MINISTÈRE
DES ARMÉES

État-major des armées

Voir le fil d'Ariane

Présentation des fondamentaux de l'audit des systèmes CYBER

Direction : État-major des armées / Publié le : 27/04/2022

Les Matinales de la division audit de l'inspection des armées (IDA) sont l'occasion de faire rayonner la culture de l'audit auprès des organismes d'évaluation sous la responsabilité du CEMA et, pour les auditeurs internes, d'approfondir leurs connaissances au regard de la technique et de l'environnement d'audit. A cet égard, les systèmes d'information (SI) prennent une place croissante dans la plupart des processus audités.

Présentation des fondamentaux de l'audit des systèmes CYBER -

Si les auditeurs n'ont pas à proprement parler vocation à auditer des SI, ils doivent

cependant être capables d'apprécier dans quelle mesure ils concourent à la performance des processus et à la fiabilisation des données. C'était tout l'objet de l'intervention de l'ingénieur civil défense hors classe Martial Ruellan, chef du bureau « synthèse cybersécurité » au groupement de la cyberdéfense des armées (GCA) de Rennes.

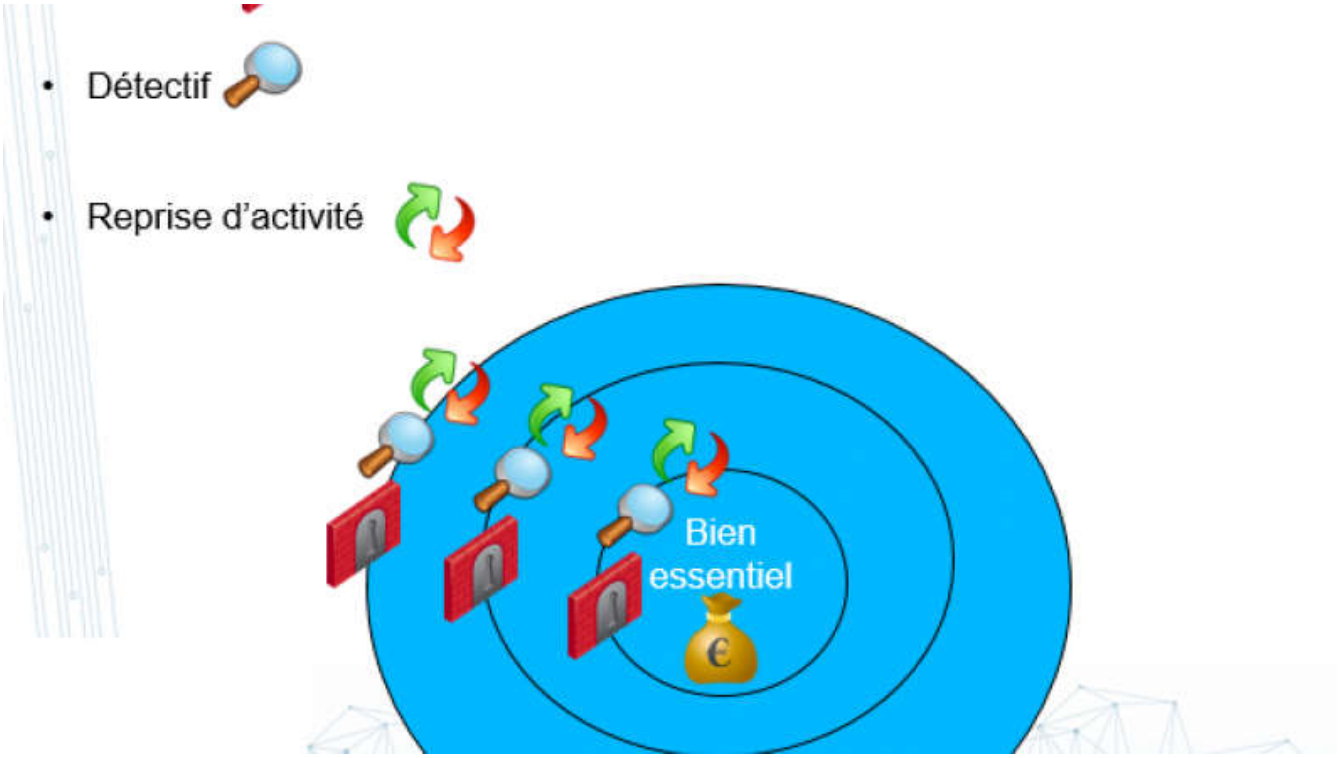
Outre le corpus de normes régissant ces audits spécifiques, la présentation a mis en lumière certains fondamentaux permettant d'appréhender l'audit des SI. Ainsi, la sécurité des systèmes doit être appréciée à travers plusieurs critères tels que la confidentialité, la disponibilité, l'imputabilité, l'authenticité et l'intégrité, cette dernière étant la pierre angulaire de la sécurité. Celle-ci est portée par les trois fonctions *préventive* (contrôles d'accès), *détective* et de *reprise de l'activité* après attaque.

Chaque système doit donner lieu à une analyse des risques selon une équation intégrant les vulnérabilités et les menaces en miroir. Le risque s'apprécie notamment au regard de l'enjeu majeur ou du « bien essentiel » à protéger et qui doit déterminer la mise en place d'un dispositif dit de « défense en profondeur ». L'objet des audits de sécurité des SI réside ainsi dans la mise en évidence des failles (vulnérabilités) du système et l'évaluation des dispositifs de défense déployés. *In fine*, l'auditeur se prononce sur le niveau d'exposition du système au risque.

Pour établir ce diagnostic, l'auditeur interne examine les failles techniques (tests) et les failles organisationnelles (description des processus, actualisation du référentiel du système).

Au-delà de la complexité de nos organisations qui peuvent constituer des failles organisationnelles, l'intervenant a surtout insisté sur la nécessité d'un pilotage fin des risques notamment par une bonne visibilité du niveau de sécurité de l'ensemble des SI.

Dans l'écosystème foisonnant des nouvelles conflictualités, le cyber constitue une couche offrant des opportunités d'action mais aussi des vulnérabilités qu'il convient de maîtriser : cette matinale a parfaitement démontré comment l'audit concourait à ce défi.



Présentation des fondamentaux de l'audit des systèmes CYBER -