

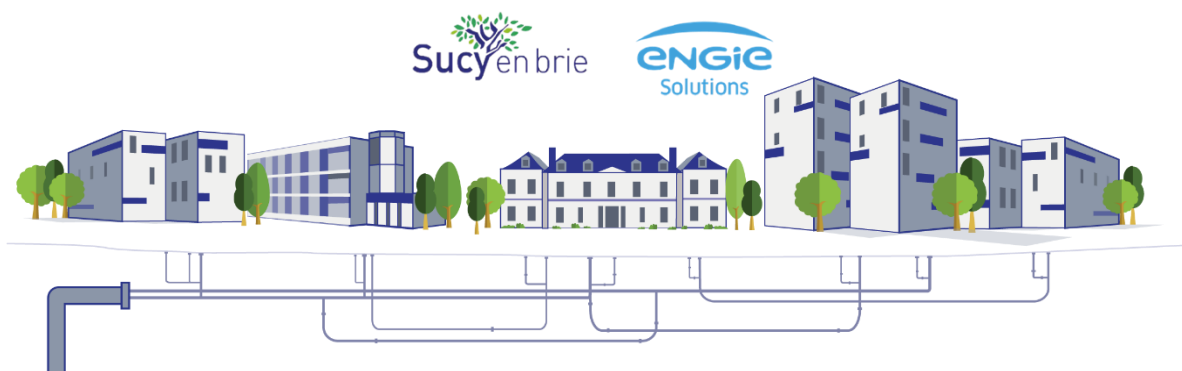


Attribution d'une Concession de Service Public relative au Réseau de Chaleur Urbain de la Ville de Sucy-en-Brie

Annexe au contrat - Base 25 ans

Annexe 13 – Sécurité des systèmes d'information

Offre finale – 31/07/2024



SOMMAIRE

1

UN SOCLE DE SECURITE DU GROUPE ENGIE

1

1.1

UNE PREVENTION EN AMONT

1

1.2

UNE DETECTION COMPLETE

2

1.3

UNE REACTION RAPIDE

2

1.4

LA SECURITE DU SI

2

1 Un socle de sécurité du Groupe ENGIE

Fort de son appartenance au Groupe ENGIE, ENGIE Solutions peut s'appuyer sur un socle de sécurité solide s'articulant autour de trois axes :

- La prévention ;
- La détection ;
- La réaction.

Ce socle représente une base minimale de sécurité pour chaque brique constituante du Système d'Information (SI). Il permet d'assurer un niveau de sécurité correct même pour les briques les moins critiques de l'ensemble.

1.1 Une prévention en amont

Le groupe ENGIE investit fortement dans la protection de ses systèmes d'information industriels de manière à garantir à ses collaborateurs une continuité de leur activité. Cela se décline par plusieurs dispositifs :

- Un CERT interne (Computer Emergency Response Team) : centre de gestion de la sécurité pluridisciplinaire qui assure une gestion des vulnérabilités sur les systèmes déployés dans l'ensemble du groupe ainsi que la réponse à incident. L'équipe est en charge de la gestion des alertes et de la réaction en cas d'attaque informatique ;
- L'outil ZScaler en tant que Proxy Cloud. Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Il permet de masquer un sous-réseau d'une entreprise d'un point de vue externe ;
- Des scans de vulnérabilité réalisés mensuellement ;
- Un suivi de l'évolution des Active Directory ;
- Des serveurs équipés d'anti-virus et de pare-feu.
- Des postes de travail incluant un anti-virus et protégés par chiffrement pour éviter tout problème de confidentialité en cas de vol et patchés mensuellement ;
- Un programme de sensibilisation et un ensemble documentaire sur la cybersécurité accessibles à tous les employés via l'intranet avec des fiches théoriques et pratiques ainsi que des modules de formation en ligne ;
- Des collaborateurs informés et sensibilisés aux méthodologies d'attaques les plus fréquentes (phishing, social engineering, attaque au président, ...) Ils ont fait l'objet de campagnes tests de phishing et vishing (phishing par téléphone).

Enfin Engie Solutions est tenue, comme n'importe quelle entité du groupe ENGIE de compléter une analyse de risque pour chaque projet. Cette démarche permet d'assurer que chaque projet possède un niveau minimum de sécurité.



1.2 Une détection complète

Engie Solutions bénéficie des moyens mis en place au niveau du groupe dont le GSOC ENGIE (Global Security Operationg Center). L'équipe de sécurité est en charge de collecter et analyser les événements de sécurité propres à l'entreprise. Elle qualifie les événements et gère les incidents de la création à la fermeture :

- Collecte et supervision des événements de sécurité 24h/24, 7J/7 ;
- Corrélation de ces différents éléments pour générer des alertes de sécurité.

Le GSOC ENGIE travaille en collaboration avec Thales agréée PDIS (Prestataire de Détection d'Incidents de Sécurité) par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour respecter les exigences des OIV (Organismes d'Importance Vitale).

1.3 Une réaction rapide

Le groupe ENGIE est équipé d'un outil spécialisé dans le traitement d'incidents de sécurité nommé SIRP (Security Incident Response Platform) basé sur le logiciel Resilient d'IBM. Cet outil permet notamment d'automatiser les actions liées à la réponse à incident. Cet outil implémente un ensemble de procédures dédiées à la réponse à incident. Ces procédures décrivent pour chacune des typologies d'attaque les actions à réaliser. Le SIRP est l'outil utilisé par le GSOC afin de gérer les différents incidents de sécurité.

1.4 La sécurité du SI

Les systèmes d'information industriels doivent être protégés contre les actions non autorisées (accès, divulgation d'informations, interruption et perturbation du système, modification ou destruction).

Pour traiter cette question, ENGIE a mis en œuvre une politique de sécurité Groupe s'appuyant sur 19 contrôles de sécurité :

- Sensibilisation et formation à la sécurité ;
- Point unique de responsabilité pour la cybersécurité des SI ;
- Gestion des modifications des SI ;
- Inventaire des composants des SI ;
- Plan de réponse aux incidents ;
- Acquisition et projets ;
- Sécurité d'intervention des contractants ;
- Architecture de sécurité des SI ;
- Renforcement de la configuration ;
- Gestion des correctifs de sécurité et des vulnérabilités ;
- Détection des codes malicieux ;
- Gestion des dispositifs amovibles ;



- Gestion des comptes utilisateurs ;
- Identification et authentification ;
- Sécurité de l'information, installations et leur accès ;
- Sécurité sans fil ;
- Audit de cybersécurité ;
- Gestion de l'obsolescence.

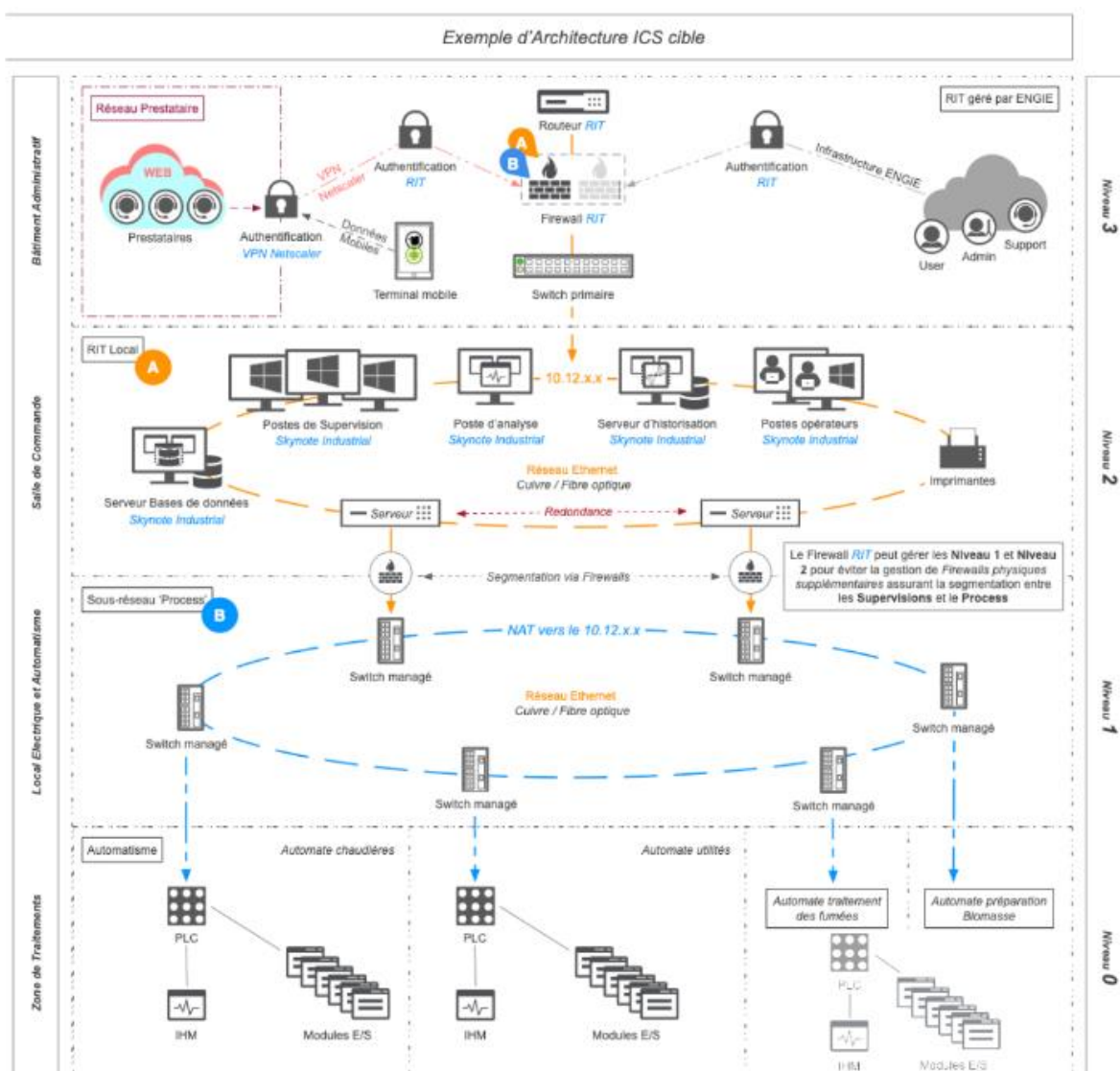


Figure 1 : Exemple de schéma d'architecture d'un site

L'architecture SI du système industriel repose sur le RIT (Réseau Industriel et Technique) d'ENGIE Solutions.

Le RIT est constitué d'un réseau MPLS privé dédié à nos réseaux industriels. Le RIT est supervisé et monitoré. Chaque événement (logs) enregistré par les actifs de sécurité positionnés en bordure et au cœur du réseau RIT est adressé à un équipement de collecte central. Cet équipement reporte les données en temps réel au GSOC (Global Security



Operations Center), en charge de la collecte, de l'analyse, de la corrélation de ces informations entre elles, tout en tirant parti des événements pouvant être connus par ailleurs (alertes de sécurité hors contexte ENGIE Solutions).

Les signalements sont analysés et peuvent donner lieu à des traitements d'incident immédiats ou/et des remédiations / améliorations à plus long terme.

Le réseau RIT est totalement étanche du réseau Internet.

Deux réseaux LAN isolés sont créés pour séparer physiquement les équipements du système industriel du système bureautique.

Le réseau LAN Industriel peut disposer de plusieurs zones logiques (VLAN) en fonction de l'usage des matériels. Pour le site nous n'avons que le VLAN Automate.

Ce LAN sera sécurisé par un pare-feu permettant d'ouvrir au strict minimum les flux suivants : l'usage, les habilitations, les adresses IP et les ports des applications.

