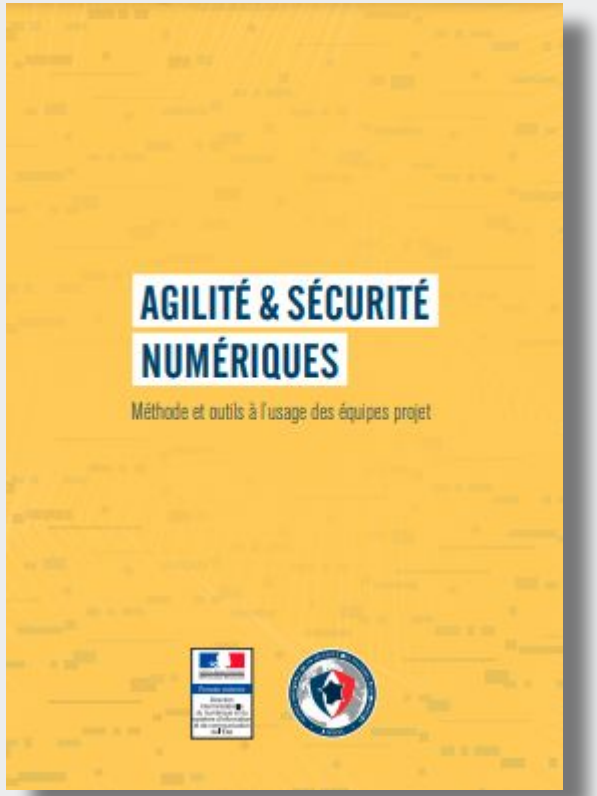
GOUVERNEMENT
Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Atelier d'Analyse de Risques de sécurité informatique en mode Agile



Novembre 2023

Quel est le contenu de ce support ?

- *Objectifs de l'atelier d'analyse de risques*
- *Présentation de la méthode*
- *Prérequis*
- *Présentation différentes étapes*
- *Détails des étapes une à une*
- *Exemple*
- *Homologation*
- *Ressources*

Les objectifs de l'atelier d'analyse de risques de sécurité

1. Sensibiliser l'équipe aux risques de sécurité du produit

pour construire services publics numériques protégeant les données des utilisateurs

2. Avoir un endroit unique regroupant l'ensemble des risques de sécurité

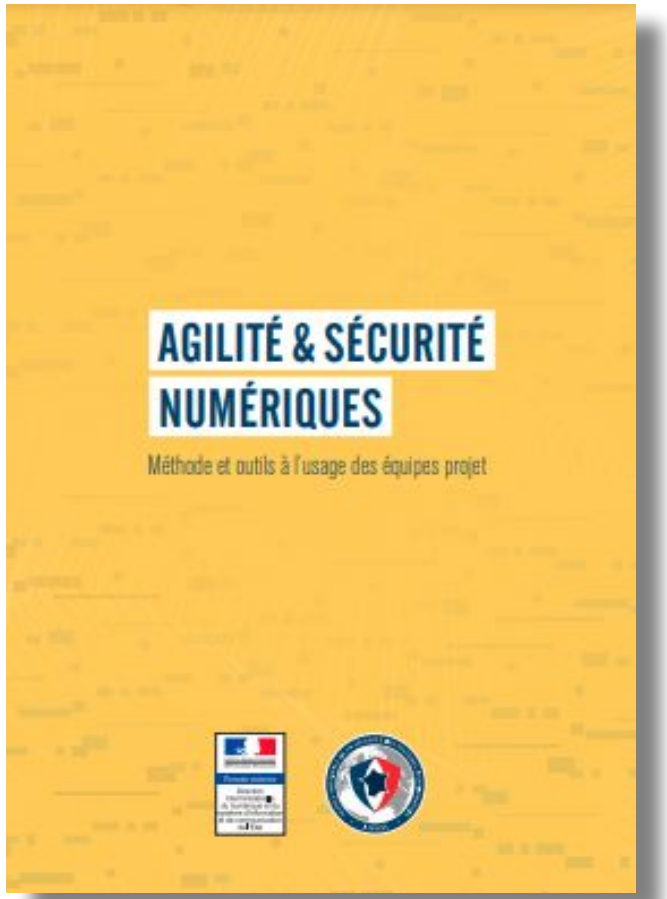
permettant à l'équipe de faire avancer la sécurité du produit

3. Aller vers l'homologation

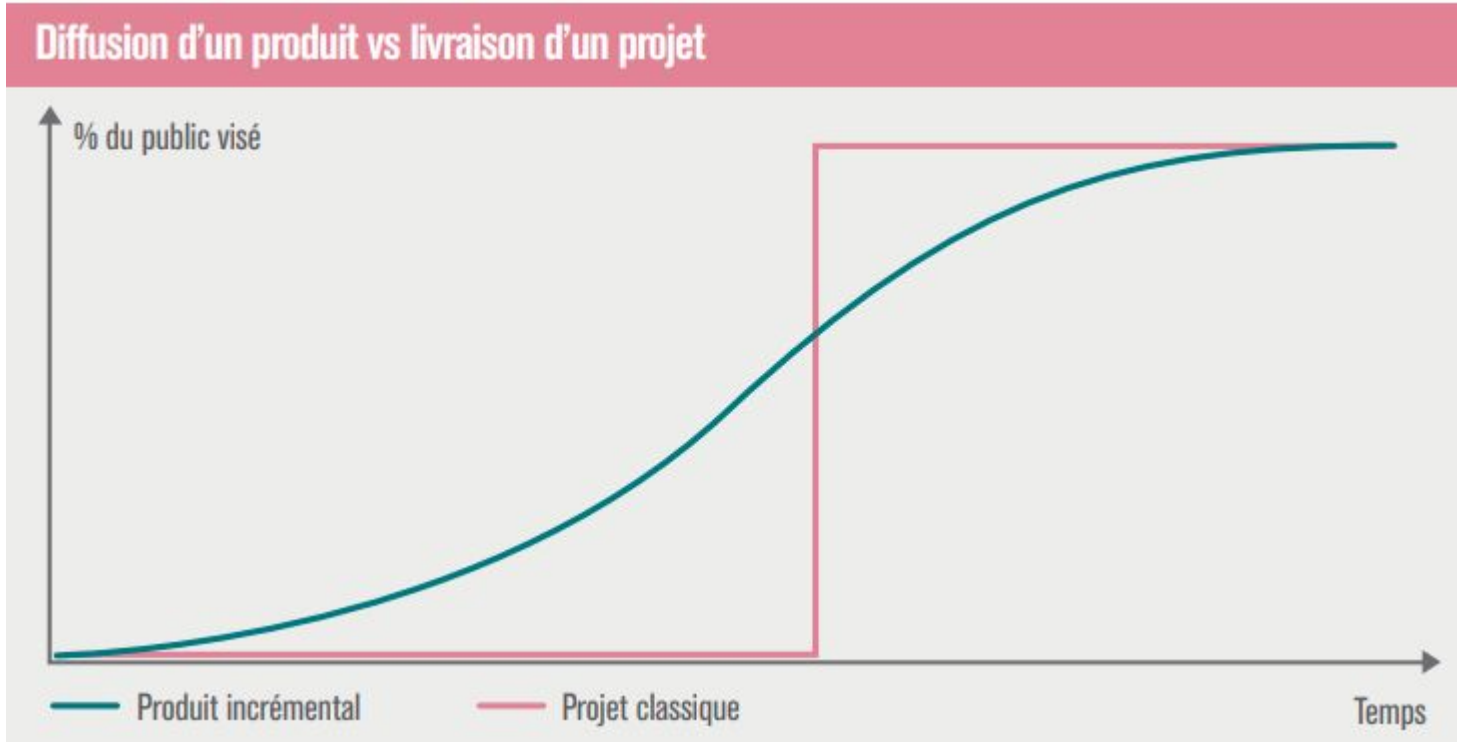
en utilisant le document d'analyse de risques comme base du dossier d'homologation

La DINUM est familié à l'animation d'atelier d'analyse de risques, n'hésitez pas à demander de l'aide avant l'atelier, pendant un atelier et après un atelier.

La méthode



- Issue d'une collaboration ANSSI / DINUM
- Construit comme étant plus accessible que la méthode EBIOS RM
- Une vision incrémentale de la sécurité :



Vous avez besoin de :

Un document collaboratif

Tous les membres de l'équipe pour le premier atelier : intra, dev, bizdev, design, …

Une envie collectif de découvrir les risques de sécurité du produit

Un animateur ayant connaissance de la méthode

Conseils :

- ➔ **Ecrivez une première version plutôt que de débattre à l'oral**
- ➔ **Le chemin fait partie de l'atelier, il n'y a pas que le résultat qui compte**
- ➔ **Ecoutez-vous bien : le point de vue de chacun va être utile à la fois pour identifier les risques mais aussi trouver des solutions**
- ➔ **Il vaut mieux une mauvaise première version que pas de version du tout (better done than perfect)**

Les étapes


User Stories
Abusers stories
LISTER
EVALUER
LISTER
EVALUER
15 minutes
Présentation
Périmètre
Composants
Fonctionnalités
15 minutes
Disponibilité
Intégrité
Confidentialité
Preuve
45 minutes
Attaquants
Evénements redouté
Mesures en place
Mesures possibles
45 minutes
Gravité
Vraisemblance
Vraisemblance cible
Risques résiduels

Commencer par la description du Produit

Description

Le service AudioConf permet de réserver une conférence téléphonique en quelques clics.
Un numéro de téléphone et un code d'accès sont fournis au demandeur pour rejoindre la conférence téléphonique, ce code est valide de 1 jour jusqu'à 6 mois (au choix de l'utilisateur).
Le service est ouvert à tous les agents publics et toutes personnes disposant d'une adresse email de l'état.
Ce service est opéré par la DINUM.

Rappel du périmètre de l’analyse

Intégré au périmètre :
Tout ce qui engage la responsabilité de l’équipe vis-à-vis des autorités administratives utilisatrices.

Hors périmètre :
Tout ce qui relève d’autres acteurs pour lesquels l’équipe ou l’administration sponsor du produit n’a pas de lien de subordination.

Lister les composants

- Code source
- Hébergeur
- Services utilisés
  - Envoi d’email
  - API Tierces

Exemple : AudioConf

Composants

- Code source de l'application :
  - https://github.com/betagouv/audioconf
- Hébergeur PaaS Scalingo
- Services utilisés
  - Service d'envoi email (SMTP - Brevo)
  - API OVH de réservation de conférences

Les parties prenantes

Par exemple :

- Utilisateurs du service
- Administrateur/Modérateur
- Administrateur Système

Si 2 types d’utilisateurs peuvent faire les mêmes actions, on les regroupes.
Un même utilisateur pourrait faire partie de 2 groupes de parties prenantes.

Exemple : AudioConf

Partie prenantes

- Agent public et prestataire de l'administration
  - Dispose d'une adresse email de l'administration
- Administrateur technique
  - Développeurs de l'application AudioConf

User Stories

- Grandes fonctionnalités de l’application
- 5 à 10 users stories maximum
- On groupe ce qui est similaire

Exemple : AudioConf

User stories

- En tant qu'agent public, je souhaite réserver une conférence téléphonique
- En tant que participant, je souhaite rejoindre une conférence téléphonique
- En tant qu'organisateur, je souhaite voir les participants à la conférence téléphonique

Evaluation des users stories suivant la matrice DICP

- **[D] Disponibilité** : la fonctionnalité peut être utilisée au moment voulu
- **[I] Intégrité** : les données sont exactes et complètes
- **[C] Confidentialité** : les informations ne sont divulguées qu'aux personnes autorisées
- **[P] Preuve (ou [T] Traçabilité)** : les traces de l'activité sur le système permettent d'être opposables en cas de contestation

Cette étape peut générer beaucoup de discussions sur des questions que l'équipe ne s'est jamais posé :

- *Ecrivez une première version et éviter les longs débats*
- *Répartissez-vous en sous-groupe après avoir fait 1 ou 2 users stories ensemble*

DICT : AudioConf

En tant qu'agent public, je souhaite réserver une conférence téléphonique

[D] La fonctionnalité doit être disponible dans les 24h ouvrés
[I] Il n'y a pas de besoin d'intégrité forte
[C] Le numéro de conférence est confidentiel
[P] Le domaine est associé à la réservation pour facturer le service

En tant que participant, je souhaite rejoindre une conférence téléphonique

[D] La fonctionnalité doit être disponible dans les 5 minutes ouvrés
[I] Il n'y a pas de besoin d'intégrité forte
[C] Le numéro d'appel du participant est confidentiel
[P] Il n'y a pas de besoin de preuve

En tant qu'organisateur, je souhaite voir les participants à la conférence téléphonique

[D] La fonctionnalité doit être disponible dans les 10 jours ouvrés
[I] Il n'y a pas de besoin d'intégrité forte
[C] Les numéros d'appels des participants sont confidentiel
[P] Il n'y a pas de besoin de preuve

Vous êtes un journaliste,

vous écrivez le titre d'un article qui va faire la une du journal à propos d'un incident de sécurité ayant touché le produit.

A vous de jouer !

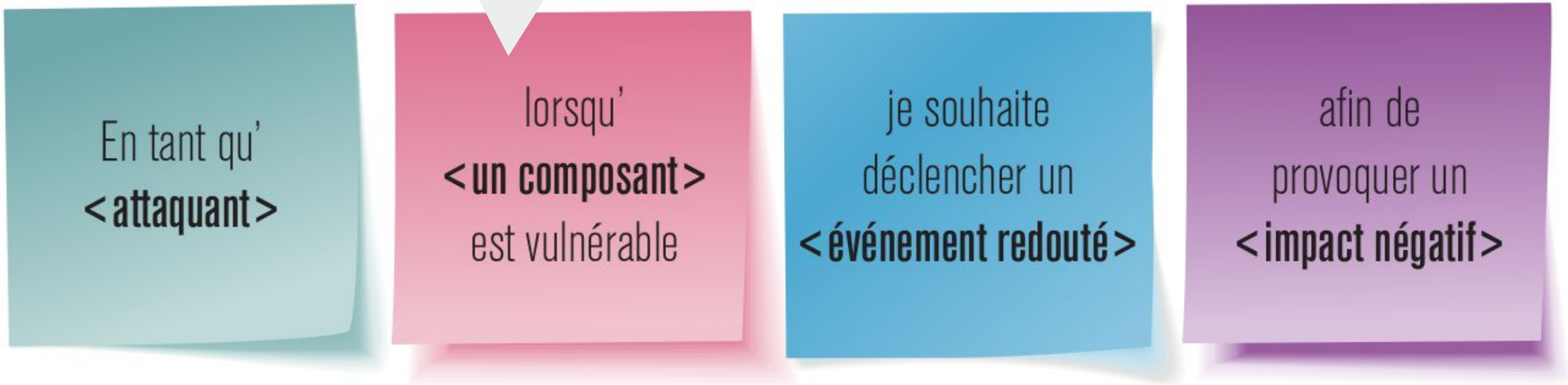
- Vous pouvez écrire plusieurs titres (c'est même recommandé)
- Vous pouvez écrire pour le Gorafi
- Vous devez intéresser vos lecteurs

Titre de journaux : AudioConf

- Des conférences de l'état espionné par la Syldavie
- Des hacktivistes ont bloqué les appels servant à faire les réunions de prise de décisions du gouvernement
- King Kong a arraché l'antenne en haut de la tour montparnasse faisant tomber le réseau de conférence téléphonique de l'État

Abuser Story

Composant que vous avez identifiés au début de l'atelier

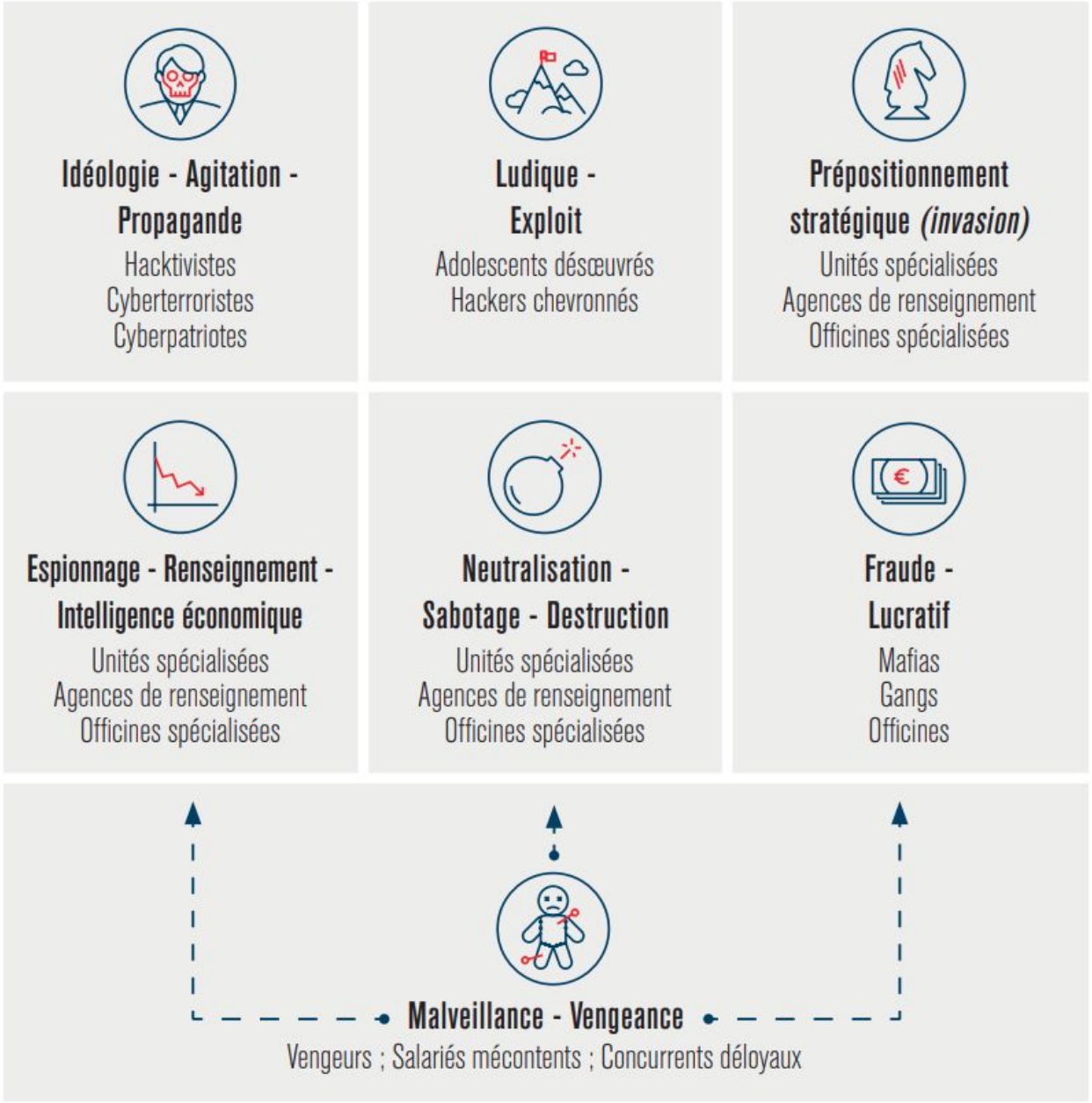


Page 22 et 23 du Guide

Sources de risques

La majeure partie du temps, vous allez utiliser le mot "hacker" pour désigner un attaquant

Fiche memo 3, page 44 du Guide



Abuser Stories : AudioConf

Des conférences de l'état espionné par la Syldavie

En tant qu'**attaquant étatique**,
lorsque le **code source** est vulnérable,
je souhaites **récupérer les codes de conférences pour espionner les conférences téléphoniques**
afin de **récupérer des informations stratégiques**

Des hacktivistes ont bloqué les appels servant à faire les réunions de prise de décisions du gouvernement

En tant qu'**hacktiviste**,
lorsque l'**API OVH** est vulnérable,
je souhaites **saturer les capacités d'appels**
afin de **ridiculiser le gouvernement et perturber son fonctionnement**

Echelle de Gravité

Si vous n'êtes pas d'accord après un échange, la personne la plus proche du sponsor ou le sponsor à le dernier mot.

Niveau de gravité	Description
🟩 1-Mineure	L'impact sera négligeable.
🟨 2-Significative	L'impact aura des conséquences significatives mais surmontables malgré quelques difficultés.
🟧 3-Importante	L'impact aura des conséquences importantes qui pourront être surmontées mais avec des difficultés réelles et conséquentes.
🟥 4-Critique	L'impact aura des conséquences graves, voire irrémédiables, sans doute insurmontables.

Les mesures

- Rédiger les mesures de la manière la plus simple:
  - Pas d'acronyme
  - Utiliser un vocabulaire compréhensible par les personnes qui ne maîtrisent pas le langage technique

- Il y a des mesures techniques et d'autres organisationnelles:
  - Technique : scan automatique du vulnérabilités connues dans les dépendances de l'application…
  - Organisationnelle : modération des contenus, relecture de code par un autre développeur…

Abuser Stories : AudioConf

En tant qu'**attaquant étatique**, lorsque le **code source** est vulnérable,
je souhaites **récupérer les codes de conférences pour espionner les conférences téléphoniques**
afin de **récupérer des informations stratégiques**

- **Gravité : 4/4** 🟥
- **Mesures en place :**
  - **[Tech]** Analyse de code automatique par Github
  - **[Orga]** Les utilisateurs sont sensibilisé aux fait que les services ne peut accueillir que des informations non-privilégié
  - **[Tech]** Ne pas stocker les codes d'accès au conférence en base de donnée
- **Mesures possible :**
  - **[Tech]** Lancer un programme de bug bounty

Echelle de vraisemblance

La motivation et les moyens de l'abuser ainsi que les mesures en places sont à prendre en compte dans l'évaluation de la vraisemblance

Niveau de vraisemblance	Description
🟩 1-Peu probable	L'abuser a peu de chance et/ou n'a pas la volonté d'atteindre son objectif, selon l'un des modes opératoires envisagés. La concrétisation du scénario est faible.
🟨 2-Probable	L'abuser est susceptible et/ou a la volonté d'atteindre son objectif, selon l'un des modes opératoires envisagés. La concrétisation du scénario est significative.
🟧 3-Très probable	L'abuser va probablement atteindre son objectif et/ou a la forte volonté d'y parvenir, selon l'un des modes opératoires envisagés. La concrétisation du scénario est élevée.
🟥 4-Quasi-certain	L'abuser va certainement atteindre son objectif et/ou a la très forte volonté d'y

Si vous n'êtes pas d'accord après avoir échangé, la personne ayant le plus haut niveau de connaissances en sécurité informatique à le dernier mot

Abuser Stories : AudioConf

AS1 - En tant qu'**attaquant étatique**, lorsque le **code source** est vulnérable,
je souhaites **récupérer les codes de conférences pour espionner les conférences téléphoniques**
afin de **récupérer des informations stratégiques**

- **Gravité : 4/4** 🟥
- **Mesures en place :**
  - **[Tech]** Analyse de code automatique par Github
  - **[Orga]** Les utilisateurs sont sensibilisé aux fait que les services ne peut accueillir que des informations non-privilégié
  - **[Tech]** Ne pas stocker les codes d'accès au conférence en base de donnée
- **Vraisemblance actuelle : 2/4** 🟨
- **Mesures possible :**
  - **[Tech]** Lancer un programme de bug bounty
- **Vraisemblance cible : 1/4** 🟩

Abuser Stories : AudioConf

AS2 - En tant qu'**hacktiviste**, lorsque l'**API OVH** est vulnérable, je souhaites **saturer les capacités d'appels** afin de **ridiculiser le gouvernement et perturber son fonctionnement**

- **Gravité : 2/4** 🟨
- **Mesures en place :**
  - **[Tech]** Analyse de code automatique par Github
  - **[Orga]** Contractualisation avec OVH
- **Vraisemblance actuelle : 1/4** 🟩
- **Mesures possible :**
  - **[Tech]** Bannissement automatique de numéro spammeur
  - **[Orga]** Proposer des outils alternatifs pour les réunions distanciels
- **Vraisemblance cible : 1/4** 🟩

Bravo 🎉

Si vous avez un peu de temps ?
Allons voir la suite

Cartographie des risques

🟥 *Risques Important vous devez prendre des mesures rapidement*

⬛ *Risques inacceptable : vous ne pouvez pas lancer*

Gravité	**4 – Critique**		**AS1**		
	3 – Importante	**AS2**			
	2 – Significative				
	1 – Mineure				
		1 – Peu probable	**2 – Probable**	**3 – Très probable**	**4 – Quasi-certain**
		Vraisemblance			

Numéroter vos abusers stories (les plus graves en premières) et placez-les dans la cartographie

Beaucoup de mesures ? Établissez un socle

- [tech] Revue systématique du code écrit obligatoire et renforcé par l'outil de gestion de code
- [tech] Double authentification sur le repository de code et l'hébergement
- [tech] Développement dans un environnement containeriser, permettant de protéger le poste de développement des dépendances malveillantes
- [tech] Outil de vérification automatique de faille de sécurité dans le code : CodeQL sur Github
- [tech] Vérification de la non présence de clefs secrètes ou mot de passe en dur dans le code : Git Guardian & Secret scanning de Github
- [tech] Mot de passe aléatoire et unique de l'accès pour tous les comptes services (notamment Scalingo & Github)
- [tech] Organisation d'ateliers d'Analyse de Risques de sécurité, en mode agile.
- [tech] Chiffrement et protection par mot de passe robuste des postes de travail
- [tech] Ajouter du service sur https://dashlord.incubateur.net/ l'outil de scan automatique à destination des startups d'état
- [tech] Ne pas faire des publications automatiques en production depuis le dépôt de code
- [tech] Sauvegarde automatique de la base de donnée
- [orga] Lancer un Bug Bounty

Le socle regroupe les mesures communes à plusieurs produits

Et après ?

- Nommer une personne référence dans l'équipe qui va nettoyer le document produit et finaliser les derniers éléments
- Présenter le document à votre RSSI pour récupérer ces commentaires et les intégrer
- Présenter ce document à votre sponsor pour l'aider à comprendre les risques que vous avez pris en compte et qu'il va devoir accepter
- Revoir régulièrement le document et le mettre à jour en équipe (tous les 3 à 6 mois)
- Aller vers l'homologation

L’homologation

- Attestation formelle par l’autorité responsable, ou son représentant, que les besoins de sécurité sont correctement exprimés, que les risques résiduels sont maîtrisés et acceptables et que le système est apte à être mis en production.
- Préparation de la commission d’homologation :
  - Identifier l’autorité d’homologation (personne qui va accepter les risques)
  - Rassembler les pièces du dossier d’homologation (les documents apportant de la confiance rédigées tout au long du projet)
  - Préparer le support de la commission (synthèse des documents)
  - Présenter le calendrier de mise en œuvre des mesures
  - Les risques présentés ne sont pas techniques mais métier.
  - La commission se prépare avec le CSN du sponsor.

- **L’apprentissage passe par la répétition**
  - Faite régulièrement des ateliers
  - Relisez le guide de temps en temps
  - Demander du feedback

Ces conseils sont pour l’animateur et aussi pour l’ équipe présente à l’atelier

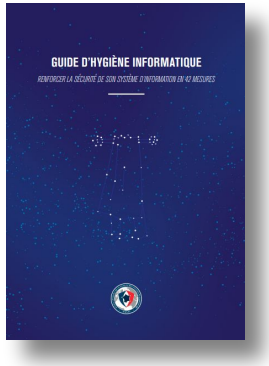
- **Mieux vaut fait que parfait**
  - Ecrivez une première version plutôt que de débattre à l’oral
  - S’il y a beaucoup d’échange -> faite des sous-groupes
  - Mettez un chronomètre et indiquer le temps restant
  - Si vous n’avez pas eu le temps de finir, re-programmer un atelier de 30-45 minutes pour finaliser
- **Le risque zéro n’existe pas, il y aura toujours des risques**

Des questions ?

Ressources

- Un outil d'auto-évaluation en ligne : https://www.monservicesecurise.ssi.gouv.fr/
- Le guide Agile et Sécurité ANSSI/DINUM : https://cyber.gouv.fr/sites/default/files/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf
- Le guide d'hygiène ANSSI : https://cyber.gouv.fr/publications/guide-dhygiene-informatique
- Les publications de l'ANSSI :https://cyber.gouv.fr/publications
- Gabarit atelier en markdown : https://pad.numerique.gouv.fr/gdT-AmDzTwCKZk9lYjgO_Q

MonService Sécurisé
Innovation ANSSI



Annexe : Modèle cartographie des risques

Gravité	4 – Critique				
	3 – Importante		AS2-AS3-AS4-AS5		AS1
	2 – Significative	AS7		AS6	
	1 – Mineure	AS8			
		1 – Peu probable	2 – Probable	3 – Très probable	4 – Quasi-certain
		Vraisemblance			