EDR HarfangLab

Endpoint Detection & Response

Cible de securite

Ref DINT-KLIF-CIBLE-01 Ed 7 du 24/06/2024

Validité du document — HarfangLab sas			
Écrit par	Pierre-Louis MAURATILLE	Chef de projet	06/12/2022
Vérifié par	Mathieu GASPARD	Responsable technique	06/12/2022

Revisions du document		
Version	**Date**	**Commentaire**
1.0	16/12/2021	Création • version préliminaire
2.0	07/11/2022	Mise à jour
3.0	25/11/2022	Mise à jour
4.0	06/12/2022	Mise à jour
5.0	09/01/2024	Mise à jour
6.0	29/04/2024	Mise à jour
7.0	24/06/2024	Mise à jour

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

GLOSSAIRE

ANSSI	Agence nationale de la sécurité des systèmes d'information (site)
CIS	Center for Internet Security (https://www.cisecurity.org)
EDR	Endpoint Detection & Response
LDAP(S)	Lightweight Directory Access Protocol (Secure)
HTTP(S)	HyperText Transfer Protocol (Secure)
TLS	Transport Layer Security

Partie I.

PREAMBULE

HarfangLab

Deep Integrity | Paramount Security

I.1 INTRODUCTION

I.1.1 OBJET DU DOCUMENT

Ce document constitue la cible de sécurité pour l'évaluation de la solution EDR (Agent et Manager) de l'éditeur HarfangLab.

I.1.2 REFERENCES

Références	Titre	Lien
[ANSSI1]	Recommandations de sécurité relatives au déploiement de conteneurs Docker	https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-au-deploiement-de-conteneurs-docker/
[ANSSI2]	Recommandations pour la mise en place de cloisonnement système	https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-mise-en-place-de-cloisonnement-systeme/
[CIS]	CIS Benchmark for Kubernetes	https://www.cisecurity.org/benchmark/kubernetes/
[ANSSI3]	Points de contrôle Active Directory	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html

I.2 IDENTIFICATION DU PRODUIT

I.2.1 REFERENCE ET VERSION

Nom de l'éditeur	HarfangLab
Nom du produit	EDR
N de version	Agent : 3 Manager : 3
Divers	-

I.2.2 PROCEDURE D'IDENTIFICATION DU PRODUIT ÉVALUE

Manager EDR

L'identification de la version du manager se fait en examinant l'interface d'administration (texte en bas dans le bandeau situé à gauche de l'interface).

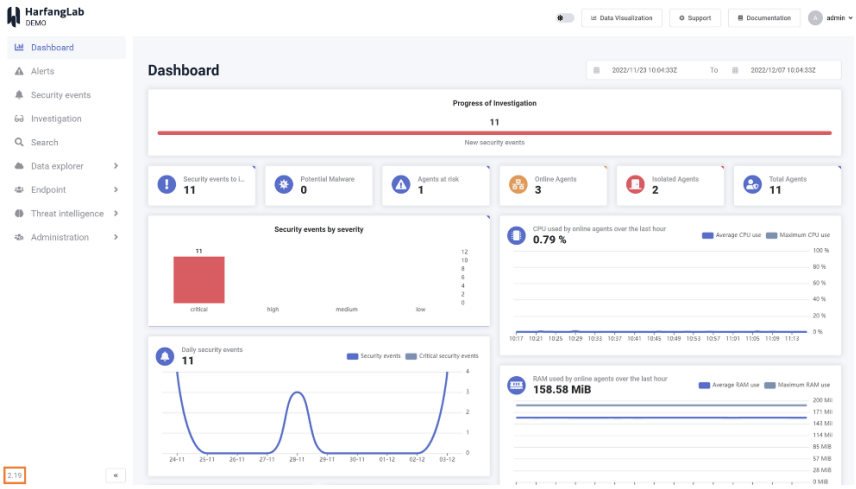

Figure 1 : Identification de la version du manager (exemple)

Agent EDR

L'identification de la version de l'agent se fait en examinant les propriétés de l'exécutable « hurukai.exe » dans le dossier d'installation de l'agent (clic droit puis « Propriétés »).

L'onglet « Détails » comporte un champ « Version du produit ». La capture suivante montre par exemple cet onglet dans une version en anglais de Windows :

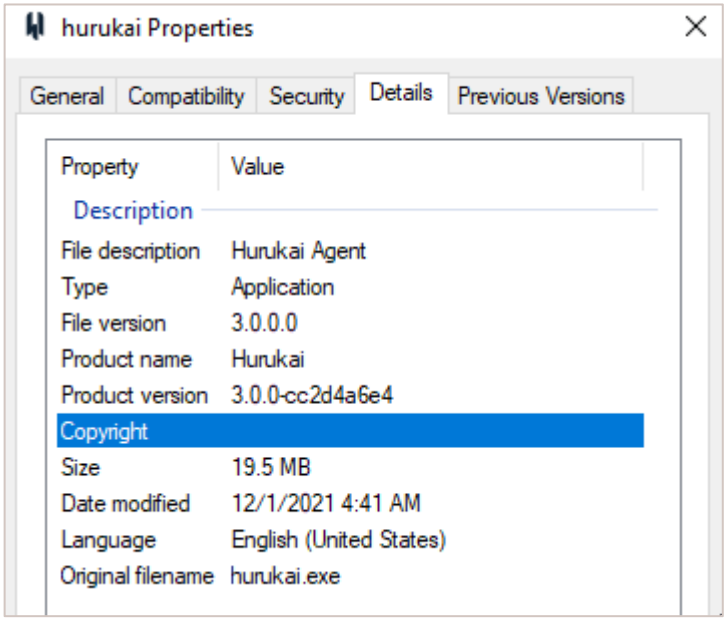

Figure 2 : Identification de la version de l'agent (exemple)

Partie II.

DESCRIPTION PRODUIT & ENVIRONNENMENT OPERATIONNEL

Le produit objet de la présente cible de sécurité est l'ensemble de la solution EDR (« Endpoint Detection & Response ») de l'éditeur HarfangLab. Il comprend le module Agent et le module Manager.

HarfangLab

Deep Integrity | Paramount Security

II.1 DESCRIPTION DU PRODUIT

II.1.1 DESCRIPTION GENERALE & FONCTIONNALITES

La solution HarfangLab EDR a pour objectif la surveillance de terminaux (ordinateurs ou serveurs) au sein d'un réseau, dans un des scénarios d'utilisation suivants :

- Observation permanente à des fins de détection d'intrusion et de réaction,
- Réponse à incident et analyse

Cette solution est basée sur l'utilisation d'un manager centralisé et d'agents installés sur les postes à monitorer.

Manager EDR

Le manager EDR a pour rôle la collecte des données émises par les agents EDR, leur traitement et leur mise à disposition dans un puits de données pour permettre ainsi leur présentation dans une console d'administration.

Ce manager s'interface avec :

- Les agents dont il doit collecter les données
- Les utilisateurs auxquels il présente les données collectées et le résultat de leur analyse. Ces utilisateurs peuvent avoir des rôles distincts :
  - administration du manager
  - gestion de la détection
  - gestion des agents
  - télémétrie (consultation)
  - visualisation ou modification de la base de « threat intelligence »
- Des services externes permettant d'étendre ses fonctionnalités, par exemple le recours à des services tiers pour enrichir la détection, ou l'émission de données vers un SIEM.
- Un annuaire LDAP permettant l'authentification des utilisateurs interagissant avec le manager.

Les fonctions locales d'analyse de données sont hors du périmètre d'évaluation du manager.

Sont ici évaluées :

- La protection du manager vis-à-vis des entités externes interagissant avec lui (agents, utilisateurs et services externes)
- La protection des données échangées entre le manager et les services externes

Agent EDR

L'agent comporte plusieurs fonctions locales hors périmètre d'évaluation telles que :

- la surveillance des processus,
- le relevé d'informations.

Par rapport à ces fonctions locales, sont évalués :

- l'innocuité de l'agent, c'est-à-dire le fait que la présence de l'agent ne dégrade pas la sécurité des machines sur lesquelles il est déployé. Celle-ci s'appuie notamment sur les mécanismes de contrôle d'accès du système d'exploitation.
- l'autoprotection de l'agent en empêchant qu'un utilisateur standard ne puisse facilement désactiver le service EDR ou désinstaller l'agent.

Ces fonctions sont dans le périmètre d'évaluation.

Communication entre agent et manager

La solution EDR repose sur la collecte des données recueillies par les agents et leur traitement au sein du manager. La transmission sécurisée de ces données repose sur les fonctions suivantes :

- Authentification du manager par les agents (par rapport notamment à une autorité de certification racine),
- Protection de la confidentialité et de l'intégrité des données et des ordres échangés avec les agents. Ces fonctions sont dans le périmètre d'évaluation.

Pour cela, l'agent commence par monter un canal de transport sécurisé via un tunnel TLS chiffré. Le tunnel est monté à l'initiative de l'agent et jamais à l'initiative du manager. L'identité du manager est vérifiée selon deux paramètres présentés par celui-ci :

- l'autorité de certification racine, comparée à une valeur codée en dur dans l'agent et évitant ainsi une usurpation du certificat du manager,
- la clé d'identification du manager (qui est en fait la clé publique de signature, non liée à la négociation TLS), saisie lors de l'installation de l'agent.

A l'intérieur du tunnel TLS, les données transitent avec un chiffrement supplémentaire.

II.1.2 DESCRIPTION DE L'UTILISATION DU PRODUIT

La figure ci-dessous présente une architecture type de solution, illustrant l'intégration de l'agent avec son manager :

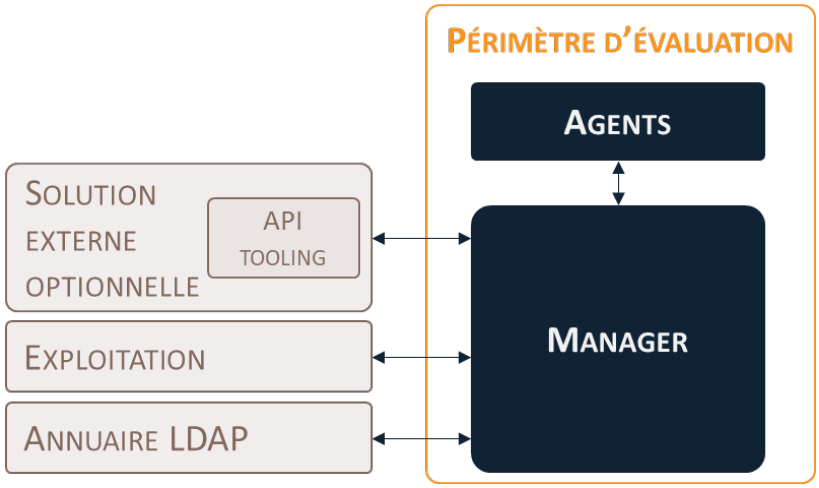

Figure 3 : Périmètre d'évaluation dans la solution

Note : les flux présentés ci-dessus sont protégés par TLS (HTTPS ou LDAPS).

II.1.3 PLATEFORME D'EVALUATION

La plateforme d'évaluation du produit est constituée d'une configuration standard de manager sous la forme d'une machine virtuelle et de l'agent sur une version de référence de Windows :

- la dernière version de Windows 11 disponible au début des tests
- la dernière version de Windows Server 2022 disponible au début des tests

Après l'installation locale de l'agent par un administrateur système de la machine concernée, l'agent est administré depuis le manager.

Aucune interaction n'a lieu avec les utilisateurs locaux. Les droits sur les agents font l'objet d'une politique de gestion des droits propre au manager.

II.2 ENVIRONNEMENT OPERATIONNEL DU PRODUIT

II.2.1 UTILISATEURS DU PRODUIT

Manager

La configuration initiale du manager est effectuée par l'administrateur système.

Les interactions post installation se font par la console d'administration du manager. Les accès à cette console d'administration peuvent se faire :

- via l'interface utilisateur front-end,
- via une API permettant d'automatiser le pilotage de la solution et l'extraction de données.

Après l'installation locale de l'agent par un administrateur système de la machine concernée, l'agent est administré depuis le manager.

Trois types de profils peuvent être définis :

- Le profil analyste qui accède au manager dans le but d'opérer la solution en traitement d'alertes, sans droits d'administration ni d'investigation.
- Le profil administrateur de la solution, acteur de confiance qui accède au manager avec les droits les plus élevés.
- Le profil administrateur système, acteur de confiance en charge de la configuration initiale et du déploiement.

Aucune interaction n'a lieu avec les utilisateurs locaux. Les droits sur les agents font l'objet d'une politique de gestion des droits propre au manager.

Agent

Après l'installation locale de l'agent par un administrateur système de la machine concernée, l'agent est administré depuis le manager.

Aucune interaction n'a lieu avec les utilisateurs locaux. Les droits sur les agents font l'objet d'une politique de gestion des droits propre au manager.

II.2.2 ENVIRONNEMENT D'EXPLOITATION DU PRODUIT

Manager

Le manager est déployé sous la forme d'un cluster Kubernetes par le gestionnaire de paquets Helm.

Ce cluster est en charge d'exécuter les services du manager. Ces services permettent de :

- récupérer les données émises par les agents,
- traiter ces données ,
- les injecter dans un puits de données,
- permettre leur présentation dans la console d'administration.

Le Manager permet également de déléguer la fonction d'authentification à un service d'authentification externe.

Les versions de systèmes d'exploitation supportées pour l'installation du manager sont :

- CentOS Stream 8
- RHEL 8
- Debian 10
- Debian 11
- Ubuntu 20.04
- Ubuntu 22
- Rocky 8

Agent

Le logiciel agent, s'intègre dans son environnement selon le principe illustré par la figure ci-contre :

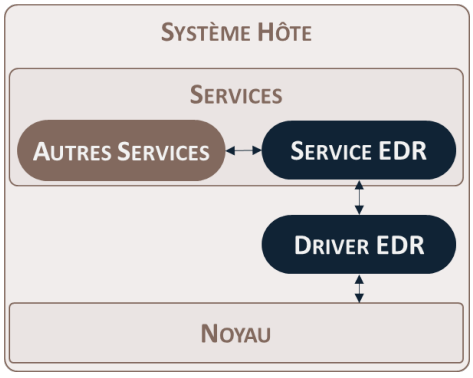

Figure 4 : environnement du logiciel agent

Comme illustré ci-dessus, l'agent est composé d'un service et d'un module noyau fonctionnant sous Windows.

Les versions de Windows supportées par l'agent sont :

- Windows 7 SP1 et versions ultérieures,
- Windows Server 2008 R2 et versions ultérieures,

II.2.3 HYPOTHESES D'EXPLOITATION DU PRODUIT

H1.Host_agent

L'environnement dans lequel s'exécute les agents ne doit pas nécessairement faire l'objet d'un durcissement, mais ne fait pas l'objet d'affaiblissement de sécurité par la configuration appliquée ou l'utilisation qui en est faite.

En particulier :

- une séparation des rôles « utilisateur » et « administrateur » est mise en place. L'utilisation nominale est faite depuis un compte avec un rôle « utilisateur ».
- une authentification robuste des utilisateurs et des administrateurs est mise en place sur les hôtes.
- le contrôle d'accès aux fichiers limite les droits en modification des fichiers du système d'exploitation et des programmes installés.
- la séparation des privilèges d'accès aux ressources est mise en place, d'une part entre les espaces noyau et application, et d'autre part entre les différents processus s'exécutant dans ces espaces.
- les systèmes hôtes sont maintenus à jours vis-à-vis des correctifs de vulnérabilités.
- l'administrateur local à l'agent est de confiance.

Note : HarfangLab conseille d'utiliser une chaine de démarrage sécurisée et de mettre en place du chiffrement de disque en suivant les recommandations de l'ANSSI.

H2.Host_manager

L'environnement dans lequel s'exécute le manager fait l'objet d'un durcissement physique et logique le protégeant des attaques locales. Ce durcissement n'est pas à la charge d'HarfangLab et est mis en place par le client.

Les administrateurs système en charge de la gestion du manager sont de confiance et formés à l'utilisation du produit.

Les administrateurs de la console (avec les privilèges les plus élevés sur la console) sont de confiance.

L'accès local aux machines sur lequel le manager est exécuté est réglementé et restreint aux seules personnes autorisées.

En cas d'utilisation d'une authentification externe, le service utilisé est renforcé de sorte à ce que celui-ci permette de garantir l'authentification sans constituer de menace.

Note : HarfangLab conseille dans sa documentation de suivre les recommandations de l'ANSSI pour sécuriser le service d'authentification externe utilisé.

Note : dans le cadre d'un déploiement *on premise*, l'installation du manager est réalisée par le client avec l'assistance d'HarfangLab en cas de problème.

II.2.4 MESURE DE SECURITE APPORTEES PAR L'ENVIRONNEMENT DU PRODUIT

Les mesures de sécurité mises en œuvre sur l'hôte de l'agent, détaillées en section précédente, protègent vis-à-vis d'un utilisateur standard de l'hôte ou d'un processus d'exécutant sur celui-ci :

- L'intégrité du logiciel de l'agent lui-même et de sa configuration (dont la clé publique du manager).
- La confidentialité et l'intégrité des données en mémoire.
- L'intégrité d'exécution des processus de l'agent.

La bi-clé utilisée pour authentifier et sécuriser les échanges est générée lors du déploiement et est protégée en confidentialité et en intégrité par les mesures de durcissement du « manager » et par les politiques de sécurité de l'organisation. Tous les secrets sont différents pour chaque client.

Les mesures de sécurités décrites dans l'hypothèse H2 protègent le manager des attaques locales ou depuis le service d'authentification externe.

Partie III.

Analyse de risque

HarfangLab

Deep Integrity | Paramount Security

III.1 BIENS SENSIBLES

III.1.1 BIENS UTILISATEUR

Les biens utilisateur à protéger par l'agent et le manager sont :

B1.Collecte L'ensemble des données collectées par l'agent et utilisées pour la détection locale et l'envoi pour traitement au manager. Ces données doivent être protégées en confidentialité, en intégrité, en authenticité (dont l'anti-rejeu).

B2.Ordre Les ordres envoyés par le manager à l'agent en vue de réaliser des opérations sur l'hôte. Ces données doivent être protégées en authenticité (dont l'anti-rejeu) et en confidentialité. Ce bien peut contenir les biens B3 et B5 dans le cadre de la récupération d'une mise à jour et de façon temporaire dans le cadre de la récupération par un agent de sa configuration.

III.1.2 BIENS DU PRODUIT

Les biens du produit sont :

B3.Logiciel agent Ce bien est protégé:

- en authenticité lors de l'installation (vérification de signature),
- en intégrité hors exécution par le contrôle d'accès du système hôte,
- en intégrité lors de l'exécution par les fonctions de sécurité du produit.

B4.Logiciel manager Ce bien est protégé:

- en authenticité lors de l'installation,
- en intégrité hors exécution par le contrôle d'accès du système hôte,
- en intégrité lors de l'exécution par les fonctions de sécurité du produit.

B5.Configuration agent La configuration de l'agent comportant notamment la clé d'identification du manager définie par l'opérateur réalisant l'installation. Ce bien est protégé :

- en intégrité hors exécution par le contrôle d'accès du système d'exploitation pour un utilisateur non administrateur,
- en intégrité lors de l'exécution par les fonctions de sécurité du produit,
- en confidentialité grâce aux mécanismes de protection du système d'exploitation pour un utilisateur non administrateur.

Ce bien comprend également la stratégie de détection qui doit être protégée :

- en confidentialité pour un utilisateur non administrateur
- en intégrité pour un utilisateur non administrateur.

B6.Configuration manager La configuration du manager comportant notamment les éléments liés à son interaction avec les services externes, le gestionnaire d'authentification et les agents. Ce bien est protégé:

- en intégrité hors exécution par le contrôle d'accès de l'hôte du manager,
- en intégrité lors de l'exécution par les fonctions de sécurité du produit.

B7.Secrets cryptographiques de l'agent Ce bien regroupe les clés de trafic TLS et autres secrets cryptographiques négociés lors de la connexion de l'agent avec le manager. Ces biens sont protégés en confidentialité et intégrité par le cloisonnement de processus du système d'exploitation hôte sur l'agent (hypothèse H1.Host) et par les fonctions de sécurité du produit.

B8.Secrets cryptographiques du manager Ce bien regroupe les clés de trafic TLS et autres secrets cryptographiques négociés lors de la connexion du manager avec le gestionnaire d'authentification, les services externes, l'exploitation et les agents. Ces biens sont protégés : en confidentialité et intégrité par les mesures de durcissement appliquées sur l'hôte du manager (hypothèse H2.Host Manager) et par les fonctions de sécurité du produit.

Les secrets peuvent être changés par l'utilisateur du produit.

La figure ci-dessous représente la localisation de ces biens :

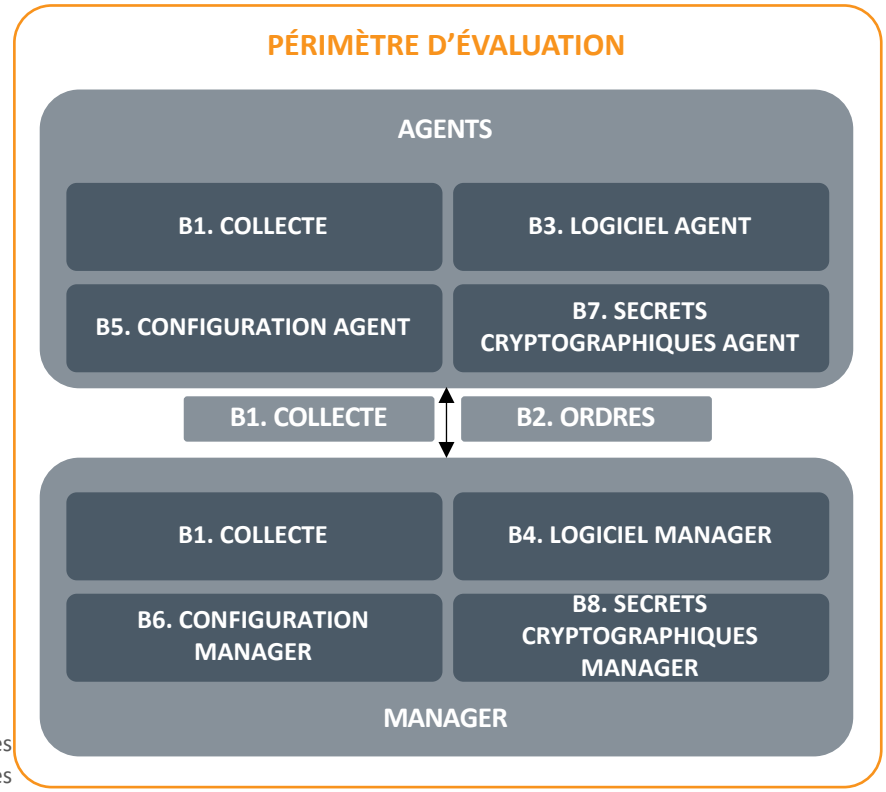

Figure 5 : Schéma des biens sensibles

III.1.3 SYNTHESE DES BIENS SENSIBLES

	Identifiant	Confidentialité	Intégrité	Authenticité
Biens utilisateurs	B1.Collecte	Sécurisation des flux	Sécurisation des flux	Anti-rejeu et chiffrement authentifié
	B2.Ordre	Sécurisation des flux		Anti-rejeu et chiffrement authentifié
Biens du produit	B3.Logiciel agent		Contrôle d'accès OS	Vérification de signature
	B4.Logiciel manager		Protection en fonctionnement	Vérification du condensat
	B5.Configuration agent	Protection OS	Contrôle d'accès OS	
	B6.Configuration manager		Durcissement de la configuration	
	B7.Secrets cryptographiques agent	Cloisonnement des processus	Cloisonnement des processus	
	B8.Secrets cryptographiques manager	Contrôle d'accès	Contrôle d'accès	

III.2 MENACES

III.2.1 MENACES SUR LES BIENS A PROTEGER

M1. Vol de données relatives à l'agent Un attaquant local sans privilège *accède* à **des données confidentielles de l'agent**. Il peut par exemple tenter d'obtenir des données relatives à l'agent comme sa configuration ou des données collectées… (biens B1, B2, B5 et B7).

M2. Altération locale de l'agent sans privilège Un attaquant local sans privilège *accède* à l'agent pour *modifier* **le comportement de celui-ci**. Cette menace ne concerne pas directement des biens protégés par l'agent.

M3. Elévation de privilèges Un attaquant local sans privilège *exploite* une vulnérabilité dans l'agent afin d'élever ses privilèges sur le poste.

M4. Altération de la mise à jour d'un agent Un attaquant local sans privilège ou sur le réseau *cherche à altérer* la mise à jour proposée à un agent par le manager dans le but d'altérer son comportement.

M5. Suppression de traces Un attaquant sans privilège sur le poste *cherche à effacer* ses traces relevées par l'agent dans le cadre d'une déconnexion temporaire d'internet.

M6. Ecoute passive Un attaquant sur le réseau *accède* à **des données confidentielles** échangées entre l'agent et le manager (**B1 et B2**). Il peut par exemple enregistrer le trafic réseau et attaquer le chiffrement a posteriori sur cet enregistrement.

M7. Intrusion réseau Un attaquant sur le réseau *altère* **les données échangées** entre l'agent et le manager (**B1** et **B2**) dans le but d'usurper le manager ou de *lancer* **des opérations non souhaitées sur l'agent**. Il peut par exemple usurper l'identité du manager pour exécuter du code arbitraire depuis l'agent afin de prendre le contrôle de l'hôte.

M8. Intrusion réseau et usurpation d'agent Un attaquant sur le réseau sans accès préalable à la machine de l'agent ni connaissances préalables de la configuration de cet agent *tente d'usurper* **cet agent auprès du manager.**

M9. Compromission par usurpation ou compromission d'agent Un attaquant local qui a compromis un agent utilise cet accès pour **modifier le comportement du manager et de sa configuration (B4 et B6)**. Via une primitive d'exécution de code sur l'hôte du manager, il peut compromettre les données collectées et l'intégrité d'autres services exécutés sur la même plateforme.

M10. Compromission par usurpation d'un service externe Un attaquant externe *utilise* les accès liés aux services externes pour **modifier le comportement du manager et de sa configuration (B4 et B6)**. Via une primitive d'exécution de code sur l'hôte du manager, il peut compromettre les données collectées et l'intégrité d'autres services exécutés sur la même plateforme.

M11. Abus de droits depuis le réseau Un attaquant sur le réseau sans accès préalable à la console *contourne* les mécanismes d'authentification des utilisateurs du manager. Il est ainsi en mesure d'exécuter des opérations non autorisées ou d'accéder à des données sur le manager (absence d'accès initial à la console).

M12. Abus de droits depuis la console Un attaquant avec de bas niveaux de privilèges sur la console (profil analyste) *élève* ses privilèges sur le manager ou usurpe un autre compte auprès du manager. Il est ainsi en mesure d'exécuter des opérations non autorisées ou d'accéder à des données sur le manager.

M13. Divulgation des éléments d'authentification Un attaquant sur le réseau *exploite* une mauvaise configuration du manager pour compromettre les éléments d'authentification du manager et de ses clients.

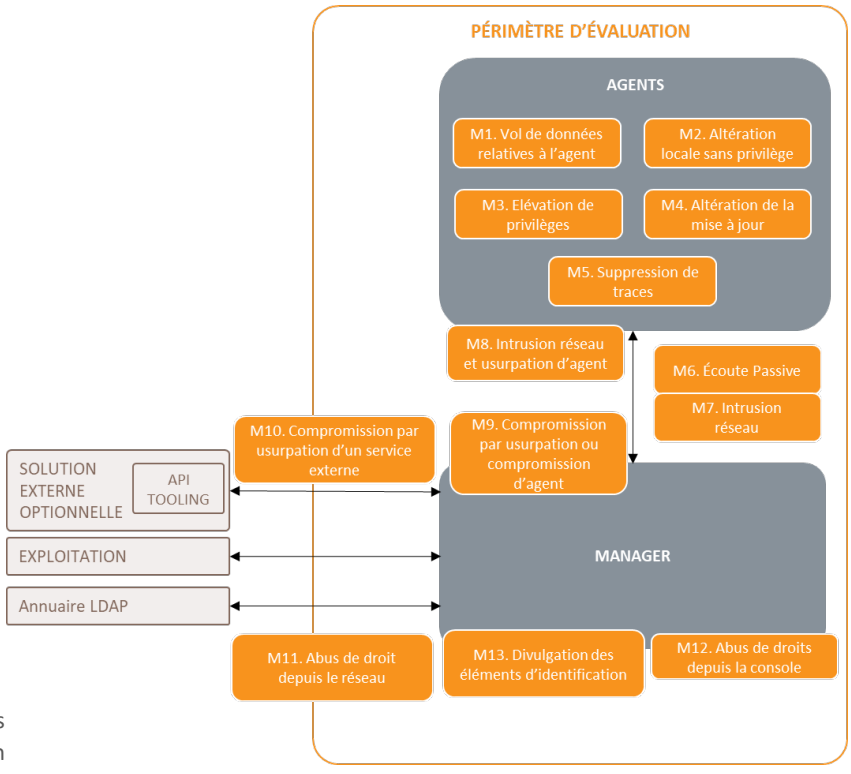

Figure 6 : distribution des menaces sur le périmètre d'évaluation

III.2.2 SYNTHESE DES MENACES

Source de la menace	Identifiant	Biens sensibles	Évènement redouté
Locale sur agent	M1. Vol de données relatives à l'agent	B1.Collecte B2.Ordre B3.Logiciel Agent B5 Config B7 Secrets agent	Accès à des données confidentielles (secrets de chiffrement de disque ou d'autres utilisateurs)
	M2. Altération locale sans privilège	B1.Collecte B2.Ordre B3.Logiciel Agent B5 Config B7 Secrets agent	Modification du comportement de l'agent
	M3. Elévation de privilèges	B1.Collecte B2.Ordre B3.Logiciel Agent B5 Config B7 Secrets agent	Utilisation de l'agent pour élever ses privilèges sur le poste
	M4. Altération de la mise à jour d'un agent	B2.Ordre B3.Logiciel Agent B5. Config	Modification de la mise à jour de l'agent
	M5. Suppression de traces	B1.Collecte B3.Logiciel Agent	Suppression de traces relevées par l'agent
	M9. Compromission par usurpation d'agent	B1.Collecte B2.Ordre B4.Logiciel Agent B6 Config B8 Secrets manager	Modification du comportement du manager (compromission du système hôte)
Attaquant sur le réseau	M6. Ecoute passive	B1.Collecte	Accès à des données confidentielles (enregistrement du trafic réseau)
	M7. Intrusion réseau	B1.Collecte B2.Ordre	Altération des données échangées (usurpation du manager)

Source de la menace	Identifiant	Biens sensibles	Évènement redouté
	M8. Intrusion réseau et usurpation d'agent	B1.Collecte B2.Ordre	Usurpation de l'agent
	M11. Abus de droits depuis le réseau	B1.Collecte B2.Ordre	Abus de contrôle d'accès du manager
	M12. Abus de droits depuis la console	B1.Collecte B2.Ordre	Abus de privilèges sur la console (élévation)
	M13. Divulgation des éléments d'authentification	B8 Secrets manager	Abus d'une configuration faible du manager
Attaquant externe	M10. Compromission par usurpation d'un service externe	B1.Collecte B2.Ordre B4.Logiciel Agent B6 Config B8 Secrets manager	Modification du comportement du manager (compromission du système hôte)

III.3 COUVERTURE DE LA MENACE

III.3.1 FONCTIONS DE SECURITE

F1. Authentification entre agent et manager

Lors de la configuration de l'agent à l'installation, une adresse de manager (collecteur) et une clé d'identification de celui-ci sont définies par l'opérateur réalisant l'installation de l'agent. La clé d'identification est générée à l'installation du manager.

Lors de la connexion, un tunnel HTTPS (HTTP dans TLS) est établi avec le manager qui s'authentifie au moyen d'un certificat x509. Ce certificat est vérifié par l'agent jusqu'à une autorité de certification racine embarquée dans le logiciel de l'agent.

F2. Identification des agents

Chaque agent est identifié de manière unique auprès du manager avec un ID et des secrets cryptographiques qui lui sont propres.

F3. Vérification de mise à jour d'agent

Dans le cadre d'une mise à jour des agents depuis la console, chaque mise à jour de l'agent est vérifiée par celui-ci à travers un mécanisme de signature (RSA 4096) afin de vérifier qu'aucun intermédiaire n'a altéré cette mise à jour.

F4. Confidentialité et intégrité du trafic utilisateur

Les données échangées entre l'agent et le manager sont protégées en confidentialité et en intégrité par cette fonction (tunnel TLS et chiffrement des données).

F5. Cloisonnement de l'exécution sur agent

Le but de cette fonction est de collecter des événements et de traiter les ordres du manager de manière sûre sans que les utilisateurs standards n'aient accès aux informations collectées ou aux ordres reçus. Pour cela, la fonction s'appuie sur les mécanismes de sécurité du système d'exploitation hôte en exécutant ses processus avec des niveaux de privilège interdisant à un utilisateur standard d'accéder aux données et à la mémoire de ces processus et en spécifiant des droits d'accès restreints sur ses fichiers.

Il s'agit notamment du service EDR de l'agent qui s'exécute avec le compte SYSTEM et d'un module noyau, comme illustré par la figure 4.

F6. Protection de l'exécution sur agent

Le but de cette fonction est de renforcer la fonction précédente de sorte que les utilisateurs standards ne puissent pas non plus facilement modifier le comportement de l'agent.

F7. Stockage des données en déconnecté

Dans le cadre d'une déconnexion internet temporaire, les données (télémétrie et alertes) sont enregistrées de manière chiffrée sur le poste.

F8. Limitation des droits utilisateurs sur le manager

Cette fonction a pour but de cloisonner et restreindre les accès d'un utilisateur non-administrateur de la console (analyste) accordés par un administrateur de la console.

Les privilèges peuvent être définis finement par module et au sein d'un même module.

Ainsi, le manager identifie les droits des utilisateurs associés aux différents services offerts et assure une stricte limitation des accès aux seuls droits accordés.

F9. Limitation des droits et isolation des composants manager

Le but de cette fonction est de cloisonner et restreindre au minimum les accès aux entités accédant aux services du manager. Les composants du manager associés à :

- La gestion des agents,
- La gestion des services externes,
- Les connexions des utilisateurs

Sont tous distincts, isolés des composants de traitements, et exécutés avec le minimum de droits nécessaires à leurs besoins opérationnels.

En particulier, du filtrage est réalisé entre ces composants qui ont également été durcis d'un point de vue système.

F10. Vérification des données entrantes

La structure des données reçues par le manager est strictement contrôlée, afin d'assurer que seuls des messages correctement formatés sont traités par le manager. Cette vérification s'applique aux données reçues des sources suivantes :

- Agents,
- Services externes,
- Utilisateurs.

F11. Contrôle d'accès Manager

Authentification des utilisateurs et services externes par utilisation de protocoles sécurisés pour les interfaces réseau, et la configuration durcie d'un service externe d'authentification.

F12. Sécurisation des interconnexions

Les interconnexions d'authentification (LDAP) et de transfert de données (syslog) doivent offrir de respecter les bonnes pratiques de sécurité. En particulier, il est possible et recommandé de chiffrer les communications avec ces services externes (TLS).

III.3.2 COUVERTURE DES MENACES PAR LES FONCTIONS DE SECURITE

	F1. Authentification	F2. Identification des agents	F3. Vérification de mise à jour d'agent	F4. Protection du trafic utilisateur	F5. Cloisonnement de l'exécution	F6. Protection de l'exécution	F7. Stockage des données en déconnecté	F8.Limitation des droits utilisateurs	F9. Limitation des droits et isolation composants	F10. Vérification des données entrantes	F11. Contrôle d'accès manager	F12. Sécurisation des interconnexions
M1. Vol de données relatives à l'agent				X	X							
M2. Altération locale de l'agent sans privilège					X	X						
M3. Elévation de privilèges					X	X						
M4. Altération de la mise à jour d'un agent			X	X								
M5. Suppression de traces					X	X	X					
M6. Ecoute passive	X			X								
M7. Intrusion réseau	X			X								
M8. Intrusion réseau et usurpation d'agent	X	X		X								
M9. Compromission par usurpation d'agent									X	X		
M10. Compromission par usurpation d'un service externe									X	X	X	X

M11. Abus de droits depuis le réseau									X	X	X	
M12. Abus de droits depuis la console								X	X	X	X	
M13. Divulgation des éléments d'identification											X	X