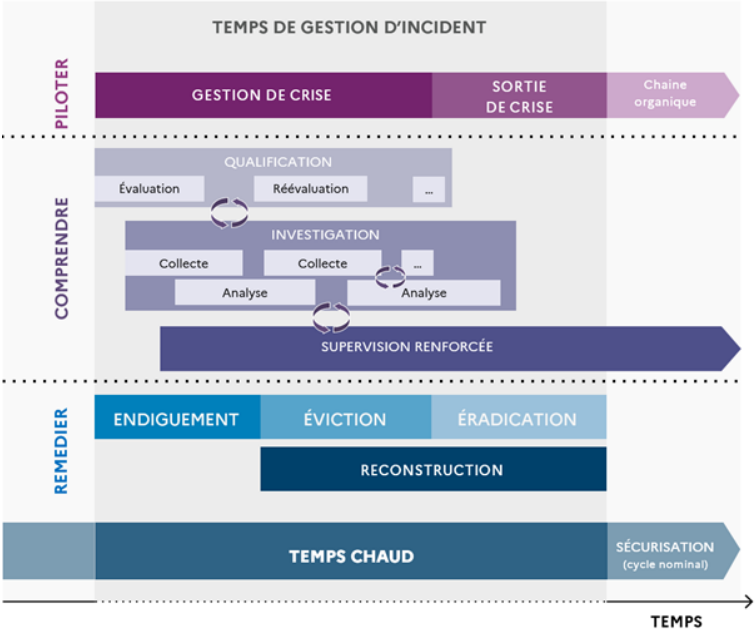
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

L'INVESTIGATION ET LA QUALIFICATION D'INCIDENTS : LES CLÉS DE DÉCISION

COLLECTION
INVESTIGATION

L'ANSSI publie un ensemble de guides sur l'investigation, qui décrit les principes du pilotage et de la mise en œuvre d'une qualification et d'une investigation au sein d'une organisation affectée par ou soupçonnant un incident de sécurité. Ces guides se concentrent uniquement sur les incidents de cybersécurité d'origine malveillante. Ils sont complémentaires des guides de gestion de crise permettant de s'organiser en prévision de la survenue d'un incident [1], et dont certains accélérateurs indispensables sont repris ici ; ainsi que des guides sur la remédiation [2]. L'objet du présent document, de niveau stratégique, est de définir les principaux piliers conceptuels pour orienter les décideurs dans la compréhension des incidents de cybersécurité touchant leur organisation.



1. Guide crise cyber : https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/
2. Guide remédiation : https://cyber.gouv.fr/securisation/gestion-de-crise/piloter-la-remediation-dun-incident-cyber/

La qualification et l'investigation sont, avec la remédiation et la gestion de crise, des dimensions majeures de la réponse à incident cyber (atteinte aux activités ou espionnage).

La qualification d'un incident se définit comme une estimation de la gravité avérée et potentielle d'un incident, pour déterminer un engagement adapté aux impacts métiers et aux risques identifiés. Elle permet de distinguer les incidents a priori traitables dans un processus habituel de réponse à incident défini par l'organisation de ceux qui nécessitent un dispositif et une attention particulière.

L'investigation d'un incident se définit comme l'acquisition d'une connaissance technique sur un incident, afin d'en comprendre les impacts, d'identifier le périmètre compromis et d'effectuer les choix les plus appropriés, notamment en matière de remédiation.

Une supervision renforcée et dédiée à un incident permet d'enrichir la compréhension technique en apportant plus de visibilité sur les actions en cours de l'attaquant, par exemple en ajoutant des signatures ou configurations spécifiques aux outils de supervision existants, en déployant des outils de supervision supplémentaires, ou encore en augmentant le niveau de vigilance des équipes de supervision sur le périmètre compromis. Certaines mesures de supervision renforcée peuvent être pérennisées après la résolution de l'incident afin de détecter une reprise d'activité malveillante similaire.

L'ensemble de ces étapes constitue la phase de compréhension d'un incident. Celle-ci est indispensable à la mise en œuvre d'une remédiation efficace et adaptée aux caractéristiques précises de l'incident, utile à la recherche d'une maîtrise du coût global de l'incident, et potentiellement nécessaire au respect de certaines obligations légales (CNIL, RGPD, assurance). Elle se conduit en parallèle et en interaction avec les autres dimensions de la gestion de crise et de la remédiation.

COMPRENDRE UN INCIDENT : UN PROCESSUS MULTI-ITÉRATIF

La phase de compréhension d'un incident peut être décrite en utilisant plusieurs typologies d'itérations :

- L'itération qualification – investigation : l'investigation éclaire la compréhension de la compromission. Dès que les enjeux associés à l'incident évoluent significativement, il convient de relancer une phase de qualification pour confirmer ou redéfinir l'engagement adapté au traitement de l'incident ;
- L'itération collecte – analyse : l'analyse des premières données collectées met en évidence un périmètre effectivement compromis et les actions précises de l'attaquant. La détection d'un élargissement de ce périmètre, la découverte de méthodes d'attaques spécifiques ou encore l'activité continue de l'attaquant sont des raisons motivant une nouvelle collecte ;
- L'itération investigation – supervision : l'investigation fournit des éléments techniques permettant de focaliser la supervision dédiée à l'incident. Cette dernière permet alors d'observer de l'activité en cours de l'attaquant, à prendre en compte dans l'investigation.

LES ACCÉLÉRATEURS DE L'INVESTIGATION

La compréhension de l'attaque et des enjeux associés s'appuie sur des connaissances tierces dont l'acquisition au préalable constitue un facteur important de réussite et d'accélération des investigations :

- La cartographie du système d'information [3] ;
- Les vulnérabilités présentes dans celui-ci, identifiées via des audits et des analyses de risque [4] ;
- La nature des menaces et leurs objectifs respectifs [5] ;

3. Guide cartographie : https://messervices.cyber.gouv.fr/guides/cartographie-du-systeme-dinformation
4. Guide risque : https://messervices.cyber.gouv.fr/guides/maitrise-du-risque-numerique-latout-confiance
5. Bulletin CTI du CERT-FR : https://www.cert.ssi.gouv.fr/cti/

- Les périmètres d'administration de chaque équipe technique, interne ou prestataire, avec des points de contacts actionnables [6].

La capacité à investiguer est également conditionnée à la capacité du système d'information à conserver des traces des activités antérieures et à les protéger.

Tous ces éléments se préparent en dehors de tout incident et font partie des bonnes pratiques de gestion des risques sur un système d'information. Ils constituent des éléments clés dans le choix d'une stratégie d'investigation. Ces accélérateurs permettront d'être plus efficace dans les investigations et donc de réduire leur coût mais pas de répondre à toutes les questions.

LES LIMITES DE L'INVESTIGATION

Les investigations d'incident d'origine malveillante se font dans un cadre particulier, avec des attaquants potentiellement dynamiques et réactifs à nos actions : ils peuvent poursuivre leur attaque, prévoir une entrée alternative, se mettre en veille… Ces attaquants peuvent également supprimer ou brouiller les traces qu'ils laissent pour tromper les investigateurs.

La plupart des investigations sont confrontées à des incertitudes sur les activités réelles de l'attaquant. La levée de ces incertitudes n'est pas toujours possible ou souhaitable au regard des coûts et des contraintes induites par de tels approfondissements. Ces incertitudes doivent faire l'objet d'une analyse de risque, être validées par le bon niveau hiérarchique et être prises en compte lors de la remédiation. Par exemple, l'absence d'investigation sur l'infrastructure d'hypervision pourrait laisser une porte dérobée et conduire à la mise en échec de l'ensemble de la réponse à incident. A contrario, une investigation poussée de cette infrastructure pourrait être coûteuse et décevante si aucune activité malveillante n'est découverte.

Il est indispensable d'anticiper la collecte et le prétraitement des informations nécessaires à l'investigation. Les systèmes d'information

6. L'absence d'accord de niveau de service (SLA) adapté aux incidents urgents dans les contrats d'infogérance peut entraver la mise en place rapide de l'investigation.

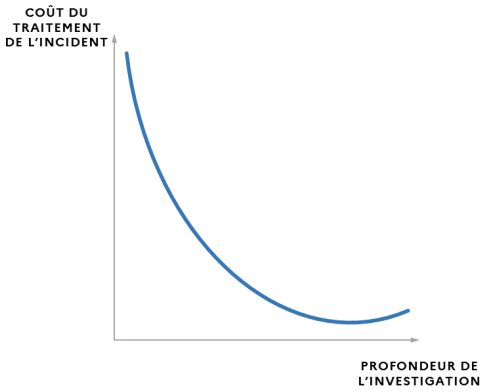
stockent un volume très important de données et se comptent en centaines ou milliers d'équipements. Une collecte d'équipement peut prendre plusieurs heures avant tout traitement et analyse. Même correctement anticipée grâce aux accélérateurs, l'investigation peut donc prendre beaucoup de temps avant de fournir des éléments caractérisant la menace sur le système d'information.

La prise en compte de ces incertitudes et ces délais est essentielle dans le choix d'une stratégie d'investigation adaptée à ses objectifs stratégiques.

BIEN CHOISIR SON PLAN D'INVESTIGATION : UN JEU D'ÉQUILIBRISTE

L'identification des objectifs stratégiques à atteindre lors de la réponse à incident, orientés par les besoins et les responsables métiers, permet de choisir un plan d'investigation adapté.

L'investigation ne doit pas être simplement pensée comme un coût et un retard à la reprise d'activité, mais comme un investissement permettant de comprendre les actions de l'attaquant pour mieux le combattre. La volonté de reconstruire trop vite peut être le fait d'une pression financière (perte de production), d'une mécompréhension du risque (retour rapide de l'attaquant probable) ou de facteurs externes à l'entreprise (pression médiatique, sentiment de honte). Ces facteurs peuvent être partie prenante du choix de stratégie d'investigation mais ne devraient jamais être les seuls car potentiellement de mauvais conseillers dans ce genre d'événement.



Un équilibre est à rechercher afin de minimiser le coût global de l'incident. Tout investiguer en détail coûte cher en temps et en ressources mais ne pas assez investiguer peut coûter cher en entraînant une remédiation inefficace et une présence renouvelée d'un attaquant. Prendre des mesures drastiques d'endiguement peut coûter cher en interrompant les processus métier mais laisser un attaquant actif peut coûter cher en prolongeant ou aggravant les conséquences de l'attaque. Cet équilibre dépendra de la taille de l'entreprise, des ressources internes et externes, de la taille et de la complexité du système d'information, des impacts métiers de la compromission, et restera un choix réalisé et ré-évalué dans une situation incertaine.

Ce guide propose plusieurs stratégies d'investigation, archétypes qu'il convient d'adapter à chaque situation. Le plan d'investigation n'est pas figé dans le temps, et plusieurs stratégies peuvent être utilisées successivement selon l'évolution de l'incident et de la compréhension que l'on en acquiert.

Stratégie 1 - « Investigation sous isolement »

Cette stratégie consiste à couper l'ensemble des accès réseau entre le système d'information compromis et tout autre système (internet, interconnexions). Elle permet de réaliser des investigations sans que

l'activité malveillante ne puisse se poursuivre[7]. Elle ne privilégie pas la discrétion par rapport à l'attaquant qui sera alerté de la perte de ses accès.

> **Application pratique** le rapport gain-coût de cette option est généralement favorable lorsque des destructions ou des atteintes de systèmes d'information sont considérées imminentes, ce qui est souvent le cas des rançongiciels.

Investiguer à l'abri de nouvelles actions de l'attaquant permet d'effectuer plusieurs itérations collectes-analyses et d'approfondir celles-ci sans avoir à les remettre en question au moment de la remédiation, parce que l'attaquant ne peut plus interagir avec le système d'information compromis.

Le choix de cette stratégie implique des arbitrages décisionnels ; ce n'est pas qu'un choix technique. Cet isolement implique un fonctionnement dégradé du métier et est rarement tenable dans la durée sur des périmètres importants en raison des coûts et de la surcharge de travail qu'elle engendre. Dans certains cas, l'isolement n'est pas possible, notamment lorsque la connectivité en continu des équipements compromis est impossible à interrompre au regard des enjeux métier, ou quand la cartographie complète des interconnexions n'est pas connue.

Stratégie 2 - « Investigation en environnement dégradé »

Cette stratégie consiste à privilégier la remédiation au détriment de l'investigation, lorsque l'attaquant a causé des destructions importantes au système d'information.

> **Application pratique** cette option est subie, au vu des destructions importantes déjà causées par l'attaquant. L'objectif de l'investigation est alors d'éclairer la reprise d'activité.

Le niveau de dégradation du système d'information rend plus simple la mise en œuvre de mesures radicales d'isolement et de remédiation puisque les fonctions métier sont déjà gravement atteintes.

7. Des actions déjà initiées ou programmées par l'attaquant avant la coupure peuvent tout de même se poursuivre.

L'obtention de la connaissance via ce mode d'investigation est complexe, du fait de la perte d'information. L'investigation en environnement dégradé change les enjeux de l'investigation :

- L'attaquant était-il déjà présent dans les systèmes restaurés ?
- Quelle date choisir pour la restauration ?
- Comment empêcher l'attaquant de revenir ?
- Comment répondre aux obligations légales sur les données auxquelles l'attaquant a potentiellement accédé ?

Ces questions sont importantes à répondre rapidement car les opérations de restauration s'appuient potentiellement sur le matériel compromis et impliquent de supprimer les traces associées.

Stratégie 3 - « Observer et contraindre »

Cette stratégie consiste à observer en temps réel les actions de l'attaquant et à réagir le plus rapidement possible en coupant systématiquement ses accès au moment où ceux-ci sont identifiés. Elle ne privilégie pas la discrétion par rapport à l'attaquant qui sera alerté de la perte de ses accès au fur et à mesure.

Cette stratégie d'observation repose sur des mesures de détection en temps réel (EDR, sondes, ...) et des équipes en capacité de traiter des alertes. Lorsqu'elle est applicable, l'impact métier est très faible et le coût de l'investigation est réduit.

Application pratique si la détection de l'activité malveillante survient dès son commencement, que la visibilité sur cette activité est jugée très bonne, il devient favorable de couper tout accès le plus tôt possible afin d'éviter la propagation de l'attaquant.

Une qualification erronée du périmètre effectivement compromis, éventuellement liée à un mauvais jugement de la capacité à superviser les activités malveillantes, entraînerait une inefficacité complète de cette stratégie, l'attaquant rétablissant ses accès au fur et à mesure que certains sont coupés tout en épuisant les équipes en charge de cette stratégie.

Stratégie 4 - « Observer et laisser faire »

Cette stratégie consiste à observer en temps réel[8] les actions de l'attaquant afin d'obtenir une compréhension la plus exhaustive possible de ses capacités. On recherche alors un niveau de discrétion fort et des mesures doivent être prises afin de limiter la possibilité pour l'attaquant de prendre connaissance des informations et actions liées à la réponse à incident.

Application pratique le rapport gain-coût de cette option est généralement favorable lorsque l'analyse des éléments techniques disponibles ne permettra pas de couvrir l'ensemble des activités malveillantes, par exemple lorsque l'attaquant est présent depuis longtemps et que les chances de son retour sont fortes, ou que les capacités de supervision préalables à l'incident sont insuffisantes.

Cette stratégie d'observation repose sur des mesures de détection en temps réel (EDR, sondes, ...), éventuellement déployées spécifiquement en réponse à l'incident, et des équipes en capacité de traiter des alertes. Elle permet d'identifier des lacunes dans la détection et de les combler.

Dans cette stratégie, l'attaque continue d'évoluer et les conséquences de l'attaque continuent d'être subies. Il convient alors de définir les lignes rouges guidées par le métier qui, du fait du risque inacceptable induit, impliquent une bascule vers une autre stratégie et par exemple la mise en place d'un isolement.

Stratégie 5 - « Investigation exploratoire »

Cette stratégie consiste à réaliser des investigations sur un périmètre potentiellement large et à rechercher toute activité malveillante quels que soient ses liens avec une activité déjà connue.

8. Sur la base de journaux générés par des équipements de supervision, avec un temps éventuellement différé.

Application pratique cette option peut être choisie à la suite d'un signalement d'incident peu précis (levée de doute) ou pour une recherche sur un plus large périmètre (chasse) avant une remédiation. Elle vise à identifier la présence d'un potentiel attaquant sur le système d'information.

Cette investigation est agnostique à la menace. Elle permet donc d'éviter un effet « œillères » où l'on se concentrerait exclusivement sur un type de menace préalablement identifié. Elle entraîne de plus peu ou pas de perturbations sur le SI.

La mise en avant de comportements suspects nécessite une bonne connaissance des pratiques métier et une homogénéité de celles-ci. Une trop grande hétérogénéité entraînerait un coût très élevé d'investigation. La recherche doit également être correctement cadrée pour conserver la maîtrise des ressources qui y sont affectées : rechercher sans piste initiale à suivre peut également coûter cher.

CONCLUSION

Sur la base des éléments de ce document, une compréhension technique de l'incident a été établie, en suivant un plan d'investigation en accord avec les objectifs stratégiques définis. Cette compréhension permet de réaliser sereinement la remédiation du système d'information et donc d'assurer la reprise des activités. Le volet stratégique du guide de remédiation [9] permet de guider ces étapes. Les équipes de pilotage et d'exploitation peuvent quant à elles s'orienter vers les volets respectifs opérationnels et techniques des différents corpus.

9. Guide remédiation : https://cyber.gouv.fr/securisation/gestion-de-crise/piloter-la-remediation-dun-incident-cyber/

POUR ALLER PLUS LOIN : SEPT RECOMMANDATIONS POUR RÉUSSIR SON INVESTIGATION

Répondez aux objectifs stratégiques

La qualification éclaire la prise de décision et l'identification des objectifs stratégiques de la réponse à incident. L'investigation aide à répondre à ces objectifs stratégiques et également à leur réévaluation.

Évitez les idées fixes

La connaissance du patient zéro est souvent mise en avant. Pour des attaques anciennes ou destructrices (type rançongiciel), celle-ci n'est plus forcément atteignable ni l'enjeu prioritaire de l'investigation.

Préservez les traces

Les collectes doivent être reproductibles, centralisées et préservées de toutes altérations. L'inventaire et la réalisation d'empreintes des éléments collectés en valident l'intégrité et seront indispensables dans le cadre de la judiciarisation de l'incident.

Tracez votre analyse

Une investigation doit être traçable et répétable afin d'être objective et opposable dans le cadre de la judiciarisation de l'incident.

Pensez aux angles morts

Une absence de traces d'attaquants est-elle une absence d'activité malveillante sur ce périmètre ou un manque de visibilité sur le système d'information ?

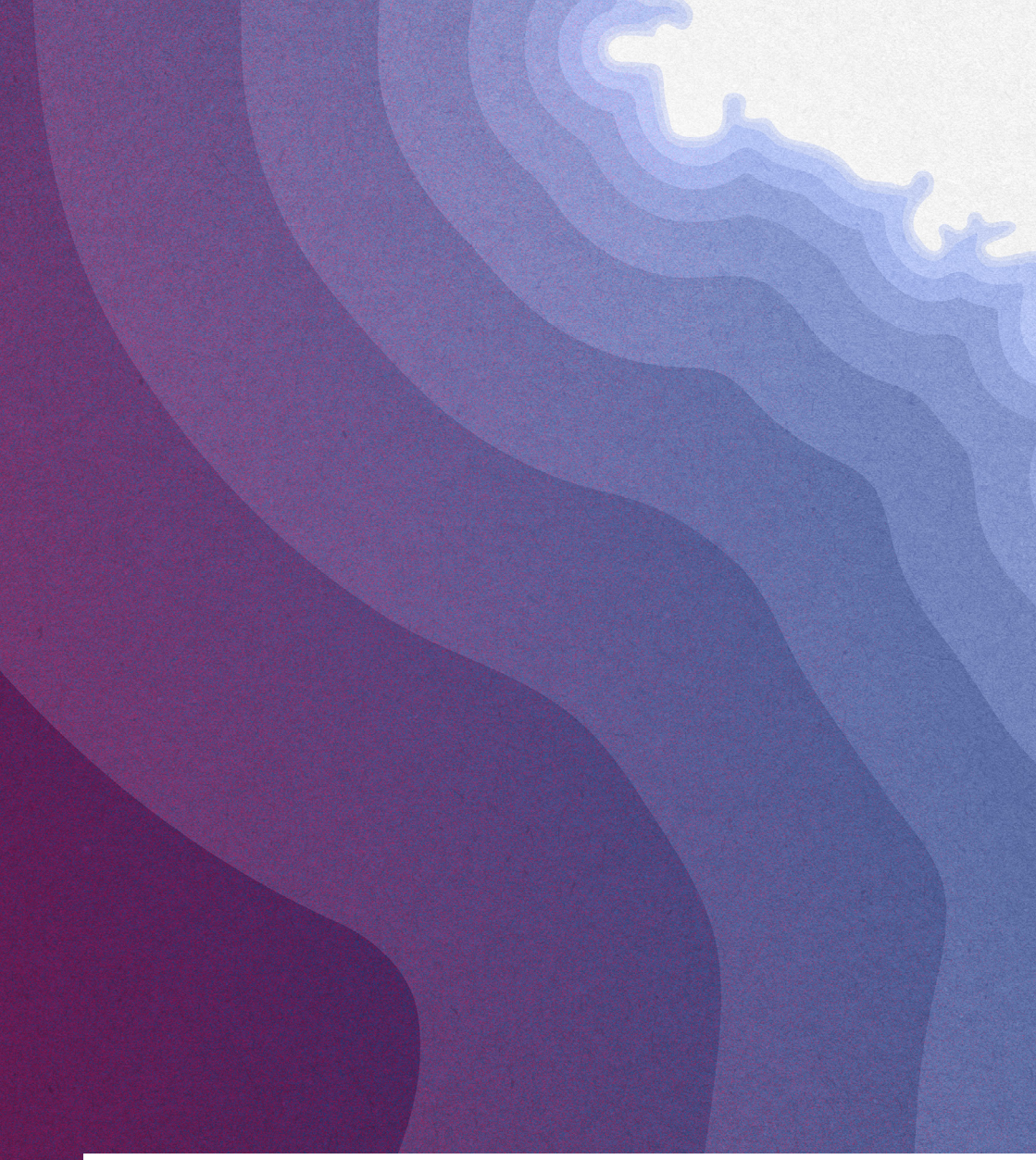
Pensez attaquant

La connaissance des atouts ou activités métiers d'intérêt de l'organisation peut permettre de supposer une cible de l'attaquant et donc de déterminer un périmètre initial de recherche et les chemins d'accès ainsi que les critères pour les lignes rouges du cadre de l'investigation.

Ne restez pas seul

Des expertises spécialisées doivent être mobilisées pour réaliser les investigations. Des prestataires de réponse à incident, comme les PRIS [10] qualifiés par l'ANSSI ou d'autres autodéclarés sur le site Cybermalveillance [11], peuvent être contactés, ainsi que les différents centres de réponse aux cyber-incidents [12] (CSIRT).

10. PRIS : https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/pris/
11. https://www.cybermalveillance.gouv.fr/
12. Ministériels, sectoriels, territoriaux ou national (CERT-FR).



Version 1.0 – Septembre 2026

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr