SERVICE DE RÉPONSE À INCIDENT DE SÉCURITÉ

BESOIN D'ASSISTANCE POUR RÉPONDRE À UN INCIDENT DE SÉCURITÉ ?

Notre équipe de réponse à incident est joignable
du lundi au dimanche inclus, de 8h30 à 22h30, UTC+1(*).

+33 (0)1 40 17 91 28

CSIRT@lexfo.fr – Clé publique PGP : CSIRT-LEXFO_public_key.asc

(*) Ces horaires peuvent être étendus en J7/H24 contractuellement.

Prise de connaissance du contexte client

Levée de doute

Rétro-ingénierie de code malveillant

Analyse forensique

Depuis près de 8 ans, LEXFO a développé une **activité de réponse à incident de sécurité**, aujourd'hui structurée et organisée autour d'une **équipe** et d'un **système d'information dédiés**, au profit de nombreux acteurs issus de secteurs tels que les transports, la grande distribution, le numérique, la communication, l'audiovisuel, la banque, les assurances, les collectivités territoriales, etc.

LEXFO est aujourd'hui engagé dans un processus de qualification piloté par l'ANSSI, en vue de **devenir prestataire de confiance en matière de réponse à incident (PRIS)**, au titre du décret du 27 mars 2015 relatif à la qualification de produits de sécurité et de prestataires de service de confiance pour les besoins de la sécurité nationale.

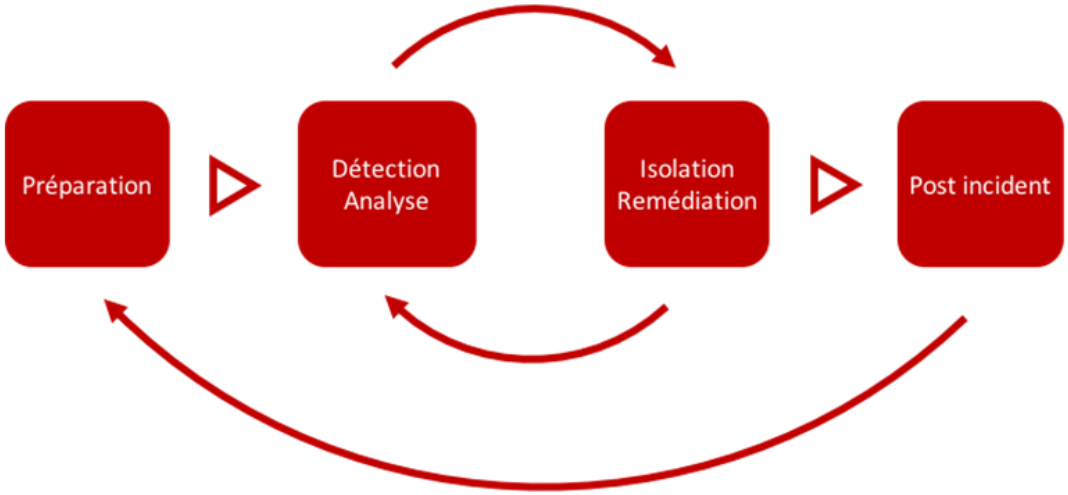
Notre approche

PRÉPARATION

La **phase de préparation** permet à toute entreprise confrontée à un incident de sécurité de se préparer à répondre rapidement et efficacement à ce dernier, tout en préservant les éléments de preuve nécessaires aux investigations post-incident.

DÉTECTION / ANALYSE

La **phase de détection** permet de repérer les artéfacts pouvant être caractéristiques d'un incident de sécurité.
L'**analyse** permet d'investiguer en détail afin d'identifier le mode opératoire des attaquants et de déterminer l'ampleur de l'incident.



ISOLATION / REMÉDIATION

La **phase d'isolation** permet de contenir l'incident de sécurité pour éviter une surinfection à l'échelle des actifs numériques de l'entreprise.
La **remédiation** permet de traiter en profondeur l'incident en supprimant toute trace de celui-ci sur le SI pour revenir à des conditions nominales de fonctionnement.

POST-INCIDENT

Enfin, la **phase post-incident** doit servir à tirer profit des étapes préalables de façon à identifier les manquements, mettre en œuvre les moyens de protection nécessaires et enclencher un cercle vertueux dans le traitement des incidents de sécurité.

Pour chaque phase, LEXFO vous propose un accompagnement adapté au contexte, au type d'incident et à vos besoins. Ces différentes étapes peuvent ainsi s'avérer nécessaires ou optionnelles en fonction des cas.

Nos services

Prise de connaissance du contexte client

Dès lors que vous souscrivez au service de réponse à incident de LEXFO en amont de tout incident de sécurité, ou préalablement à toute réponse à incident, les équipes de LEXFO procèdent à une prise de connaissance du contexte et de votre environnement, afin de permettre à l'équipe d'analyse d'être la plus réactive et la plus efficace possible dans le cadre de la réponse à incident.

Levée de doute

Cette activité a pour objectif, en cas d'alerte par le commanditaire, de recueillir un ensemble d'informations attestant d'un incident avant de déclencher une prestation de réponse à incident.

Analyse et rétro-ingénierie de code malveillant

Le domaine d'expertise des analystes de LEXFO couvre tous les types de *malware* : *malware* bancaire, *Nation State Sponsored malware* de type *Advanced Persistent Threat* (APT), *malware Fileless* résidant uniquement en mémoire, *ransomware*, *malware* plus exotique.

Analyse forensique

LEXFO propose des analyses forensiques de machines (postes de travail, serveurs), de téléphones mobiles, etc. selon la méthodologie suivante :

- Phase 1 : Collecte des informations
- Phase 2 : Analyse des artéfacts collectés
- Phase 3 : Synthèse des analyses et capitalisation des IoC*

**Indicators of compromise ou indicateurs de compromission*

Notre équipe

LEXFO mobilise ses experts les plus compétents en fonction des typologies d'incidents :

- **Directeur de mission ou Responsable de l'équipe d'analyse** chargée notamment d'organiser toutes les tâches au sein de l'équipe d'analyse, d'assurer la coordination avec vos équipes et de vous communiquer les synthèses d'investigation de manière claire et concise.
- **Analyste de codes malveillants** (spécialiste en rétro-ingénierie de logiciels malveillants) pour la compréhension d'une charge malveillante (malware, ransomware, scripts malveillants, etc.) ayant touché l'un de vos actifs.
- **Analyste système et/ou réseau** pour la récupération et l'investigation de données sur de multiples composants d'infrastructure.

Nos engagements

- **Expertise** : Une expertise dans les différents métiers de la réponse à incident (pilotage de mission, analyse système/réseau, analyse et rétro-ingénierie de codes malveillants) et un engagement dans les processus de qualification des services d'audit de la SSI (PASSI) et de réponse à incident de sécurité (PRIS) pilotés par l'ANSSI.
- **Disponibilité & Réactivité** : Notre équipe de réponse à incident est joignable du lundi au dimanche inclus, de 8h30 à 22h30. Une procédure d'urgence nous permet d'être réactifs en heures ouvrées et non ouvrées (intervention sur site en 4h en Région parisienne, 24h en France métropolitaine, 48h au sein de l'Union européenne et 96h à l'International).
- **Méthodologie** : Une approche offensive de la sécurité via l'utilisation de méthodologies équivalentes à celles des cyberattaquants, renforcée par une veille quotidienne des nouvelles attaques de sécurité au travers du CSIRT-LEXFO.
- **Moyens logistiques et matériels** : Un système d'information dédié et sécurisé et un investissement en matière de R&D et d'innovation nous permettant de développer des solutions dédiées à l'investigation forensique et à l'analyse de codes malveillants.
- **Suivi & Reporting** : Une plateforme dédiée et sécurisée vous permettant de suivre les investigations et les analyses et de dialoguer avec notre équipe.
- **Livrables** : Des comptes-rendus périodiques (formels et téléphoniques), un rapport final d'investigation (incluant les IoC détectés), un plan de remédiation (recommandations directement actionnables), des scripts de détection d'IoC, etc.
- **Confidentialité :** Afin d'assurer la confidentialité des informations échangées, LEXFO met en place des moyens de communication sécurisés préalablement au commencement de chaque réponse à incident et vous transmet une convention de service dans un délai de 4h à compter de votre sollicitation.
- **Langues** : Nos ressources sont disponibles en français et en anglais.
- **Éthique** : En dix ans d'existence, la réputation de LEXFO s'est construite sur de fortes valeurs d'indépendance, d'intégrité, de rigueur et de réactivité, partagées par l'ensemble de nos collaborateurs via la signature d'une Charte dédiée.

CONTACTEZ-NOUS

Notre équipe de réponse à incident est joignable
du lundi au dimanche inclus, de 8h30 à 22h30, UTC+1(*).

+33 (0)1 40 17 91 28

CSIRT@lexfo.fr – Clé publique PGP : CSIRT-LEXFO_public_key.asc

(*) Ces horaires peuvent être étendus en J7/H24 contractuellement.