Engineer

Incident

Événement menaçant les données ou le service d'un système

Ce que c’est

Un incident survient lorsqu’un problème dans un système en service devient assez grave pour que les personnes concernées mettent de côté le travail prévu et s’en occupent immédiatement : service qui ne répond plus, enregistrements altérés, machine sans mémoire disponible, compte utilisé par quelqu’un d’autre. La sécurité parle d’« incident de sécurité », l’exploitation d’« incident de production » ou simplement de « panne ». La plupart des organisations les classent en niveaux de gravité.

Le guide de réponse aux incidents du NIST trace trois étapes, valables bien au-delà de la sécurité. Un événement est tout fait observable impliquant des actifs informatiques : tentative de connexion, mise à jour logicielle, application répondant à une requête. Un événement indésirable a une conséquence négative, quelle qu’en soit la cause ; le guide place catastrophes naturelles et coupures électriques à côté des attaques. Un incident est un événement indésirable que quelqu’un a jugé conforme aux critères de l’organisation : le verbe du guide est *déclarer*. Sa définition, tirée du droit fédéral américain, couvre un fait qui menace effectivement ou de façon imminente la confidentialité, l’intégrité ou la disponibilité d’informations ou d’un système, ou qui viole une politique de sécurité.

Sécurité et exploitation emploient le mot avec des centres de gravité différents. En sécurité, il implique généralement un adversaire, une violation de politique ou des données peut-être sorties de l’organisation. En exploitation, il désigne toute interruption imprévue ou dégradation grave du service, sans attaquant. Les deux se recoupent plus que le vocabulaire ne le suggère : une attaque par déni de service et un pic de trafic ordinaire peuvent d’abord se ressembler sur un graphique, et un disque plein peut perdre des données aussi complètement qu’un intrus.

Les mots voisins doivent rester distincts. Un défaut est une imperfection du produit qui peut passer inaperçue pendant des années ; il ne fait partie d'un incident que lorsqu'il commence à causer des dommages. Une alerte est un message annonçant qu'un problème est possible : beaucoup ne deviennent jamais des incidents, et beaucoup d'incidents sont d'abord signalés par un client. La gestion des services suit séparément la cause d'un ou plusieurs incidents, sous le nom de problème.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un incident ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Une supervision et des alertes qui signalent les incidents tant qu'ils restent mineurs, avec les chiffres qui montrent à quelle fréquence ils le restent.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. Premier tableau de bord d'observabilité — première vue de l'entreprise sur ses propres systèmes

Premier tableau de bord d'observabilité Contactez-nous →

Pourquoi c'est important

La décision cachée dans le mot est un seuil. Quand une page lente, une connexion étrange ou une file croissante cessent-elles d'être le ticket d'un ingénieur pour devenir la première priorité de l'équipe ? Si le seuil est trop haut, une intrusion qui se propage est traitée comme une tâche ordinaire par quelqu'un qui n'en voit pas la progression. Trop bas, il interrompt si souvent le travail que déclarer ne veut plus rien dire. Le NIST propose de convenir des critères avant d'en avoir besoin : les événements indésirables deviennent des incidents déclarés lorsqu'ils satisfont des critères déjà définis, tenant compte des faux positifs connus. Des critères écrits avec exemples coûtent bien moins qu'une discussion à deux heures du matin.

La déclaration change les rôles. Une personne dirige et coordonne au lieu de déboguer, d'autres quittent leurs tâches habituelles, un canal porte les faits et un journal horodaté commence. Sans cela, les mêmes personnes dupliquent les mêmes travaux en parallèle et le premier énoncé clair du problème vient d'un client.

Pour certaines entreprises, un délai légal commence aussi. La directive européenne NIS2, directive (UE) 2022/2555, impose aux organisations concernées de signaler un incident important à l'autorité nationale : alerte

précoce dans les 24 heures après en avoir connaissance, notification d'incident dans les 72 heures après cette prise de connaissance et rapport final dans le mois suivant cette notification. Sa définition dépasse les attaques : elle couvre tout événement compromettant disponibilité, authenticité, intégrité ou confidentialité des données ou des services d'un réseau et système d'information ; une panne grave peut donc compter. Une équipe se demandant le deuxième jour « est-ce un incident ? » a déjà consommé la première fenêtre.

Le coût récurrent est le temps consacré par les personnes, plus élevé qu'autrefois. La révision 2025 du guide NIST constate des incidents fréquents dont la récupération prend souvent des semaines ou des mois ; son prédécesseur de 2012 les supposait rares et terminés en un ou deux jours. Les budgéter, c'est prévoir le suivi autant que la nuit elle-même.

À quoi cela ressemble en pratique

Un incident documenté sur ce site concernait une application de bureau macOS. Ses rapports de diagnostic ont enregistré 111 Go de pages compressées sur une machine de 36 Go le 1er septembre 2026 ; un échantillon distinct de l'empreinte mémoire a enregistré une croissance d'environ 41 Mo par seconde pendant une boucle de nouvelles tentatives de connexion émettant des événements du cœur applicatif. L'intervention a trouvé des événements de journal retenus dans un flux principal non borné et copiés à des abonnés qui ne les utilisaient pas. Les tampons ont été bornés, les abonnements filtrés par type d'événement et la journalisation dotée d'un budget de fréquence. Une comparaison d'exécutions complètes de tests a enregistré une baisse de 610 996 lignes du journal du cœur applicatif à 1 411. Ces mesures concernent l'exécution de tests, pas le trafic de production ni la mémoire après correction. Les contrôles d'architecture et tests de budgets applicatifs protègent la conception bornée. Sa politique de débordement peut abandonner des diagnostics répétitifs et rafraîchir l'état affecté ; des mécanismes distincts de délai d'attente à l'arrêt ont nécessité leur propre correction.

D'autres incidents sont récurrents. Huit tunnels WireGuard et IPsec entre Google Cloud et Linux étaient fragiles et lents à diagnostiquer ; un tunnel hors service pouvait couper la communication entre environnements. Le travail a uniformisé leur configuration, supervisé leur état de fonctionnement et attaqué à la racine les problèmes récurrents de routage et d'échange de clés plutôt que de redémarrer les tunnels. Les incidents récurrents de connectivité ont cessé. Quand la même chose arrive une troisième fois, la cause est l'incident.

Certains incidents commencent par une volonté d'aider. Sur une plateforme sans outil d'administration, approuver une demande de reconnaissance de propriété, masquer un avis ou vider un cache revient à un ingénieur avec une console de base de données. La réalisation décrit cela comme lent, non journalisé et à une faute de frappe de l'incident. L'outil interne d'exploitation, environ 40 routes d'administration construites avec 128 composants, place ce travail derrière les mêmes autorisations et la même piste d'audit que le produit, au prix d'une vaste surface interne à maintenir testée et accessible.

Où les problèmes surviennent

Cinq personnes travaillent dessus, personne ne dirige. Le canal de discussion se remplit d'hypothèses, deux ingénieurs annulent des choses différentes et les clients n'ont aucune nouvelle pendant une heure : personne n'a déclaré, donc personne n'a reçu la coordination. Autorisez tout membre de l'équipe à déclarer et faites du premier acte la désignation d'une personne responsable de la vue d'ensemble et du journal.

Le même incident revient à quelques semaines d'intervalle. La réponse s'arrête au retour du service et un redémarrage fait office de solution. Traitez le rétablissement du service et l'élimination de la cause comme deux tâches : terminez la première cette nuit-là et donnez à la seconde un responsable et une date avant de retourner dormir.

L'outillage aggrave l'incident. Une ligne de journal par événement produit un journal aussi grand que le défaut, et les règles d'alerte envoient des centaines de notifications pour une seule cause. Fixez des budgets aux journaux et alertes à l'avance, regroupez les répétitions et testez le chemin de signalement sous la charge de la panne signalée.

La réparation cause l'incident suivant. Une modification urgente tapée à la main en production corrige un symptôme, crée un autre problème et laisse un trou dans la chronologie nécessaire à la revue. Gardez une courte liste d'actions de récupération préapprouvées laissant une trace et enregistrez tout changement pendant l'incident.

Les enseignements arrivent des mois après ou sous forme de reproches. Une revue après des semaines de récupération se souvient de peu ; demander qui a fauté apprend à cacher l'erreur suivante. Le guide révisé NIST recommande souvent de partager les enseignements dès leur identification. Ses

recommandations de récupération se terminent par un rapport après action sur l'incident, les mesures et les enseignements. Notez ce qui rendait l'erreur facile et changez-le.

Pour aller plus loin

- Incident — Définitions des publications NIST, chacune accompagnée de la loi ou norme dont elle vient.
- SP 800-61 Rev. 3 — Recommandations NIST de 2025, organisées selon les fonctions CSF 2.0 plutôt qu'un cycle unique de réponse.
- Cadre de cybersécurité — Cadre dont les fonctions Gouverner, Identifier, Protéger, Détecter, Répondre et Récupérer structurent le guide d'incident.
- RFC 2350 : attentes envers la réponse aux incidents de sécurité informatique — Bonnes pratiques actuelles de l'IETF sur ce qu'une équipe de réponse devrait publier à son sujet.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un incident ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/incident/