CloudCERT

Testbed Framework to Exercise

Critical Infrastructure Protection

indra

CNPIC

EUROPE for business

INTECO

Fondazione ICSA

Zanasi & Partners

CONTACT

http://cloudcert.european-project.eu
info@cloudcert.european-project.eu

http://en.wikipedia.org/wiki/CloudCERT

RÉSULTATS DU SYSTEME DE BANC DE TEST CLOUDCERT POUR EXERCER UNE PROTECTION ESSENTIELLE DES INFRASTRUCTURES

Edité par:
Instituto Nacional de Tecnologías de la Comunicación S.A.
INTECO
Avenida José Aguado, 41- 24005 León
(+34) 987 877 189
www.inteco.es

Version électronique disponible à l'adresse:

http://cloudcert.european-project.eu/

INDEX

CONTEXTE et MOTIVATION

PRESENTATION DU PROGRAMME

La sécurité et l'économie de l'Union Européenne ainsi que le bienêtre de ses citoyens dépendent de certaines infrastructures et des services qu'elles apportent. La destruction ou le bouleversement des infrastructures apportant des services clés peut entraîner une perte de vies, de biens, un effondrement de la confiance et de l'état d'esprit du public dans l'UE.

2004 Pour neutraliser ces vulnérabilités potentielles, le Conseil Européen a requis en 2004 le développement d'un Programme Européen pour la Protection des Infrastructures Critiques (*PEPIC*). Depuis, un travail préparatoire complet a été mené, incluant l'organisation de séminaires pertinents, la publication d'un Livre Vert, des discussions avec les parties prenantes publiques et privées et le financement d'un projet pilote.

2006 Gardant cela à l'esprit, le 12 Décembre 2006, la Commission a adopté la communication sur le PEPIC fixant le système horizontal général pour les activités de protection des infrastructures critiques au niveau de l'UE. Le programme UE proposé sur la "Prévention, Préparation et Gestion des Conséquences en matière de Terrorisme et autres Risques liés à la Sécurité" a été adopté le 12 Février 2007.

2008 La Directive du Conseil 2008/114/EC sur l'identification et la désignation des infrastructures critiques Européennes et l'évaluation de la nécessité d'améliorer leur protection a fixé une procédure pour identifier et désigner les infrastructures critiques européennes (ICE). Au même temps, elle fournit une approche partagée pour l'évaluation des infrastructures, afin de les améliorer pour mieux protéger les besoins des citoyens.

2009 Finalement, le 30 Mars 2009, la Commission a adopté la communication sur la protection des infrastructures critiques de l'information (PICI) [COM(2009) 149], qui donne des informations sur les principales défis qui se posent aux infrastructures critiques de l'information et propose un plan d'action visant à accroître leur protection.

HOME/2010/CIPS/AG/20

Le Programme UE sur la "Prévention, Préparation et Gestion des Conséquences en matière de Terrorisme et autres Risques liés à la Sécurité" vise à encourager un échange de savoir-faire et bonnes pratiques entre les différents agents responsables de la gestion des crises et à organiser des exercices communs pour renforcer la coordination entre les départements pertinents.

La Commission Européenne élabore des programmes de travail annuels couvrant les priorités chaque année. Ces programmes incluent des appels à propositions pour fixer des subventions à l'action à octroyer aux projets transnationaux et/ou nationaux censées contribuer à la réalisation des objectifs généraux et spécifiques du programme.

À la suite de cet appel à propositions du programme 2010, le projet "**CloudCERT**" a été sélectionné parmi les projets financés.

MOTIVATION

Comme il a été déclaré dans le PEPIC, les parties prenantes doivent partager les informations sur la Protection des Infrastructures Critiques (PIC), notamment sur les mesures concernant la sécurité des infrastructures critiques et les systèmes protégés, les études d'interdépendance et l'évaluation des vulnérabilités, des menaces et des risques liés à la PIC. Au même temps, il faut assurer que les informations partagées de nature propriétaire, sensible ou personnelle ne soient pas rendues publiques, et que le traitement personnel des informations soit soumis à un niveau approprié de contrôles de sécurité par leur Etat Membre.

Pour répondre à ce besoin réel, le projet CloudCERT vise à fournir ce système de Banc de test pour le partage sécurisé des informations afin d'exercer une coordination unifiée en exploitant les mêmes standards du protocole de communication pour améliorer la visibilité de la connaissance des menaces, des vulnérabilités, des avis et des alertes spécifiques à la PIC.

Pour atteindre cet objectif, il faut mener un travail important fondé sur le modelage et l'architecture de communication conceptuelle CSIRT; définition de partage sécurisé d'informations; définition des standards et du protocole d'information ; conception et implémentation de la plateforme Banc de test; et enfin déploiement d'un pilote pour vérifier la situation réelle en exploitant des scénarios de cas d'utilisation.

La portée de ce projet se limite à la création de la plateforme pilote CloudCERT pour échanger des informations sur la PIC. Donc, dans le long terme, ce projet couvre seulement le premier stade de la feuille de route.

La plateforme finale est un pilote opérationnel, incluant un ensemble d'utilisateurs et d'informations suffisamment utiles pour tester sa fonctionnalité et mener des exercices de simulation pour l'échange d'informations concernant la PIC.

La plateforme permet l'échange de mesures opérationnelles, méthodologies, expériences et savoir-faire sur la PIC entre les utilisateurs jouant le rôle d'un référentiel d'informations, incluant au moins les types d'informations suivants:

- Vulnérabilités.
- Notes, Notifications et Alertes.
- Prise de conscience des menaces.
- News.
- Bonnes Pratiques sur la PIC.
- Leçons Apprises sur la PIC.

La plateforme CloudCERT est techniquement basée sur une application web pourvu d'une interface de gestion par l'utilisateur, incluant un système d'authentification solide et un échange sécurisé d'informations suivant des standards interopérables.

DESCRIPTION du PROJET

PARTICIPANTS

COORDINATEUR

- INTECO - National Institute for Communication Technologies.

CO-BENEFICIAIRES

- CNPIC - National Centre for Critical Infrastructure Protection.
- Europe for business.
- Fondazione Intelligence Culture and Strategic Analysis (ICSA).
- Indra Systems, Inc.
- INTECO - National Institute of Communication Technologies.
- Zanasi & Partners.

PARTENAIRES UTILISATEURS

- INTECO - National Institute for Communication Technologies.
- CNPIC - National Centre for Critical Infrastructure Protection.

OBJECTIFS

- Fournir une approche sur le **système de Banc de test** pour intégrer les mécanismes de coordination des efforts des partenariats et des parties prenantes pour échanger efficacement les informations concernant la PIC et leurs aspects de sécurité.
- **Sécuriser les infrastructures de l'UE**, en améliorant la compréhension des relations entre leurs éléments ainsi que le lien entre gestion des risques et protection des infrastructures.
- Assurer les habilités nécessaires pour **éliminer les vulnérabilités potentielles** dans les infrastructures critiques, en partageant les informations sur les vulnérabilités.
- **Gérer la sécurité** dans son ensemble en utilisant un procès unifié d'échange d'informations pour déterminer le risque et envisager et mettre en œuvre des actions pour réduire le risque à un niveau défini et acceptable, à un cout acceptable.
- **Obtenir une valeur** dérivée de l'échange d'informations à travers l'implémentation d'exercices, mesurée par l'efficacité de la prévention, dissuasion et réponse aux cyber attaques sur les systèmes de contrôle dans une infrastructure critique.
- Un **système commun de signalisation et d'échange d'informations** dans les six stades du cycle de vie de la PIC pour produire une solution exhaustive.

AVANTAGES

L'impact attendu à **court terme** est celui de fournir aux organes de PIC une plateforme banc de test conçue pour supporter l'échange d'information sur la PIC, la coordination et la supervision par les Etats Membres.

Au **moyen terme**, CloudCERT est censé renforcer la coopération à travers l'implémentation de la plateforme dans un environnement de production réel et contribuer à la minimisation des entraves à la coopération entre les operateurs de PIC et les autorités de protection dans des différents pays Européens.

À **long terme**, CloudCERT est censé contribuer à l'établissement d'un environnement de Sécurité Intérieure Européenne pour la Protection des IC Européennes.

GROUPES CIBLES

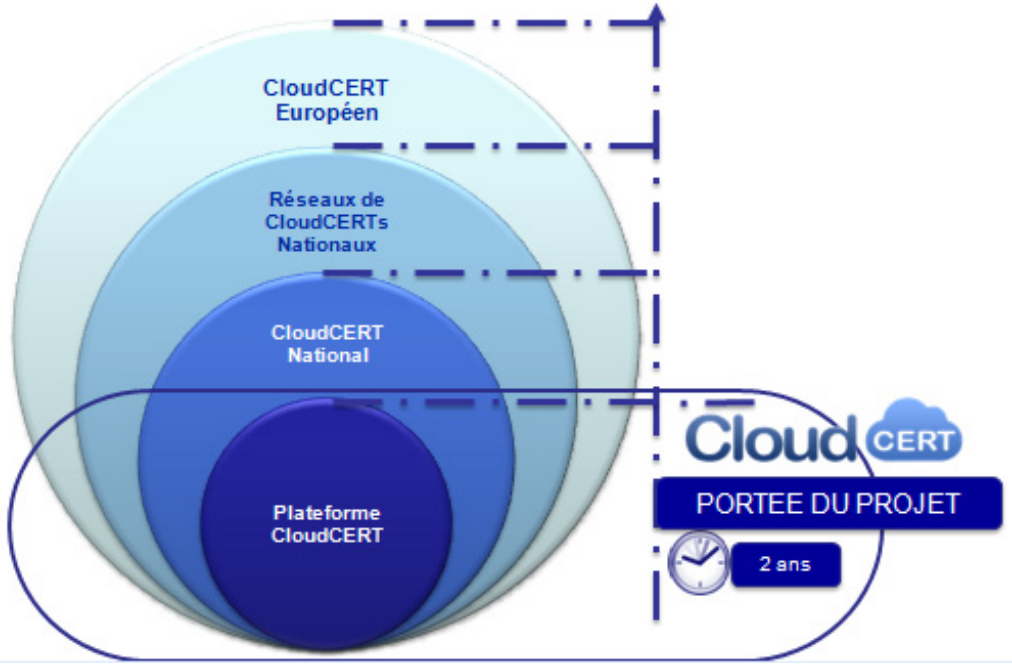
Les principaux groupes cibles et bénéficiaires de ce projet sont:

- Les Etats Membres, par le biais des Autorités de Protection des Infrastructures Critiques.
- CERT ou CSIRT compétents en matière de PIC.
- Operateurs ou Propriétaires des infrastructures Critiques (IC).

CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

DIMENSION EUROPEENNE ET FEUILLE DE ROUTE DU PROJET



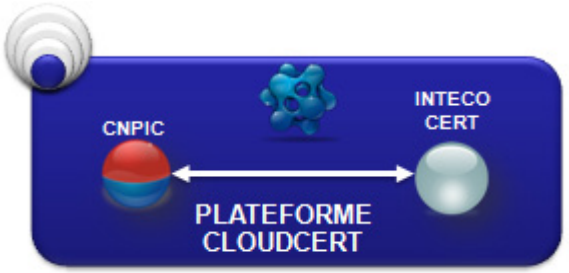
CloudCERT est un **projet transnational**, impliquant partenaires d'au moins deux Etats Membres.

L'approche du projet à long terme peut être considérée comme suivant une feuille de route incluant les étapes suivantes:

- Plateforme CloudCERT.
- CloudCERT national.
- Réseau National CloudCERT.
- CloudCERT Européen.

Pour établir un réseau de collaboration paneuropéen, nous proposons une méthodologie fondée sur des approches incrémentales progressives, générant des produits en phases qui vont être améliorés par chaque interaction. Au cours de la durée du projet (2 ans) seulement la **plateforme pilote** sera créée, dans la perspective de construire un CloudCERT national.

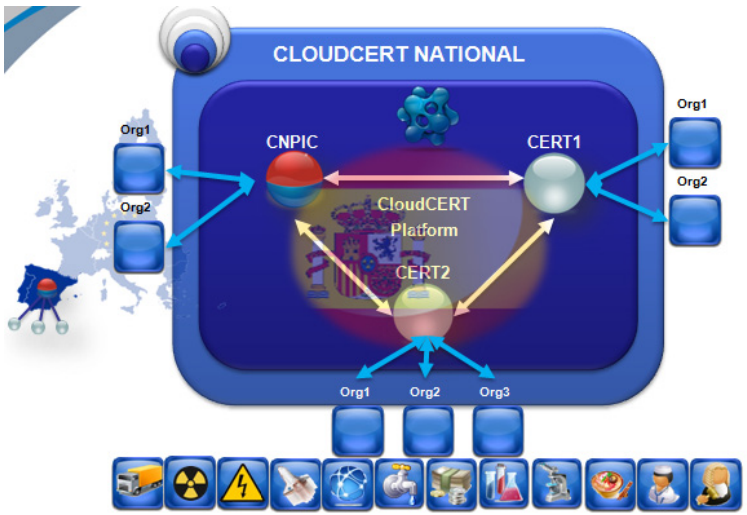
PHASE 1 - PILOTE CLOUDCERT (ACTUELLEMENT FINANCE PAR L'UE)



Dans ce première phase du feuille de route, le but est la création de la plateforme pilote afin d'ajouter les acteurs PIC d'un pays comme utilisateurs.

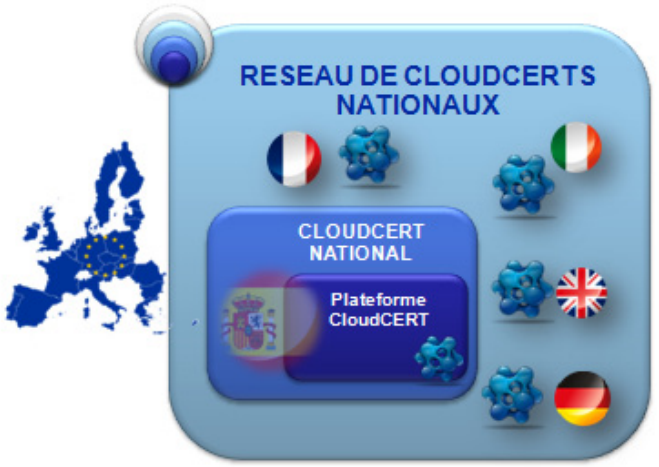
En raison des limitations du projet, les utilisateurs de cette plateforme seront les CERT participants au projet (INTECO-CERT) ainsi que les Centres Nationaux PIC participants (CNPIC).

PHASE 2 - CLOUDCERT NATIONAL (OPPORTUNITE)



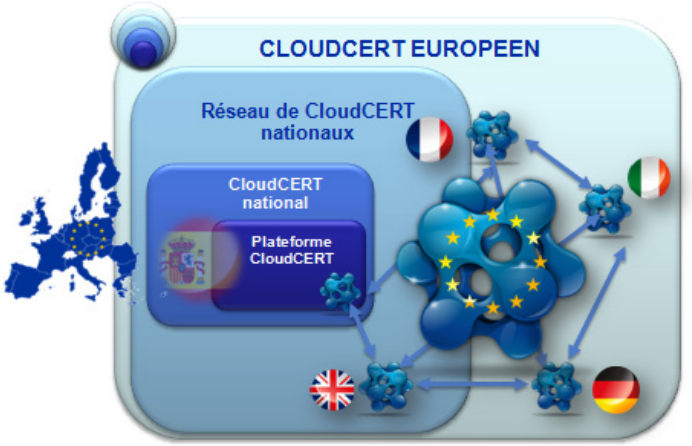
Une fois le pilote délivré, s'ouvre la phase d'exploitation de la plateforme. Cette phase peut commencer par le déploiement de la plateforme dans un environnement de production réel visant à l'établissement d'un CloudCERT National intégrant le Centre National PIC ainsi que les CERT principaux ayant des habilités en matière de PIC et d'autres possibles acteurs d'intérêt et pertinents.

PHASE 3 - NŒUDS DE CLOUDCERT (OPPORTUNITE)



La phase suivante dans le feuille de route sera la réplication sans difficultés dans d'autres Etats Membres pour créer les nœuds CloudCERT nationaux. Les différences existant dans les cadres réglementaires de chaque pays peuvent affecter l'échange des informations. Il vaudrait mieux ajouter de petites nuances ou conditions pour modifier la plateforme, mais sans modifier ou altérer de façon drastique son objectif principal.

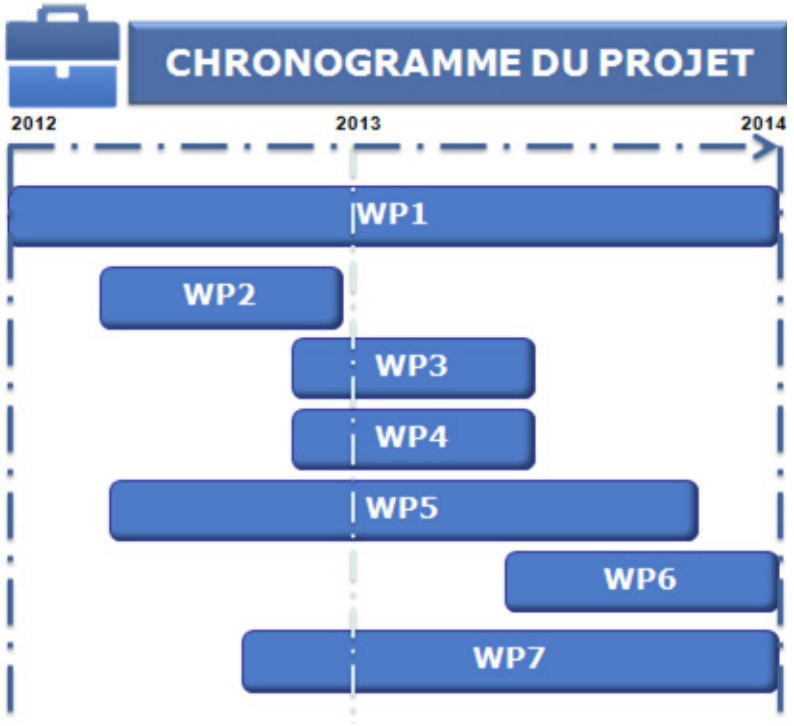
PHASE 4 - CLOUDCERT EUROPEEN (OPPORTUNITE)



Si ces étapes de la feuille de route donnent des bons résultats, il y aura une phase finale qui représentera l'interconnexion des nœuds Nationaux CloudCERT, formant un CloudCERT Européen par la somme de tous les membres nationaux, ou un CloudCERT Paneuropéen impliquant les Centres Nationaux PIC.

LOTS de TRAVAUX

PRESENTATION DES LOTS DE TRAVAUX (WORK PACKAGES)



WP1: GESTION DE PROJET

- Coordination des partenaires et de leur travail.
- Gestion des risques.
- Gestion financière.

WP2: MODELAGE ET ARCHITECTURE CONCEPTUELS

- Concevoir l'architecture du système sur la base de la définition conceptuelle du système de la Plateforme CloudCERT.

WP3: STANDARDS D'INFORMATION ET DE COMMUNICATION

- Définition des contenus et du format des informations à échanger.
- Définition du protocole d'échange d'informations.

WP4: DEFINITION D'UN SYSTEME SECURISE

- Explorer les pratiques de travail actuelles pour la gestion et le partage sécurisé d'informations sensibles et, enfin, proposer une liste des caractéristiques requises.

WP5: DEVELOPPEMENT DE LA PLATEFORME

- Développer un système de partage sécurisé pour échanger des informations sensibles, un catalogue et une base de données des vulnérabilités de la PIC.

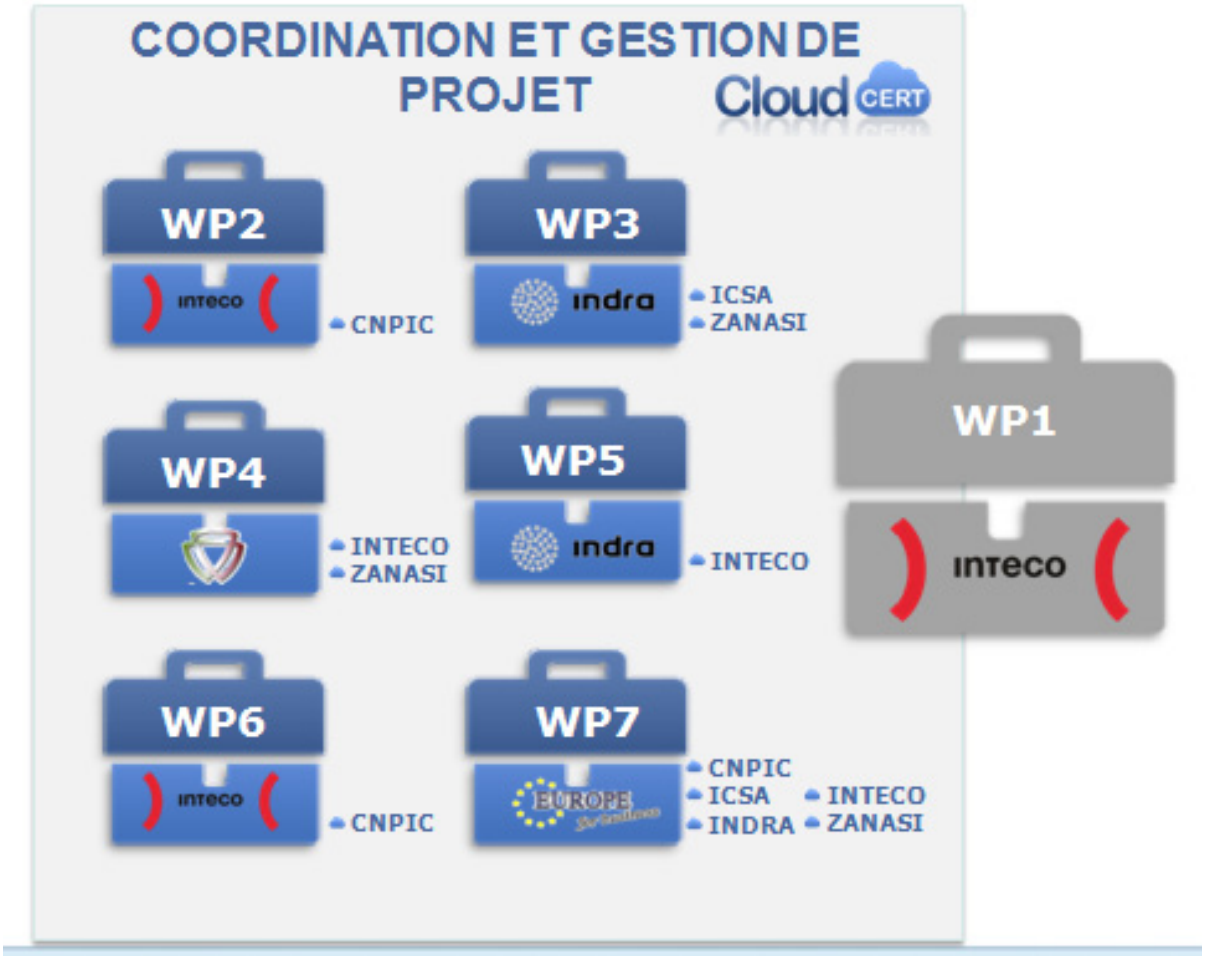
WP6: EXPERIMENTATION PILOTE

- Essayer l'outil de la plateforme par des cas d'utilisation d'intégration.

WP7: DISSEMINATION DES RESULTATS DU PROJET

- Dissémination des résultats du projet par des publications, conférences et séminaires.

WP1. GESTION DE PROJET

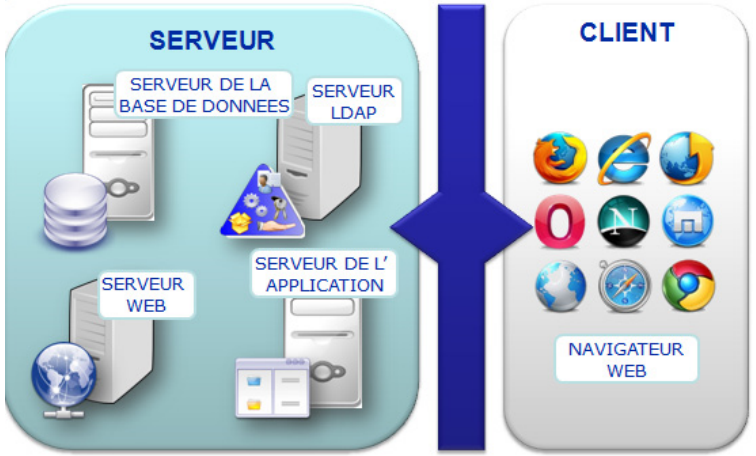


INTECO, en tant que coordinateur du Projet CloudCERT, est le responsable final de l'achèvement de tous les lots de travaux et le chef de fil des activités de gestion de projet.

WP2. CONCEPTION DE LA PLATEFORME

MODELE D'ARCHITECTURE

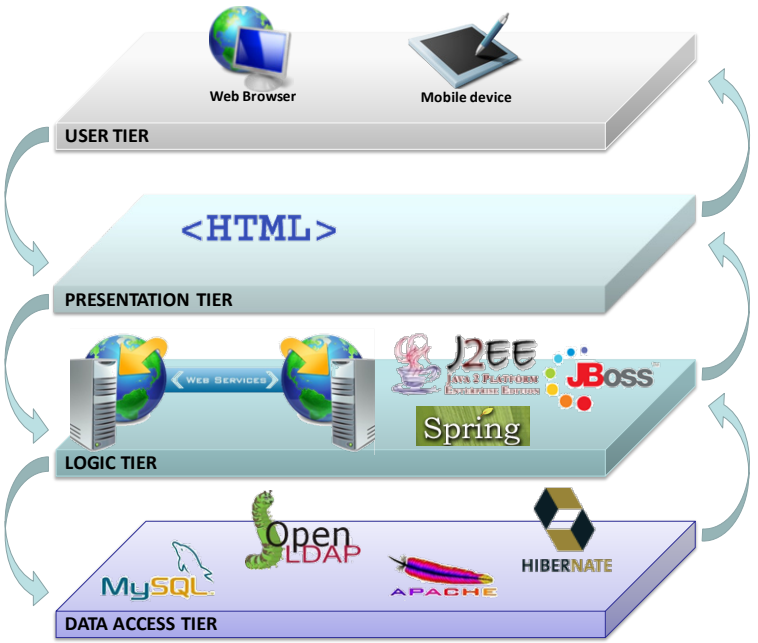
CloudCERT se fonde sur une architecture client / serveur. Le modèle des différents composants de la plateforme CloudCERT repose sur le standard J2EE.



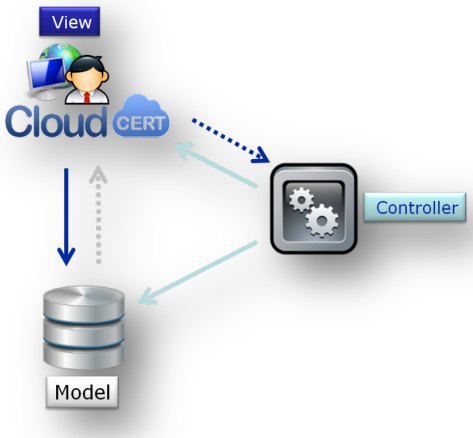
MODELE LOGIQUE

Les composants logiques du modèle de la plateforme sont groupés dans les types suivants:

- **Persistance des données.** CloudCERT a un modèle de données complexe. Pour traiter ce modèle, on a utilisé des systèmes permettant de le gérer de façon efficace.
- **Sécurité des Applications.** Toutes les tâches relatives à la sécurité des applications sont fondées sur les informations stockées sur le LDAP.
- **Gestion du contrôle des flux d'applications**. CloudCERT emploie le Framework Struts. Les Struts sont un outil d'appui pour le développement d'applications web sous le standard MVC et la plateforme J2EE.
- **Services Web**. Ils sont déployés en AXIS CloudCERT. AXIS est une implémentation SOAP développée par Apache et satisfaisant les standards OASIS et W3C.
- **Palier de présentation**. Il se fonde sur l'utilisation des Framework Struts et DWR.



STRUCTURE MVC

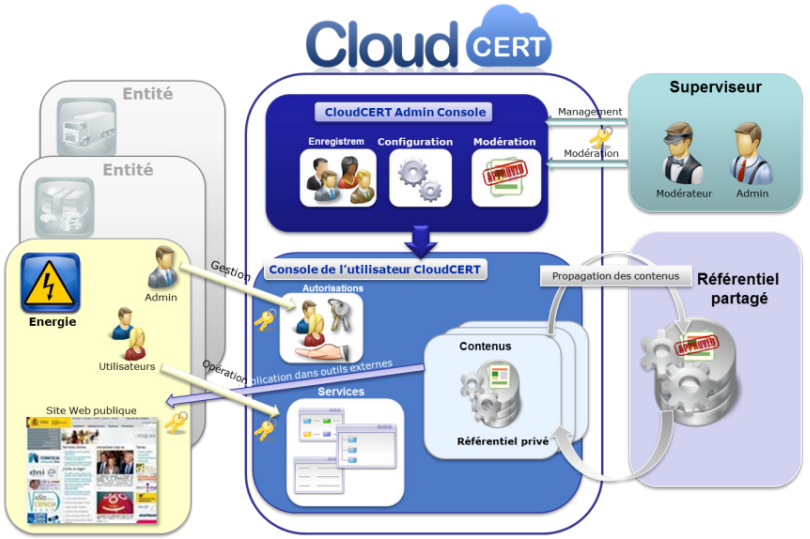


Comme la plupart des applications J2EE existant, le Modèle-Vue-Contrôleur a été adopté dans la plateforme CloudCERT.

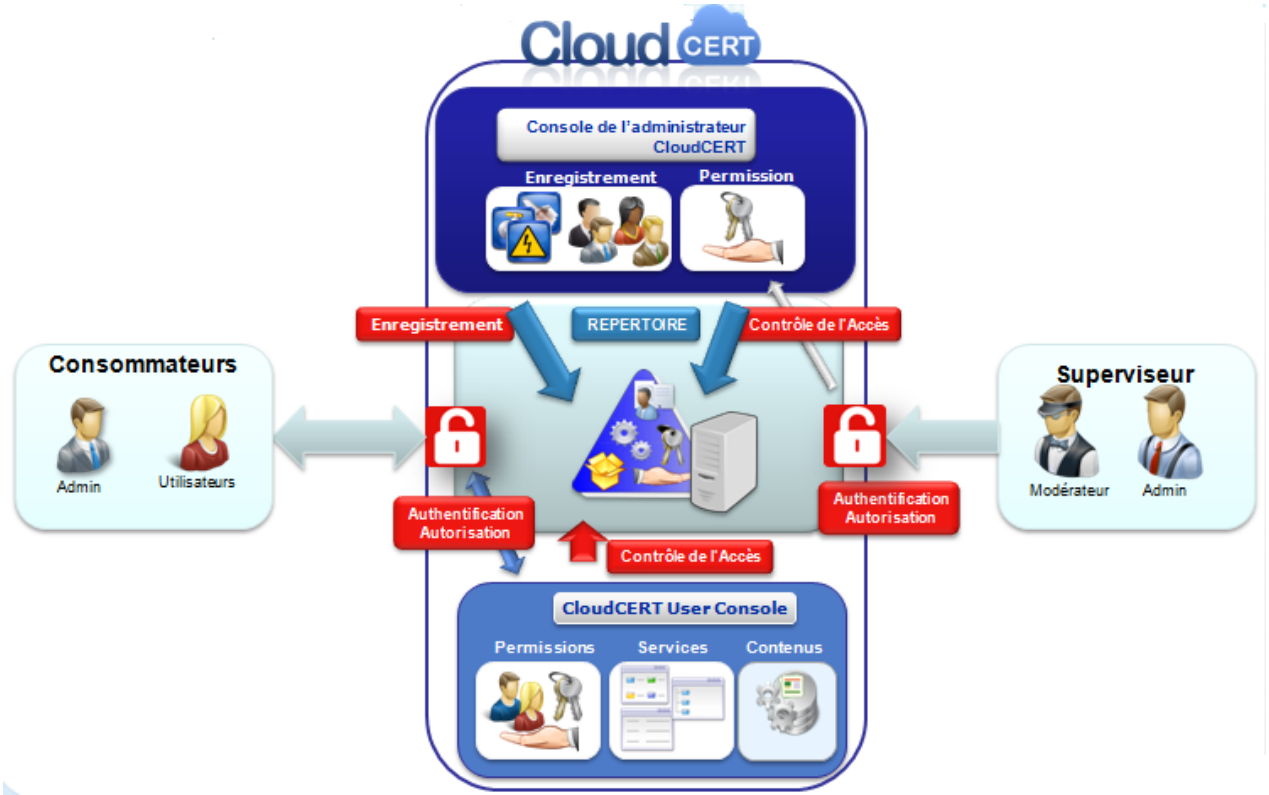
DESIGN FONCTIONNEL

Les applications et modules qui composent la plateforme CloudCERT incluent:

- **Modules d'Authentification CloudCERT**: Service Central d'authentification (Central Authentication Service - CAS).
- **Module de Gestion de Mot de passe**: module pour la gestion du changement des mots de passe et l'activation des comptes d'utilisateur.
- **Console de l'utilisateur CloudCERT:** Console de gestion des applications pour de différentes entités.
- **Console d'Administration CloudCERT**: gestion des applications pour la Plateforme CloudCERT (services, services web, entités, et contenus).
- **Services WEB CloudCERT.**



SECURITÉ

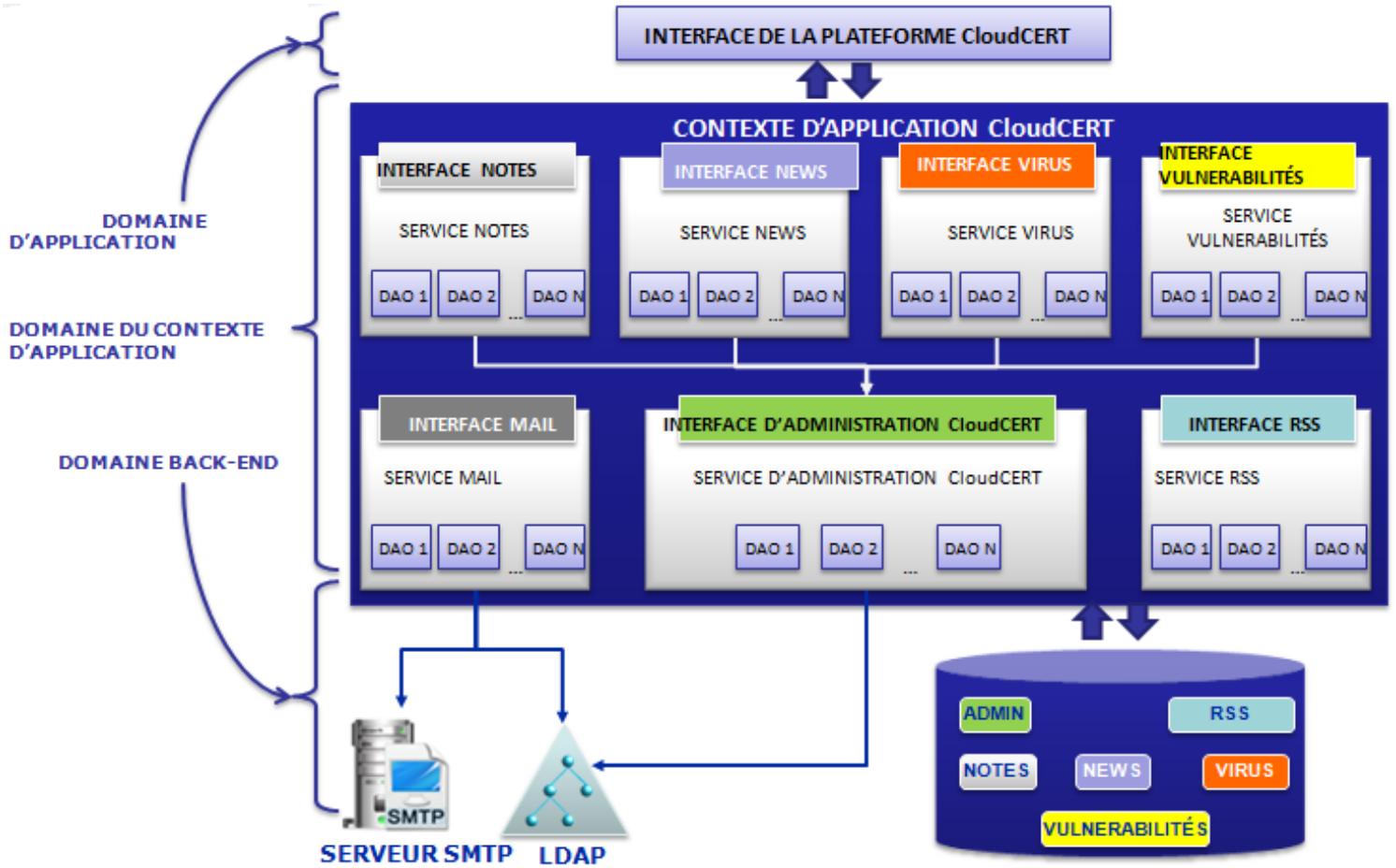


Toutes les questions relatives à la sécurité des applications reposent sur les informations stockées dans le LDAP. Les systèmes suivants ont été utilisés pour gérer la sécurité de CloudCERT :

- **Spring Security.** Module appartenant au Framework Spring qui permet une logique d'application pour maintenir le code de sécurité libre, en fournissant des mécanismes d''authentification et autorisation pour les applications J2EE. En outre, Spring Security aide l'authentification sur le Service Central d'Authentification (Central Authentication Service - CAS) en fournissant un client API pour interagir avec le serveur CAS.
- **Spring LDAP** Module appartenant au Framework Spring fournissant des mécanismes d'interaction pour simplifier les opérations sur tous types de serveur LDAP.

DESIGN DU CONTEXTE GLOBAL

En utilisant la persistance de la base de données et du LDAP, CloudCERT a défini un contexte global accessible par de différentes applications:



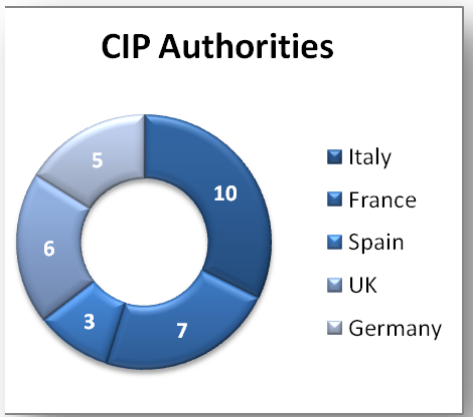
- **Domaine d'application.** Incluant toute la logique de présentation et le contrôle des flux.
- **Contexte du domaine d'application.** Le contexte définissant les différents services offerts par une interface publique aux applications supportées ou d'autres services.
- **Domaine Back-End.**
  - Base de données de la plateforme CloudCERT.
  - LDAP CloudCERT.
  - Serveur SMTP.

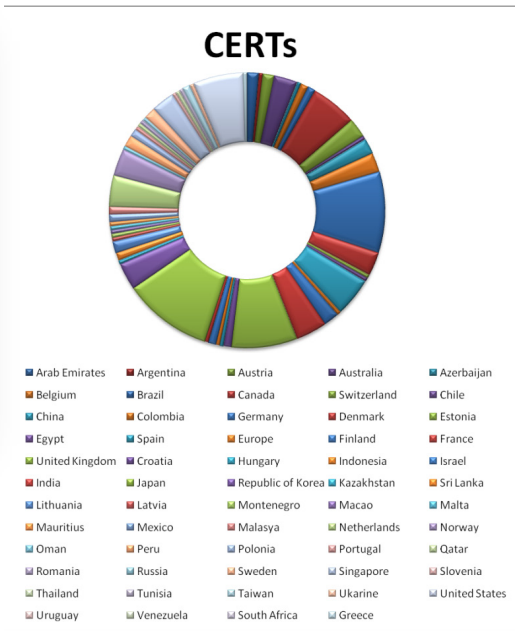
WP3. STANDARDS D'INFORMATION ET DE COMMUNICATION

ONTOLOGIES DES CONTENUS DES INFORMATIONS

- **NOTES:** gérer er partagé toutes les informations relatives aux événements institutionnels de CERT d'intérêt général dans le réseau de la plateforme CloudCERT.
- **NEWS:** présenter, gérer et partager toutes les nouvelles publiques considérées d'intérêt général.
- **ALERTES:** présenter, gérer et partager tous les cas considérés comme alertes d'intérêt spécial.
- **VIRUS:** présenter, gérer et partager tous les virus d'intérêt spécial.
- **VULNERABILITÉS:** gérer et partager toutes les vulnérabilités d'intérêt spécial.
- **PRODUITS RSS:** consulter tous les produits RSS considérés comme ressources d'intérêt spécial.

UTILISATEURS POTENTIELS DE CLOUDCERT





PROTOCOLES POUR L'ECHANGE D'INFORMATIONS ET STANDARDS DE DESCRIPTION DES INFORMATIONS

TECHNOLOGIES GENERALES POUR LE PARTAGE DES INFORMATIONS

Parmi la large variété de **protocoles pour le partage des informations** qui ont été développés au fil des années, trois protocoles ont été choisis, en partie pour leur large emploi dans de différents types d'organisations et en partie pour leur flexibilité, qui peut être exploitée avec succès dans le contexte de CloudCERT:

- EDI (Échange de Données Informatisées).
- XML (eXtensible Markup Language).
- SOAP (Simple Object Access Protocol).

STANDARDS D'ECHANGE D'INFORMATIONS SPECIFIQUES A DES FINS DE SECURITE

Le projet CloudCERT vise spécifiquement à aider les administrateurs des infrastructures critiques et des infrastructures d'information critiques à mieux se défendre face aux menaces de cyber sécurité. Les flux de sécurité sont (et seront sûrement dans un avenir proche) une menace à l'exploitation des infrastructures informatiques.

Dès qu'on découvre de nouveaux flux, informer les utilisateurs et les administrateurs sur les questions identifiées est une tâche vitale pour les vendeurs informatiques et pour les équipes de sécurité. La façon commune pour diffuser ces informations est à travers les "alertes de sécurité", des documents techniques décrivant en détail les caractéristiques de la question, son impact potentiel et fournissant souvent une liste de solutions possibles.

Cette section se focalise sur les formats normalisés **des alertes de sécurité** plus populaires :

- CAIF (Common Announcement Interchange Format).
- EISPP (European Information Security Promotion Program) Common Advisory Format.
- DAF (Deutsches Advisory Format).
- OpenIOC (Open Indicators of Compromise).
- IODEF (Incident Object Description Exchange Format).
- VERIS (Vocabulary for Event Recording and Incident Sharing).
- STIX (Structured Threat Information eXpression).

PLAN DE SOLUTIONS ALTERNATIVES

EVALUATION D'ECHANGE DES CONTENUS

Les contenus incluant des informations notables, notamment concernant le réseau CloudCERT, peuvent être soumis par **SOAP** (Simple Object Access Protocol) via **HTTPs** (Hypertext Transfer Protocol Secure):

- Alertes.
- Virus.
- Vulnérabilités.

Pourtant, les contenus suivants ne sont pas adéquats à être partagés:

- **Notes**. Ce contenu est utilisé par les utilisateurs de CloudCERT pour partager informations relatives aux événements institutionnels des CERT dans sa plateforme de réseau.
- **News**. Ce contenu est utilisé par les utilisateurs de CloudCERT pour partager les liens URL relatifs aux informations publiques concernant les CERT sans intérêt spécial hors de sa plateforme de réseau.
- **Produits RSS**. Ce contenu est utilisé par les utilisateurs de CloudCERT pour partager des produits RSS de différents flux publics.

INDICATEURS

Il est important de gérer attentivement le partage de contenus avec d'autres organisations. Dans ce but, il a fallu intégrer un module de tableau de bord dans la Plateforme CloudCERT permettant à l'administrateur de contrôler un ensemble d'indicateurs concernant cette activité.

Les indicateurs identifiés susceptibles d'être surveillés étaient:

- Nombre d'éléments produits pendant une période spécifique.
- Nombre d'éléments lus pendant une période spécifique.
- Les N contenus les plus lus.
- Les N organisations productrices les plus actives.
- Les N organisations de lecteurs les plus actives.
- Les N organisations les plus actives dans l'importation des contenus (dès référentiels partagés aux référentiels privés).
- Distribution mensuelle des journées les plus actives pour la production/consommation des contenus.

WP4. DEFINITION D'UN SYSTEME SECURISE

PRATIQUES DE TRAVAIL POUR UNE GESTION ET UN PARTAGE SECURISE DES INFORMATIONS SENSIBLES

La plateforme CloudCERT vise à faciliter l'échange d'**informations sensibles** sur la PIC entre des différents types de parties prenantes avec toutes les garanties de sécurité. Par conséquence, la première activité du lot de travail est une enquête pour étudier les pratiques de travail pour une gestion et un partage sécurisé d'informations sensibles.

SECURITE DES INFORMATIONS

Dans ce chapitre, on présente le domaine de la sécurité des informations et les questions y relatives, en mettant l'accent sur les Systèmes d'Information.

- **Confidentialité**: la divulgation inappropriée d'informations doit être détecté et prévenue.
- **Intégrité**: les informations ne doivent pas être modifiées par des sujets non autorisés.
- **Disponibilité**: les informations doivent être disponibles aux sujets autorisés, le cas échéant.

PARTAGE DES INFORMATIONS POUR LA PIC

Dans ce chapitre on va revoir ce qui a été fait pour permettre un partage d'informations efficace dans le contexte de la PIC, par les gouvernements de deux des pays les plus remarquables au monde: les Etats Unis et le Royaume Uni.

PROTECTION DES INFRASTRUCTURES CRITIQUES

Deux pays ont été pris comme exemple et leurs plans de PIC ont été décrits et analysés en détaille: les politiques élaborées par les Etats Unis et la situation italienne:

- Stratégie Nationale pour la Sécurité intérieure.
- Cadre stratégique national Italien pour la sécurité du cyberespace.

CONDITIONS DE SECURITE DE CLOUDCERT

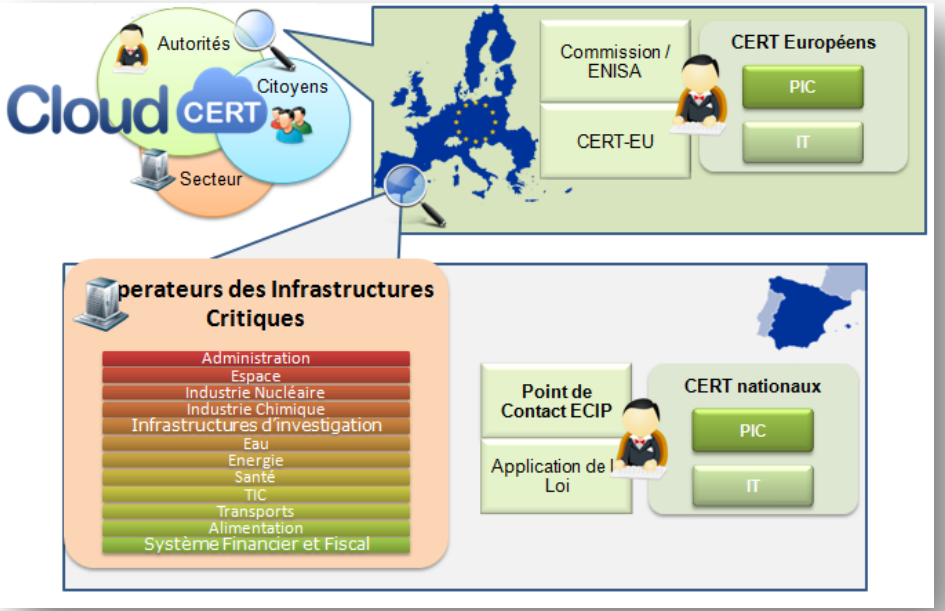
Les objectifs principaux de ce livrable sont:

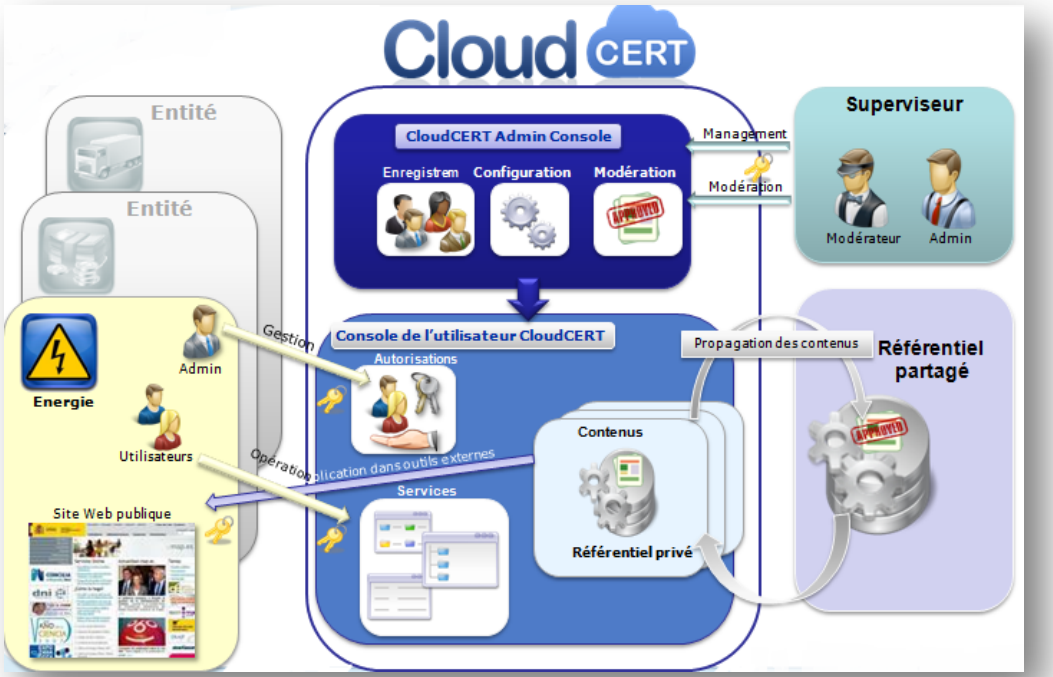
- Identifier les sources scientifiques principales dans le domaine de la PIC.
- Identifier les méthodes et démarches hypothétiques pour étendre et renforcer les processus collaboratifs du système.
- Identifier les méthodes et démarches hypothétiques pour étendre et renforcer la capacité de coordination entre les parties prenantes du système pendant le cycle de vie de l'IC.

L'objectif final est de mettre à jour le modèle opérationnel de gouvernance pour confier des rôles, responsabilités et objectifs aux parties prenantes du système.

Les parties prenantes de CloudCERT sont groupées en trois catégories:

- **Autorités** (secteur publique): autorités compétentes en matière de sécurité d'informations et de protection des infrastructures critiques, y compris le niveau légal et opérationnel. Cela inclut les décideurs politiques et les régulateurs ainsi que les équipes d'application de la loi.
- **Industrie** (secteurs privés): infrastructure critique incluant leurs fournisseurs principaux (fabricants de produits et développeurs de services).
- **Citoyens** (public cible): consommateurs de services fournis par les infrastructures critiques.



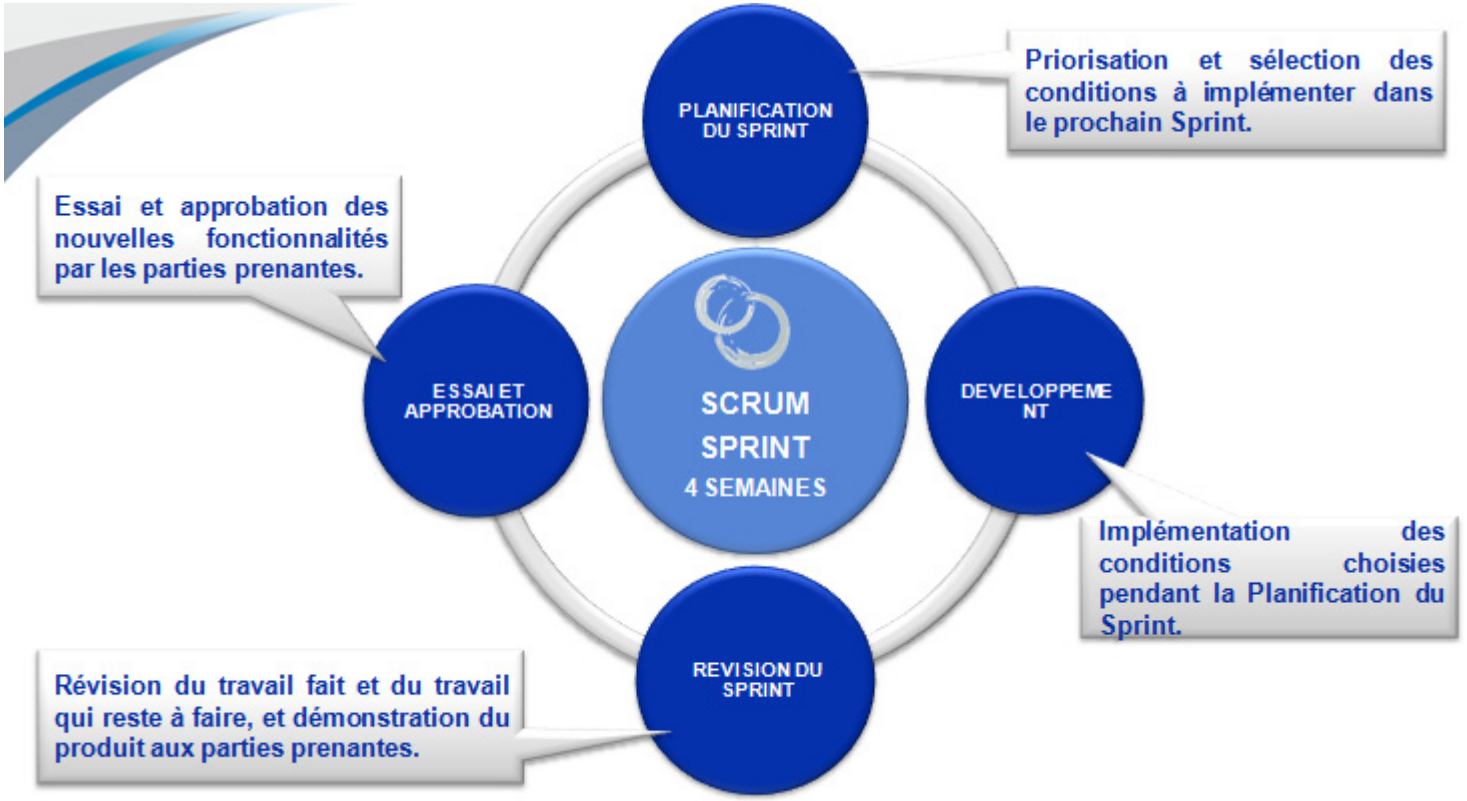


L'interaction entre ces parties prenantes et la plateforme CloudCERT se fonde sur un modèle de gouvernance règlementée de la façon suivante:

- De différentes **entités** peuvent avoir accès à la plateforme: CERT, équipes d'application de la loi, et operateurs des infrastructures critiques. Chaque entité a son espace pour publier ses contenus et peut importer contenus des référentiels partagés. Ils peuvent automatiquement exporter les contenus sur des outils externes comme, par exemple, leur site web interne.
- Une organisation de **supervision**:
  - **Gère** la plateforme en registrant les organisations et leur administrateur, mais aussi en configurant et en gérant les services disponibles. Le superviseur configure les autorisations des entités à l'accès aux contenus et services établis par contrat.
  - Fournit la **modération**. Tous les contenus doivent être sujets à modération et faire partie d'un **référentiel partagé**. La modération concerne aussi les publications dans des outils tels que les forums, les wikis etc.
- Chaque entité a un **administrateur** qui peut créer des utilisateurs et donner autorisations pour son Entité. Les contenus du référentiel privé de l'entité peuvent être publiés dans un référentiel publique avec l'approbation du superviseur.
- Les **utilisateurs** peuvent interagir avec les contenus et les services de la plateforme.

WP5. DEVELOPPEMENT DE LA PLATEFORME

C'est la phase de l'implémentation du projet pilote. Dans ce but, il faut accomplir les tâches suivantes:



CONDITIONS ET ANALYSE

La spécification des conditions du logiciel vise à :

- Identifier, en demandant aux utilisateurs finaux les conditions et fonctionnalités de la plateforme CloudCERT.
- Incorporer les conditions du système de sécurité et l'échange d'informations sensibles.
- Définir et prioriser les conditions pour la plateforme CloudCERT.

DEVELOPPEMENT

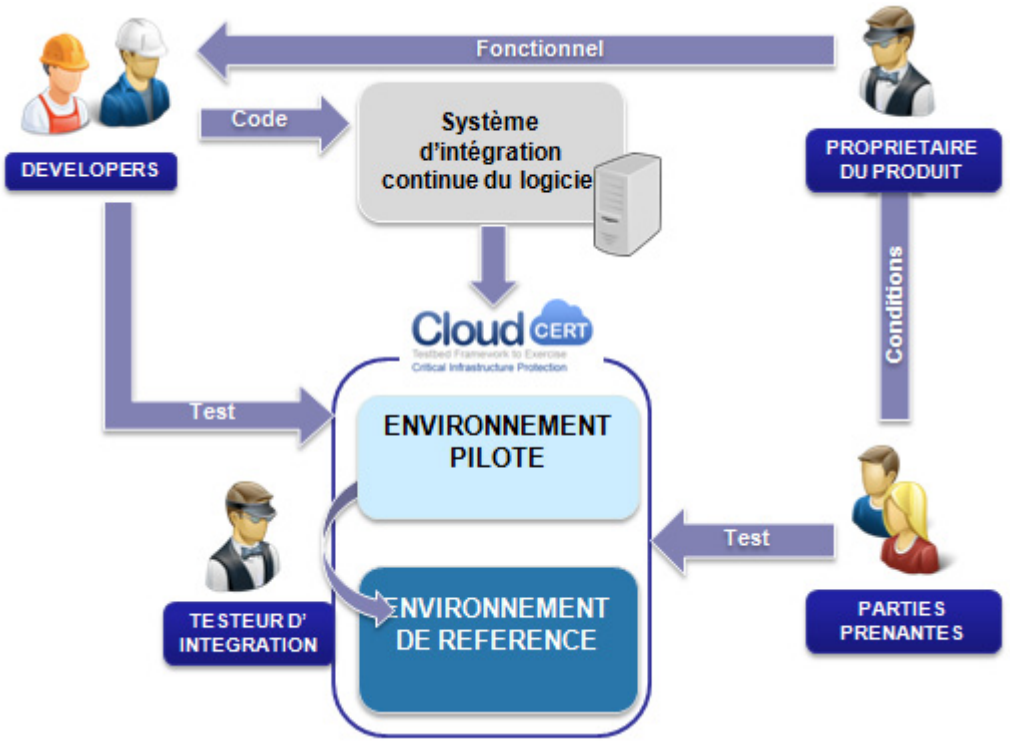
Suivant la méthodologie agile **scrum**, la phase de développement inclut:

- Implémentation des conditions acquises dans la phase précédente afin de créer un pilote fonctionnel.
- Création de la documentation de l'utilisateur et de l'administration du pilote développé.

INSTALLATION ET CONFIGURATION DE LA PLATEFORME

Pendant cette phase, on fournit des environnements de développement et d'essai et on crée des manuels d'installation et de configuration.

ENVIRONNEMENTS



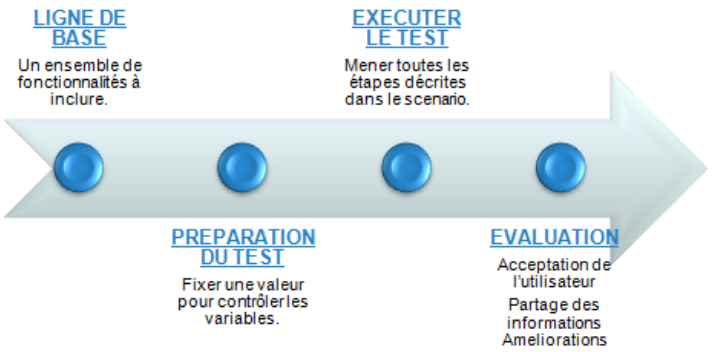
L'**environnement Pilote** est utilisé pour télécharger et essayer de nouveaux développements et pour les vérifier après chaque sprint.

Quand la phase d'essai est finie et tout a été vérifié, le nouvel produit est déployé dans l'**environnement de référence**, contenant une version plus stable de la Plateforme CloudCERT.

WP6. EXPERIMENTATION PILOTE

Les activités du WP6 se focalisent sur l'expérimentation et l'évaluation, fondée sur les cas d'utilisation d'intégration, sur la plateforme pilote développée et installée dans les WP précédents.

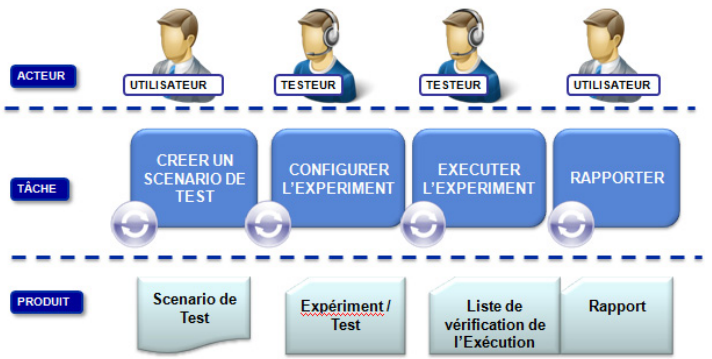
Ces activités incluent l'essai fonctionnel et l'acceptation du produit, ainsi que les exercices de simulation pour l'échange d'informations entre les utilisateurs de la plateforme afin d'expérimenter e démontrer les cas simulés, l'échange d'informations sur la découverte des vulnérabilités, les alertes et les alarmes de sécurité et pour notifier les incidents de sécurité.

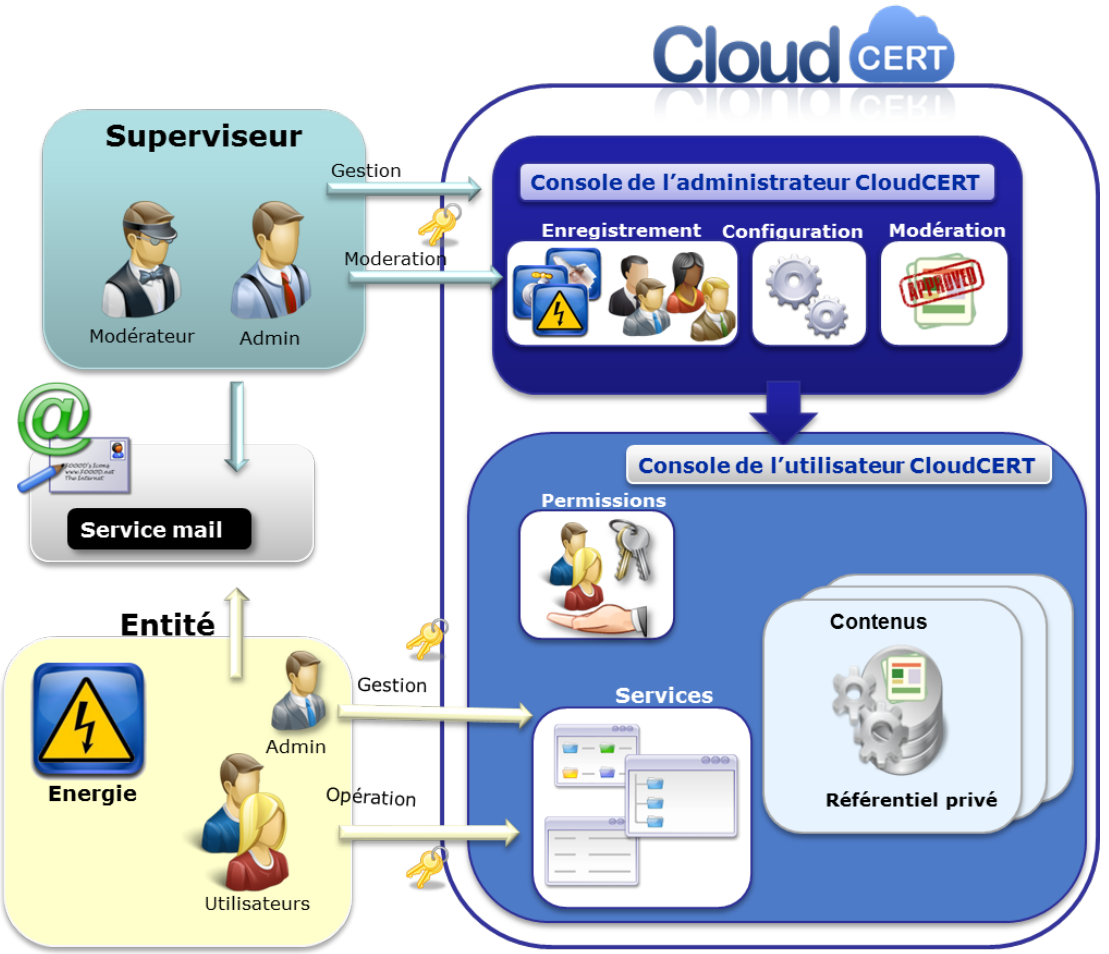


L'objectif de l'évaluation et de l'expérimentation est d'utiliser l'expérimentation par scenario comme une base pour évaluer la contribution de la solution de la plateforme CloudCERT pour améliorer la collaboration et la coopération entre les acteurs de PIC dans le partage des informations concernant la cyber-sécurité et ainsi testant la fonctionnalité et les flux de travail disponibles pour la communication à instaurer.

L'objectif de l'évaluation fondée sur les résultats de l'expérimentation, est de:

- tester CloudCERT (si les procédures de partage des informations sont supportées correctement);
- vérifier de quelle façon CloudCERT adresse les défis et les besoins du domaine en termes de collaboration et coopération;
- et évaluer les améliorations potentielles en matière de PIC permises par CloudCERT.





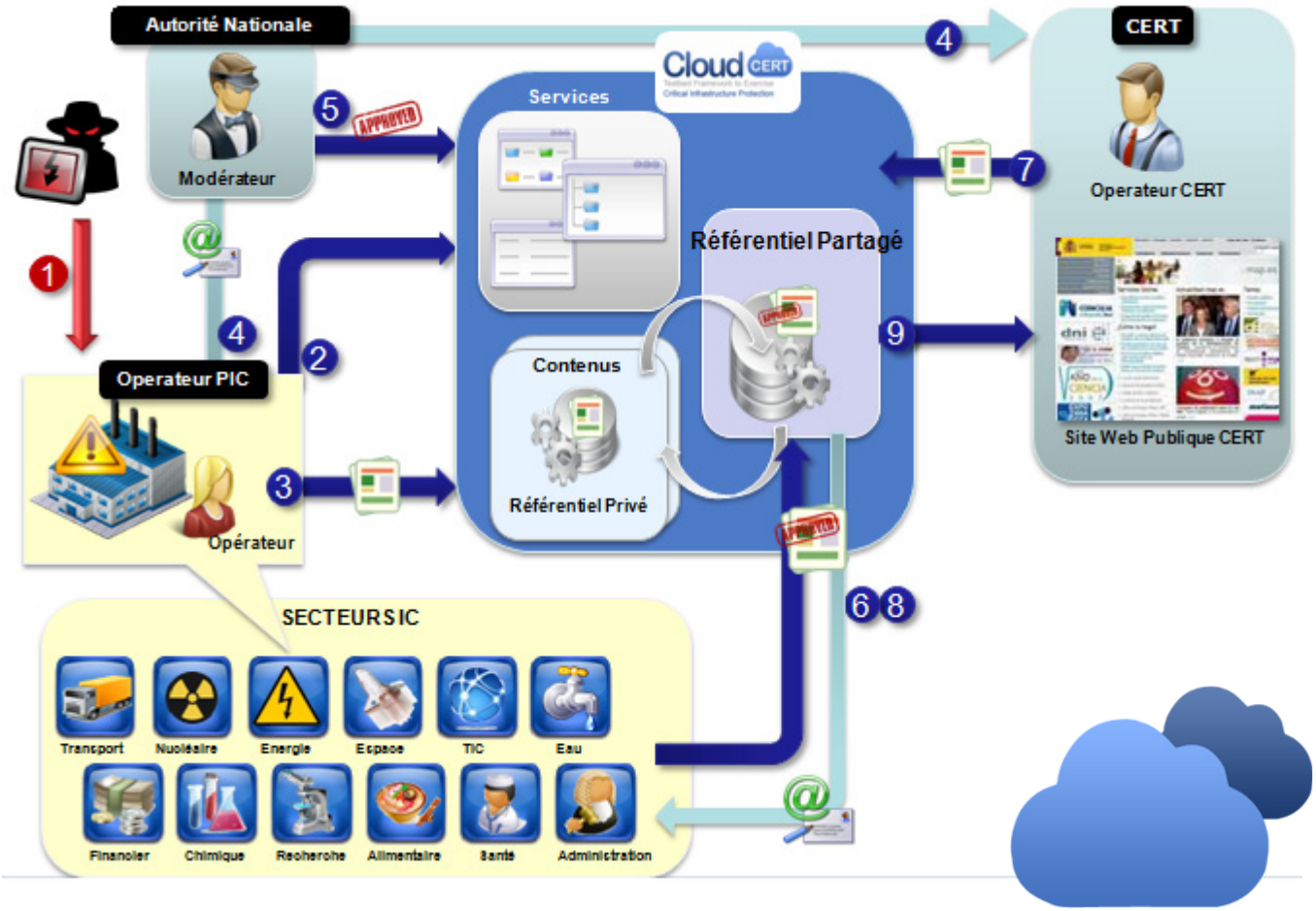
OUTILS POUR L'EXPERIMENTATION

- **Console d'Administration CloudCERT.** permet l'entière gestion des fonctionnalités de la plateforme CloudCERT.
- **Console de l'Utilisateur CloudCERT**. Facilite la création, l'implémentation et l'opération de nouvelles entités pour faire face aux incidents de sécurité.
- **Outil de client mail.**

ACTEURS

- Utilisateur –Operateur d'IC.
- Administrateur – Operateur d'IC.
- Modérateur. – CERT / Autorité
- Administrateur.- Autorité

EXEMPLE DE SCENARIO DE CAS D'UTILISATION



1. L'operateur détecte une vulnérabilité dans un produit et une intrusion sur le réseau interne.

2. Il cherche des informations et lit la procédure de Gestion des Incidents dans le wikiCIP.

3. Il crée une alerte et des post dans le Forum.

4. Système officiel de signalisation des incidents.

5. CNPIC valide l'alerte.

6. et **8.** Alerte visible sur CloudCERT et par courrier électronique à travers le bulletin.

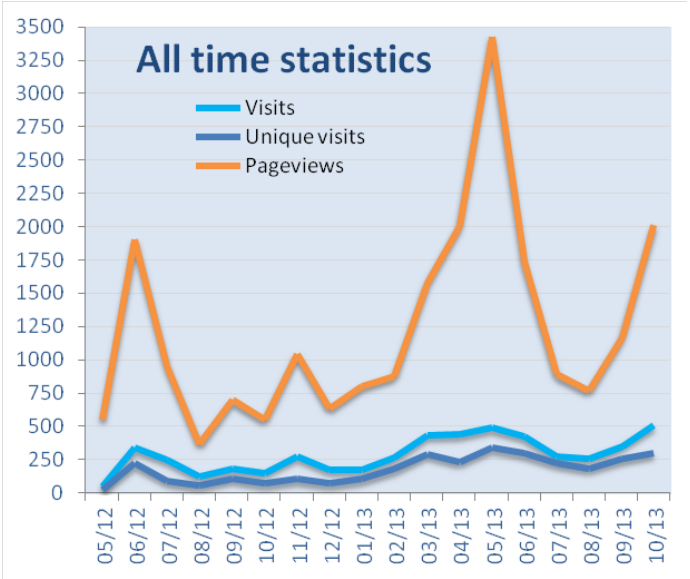
7. CERT résout l'alerte et supprime le post sur le Forum par une solution de contournement.

9. L'alerte est publiée dans un site web externe.

WP7. DISSEMINATION DES RESULTATS DU PROJET

Les indicateurs les plus pertinent du site web du projet CloudCERT **http://cloudcert.european-project.eu/** :

- Plus que **200** news publiées.
- Plus que **5.000** visites (reçues).
- Plus que **40** ressources partagées.
- Plus que **22.000** visualisations de la page (accumulées).



WIKIPEDIA

- Anglais: http://en.wikipedia.org/wiki/CloudCERT
- Espagnol: http://es.wikipedia.org/wiki/CloudCERT
- Italien: http://it.wikipedia.org/wiki/CloudCERT

EVENEMENTS

2012

- CRITIS12 Conférence sur la Sécurité des infrastructures critiques d'information. http://critis12.hig.no/

2013

- Semaine d'innovation des Jeunes Chercheurs
- 8ème atelier CERT ENISA.
- Protection des infrastructures critiques – Télécommunications.

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Cloud CERT
Testbed Framework to Exercise Critical Infrastructure Protection

Keywords	CERT, CSIRT, Critical Infrastructure Protection (CIP), Critical Infrastructure (CI), Information Sharing, Infrastructure Security
Funding Agency	European Union
Project Type	4rth Annual Work Programme adopted under the Council Decision No 2007/124/EC, Euratom, of Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007–2013" as part of the General Programme on "Security and Safeguarding Liberties".
Reference	HOME/2010/CIPS/AG/20

FINANCIADO POR LA UE

Innova.- Inteco publica la web del proyecto 'Cloud Cert' sobre protección de infraestructuras críticas

LEÓN, 14 Jun. (EUROPA PRESS) -

El INTECO presenta la web de un consorcio europeo en defensa de las infraestructuras críticas

PROYECTOS

Cloud CERT de INTECO: innovación internacional para la seguridad de las Infraestructuras Críticas

La Comisión Europea seleccionó el proyecto Cloud CERT del Instituto Nacional de Tecnologías de la Comunicación (INTECO), dirigido a desarrollar una plataforma para ejercicios específicos de cooperación en la seguridad de las infraestructuras críticas en la Unión Europea. El Instituto pondrá en valor la experiencia de INTECO CERT en esta materia, los estándares de comunicación segura, y otros desarrollos que ha llevado a cabo relacionados con la seguridad en las infraestructuras críticas. INTECO será el líder del proyecto, que tendrá una duración de dos años y un presupuesto estimado de 454.952,73 euros. Del consorcio también forman parte CNPIC (ES), Indra (ES), Zanasi Alessandro Srl. (IT), Europe for Bussiness Ltd (UK), ICSA (IT), y como asociado Theodore Puckas Foundation (HU).

Raúl Rivas / Ignacio Cano

CONFERENCE FINALE

Conférence finale de CloudCERT pour disséminer les résultats du projet Européen auprès du public cible.

- **Date:** 22 novembre 2013.
- **Lieu:**
  - Secrétariat d'État Espagnol aux télécommunications et à la société de l'information (SETSI). Madrid (Espagne)
- **Public cible:**
  - Parties prenantes du projet CloudCERT.
  - Opérateurs espagnols des Infrastructures critiques y compris les principaux fournisseurs et vendeurs.
  - D'autres CERT Européens et équipes d'application de la loi impliquées dans la PIC.
- **Admission:**
  - Admission gratuite sur invitation et vidéotransmission en direct http://www.cloudcert.webcastlive.es.


Spain, 22 November 2013

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Publication date: 28.10.13
Subject: CloudCERT final conference

Final Conference of CloudCERT European Project to Present Results Achieved

The CloudCERT European Project, which is co-financed by the European Union (E.U.) and whose project consortium is co-ordinated by INTECO, is holding its **Final Conference on 22 November at the Spanish Secretariat of State for Telecommunications and the Information Society (SETSI) in Madrid.** The conference will present the results obtained during the execution of the project (2012 to 2013), demonstrating the CloudCERT platform for sharing cyber-security information that it has produced, as well as the various other deliverables generated by the project.

The CloudCERT Project provides a test-bed environment for the exchange of information on Critical Infrastructure Protection (CIP) and its security aspects, enabling co-operation and co-ordination of the agents involved so as to manage cyber-risk-critical assets effectively.

The EU has supported this project financially through the specific programme entitled "Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks", falling within the "Security and Safeguarding Liberties" framework programme.

The project consortium is made up of the National Institute for Communication Technologies (INTECO), a company dependent upon the Ministry of Industry, Energy and Tourism (MINETUR) through the Secretariat of State for Telecommunications and the Information Society (SETSI) (Spain) **as project co-ordinator**, together with the National Centre for Critical Infrastructure Protection (CNPIC) of the Ministry of the Interior (Spain), Indra (Spain), ZANASI and Partners (Italy) , Europe for Business Ltd. (United Kingdom) and the ICSA Foundation (Italy).


CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

Conference

Agenda

09h00 Registration

09h30 Welcome reception

10h00 CloudCERT project:
- Background of the project.
- Project objectives and motivation.
- Project results and main deliverables.

11h15 Coffee Break

11h45 CloudCERT Pilot:
- Exchanging critical infrastructure information security.
- Demo.

13h00 Next steps for the project and Closing remarks

22/11/2013

SOLUTION TECHNOLOGIQUE

PLATEFORME COLLABORATIVE

CLOUDCERT POURRAIT-IL ETRE INTERESSANT POUR VOUS?

- Si votre organisation est un **operateur CERT ou IC**, vous pouvez utiliser cette plateforme pour gérer les incidents des infrastructures critiques et partager des informations sur la cyber sécurité.
- Si la configuration de votre organisation comme **CERT ou Autorité** inclut des **operateurs d'infrastructures critiques**, vous pouvez avoir une plateforme personnalisée pour fournir des services et des outils pour votre système de protection des infrastructures critiques (forum, wiki, etc.).
- Si votre organisation doit interagir avec les **Autorités Nationales pour la Protection des Infrastructures Critiques**, et en fonction de ses compétences nationales, vous pouvez attribuer le rôle le plus convenable dans la plateforme: coordination, supervision, participation, etc.

CONTENUS

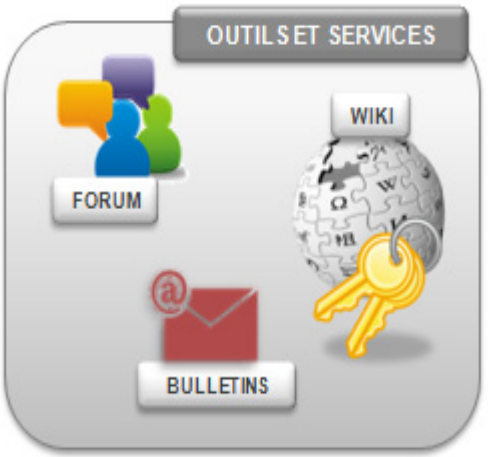
La plateforme CloudCERT vous permet de créer et diffuser des contenus sur la sécurité, notamment:

- Notes.
- News.
- Alertes.
- Virus.
- Vulnérabilités.
- Produits RSS.

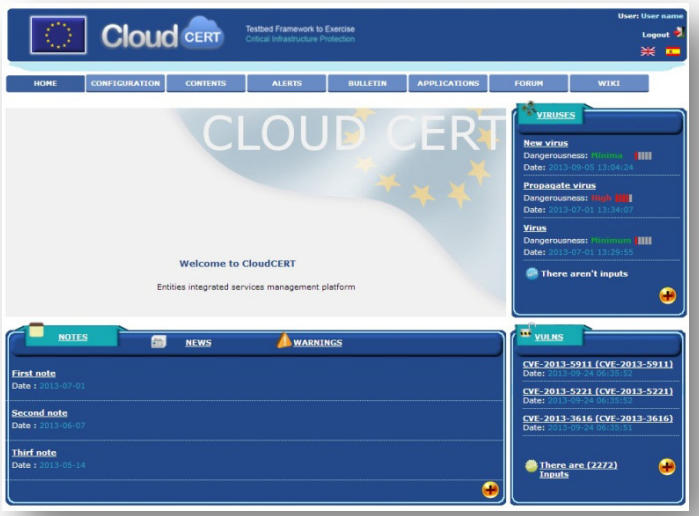
SERVICES ET OUTILS

La plateforme CloudCERT permet aux utilisateurs de partager des informations afin de prévenir les incidents de sécurité par ses services:

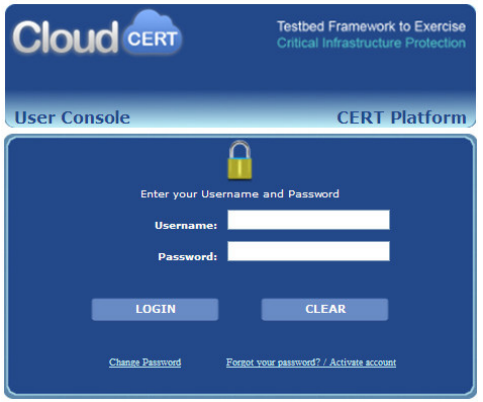
- Forum.
- WikiCIP.
- Bulletin d'information.



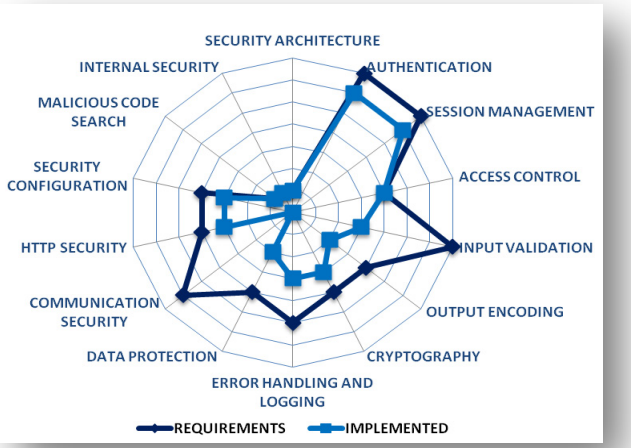
FICHE DU PRODUIT



- **Plateforme collaborative** pour gérer un référentiel partagé d'informations de cyber sécurité en coopérant d'une façon efficace.

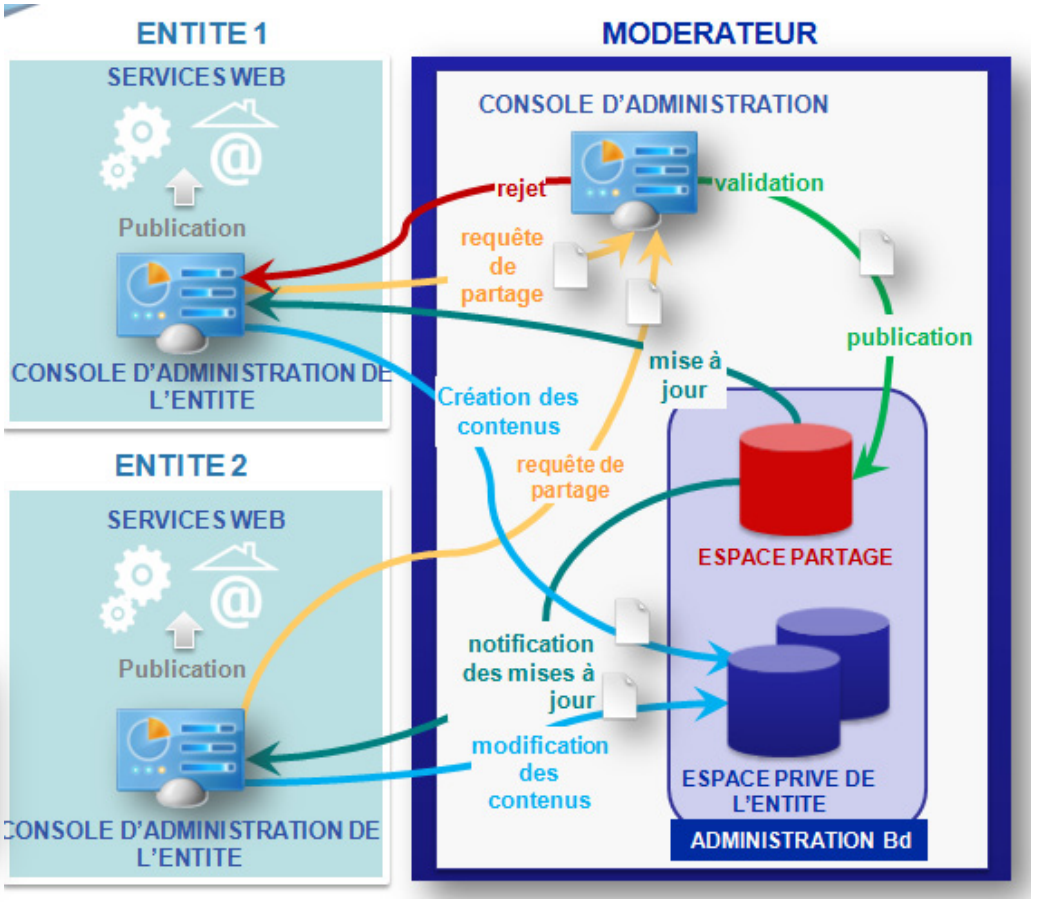


- Paradigme **Cloud** fondé sur des **référentiels partagés** et privés.
- Application **multilingue** et interface de traduction des contenus.
- **Services** personnalisés (établis par contracte).
- Plateforme **extensible** permettant l'intégration de nouveaux contenus, services, outils et flux de travail.
- **Environnement sécurisé**:
  - Mécanisme d'authentification basé sur nom d'utilisateur et mot de passe: Service Central d'Authentification (Central Authentication Service - CAS).
  - Autorisation basé sur des droits d'accès et rôles.
  - Gestion sécurisée des sessions.
  - Garantie de confidentialité et de protection des données.



CYCLE DE VIE DES CONTENUS

- CloudCERT permet la création et **mise à jour** des contenus (informations structurées) de façon collaborative.
- Chaque entité garde les contenus dans son **espace privé** et peut demander de partager les informations.
- Un modérateur révise les contenus à publier dans un **référentiel partagé**.
- Les entités peuvent **sauver** leurs contenus à publier sur des outils externes (tels que les intranets).

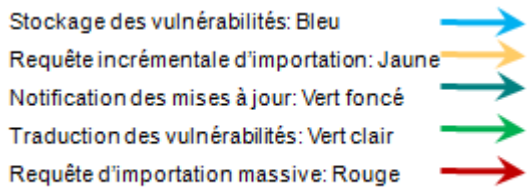


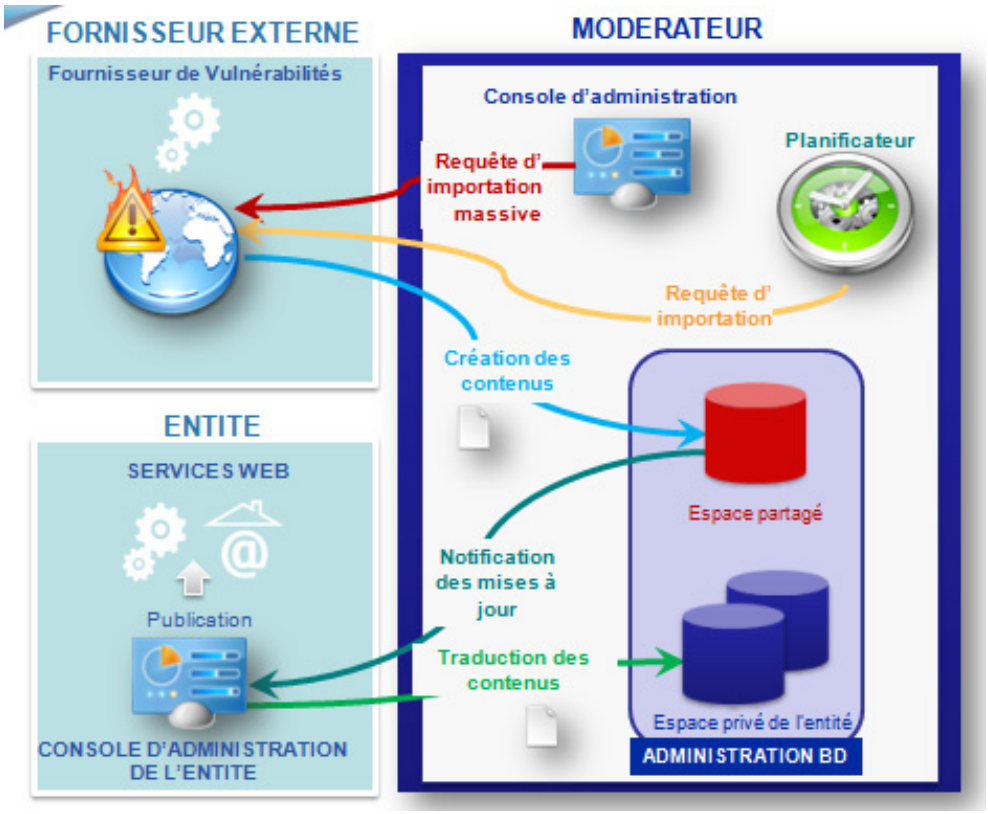
Les contenus peuvent se trouver dans un des états suivants pendant leur cycle de vie:

- Créés.
- Modifiés.
- Partagés.
- Mis à jour.
- Validés.
- Rejetés.

CYCLE DE VIE DES VULNERABILITES

- Les vulnérabilités sont un type spécifique de contenu fourni par des **sources externes** (par exemple le NIST).
- Un mécanisme ordonné **importe** automatiquement les vulnérabilités dans le système.
- Le modérateur peut aussi **requérir une importation massive** (pendant une période de temps) dans le système.
- Les entités peuvent **traduire les vulnérabilités** dans leur espace privé.





Donc, une vulnérabilité peut se trouver dans un des états suivants pendant son cycle de vie:

- Importée.
- Notifiée (mise à jour).
- Traduite.

WIKICIP

Un wiki est un système flexible permettant à l'administrateur de définir des hiérarchies de pages. WikiCIP permet de maintenir des **contenus non structurés** de façon collaborative, en mettant à disposition les éléments structurels suivants:

- **Index** – Page de l'index affichant des liens à de différentes pages wiki ayant un sujet semblable.
  - **Page** – Pages individuelles concernant un sujet spécifique.

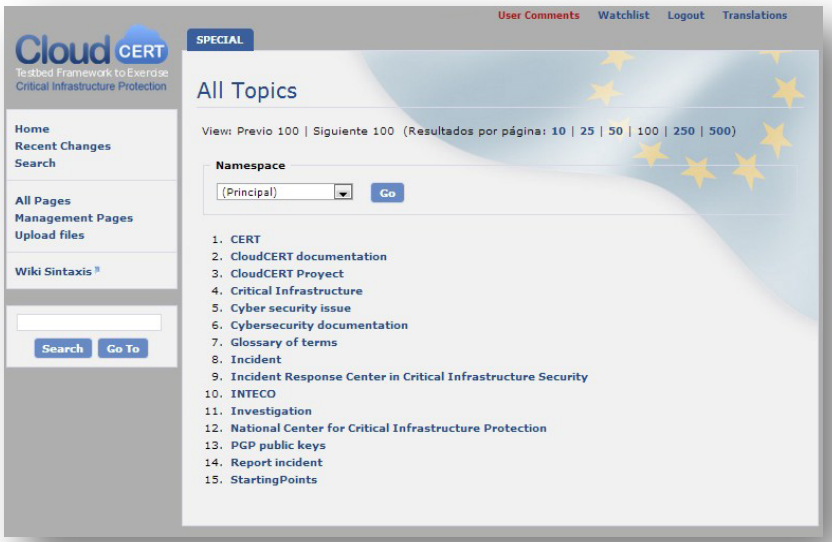
Les sujets dans le WikiCIP sont structurés de la façon suivante:

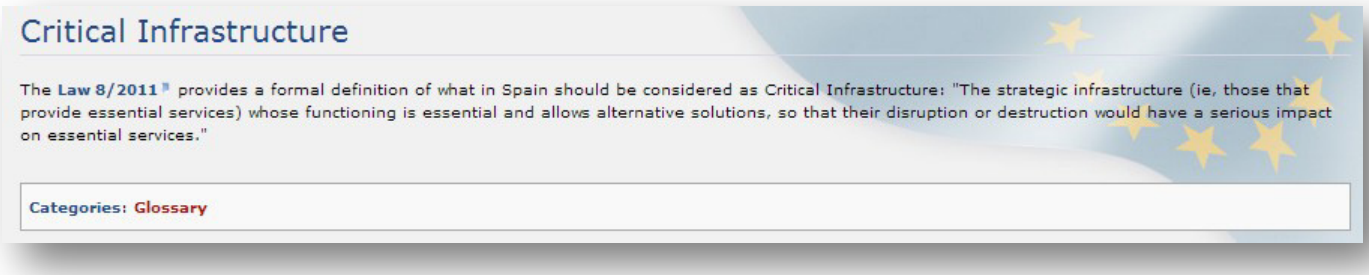
Documentation CloudCERT:

- Présentation générique du projet et des ressources principales.
  - Manuel de l'utilisateur.
  - Manuel de l'administrateur.
  - Manuel du développeur.

- **Documentation sur la cyber sécurité**:
  - Procédure opérationnelle pour faire face aux incidents de cyber sécurité.
  - Cadre juridique.
  - Liens intéressants sur la PIC.

- **Glossaire.** Les vocables principaux relatifs à la Protection des Infrastructures Critiques.





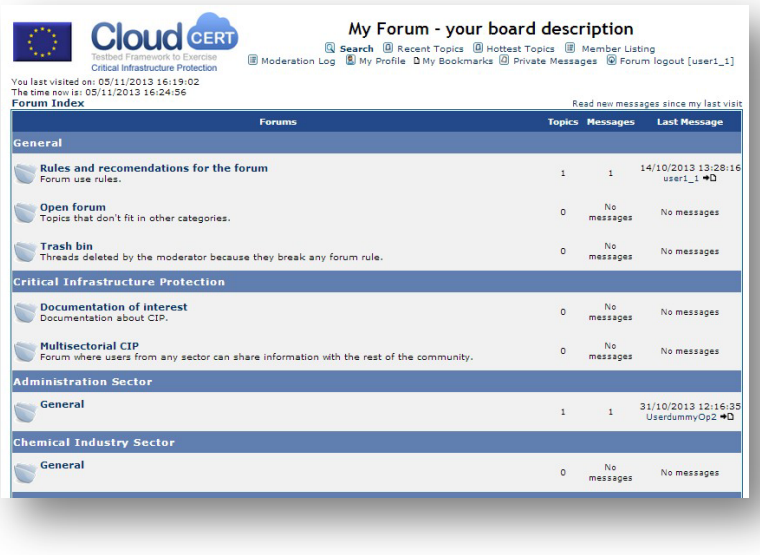
FORUM

Le service de forum permet l'échange d'informations non structurées avec les suivants éléments de groupement disponibles:

- **Catégorie**. Représente le sommet de la hiérarchie et est généralement utilisée pour rassembler de différent forums associés. C'est un group logique, et chaque forum dans une catégorie à son cycle de vie.

.

  - **Forum**. Un forum est un ensemble de fils de discussion concernant le même sujet.
    - **Fil de discussion ou Topic**. C'est la discussion elle-même, les messages par les utilisateurs concernant un sujet spécifique.



Le Forum CloudCERT inclut les catégories suivantes:

- **Général**. Forums contenant des informations générales.
- **Protection des Infrastructures Critiques**. Un espace où les utilisateurs peuvent discuter et partager des informations générales sur la protection des infrastructures critiques avec le reste de la communauté.
- Chaque operateur des infrastructures critiques a un forum réservé à son **secteur** (selon la classification juridique nationale Espagnole de PIC) où les utilisateurs peuvent partager les informations avec d'autres acteurs pertinents dans ce secteur.

  - Administration.
  - Espace.
  - Industrie nucléaire.
  - Industrie chimique.
  - Services d'investigation.
  - Eau.
  - Energie.
  - Santé.
  - Technologie de l'Information et de la Communication (ICT).
  - Transports.
  - Secteur alimentaire.
  - Système Financier et Fiscal.

BULLETINS D'INFORMATION

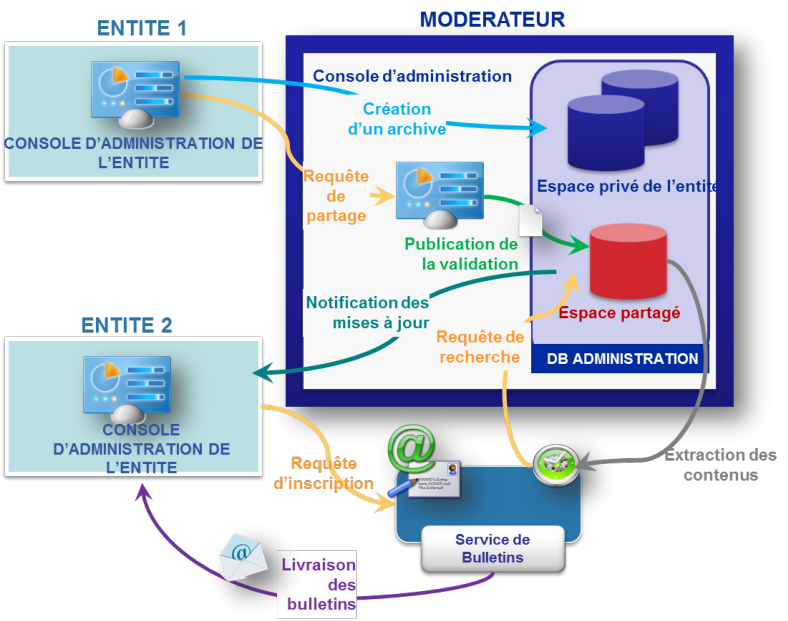
Le Service de Bulletin d'information est un service externe communiquant avec la Plateforme CloudCERT pour **recevoir les inscriptions des utilisateurs** et **accéder aux contenus de sécurité stockés** dans les bases de données CloudCERT pour créer les bulletins. Le service de bulletins est responsable de la création et du formatage des bulletins, et de la livraison des bulletins aux utilisateurs finaux selon leurs préférences.

Chaque entité CloudCERT enregistrée peut inscrire des utilisateurs (déjà enregistrés ou externes) à de différents bulletins de sécurité, pour recevoir les bulletins périodiquement dans leur boîtes mail.

L'inscription peut être élaborée par l'administrateur de l'entité ou par l'utilisateur final.

- Le service de bulletins permet aux utilisateurs d'être informés sur la mise à jour des contenus à travers une notification par courrier électronique.
- Pour sélectionner le type de bulletin et les contenus il faut suivre un processus d'inscription.
- Le service de bulletins rassemble les contenus, crée les bulletins personnalisés et les distribue à tous les utilisateurs finaux.

Création des contenus : Bleu
Requêtes: Jaune
Notification des mises à jour: Vert Foncé
Validation de la requête: Vert clair
Requête d'importation massive: Rouge
Extraction des contenus pour la création de bulletins: Gris
Livraison des bulletins: Violet



CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

CloudCERT - Système de banc de test pour exercer la protection des infrastructures critiques.

HOME/2010/CIPS/AG/20.
Avec le support financier du Programme pour la Prévention, Préparation et Gestion des conséquences en matière de Terrorisme et autres Risques liés à la Sécurité - Commission Européenne - Direction générale Justice, Liberté et Sécurité