RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

TRUSTED CORE

Check out the French cybersecurity agency (ANSSI)'s methodology and essential resources for identifying the trusted core (🖤) of an information system (IS), along with key steps to secure it.

The trusted core of an IS refers to all the IT resources that, if compromised by an attacker, could lead to extensive control over the IS.

1/ METHOLOGY TO IDENTIFY THE TRUSTED CORE

- **Identify the initial perimeter,** i.e. the few IT resources on which the centralised management of the IS fundamentally relies. For example, it can refer to Active Directory (AD) domain controllers for an IS running on Windows systems. This initial perimeter is not exhaustive; it serves as the starting point for the methodology.
- **Identify and analyse control and attack paths:**
  - If a resource **A** within the IS legitimately manages a resource **B** of the 🖤 (e.g. by administering it), then **A** controls the 🖤 (control path);
  - If the compromise of a resource **A** likely leads to the compromise of a resource **B** part of the 🖤, then **A** could take control of the 🖤 (attack path). The identification of these paths is notably based on configuration vulnerabilities or weaknesses of **B**, and with regards to the sensitivity of the IS and the attacker profiles determined by the organisation.
- **Readjust the perimeter:**
  - It grows depending on the control and attack paths identified previously. Resources that control or can take control of the 🖤 are included within the logical perimeter of the 🖤.
  - It shrinks following security measures implemented to eliminate control or attack paths: removal of permissions, hardening, vulnerability patching, etc. Resources that no longer control the 🖤, or are unlikely to, leave the logical perimeter of the 🖤.
- **Repeat the previous steps.** The 🖤 evolves throughout the course of analyses, implementation of security measures, and the IS lifecycle. Whenever its perimeter changes, control and attack paths must be identified and analysed once again. Examples are provided page 2.

How to identify control paths ?

- **Acquire the necessary skills.** Analysing control and attack paths requires a sound understanding of the technologies used in the IS and, on a broader level, of cybersecurity. Use external services when needed, giving priority to providers accredited by ANSSI.
- **Employ automated tools for control paths analysis**. Open-source tools are available for analysing an Active Directory (BloodHound, PingCastle), a Kubernetes infrastructure (OSAKA), etc.
- **Use ANSSI's automated audit services** (particularly for AD), available to regulated operators and public bodies.

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Exemple 1 : Identifying the 🖤 of IS based on an AD domain

→ The 🖤 of an IS based on AD often consists, amongst other things, of:

- > **AD domain controllers;**
- > **administration systems** (administration workstations, jump servers, etc.) of the 🖤;
- > **WSUS** (Windows Server Update Services) servers that distribute updates to the 🖤;
- > **Public key infrastructures** (e.g. AD-CS) that enable the distribution of authentication certificates;
- > **hypervisors** hosting virtual machines (VMs) of the 🖤 (unless mechanisms are in place to protect these VMs' guest systems from the hypervisors and VM administrators);
- > **identity federation or synchronisation services** (e.g. AD-FS, Microsoft Entra Connect);
- > devices that store **sensitive backups** of the 🖤 (except those that have been encrypted beforehand);
- > servers that control **centralised management agents** deployed across assets of the 🖤 (e.g. antivirus agents, EDR agents, backup agents, centralised software deployment agents).

→ **Consider the 🖤 as Tier 0** in Microsoft's tiering model.

→ **Analyse, in the event of IS expansion in the cloud, the control paths** specific to each cloud service provider (e.g. tenant administration accounts).

Exemple 2 : Identifying the 🖤 of industrial IS

→ The 🖤 of an industrial IS often consists, amongst other things, of:

- > **central SCADA servers** that control the majority of programmable logic controllers (PLC);
- > **MES** (Manufacturing Execution System) servers, that transmit commands to the SCADA systems based on data from ERP (Enterprise Resource Planning) systems;
- > **IT resources on which these servers depend.** Please note that if any resources part of the 🖤 are members of an AD domain, the 🖤 of the industrial IS must include the 🖤 of that AD environment.

2/ SECURING THE TRUSTED CORE

→ **Reduce the 🖤 to the absolute minimum** by covering as many attack and control paths as possible.

→ **Secure, harden and monitor each of the resources that make up the 🖤.** Their attack surfaces must be narrowed as much as possible.

→ **Implement a fine-tuned delegation of rights** so that only a small number of IS administrators have control over the 🖤. Ultimately, fewer people administer the 🖤, and these administrative tasks are infrequent.

→ **Secure and partition administrative systems and accounts of the 🖤.** They should ideally be dedicated to administering the 🖤, and operate from a dedicated, finely filtered network or VLAN.

→ **Manage the risks associated with outsourcing 🖤 management:** its security depends on that of the service providers' IS.

→ **Find out more** by reading the ANSSI guides on AD tiering (only available in French) and on remediation.