< Seuils et Alertes >

Fiche méthodologique

Groupe de travail Gestion de crise et entraînement
Campus Cyber

Juin 2026

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CDSE CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

AMRAE la Maison du risk management

CESIN

BANQUE DE FRANCE EUROSYSTÈME

CLUSIF

CCA Club de la Continuité d'Activité

Cette fiche a pour objectif de partager quels types de seuils et d'alertes peuvent être mis en place pour pouvoir réagir face à des événements de nature cyber. Elle peut également s'appliquer sur d'autres natures d'événements. L'amélioration continue (ajustement des seuils, de la chaîne d'alerte...) est un fondamental qu'il convient d'appliquer en particulier sur cette thématique.

Pour ce faire, il a été jugé pertinent par le groupe de travail de partager en premier lieu les définitions nécessaires. Dans un second temps, sur la base des définitions, une approche d'identification des seuils et alerte cyber est proposée. Finalement, des cas d'usage présents dans des fiches indépendantes permettent d'illustrer les alertes qui pourraient être mises en œuvre dans les principaux scénarios cyber, quel que soit le contexte de l'organisation.

Définitions

Il est important de partager la même terminologie afin de pouvoir se comprendre et pour appréhender ce qui compose la notion d'alerte. Plusieurs termes sont identifiés comme importants pour pouvoir cadrer les informations constitutives d'une alerte de qualité dans une situation d'urgence cyber.

Les définitions proposées ont vocation à aider à la compréhension des fiches et non à servir de référence ou à suppléer toute autre définition de la littérature.

Alerte

L'alerte est un **signal émis pour avertir d'une situation (menace, danger, incident, ...) nécessitant une action de vigilance a minima ou d'actions ou de réactions (urgente ou non)**, dont l'application de consignes ou la mobilisation de ressources complémentaires.
Exemples :

- *Alerter [la direction générale, le DPO, ...] d'une attaque cyber avérée sur les systèmes d'information,*
- *Prévenir les administrateurs de systèmes d'une activité suspecte ou d'une vulnérabilité,*
- *Alerter les utilisateurs de déconnecter du réseau leur ordinateur dans le cadre d'un rançongiciel.*

Une alerte est émise par une source vers un ou plusieurs destinataires. La source peut être humaine ou logicielle, de même pour un destinataire.
Exemples :

- *Système de supervision de la sécurité vers un premier niveau de support sécurité ;*
- *Astreinte exploitation vers une astreinte managériale IT et vers une astreinte de crise.*

De plus, la source peut être **interne ou externe** à une organisation. Il en va de même pour le destinataire.
Exemples :

- *Alerte de sa compromission par un partenaire dont le système d'information aurait été attaqué ;*
- *Notification d'une autorité de régulation.*

Plusieurs vecteurs / moyens peuvent être utilisés pour lancer l'alerte.

Exemples :

- *SMS ;*
- *Courrier électronique ;*
- *Téléphone ;*
- *...*

Le signal est émis lorsqu'un seuil est atteint pour un ou plusieurs critères donnés ou que la source juge que la situation nécessite de prévenir qui de droit (ex. : incertitude dans les faits et impacts mais des conséquences possibles importantes).

Il est important de pouvoir déterminer pour quel motif une alerte doit être déclenchée afin de la faire correspondre au juste besoin des destinataires.

L'alerte doit donc également comprendre la description de l'événement sur lequel porte l'alerte et peut donner une indication de la gravité et de l'urgence de la situation.
La description comporte généralement la notion temporelle, la nature, le numéro de l'incident ou de dossier.
Exemples :

- *28/02/2025- 18h32 - Tentative d'hameçonnage*
- *SSI250136 - Faille de sécurité 0 Day sur serveur Apache v1.2.3 - CVSS 8*
- *20250116 – URGENT - À la suite d'une intrusion dans le SI Logistique le 16/01/2025 à 7 :00, les flux d'accès à Internet ont été coupés*
- *CRISE – CYBER - Mobilisation de la cellule de crise décisionnelle de "l'organisation XXX" à 20h00*

La description peut être plus ou moins exhaustive en fonction de la nature du vecteur de communication utilisé (contenu d'un SMS plus court qu'un mail).

Bulle info : Il est à noter que la chaîne d'alerte peut également permettre de désarmer une escalade réalisée.

Critère

Le critère est un champ d'application d'un seuil ou d'un état.

Exemples :

- *1- Volume de trafic : Un nombre inhabituel de requêtes ou une augmentation soudaine du trafic réseau.*
- *2- Taux d'erreur : Un nombre élevé de tentatives de connexion échouées ou d'erreurs de système.*
- *3- Utilisation des ressources : Un usage anormalement élevé de la CPU, de la mémoire, ou de la bande passante.*
- *4- Activité des comptes : Des connexions provenant de lieux géographiques inhabituels ou à des heures non conventionnelles.*
- *5- Modifications système : Des changements inattendus ou non autorisés dans les configurations ou les fichiers système.*

La combinaison de plusieurs critères peut correspondre à ce qu'une alerte nécessite pour être pertinente.

Seuil

Un seuil est une limite (valeur) ou un changement d'état qui, une fois atteint, peut amener à déclencher une ou plusieurs actions dont l'alerte.
Plusieurs seuils pour un même critère peuvent être définis pour identifier la gravité de l'événement.

Exemples :

- *En supervision, les deux niveaux Critical et Warning sont généralement définis.*

Les seuils sont idéalement définis en amont d'une situation (sur des modèles de référence ou sur la base de l'expérience) mais certains peuvent être définis "à chaud" en fonction du contexte.

Ils dépendent à la fois de la maturité de l'organisation, des contre-mesures mises en œuvre… Au sein d'une même organisation, certains seuils pourront être différents des différentes entités qui la constituent. En effet, le contexte peut modifier l'ampleur de la mobilisation.

Ils doivent être revus régulièrement au regard des incidents ou situations connus, et de l'évolution de l'environnement de l'organisation (enjeux, priorités, …).

Idéalement un seuil est facilement mesurable pour qu'en situation d'urgence il ne soit pas compliqué de l'estimer (les indicateurs d'impacts financiers peuvent être difficiles à estimer rapidement dans le cadre d'un rançongiciel).

Chaine d'alerte / Niveaux de mobilisation

En fonction des organisations et des situations, une alerte peut en entraîner d'autres pour constituer une chaîne d'alertes.
Différents paliers ou niveaux d'alerte peuvent être ainsi définis en fonction de l'organisation ou de la nature de la situation. Chaque niveau peut correspondre à un niveau de mobilisation opérationnel ou décisionnel (Cf. Fiche réflexe sur organisation de gestion de crise) ou à des actions de différentes natures.
Exemples :

- *Incident/Incident Majeur / Pré-crise / Crise ;*
- *Defcon1 / Defcon 2 / Defcon 3 / Defcon4*
- *Vert / Jaune / Orange / Rouge*

Cela constitue un schéma d'escalade ou d'alerte, et permet de matérialiser différents niveaux de mobilisation en fonction de la gravité.

Bulle info : Certaines organisations préconisent la mise en place d'un dispositif complémentaire avec une notion de pré-alerte ou de vigilance à l'approche d'un seuil.
Bulle info : les seuils et critères sont indicatifs, ils sont une aide à la prise de décision mais ils ne doivent pas enfermer l'organisation dans l'appréciation de la situation si jamais les seuils fixés ne sont pas pleinement atteints.
Bulle info : Prendre en compte la notification ou l'information des autres parties prenantes dans la chaine de réaction :

- L'impact des notifications réglementaires (ANSSI, CNIL, ACPR / AMF - DORA)
- L'information des partenaires

Identification des alertes et seuils dans la cybersécurité

Comme le chapitre précédent le suggère, définir les seuils et alertes dans le monde du cyber peut avoir plusieurs objectifs :

- Alerter techniquement d'un événement à prendre en compte,
- Alerter l'organisation d'une mobilisation interne à mettre en œuvre à la suite d'un événement de nature cyber,
- Alerter un tiers à la suite d'un événement

Faire le lien avec la gestion des risques de sécurité des systèmes de l'information est une bonne base pour définir les alertes à mettre en place et à suivre : cela permet de poser le cadre d'identification des critères qui seront à prendre en compte dans la réalisation d'un événement redouté (Cf. EBIOS RM[1]).

Les alertes techniques s'appuieront principalement sur les vulnérabilités et les menaces alors que les alertes organisationnelles relèveront probablement des conséquences possibles et de leur analyse.

Alerte technique

Les alertes techniques doivent être identifiées sur la base des risques et plus particulièrement des menaces. Les scénarios de compromission mis en œuvre dans le cadre de la détection peuvent être une approche pertinente ou des alertes paramétrées au niveau des logiciels ou matériels.

Les alertes techniques peuvent être émises automatiquement ou générées manuellement suite à leur analyse par des équipiers.

Voici quelques cas d'illustration :

- *Alerte du niveau 1 de supervision de sécurité[2] si une élévation de droit est constatée sur un compte d'un actif critique pendant les heures non ouvrées ;*
- *Alerte au responsable de l'exploitation d'un actif dont le processeur est utilisé à 100% en permanence (cas possible d'un crypto miner) ;*
- *Alerte d'un grand nombre de requêtes de résolution de noms pouvant mener à la saturation des services ;*
- *Alerte sur la modification de données sur le système de sauvegarde alors qu'il n'y a pas de sauvegarde planifiée des données en question.*

[1] La méthode EBIOS Risk Manager - Le guide | ANSSI
[2] La supervision de sécurité | ANSSI

Alerte organisationnelle

Plusieurs natures d'alertes peuvent mener à mobilisation pour traiter l'événement, voici quelques exemples :

- Escalade de mobilisation au niveau des équipes techniques comme l'alerte et la mobilisation d'une cellule d'incident majeur ;
- Escalade de la chaine managériale si des conséquences pour l'organisation peuvent amener à des décisions et arbitrages (impact sur : l'image de marque, le financier, l'humain, le juridique, ou l'organisation de l'entreprise en général) ;
- Communication vers les utilisateurs du système d'information pour leur partager des consignes (comme de débrancher leur poste de travail de tout réseau) ;
- Remontée d'alerte pour aboutir à une notification à une autorité régulatrice : les référents auprès des autorités doivent obtenir l'information pour vérifier que cela correspond aux critères et seuils attendus dans la réglementation, le tout généralement dans un délai contraint.
  Exemples d'alertes réglementaires :
  - Déclaration initiale vers la CNIL (sous 72H)[3]
  - Alerter l'ANSSI (aussi rapidement que possible)[4]
  - Notification initiale de l'ACPR dans le cadre de DORA (4h après classification de l'incident ou 24h après sa détection).

Ces différents exemples ne sont pas exhaustifs. Chaque organisation doit identifier en amont, avant la crise, les exigences réglementaires de notification auxquelles elle est soumise.

Alerte de tiers

L'alerte de tiers est très proche de l'alerte organisationnelle mais concerne des parties prenantes extérieures à l'organisation. Voici quelques cas d'illustration :

- Alerte vers des autorités ;
- Alerte vers des partenaires pour leur partager l'information d'une compromission ou des IOC de celle-ci ;
- Alerte des clients (par exemple dans le cas d'un hébergeur) ;

L'alerte peut également venir de la part d'un tiers qui peut observer des anomalies sur le service que vous lui rendez ou par des tiers autres (comme les chercheurs en sécurité qui pourraient découvrir une vulnérabilité sur vos systèmes).

Bulle info : L'IA peut être un atout potentiel dans la classification et l'alerte, en fonction de la maturité du dispositif mis en œuvre

[3] Notifier une violation de données personnelles | CNIL
[4] Contact - CERT-FR