Externalisation du SI

Enjeux et référentiels pour la maîtrise des sous-traitants

Aurélien LETEINTURIER

Chef du bureau Qualification et Agrément (ANSSI)

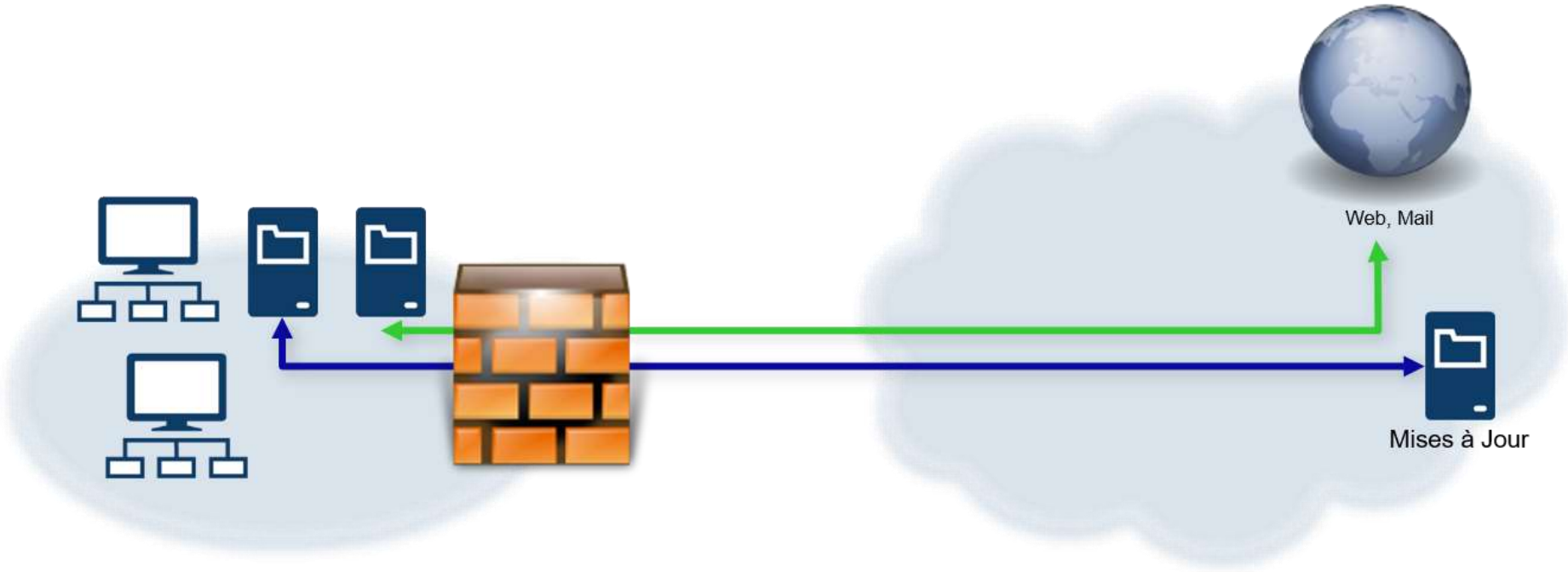
Plan

- Historique de l’externalisation
- Menaces, risques et acteurs
- Référentiels et pratiques

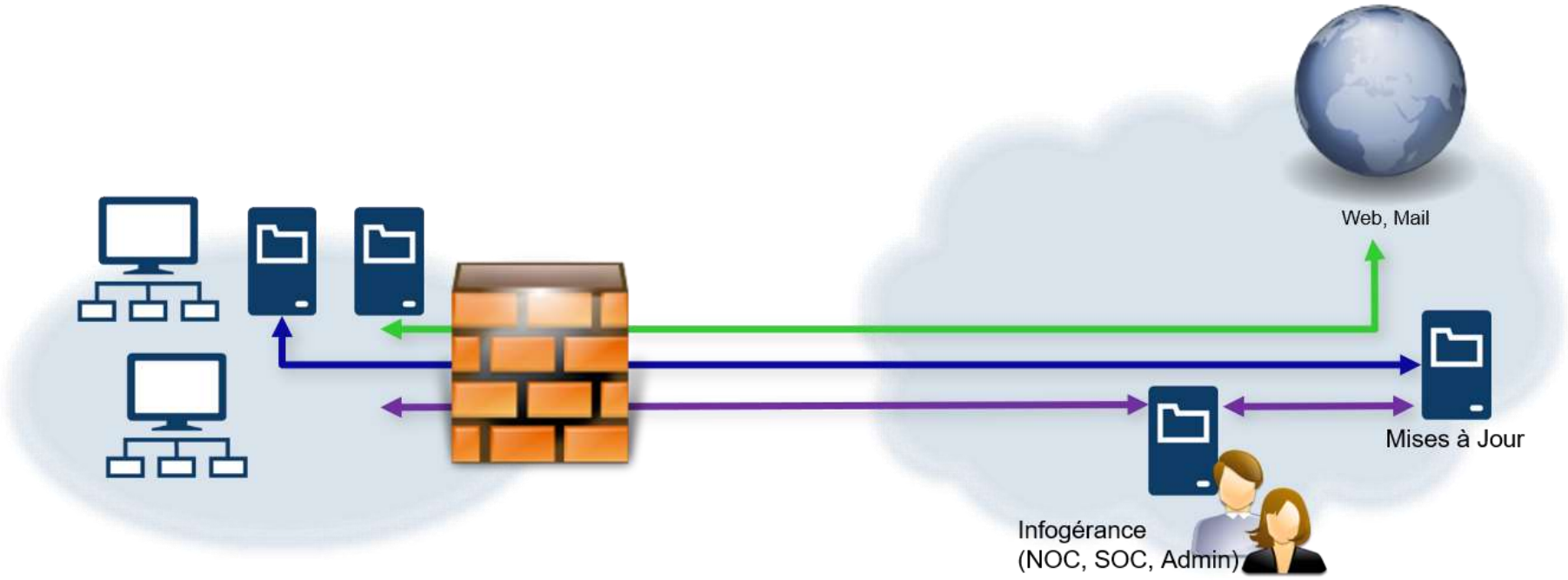
Plan

- **Historique de l'externalisation**
- Menaces, risques et acteurs
- Référentiels et pratiques

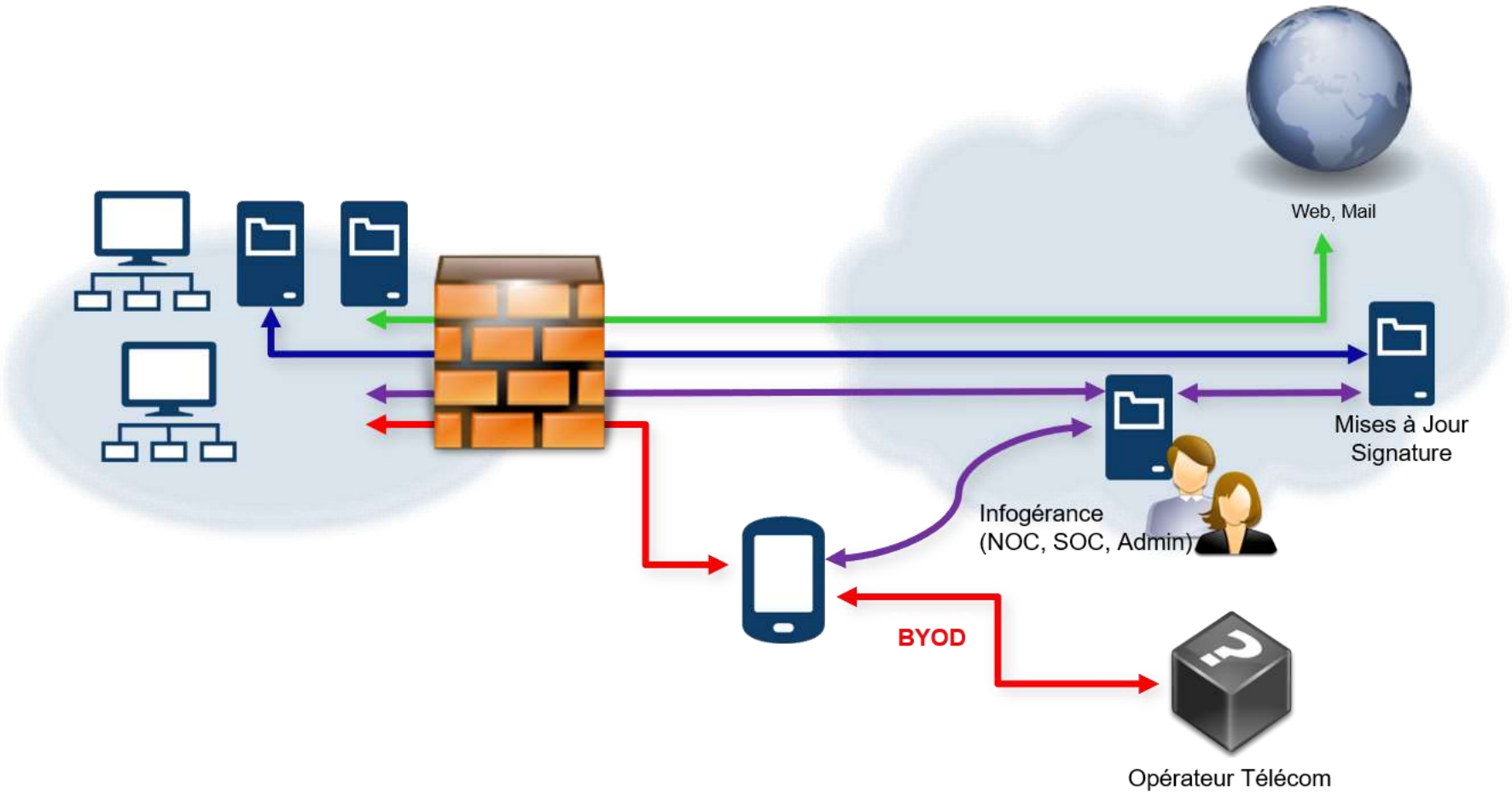
Ouverture de l'infrastructure



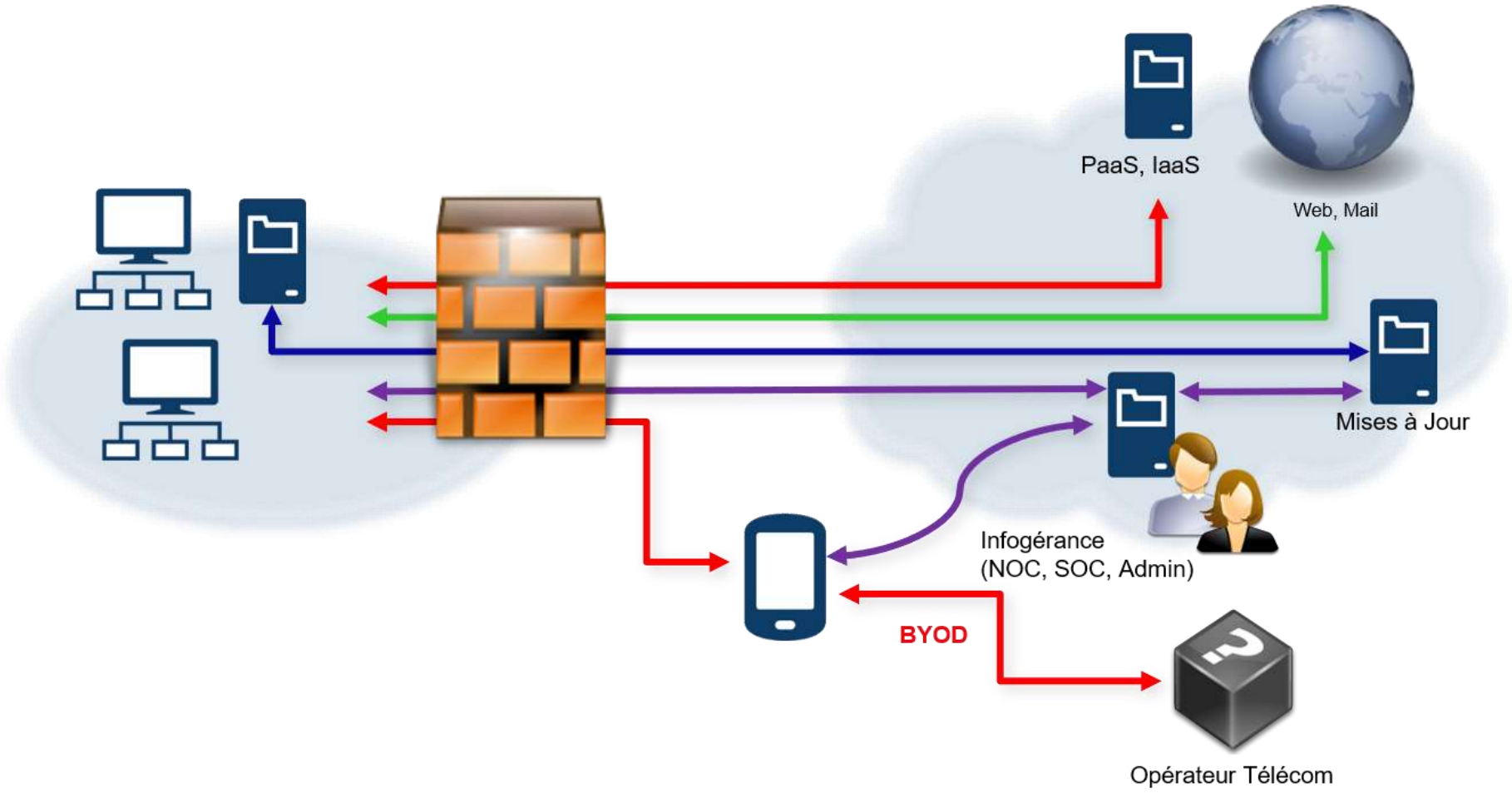
Ouverture pour l'infogérance



Ouverture vers la mobilité

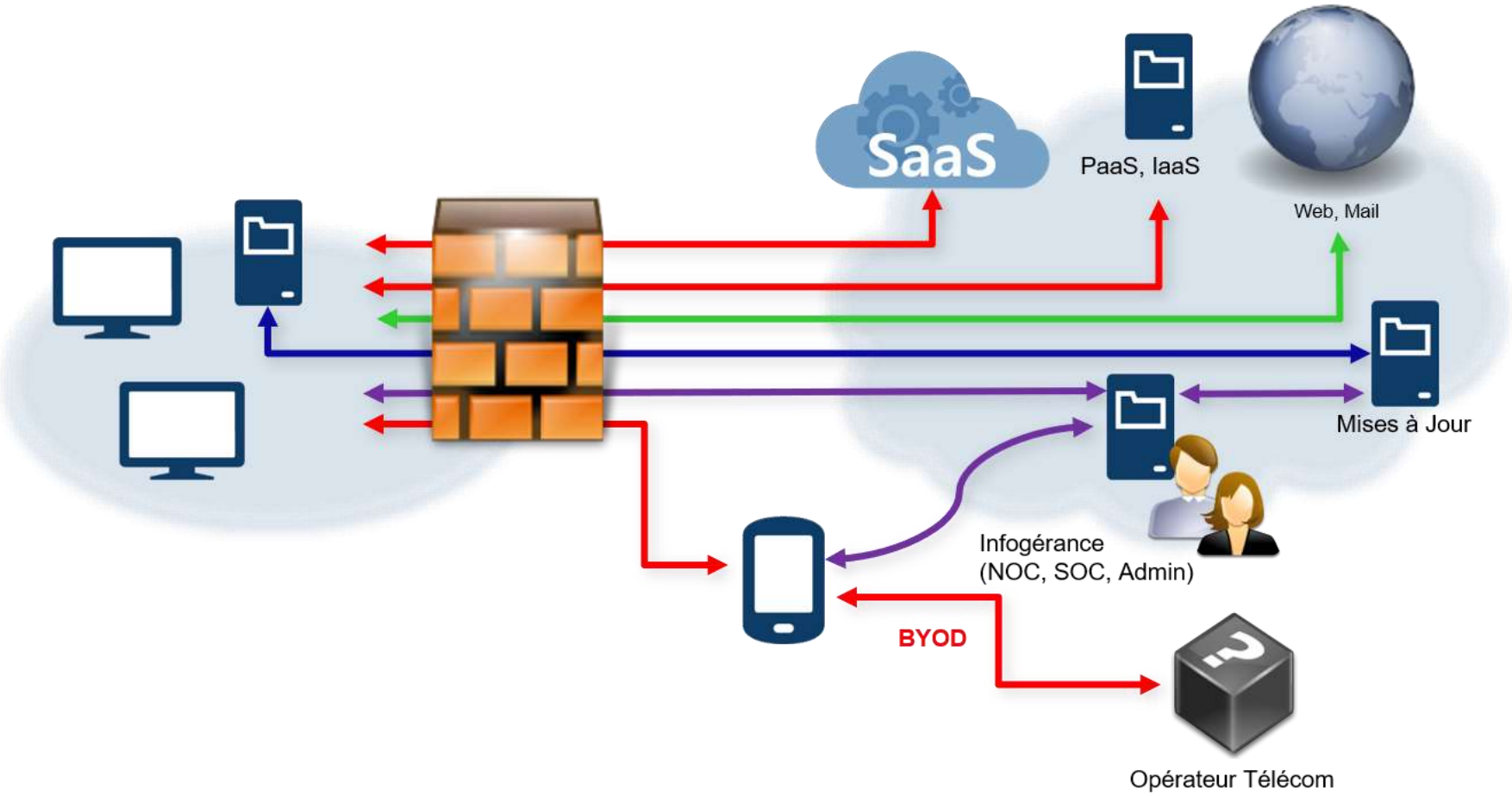


Externalisation de l'infrastructure

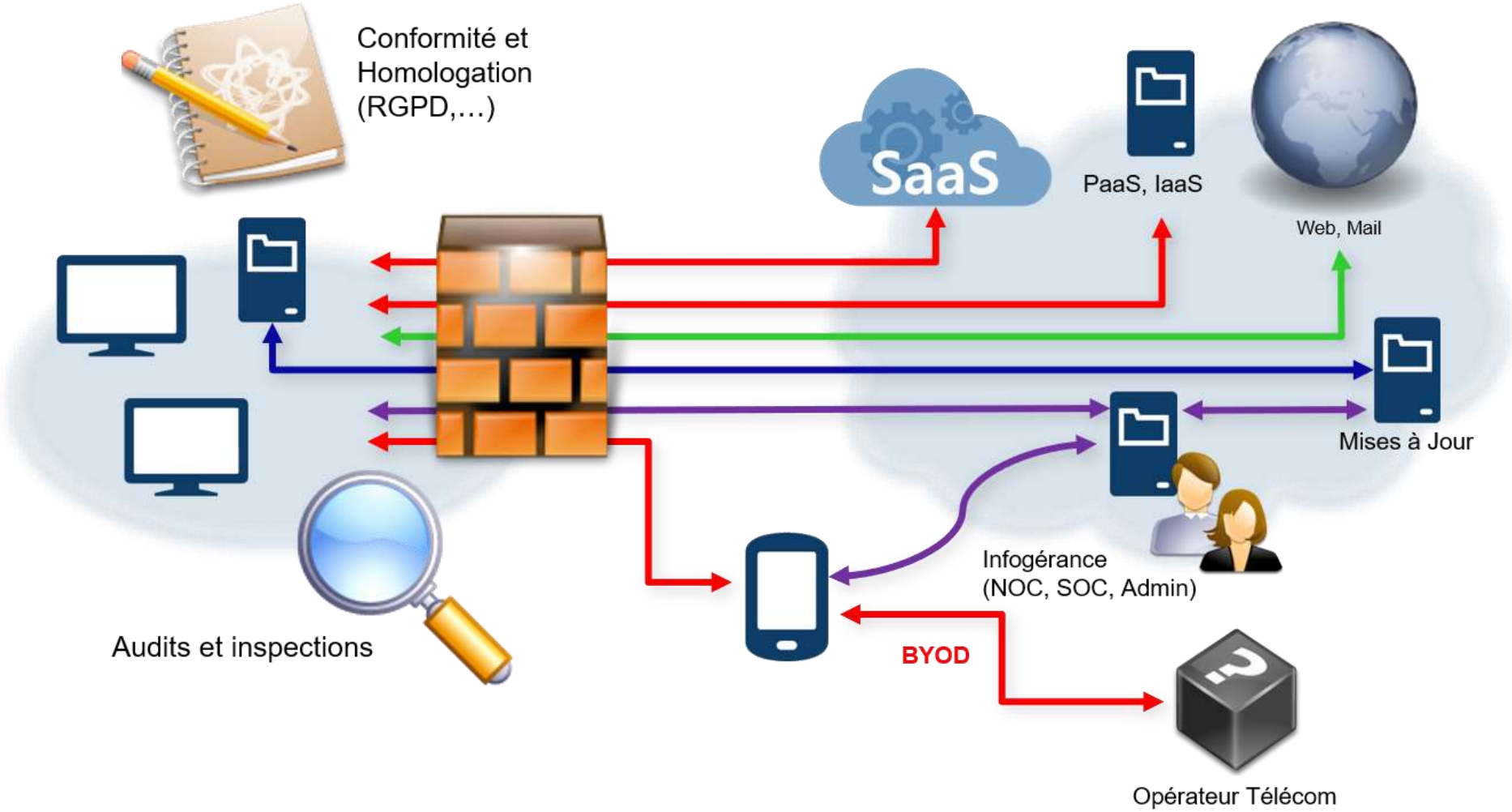


Externalisation des services

1/2



Externalisation des services



Plan

- Historique de l'externalisation
- **Menaces, risques et acteurs**
- Référentiels et pratiques

Menaces et impacts

Menaces Cyber

Impacts concrets

- Entrave d'activité
- Arrêt d'activité
- Pertes financières
- Perte de patrimoine
- Faillite

Types de risques

Perte de confidentialité

- Divulgation d'informations sensibles : dossiers internes, appels d'offre, plans, procédés, carnets de commande, listing clients, contrat RH, données personnelles

Perte d'intégrité

- Destruction de données sensibles
- Fonctionnement / performance des logiciels altérés

Perte de disponibilité

Origine des menaces

Attaquant externe

- Motivations diverses
- Pas forcément en lien avec l'activité de l'entreprise
- (Opportunisme, espionnage, malveillance…)

Attaquant interne

- Motivations diverses (vengeance, vol)
- En lien avec l'activité de l'entreprise

Origine des menaces

Attaquant externe

- Motivations diverses
- Pas forcément en lien avec l'activité de l'entreprise
- (Opportunisme, espionnage, malveillance…)

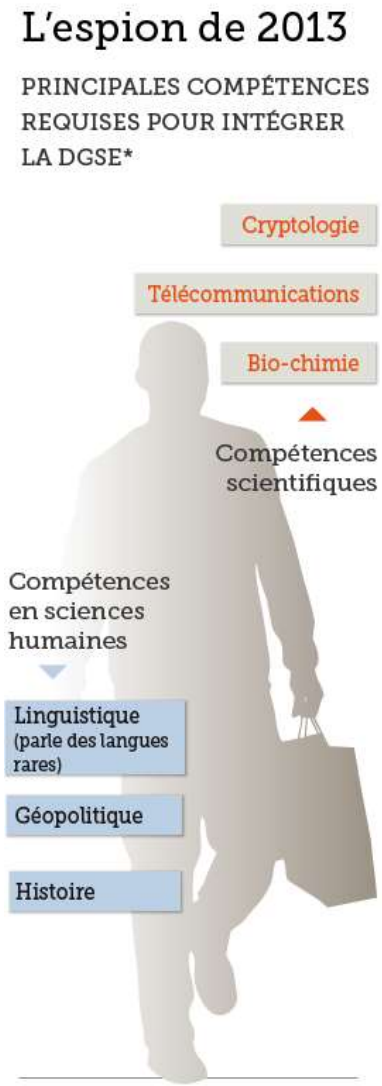
Attaquant externe / internalisé

- Motivations diverses (vengeance, vol)
- En lien avec l'activité de l'entreprise et/ou celle des prestataires

Attaquant interne

- Motivations diverses (vengeance, vol)
- En lien avec l'activité de l'entreprise

Profils différents et variés



Failles et vulnérabilités

Techniques

- Vulnérabilités des équipements ou des protocoles
- Mauvaise configuration ou architecture des systèmes…

Personnel / Humain

- Niveau de compétence et de formation
- Facteur humain, éthique personnelle

Gouvernance et réglementation

- Régimes juridiques applicables aux données (International ?)
- Perte de gouvernance / maîtrise de son système

Vulnérabilités et menaces aujourd'hui

Vulnérabilités informatiques

- Failles des logiciels et matériels déployés : SI, **passerelles et infogérance, flotte mobile**

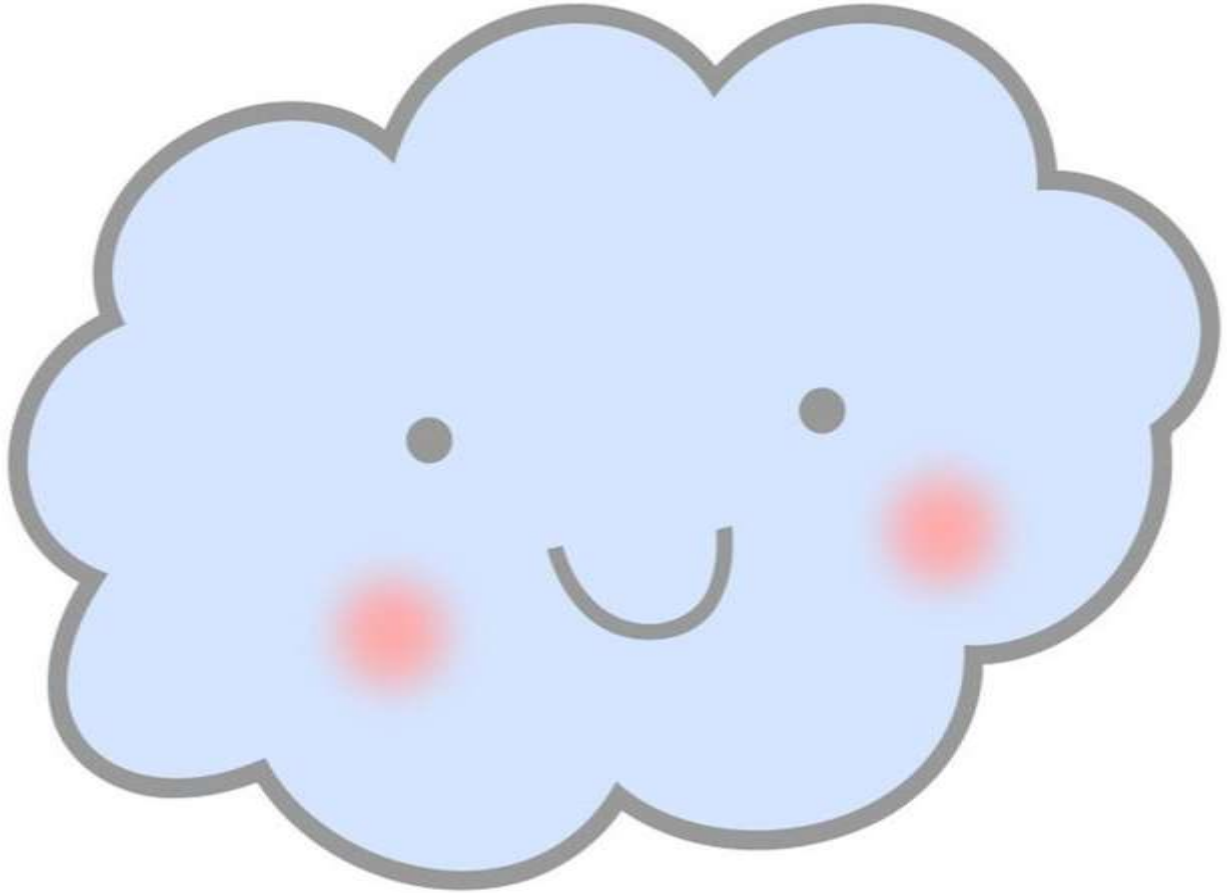
Attaques et menaces

- Malware, Phishing, APT…
- **Accès direct et légitime aux équipements / données / métadonnées du SI**
- **Perte de maîtrise des données (réglementaires, techniques)**

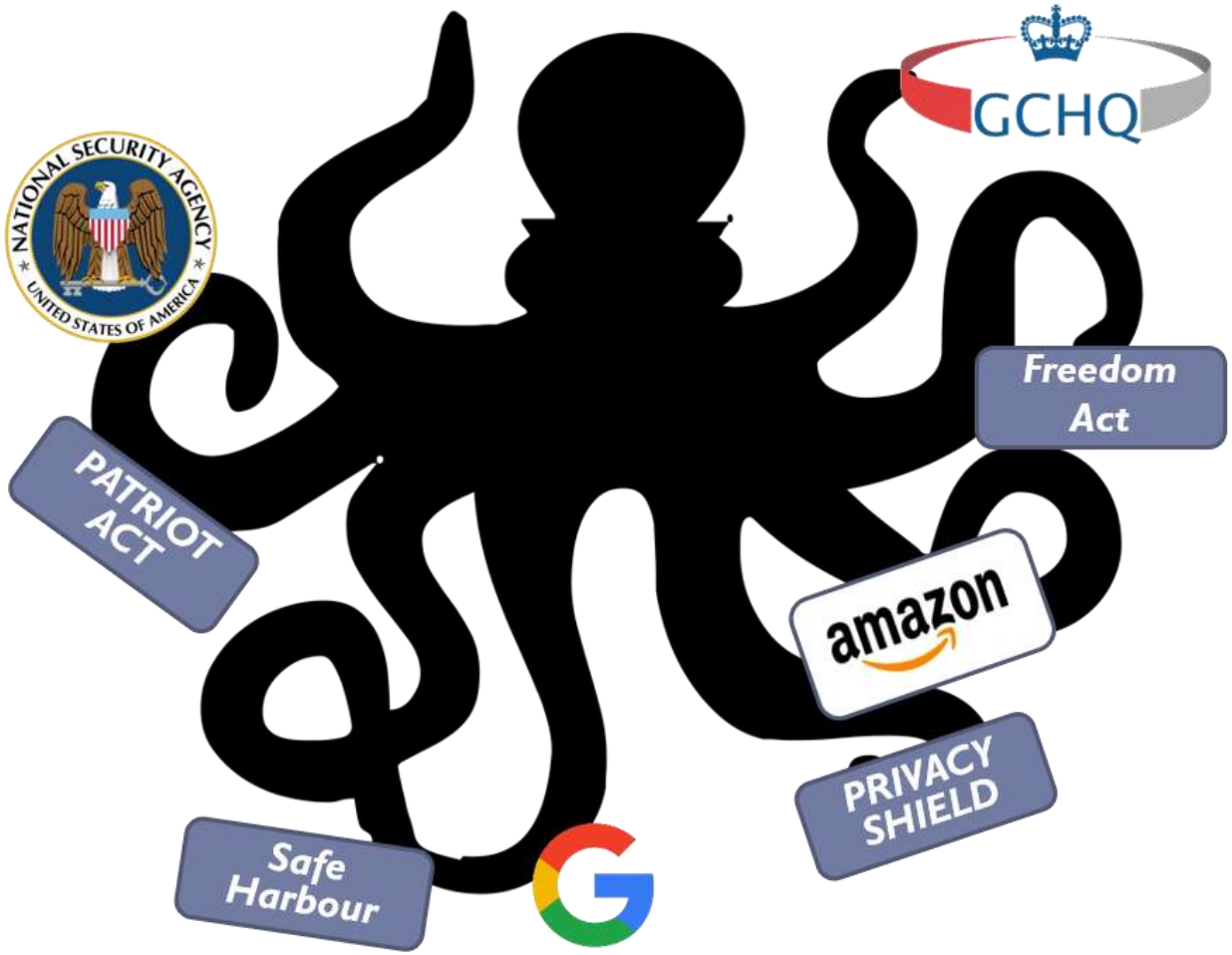
Attaquants

- Extérieurs ou **internes à l'infogérant**, de niveaux divers
- Script kiddies, hacktivists, « mercenaires », organisations criminelles, gouvernements…

TaaS / « Trust » as a service



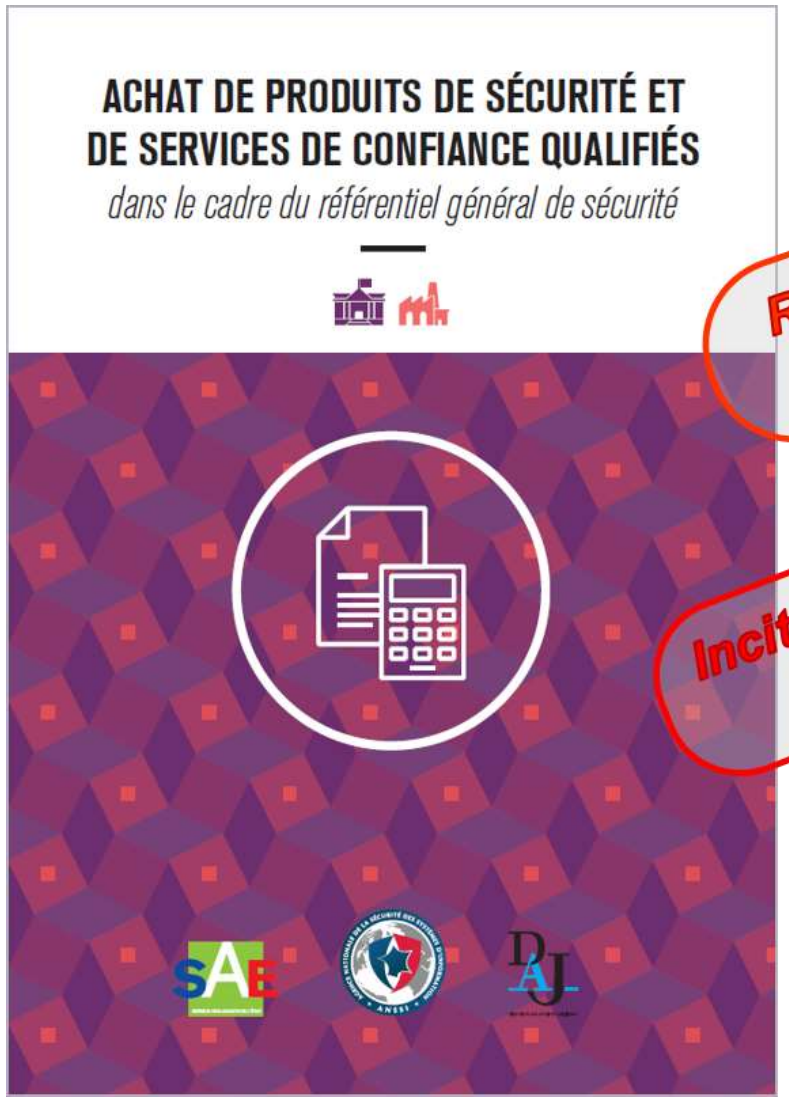
TaaS / « Threat » as a service ?



Plan

- Historique de l'externalisation
- Menaces, risques et acteurs
- **Référentiels et pratiques**

S’inspirer des procédures d’achat public



Recours à des produits qualifiés ou certifiés

Incitations des soumissionnaires à qualifier leurs produits

Recours aux produits et services qualifiés

Produits qualifiés

- La qualification comprend une étude de la Supply Chain
- Certains services en SaaS / Cloud pouvant être couverts

Services qualifiés

- SecNumCloud pour l'externalisation PaaS / IaaS / SaaS
- PDIS, pour l'externalisation de la détection
- PRIS, pour l'externalisation de la réponse à incident
- PASSI, expertise SSI (Réponse à incident, audit)
- **PAMOA, expertise architecture**
- **PAMS, infogérance en toute confiance**

S’inspirer des procédures ANSSI

- S’inspirer des engagements de la qualification…

ANNEXE 2

ENGAGEMENTS DU FOURNISSEUR DE SERVICE

L’entreprise :

(dénomination sociale du fournisseur) :

ayant son siège social sis :

(adresse du siège social du fournisseur)

Atteste par la présente que le service

(nom du service) :

- n’intègre aucune fonction ou accès non documenté, aucun point faible intentionnellement implémenté permettant la divulgation ou la mise à disposition de la société ou à des tiers, d’aucune manière, même partielle, des communications confidentielles, des informations sur la localisation ou toute autre méta-information confidentielle ou personnelle de l’utilisateur ;
- ne peut être conditionné, pour son fonctionnement, à l’utilisation de données confidentielles ou à caractère personnel à l’insu de son utilisateur ;

a) Dans le cas où le service propose des fonctions non couvertes par le périmètre de la qualification, celles-ci ne peuvent ni avoir préséance, ni contredire aux conditions d’utilisation du service figurant dans la décision de qualification ;

b) La collecte, la manipulation et le stockage des données confidentielles et à caractère personnel faits dans le cadre de l’avant-vente, de la mise en œuvre, de la maintenance et l’arrêt du service sont conformes aux exigences édictées par la législation française et européenne en vigueur et ces mêmes données ne sont pas soumises à d’autres régimes juridiques.

c) Les éléments mis à disposition pour l’évaluation et la qualification du service ne sont aucunement frauduleux.

S’inspirer d’autres réglementations

Réglementation de l’OTAN

- Impose de déclarer sa maîtrise de la Supply Chain, pour différents domaines

Questions / Remarques