RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

IDENTIFICATION DU CŒUR DE CONFIANCE D'UN SI

Découvrez la méthodologie et les ressources essentielles de l'ANSSI pour l'identification du cœur de confiance (🖤) d'un système d'information (SI), ainsi que les lignes directrices prioritaires à suivre pour sa sécurisation.

Le cœur de confiance d'un SI désigne l'ensemble des ressources informatiques dont la compromission pourrait mener à la prise de contrôle étendue du SI.

1/ MÉTHODOLOGIE D'IDENTIFICATION DU CŒUR DE CONFIANCE

➔ **Identifier le périmètre initial** : il s'agit des quelques ressources informatiques sur lesquelles reposent fondamentalement la gestion centralisée du SI, par exemple les contrôleurs de domaine *Active Directory* (AD) pour les SI composés de systèmes Windows. Ce périmètre initial n'est pas exhaustif, il s'agit du point de départ de la méthodologie.

➔ **Procéder à l'identification et à l'analyse des chemins de contrôle et des chemins d'attaque :**

> si une ressource **A** du SI gère légitimement une ressource **B** du 🖤 (p. ex. car elle l'administre), alors **A** contrôle le 🖤 (chemin de contrôle) ;

> si la compromission de **A** entraîne la compromission vraisemblable d'une ressource **B** du 🖤, en raison notamment de vulnérabilités ou de faiblesses de configuration de cette dernière (et au regard de la sensibilité du SI et du profil d'attaquants déterminé par l'entité), alors **A** pourrait prendre le contrôle du 🖤 (chemin d'attaque).

➔ **Réajuster le périmètre** :

> Il grandit en fonction des chemins de contrôle et d'attaque identifiés précédemment. Les ressources qui contrôlent ou peuvent prendre le contrôle du 🖤 rejoignent le périmètre logique du 🖤.

> Il réduit suite aux actions de sécurisation mises en œuvre pour éradiquer des chemins de contrôle ou d'attaque : suppression de droits, durcissement, correction de vulnérabilités, etc. Les ressources qui ne contrôlent plus ou ne peuvent vraisemblablement plus prendre le contrôle du 🖤 quittent le périmètre logique du 🖤.

➔ **Itérer les 2 étapes précédentes.** Le 🖤 évolue au fil des analyses, des sécurisations et du cycle de vie du SI. Chaque fois que son périmètre évolue, les chemins de contrôle et d'attaque doivent à nouveau être identifiés et analysés. Des exemples figurent en fin de chapitre.

Aide à l'identification des chemin de contrôle

➔ **Se doter des compétences adéquates.** L'analyse des chemins de contrôle et d'attaque nécessite de bonnes connaissances des technologies utilisées dans le SI, et plus largement en cybersécurité. Recourir à des prestations de service si nécessaire, en privilégiant les prestataires qualifiés par l'ANSSI.

➔ **S'aider d'outils d'analyse automatique des chemins de contrôle.** Il en existe en sources ouvertes pour l'analyse d'un annuaire AD (BloodHound, PingCastle), d'une infrastructure Kubernetes (OSAKA), etc.

➔ **Utiliser les services d'audit automatisé de l'ANSSI** (notamment de l'AD), accessibles aux opérateurs régulés et aux entités publiques.

V1.0 (07/26)

cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

Exemple 1 : Identification du 🖤 dans un SI reposant sur un domaine AD

Le 🖤 d'un SI reposant sur AD est souvent constitué, entre autres, des :

- **contrôleurs de domaine AD** ;
- **systèmes d'administration** (postes d'administration, rebonds, etc.) du 🖤 ;
- **serveurs WSUS** (*Windows Server Update Services*) qui distribuent des mises à jour au 🖤 ;
- **infrastructures de gestion de clés** (p. ex. AD-CS) qui permettent la distribution de certificats d'authentification ;
- **hyperviseurs** qui hébergent des machines virtuelles (VM) du 🖤 (sauf si des mécanismes sont mis en œuvre pour protéger les systèmes invités de ces VM vis-à-vis des hyperviseurs et des administrateurs de VM) ;
- **services de fédération ou de synchronisation d'identités** (p. ex. AD-FS, *Microsoft Entra Connect*) ;
- équipements qui stockent des **sauvegardes sensibles** du 🖤 (sauf celles préalablement chiffrées) ;
- serveurs qui pilotent des **agents de gestion centralisée** déployés sur des ressources du 🖤 (p. ex. agent antivirus, agent EDR, agent de sauvegarde, agent de déploiement centralisé de logiciels).

→ **Assimiler le 🖤 au Tier 0** du modèle de *tiering* de Microsoft.

→ **Analyser, en cas d'extension du SI dans le *cloud*, les chemins de contrôle** spécifiques à chaque éditeur d'offre *cloud* (p. ex. les comptes d'administration des *tenants*).

Exemple 2 : Identification du 🖤 dans un SI industriel

Le 🖤 d'un SI industriel est souvent constitué, entre autres, des :

- **serveurs SCADA** centraux qui pilotent la majorité des automates programmables industriels (souvent abrégés PLC en anglais) ;
- **serveurs MES** (*Manufacturing Execution System*) qui transmettent des commandes aux SCADA à partir des données des ERP (*Enterprise Resource Planning*) ;
- **ressources IT dont ces serveurs dépendent**. À noter que si des ressources du 🖤 sont membres d'un domaine AD, le 🖤 du SI industriel doit inclure le 🖤 de cet environnement AD.

2/ SÉCURISATION DU CŒUR DE CONFIANCE

→ **Réduire le 🖤 au strict minimum** en traitant un maximum de chemins d'attaque et de contrôle.

→ **Sécuriser, durcir et superviser chacune des ressources qui composent le 🖤**. Leur surface d'attaque doit être aussi réduite que possible.

→ **Mettre en œuvre une délégation fine des droits** de sorte que peu d'administrateurs du SI aient le contrôle du 🖤. *In fine*, peu de personnes l'administrent et ces actions d'administration sont peu fréquentes.

→ **Sécuriser et cloisonner les systèmes et comptes d'administration du 🖤**. Il est recommandé qu'ils soient dédiés à l'administration du 🖤 et qu'ils opèrent depuis un réseau ou un VLAN dédié et finement filtré.

→ **Maîtriser les risques de sous-traitance de gestion du 🖤 :** sa sécurité dépend de celle des SI des prestataires.

→ **Aller plus loin** en lisant les guides ANSSI sur le *tiering* AD et la remédiation.

V1.0 (07/26)

cyber.gouv.fr / conseil.technique@ssi.gouv.fr