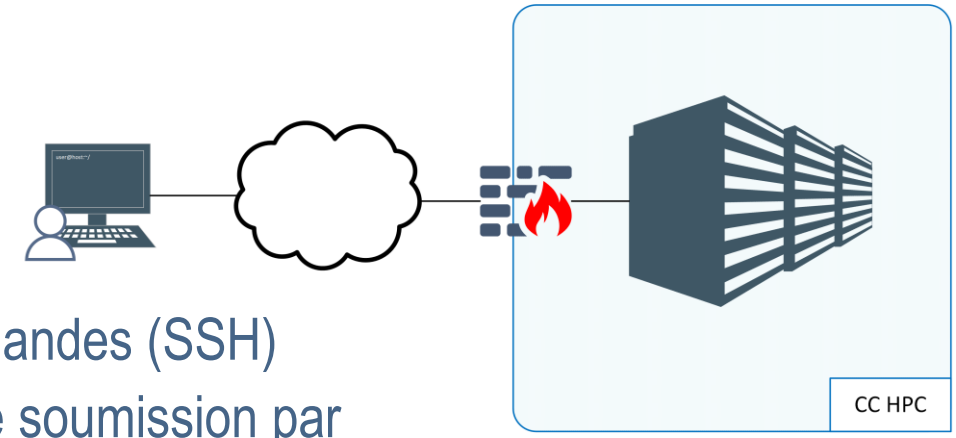
Forum ORAP #43

Chaînes de traitements automatiques et sécurité
Quels enjeux ?

Ludovic Billard – CNRS/IDRIS – 19/03/2019

Point de vue d'un CC FR : l'IDRIS



Historique IDRIS

- Approche traditionnelle de soumission en ligne de commandes (SSH)
- Quelques projets incluant une soumission par portails (hébergés et/ou administrés) ou l'utilisation de *middlewares*
- Modèle de sécurité défini et robuste

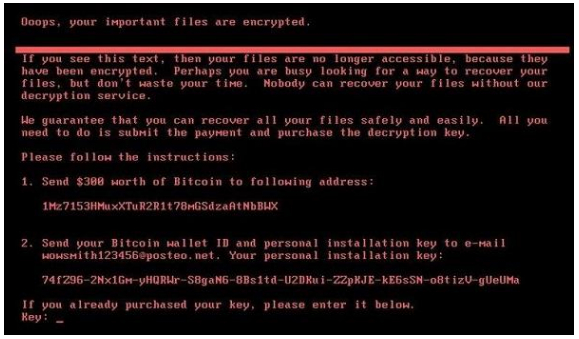
Pour tout projet

- Démarche systématique d'analyse de risques
- Conformité PSSI-E, PSSI-C, RGPD, PPST
- Valorisation des actifs selon les besoins de sécurité : Disponibilité, Intégrité, Confidentialité et Traçabilité, identification des vulnérabilités, menaces et scénarios d'attaques.

Quels risques pour les CC ?

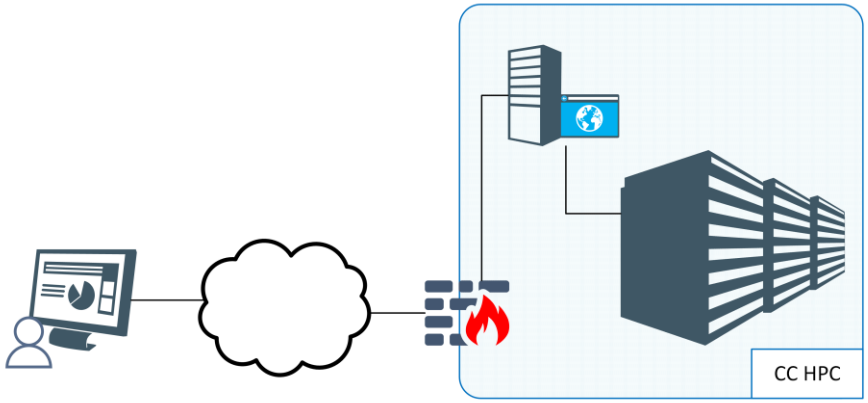
Compromission des éléments du calculateur ou utilisation frauduleuse des ressources du centre ayant comme conséquences

- Atteinte à l'image du centre / tutelle / partenaire
- Juridique : RGPD, engagements contractuels
- Scientifique : altération des résultats de recherches ou vol de résultats
- Perte financière : indisponibilité des ressources, coût de remise en MCO/MCS du centre, pénalités contractuelles, brevets



Approche portail et/ou *middleware*

Induit de nouvelles problématiques de sécurité car augmente la surface d'attaque :



- Qui héberge la ressource de soumission ? (disponibilité, gestion des accès)
- Qui l'administre ? (intégrité, disponibilité, risques induits par une erreur d'administration)
- Moyens et contrôles d'accès ? (confidentialité, PPST, comptes)
- Vulnérabilités de l'application et de sa pile logicielle ? (intégrité, disponibilité, attaque par rebond)
- Sécurité de l'agent de soumission

Questions relatives aux données

De plus, la nature des données manipulées est à prendre en compte

- Conformité RGPD ? Attention aux données personnelles, sensibles, médicales, de santé !
- Besoin de disponibilité ? (localisation et moyens de stockage)
- Besoin d'intégrité ? (somme de contrôle)
- Besoin de confidentialité ? (chiffrement, cloisonnement)
- Besoin de traçabilité ? (imputabilité, journalisation)

Responsabilité

Qui est responsable en cas de compromission ? Engagement contractuel.

Escalade de l'information : la chaîne fonctionnelle de traitement d'incident doit être identifiée et réponse doit être adaptée selon la nature de l'incident.

Quels besoins pour les équipes sécurité ?

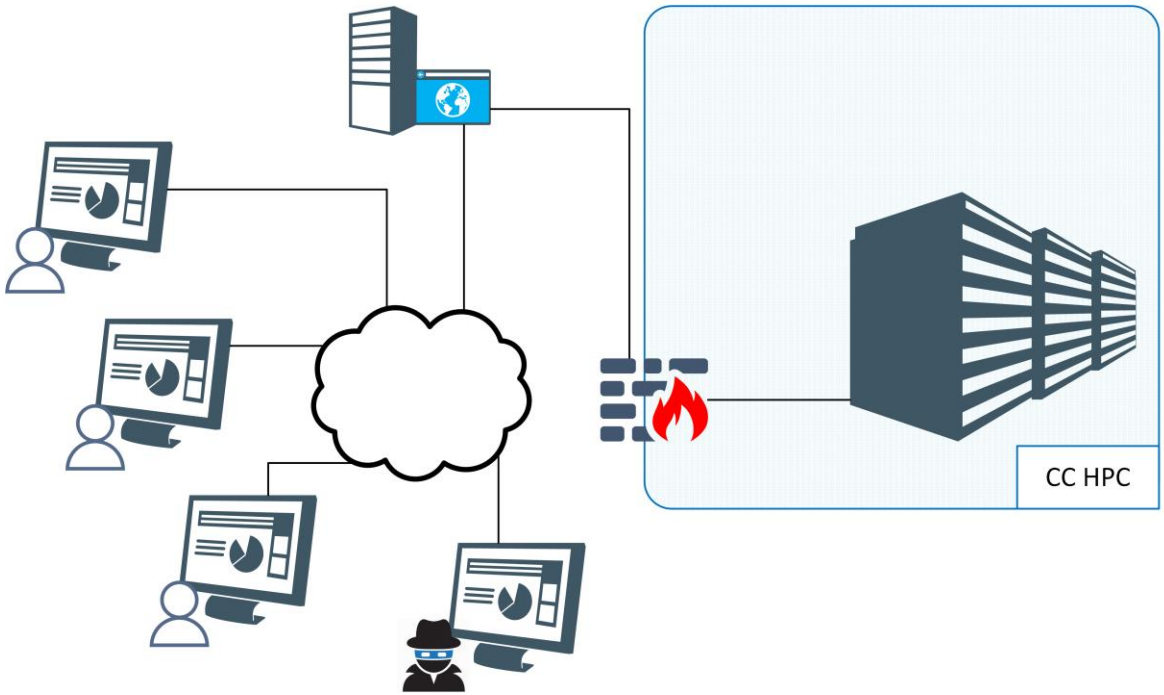
- Détection de compromission du système de soumission de travaux ?
- Détection de compromission des données ?
- Détection du types de données (sensibles, nominatives, personnelles) ?
- Détection de compromission d'un compte utilisateur ?

Enrichissement du modèle

Modèles simples : capitalisation de l'historique et de l'expérience des équipes du CC.

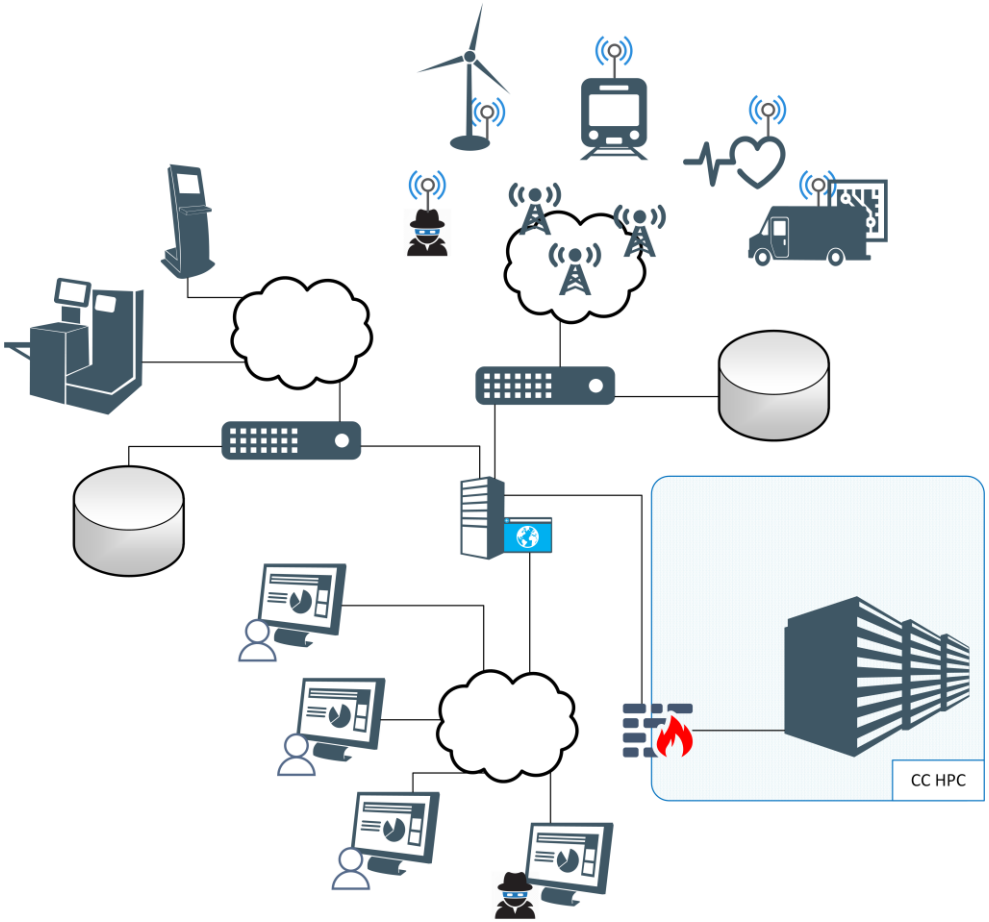
Modèle complexes : besoin de conduire une analyse de risques globale.

Attention au *aaS cloud public !!



Architecture complète

IoT, systèmes SCADA, entrepôts de données, etc. entraînent une complexité du modèle et augmentent le besoin en sécurité



Points de vigilance

- Évaluer les solutions type « boîte noire » avec équipes sécurité et fournisseur
- Limiter l'exposition des éléments
- Utilisation de *middlewares* intégrant ces composantes de sécurité « *by design* »
- Connaître la nature des données traitées

Conclusion

Objectifs des équipes de sécurité : assurer le maintien en condition opérationnelle, et de sécurité, de chaque brique en fonction des besoins :

- Mise à jour (attention aux objets connectés, capteurs, etc.)
- Sécurisation des échanges : chiffrement des protocoles, imputabilité
- Authentification (multi-facteurs)
- Traçabilité et centralisation des journaux
- Intégration avec l'impact le plus faible au sein du CC
- Audit des applicatifs mis en œuvre (OWASP)
- Mesures organisationnelles

Merci de votre attention