Recherche de compromission & réponse à incident

LE CERT AMOSSYS

Lorsqu'une concordance de signaux permet de soupçonner ou d'attester une activité informatique malveillante au sein de votre système d'information, il est indispensable de réagir rapidement en faisant appel à un prestataire capable d'identifier si votre système est compromis et, si c'est le cas, de prendre les mesures pour rétablir et renforcer sa sécurisation.

La solution AMOSSYS

Expert de la cybersécurité, AMOSSYS a mis en place un CERT (Computer Emergency Response Team) pour vous permettre d'anticiper et d'appréhender tout incident de sécurité pouvant affecter vos systèmes d'information ou votre patrimoine informationnel. Le CERT AMOSSYS met à votre disposition trois prestations complémentaires : la réponse à incident, la recherche de compromission et la recherche d'indicateurs de compromission pour vous permettre de pallier toute situation critique.

→ En cas d'incident de sécurité avéré : la réponse à incident

Le CERT AMOSSYS dépêche sur place **en moins de 24h** son équipe d'intervenants experts et vous accompagne durant toute la phase de crise et au-delà.

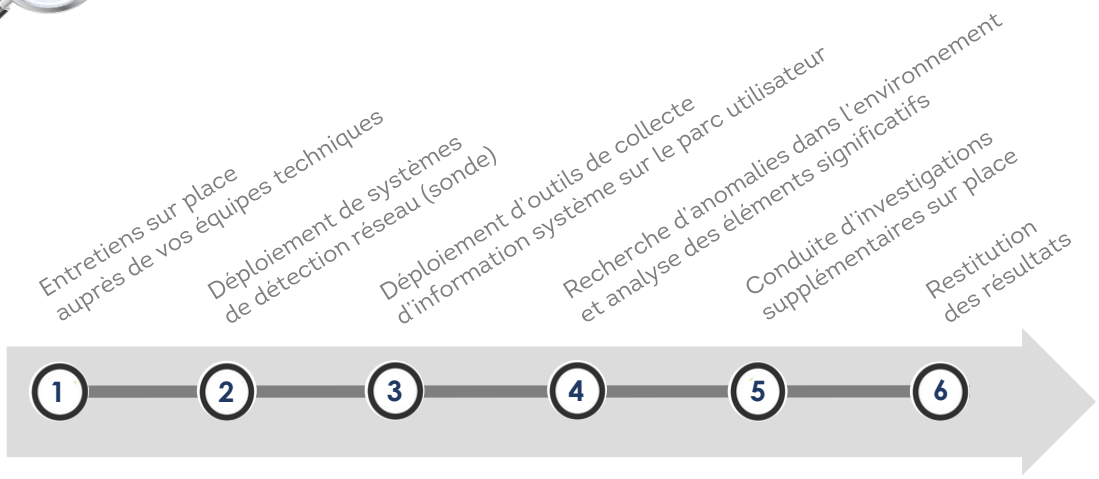
→ En cas de suspicion d'incident : la recherche de compromission (hunting)

La recherche de compromission vous permet de détecter si votre système a été corrompu et s'il existe des attaques en cours. Recherche opportuniste dans le cadre d'audit de sécurité ou pour définir un niveau de confiance de l'intégrité du système d'information, la recherche de compromission met en œuvre les mêmes techniques et outils dédiés que ceux utilisés en réponse sur incident et est effectuée par les mêmes équipes techniques expérimentées. Elle représente une étape indispensable pour s'assurer de la sûreté totale de votre système.

→ Selon le contexte opérationnel : la recherche d'indicateurs de compromission

La recherche d'indicateurs de compromission vise à déterminer si une menace spécifique peut être identifiée sur le système d'information. Cette recherche est beaucoup plus rapide qu'une recherche de compromission générique puisqu'elle est davantage ciblée. AMOSSYS met à disposition ses outils dédiés de collecte d'information ainsi que son savoir-faire technique lors de l'exploitation des résultats.

Trois prestations, une même démarche



Vos bénéfices clients

Des réponses concrètes

Le diagnostic établi par nos équipes lors d'une recherche de compromission vous permettra de savoir avec certitude si votre système a été compromis et de connaître précisément l'ampleur et la gravité de la compromission.

Une synthèse des activités malveillantes

Réponse sur incident, recherche de compromission ou d'indicateurs de compromission, nous vous fournissons une synthèse complète sur la chronologie de l'attaque ou le logiciel malveillant (malware) en cause.

Des recommandations

Sur la base de leur diagnostic, nos experts vous livrent leurs recommandations pour endiguer immédiatement les dommages et améliorer la sécurité du système à plus long terme.

Nos atouts

- ✓ Une équipe formée et expérimentée dans le traitement des incidents de sécurité.
- ✓ Des outils de recherche et de collecte spécifiques développés en interne.
- ✓ Une veille active sur les cyberattaques (Threat intelligence).
- ✓ Une expertise éprouvée en analyse de logiciel malveillant.
- ✓ Un rapport complet remis à l'issue de notre intervention.

Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) agréé par l'ANSSI et accrédité par le COFRAC

Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI-LPM) qualifié par l'ANSSI

Certificateur agréé par l'ARJEL

Accrédité évaluateur eIdas pour la sécurité des transactions électroniques

CERT AMOSSYS

Titulaire du label France Cybersecurity

www.amossys.fr

4 bis Allée du Bâtiment
35000 RENNES
Tel : 02 99 23 15 79
contact@amossys.fr