UNIVERSITÉ DE RENNES 1

La sécurité au cœur des métiers

date de la formation :
23/01/2019

lieu de la formation : Rennes

orange™

UNIVERSITÉ DE RENNES 1

#0 L’entreprise

Contexte & objectifs

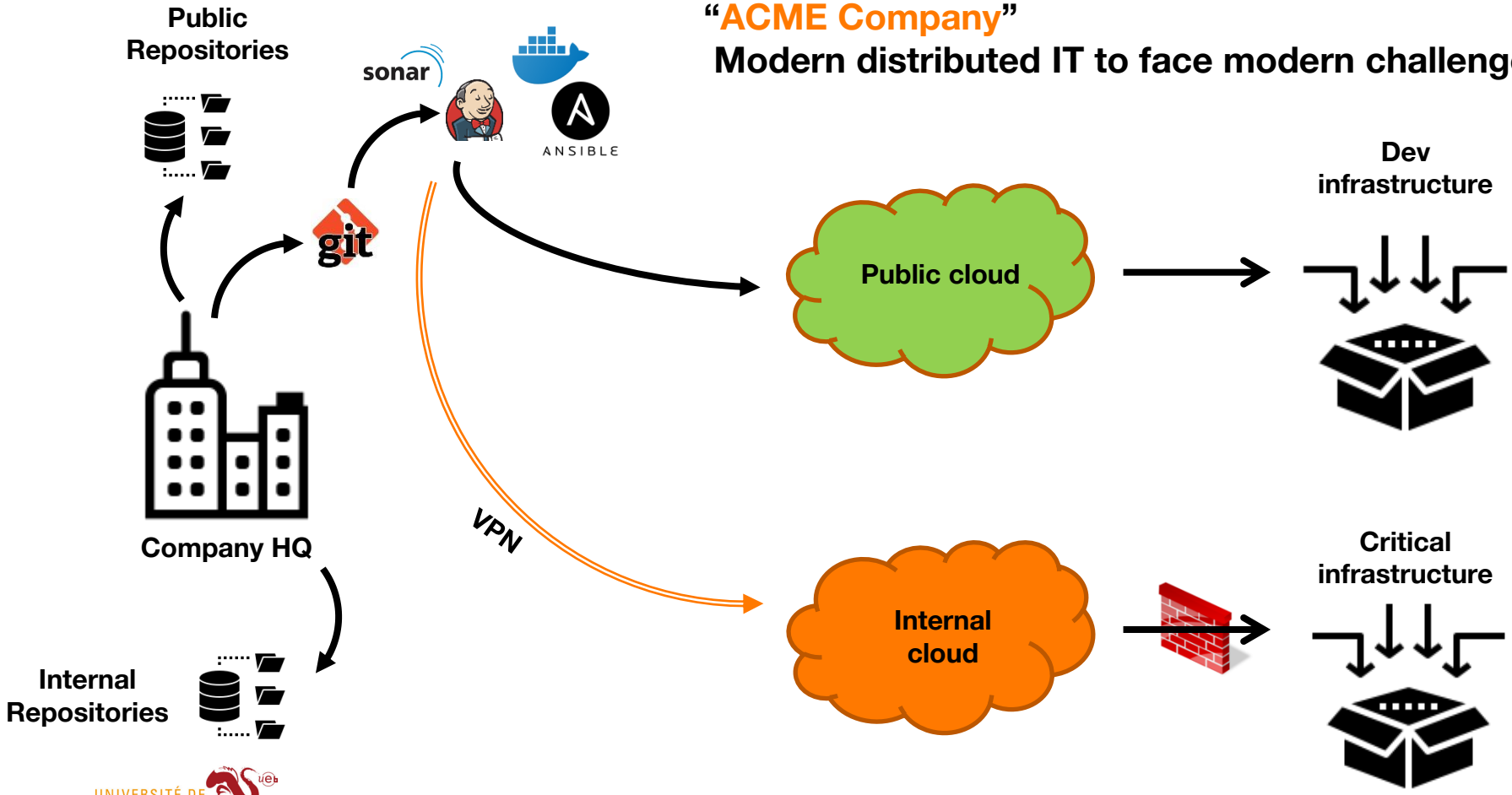
- **Utilisation d'une société fictive afin de débattre de véritables incidents de sécurité et de conséquences réelles**

  "ACME Company"
  Une vénérable entreprise du 20ème siècle,
  Produisant des biens pour tout le monde,
  Qui adopte des processus et outils « derniers cris »

- **Décrire plusieurs incidents de sécurité qui sont réellement arrivés et discuter de comment se protéger**
  - **Incidents du monde réel**
  - **Solutions de sécurité fonctionnelles et déjà prêtes**

- **Montrer comment la sécurité peut affecter tous les domaines d'une entreprise et comment des simples incidents de sécurité indépendants peuvent causer des catastrophes.**

“ACME Company”
Modern distributed IT to face modern challenges



L’équipe

Parce que les incidents de sécurité n’arrivent pas qu’aux autres,
MAIS à chacun d’entre nous !

Kevin – Developer

Jennifer - Marketing

Oscar – Bad guy

Roland – Network Admin

Brian – Security Guy

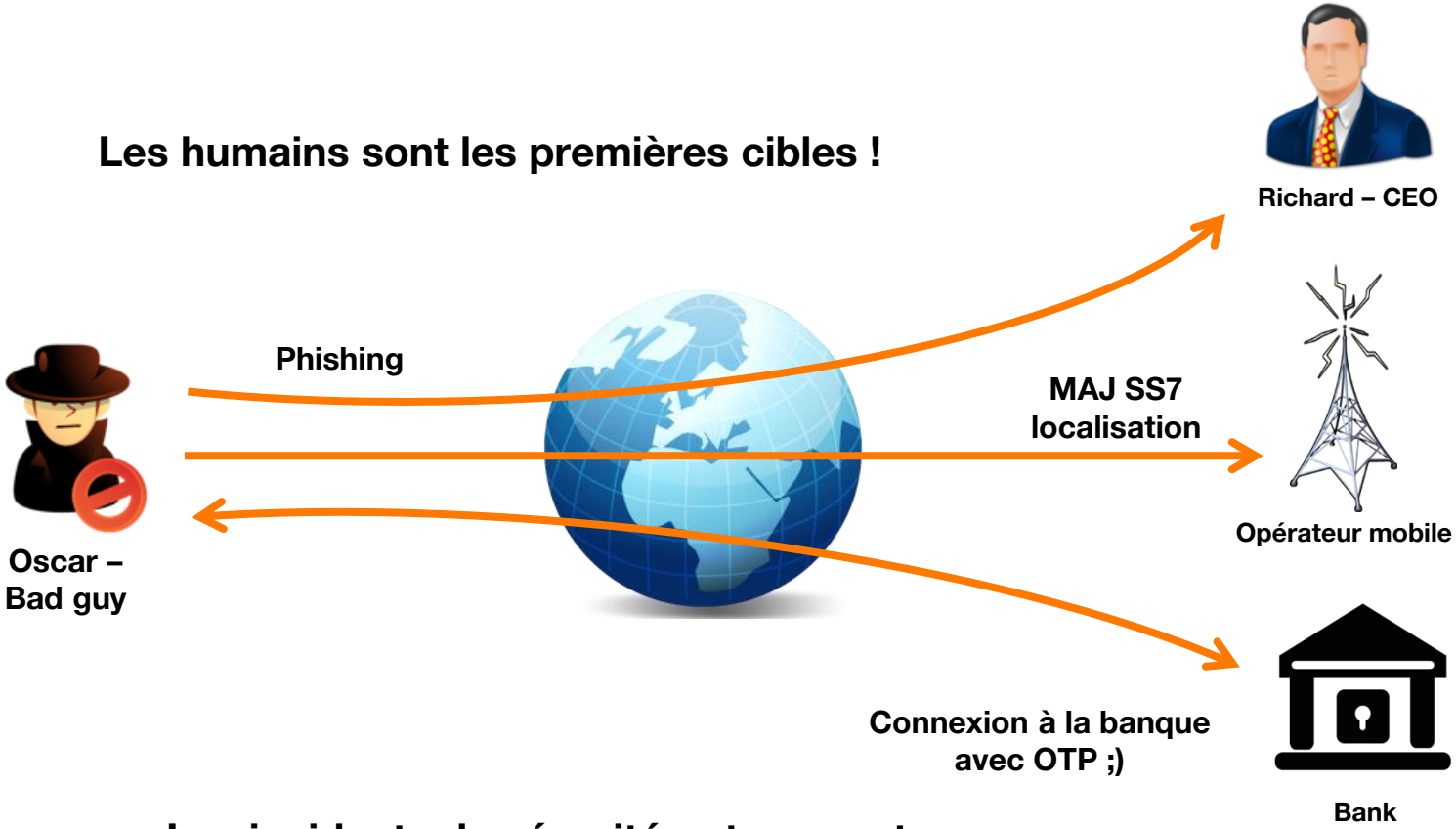
Richard – CEO

#1 SCENARIO

Vulnérabilité humaine

Vulnérabilité humaine

Les humains sont les premières cibles !



Les incidents de sécurité ont souvent des conséquences concrètes

UNIVERSITÉ DE RENNES 1

Vulnérabilité humaine

- Ne pas vérifier les certificats des sites TLS
  - Conséquence : Eavesdropping
- Ouvrir des mails d'origines inconnues
  - Conséquence : Escroquerie

- Mélanger environnements publics/privés
  - Conséquence : Fuite de données
- Shadow IT
  - Conséquence : Fuite de données

Les incidents de sécurité ont souvent des conséquences concrètes !

Do not let your passwords at sight

https://www.nouvelobs.com/tech/20150410.OBS6850/tv5-monde-laisse-trainer-ses-mots-de-passe-devant-les-cameras.html

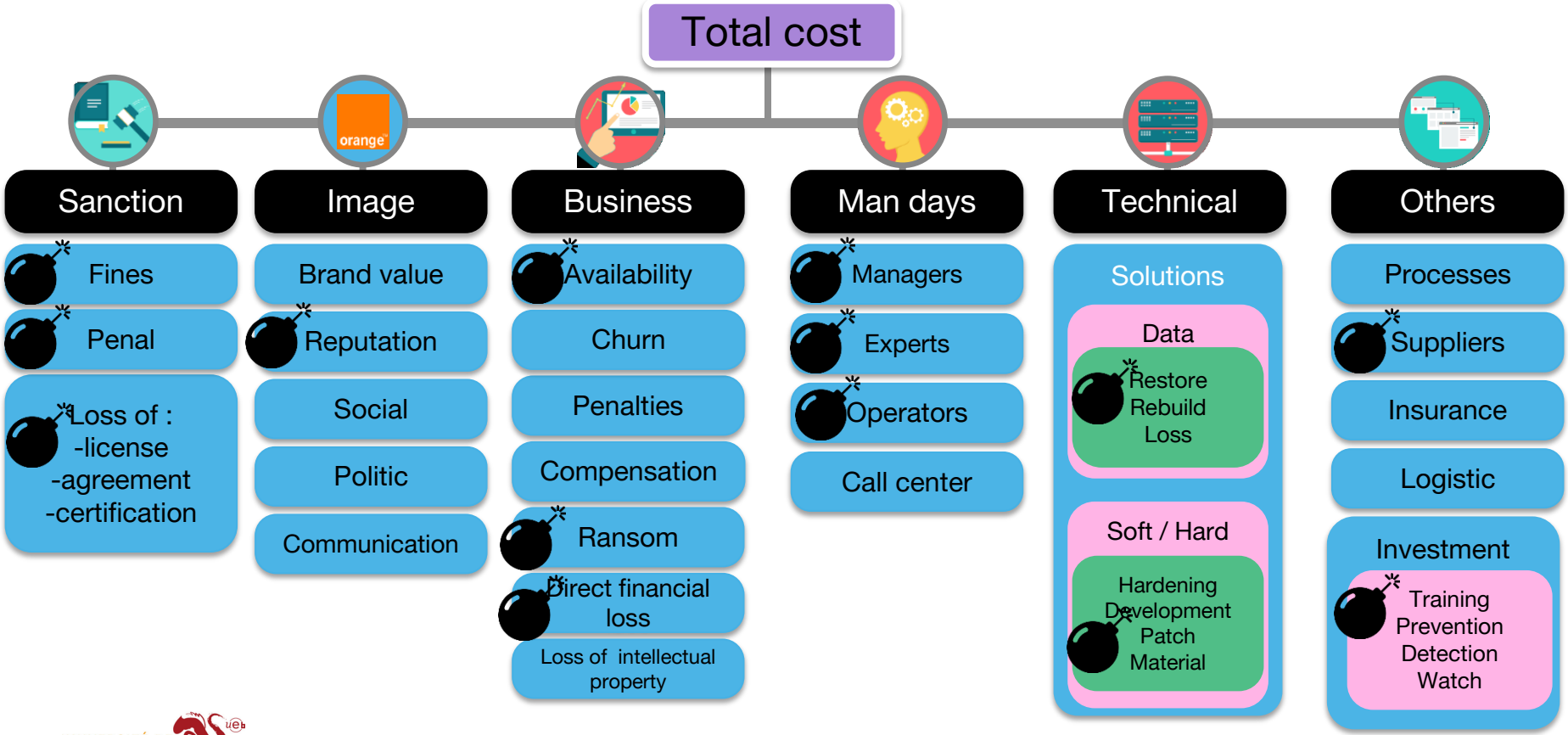
Beware when you're travelling

https://twitter.com/flzara/status/862281250315980 8

http://lavdn.lavoixdunord.fr/461997/article/2018-10-03/le-departement-du-nord-victime-d-une-arnaque-800-000-euros

UNIVERSITÉ DE RENNES 1

Vulnérabilité humaine



UNIVERSITÉ DE RENNES 1

Vulnérabilité humaine

Sensibilisation

- Politique de sécurité du SI
- Former le personnel pour avoir de bonnes pratiques : e-learning, Plazza, Red team …

Solutions MDM

- Gérer et mettre à jour les appareils
- Contrôler les logiciels

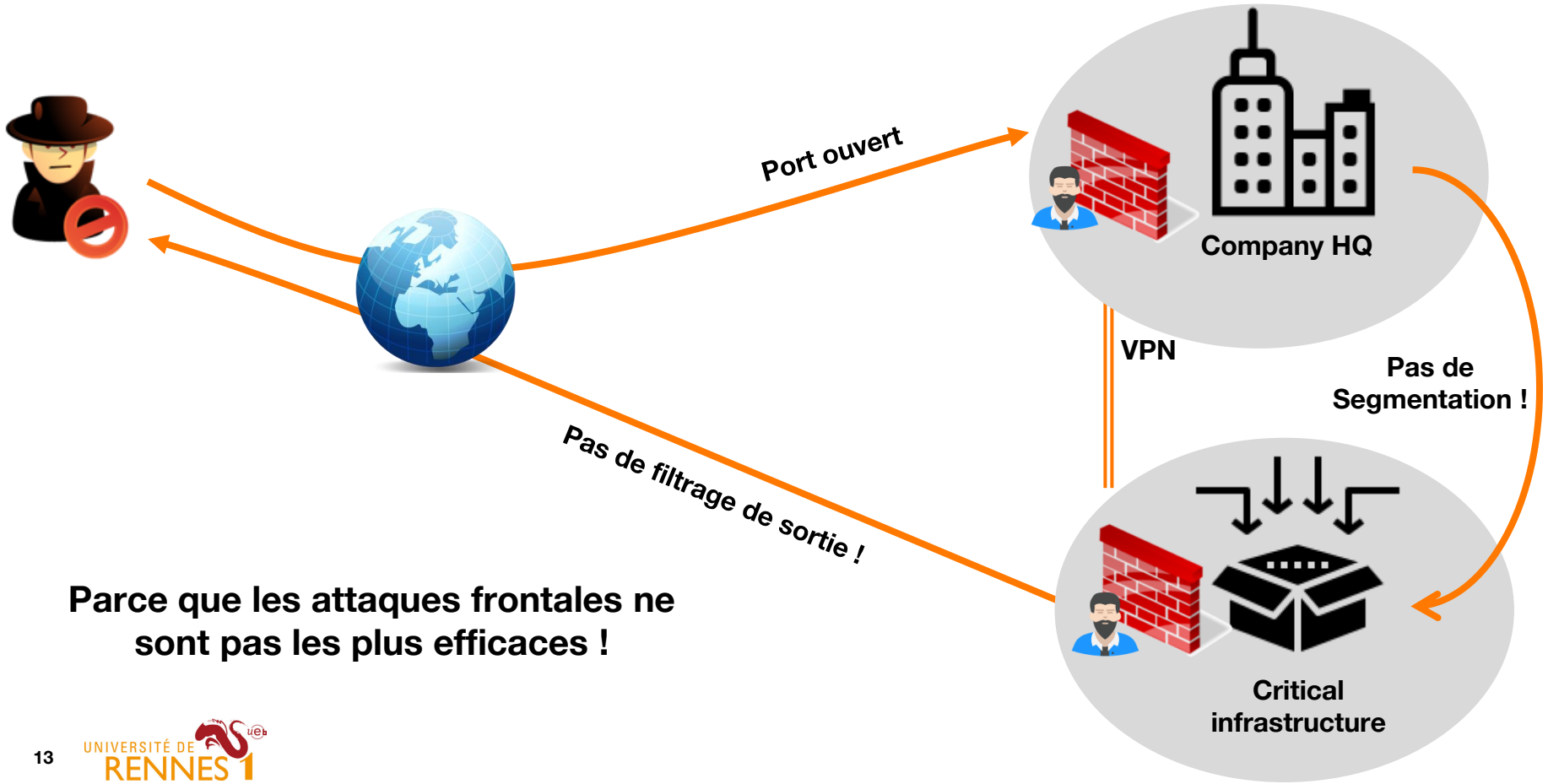
Contrôle

- Identifier et contrôler les matériels inconnus

#2 SCENARIO

Sécurité
Des réseaux

Sécurité des réseaux



Parce que les attaques frontales ne sont pas les plus efficaces !

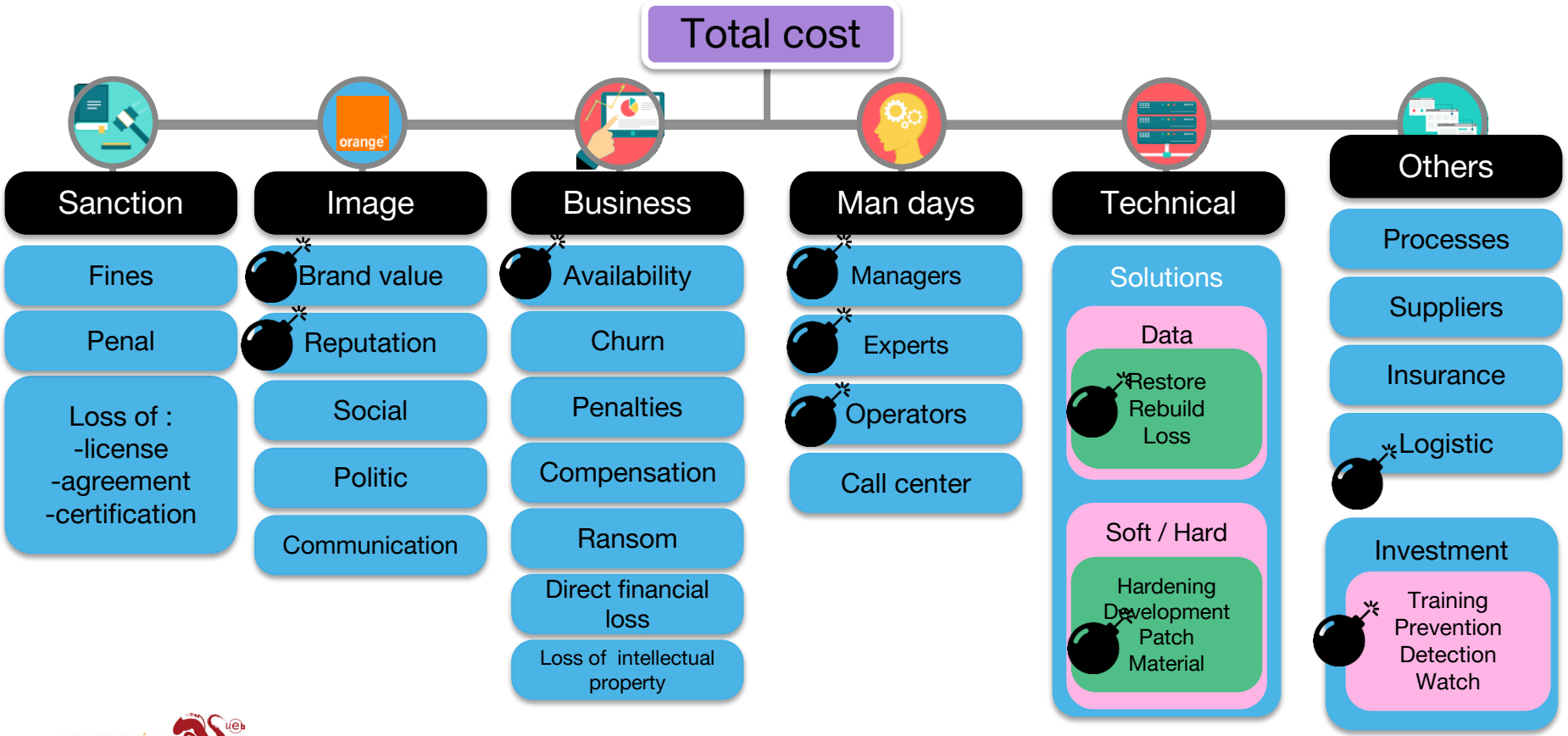
Sécurité des réseaux

- **Le manque de segmentation réseau** entraine une prolifération facile des malware au travers du LAN
  - exemple: WannaCry

- **Des ports ouverts par inadvertance** peuvent rendre votre système accessible depuis Internet
  - exemple: #shodansafari sur Twitter

- **Le manque de filtrage sortant** facilite l'exfiltration des données et peut amener un attaquant à prendre le contrôle de votre système
  - exemple: Botnets

Sécurité des réseaux



Sécurité des réseaux

- Mettre en œuvre des revues fréquentes
  - Peuvent être automatisées

- Contrôle organisationnel des changements de configuration
  - Pas une seule en charge de la gestion !
  - Procédures documentées
  - Rien n'est fait sans validation

- Pentests proactifs et post-mortem
  - Peuvent être faits par des personnes internes ou externes

#3 SCENARIO

Sécurité
Des développements

Sécurité des développements

Ransomware As A Service

Europol fournit la clé gratuitement

Impact Business

Développeurs: Hacker group GandCrab

Produit vendu aux clients:

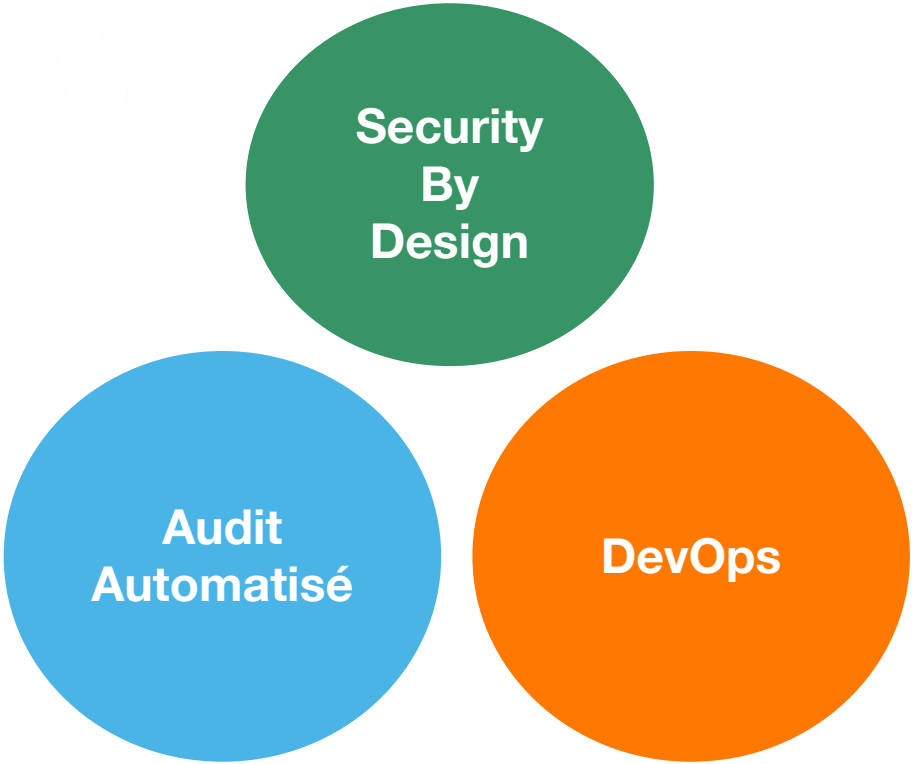
- **Un ransomware sur mesure qui permet au clients de récuperer une ransom auprès de victimes**

Logiciel non sécurisé

UNIVERSITÉ DE RENNES 1

Sécurité des développements

Comment prévenir ?



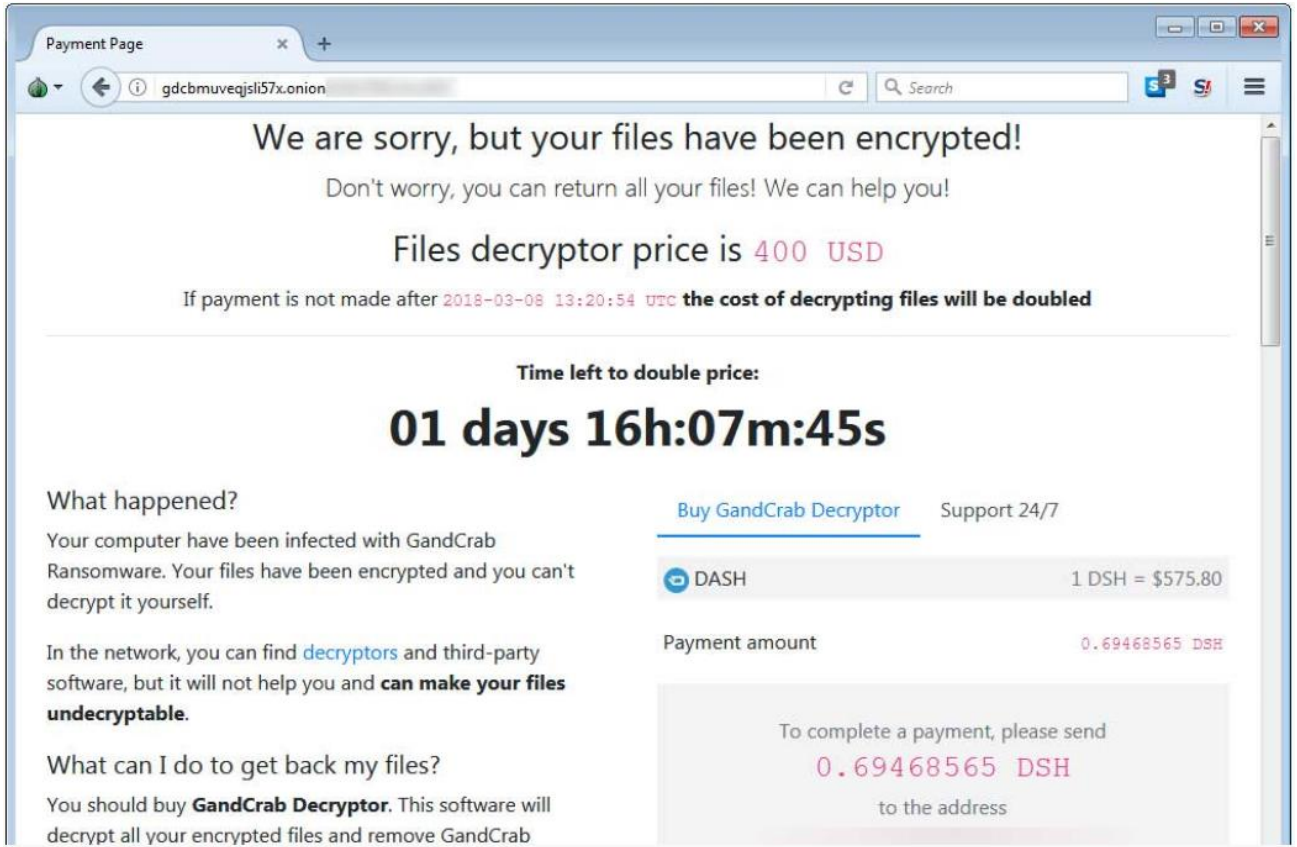
Les hackers ont sécurisés leur code

- **Chiffrement des fichiers**
- **Random Mode / Polymorphing**
- **Clé AES 256 bits**
- **Chiffrement de la clé : 2048 bits RSA**

+

- **Nouvelles fonctionnalités pour le plaisir des clients :**
  - **Chat avec les hackers**
  - **Taille du Ransomware : 5Mo ⇨ 69 ko**

UNIVERSITÉ DE RENNES 1



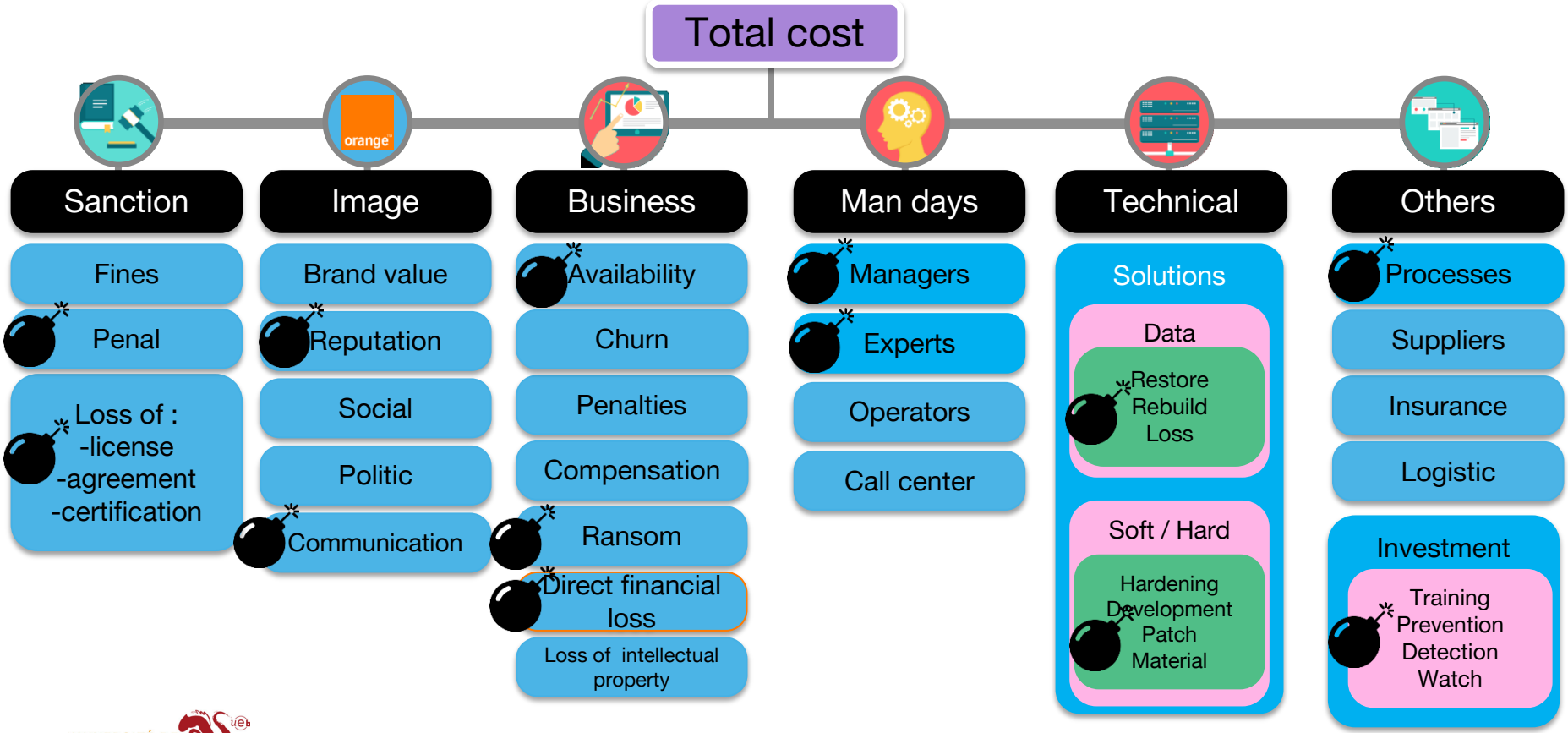
On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

The alternative way to contact us is to use Tox messenger.

Read how to:
1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.

DANGEROUS!
Do not try to modify files or use your own private key - this will result in the loss of your data forever

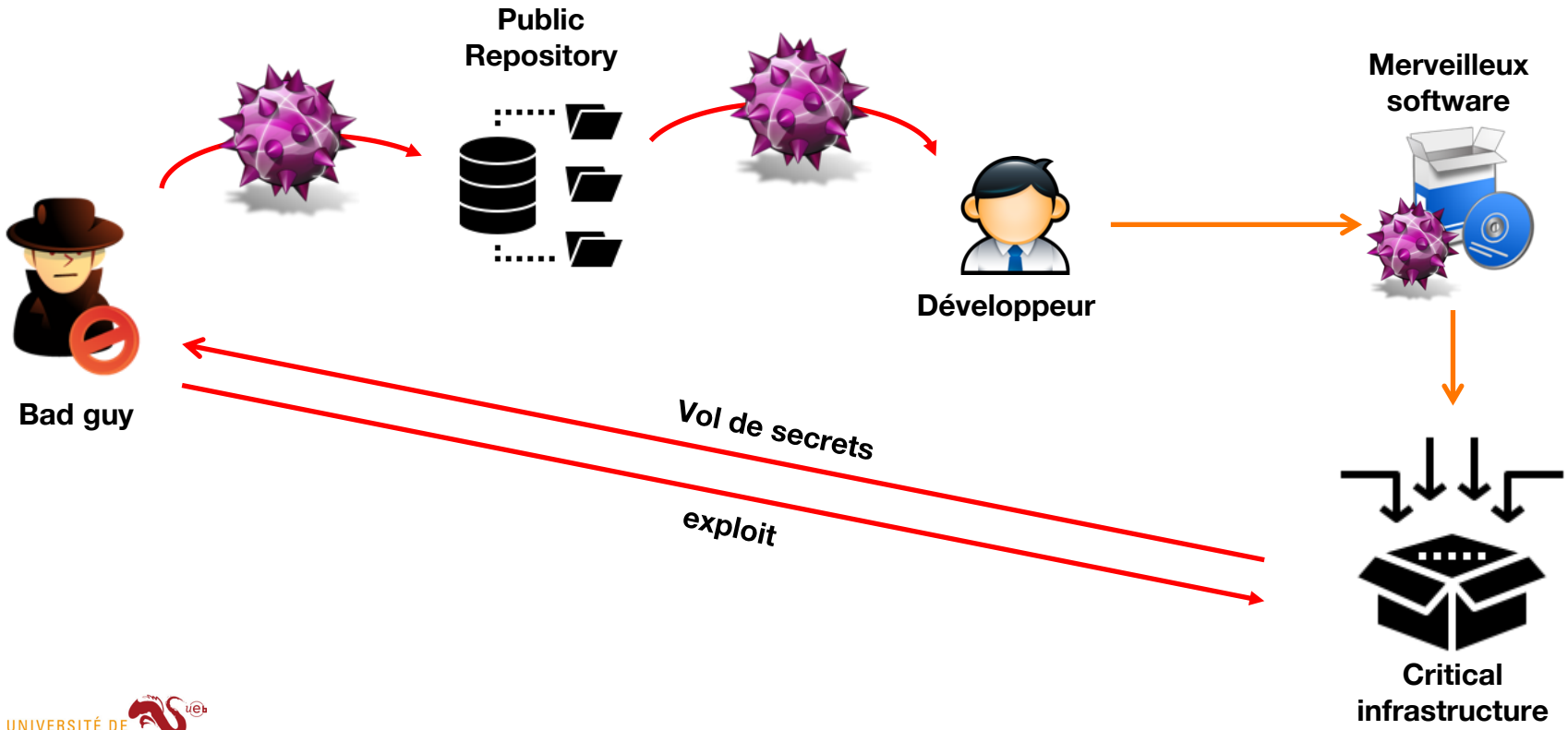
Sécurité des développements



#4 SCENARIO

Sécurité
Des développements

Sécurité des développements



https://linuxfr.org/news/d%C3%A9couverte-dune-faille-de-s%C3%A9curit%C3%A9-critique-dans-openssl-de-deb

Découverte d'une faille de sécurité critique dans OpenSSL de Debian

Posté par **Amaury** le 15/05/08 à 15:00. Modéré par **Bruno Michel**.
Tags : **sécurité**

Le 13 mai, un message publié sur la liste de sécurité Debian identifiait une anomalie impactant le paquet openssl. Ce *bug* a été introduit par un mainteneur Debian, qui a eu la main lourde en voulant "*corriger*" des alertes remontées par Valgrind [W] (un logiciel qui audite le code). Résultat des courses : le générateur de nombres aléatoires, composant critique de nombreux systèmes de chiffrements, n'est au final pas si aléatoire que ça, voire carrément prévisible.

En conséquence, tous les certificats et clefs SSL [W]/SSH [W] générés sur une Debian (ou dérivée) depuis 2006 l'ont été à partir d'un univers des possibles très restreint (environ 250 000 clefs, à confirmer) et présentent donc un niveau de sécurité largement inférieur à celui estimé.

Home » Security Boulevard (Original) » News » Gentoo Repository Compromised Due to Weak Admin Password

Gentoo Repository Compromised Due to Weak Admin Password

by Lucian Constantin on July 5, 2018

The Gentoo Linux pro[illegible]shed investigating the hacking last week of its GitHub-hosted package repository, an incident that resulted in attack[illegible]ting malicious code to users. The point of entry turned out to be a weak admin password that was probably guesse[illegible]data stolen from another website.

On June 28, unknown individuals gained control over the Gentoo Organization on GitHub and locked out other administrators.

https://securityboulevard.com/2018/07/gentoo-repository-compromised-due-to-weak-admin-password/

https://www.theregister.co.uk/2018/07/12/npm_eslint/

Security

Now Pushing Malware: NPM package dev logins slurped by hacked tool popular with coders

Tokens killed after eslint-scope utility compromised

By Shaun Nichols in San Francisco 12 Jul 2018 at 20:13 9 SHARE ▼

Updated An unfortunate chain reaction was averted today after miscreants tampered with a widely used JavaScript programming tool to steal other developers' NPM login tokens.

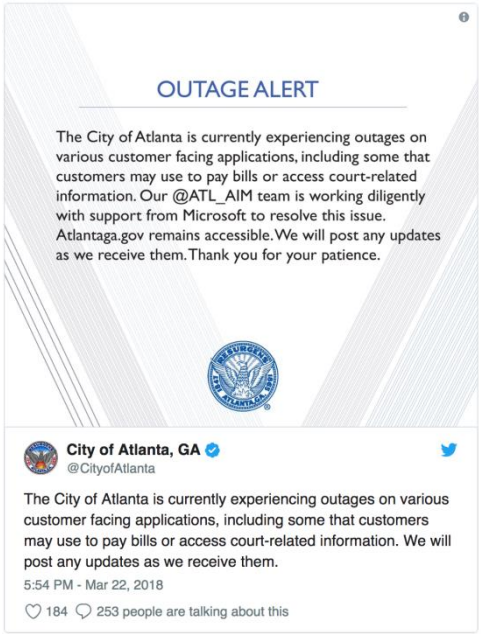
The open-source utility eslint-scope was altered by hackers so that, when used to analyze source code, it would copy the contents of the user's `~/.npmrc` file to an outside server via HTTPS – that file would include the victim's NPMjs.org login token.

Les incidents de sécurité ont souvent des conséquences concrètes !

Voler une Tesla avec seulement une tablette

https://www.20minutes.fr/arts-stars/web/2360235-20181024-video-piratent-volent-tesla-aide-tablette

Smartcities: Augmentation future des pannes



https://www.checkmarx.com/2017/12/11/smart-cities-can-city-hacked/

UNIVERSITÉ DE RENNES 1

Les incidents de sécurité ont souvent des conséquences concrètes !

The cybersecurity risk of self-driving cars

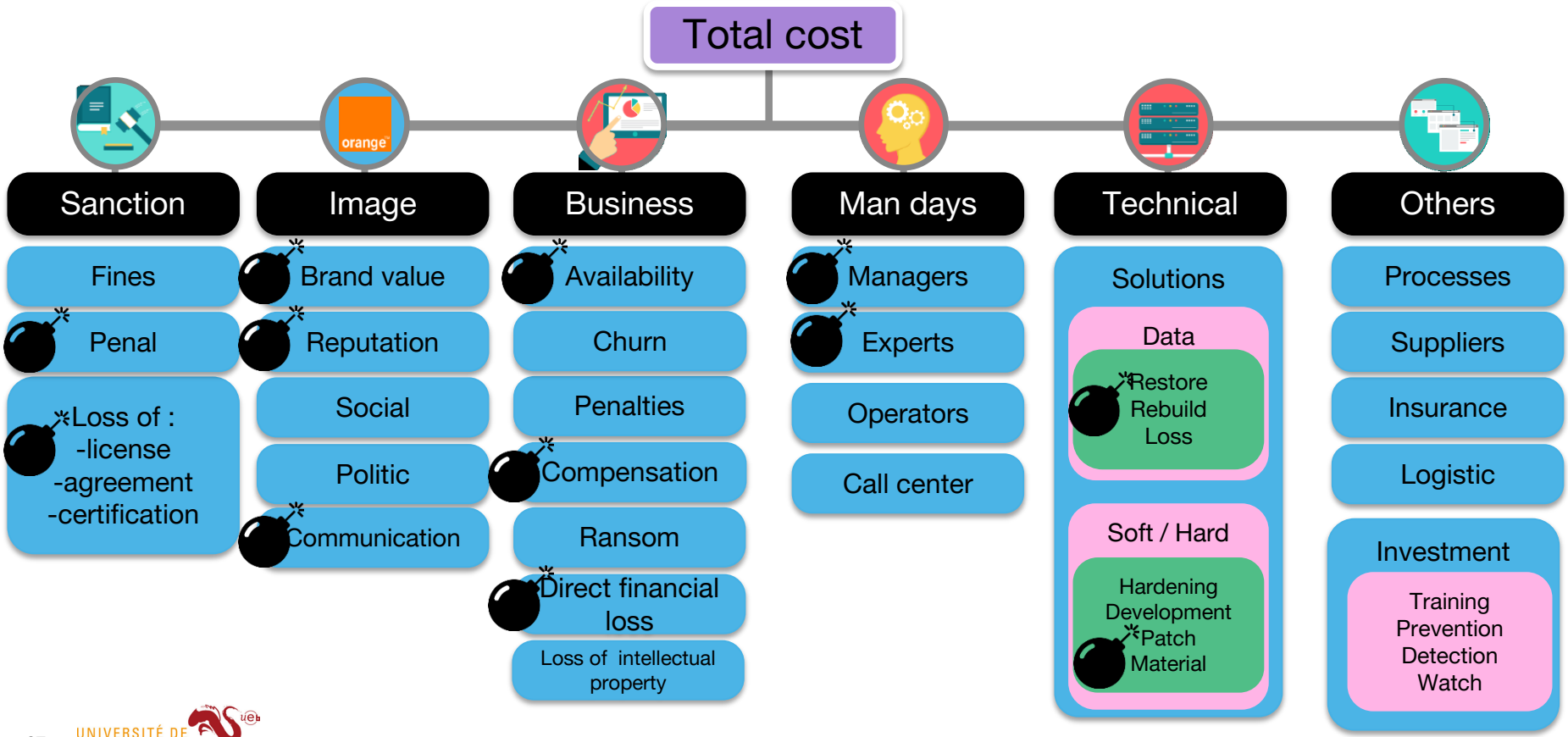
https://phys.org/news/2017-02-cybersecurity-self-driving-cars.html

Data Sabotage: The Serious Security Risk of Smart Cities

https://securityintelligence.com/data-sabotage-the-serious-security-risk-of-smart-cities/

UNIVERSITÉ DE RENNES 1

Sécurité des développements



UNIVERSITÉ DE RENNES 1

Remédiation

- Ne récupérer des logiciels que de lieux de confiance (i.e. repos internes)

- Utiliser des outils pour tester son code et ses dépendances (SAST / DAST)

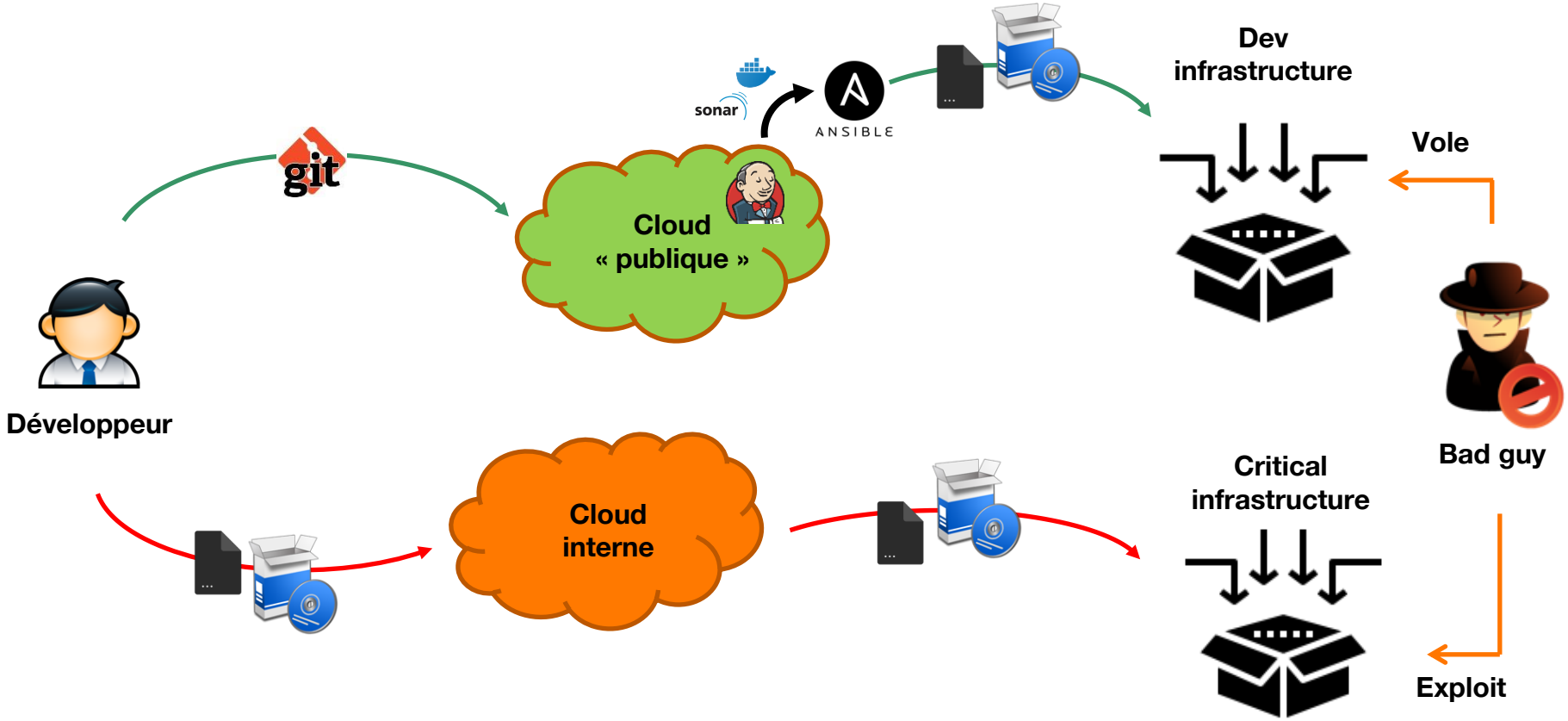
- Ne pas installer de logiciel inconnu

- Utiliser de l’open-source est sûr… seulement si le code est revu

#5 SCENARIO

Sécurité
Des développements

Sécurité des développements



http://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/

AWS Cloud Hacked by Bitcoin Miners

October 9, 2017 by George Leopold

Bitcoin mining is among the lates
to public cloud security as hacke
enterprise computing resources t
the digital currency.

Cloud security vendor RedLock r
earlier this month that hackers w
Amazon Web Services (NASDAC
cloud computing resources to mi
bitcoins. The process involves co
transactions made during a set p
a list, called a block. Bitcoin mine
those transactions, and write the
general ledger. They are then pa

currency.

Tesla Hackers Hijacked Amazon Cloud Account to Mine Cryptocurrency

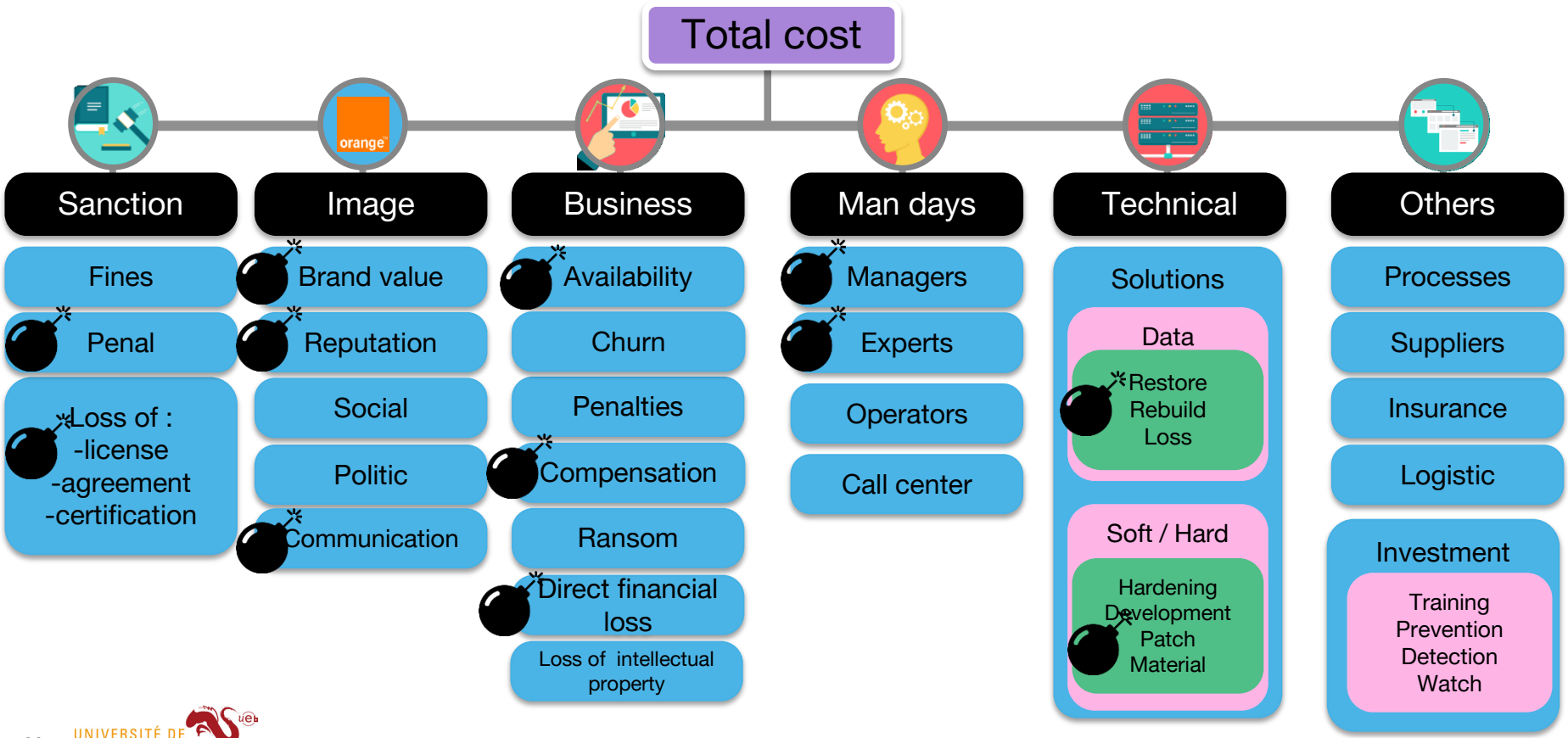
By ROBERT HACKETT Updated: February 20, 2018 2:14 AM ET

An unidentified hacker or hackers broke into a Tesla-owned Amazon cloud account and used it to "mine" cryptocurrency, security researchers said. The breach also exposed proprietary data for the electric carmaker.

https://www.enterprisetech.com/2017/10/09/aws-cloud-hacked-bitcoin-miners/

UNIVERSITÉ DE RENNES 1

Sécurité des développements



Remédiation

- **Ne pas utiliser les mêmes identifiants sur les infrastructures de DEV et PROD**

- **Ne pas utiliser les mêmes données sur les plateformes de DEV et PROD**

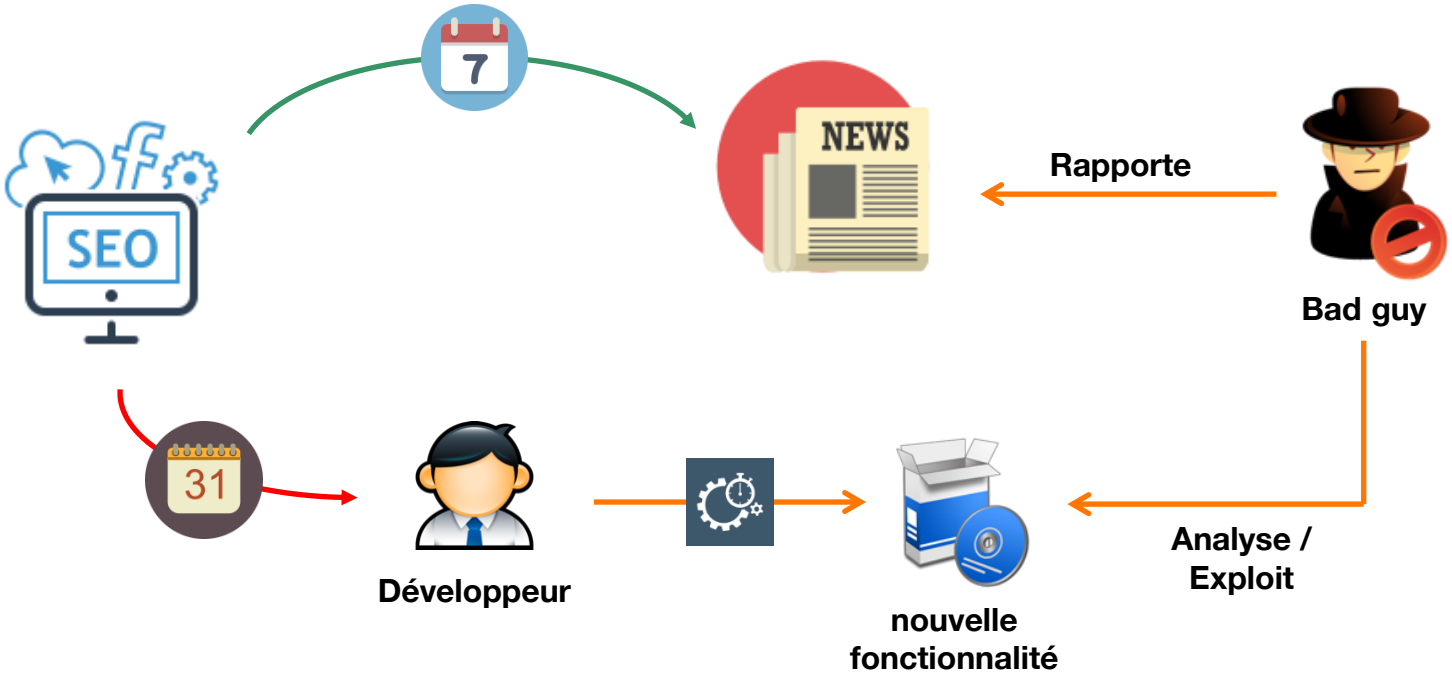
- **Cloisonner fortement les environnements de qualification et de production**

- **Utiliser des techniques d'anonymisation sur les données de développement**

#6 SCENARIO

Sécurité
De la communication

Sécurité de la communication



https://www.forbes.com/sites/jasonevangelho/2018/10/23/sorry-windows-10-has-yet-another-file-deleting-bug-that-microsoft-missed/#d09ab746d8e3

Sorry, Windows 10 Has Yet Another File-Deleting Bug That Microsoft Missed

Jason Evangelho Contributor ⓘ
Games
I cover the fascinating worlds of Linux, PC gaming & consumer hardware

Apparently I'm not done beating this dead horse yet. That's because yet another file-deleting bug has surfaced in Microsoft's Windows 10 Build 1809 update. The same update Microsoft pulled from public circulation because it was wiping entire user folders from existence. The new bug centers around Microsoft's Unzip application, and seems to present itself in two distinct forms.

GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS

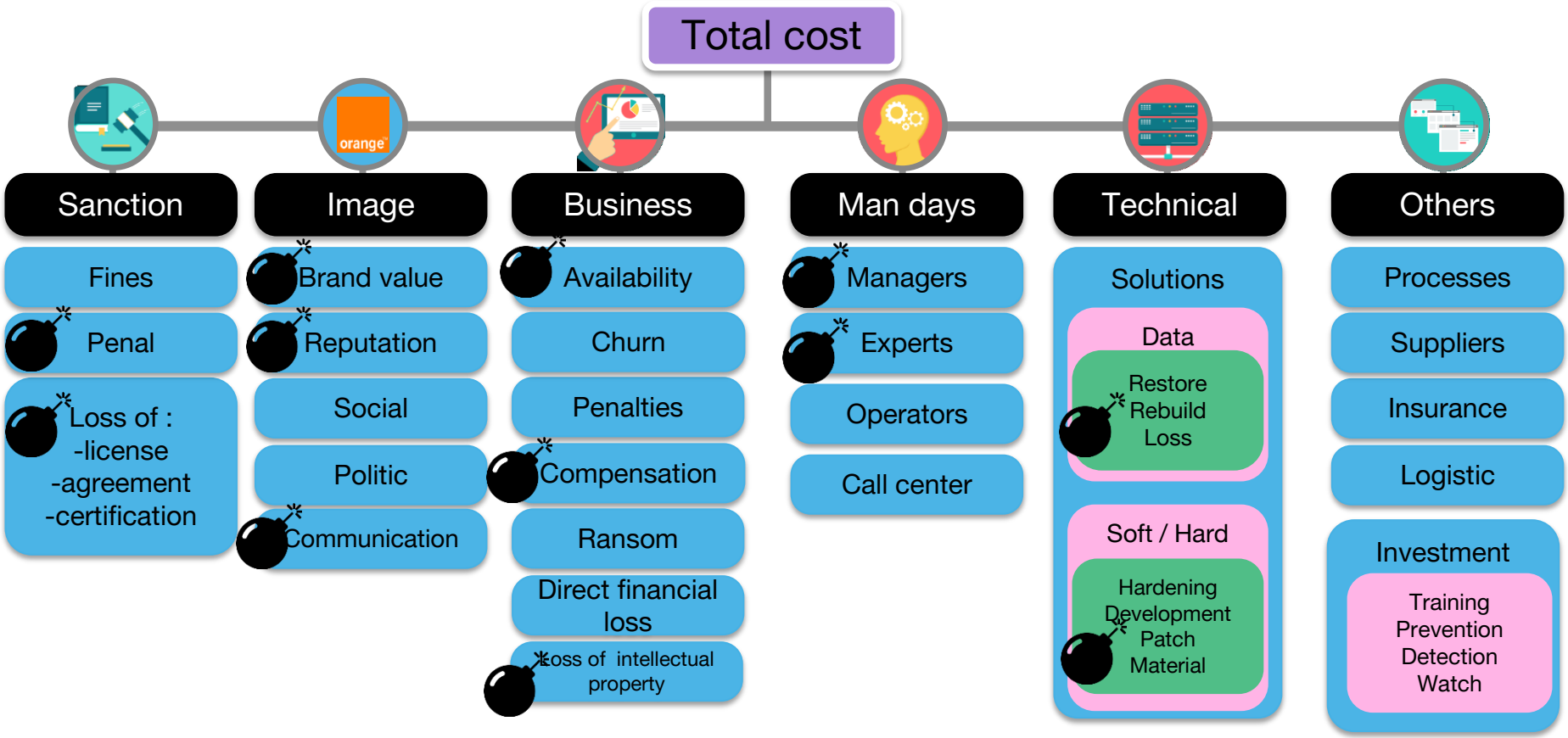
DANIEL ACKER/BLOOMBERG/GETTY IMAGES

WHEN A PAIR of security researchers showed they could hack a Jeep over the Internet earlier this summer to hijack its brakes and transmission, the impact was swift and

https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

UNIVERSITÉ DE RENNES 1

Sécurité de la communication



UNIVERSITÉ DE RENNES 1

Remédiation

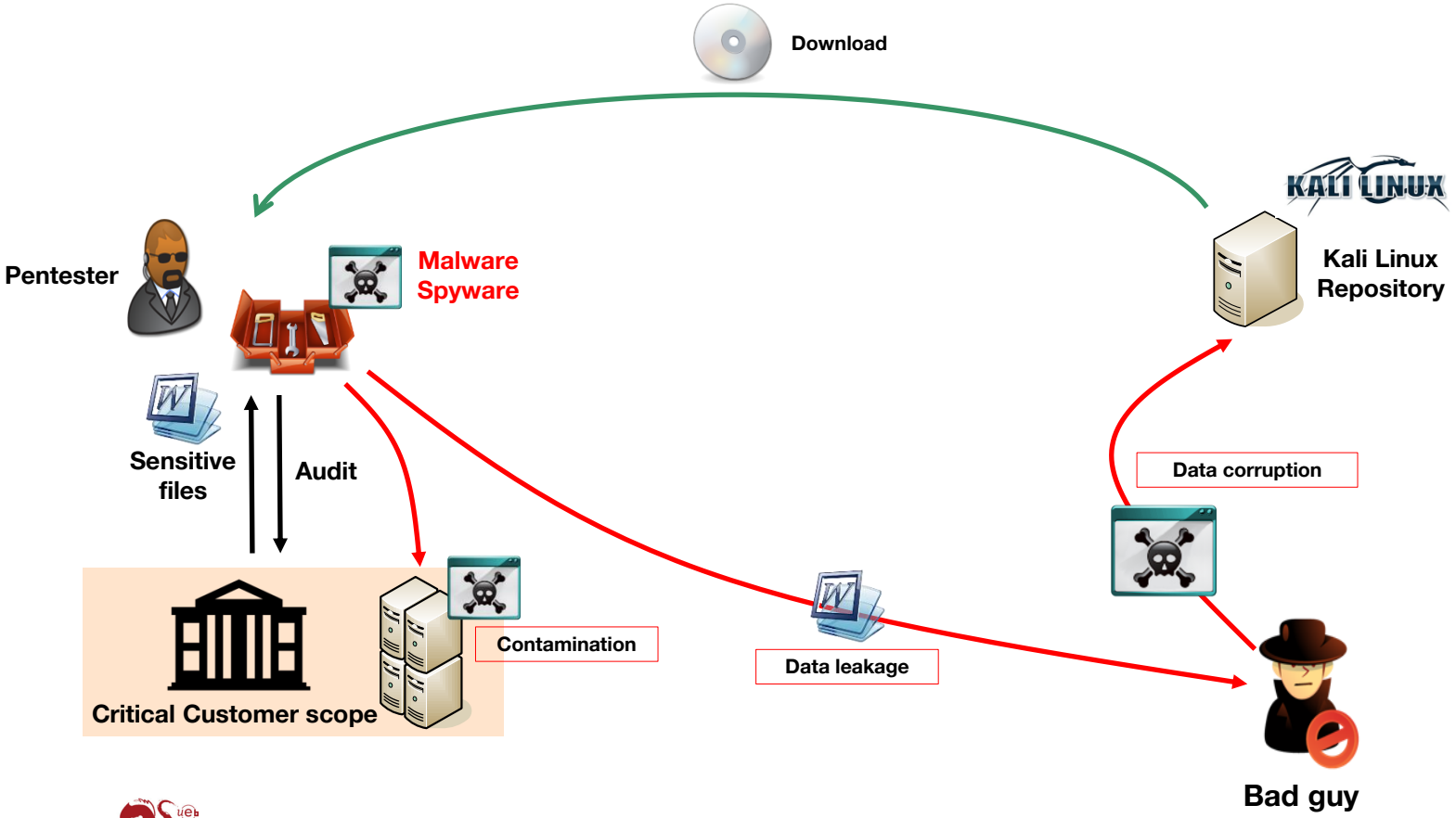
- **Communication bidirectionnelle entre marketing et build**

- **Toujours inclure les tests fonctionnels et de sécurité dans les deadlines**

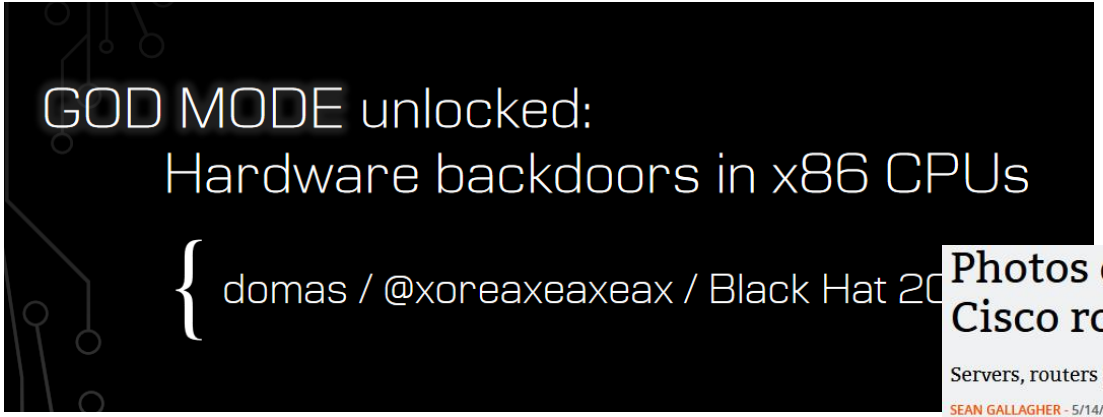
#7 SCENARIO

Sécurité
De la confiance

Sécurité de la confiance



Les incidents de sécurité ont souvent des conséquences concrètes !



https://www.blackhat.com/us-18/briefings.html#god-mode-unlocked-hardware-backdoors-in-x86-cpus

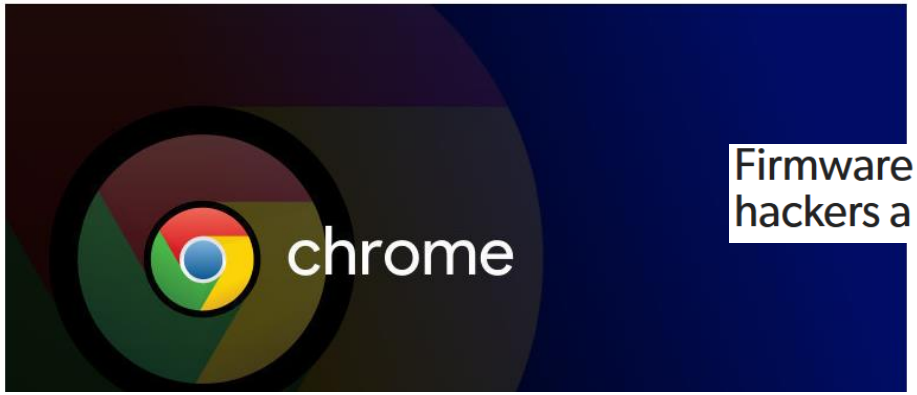
https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

UNIVERSITÉ DE RENNES 1

Les incidents de sécurité ont souvent des conséquences concrètes !

Rogue extensions that hijack Chrome & Firefox are near impossible to remove

By Muhammad Jarir Kanji · Jan 20, 2018 08:12 EST · HOT! 36



https://www.neowin.net/news/rogue-extensions-that-hijack-chrome--firefox-are-near-impossible-to-remove/

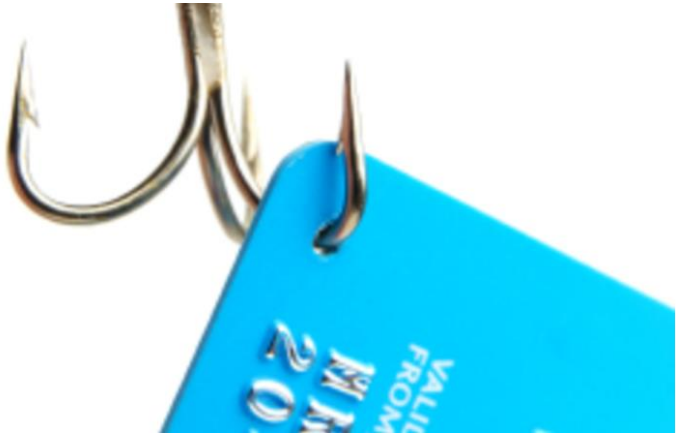
Firmware bug in CCTV software may have given POS hackers a foothold

https://www.pcworld.com/article/3048073/firmware-bug-in-cctv-software-may-have-given-pos-hackers-a-foothold.html

UNIVERSITÉ DE RENNES 1

Les incidents de sécurité ont souvent des conséquences concrètes !

Fake banking websites issued with SSL certificates by Symantec, Comodo and GoDaddy

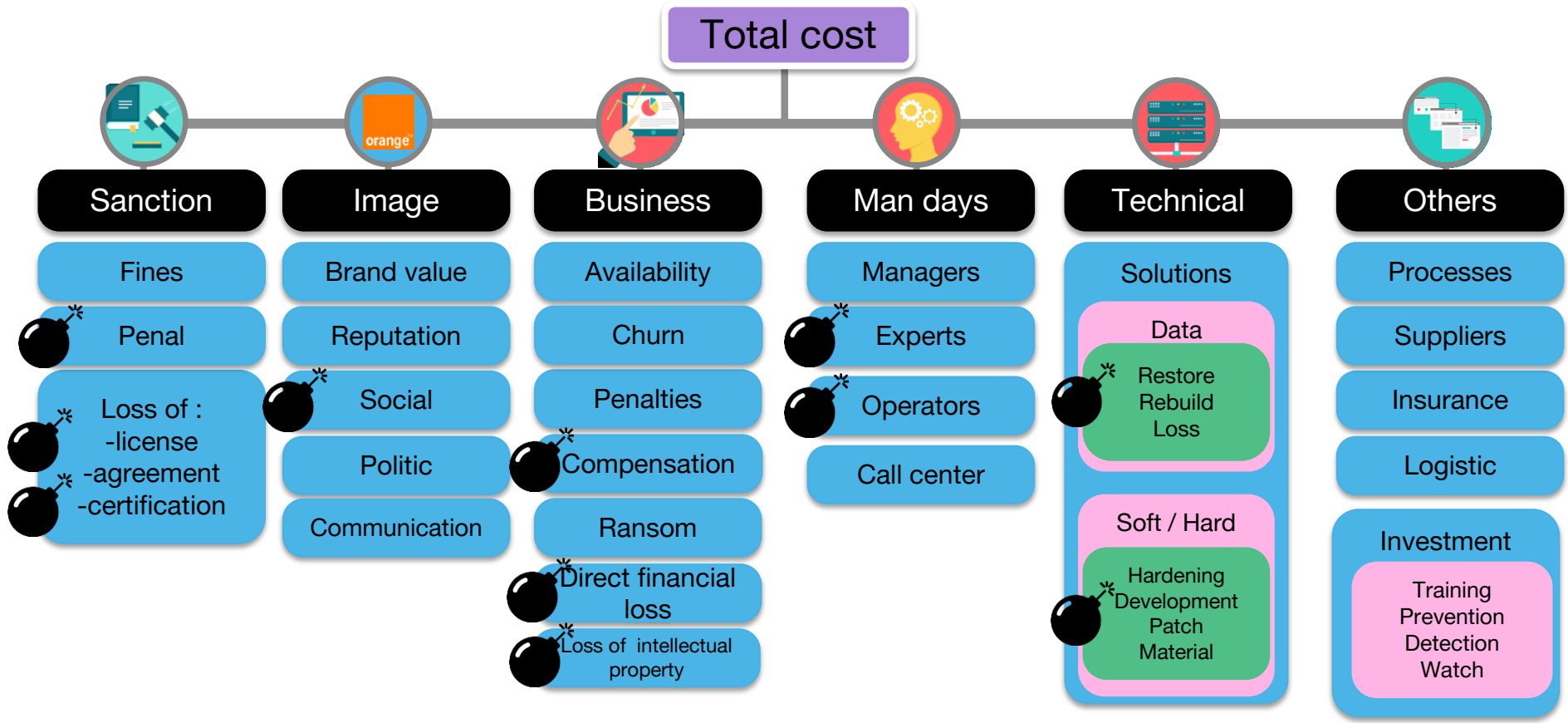


https://www.computing.co.uk/ctg/news/2430138/fake-banking-websites-issued-with-ssl-certificates-by-symantex-comodo-and-godaddy

Linux distro hacked on GitHub, “all code considered compromised”

https://nakedsecurity.sophos.com/2018/06/29/linux-distro-hacked-on-github-all-code-considered-compromised/

Sécurité de la confiance



UNIVERSITÉ DE RENNES 1

Remédiation

- Ne récupérer des logiciels que de lieux de confiance (i.e. repos internes)

- Ne pas installer de logiciel inconnu (ou obtenu illégalement)

- Ne pas essayer de contourner les outils et/ou contrôles de sécurité

- Utiliser de l’open-source est sûr… seulement si le code est revu

- Utiliser de l’open-source est sûr… seulement si le code est revu

Conclusion

- Tout le monde peut causer des problèmes de sécurité
- Les hackers ciblent tout et tout le monde
- Des petites failles de sécurité peuvent causer des catastrophes majeures
- Il existe des outils et formations pour éviter/réagir
- La sécurité n'est pas qu'un problème technologique – votre attitude fait la différence
- Tout le monde doit contribuer pour améliorer la résistance aux failles
- "Security is a process, not a product" - Bruce Schneier

Un effort de sécurité continu est requis…
au travers du cycle de vie des projets.

Merci