés classifiés Très Secret-Défense est **formellement interdite**.

Une informations ou support TSD ne peuvent être élaborés, reproduits, préparés en vue de leur circulation, conservés, archivés, ou détruits que dans les **zones réservées**.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page

- ▶ **identification** :

- ▶ Sur la première page : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification

- ▶ nom(s) d'exemplaire

- ▶ **pagination** :

- ▶ numérotation de chaque page
- ▶ nombre de page sur la 1^{re} page
- ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page

- ▶ **identification** :

- ▶ Sur la première page : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification

- ▶ **pagination** :

- ▶ numérotation de chaque page entre 1 et 1000

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ Sur la première page : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ nombre total d'exemplaire
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{re} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ Sur la première page : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ nombre total d'exemplaire
- ▶ **pagination** :
 - ▶ numérotation de chaque page sauf la 1^{re} page

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ **nombre total de pages**
 - ▶ **nombre de page sur la 1^{re} page**
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ **nombre total de pages** dans la 1^{re} page
 - ▶ **nombre de page sur la 1^{re} page**

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ nombre de page sur la 1^{re} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ nombre de page sur la 1^{re} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ les pages blanches portent la mention [P00000000]

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ les pages blanches portent la mention [P00000000]

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ les pages blanches portent la mention **PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ nom de l'organisme émetteur
 - ▶ date d'émission
 - ▶ numéro d'enregistrement
 - ▶ signature
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :
 - ▶ numérotation de chaque page

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ **nombre de page sur la 1^{ère} page**

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le **marquage** sur support papier

SECRET DÉFENSE

- ▶ **timbrage** : **SECRET-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
 - ▶ **nombre total d'exemplaire**
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page
 - ▶ **les pages blanches portent la mention PAS DE TEXTE**

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : **CONFIDENTIEL-DÉFENSE** en haut et en bas de chaque page
- ▶ **identification** :
 - ▶ **Sur la première page** : service émetteur, date d'émission, numéro d'enregistrement, timbre de classification
- ▶ **pagination** :
 - ▶ numérotation de chaque page
 - ▶ nombre de page sur la 1^{ère} page

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le marquage sur support non papier

SECRET DÉFENSE

- ▶ **timbrage** : SECRET-DÉFENSE sur le support

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : CONFIDENTIEL-DÉFENSE sur le support

- ▶ **identification** : inscription des références et du volume de chacune des informations enregistrées. L'identification peut se faire sur le support ou sur une fiche papier annexée.

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le marquage sur support non papier

SECRET DÉFENSE

- ▶ **timbrage** : SECRET-DÉFENSE sur le support

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : CONFIDENTIEL-DÉFENSE sur le support

- ▶ **identification** : inscription des références et du volume de chacune des informations enregistrées. *L'identification peut se faire sur le support ou sur une fiche papier annexée.*

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour le marquage sur support non papier

SECRET DÉFENSE

- ▶ **timbrage** : SECRET-DÉFENSE sur le support

CONFIDENTIEL DÉFENSE

- ▶ **timbrage** : CONFIDENTIEL-DÉFENSE sur le support

- ▶ **identification** : inscription des références et du volume de chacune des informations enregistrées. *L'identification peut se faire sur le support ou sur une fiche papier annexée.*

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour l'**enregistrement**

Tout support contenant des informations protégées classifiées au niveau SD ou CD est **enregistré** :

- ▶ dans l'ordre chronologique
- ▶ en attribuant sans ambiguïté l'ISC à une **personne physique**

Exemple de tableau d'enregistrement d'ISC :

Numéro	Date	Référence	Détenteur	Support	Observations
001-00/2014	06/01/2014	64/DEF/DCSSA/CAB	CDT Jean Dupont	Papier (original)	
001-01/2014	06/01/2014	64/DEF/DCSSA/CAB	CNE Jacques Martin	Papier (photocopie)	
002-00/2014	07/01/2014	860/DEF/DCSSA/AA	CDT Jean Dupont	Papier (original)	

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour l'**enregistrement**

Tout support contenant des informations protégées classifiées au niveau SD ou CD est **enregistré** :

- ▶ dans l'ordre chronologique
- ▶ en attribuant sans ambiguïté l'ISC à une **personne physique**

Exemple de tableau d'enregistrement d'ISC :

Numéro	Date	Référence	Détenteur	Support	Observations
001-00/2014	06/01/2014	64/DEF/DCSSA/CAB	CDT Jean Dupont	Papier (original)	
001-01/2014	06/01/2014	64/DEF/DCSSA/CAB	CNE Jacques Martin	Papier (photocopie)	
002-00/2014	07/01/2014	860/DEF/DCSSA/AA	CDT Jean Dupont	Papier (original)	

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour l'**enregistrement**

Tout support contenant des informations protégées classifiées au niveau SD ou CD est **enregistré** :

- ▶ dans l'ordre chronologique
- ▶ en attribuant sans ambiguïté l'ISC à une **personne physique**

Exemple de tableau d'enregistrement d'ISC :

Numéro	Date	Référence	Détenteur	Support	Observations
001-00/2014	06/01/2014	64/DEF/DCSSA/CAB	CDT Jean Dupont	Papier (original)	
001-01/2014	06/01/2014	64/DEF/DCSSA/CAB	CNE Jacques Martin	Papier (photocopie)	
002-00/2014	07/01/2014	860/DEF/DCSSA/AA	CDT Jean Dupont	Papier (original)	

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour l'**enregistrement**

Tout support contenant des informations protégées classifiées au niveau SD ou CD est **enregistré** :

- ▶ dans l'ordre chronologique
- ▶ en attribuant sans ambiguïté l'ISC à une **personne physique**

Exemple de tableau d'enregistrement d'ISC :

Numéro	Date	Référence	Détenteur	Support	Observations
001-00/2014	06/01/2014	64/DEF/DCSSA/CAB	CDT Jean Dupont	Papier (original)	
001-01/2014	06/01/2014	64/DEF/DCSSA/CAB	CNE Jacques Martin	Papier (photocopie)	
002-00/2014	07/01/2014	860/DEF/DCSSA/AA	CDT Jean Dupont	Papier (original)	

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour la reproduction

SECRET DÉFENSE

CONFIDENTIEL DÉFENSE

- ▶ reproduction avec l'autorisation de l'autorité émettrice
- ▶ reproduction par l'autorité détentrice

Les photocopieurs, télécopieurs et imprimantes utilisés pour la reproduction d'informations classifiées doivent être physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées.

Chaque ISC reproduit doit être enregistré

Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour la conservation

SECRET DÉFENSE

- ▶ Les ISC sont conservés dans des **coffres-forts** ou des **armoires fortes à combinaisons multiples**
- ▶ Les combinaisons sont changées au moins tous les **six mois**



CONFIDENTIEL DÉFENSE

- ▶ Les ISC CD sont conservés dans des **armoires fortes**



Classification des données

Secret de la défense nationale – IGI 1300/SGDN/PSE/SSD du 25 août 2003

Règles pratiques pour l'acheminement

SECRET DÉFENSE

CONFIDENTIEL DÉFENSE

À l'intérieur d'un même immeuble

- ▶ effectué par le détenteur lui-même
- ▶ compte-rendu au Bureau Sécurité

- ▶ effectué par une personne habilitée

Avec changement d'immeuble

- ▶ acheminement effectué par toute personne habilitée au niveau SD
- ▶ placement des ISC dans une sacoche ou une valise fermant à clef et dépourvue d'indication extérieure

- ▶ acheminement sous double enveloppe

Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

CONFIDENTIEL MÉDICAL

Secret médical – article L1110-4 du CSP

Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

Secret médical – article 226-13 du CP

La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'**un an d'emprisonnement et de 15000 euros d'amende**.



FICHE D'INFORMATION

Service hospitalier



Ce service hospitalier dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à réaliser, le cas échéant, des travaux statistiques à usage du service.

Les informations recueillies lors de votre consultation ou de votre hospitalisation, feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique. Ces informations sont réservées à l'équipe médicale qui vous suit ainsi que pour les données administratives, au service de facturation.

Conformément aux dispositions de la loi Informatique et Libertés*, vous pouvez obtenir communication des données vous concernant en vous adressant au correspondant Informatique et Liberté du Service de santé des Armées à l'adresse ci-dessous.

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

**Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Correspondant Informatique et Liberté
Direction centrale du Service de santé des Armées
Bureau des Systèmes d'Information et de Communication
Fort neuf de Vincennes
Cours des Maréchaux
Case 125
75614 Paris CEDEX 12

Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

CONFIDENTIEL MÉDICAL

Secret médical – article L1110-4 du CSP

Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

Secret médical – article 226-13 du CP

La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'**un an d'emprisonnement et de 15000 euros d'amende**.



FICHE D'INFORMATION

Service hospitalier



Ce service hospitalier dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à réaliser, le cas échéant, des travaux statistiques à usage du service.

Les informations recueillies lors de votre consultation ou de votre hospitalisation, feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique. Ces informations sont réservées à l'équipe médicale qui vous suit ainsi que pour les données administratives, au service de facturation.

Conformément aux dispositions de la loi Informatique et Libertés*, vous pouvez obtenir communication des données vous concernant en vous adressant au correspondant Informatique et Liberté du Service de santé des Armées à l'adresse ci-dessous.

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

**Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Correspondant Informatique et Liberté
Direction centrale du Service de santé des Armées
Bureau des Systèmes d'Information et de Communication
Fort neuf de Vincennes
Cours des Maréchaux
Case 125
75614 Paris CEDEX 12

Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

Règles pratiques pour le **CONFIDENTIEL MÉDICAL**

- ▶ **Gestion des listes des professionnels habilité à accéder au SIH et au SISMU**
- ▶ À chaque identifiant de connexion correspond une seule et unique personne physique
- ▶ Authentification par carte CPS pour tout accès à un SI de santé
- ▶ Toute information médicale à caractère personnelle devant être transmise sous forme numérique doit être chiffrée
- ▶ Interdiction de stockage de données médicales à caractère personnelle sur support de stockage de masse



Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

Règles pratiques pour le **CONFIDENTIEL MÉDICAL**

- ▶ Gestion des listes des professionnels habilité à accéder au SIH et au SISMU
- ▶ À chaque identifiant de connexion correspond une seule et unique personne physique
- ▶ Authentification par carte CPS pour tout accès à un SI de santé
- ▶ Toute information médicale à caractère personnelle devant être transmise sous forme numérique doit être chiffrée
- ▶ Interdiction de stockage de données médicales à caractère personnelle sur support de stockage de masse



Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

Règles pratiques pour le **CONFIDENTIEL MÉDICAL**

- ▶ Gestion des listes des professionnels habilité à accéder au SIH et au SISMU
- ▶ À chaque identifiant de connexion correspond une seule et unique personne physique
- ▶ Authentification par carte CPS pour tout accès à un SI de santé
- ▶ Toute information médicale à caractère personnelle devant être transmise sous forme numérique doit être chiffrée
- ▶ Interdiction de stockage de données médicales à caractère personnelle sur support de stockage de masse



Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

Règles pratiques pour le **CONFIDENTIEL MÉDICAL**

- ▶ Gestion des listes des professionnels habilité à accéder au SIH et au SISMU
- ▶ À chaque identifiant de connexion correspond une seule et unique personne physique
- ▶ Authentification par carte CPS pour tout accès à un SI de santé
- ▶ Toute information médicale à caractère personnelle devant être transmise sous forme numérique doit être chiffrée
- ▶ Interdiction de stockage de données médicales à caractère personnelle sur support de stockage de masse



Classification des données

Secret médical – *Code de la santé publique et Loi informatique & libertés*

Règles pratiques pour le **CONFIDENTIEL MÉDICAL**

- ▶ Gestion des listes des professionnels habilité à accéder au SIH et au SISMU
- ▶ À chaque identifiant de connexion correspond une seule et unique personne physique
- ▶ Authentification par carte CPS pour tout accès à un SI de santé
- ▶ Toute information médicale à caractère personnelle devant être transmise sous forme numérique doit être chiffrée
- ▶ Interdiction de stockage de données médicales à caractère personnelle sur support de stockage de masse



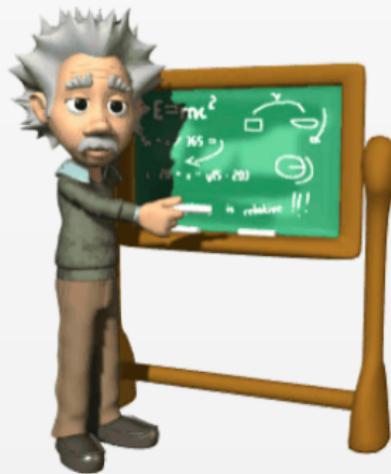
Politiques & Procédures

3 Contres mesures

- Organisation & Personnel
 - Organisation
 - Le personnel
- Techniques & Logiques
 - Les mots de passe
 - La lutte antivirale
 - Les clefs USB
 - La messagerie
 - Classification des données
- Politiques & Procédures
 - La réglementation
 - La politique SSI
 - Code de bon usage



La réglementation



La réglementation

Que dit la loi ?



La réglementation

Traitement des données à caractère personnel

Loi 78-17 du 6 janvier 1978 modifiée par la loi 2004-801 du 6 août 2004

Article 34 Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Code pénal art. 226-17 modifié par la loi 2004-801 du 6 août 2004

Article 226-17 Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de **cinq ans d'emprisonnement** et de **300 000 Euros d'amende**.

La réglementation

Des atteintes aux systèmes de traitement automatisé de données

Code pénal – articles L323-1 à L323-7 modifiés par la loi 2004-575 du 21/06/04

Article L323-1 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement** et de **30000 euros d'amende**.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **trois ans d'emprisonnement** et de 45000 euros d'amende.

Article L323-2 Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **cinq ans d'emprisonnement** et de **75000 Euros d'amende**.

Article L323-3 Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement** et de **75000 Euros d'amende**.

La réglementation

Des atteintes aux systèmes de traitement automatisé de données

Code pénal – art. L323-1 à L323-7 modifiés par la loi 2004-575 du 21/06/04

Article L323-3-1 Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article L323-4 La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

La réglementation

Des atteintes au secret de la défense nationale

Code pénal – art. L413-9 à L413-12 modifiés par la loi 2009-928 du 29/07/09

Article L413-10 Est puni de **sept ans d'emprisonnement** et de **100 000 euros d'amende** le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, **d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer** le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de **trois ans d'emprisonnement** et de **45000 euros d'amende**.

La réglementation

Copie illicite de logiciels

Code de la propriété intellectuelle – art. L335-2 et suivants

Article L335-2 Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

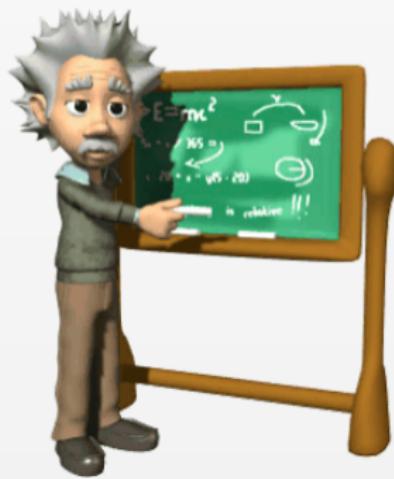
La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Article L335-3 Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.

Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6.

Est également un délit de contrefaçon toute captation totale ou partielle d'une œuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique.

La politique SSI



La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Technologie et outils utilisés pour les services
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Information technique et normative
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Information technique et normative
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Formation à la cybersécurité pour les services
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Technologie et technique de protection des données
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Messageries électroniques, commentaires de service
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Messages électroniques et notes de service
- ▶ ...

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Messages électroniques et notes de service
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Messages électroniques et notes de service
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

La politique SSI

Politique SSI

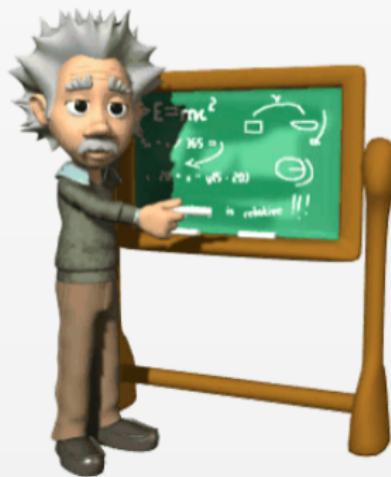
Ensemble **formalisé** des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. **La PSSI constitue le socle de la SSI**

La PSSI est un outil de communication

La PSSI se décline en documents d'application de manière adaptée aux acteurs destinataires

- ▶ Charte des utilisateurs ou code de bon usage
- ▶ Procédures d'exploitation de sécurité
- ▶ Tutoriels sur le réseau interne
- ▶ Séances de sensibilisation
- ▶ Messages électroniques et notes de service
- ▶ Site Web : <http://ssi.sante.defense.gouv.fr>

Code de bon usage



Le code de bon usage

Objectifs :

- ▶ définir les modalités d'usage attendu des systèmes d'information
- ▶ définir les dispositions spécifiques liées à l'usage de certains médias
- ▶ fixer les attributions particulières des acteurs de la SSI
- ▶ définir les moyens de contrôle mis en œuvre.



Le code de bon usage

Objectifs :

- ▶ définir les modalités d'usage attendu des systèmes d'information
- ▶ définir les dispositions spécifiques liées à l'usage de certains médias
- ▶ fixer les attributions particulières des acteurs de la SSI
- ▶ définir les moyens de contrôle mis en œuvre.



Le code de bon usage

Objectifs :

- ▶ définir les modalités d'usage attendu des systèmes d'information
- ▶ définir les dispositions spécifiques liées à l'usage de certains médias
- ▶ fixer les attributions particulières des acteurs de la SSI
- ▶ définir les moyens de contrôle mis en œuvre.



Le code de bon usage

Objectifs :

- ▶ définir les modalités d'usage attendu des systèmes d'information
- ▶ définir les dispositions spécifiques liées à l'usage de certains médias
- ▶ fixer les attributions particulières des acteurs de la SSI
- ▶ définir les moyens de contrôle mis en œuvre.



Le code de bon usage

Objectifs :

- ▶ définir les modalités d'usage attendu des systèmes d'information
- ▶ définir les dispositions spécifiques liées à l'usage de certains médias
- ▶ fixer les attributions particulières des acteurs de la SSI
- ▶ définir les moyens de contrôle mis en œuvre.



Le code de bon usage

Les bons usages ?

- ▶ Ne pas **modifier** son environnement de travail
- ▶ Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- ▶ Les droits d'accès et priviléges sont **personnels** et **inaccessibles**
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les contenus malveillants
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas **modifier** son environnement de travail
- ▶ Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- ▶ Les droits d'accès et priviléges sont **personnels** et **inaccessibles**
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les **contenus malveillants**
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas **modifier** son environnement de travail
- ▶ Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- ▶ Les droits d'accès et privilèges sont **personnels** et **inaccessibles**
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les **contenus malveillants**
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas **modifier** son environnement de travail
- ▶ Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- ▶ Les droits d'accès et privilèges sont **personnels** et **inaccessibles**
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les **contenus malveillants**
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour **conserver** les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas **modifier** son environnement de travail
- ▶ Ne pas connecter un équipement **personnel** sur un SI **professionnel**
- ▶ Les droits d'accès et priviléges sont **personnels** et **inaccessibles**
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les **contenus malveillants**
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour **conserver** les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas modifier son environnement de travail
- ▶ Ne pas connecter un équipement personnel sur un SI professionnel
- ▶ Les droits d'accès et priviléges sont personnels et incessibles
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les contenus malveillants
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

Les bons usages ?

- ▶ Ne pas modifier son environnement de travail
- ▶ Ne pas connecter un équipement personnel sur un SI professionnel
- ▶ Les droits d'accès et priviléges sont personnels et incessibles
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les contenus malveillants
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Le code de bon usage

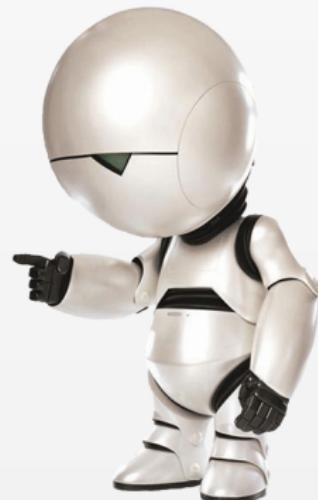
Les bons usages ?

- ▶ Ne pas modifier son environnement de travail
- ▶ Ne pas connecter un équipement personnel sur un SI professionnel
- ▶ Les droits d'accès et priviléges sont personnels et incessibles
- ▶ Rendre compte en cas d'incident
- ▶ Respecter les mesures de lutte contre les contenus malveillants
- ▶ L'usurpation d'identité constitue un délit
- ▶ L'utilisateur doit prendre toute mesure pour conserver les documents électroniques
- ▶ Vider régulièrement sa boîte aux lettres

Signature des engagements de sécurité

Conclusion

- 1** Introduction
- 2** Risques, menaces et vulnérabilités
- 3** Contres mesures
- 4** Conclusion



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...



Petit Quiz final ...

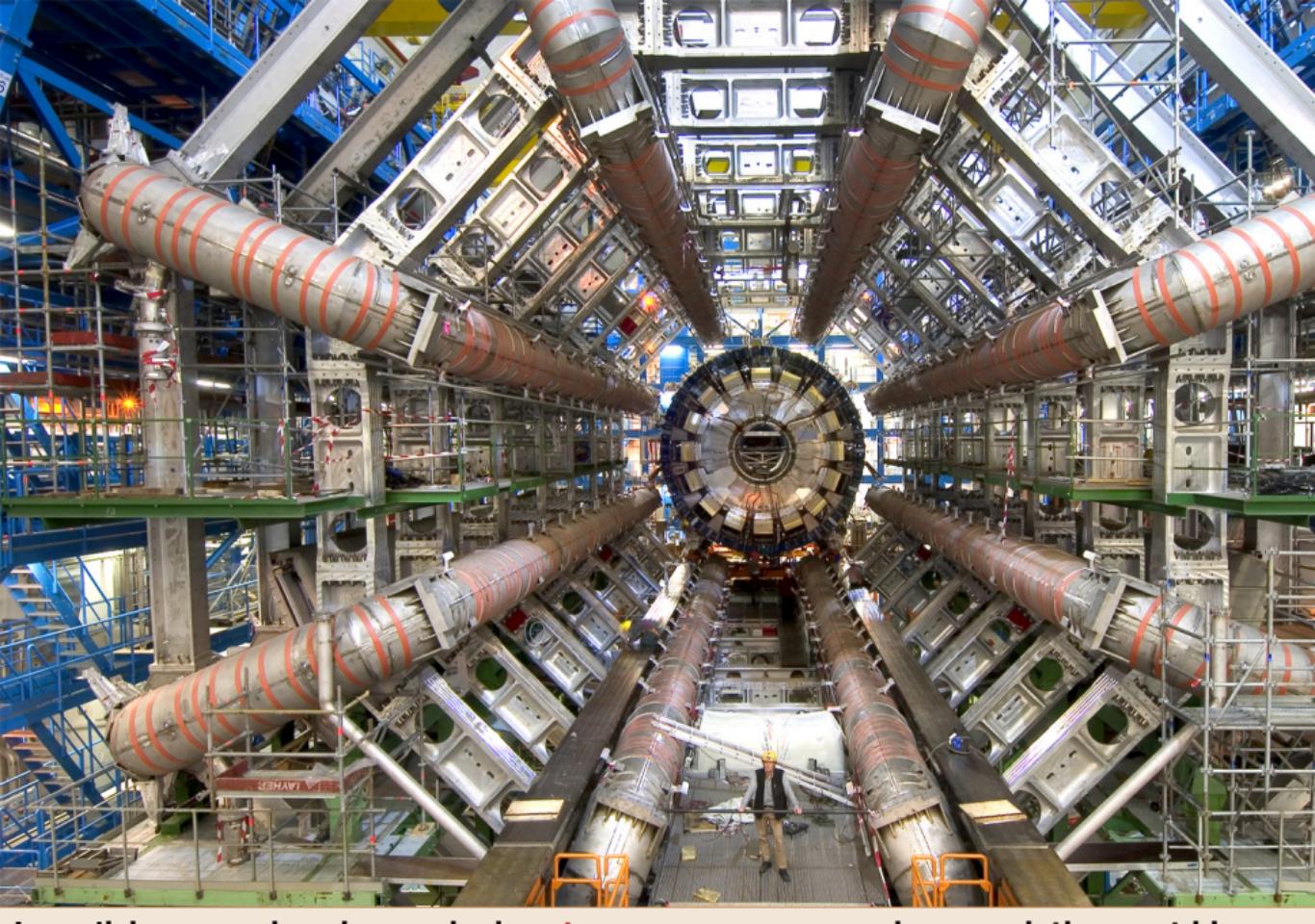


Petit Quiz final ...



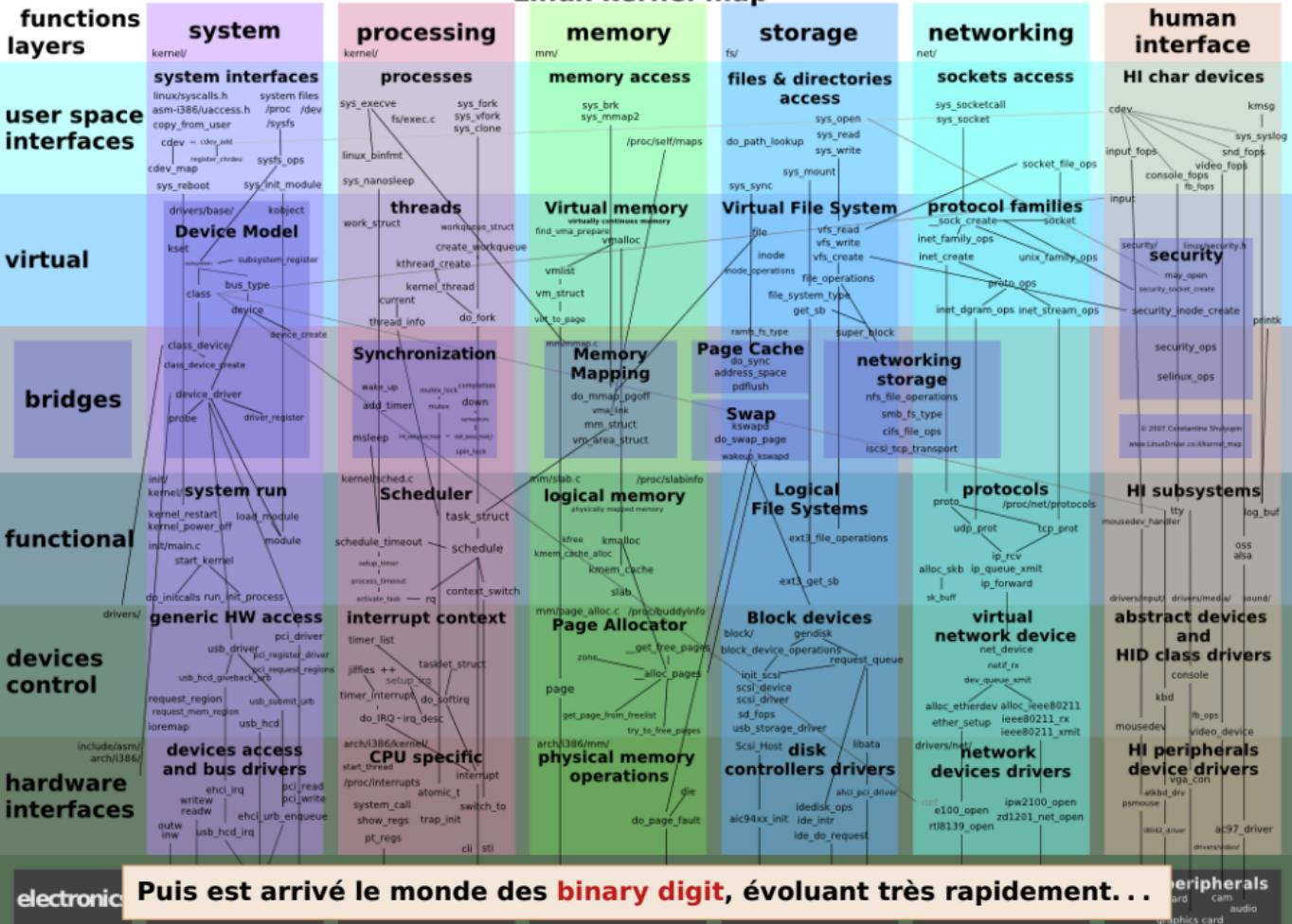
Petit Quiz final ...

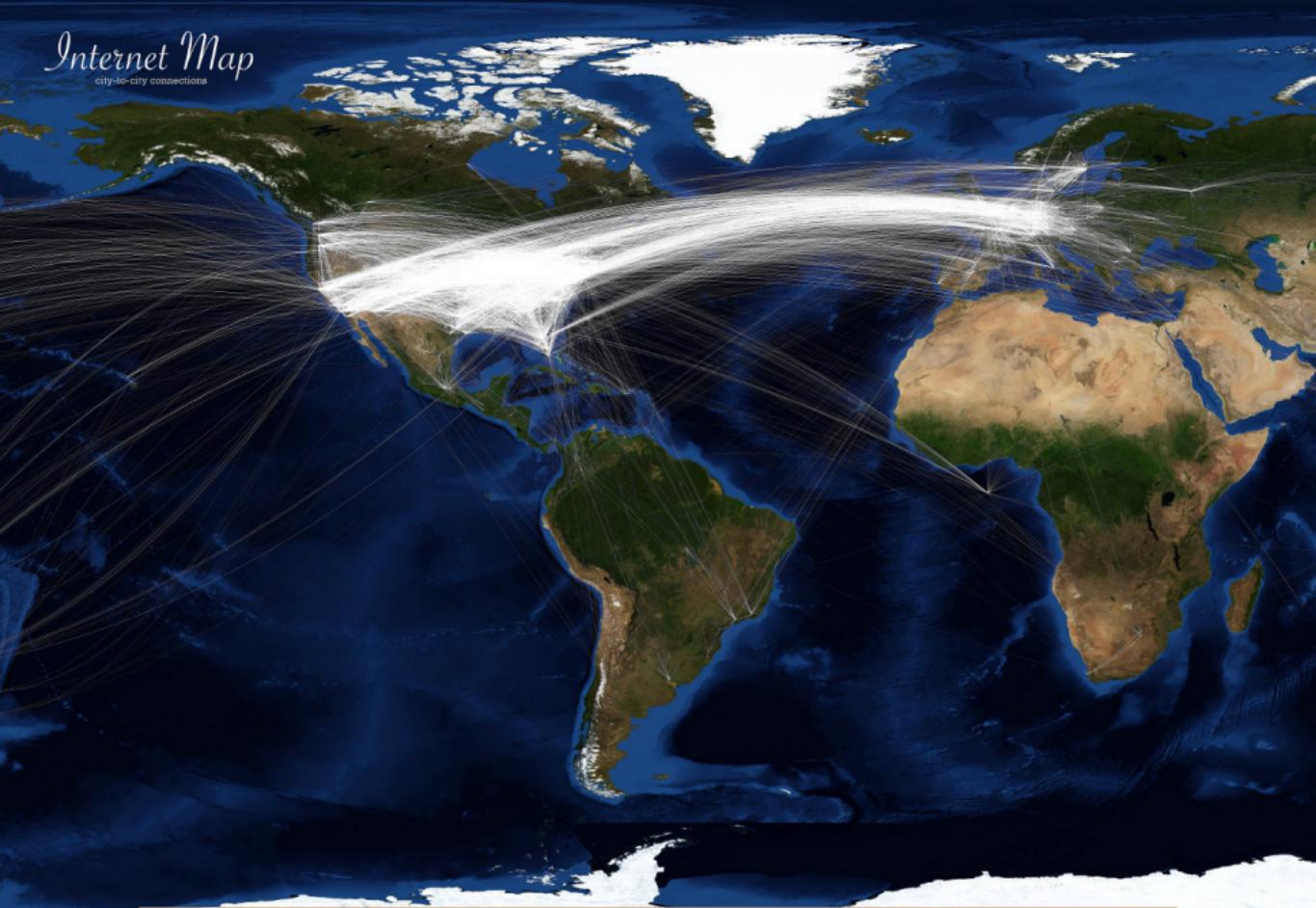




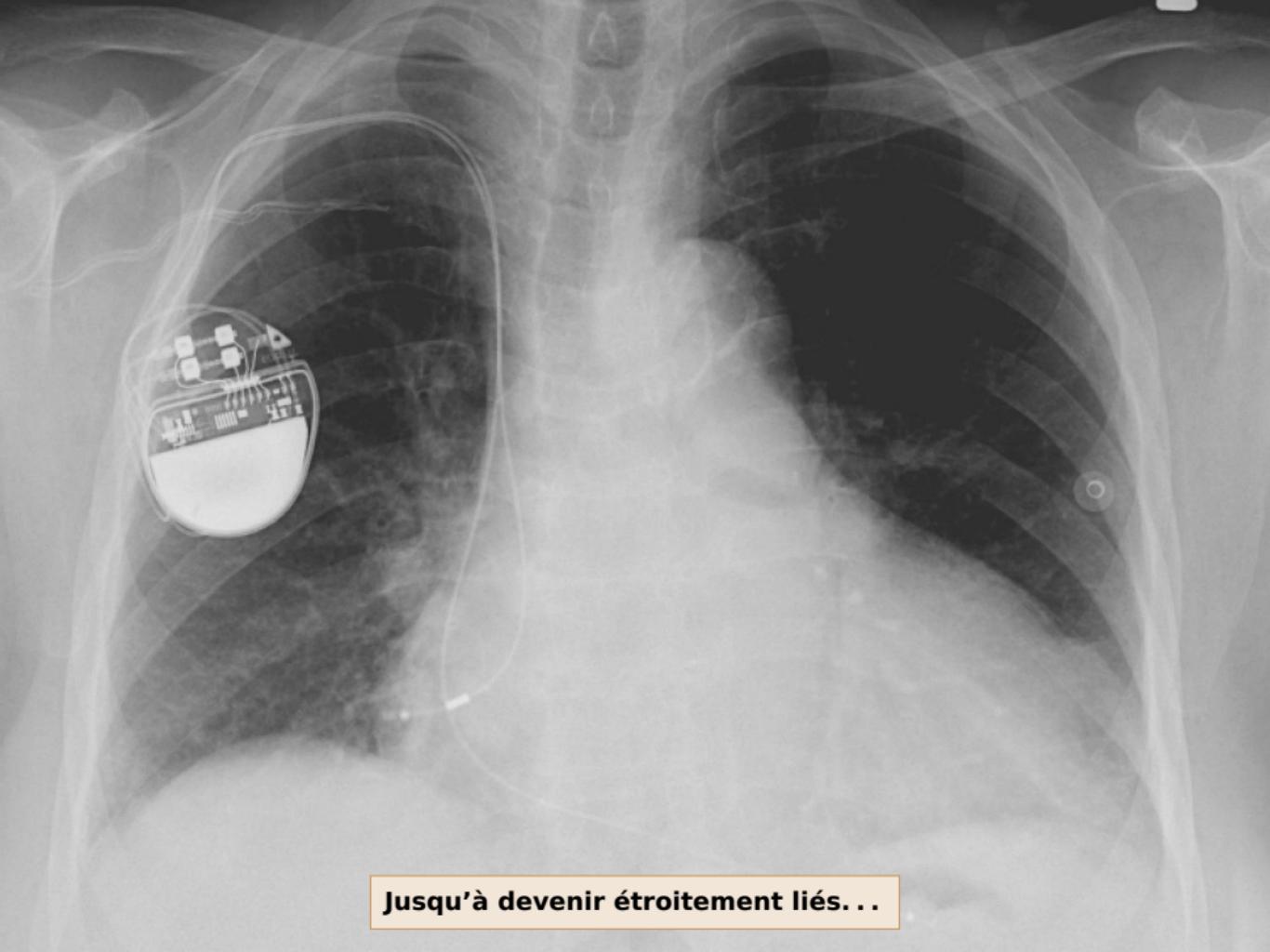
Jusqu'ici, nous avions le monde des **atomes** que nous connaissons relativement bien...

Linux kernel map





Initialement séparés, ces deux mondes se **rapprochent** peu à peu...



Jusqu'à devenir étroitement liés...

Conclusion

La **SSI** est un domaine vaste, demandant beaucoup d'**humilité**, difficile à mettre en œuvre, où la perfection n'existe pas et qui implique la participation de chacun.



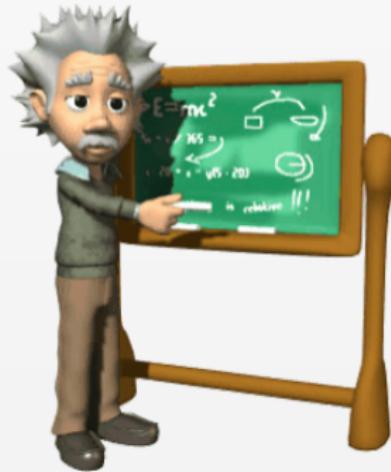
Conclusion

La sécurité doit devenir comme les freins d'une voiture :
elle doit permettre d'aller vite.

Joshua Corman – IBM ISS



Questions ?



Références

-  **Wikipedia**
http://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information
-  **Clusif**
<http://www.clusif.asso.fr/>
Le Club de la Sécurité de l'Information Français est un club professionnel dont la finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.
-  **Défense et Sécurité nationale – Le Livre Blanc**
Éditions Odile Jacob
Quelle doit être, à l'heure de la mondialisation, la politique de la France pour garantir la sécurité du pays, assurer la défense de ses intérêts dans le monde et contribuer à l'affirmation de l'Europe sur la scène internationale ?

Références

Agence nationale de la sécurité des systèmes d'information

<http://www.ssi.gouv.fr/>

Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information.

Portail de la sécurité informatique

<http://www.securite-informatique.gouv.fr/>

Ce portail d'information propose des fiches pratiques et des conseils destinés à tous les publics (particuliers, professionnels, PME). Il comporte également des actualités et avertit de menaces nouvellement rencontrées qui appellent une action rapide des utilisateurs pour en limiter les effets.

Sécurité des Systèmes d'Information

Philippe Loudenot

Philippe Loudenot, membre de l'ARCSI, est FSSI du ministère de la santé.

Références



L'art de la supercherie

Kevin Mitnick

Éditions Campus press

Dans cet ouvrage, Kevin Mitnick propose de découvrir des scénarios réalistes d'arnaques et d'escroqueries, tous basés sur l'art de la persuasion et de la manipulation.



Management de la sécurité de l'information

Alexandre Fernandez-Toro

Édition Eyrolles

Cet ouvrage apporte les éléments indispensables à la compréhension et à l'application de la norme ISO 27001.



Menaces sur le réseau

Michał Zalewski

Éditions Pearson Education France

À travers l'étude de quelques défis exceptionnels, l'auteur nous plonge dans les entrailles de l'informatique moderne. Il apporte un regard nouveau sur la SSI en détaillant les failles conceptuels que traverse un bit d'information de sa création lors d'une frappe clavier à sa transmission sur le réseau.

Licence

Copyright 2008 - 2014 – CDT Michel Dubois

Paternité



Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).

Pas d'utilisation commerciale



Vous n'avez pas le droit d'utiliser cette création à des fins commerciales sans autorisation écrite de l'auteur.

Partage des conditions initiales à l'identique



Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.