Risques de cyber sécurité et résilience dans les secteurs critiques

DRIDI Mohamed

Septembre 2019

Notre mission

- Sécuriser les applications nationales les plus critiques exploitées par les ministères, les municipalités et les établissements publics (telles que INSAF, RACHED, ADEB, GEC, MADANIA, Suivi des grands projets et GRB, …) ainsi que les utilisateurs de ces applications.

Introduction

- Avec la montée en puissance des menaces cybernétiques, toute organisation doit mettre en œuvre les mesures adéquates pour assurer la sécurité de :
  - son infrastructure,
  - ses systèmes
  - l'intégrité de ses données.
- dans le contexte actuel d'hyper connectivité des systèmes, il devient de plus en plus difficile de se prémunir contre les cyber attaques.
- il n'est plus question de savoir si oui ou non on pourrait être victime d'une attaque mais plutôt sommes-nous capables d'y faire face lorsqu'elle se produira tout en garantissant une reprise de l'activité dans des délais acceptables?

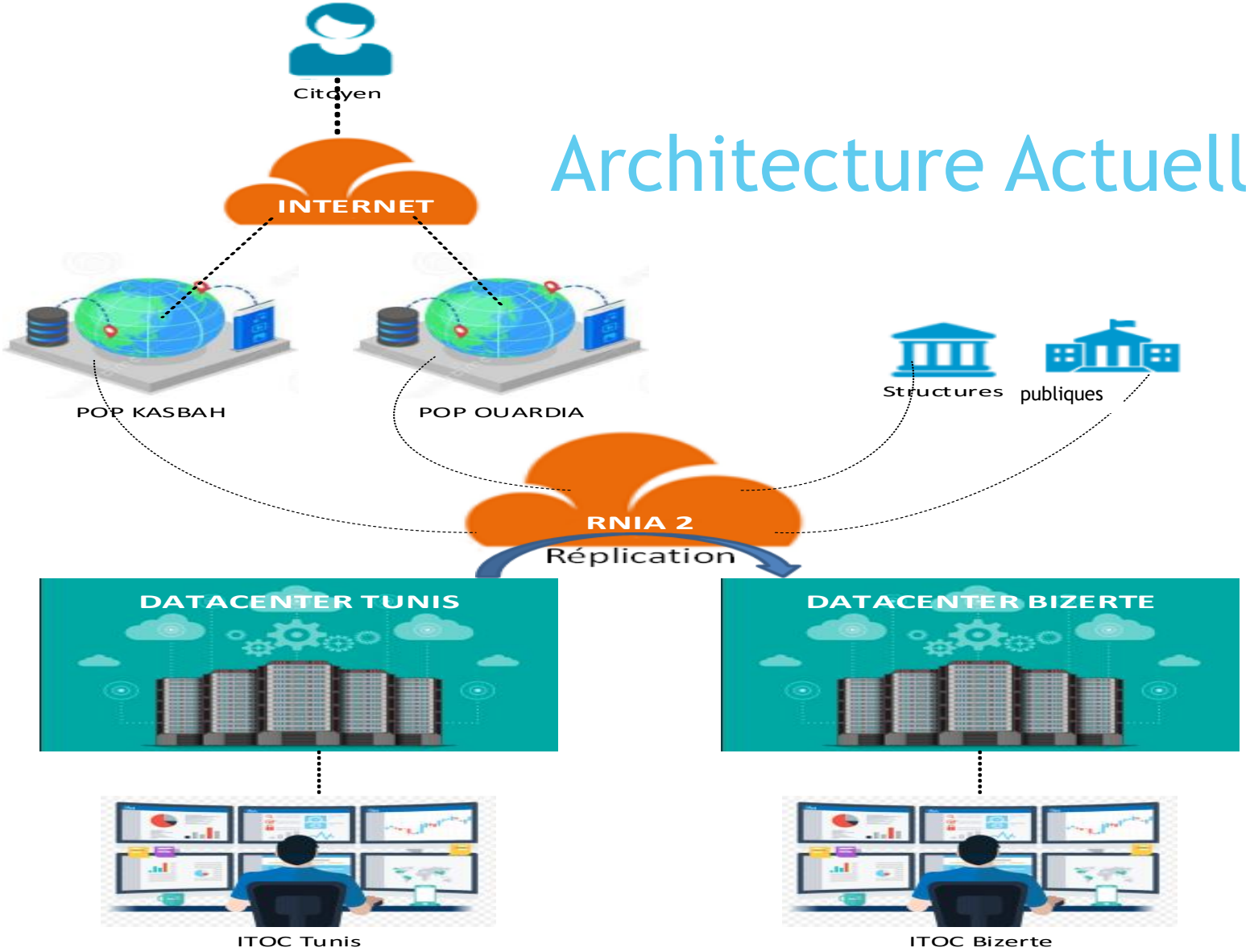
  On parle alors de cyber-résilience

Notre approche

Gérer la sécurité en adoptant une approche qui implique **les individus**, **les processus** et la **technologie** afin de renforcer les cinq piliers de la cyber-résilience :

- Identifier :par l'identification des informations essentielles à l'activité, leur emplacement, leur degré de vulnérabilité ainsi que la tolérance aux risques.
- Protéger : par la mise en œuvre de mesures de protection destinées aux infrastructures et aux services critiques afin de limiter l'impact d'une attaque.
- Détecter : par la mise en place de moyens adéquats permettant de surveiller de manière continue les événements internes de sécurité et leur mise en corrélation avec les menaces externes.
- Répondre : par la définition de procédures claires à suivre en cas d'incident et la mise en place d'équipes d'intervention avec des rôles et responsabilités prédéfinis.
- Récupérer: par la mise en œuvre de systèmes et plans appropriés pour restaurer les données et les services susceptibles d'avoir été impactés.

Architecture Actuelle



Projets réalisés / en cours

- Mise à niveau des Datacenters du CNI
- RNIA2 et RNIA3
- SOC
- Centre National de BACKUP
- Cloud Privé du CNI

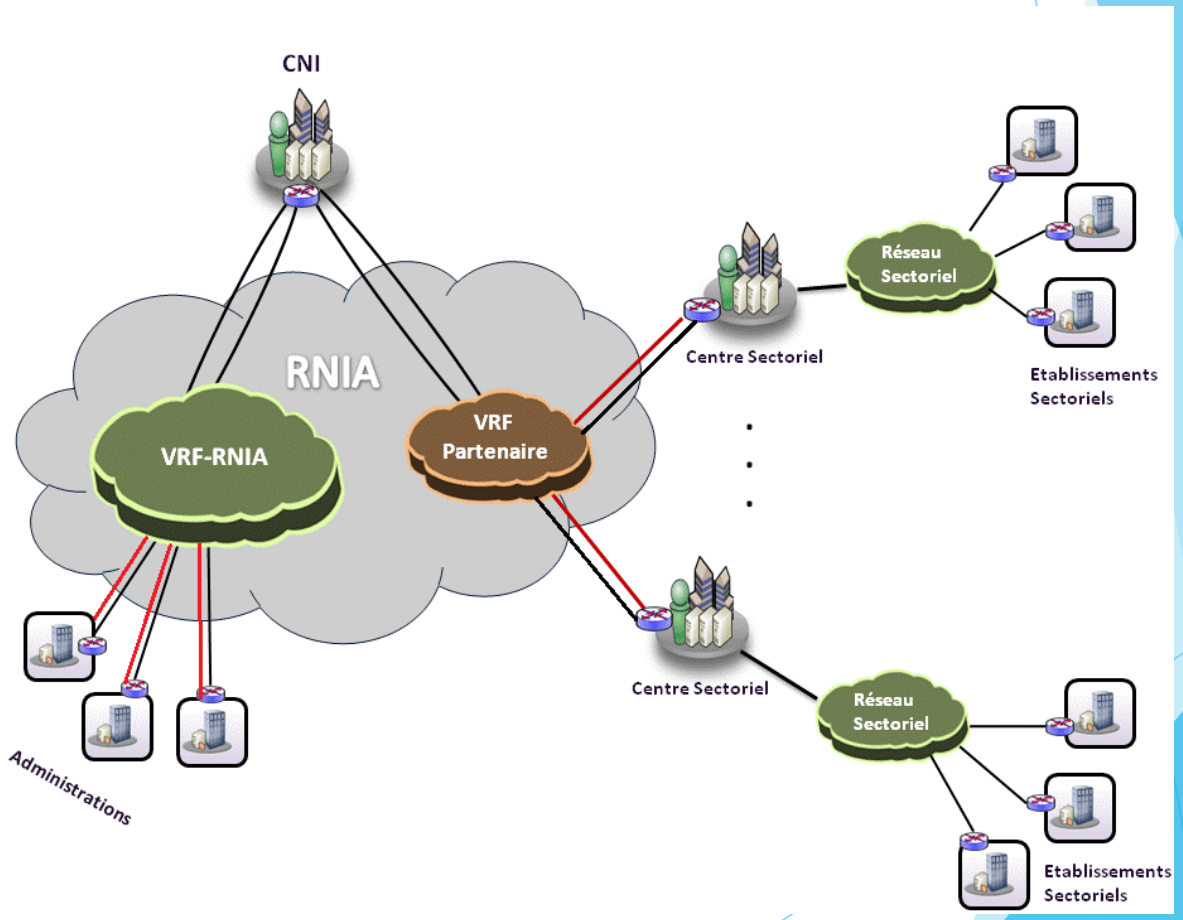
Mise à niveau des DATACENTERs du CNI

- Nouvelle architecture selon la norme TIA 942 Datacenters (Tier 3)
- Sécurité incendie
- Sécurité d’accès
- Vidéo surveillance
- Énergie (redondance)
- Climatisation (redondance)
- Câblage structuré

RNIA

La mise en place d'un réseau de transmission **sécurisé** de l'administration

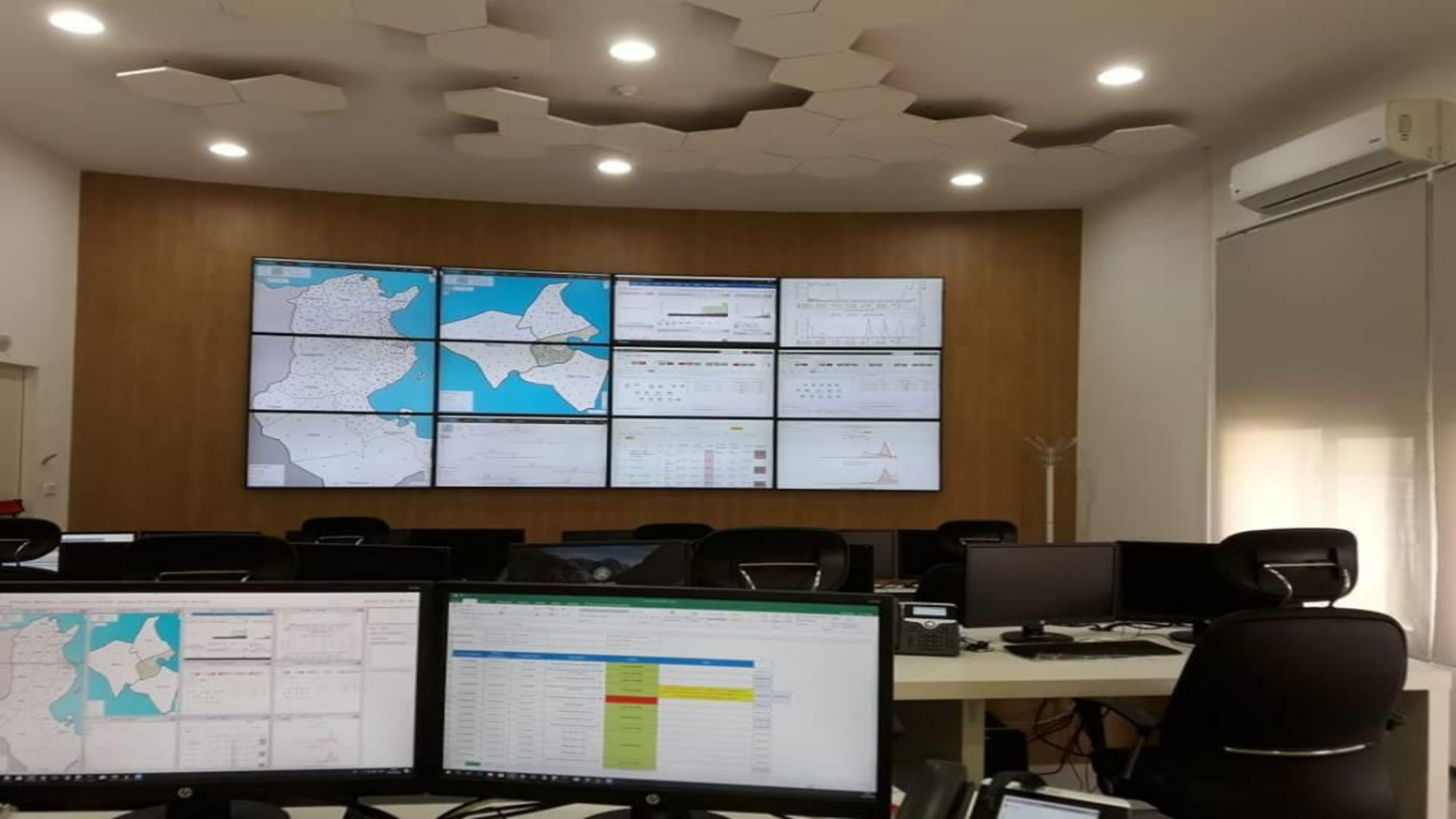
- \+ 500 sites de l'administration connectés en Fo sur MPLS
- Interfaçage avec les différents réseaux sectoriels via leurs centres informatiques(IRESA, CCK,CIMF,CIMS)
- Solution de sécurité pour chaque site (FW+IPS)
- Réceptionné 2018 en phase d'exploitation
- RNIA3 : connexion de + 600 sites en Fo sur MPLS (Gouv, Municipalités et arrondissements)
- En cours de réalisation (+ 250 migrés)
- Connexion avec le centre National de Backup à Bizerte
- Mise en place d'un centre de supervision réseau NOC au CNI et au CNBB pour la gestion de la qualité de service et le suivi des contrats SLA avec les opérateurs.



SOC

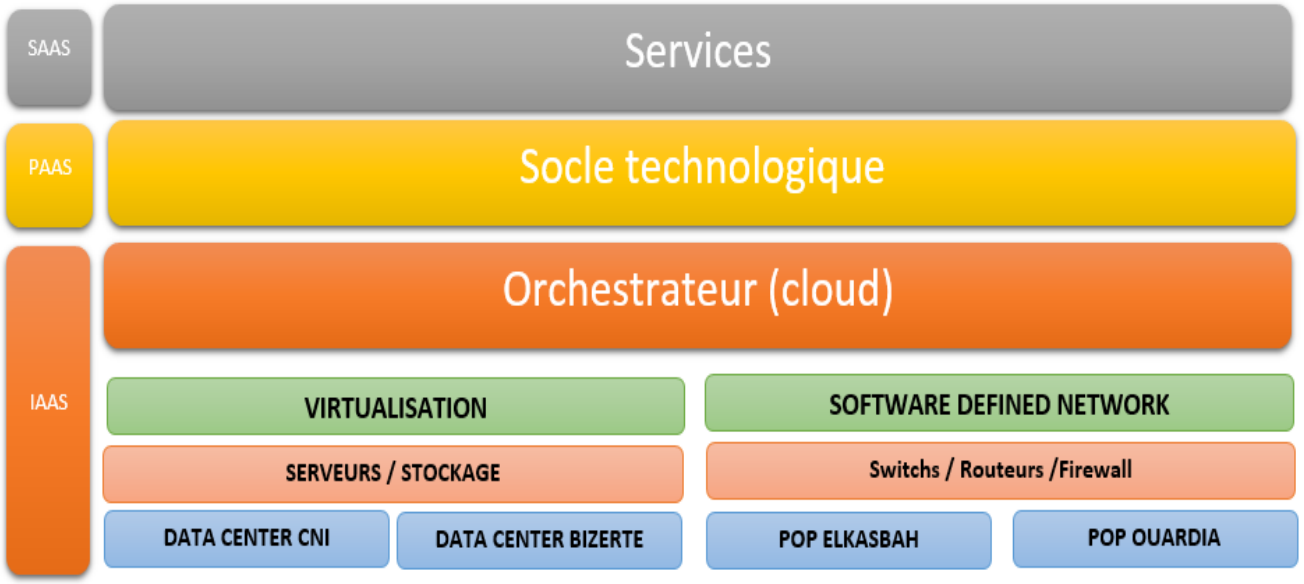
Le déploiement de Centres Opérationnels de Sécurité (SOC) au sein du CNI et de CNBB afin de se doter de capacités propres de supervision,

- Assurer la supervision du SI, la détection et la résolution des incidents de sécurité
- Rapidité du temps de réponse
- Capacité à se remettre d'une attaque en un temps raisonnable
- Identification plus rapide d'attaques potentielles et prévention desdites attaques avant qu'elles ne causent des dommages
- Le SIEM est le principal outil du SOC
  - Permet d'agréger les événements de sécurité en un point
  - Avoir une visibilité de l'ensemble du périmètre
- Evolution vers un ITOC (qui intègre la supervision réseau, sécurité, système et applications-services) en cours.
- Evolution vers un CERT gouvernemental à moyen terme.



Cloud Privé du CNI

- Avoir des Datacenters classifiables selon des critères adoptés par les normes en vigueur (local, International)
- Mutualisation des 2 Datacenters avec une répartition fonctionnelle souple.
- Automatisation des tâches d'administration
- Mutualisation des ressources entre les applications en exploitation
- Avoir une architecture orientée services « cloud ready »



Actions Planifiées

Les mesures à mettre en place pour renforcer la cyber résilience face aux menaces et aux attaques:

- Agir sur tous les projets IT en intégrant la sécurité dans le cycle de vie des projets
- Renforcer les dispositifs d'audit automatisés et proactifs de la sécurité des infrastructures, réseaux, codes sources et applications ;
- Former et sensibiliser les équipes et les utilisateurs ;
- Renforcer la gouvernance de la sécurité à travers la mise en place d'un SMSI et la certification ISO 27001
- Faire évoluer notre SOC vers un Cert-Gouvernemental pour assurer la **Coordination** avec les autres entités (hors du domaine d'action) : opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux
- Fédération et Gestion d'identité pour tous les applications du CNI.

MERCI DE VOTRE ATTENTION