Partagé avec
TLP (Traffic Light Protocol) –
VERT

Approuvé

Norme en matière de journalisation et de suivi de la sécurité des systèmes

ID du document : **SEC-06**
À l'attention de: Fédération de l'Alliance
Approuvé le 2023-03-22
Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

L'objectif de la présente norme est de définir une approche cohérente pour la mise en œuvre des pratiques de journalisation et de surveillance pour toute la Fédération de l'Alliance. Cette norme assurera la détection et l'identification efficaces et précoces des événements touchant la sécurité ou les opérations et permettra l'investigation.

2. Définitions

Pour la définition des termes relatifs à la sécurité informatique, reportez-vous à SEC-00 Glossaire de la sécurité de l'information. Aucune définition spécifique ne s'applique à la présente norme.

3. Applicabilité

La présente norme s'applique à tous les Systèmes et services de la Fédération de l'Alliance, y compris tous les services, systèmes, composants, hôtes (physiques et virtuels), équipements de mise en réseau et applications, ou tous systèmes et services internes ou externes qui prennent en charge directement ou indirectement les services mandatés.

Les Propriétaires de service doivent s'assurer que les services, systèmes ou composants sous leur responsabilité sont conçus, configurés et exploités conformément à la présente norme.

4 Exigences en matière de journalisation et de surveillance

4.1 Activités de journalisation requises

Tous les composants concernés doivent générer des journaux ou des enregistrements, selon le cas, pour les types d'événements suivants :

- **Utilisation des ressources** : Pour chaque ressource allouée via un processus d'allocation, un journal de la ressource effectivement allouée et un journal de sa consommation doivent être enregistrés.
- **Métriques** : Les métriques requises pour évaluer l'état actuel du système ou du service (c'est-à-dire leur disponibilité, performance, utilisation, etc.) doivent être enregistrées.
- **Accès et autorisation** : Tous les événements d'accès et d'autorisation doivent être enregistrés lorsqu'une session initiée par un utilisateur ou par une machine est créée ou rétablie.
- **Authentification** : Tous les événements d'authentification doivent être enregistrés.
- **Activité sur le réseau** : Toutes les activités de communication sur le réseau concernant les données entrant ou sortant d'un périmètre sécurisé d'un site doivent être enregistrées. Il est également recommandé de consigner de la même manière toutes les communications entre les domaines de sécurité internes.
- **Informations sur les actifs** : Les informations sur les actifs doivent être enregistrées conformément aux exigences définies dans *SEC-10 Norme de la gestion des biens de la Fédération de l'Alliance*.
- **Vulnérabilités** : Les informations sur les vulnérabilités doivent être enregistrées conformément aux exigences définies dans la norme *SEC-04 Norme de la gestion des vulnérabilités de la Fédération de l'Alliance.*
- **Utilisation des privilèges** : Pour chaque service, système ou composant, un journal de toutes les escalades de privilèges tentées et réussies doit être enregistré.
- **Audit d'identité** : Pour chaque compte ou identité, les événements relatifs à la création, la modification ou la suppression doivent être enregistrés.

Chaque système ou composant doit être configuré pour s'assurer que son horloge est synchronisée avec une référence de temps fiable et digne de confiance. Chaque système ou composant doit également être configuré pour maintenir la précision de l'heure et pour empêcher la dérive ou la falsification de l'horloge. Dans la mesure du possible, chaque journal ou enregistrement doit avoir une marque d'horodatage conforme au format ISO 8601 et, dans la mesure du possible, mappée sur le Temps Universel Coordonné (UTC), ou utiliser l'heure locale avec un décalage par rapport à l'UTC. L'horodatage doit avoir une résolution temporelle à la milliseconde et l'horloge système doit viser à maintenir une précision compatible avec cette résolution.

Dans le cas où les enregistrements contiennent des identifiants ou des clés uniques qui peuvent changer au fil du temps, un enregistrement de ces modifications doit également être disponible pour garantir l'unicité des enregistrements des journaux.

4.2. Journalisation centralisée

Chaque système ou composant doit être configuré pour enregistrer ses journaux dans un système de journalisation à distance fiable et autorisé. Dans la mesure du possible, un seul système de journalisation doit être utilisé pour un domaine de sécurité. Les événements de journalisation requis identifiés au paragraphe 4.1 doivent être mis à la disposition de la Fédération de l'Alliance via la ou les plateformes de surveillance autorisées par la Fédération de l'Alliance et conformément à toutes les normes de la Fédération de l'Alliance qui sont applicables aux données.

Les systèmes de journalisation et de surveillance doivent être configurés pour détecter et générer des alertes en temps opportun en cas d'erreur système, de perte d'intégrité ou de défaillance ou d'épuisement du stockage qui pourraient empêcher la capture des journaux ou leur exactitude.

4.3. Activités de surveillance requises

Les journaux doivent être utilisés pour détecter ou identifier les anomalies ou les activités suspectes. Il est recommandé de développer des configurations de référence et d'utiliser l'automatisation pour générer des alertes rapidement. Par les activités de surveillance, les journaux seront utilisés par le personnel autorisé pour détecter, alerter, enquêter ou suivre les activités suspectes ainsi que pour signaler l'état et l'utilisation du système ou du service. La surveillance des cas d'utilisation et des configurations de référence doit être documentée, y compris l'identification appropriée des journaux et des ensembles de données requis, ainsi que l'utilisation prévue ou autorisée.

4.4. Contrôle de l’accès

Les systèmes de journalisation doivent être configurés pour limiter l'accès aux personnes ou systèmes autorisés uniquement. Un tel accès doit être limité à l'accès minimal nécessaire pour effectuer les tâches et doit protéger les journaux de toute modification non autorisée. L'accès aux systèmes de journalisation et aux journaux qu'ils contiennent doit être enregistré. L'accès aux journaux ou à leur contenu doit être fourni via une interface ou un système qui empêche la falsification ou la modification des journaux ou des enregistrements.

4.5. Classification et partage des journaux

La classification des données dans les journaux doit être conforme à *SEC-02 Politique de classification des données*. La classification des données par défaut pour les journaux est Information de risque élevé (niveau 3), à l'exception de l'Utilisation des ressources et des Métriques pour lesquels la classification par défaut est Information de risque modéré (niveau 2). Le Propriétaire des données ou l’Intendante ou Intendant des données est responsable de s'assurer que la Classification des données est appropriée et de reclasser au besoin. Toute reclassification doit être documentée et communiquée tout en s'assurant que des systèmes de journalisation appropriés sont utilisés.

Par défaut, les journaux doivent être traités comme étant TLP–AMBRE. Cette désignation signifie que les journaux peuvent être partagés avec la Fédération de l'Alliance selon le principe du moindre privilège et que tout autre partage nécessite l'approbation préalable du Propriétaire des données ou du Gestionnaire des données. Le partage des journaux doit se faire via des plateformes approuvées et conformément à *SEC 03 Norme de gestion des données*.

4.6. Conservation des journaux

Les systèmes de journalisation doivent être conçus pour tenir compte du volume de journaux attendu, y compris les rafales raisonnables potentielles. Les journaux électroniques qui sont collectés doivent être conservés et facilement disponibles pendant une durée minimale de 90 jours. Diverses situations peuvent entraîner la nécessité d'une destruction précoce. Toute situation de ce type doit être documentée et approuvée par le Propriétaire des données ou le Gestionnaire des données.

4.7. Élimination des journaux

À leur fin de vie, les journaux et les systèmes de journalisation doivent être éliminés en toute sécurité et conformément à *SEC-03 Norme de gestion des données*.

5. Information connexe

SEC-00 Glossaire de la sécurité de l'information
SEC-02 Politique de classification des données
SEC-03 Norme de gestion des données
SEC-04 Norme de la gestion des vulnérabilités
SEC-10 Norme de la gestion des biens