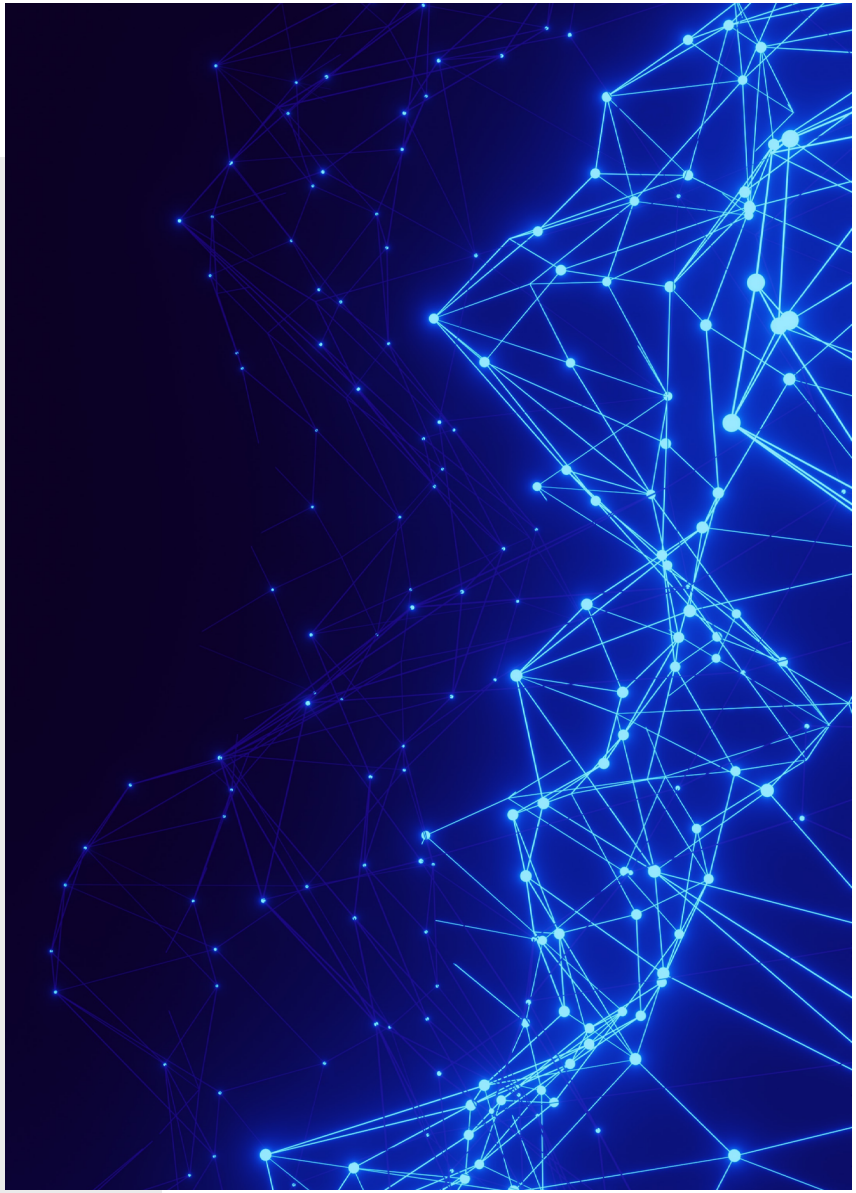
< LIVRE BLANC : GESTION DES VULNÉRABILITÉS >

IDENTIFIER ET TRAITER LES VULNÉRABILITÉS AFFECTANT LES LOGICIELS, LES PROGICIELS, LES COMPOSANTS LOGICIELS ET LES INFRASTRUCTURES



< REMERCIEMENTS >

Ce livre blanc est le fruit d'échanges coanimés par Julie GOMMES (AXA) et Anthony CHARREAU (Crédit Mutuel Euro-Information), et du travail de :

- ALARDET Eric (Yogosha)
- BEAULIEU Benoit (Dattack)
- BREEDSTRAET Robert (Amadeus)
- CECILE Geoffroy (Sopra-Steria)
- CERDAN Vanessa (Cap Gemini)
- CHARREAU Anthony (Crédit Mutuel Euro Information)
- CORDIVAL Laurent (Headmind Partners)
- CORTES Sylvain (Hackuity)
- CREACH Jean-Baptiste (Sanofi)
- ERARD Patrick (Pôle d'Excellence Cyber)
- FIORUCCI Fabrice (Amadeus)
- GACHIGNARD Franck (Air France-KLM)
- GOMMES Julie (AXA)
- GUILLOT Yann (Amadeus)
- KHALIL Ayman (Red Alert Labs)
- KOLLA Vladimir (Patrowl)
- LESAGE Nadege (AntemetA)
- MASSONI Lauren (Wavestone)
- PARTOUCHE Johnathan (Accenture)
- PETERSEN Axel (Wavestone)
- PEYRON Lauranne (Headmind partners)
- POMMIER Christophe (Michelin)
- VALENTIN Yann (BPCE)

Le groupe de travail tient à remercier :

- La SAS Campus Cyber, et plus particulièrement Angèle GUILBERT et Alice Aude BABOLACK NISSACK, pour avoir facilité l'organisation de nos réunions de travail et apporté de précieuses suggestions et conseils
- Yann VALENTIN (BPCE) pour avoir débuté l'animation de ce groupe de travail avant d'évoluer vers d'autres fonctions
- Le groupe Banques, Assurances et Services Financiers du Campus Cyber pour les travaux de préfiguration de ce livre blanc réalisés en 2022.

< SOMMAIRE >

< SOMMAIRE >

< SOMMAIRE >

INTRODUCTION

Ce groupe projet a été constitué au sein du Campus Cyber et s'est appuyé sur le travail préliminaire du groupe banques, assurances et services financiers réalisé en 2022 sur la même thématique.

Le déclencheur est la problématique majeure rencontrée avec la vulnérabilité CVE-2021-44228 baptisée « log4shell ». Publiée le 9 décembre 2021[1], elle touche le composant « log4j » utilisé dans le développement d'applications Java/J2EE. Ce composant est maintenu par l'Apache Software Fondation et largement utilisé dans le monde. La vulnérabilité permet une exécution de code à distance, sans avoir de privilège particulier et avec peu de moyen d'atténuer la capacité à l'exploiter.

L'ANSSI, via son « Panorama de la menace informatique 2022 » publié le 24 janvier 2023, rappelle que « *l'exploitation de vulnérabilités disposant de correctifs est encore trop souvent observée, notamment dans le cadre des incidents traités ou rapportés à l'ANSSI et ce malgré la publication d'avis et d'alertes sur le site du CERT-FR ou de campagnes de signalement. L'ANSSI appelle à l'application prioritaire des correctifs sur les systèmes exposés sur Internet ou, à défaut, la mise en place de mesures de contournement* ».

De plus, l'ANSSI indique que « *Le groupe [Kinsing] se démarque également par l'automatisation de l'exploitation de vulnérabilités comme Log4J, exploitée deux jours après sa divulgation* ».

L'identification et le traitement très rapide des vulnérabilités les plus critiques et/ou sur les actifs (assets) les plus sensibles, mais plus généralement de toutes les vulnérabilités, est donc un enjeu de premier plan, en réponse à un risque qui l'est tout autant. Dès 2014, le CLUSIF publiait un livre blanc sur la gestion des vulnérabilités.[2,3]

L'exploitation d'une vulnérabilité peut être la première étape d'une cyberattaque (obtention d'un accès initial à un Système d'Information) et/ou un moyen d'augmenter la portée et l'impact d'une attaque déjà en cours (élévation de privilèges de l'attaquant ou latéralisation de l'attaque vers d'autres systèmes non impactés jusqu'alors).

La surface à protéger est immense, et tous les éditeurs de logiciel, y compris de premier plan, sont concernés par l'existence de failles dans leur code avec une tendance de volumétrie en hausse. Cela s'inscrit dans ce que le CESIN qualifie de « *sorte de fatalité de la médiocrité numérique* » où la publication de nombreuses vulnérabilités, et parfois graves, devient une sorte de normalité pour les éditeurs et avec laquelle les responsables informatiques doivent s'accommoder en appliquant régulièrement les correctifs de sécurité.

Le présent livre blanc est le livrable du groupe de travail. Il s'adresse notamment aux responsables informatiques et sécurité de structures de toutes tailles, publiques comme privées, disposant de leurs propres équipes informatiques ou sécurité, ou ayant recours aux services d'intégrateurs. Ce livre blanc peut également être utilisé par des équipes juridiques ou communication travaillant sur la gestion des crises.

Il propose une méthodologie pour identifier, prioriser et traiter les vulnérabilités affectant :

- Les logiciels : développés par des équipes internes de l'organisation ;
- Les progiciels : issus du commerce ou disponibles en source ouverte ;
- Les composants logiciels : librairies, cadriciels (frameworks), dépendances intégrées dans des logiciels ou progiciels utilisés par l'organisation ;
- Les éléments d'infrastructure : serveurs, postes de travail, équipements réseau, appliances en boite noire, équipements industriels.

Ce livre blanc détaille les étapes d'identification de nouvelles vulnérabilités, d'analyse préliminaire, de communication interne et externe, de traitement et éventuellement de gestion de crise.

Il énonce par ailleurs les bonnes pratiques recommandées par le groupe de travail pour limiter ou supprimer l'impact des vulnérabilités.

Bonne lecture.

[1] https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
[2] Gestion des vulnérabilités informatiques tome 1 https://clusif.fr/wp-content/uploads/2015/09/clusif-2014-gestion-vulnerabilites-tome-1.pdf
[3] Gestion des vulnérabilités informatiques tome 2 https://clusif.fr/wp-content/uploads/2016/04/clusif-2015-gt-gestionvulnerabilites-tome2_vf.pdf

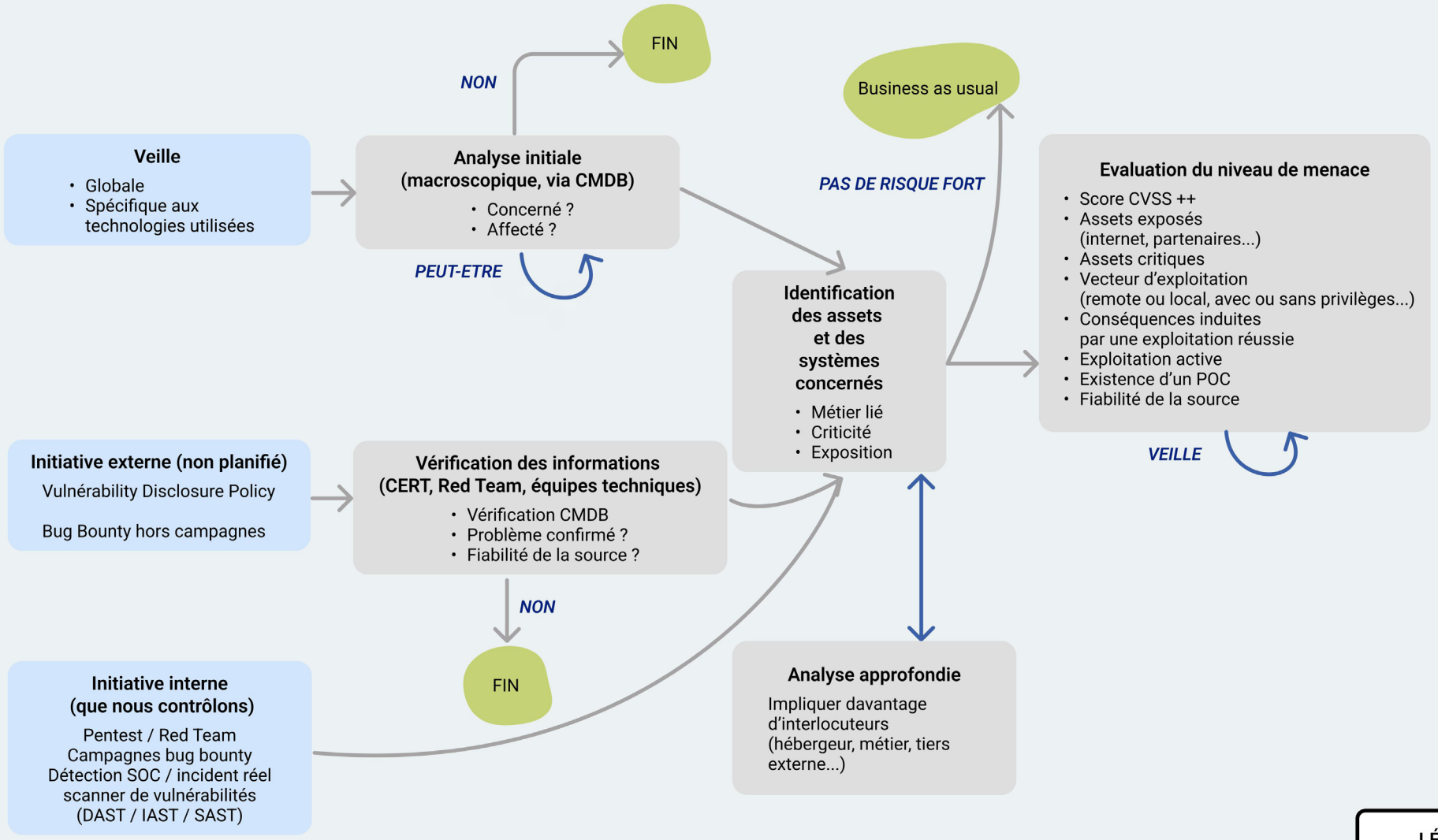
INFOGRAPHIE RÉCAPITULATIVE

Afin de vous accompagner dans l'identification et le traitement des vulnérabilités affectant les logiciels, composants logiciels et les infrastructures, le logigramme suivant vous propose une méthodologie en 4 étapes :

CAMPUS CYBER

IDENTIFICATION DÉTECTION

ANALYSE

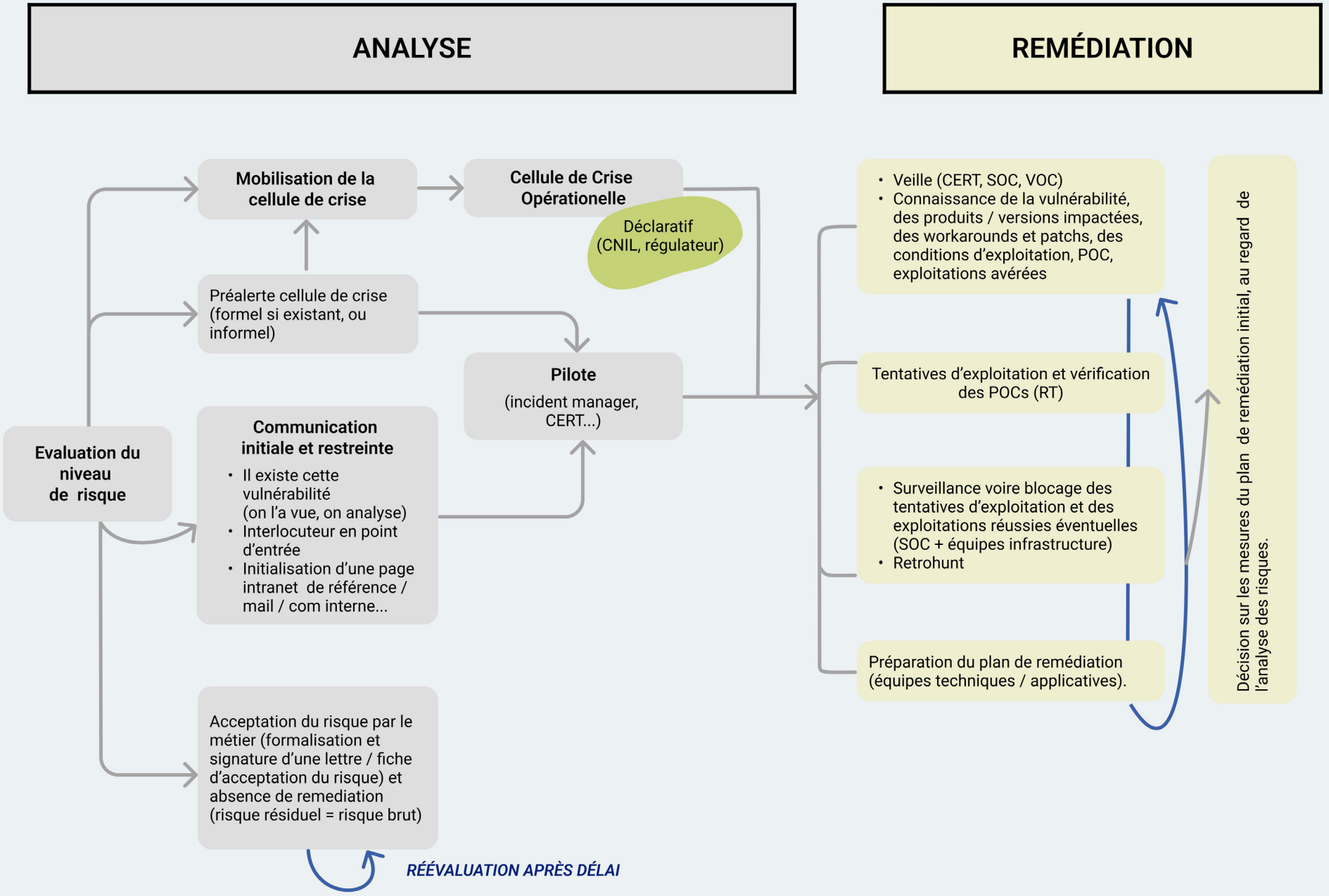


LÉGENDE

Suites possibles

Processus itératif

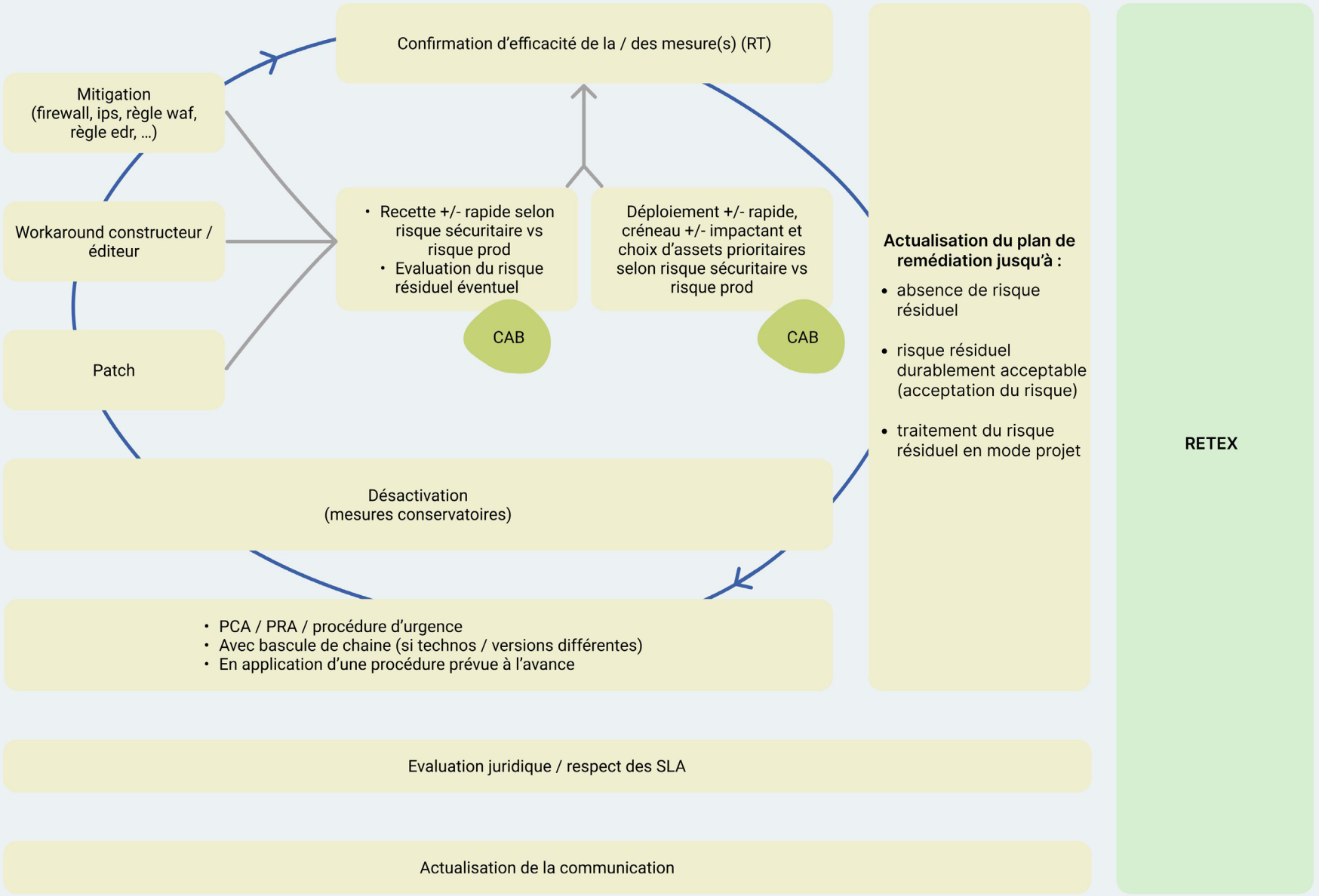
CAMPUS CYBER



CAMPUS CYBER

REMÉDIATION

RETEX



VEILLE

GÉNÉRALITÉS

Afin d'identifier les nouvelles vulnérabilités pouvant affecter le système d'information d'une entreprise, il est nécessaire de réaliser une **veille** sur la publication des nouvelles vulnérabilités et de surveiller les menaces associées (publication de code d'exploitation, attaque exploitant une de ces vulnérabilités…).
Un des **prérequis** pour réaliser une veille efficace est d'avoir un **inventaire** des différentes technologies et produits utilisés dans son entreprise : systèmes d'exploitation, intergiciel (middleware), logiciels, progiciels intégrés, microcode (firmware), systèmes industriels (SCADA) …
Différentes approches complémentaires sont possibles pour réaliser cette veille :

- Veille globale, pour être informé des vulnérabilités et menaces majeures tout produit confondu ;
- Veille spécifique par éditeur ;
- Veille spécifique aux technologies utilisées via un service de veille en vulnérabilités, gratuit ou commercial.

VEILLE GLOBALE

Différentes sources d'information sur Internet permettent d'être informés des vulnérabilités majeures et des vulnérabilités affectant les principaux éditeurs informatiques :

- **Sources gouvernementales ou institutionnelles**

Un grand nombre de pays dispose de leur propre CERT publiant sur leur site web des avis et des alertes de sécurité, par exemple :

  - CERT-FR (centre gouvernemental français de veille, d'alertes et de réponses aux attaques informatiques)
    https://www.cert.ssi.gouv.fr/
  - CERT-EU (CERT des institutions et agences de l'Union européenne)
    https://cert.europa.eu/publications
  - CISA (agence américaine de cyberdéfense)
    https://www.cisa.gov/news-events/cybersecurity-advisories
    https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **Communautés sécurité**

Des associations comme :

  - L'InterCERT France propose un canal de discussion pour partager les vulnérabilités majeures, restreint aux membres de l'association ;
  - L'OSSIR présente chaque deuxième mardi du mois la revue d'actualité sécurité, dont des vulnérabilités, ouverte à tous.

- **Sites web spécialisés sur la sécurité informatique**

Différents sites web d'information sur la sécurité informatique, de blog d'éditeurs de produits de sécurité publient des articles sur les nouvelles vulnérabilités majeures et sur les principales menaces liées à ces vulnérabilités (publication d'exploit, attaques en cours).
Ces différentes sources d'information peuvent proposer différents moyens pour être alertés : liste de diffusion par mail, flux RSS, X (exTwitter)…

VEILLE SPÉCIFIQUE PAR ÉDITEUR

D'après son inventaire, il est possible de réaliser une veille par éditeur. En fonction des éditeurs, il peut être plus ou moins facile de suivre les nouvelles vulnérabilités impactant leurs produits :

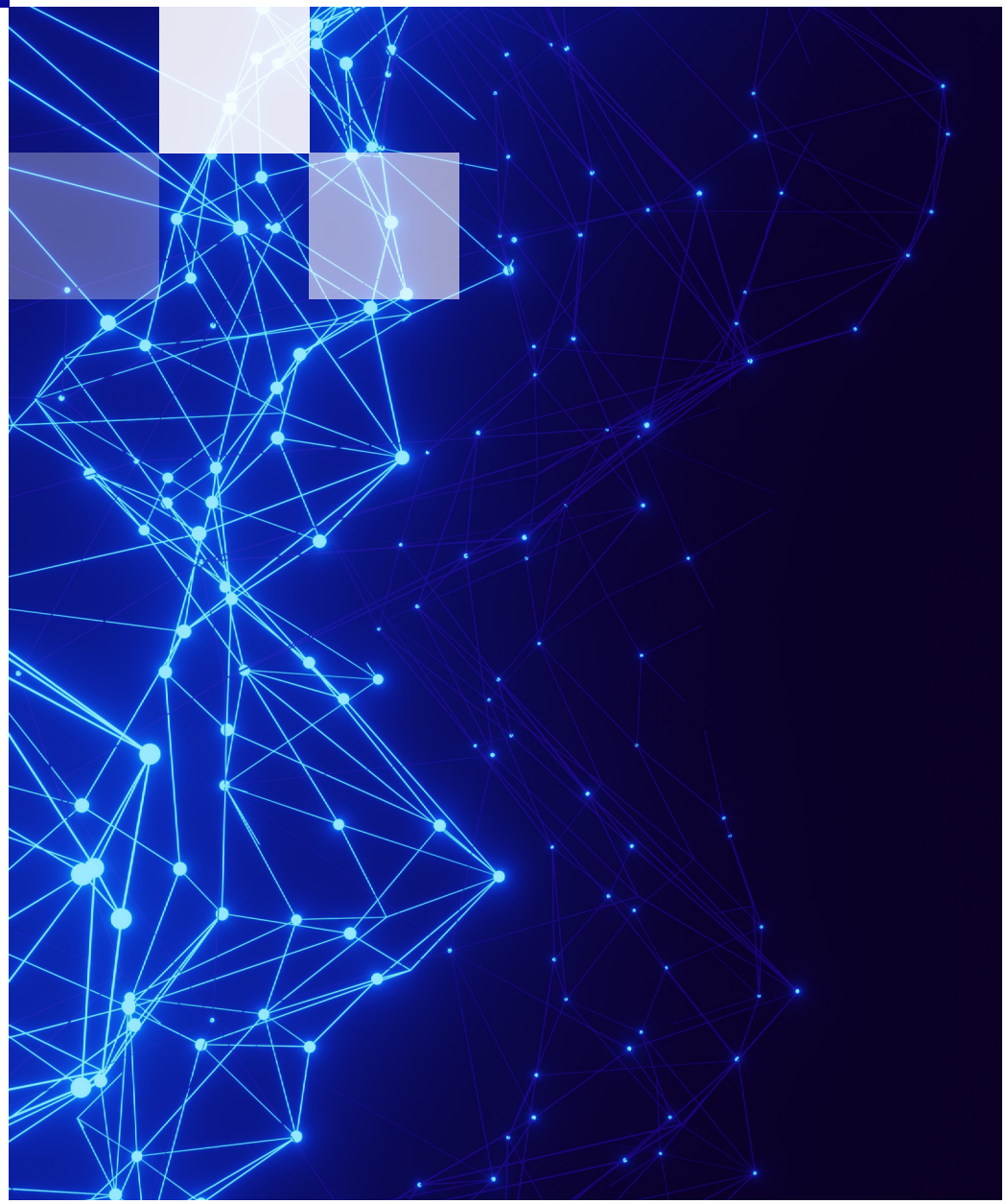
- Dans le meilleur des cas, l'éditeur publie des avis de sécurité sur une page dédiée de son site web et envoie des alertes par mail. Ces avis comportent tous les détails des nouvelles vulnérabilités incluant les versions des produits affectés, la sévérité, la référence CVE, le score CVSS et la solution qui est généralement l'application d'un correctif de sécurité ou d'une configuration de contournement ;
- Dans un niveau de suivi intermédiaire, il est possible :
  - D'avoir des informations sur les vulnérabilités corrigées dans les ChangeLog des nouvelles versions d'un produit.
  - De rechercher dans la base NVD (base de données publiques américaines de vulnérabilités basées sur les références CVE) les nouvelles vulnérabilités publiées pour un éditeur (https://nvd.nist.gov/vuln/search).
- Dans le pire des cas, il peut n'y avoir aucune information disponible.

Certains éditeurs publient de façon périodique leurs correctifs de sécurité pour corriger les vulnérabilités de leurs produits par des bulletins :

- Mensuel (par exemple Microsoft, Adobe, SAP…) ;
- Trimestriel (par exemple Oracle) ;
- Sans fréquence particulière (par exemple les distributions Linux, Apple…).

SERVICE DE VEILLE DE VULNÉRABILITÉ DU MARCHÉ

Une veille individuelle de chaque éditeur ou constructeur et une analyse humaine exhaustive ne seraient pas efficace sur un système d'information de taille intermédiaire ou significative. Il peut, dans ce cas, être pertinent de souscrire à un service de veille du marché qui centralise et qualifie les avis de sécurité des différents éditeurs. En sélectionnant les produits de son inventaire, cela permet d'être uniquement informé des vulnérabilités pouvant impacter les produits de son entreprise ainsi que les menaces associées à ces vulnérabilités.



« Différentes sources d'information sur Internet permettent d'être informés des vulnérabilités majeures et des vulnérabilités affectant les principaux éditeurs informatiques »

ANALYSE INITIALE D'UNE VULNÉRABILITÉ

Lorsqu'une vulnérabilité est identifiée dans la veille, la première étape est de réaliser une **analyse rapide** afin de savoir si son entreprise peut être concernée, affectée. Cette **analyse macroscopiqu**e s'appuie sur l'**inventaire** des actifs qui composent le système d'information de l'entreprise et l'écosystème qui constitue le périmètre d'activité de l'entreprise. Elle permet de déterminer si son entreprise :

- **N'est pas concernée** par cette vulnérabilité : produit non utilisé ;
- **Est concernée, mais n'est pas affectée** par cette vulnérabilité : utilisation d'une version du produit non vulnérable, fonctionnalité vulnérable non activée…

Dans les deux cas ci-dessus, l'analyse de la vulnérabilité prend fin, sans action complémentaire.
Elle permet également de déterminer si l'entreprise :

- **Est peut-être concernée** par cette vulnérabilité. Il n'y a pas d'information permettant de savoir si le produit est utilisé ou pas dans l'entreprise. Une analyse plus approfondie est alors nécessaire ;
- **Est concernée et est (peut-être) affectée** par cette vulnérabilité. Il s'agit du cas où le produit est utilisé dans son entreprise. Parfois, une analyse approfondie est nécessaire pour déterminer si les configurations ou les versions déployées sont vulnérables.

Dans les deux cas ci-dessus, l'analyse initiale itère et se poursuit jusqu'à parvenir à une conclusion déterministe.

INITIATIVE EXTERNE (NON PLANIFIÉE)

L'identification ou la divulgation de vulnérabilités peut venir d'une initiative externe. Ceci concerne les moyens d'être alerté d'une ou plusieurs vulnérabilités impactant son système d'information, sans que cela ne provienne d'une action initiée par l'entreprise, à l'issue de laquelle il serait attendu d'identifier des vulnérabilités.

CADRAGE INTERNE OU VDP

DÉFINITION

Le cadrage interne consiste à définir une Politique de Divulgation de Vulnérabilités ou Vulnerability Disclosure Policy (VDP) en anglais, ou, pour les éditeurs de logiciels, une Coordinated Disclosure Policy.
Il s'agit d'une organisation mise en place pour permettre le recueil légal de vulnérabilités remontées par des sources externes à l'entreprise, en toute sécurité.
Il s'agit à la fois d'un processus organisationnel (contact nommé) et d'un cadrage opérationnel des moyens techniques de communication sécurisée (canal de communication, moyens de chiffrement), permettant de récupérer toutes les informations liées aux vulnérabilités trouvées, en dehors des cadres légaux des tests d'intrusion et de programmes de primes aux vulnérabilités (Bug Bounty).
La divulgation responsable n'induit pas forcément une récompense financière pour le chercheur, car l'attente d'une compensation lors du signalement d'une vulnérabilité peut être considérée comme une extorsion.

PROCESSUS / DÉMARCHE

La mise en place d'une VDP (obligatoire dans le cas de NIS 2) peut se résumer à définir les personnes qui seront les points de contact et prévenir les équipes pouvant être impliquées dans le processus. Ce processus doit impliquer les acteurs suivants :

- Équipe sécurité (obligatoire) ;
- Equipe informatique ou DSI (recommandé) ;
- Juridique (obligatoire) ;
- Communication (recommandé) en particulier les responsables de réseaux sociaux (community manager) ;
- Métier (recommandé).

La VDP est cadrée par la norme ISO 29147 et en particulier la RFC 9116 décrivant le fichier "security.txt". A minima, il est recommandé de mettre en place sur ses sites web un fichier "security.txt" contenant les informations nécessaires à la divulgation responsable de vulnérabilités :

- Contacts nommés (équipe, personne) et des moyens de contact (mail, téléphone, formulaire web, discord...) ;
- Clef de chiffrement pour des échanges sécurisés ;
- Page web pointant vers la politique de divulgation ;
- Page web pointant vers une page de palmarès (listant les personnes ayant remonté des vulnérabilités) ;
- Explications des attendus concernant la divulgation de la vulnérabilité (exemple, moyen de rejeu, dates des tests, adresses IP des tests…).

Le site suivant permet de générer ce type de fichier, à déposer ensuite dans le répertoire "/.well-known/" de son site : https://securitytxt.org/
Une fois la VDP mise en place, des vulnérabilités pourront arriver par ce canal et devront être confirmées.

EXEMPLES

Les exemples suivants présentent des recommandations concernant une VDP :

- ENISA : https://www.enisa.europa.eu/publications/vulnerability-disclosure
- CISA : https://www.cisa.gov/vulnerability-disclosure-policy-template
- NIST : https://csrc.nist.gov/Projects/vdg/related-guidance
- Standard « security.txt » https://securitytxt.org/

TIERS DE CONFIANCE AVEC OU SANS CADRAGE

DÉFINITION

La divulgation de vulnérabilités par un tiers de confiance faisant office d'intermédiaire, avec ou sans cadrage, permet d'assurer la légalité et la sécurité de la divulgation. En général, ce type de canal est choisi par des individus lorsqu'ils ne trouvent pas de contact au sein de l'entreprise ou préfèrent rester anonyme, tant que leurs actions restent de bonne foi et sans but frauduleux. Le principal canal Français de ce type est l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
La divulgation par un tiers de confiance n'induit pas forcément une récompense financière pour le chercheur, car l'attente d'une compensation lors du signalement d'une vulnérabilité peut être considérée comme une extorsion.

PROCESSUS / DÉMARCHE

Il est recommandé de prévoir un processus à même de traiter ce type de divulgation de vulnérabilités. A minima, un contact ou point d'entrée unique doit être prévu.

Il est également recommandé de sensibiliser l'ensemble des équipes de l'entreprise sur le fait qu'elles pourraient être contactées (si le tiers n'identifie pas le bon contact) concernant un sujet de divulgation de vulnérabilités pour transmettre l'information au bon contact.
Des vulnérabilités pourront arriver par ce canal et devront être confirmées.

EXEMPLES

Les tiers suivants peuvent être amenés à contacter l'entreprise afin de divulguer des vulnérabilités :

- L'Agence nationale de la sécurité des systèmes d'information (ANSSI) https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/
- Les opérateurs télécom https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037196108 ;
- L'initiative Huntr https://huntr.dev/ ;
- Des journalistes spécialisés ;
- De sites d'actualités et de presse à sensation ayant leur propre processus d'alerte.

HORS CADRE

DÉFINITION

La divulgation de vulnérabilités hors cadre correspond à une prise de contact par un individu identifié ou non, par tout canal de communication existant (mail, réseau sociaux, appel téléphonique…) vis-à-vis de contact de l'entreprise n'étant pas forcément lié à la sécurité.

PROCESSUS / DÉMARCHE

Bien que non cadré, il est recommandé de prévoir un processus à même de traiter ce type de divulgation de vulnérabilités. A minima, un contact ou point d'entrée unique doit être prévu.
Il est également recommandé de sensibiliser l'ensemble des équipes de l'entreprise (en particulier les équipes de communication, responsable des réseaux sociaux…) sur le fait qu'elles pourraient être contactées concernant un sujet de divulgation de vulnérabilités pour transmettre l'information au bon contact et en particulier sur la conduite à tenir (ne pas rejeter le contact, répondre poliment et acquitter la demande…).
Des vulnérabilités pourront arriver par ces canaux et devront être confirmées.

EXEMPLES

Il existe de nombreux cas de divulgation de vulnérabilités hors cadre mais les entreprises impactées n'en font généralement pas la publicité.
En 2023, un jeune développeur a publié sur X (ex Twitter) une vulnérabilité critique permettant d'obtenir, très simplement, les informations personnelles des usagers d'un site de rencontre. Le seul contact vers l'entreprise a été de la citer dans le "tweet" : https://twitter.com/MathisHammel/status/1685304981803483136
Les responsables de réseaux sociaux des entreprises (community manager) doivent être sensibilisés à ces problématiques.

INITIATIVE INTERNE (SOUS CONTRÔLE DE L'ENTREPRISE)

L'identification ou la divulgation de vulnérabilités peut venir d'une initiative interne. Ceci concerne tous les moyens existants à l'initiative de l'entreprise, pour lesquels il est normal et attendu d'obtenir des vulnérabilités.

OUTILS LIÉS À LA CHAINE DE DÉVELOPPEMENT (CI/CD)

DÉFINITION

Le développement moderne d'application s'accompagne de nombreux outils permettant d'identifier des vulnérabilités connues (référencées CVE, CNNVD, CWE, OWASP...), des mauvaises pratiques de développement induisant une vulnérabilité ou des mauvaises pratiques de configuration. Cette démarche est réalisée en continu à chaque étape de développement et à chaque nouvelle mise en production, cela permet d'éviter les vulnérabilités en amont et de réduire les impacts pour l'éditeur.

Il existe trois principales catégories d'outils :

- Les outils dit SAST (Static Application Security Testing) permettant une analyse statique du code source afin d'identifier des mauvaises pratiques, des versions de librairies dépréciées ou vulnérables...
- Les outils DAST (Dynamic Application Security Testing) permettant d'interagir avec une application afin d'identifier des problèmes de configuration, de gestions des entrées et sorties...
- Les outils IAST (Interactive Application Security Testing) combinant à la fois les contrôles statiques (SAST) et dynamiques (DAST).

PROCESSUS / DÉMARCHE

La mise en place d'outils de sécurité dans la chaine de développement nécessite d'impliquer les équipes sécurité afin de bénéficier d'une expertise lors de l'étude de la solution, du choix de solution, de son déploiement et surtout, après sa mise en production afin de qualifier les alertes.
Des vulnérabilités pourront arriver par ces canaux et devront être confirmées.

SCANNERS DE VULNÉRABILITÉS AFFECTANT LES INFRASTRUCTURES

Des outils de scan automatisés existent sur le marché pour rechercher des vulnérabilités sur les équipements d'infrastructure (serveurs, réseau, …).

Ces outils peuvent être
- Authentifiés pour permettre un accès au système scanné plus étendu et découvrir des vulnérabilités qui requièrent une authentification préalable.
- Ou non authentifiés pour se comporter comme un attaquant en phase de découverte.

Ils peuvent par ailleurs être positionnés pour traverser les différentes couches et composants de sécurité de manière réaliste ou au plus proche des actifs pour découvrir plus exhaustivement les vulnérabilités présentes (mais potentiellement difficilement exploitable car non exposées largement via les mesures d'infrastructure en place : pare-feu, IPS, WAF, …)

LIMITES DES OUTILS

Ces outils présentent les principaux problèmes suivants :
- Ils remontent de très nombreuses vulnérabilités qu'il faut qualifier afin d'écarter les nombreux faux positifs ;
- Les vulnérabilités doivent être contextualisées et priorisées, en général par un traitement manuel ;
- Les recommandations de correction sont en général laconiques et génériques, ne permettant pas d'agir simplement et nécessitant un travail manuel d'enrichissement.

TEST D'INTRUSION ET ÉVOLUTION

DÉFINITION

Un test d'intrusion (pentest) est une pratique d'évaluation technique de la sécurité d'un environnement informatique. Cela consiste à tester une application, un système d'information, un matériel du point de vue de l'attaquant, afin d'identifier les vulnérabilités et défauts susceptibles d'induire des risques métiers, soit accidentels soit intentionnels.
Les tests d'intrusion peuvent être plus ou moins automatisés, existant en plusieurs variantes :
- Prestations de service assimilables à un audit : test d'intrusion, tests d'intrusion réguliers par abonnement (Pentest-as-a-Service ou PTaaS);
- Prestations de service réalisant des scénarios d'attaques spécifiques et avancées : exercices internes de sécurité offensive (Red Team) ;
- Campagnes de Bug Bounty ;

- Solutions dites de gestion de l'exposition aux menaces (CTEM pour Continuous Threat Exposure Management) assurant une cartographie des actifs et des tests d'intrusion en continu, en permanence.

Les avantages par rapport aux SAST/DAST/IAST sont, en règles générales :

- La finesse et la profondeur de la recherche de vulnérabilités ;
- La préqualification des vulnérabilités ;
- Les recommandations contextualisées et applicables.

PROCESSUS / DÉMARCHE

La démarche va dépendre de la solution adoptée mais en général, les principales phases sont les suivantes :

- Définition du périmètre à évaluer ;
- Contractualisation ;
- Initialisation, accompagnée suivant les cas de différents livrables (convention d'audit, plan d'audit, autorisation d'audit...) et d'une réunion d'initialisation ou de lancement ;
- Evaluation technique ponctuelle (test d'intrusion, PTaaS, Bug Bounty) ou continue ;
- Restitution ponctuelle au cours d'une réunion ou continuellement à partir d'un portail web ;
- Clôture dans le cas d'une prestation de service.

Des vulnérabilités pourront arriver par ces canaux et devront être confirmées.

CENTRE DE SECURITÉ OPERATIONELLE (SOC)

DÉFINITION

Les entreprises matures en cybersécurité disposent d'un Security Operation Center (SOC) correspondant à une organisation mise en place afin de détecter de potentiels incidents de sécurité.

Sans rentrer dans les détails du fonctionnement d'un SOC (dont certains périmètres peuvent être couverts par un CERT / CSIRT, suivant l'organisation mise en place), ces équipes peuvent intervenir sur des détections d'incident de sécurité dont une ou plusieurs phases exploitent une ou plusieurs vulnérabilités du système d'information.

PROCESSUS / DÉMARCHE

Le processus de création d'un SOC ne sera pas détaillé ici mais, bien que faisant parti des équipes de sécurité, il est nécessaire de définir un processus de remontée des vulnérabilités par le SOC en cas d'identification de l'exploitation de celles-ci lors d'une attaque.
Des vulnérabilités pourront arriver par ce canal et devront être confirmées.

VERIFICATION DES INFORMATIONS

Une fois une vulnérabilité identifiée (ou divulguée par un canal externe ou interne), il est nécessaire de déterminer si l'actif lié à la vulnérabilité appartient bien à l'entreprise et si la vulnérabilité est bien confirmée, au regard de la fiabilité de la source.

CONFIRMATION

ÉQUIPE

Une équipe en charge de la confirmation des vulnérabilités doit être explicitement nommée.

Il peut s'agir de :
- L'équipe CERT, généralement en charge de la veille et disposant des connaissances adaptées à cette tâche ;
- L'équipe SOC, généralement en charge de la détection des attaques et incidents ;
- L'équipe du traitement des vulnérabilités (Centre de gestion des vulnérabilités ou VOC pour Vulnerability Operation Center) ;
- Toute autre équipe ou personne disposant des prérequis techniques et d'une bonne connaissance de l'environnement de l'entreprise.

APPARTENANCE DE L'ACTIF

L'équipe en charge de la confirmation doit vérifier si l'actif informationnel impacté par la vulnérabilité appartient bien à l'entreprise.
Il s'agira de vérifier si l'actif est bien présent dans la base de données de gestion des actifs de l'entreprise (CMDB pour Configuration Management Database), faisant parti des obligations pour la gestion des vulnérabilités.
Si l'actif n'est pas présent dans la CMDB, il peut s'agir :
- D'un actif non référencé (Shadow IT) ;
- D'une erreur provenant de la source à l'origine de la vulnérabilité. La confiance accordée à cette source sera liée à sa fiabilité (cf. ci-dessous).

Il conviendra donc de vérifier manuellement la bonne appartenance de l'actif au patrimoine informationnel et/ou de recontacter la source afin d'obtenir plus d'informations.

AUTHENTICITÉ DE LA VULNÉRABILITÉ

Une fois l'appartenance de l'actif confirmée, l'authenticité de la vulnérabilité devra être vérifiée, à savoir : est-elle réellement avérée ?
Cette phase nécessitera d'être capable de comprendre techniquement la vulnérabilité ainsi que le moyen de la tester.
Si le moyen de la tester (code d'exploitation) est fourni, il faudra en prendre connaissance et l'analyser afin d'éviter tout problématique de piégeage (backdoor) et d'effet de bord, comme un déni de service.

Si le moyen de la tester n'est pas fourni, il sera nécessaire d'être capable de prendre une décision sans preuve, les principaux cas pouvant être les suivants :

- Vulnérabilité inconnue (non référencée CVE) :
  - Sans code d'exploitation connu : il s'agit de la situation la plus délicate à traiter. Il peut être intéressant de contacter l'éditeur, l'infogérant, les développeurs... pour obtenir plus d'information. Ce cas s'est produit en 2023 avec un simple tweet d'un expert, un dimanche, annonçant une vulnérabilité critique sur les VPN Fortinet (CVE-2023-27997). L'éditeur a ensuite communiqué sur la vulnérabilité au bout de 3 très longues journées ;
  - Avec code d'exploitation public : il faudra trouver ce code d'exploitation, l'analyser, le stabiliser et le tester, de préférence sur un environnement hors production ;
- Vulnérabilité référencée (CVE) :
  - Sans code d'exploitation connu : il faudra comparer les versions des actifs à celles décrites comme impactées par la source de la vulnérabilité et agir en conséquence.
  - Avec code d'exploitation connu : du fait que la vulnérabilité est référencée, la comparaison des versions pourra suffire. En cas de doute, il pourra être intéressant de tester le code d'exploitation, avec les précautions requises.

FIABILITÉ DE LA SOURCE

La fiabilité de la source n'est pas en soit un critère de confirmation mais plutôt un élément de pondération quant à la confiance à accorder à une source.

Une vulnérabilité provenant d'un outil totalement automatisé (et réputé pour ses faux positifs) comme un SAST, demandera une confirmation plus approfondie et plus de méfiance qu'un test d'intrusion. De la même façon, une alerte provenant de la VDP demandera plus d'approfondissement et de méfiance qu'une remontée par l'équipe SOC.

Il appartiendra à l'entreprise de définir sa propre grille de confiance mais voici un premier classement permettant d'aider :

		Fiabilité concernant...	
		Appartenance	**Authenticité**
INITIATIVE EXTERNE	Cadrage interne ou VDP	Faible	Faible
	Hors cadre	Faible	Faible
	Tiers de confiance avec ou sans cadrage	Faible	Modérée
INITIATIVE INTERNE	Outils liés à la chaine de développement (CI/CD)	Forte	Faible
	Test d'intrusion	Forte	Modérée
	Test d'intrusion automatisé avec rejeu automatisé	Forte	Forte
	Equipe de détection des menaces (SOC)	Forte	Forte

La criticité de l'actif, la facilité d'exploitation de la vulnérabilité et son exposition permettent ainsi de qualifier la vulnérabilité. En l'absence d'actif impacté, de confirmation de l'authenticité de la vulnérabilité ou de moindre fiabilité de la source, le processus peut prendre fin.

Dans le cas contraire, la démarche se poursuit par l'identification des actifs et des systèmes concernés à l'échelle de l'entreprise.

IDENTIFICATION DES ACTIFS ET DES SYSTÈMES CONCERNÉS

L'inventaire et la découverte des actifs vulnérables est indispensable afin de mieux se protéger.

Il est nécessaire d'énumérer les composants de son environnement avec un maximum d'informations, voici une liste non exhaustive :

- Nom du produit
- Fabricant
- Version du produit
- Dépendances, s'il en existe
- Date d'implémentation
- Responsable du produit
- Criticité
- Nombre de composant dans le parc
- Localisation physique
- Liens avec tierces partie (mainteneurs, infogérant, développeurs…)
- Les autres systèmes ou applications qui dépendant de ce composant (afin d'évaluer la criticité de cet actif)

Il est aussi important de mettre à jour régulièrement ces informations et de suivre les évolutions des :

- Versions
- Dépendances
- Niveaux contractuels de support
- Calendrier de fin de support (complet, limité, limité payant, fin de support)
- Date de décommissionnement (si celui-ci n'est plus dans le parc)
- Responsable
- Nombre de composants

Tous ces éléments apporteront une plus-value et permettront de mieux appréhender les futures vulnérabilités et de passer le moins de temps possible à se demander si l'entreprise est vulnérable ou non.

Cette base de données, si elle est bien à jour, permettra de répondre plus facilement à différentes questions tel que :

- Sommes-nous concernés par cette vulnérabilité ?
- Avons-nous le produit dans notre environnement ?
- Quel est l'exposition de cette vulnérabilité dans notre parc ?
- Quel serait l'impact d'une exploitation réussie de la vulnérabilité ?

Tout ceci permettra une analyse préliminaire plus facile et rapide.

Il existe de nombreux des outils permettant de réaliser des scans, afin de maintenir cette base de données.

Avec tous les éléments précédemment listés, il est plus simple d'identifier si l'entreprise est concernée par la vulnérabilité, mais il est important dans un premier temps de comprendre la vulnérabilité et de l'analyser.
Si l'entreprise n'est pas concernée par la vulnérabilité, il n'est pas nécessaire de passer en mode crise.

GESTION DE L'OBSOLESCENCE

L'explosion des vulnérabilités (ordre du jour actuel : plusieurs vulnérabilités critiques CVE publiées chaque jour) et les dépendances open source largement utilisées dans les logiciels ont fait prendre conscience du besoin d'une dynamique de mise à jour des infrastructures.

De la même manière, la fin de vie des produits (End Of Life) motive le pilotage de l'obsolescence.

Toutefois, les fréquences d'application de correctifs et le délai de déploiement de nouveaux systèmes se réduisent, il est donc recommandé d'adopter une posture basée sur des principes tels que :

- Un socle obsolète comme motif de refus ou d'avis défavorable dans les projets ;
- Considérer comme inacceptable l'argument affirmant que l'actif utilisant une technologie obsolète n'est pas exposé directement (rebond possible) ;
- Facturer les métiers pour les coûts d'exploitation liés à l'obsolescence (virtual patching, zone réseau isolée dite "cul de sac"...) ;
- Faire accepter la notion de 'bouton rouge' : en cas de risque important, le métier est conscient que l'application peut être arrêtée ou mise en maintenance.

Avoir une stratégie de gestion de l'obsolescence permet de mieux connaitre son système d'information et ainsi d'être plus efficient pour gérer une vulnérabilité éventuelle.

ANALYSE APPROFONDIE

Cette étape consiste à impliquer, si nécessaire, davantage d'acteurs en dehors des équipes informatiques internes (hébergeur, collaborateurs métier, tiers externes) et venir enrichir les travaux d'identification des actifs et des systèmes concernés. Cette étape itère avec la précédente et permet de préciser la criticité et l'exposition à la vulnérabilité via les éléments d'expertise collectés.

EVALUATION DU NIVEAU DE LA MENACE

Plusieurs éléments peuvent être appréciés pour qualifier une nouvelle vulnérabilité et prendre les mesures appropriées

- Des informations concernant la vulnérabilité elle-même :
  - Le score de base CVSS ;
  - Le type de vulnérabilité : Remote Code Execution, Local Code Exécution, Denial Of Service...
  - La nécessité d'une authentification préalable ou non ;
  - L'existence ou non d'un code d'exploitation ainsi que la connaissance de son exploitation publiquement ;
  - La disponibilité d'un correctif ou d'un contournement.
- Des informations concernant le ou les actifs impactés :
  - L'exposition : Internet, partenaires, clients, interne uniquement, derrière un équipement filtrant le service vulnérable...
  - L'impact de l'exploitation réussie de la vulnérabilité ;
  - La criticité et le besoin en disponibilité des données liées ;
  - L'ampleur de l'usage opérationnel, métier et technique, du composant touché (dans l'absolu, et plus particulièrement dans le cadre du Système d'Information considéré).

L'organisation doit prioriser la typologie des vulnérabilités selon ses priorités métier. Par exemple :

- Exécution de code à distance (RCE) sans authentification.
- Injection de commande à distance (RCI) permettant une prise de contrôle partielle ou totale.
- Accès en lecture et écriture aux fichiers du système vulnérable.
- Accès en lecture aux fichiers du système vulnérable
- Escalade de privilèges en local
- Déni de service (DOS)

Cela est en adéquation avec le contexte des alertes généralement émises par le CERT-FR ou d'autres instances telles que le CERT-US par exemple, concernant très souvent:

- Des produits populaires : Microsoft, équipements de sécurité, VMWare, Confluence, Acrobat, des librairies connues et largement utilisées
- Des exécutions de code à distance et contournements de l'authentification

Cette analyse préliminaire mobilise des compétences techniques ainsi qu'une bonne culture du domaine, que l'on retrouve dans les équipes : SOC, CERT, administration opérationnelle, experts et analystes en sécurité ou risques.

Le résultat du travail d'analyse préliminaire est une analyse des risques, contextualisée à la vulnérabilité étudiée et dans le contexte précis du système d'information ou de la solution considérés avec les critères présentés ci-dessus, complétés de l'effort nécessaire à la mitigation.

Un complément utile peut être la production d'un score CVSS net (comme par exemple en faisant varier l'Environnemental Score CVSS), système par système, pour traduire ce travail d'analyse dans un mode d'évaluation de vulnérabilité standard. Par ailleurs, il peut être intéressant de prendre en compte le score EPSS.

EVALUATION DES IMPACTS MÉTIERS

L'évaluation des impacts métier, parfois appelé «Business Impact Analysis» (BIA), permet d'évaluer comment l'atteinte à la confidentialité, à l'intégrité, à la disponibilité et à la traçabilité vont bloquer ou réduire l'activité de l'entreprise en regardant comment tous les produits et service peuvent être affectés. La norme ISO 22301 donne des grandes lignes pour réussir son évaluation d'impact.

Les résultats de cette analyse doivent comprendre :

- La définition du périmètre concerné par les activités opérationnelles ;
- La cartographie des dépendances entre les produits/services, les processus, les activités et les ressources ;
- L'ordre de priorité de reprise d'activité des produits/services/processus à la suite d'un incident : que redémarrer/reprendre en premier car plus important pour le business ?
- La détermination des ressources nécessaire pour les activités/produits/services prioritaires : bureaux, personnes, équipements, données, moyens de communication, actifs technologiques, tiers, budget…
- L'identification des exigences légales, réglementaires et contractuelles ainsi que leurs effets sur la reprise d'activité. Par exemple, une application peut ne pas être critiques pour le métier mais doit être parmi la liste des applications prioritaires à redémarrer du fait de contraintes légales ou techniques (comme le DNS) ;
- La cartographie des dépendances vis-à-vis des autres activités, des fournisseurs...
- L'évaluation des impacts dans le temps vis-à-vis d'un incident.

Les impacts doivent être mesurés notamment en ces termes, à l'appréciation de chaque entreprise :

- Financiers : quel montant l'entreprise peut perdre (et/ou ne pas gagner) à cause de l'incident, stabilité des marchés, fraude et gains financiers…
- Réputationnels : estimation de la dégradation de l'image de marque suite à l'incident
- Juridiques/réglementaires : évaluation des sanctions et litiges pouvant résulter de l'incident
- Opérationnels : Impacts sur les ventes, les opérations, la productivité, les projets, désavantage concurrentiel
- Sûreté : Risque social, sanitaire ou de décès, industriel (pollution, incendie…)

Une fois ces impacts évalués, la reprise d'activité doit être programmée par ordre de priorité.

COMMUNICATION

La communication doit être adaptée à la situation et sa portée doit être réduite au maximum possible, considérant que le traitement et la remédiation du problème restent en cours à ce stade (il n'est donc pas opportun de diffuser largement une recette permettant de porter atteinte aux intérêts de l'entreprise).

Trois types de communications peuvent être à prévoir selon la nécessité et les obligations légales :

1. **Communications internes** : échanges d'informations au sein de l'entreprise entre ses collaborateurs et départements
   a. Communication interne restreinte émise vers les équipes techniques et cybersécurité concernées, ainsi que le management de la sécurité
   b. Communication interne destinée à la Direction des Systèmes d'Information / Direction Générale de l'Entreprise
2. **Communications externes** : échanges d'informations entre l'entreprise et des parties extérieures, telles que les clients, partenaires, médias, etc. Exemples : partenaires commerciaux, fournisseurs tiers, assureurs et conseillers juridiques, clients, utilisateurs finaux, etc.
3. **Communications avec les régulateurs** : échanges d'informations entre l'entreprise et les organismes de régulation gouvernementaux. Exemples : ANSSI, ENISA, CNIL...

Ci-dessous un exemple type concernant la communication dans le cas où il est nécessaire de réaliser une **communication externe** pour une vulnérabilité confirmée :

1. **Identification des clients impactés** qui utilisent la solution concernée et qui pourraient être affectés par la vulnérabilité ;
2. **Préparation des messages clés clairs et précis** pour informer les clients de la vulnérabilité, de son impact potentiel sur leur systèmes et données, et des mesures de remédiation en cours ;
3. **Envoi des notifications de cybersécurité à chaque client concerné**, en donnant le niveau d'information pertinent par rapport à la vulnérabilité et les mesures de remédiations prises ou recommandées ;
4. **Mise en place d'une équipe de support client** si nécessaire pour répondre aux questions et préoccupations des clients concernant la vulnérabilité et les mesures de remédiation ;
5. **Suivi de toutes les communications** avec les clients et documentation des interactions pour une meilleure traçabilité.

COMMUNICATION INTERNE RESTREINTE

Cette communication est généralement émise par le SOC ou le CERT.
Elle est destinée aux interlocuteurs informatique et sécurité qui ont le besoin d'en connaitre, car ils ont un rôle dans le traitement de la vulnérabilité, la mise en œuvre des mécanismes de mitigation, le déploiement de la

mise à jour, la détection des tentatives d'exploitation ou des systèmes compromis, la veille (évolution de l'analyse de la vulnérabilité, disponibilité de kits / code d'exploitation, les compromissions connues, …) ou l'appréciation des risques induits par exemple.
Elle a une portée technique, diffuse les détails de la problématique, de l'analyse et du plan d'action suivi.
Elle peut prendre la forme d'une « fiche vulnérabilité » diffusée par mail et comportant par exemple :

- Références (CVE…)
- Description de la vulnérabilité (impact, systèmes affectés, liens vers l'avis sécurité de l'éditeur)
- Score CVSS
- Solutions possibles (patch, mitigations…)
- Etat de la menace (exploit publique, attaques en cours…)
- Evaluation du risque pour l'entreprise
- Recommandations / plan d'actions à suivre / échéances (deadlines)

Sur des vulnérabilités complexes et/ou amenant des travaux de correction conséquents (ex : log4shell), il peut être pertinent de publier un **journal interne de la vulnérabilité**, permettant de centraliser les dernières informations revues et validées et d'aligner tous les acteurs de la remédiation sur le même niveau d'information, l'analyse et le plan d'action à suivre. Cela évite que chaque acteur fasse ses propres recherches, ses analyses sur la base d'informations trouvées sur Internet à la pertinence potentiellement variable qui conduiraient à une appréciation divergente de la conduite à tenir.

Cette démarche évite à l'équipe en charge de la qualification d'une vulnérabilité d'expliquer à nouveau les actions de remédiation à chaque équipe en charge de la correction. Cette démarche est similaire à celle du CERT-FR, qui met régulièrement à jour ses bulletins et alertes en mettant en évidences les modifications apportées.

COMMUNICATION INTERNE DESTINÉE À LA DIRECTION

Cette communication est généralement émise par un interlocuteur sécurité (RSSI/CISO, SOC …) ou l'équipe en charge du pilotage des incidents. Elle vise à :

- Informer la DSI, voire la direction générale ou le conseil d'administration, de la problématique et des risques induits,
- Confirmer que le sujet est identifié et sous contrôle,
- Eviter que les sollicitations arrivent dans l'autre sens suite à la médiatisation de la vulnérabilité sur Internet, dans la presse spécialisée ou généraliste, dans des cercles et communauté d'échange dont les dirigeants font partie…

Il s'agit généralement d'une communication unique, envoyée tôt dans la chronologie de traitement, mais qui présente plusieurs complexités, avec la nécessité de :

- Vulgariser la problématique et la manière d'y répondre ;
- Être rédigée tôt (avant ou au tout début de sa popularisation, s'il est estimé que cette vulnérabilité va être médiatisée) ;
- Être rédigée lorsque suffisamment d'éléments sont disponibles : analyse préliminaire, compréhension suffisante de la problématique, de ses enjeux et de la manière dont l'entreprise pourra y répondre.

Dans de rares cas, cette communication peut être actualisée en cours de traitement, si la situation l'exige.

Le groupe de travail préconise de réfléchir et documenter, en amont d'une problématique réelle, le modèle et le processus de communication qui seront utilisés : critères de déclenchement, mise en forme graphique, rubriques abordées, circuit de validation avant diffusion, mode de diffusion, destinataires.

Cette anticipation permet un traitement efficace, rapide et avec une improvisation limitée au maximum le jour de l'évènement.

Si la vulnérabilité est médiatisée, une communication interne élargie **à l'ensemble des collaborateurs** peut être envisagée, afin de rassurer et limiter l'inquiétude, les rumeurs…

COMMUNICATIONS EXTERNES ET EN DIRECTION DES RÉGULATEURS

Le groupe de travail constate qu'il n'est généralement pas de la responsabilité ou qu'il n'est pas autorisé, pour les équipes techniques ou sécurité, de communiquer en externe sur une problématique rencontrée dans l'entreprise.

Dans le contexte d'une vulnérabilité fortement médiatisée des sollicitations peuvent provenir :

- Des clients, afin de se rassurer concernant leurs données et connaitre le degré d'exposition à cette vulnérabilité (qui peut être nulle) ;
- De partenaires, afin de savoir s'ils sont en risque (dysfonctionnement de l'activité, propagation par l'exploitation de la vulnérabilité…) ;
- De confrères (en avance ou en retard dans la compréhension de la vulnérabilité et menaces associées) ;
- D'assureurs ;
- De régulateurs (national, européen, spécifique à certains pays où opère l'entreprise …).

Une communication est indispensable pour rassurer ces différents acteurs sur la bonne prise en compte de la problématique, confirmer que la situation est sous contrôle et ne requiert pas pour ces derniers de mettre des mesures conservatoires ou d'audit en place.

Le groupe de travail observe que, de plus en plus souvent, les sollicitations sont maintenant accompagnées d'un questionnaire dont la forme et les questions posées sont à chaque fois propres à l'établissement émetteur. Cela induit une complexité dans le traitement et présuppose une réponse à chaque fois personnalisée.

Le groupe de travail préconise que l'entreprise prenne la main sur sa communication et diffuse un communiqué type, prévu et préparé à l'avance, en cas de sollicitation, sans dépenser de temps et d'énergie à apporter une réponse personnalisée, sauf si l'enjeu le requiert (client essentiel, régulateur, assureur …).

La communication externe est généralement la mission des équipes de communication (externe, réseaux sociaux, institutionnelle …) et/ou de la direction des risques pour les échanges avec les régulateurs ou autorités de tutelle. Ces équipes ne sont pas des spécialistes informatiques et doivent être alimentées par les équipes techniques et sécurité par des éléments de langage, ayant déjà fait l'objet d'un travail de vulgarisation, qui pourront être utilisés pour bâtir le communiqué.

Dans le même esprit que pour la communication interne, le groupe de travail préconise de réfléchir et documenter, en amont d'une problématique réelle, le modèle et le processus de communication qui seront utilisés :

- critères de déclenchement
- parties prenantes et rôles de chacun
- mise en forme graphique, rubriques abordée
- circuit de validation avant utilisation,
- mode de diffusion (sur sollicitation uniquement ou proactif vers certains destinataires)
- …

afin de permettre un traitement efficace, rapide et avec une improvisation limitée le jour J.

Exemple de communication aux partenaires B2B pour transmettre des informations quant à la prise en charge au sein de votre organisation

<OBJET : [SECURITE DE LA SOCIETE] - Informations sur l'alerte de sécurité Log4Shell – Log4j>

Bonjour [A personnaliser],

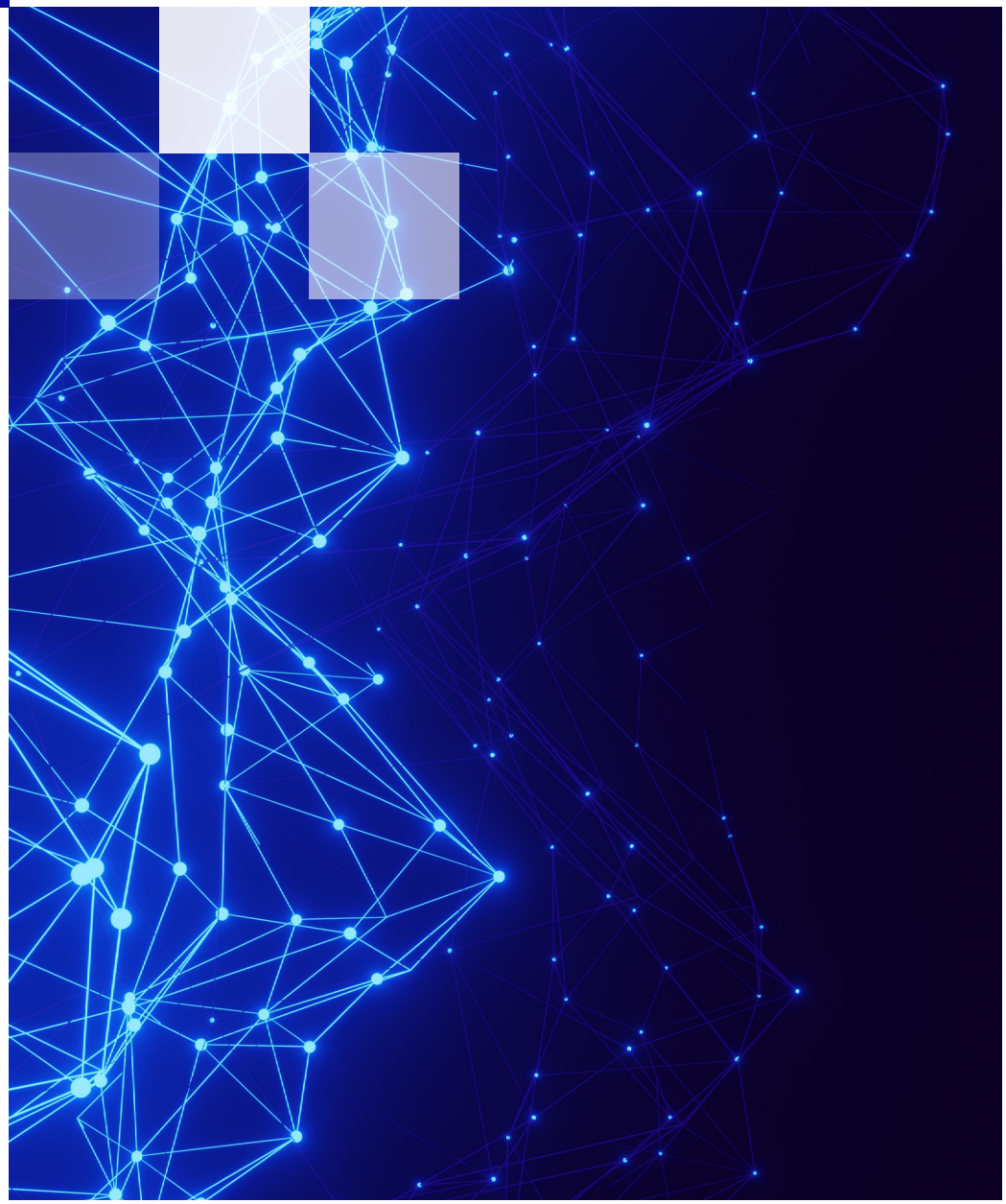
Le vendredi 10 décembre dernier, nous avons été informés d'une alerte de sécurité critique sur le logiciel Apache Log4j. Nos équipes ont immédiatement été mobilisées durant le week-end et les jours suivants pour identifier les serveurs potentiellement impactés et mettre en place au plus vite les contre-mesures préconisées par notre CERT et l'ANSSI.

Depuis cette alerte, aucun incident lié à cette vulnérabilité n'a été constaté.

Voici notamment le périmètre concerné par cette analyse dans le cadre de notre relation :
[Services à personnaliser selon le partenaire B2B]
- Application A
- Extranet B
- Site Web C
- Produit D

L'ensemble de ces services restent sous surveillance.

Nous restons à votre disposition pour tout complément d'information,
[Signature à personnaliser]



« Publier un journal interne de la vulnérabilité, permettant de centraliser les dernières informations revues et validées et d'aligner tous les acteurs de la remédiation sur le même niveau d'information, l'analyse et le plan d'action à suivre. »

GESTION DE CRISE

Le groupe de travail recommande de se référer au guide gestion de crise publié par l'ANSSI : https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/

PRÉALERTE

La pré-alerte repose sur la capacité à identifier les signaux précurseurs d'une crise, à évaluer les risques et à anticiper une évolution défavorable pour l'entreprise. Elle joue un rôle critique dans la mise en place réussie d'une cellule de crise.
C'est un processus itératif et continu qui exige une attention constante aux signaux faibles et une évaluation minutieuse des risques.
Les paragraphes suivants décrivent un processus détaillé adapté aux moyennes et grandes entreprises. Les différentes phases peuvent être allégées et les réunions ou points d'étapes moins fréquents.
Cette étape permet de réagir de manière proactive plutôt que réactive, notamment grâce à :

- La surveillance continue, qu'elle soit technique (CERT, SOC…), sociétale (médias, réseaux sociaux, des données financières) ainsi que des tendances sectorielles ;
- La réévaluation continue des risques ;
- L'identification des parties prenantes, internes et externes, qui pourraient être affectées par la crise : employés, clients, investisseurs, autorités réglementaires…
- La diffusion d'une première alerte vers ces parties prenantes, destinées à les informer de l'évènement en cours et s'assurer de leur potentielle disponibilité en cas d'activation du dispositif de crise dans les minutes / heures qui suivent ;
- L'activation rapide dès que les signaux d'alerte sont confirmés et que les risques sont évalués, l'organisation est prête à activer rapidement la cellule de crise avec notamment des rôles et des responsabilités clairement définis, ainsi qu'une infrastructure de communication efficace.

MOBILISATION

La mise en place d'une cellule de crise est une étape essentielle pour faire face aux situations critiques avec rapidité, coordination et efficacité. La mobilisation de cette équipe restreinte mais hautement compétente repose sur plusieurs grands principes fondamentaux qui guident la réponse de l'organisation face à la crise imminente.

PARTIES PRENANTES

Lors de la mobilisation, il est impératif de désigner un responsable de la crise (crisis leader/manager) clairement identifié. Cette personne doit être dotée de l'autorité nécessaire pour prendre des décisions rapidement, se faire comprendre par les membres du COMEX, et coordonner les actions de manière efficiente dans des situations de stress.

Les bonnes personnes doivent être mobilisées lors de la crise. Plus leur nombre est élevé, plus il peut être difficile de prendre des décisions. Il est donc nécessaire de mobiliser les bonnes personnes au bon moment, avec les compétences adéquates.
Les cellules de crise sont généralement composées :

- Du COMEX de l'entreprise ;
- Du responsable de la crise ;
- Du responsable des risques ;
- D'expert(s) technique(s) ;
- De la direction de la communication ;
- De représentants des RH et/ou du juridique (au besoin) ;
- Des responsables de plans de continuité d'activité.

SALLE DE CRISE

Une salle de gestion de crise doit être réquisitionnée à cet effet tout au long de la durée de l'événement, par exemple, toutes les heures. Elle servira aux réunions de différentes parties prenantes. La réquisition ne pourra prendre fin que lorsque la crise sera terminée.
Cette salle doit être dans les locaux de l'entreprise, loin des regards indiscrets et sécurisée afin que personne ne puisse y entrer quand une réunion de crise ne s'y tient pas.
Elle doit être équipée d'un accès à Internet, d'un système de conférence call, de lignes téléphoniques (au besoin, non IP), d'un tableau blanc, feutres, projecteur/système de partage vidéo et écran.

CELLULE DE CRISE OPÉRATIONNELLE

Une cellule de crise opérationnelle répond à un objectif prédéfini : prise de décision, actions techniques, …
Chaque membre de la cellule de crise doit avoir des rôles et des responsabilités clairement définis, idéalement à un niveau hiérarchique identique. Cela évite les chevauchements et les lacunes dans les actions entreprises. Chacun doit avoir compris son rôle spécifique et savoir comment il contribue à l'ensemble des efforts de gestion de crise avant l'évènement.

Il est possible de créer un sous ensemble de la cellule de crise opérationnelle, pour un temps et avec un objectif donné, afin de permettre à quelques personnes clé (experts techniques, conformité, juridique…) de se focaliser sur une mission, sans perturber le déroulement de la cellule de crise opérationnelle par ailleurs, et la réintégrer une fois le livrable produit.

OBJECTIFS

Le travail de la cellule de crise doit être guidée par des objectifs clairs et définis lors de sa première réunion. Ces objectifs doivent être alignés sur la mission et les valeurs de l'organisation, tout en visant à atténuer les effets de la crise sur les parties prenantes.

Ces objectifs seront rappelés tout au long de la crise mais les situations de crise sont rarement linéaires, et la capacité à s'adapter rapidement aux changements et une réévaluation constante sont nécessaires.

Les entreprises ayant un plan de continuité d'activité ont déjà défini un plan d'action leur facilitant le suivi des différentes étapes de la crise (protocoles d'évacuation, des procédures de communication, listes de contacts importants, etc.)

CHAINE DE COMMANDEMENT

Lors de la première réunion, il est aussi important de définir une hiérarchie claire au sein de la cellule de crise, et notamment de décider qui a le droit de voter les décisions. La chaîne de commandement doit être comprise par tous les membres.

COMMUNICATION AU SEIN DE LA CELLULE DE CRISE

Le système de communication doit être efficace et résilient.
En plus des réunions régulières, par exemple, toutes les heures, les membres doivent utiliser des canaux de communication rapides et sécurisés pour partager les informations et les mises à jour et les décisions.
Il est primordial de tenir une main courante détaillée de toutes les actions entreprises, des décisions prises et des communications effectuées.
Durant chaque réunion de la cellule de crise, chaque participant fournira une mise à jour des informations concernant son périmètre.
A la fin de chaque réunion de la cellule de crise, il est primordial de :

- Récapituler la liste des actions à prendre, leurs responsables et leurs échéances fixées ;
- Informer l'ensemble des participants de l'heure de la prochaine réunion ;
- Mettre à jour et de distribuer le rapport de situation à qui a le droit d'en connaître.

RÉÉVALUATION

Il est essentiel de réaliser des évaluations régulières pour analyser la pertinence des actions entreprises, identifier les améliorations nécessaires. Cette boucle de rétroaction contribue à renforcer la résilience de l'organisation face aux crises futures.

CRITÈRES DE SORTIE DE CRISE

Il est souvent plus simple de déclencher une cellule de crise que d'en décider sa fermeture.
Par défaut, l'atteinte du seuil d'acceptation du risque est le critère de sortie de crise. Toutefois, les critères restent à discrétion de l'entreprise : Il peut être intéressant de définir dès le démarrage de la crise les éléments qui décideront du point de sortie. Décider de la sortie de crise avec un accompagnement progressif permet de ne pas essouffler les acteurs et de maintenir le niveau d'implication.
La solution peut être de basculer, une fois le seuil atteint, en cellule opérationnelle uniquement, ou en instance classique de suivi des vulnérabilités quand elle existe.

REMÉDIATION INITIALE

A cette étape débute la phase de remédiation de l'incident. Cette dernière implique plusieurs processus qui doivent se dérouler en parallèle.

EQUIPE DÉFENSIVE (BLUE TEAM)

VEILLE

Une veille est réalisée par le CERT, SOC, VOC ou équipe d'infrastructure / applicative concernée selon l'organisation, en lien avec le constructeur ou éditeur du produit vulnérable.
Elle consiste à une actualisation continue de la connaissance de la vulnérabilité :

- Produits et versions impactées : après une évaluation initiale de l'éditeur / constructeur, cette liste peut évoluer à la lumière d'une analyse plus détaillée, excluant certains produits où un doute existait, ou incluant de nouveaux produits non pris en compte initialement
- Conditions d'exploitation : la charge utile du code d'exploitation d'attaque ou le mode opératoire pour exploiter l'attaque peut évoluer et faire émerger de nouvelles méthodes
- Publication d'un Proof Of Concept : il s'agit d'un code démontrant une possibilité d'attaque via exploitation de la vulnérabilité décrite. Ce POC peut être intégré ou non dans un Framework offensif type metasploit
- Existence de cas d'exploitation avérés : il s'agit de victimes qui se signalent, de cas de cyberattaques réussies revendiquées par des attaquants, d'informations diffusées par un CERT national ou sectoriel, …
- Publication d'un contournement (workarround) : il s'agit généralement d'un paramétrage ou d'une mesure d'infrastructure (bloquer un port réseau, bloquer un mode opératoire spécifique, …), empêchant ou limitant l'exploitation de la vulnérabilité
- Publication d'un patch : il s'agit du développement et de la mise à disposition d'une version logicielle non vulnérable par l'éditeur. Un patch doit systématiquement être vérifié pour confirmer l'absence d'impact sur la production et la bonne correction effective du problème de sécurité décrit.

Les faits marquants doivent être communiqués par l'équipe de veille vers la cellule de crise opérationnelle ou le pilote de l'incident. L'évolution des conditions peut également mener une réévaluation du niveau de risque, et la prise de décision de remédiation plus immédiates ou plus radicales.

DÉTECTION ET/OU BLOCAGE

Parallèlement aux actions de veille, le SOC doit rechercher des caractéristiques techniques remarquable des attaques, en lien avec la Red Team, afin :

- De mettre en place une règle de détection / alerte des tentatives d'attaque, et caractériser ainsi l'origine des flux malveillants ou l'intensité des tentatives
- De mettre en place une règle de blocage afin de prévenir une exploitation réussie de l'attaque, le temps que l'éditeur / constructeur publient un contournement ou un correctif.

Ces détections / blocages s'appuient sur des composants d'infrastructure préexistants : SIEM, pare-feu, IPS, EDR, NDR, WAF, proxy, …
Les principales métriques doivent être communiquées vers la cellule de crise opérationnelle ou le pilote de l'incident. L'évolution des conditions peut également mener une réévaluation du niveau de risque, et la prise de décision de remédiation plus immédiates ou plus radicales.

ANALYSE À POSTERIORI (RETROHUNT)

Une fois que les caractéristiques techniques remarquables d'une attaque sont connues, il est recommandé de procéder à une recherche de ses marqueurs dans le système d'information (retrohunt) afin de vérifier si des tentatives d'attaque antérieures à la connaissance de la vulnérabilité n'ont pas été menées. Cette tâche incombe en général au SOC (parfois au CERT ou à la DSI, selon l'organisation).

Cela requiert de disposer de journaux d'évènements (logs) ou d'historisation de flux (NetFlow), produits par des composants d'infrastructure préexistants, sur lesquels investiguer, et une profondeur de rétention suffisante pour revenir assez loin dans le passé.
La détection d'une ou plusieurs attaques réussies doit être communiquée vers la cellule de crise opérationnelle ou le pilote de l'incident. Cela change la géométrie de l'incident en cours, passant d'actions de prévention à l'instruction d'un incident de sécurité avéré.

EQUIPE OFFENSIVE (RED TEAM)

Si l'organisation dispose d'une Red Team ou d'une équipe de sécurité offensive, cette dernière peut être impliquée pour :

- Vérifier la pertinence des codes d'exploitation (PoC) publiés et confirmer qu'ils permettent réellement de réussir l'attaque redoutée. Cette étape requiert des précautions opérationnelles, notamment pour s'assurer que le code source du PoC ne comporte pas de porte dérobée (backdoor), ne permettra pas la diffusion d'informations sensibles ou n'amènera pas une compromission du Système d'Information ;

- Déterminer les caractéristiques techniques remarquables de l'attaque : charge utile (payload), signature, utilisation d'un port atypique, cinématique réseau ou système, … et communiquer ces éléments pour une potentielle détection / blocage des tentatives d'attaque par le SOC ou les équipes techniques. Une fois la détection / blocage en place, le SOC peut confirmer le bon fonctionnement avec une nouvelle tentative d'exploitation menée par la Red Team ;

- Vérifier l'efficacité d'une contre mesure (contournement, correctif) : confirmer qu'une attaque précédemment réussie ne fonctionne plus après la mise en œuvre.

Un exercice de Red Team, par une équipe interne ou externe, simulant une attaque réelle peut être organisé pour vérifier si les mesures correctives ont bien été appliquées. En général, ces exercices se déroulent comme suit :

- Phase de planification : définition de la cible et des objectifs, y compris les vulnérabilités spécifiques à tester et les scénarios d'attaque à simuler ;
- La Collecte d'Informations : L'équipe de Red Team rassemble des informations, souvent fournies par la cellule de crise ;
- L'attaque : La Red Team simule l'attaque en utilisant diverses techniques d'exploitation de la vulnérabilité comme le ferait un attaquant réel ;
- L'évaluation des résultats : Si la Red Team parvient à exploiter avec succès la vulnérabilité, cela indique que la correction n'a pas été suffisamment efficace, il faudra donc continuer à itérer en cellule de crise. Si l'attaque échoue, cela indique que la vulnérabilité a été correctement corrigée.

EQUIPES TECHNIQUES

Les équipes techniques (infrastructures, applications) sont impliquées pour implémenter les contre-mesures proposées par le SOC ou le CERT (ex : règle de pare-feu, règle WAF, etc.) et tester le bon fonctionnement des contournements ou correctifs proposés par l'éditeur, tant l'absence d'impact sur la production que la bonne capacité à déployer le correctif sur l'infrastructure (packaging, stratégie de déploiement, etc.).

Idéalement, les tests doivent se dérouler sur un environnement de qualification représentatif de la production, à défaut sur un éléments de production unitaire ou exclu du traitement des flux de production réels le temps du test..

CONCLUSION

Au regard des analyses et éléments d'appréciation du risque communiqués par tout ou partie de ces trois équipes (red team, blue team, équipes techniques, suivant la taille et l'organisation de l'entreprise), le pilote de l'incident ou la cellule de crise opérationnelle réévalue le niveau de risque et établissent un premier plan de remédiation, qui sera potentiellement réactualisé en continu, au fur et à mesure que les données communiquées par les 3 équipes évoluent.

Dans de nombreux cas opérationnels, il n'est pas possible d'attendre d'avoir une connaissance complète de la vulnérabilité et une certitude sur la pertinence du plan de remédiation pour agir. Les opérations sont fréquemment itératives, et certaines contremesures initiales peuvent être désactivées après application d'autres mesures ou d'un correctif. Le plan de remédiation doit donc rester évolutif. L'objectif est d'évaluer le risque pris sur la production et la continuité d'activité par rapport au risque sécuritaire, et de conserver un niveau de risque maitrisé et acceptable avec les actions décidées.

REMÉDIATION DÉTAILLÉE

L'analyse préliminaire de la vulnérabilité a permis d'engager rapidement des actions de communication, interne ou externe, ainsi que de se donner les moyens de poursuivre le traitement de la vulnérabilité si besoin.

La suite du traitement de la vulnérabilité mobilise un plus grand nombre d'acteurs et d'expertises afin d'être en mesure d'identifier les systèmes et applications vulnérables, d'être en mesure de mitiger les impacts potentiels, d'appliquer les correctifs, de réaliser la veille et la réponse à incident. Ainsi les équipes sécurité, productions applicatives, équipes d'infrastructure, Dev leader, CERT/CSIRT, SOC, Red Team, responsables d'applications, continuité d'activité, et plus encore si besoin - en fonction des organisations - sont mobilisées.

L'inventaire et la découverte des actifs vulnérables seront basés sur la cartographie de l'organisation quand elle existe et est à jour et peuvent être associés à des scans de vulnérabilités. Les scanners proposent l'identification des vulnérabilités publiées afin de faciliter la recherche.

L'analyse approfondie et la qualification de la menace, à l'aide de rétro-ingénierie permettront de comprendre et bloquer la menace, de tester les solutions de contournement et les exploits.

Renforcer la veille sur la vulnérabilité, par des services de veilles externes et des échanges au sein de la communauté, par la veille en cybersécurité interne (SOC, CERT/CSIRT).

Cela permettra de récupérer des informations quant à son exploitation (fréquence, ciblage, acteurs), mais aussi potentiellement des indicateurs de compromission (IOC) qui viendront enrichir les outils et règles de détection.

Le traitement d'une vulnérabilité critique se rapproche du traitement d'un incident, y compris sans impact avéré. En effet les ressources mobilisées, les actions réalisées pour mesurer le risque et les impacts potentiels, les outils de communication engagés justifient de formaliser et tracer les évènements de la même façon que pour un incident de sécurité. Le suivi dans la durée en sera d'autant facilité.

PLAN INITIAL ET PONDÉRATION DES DIFFÉRENTES REMÉDIATIONS

La phase d'analyse terminée, il sera fourni en sortie un ensemble cohérent de mesures applicables appelé « Plan de remédiation initial ». Dans le cadre de ce document, une bonne définition du terme remédiation serait : « Le processus d'amélioration ou de correction d'une situation de risque induite par une vulnérabilité. »

Ce plan initial documente dans les grandes lignes les différentes méthodes disponibles pour la correction de la vulnérabilité. Il existe globalement trois types de remédiation :

1. Correctif : dans cette situation l'éditeur ou le constructeur associé à la vulnérabilité propose un correctif logiciel permettant de la corriger. Il est possible que ce correctif ne corrige pas totalement la vulnérabilité et que l'éditeur annonce de futures publications plus complètes.
Dans tous les cas, cela peut entraîner des effets de bord sur la production auquel cas, il faut évaluer le risque induit par la vulnérabilité et l'impact du correctif.
2. Mesure de contournement : dans cette situation l'éditeur ou le constructeur ne propose pas un correctif mais une mesure de contournement rendant la vulnérabilité inexploitable. Il peut s'agir d'appliquer une configuration particulière par exemple.
3. Mesure d'atténuation : Dans cette situation, il n'est pas possible de corriger pleinement la vulnérabilité, ni par un correctif ni par une mesure de contournement : la tactique consistera à atténuer indirectement les risques associés à la vulnérabilité. Il peut s'agir de :

- "Virtual patching" consistant à bloquer l'exploitation de la vulnérabilité par une solution positionnée en amont de l'actif vulnérable. Les cas les plus classiques sont l'activation de règles sur un Web Application Firewall (WAF) ou une sonde de détection/prévention d'intrusion (IDS/IPS)
- Bloquer ou limiter l'accès au service vulnérable par du filtrage réseau ;
- La déconnexion complète du réseau, du système impacté.

Important : Pour certaines vulnérabilités, deux ou trois catégories de remédiation sont applicables. Il s'agira pour l'organisation de définir quel est le meilleur plan de remédiation dans son contexte.
Il est possible d'utiliser les attributs suivants pour caractériser chaque méthode de remédiation :

Remédiation #	% de correction - de 1 à 100%	Risque associé à la procédure (verte, jaune, orange, rouge)	Temps d'application	Niveau de perturbation de la production
(Attribut obligatoire)	(Attribut obligatoire)	(Attribut obligatoire)	(Attribut optionnel)	(Attribut optionnel)
Remédiation 1				
Remédiation 2				
Remédiation 3				

Les attributs « Temps d'application » et « Niveau de perturbation de la production » dépendent bien évidemment de l'activité de l'organisation, ils ne seront pas utiles ou systématiques dans tous les contextes.
À la suite de cette étude, un plan de remédiation est décidé, l'organisation doit maintenant confirmer l'efficacité des mesures correctives sélectionnées.

VALIDATION DES MESURES CORRECTIVES

Il est extrêmement important que l'organisation valide en situation les mesures correctives sélectionnées, plusieurs scénarios (liste non exhaustive) justifient cette étape :

- La mesure corrective ne permet pas d'atteindre l'objectif escompté ;
- La mesure corrective fonctionne mais son temps d'application laisse en risque l'organisation pendant une période trop importante ;
- La mesure corrective nécessite une interruption de service plus importante que ce qui avait été calculé ;
- La documentation du fournisseur pour appliquer la mesure corrective ne prend pas en compte, avec précision, le contexte particulier de l'organisation. Des tests sont donc nécessaires pour documenter l'application de la mesure dans ce contexte

Il conviendra d'effectuer les tests de validation sur une plateforme représentative de l'environnement de production, et de documenter la procédure si nécessaire. Les termes qualificatifs employés pour désigner l'environnement de validation peuvent variés selon l'organisation, mais il s'agit ici globalement d'environnements de type : test, intégration, validation, qualification, homologation...

Important : Il faut bien évaluer la période raisonnable consacrée à la validation en fonction du risque associé à la vulnérabilité considérée. En effet, si la vulnérabilité est porteuse d'un risque élevé pour l'organisation, celle-ci se doit de rester pragmatique est d'évaluer la dualité « risque sécuritaire » vs « risque d'interruption de service pour la production ». Il ne s'agit donc pas de « consommer » une semaine pour des tests additionnels s'il s'agit de corriger une vulnérabilité critique pour l'organisation. Il n'existe malheureusement pas de formule universelle mais l'organisation doit avoir ici une approche pragmatique et agile.

Lorsque les tests sont finalisés, l'organisation devra évaluer si le résultat escompté a bien été atteint et potentiellement corriger le tableau des remédiations présenté plus haut. De plus, il sera désormais possible de documenter la demande de changement et de préparer le rendez-vous avec le comité de validation des changements.

DOCUMENT DE DEMANDE DE CHANGEMENT ET VALIDATION PAR LE COMITÉ DE VALIDATION DES CHANGEMENTS

Appliquer une mesure corrective demeure un changement effectif d'un ou plusieurs systèmes IT. La plupart des organisations possèdent un comité de validation des changements (en anglais : CAB - Change Advisory Board) qui devra valider la demande de changement liée à l'application de la mesure de remédiation.
Dans les plus petites organisations, il n'y a pas de « CAB » formel, mais il s'agira encore ici d'être pragmatique et de réunir les personnes concernées par un impact potentiel lié à la mesure corrective.
La création d'un document de demande de changement et l'organisation d'un « CAB » dépasse le cadre de ce document, mais certaines questions seront systématiquement évaluées lors d'une réunion avec le « CAB », il s'agit de bien préparer en amont les éléments de réponse :

- Quels sont les bénéfices associés à l'application de ce correctif ?
- Quel est le risque lié à l'application du correctif ?
- Quelle est la procédure de retour-arrière si un problème survient pendant la procédure ? Quelle est sa durée de mise en œuvre ?
- Est-ce que la procédure de retour-arrière a été testée ?
- Quels sont les services de production impactés et pendant combien de temps ?
- Quelle est la procédure d'escalade en cas de problème pendant la réalisation de la remédiation ?

Une fois la demande de changement validée, il s'agira de planifier le déploiement des mesures de remédiation.
Il est à noter qu'il est important que le CAB soit sensibilisé à la gestion des vulnérabilités. Ce processus, ne doit pas être un frein trop important au maintien en sécurité du système d'informations.
Dans le cas des vulnérabilités les plus critiques, le CAB doit pouvoir être contourné, notamment grâce à la confiance dans la validation de la remédiation octroyée par les tests réalisés dans un environnement représentatif de la production.

PLANIFICATION ET RÉALISATION DU DÉPLOIEMENT

PRIORISATION PAR LES RISQUES

La priorisation par les risques consiste à définir quelles corrections sont essentielles pour conserver une posture de sécurité acceptable tout en prenant en compte la charge de travail globale des équipes de production.
Il est assez exceptionnel d'avoir la capacité de corriger toutes les vulnérabilités, c'est même généralement impossible, il faut donc pouvoir analyser les risques consécutifs à chaque vulnérabilité et prioriser celles qui sont essentielles à corriger et planifier le traitement de celles dont l'impact n'est pas critique.

La méthode est assez proche d'une gestion de risque classique. Dans le contexte de la gestion des vulnérabilités, la gestion par les risques consiste à évaluer des critères essentiels (liste non exhaustive) : le niveau de sévérité de la vulnérabilité elle-même, le maintien en condition opérationnelle de l'actif et l'application de patch réguliers, la possibilité d'usage réel de cette vulnérabilité par des attaquants, son impact potentiel dans le contexte de l'organisation.
L'ensemble de ces critères combinés appliqué à chaque vulnérabilité permettra d'établir la liste des vulnérabilités à corriger en priorité.

STRATÉGIE DE DÉPLOIEMENT

La stratégie de déploiement est liée à l'organisation elle-même et peut être influencée par différents critères :

- L'organisation possède-t-elle un ou plusieurs outils de déploiement ?
- Les différents environnements IT sont-ils gérés par une seule équipe ou la responsabilité est-elle répartie ?
- Un périmètre applicatif ou structurel est-il plus sensible à la vulnérabilité?
- Le déploiement de la mesure corrective nécessite-t-il un impact sur la disponibilité de tel ou tel service ?

Certaines organisations préfèrent gérer le rythme des mises à jour selon une catégorisation par type d'environnement : la méthode SSVC (voir. https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc) permet de définir une typologie à 4 choix possibles :

1. « Pas de remédiation appliquée »
2. « Application de la remédiation à la prochaine maintenance programmée »
3. « Application de la remédiation à une date définie spécifiquement sans attendre la prochaine maintenance programmée »
4. « Application immédiate de la remédiation »

Note : Le terme de maintenance programmée désigne une ou plusieurs dates connues et planifiées à l'avance qui sont consacrées à l'application des remédiations programmées. Il s'agit de dates ou le service de production est interrompu afin de réaliser des tâches spécifiques, cela inclue généralement des changements de matériel, des mises à jour applicatives lourdes et bien sur l'application des remédiations programmées.
Tout au long du traitement de la remédiation, le statut du plan de remédiation et de la vulnérabilité peut être modifié de la manière suivante :

- Environnement A : Risque accepté, date indéfinie
- Environnement B : Risque accepté jusqu'à la maintenance programmée
- Environnement C : Risque accepté jusqu'à la date définie
- Environnement D : En cours de remédiation

Certaines remédiations plus complexes, pourront potentiellement s'intégrer dans les projets en cours ou entraîner la création d'un projet, comme par exemple dans le cadre de la gestion de l'obsolescence.

RÉALISATION DU DÉPLOIEMENT

Il est possible de catégoriser plusieurs types de déploiements:

1. Le déploiement réalisé de manière automatique à l'aide d'outils ;
2. Le déploiement nécessitant une intervention manuelle via une session interactive sur le système lui-même ;
3. Le déploiement centralisé entraînant une action sur le code source et donc un redéploiement.

Selon la nature des actifs considérés, la gestion technique peut varier. Les principales situations rencontrées sont les suivantes :

- Les stations de travail sont gérées par un outil central
- Les serveurs sont gérés par un outil central ou par des interventions spécifiques
- Les environnements Cloud sont gérés via des modèles et du code et des outils spécifiques.

Une fois le déploiement de la remédiation effectué, le statut de la vulnérabilité pourra basculer en « déclaré corrigé ».

VALIDATION DE LA REMÉDIATION

Une fois le déploiement réalisé, il sera primordial de vérifier la bonne correction ou mitigation grâce à la réalisation d'un nouveau scan de vulnérabilité.

- Dans un contexte de fonctionnement nominal (business as usual), la vérification sera effectuée lors des scans programmés selon le rythme habituel (Par exemple : scan toutes les semaines ou en continu) ;
- Dans un contexte de crise (type vulnérabilité 0-day), il est conseillé de réaliser un scan immédiatement après le déploiement de la remédiation.

Dans certains cas, notamment dans le cas des mesures d'atténuation, les scans ne seront pas suffisants pour confirmer la bonne remédiation. Des vérifications spécifiques, telles que la réalisation d'un exercice Red Team, d'un test d'intrusion ou d'un test à l'aide d'un script sont nécessaires, selon la criticité ou selon le niveau de confiance attribué à l'éditeur.

Une fois la validation de la remédiation effectuée, le statut du traitement de la vulnérabilité pourra officiellement passer à « corrigé ».

MESURES CONSERVATOIRES DE DÉSACTIVATION

Outre l'application de mesures de mitigation, de contournement ou de correction de la vulnérabilité, la phase de remédiation peut conduire à désactiver temporairement des périmètres du Système d'Information, de solutions Cloud ou de produits vulnérables.
Ces mesures conservatoires de désactivation ont pour objectifs de minimiser les risques et de prévenir toute exploitation potentielle avant l'aboutissement du processus de remédiation.
Cette désactivation constitue une solution radicale dont la mise en œuvre doit être préparée, notamment afin d'en limiter les impacts techniques et métier.

PRINCIPES

La désactivation potentielle de périmètres vulnérables doit être anticipée sur les points suivants :

- Analyse d'impact "technique" : quels sont les services techniques vitaux pour le SI, la solution ou le produit qui peuvent être potentiellement touchés par une vulnérabilité nécessitant jusqu'à leur désactivation ?

Exemple : si la vulnérabilité impacte un service d'authentification centralisé, la désactivation de ce dernier peut conduire à bloquer l'accès à l'ensemble des ressources.

- Analyse d'impact "métier" : quel serait l'impact client, juridique, d'image, opérationnel et financier d'une désactivation forcée du SI, de la solution ou du produit et quelle en serait la durée maximum acceptable pour l'organisation ?

Exemple : une désactivation de l'accès à un site de commerce électronique supérieure à n jours aurait un impact inacceptable en perte potentielle de chiffre d'affaires et de clients.

- Solutions alternatives IT : est-il possible de basculer le périmètre vulnérable sur un périmètre alternatif non vulnérable ?

Exemple : Utiliser un serveur de présentation Web doté d'une technologie alternative ou basculer sur une version antérieure non vulnérable.
Exemple pour un SI : chaînes de secours s'appuyant sur des équipements de sécurité différents, d'OS différents, …

- Modes dégradés IT visant à réduire l'impact

Exemple pour un site web désactivé : basculer via le DNS ou le reverse proxy les flux sur une page de "maintenance" ou d'information afin de limiter l'impact sur l'image.

- Précautions à prendre pour permettre aux équipes d'investigation d'identifier dans quelle mesure la vulnérabilité a été exploitée ou non.

Exemple : Prévoir de déconnecter/isoler si besoin des périmètres vulnérables mais sans les éteindre.

L'effort requis par la préparation de ces plans alternatifs ainsi que leur efficacité peuvent être variables. Leur opportunité et faisabilité doit être étudiée en prenant en compte :

- La réduction d'impact attendue :

Exemple pour un site Internet : la bascule simple sur une page de maintenance peut permettre de limiter l'impact en matière d'image mais ne permettrait pas de réduire l'impact sur le chiffre d'affaires lié à l'indisponibilité de tel service.

- L'effort et le coût de mise en œuvre et de maintien en conditions opérationnelles du dispositif, notamment via des tests périodiques.

Exemple : L'élaboration et le maintien en conditions opérationnelles d'une chaîne de secours s'appuyant sur des technologies alternatives, peut présenter des efforts et des coûts disproportionnés par rapport à l'efficacité potentielle attendue et à la perte financière liée à l'indisponibilité de la chaîne nominale.

ACTEURS / EQUIPES CONCERNÉES

- Les **métiers** vont pouvoir évaluer l'impact lié à la désactivation de tel périmètre SI, plateforme Cloud ou produit et contribuer à la décision de retenir telle ou telle solution alternative ;

- Les **équipes IT** (applications et infrastructures) vont également contribuer à l'identification de l'impact lié à la désactivation de tel périmètre et proposer le cas échéant des solutions alternatives pour limiter cet impact.

PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE D'ACTIVITÉ

Une vulnérabilité touchant des services transverses d'un Système d'Information ou de l'accès à une plateforme Cloud (ex : cœur de confiance, DNS, référentiel d'identité, SSO…) peut nécessiter la désactivation de ces services et impacter par conséquent un large périmètre d'activités métiers.

De même, l'exploitation d'une vulnérabilité, peut également rendre indisponible un large périmètre de services pendant le temps nécessaire à sa remédiation. Afin d'en limiter l'impact, deux types de réponses sont à considérer :

- Le Plan de Continuité d'Activité (PCA) - qui vise à poursuivre les activités métier selon un plan établi et répété ;
- Le Plan de Reprise d'Activité (PRA) - composante du PCA qui vise à reconstruire, à plus ou moins long terme, le Système d'Information sur lequel s'appuient les activités métier, générant une indisponibilité partielle ou totale.

PRINCIPES

Ces plans de secours reposent principalement sur les activités suivantes :

- **Identification préalable des scénarios de risque auxquels ils doivent répondre**. Il peut s'agir par exemple de :
  - Scénarios "classiques", tels que l'indisponibilité d'un fournisseur critique ou l'indisponibilité d'un site d'hébergement à la suite d'un sinistre physique (incendie, inondation) ;
  - Scénarios d'une compromission/destruction logique du SI nominal propagée à ses réplicas hébergés sur des sites de secours ;
  - Scénarios liés à des vulnérabilités critiques ne pouvant être traitées que par un arrêt du SI de l'organisation ou de son fournisseur IT (ex : vulnérabilité critique impactant massivement le SI de l'infogérant ou du fournisseur de services Cloud).

Ces scénarios de risque sont notamment caractérisés par la vraisemblance de leur survenance (en fonction de la menace, de l'efficacité éprouvée des mesures de protection existantes, …) et par leur impact sur l'organisation s'ils se réalisent (jusqu'à la remise en cause de l'existence de l'organisation en cas de faillite par exemple). Cette caractérisation permet de prioriser les risques à couvrir et par conséquent de prioriser les plans à mettre en œuvre. *Exemple : Une organisation peut juger qu'en raison de l'état de la menace et de sa maturité cyber, le principal risque à couvrir est celui d'une cyberattaque sur son Système d'Information, avant celui d'un sinistre physique affectant l'hébergement de son SI ou le défaut de l'un de ses fournisseurs critiques.*

- **Identification des activités métiers** dont l'arrêt va avoir le plus d'impact sur l'organisation. Ces plans doivent permettre de reprendre :
  - Sous un délai défini ;
  - Avec une fraîcheur de données conforme au RTO/RPO défini.

Exemple : Les plans de secours doivent permettre de reprendre les activités liées à la vente impérativement au bout de x jours et sans avoir perdu plus de 24h de données, faute de quoi la survie de l'entreprise est en jeu.

- **Définition des grands principes** des plans de secours

Exemple : Un plan peut permettre au métier de reprendre pendant x semaines une activité dégradée avec des moyens indépendants du SI nominal de l'entreprise. Ce plan peut consister à exporter quotidiennement dans le Cloud des données des applications de gestion (listes de clients et de fournisseurs, inventaires, commandes, …) au format bureautique, de façon à permettre ensuite leur traitement via des outils standards immédiatement disponibles.

- Mise en œuvre des moyens liés à ces plans ;
- **Documentation du séquencement des opérations** liées à la reprise des fonctions SI / des activités métier et des procédures associées et déclenchées et suivies dans le cadre d'une gestion de crise ;
- **Tests** (unitaires / globaux) et mises à jour périodiques des plans et de leur documentation.

ACTEURS/ÉQUIPES CONCERNÉES

Un **sponsor**, sensibilisé aux enjeux métiers et SI, en mesure d'arbitrer l'affectation des moyens humains et financiers nécessaires à l'élaboration et à l'entretien des plans ;

- Les **métiers** qui vont exprimer leurs besoins, contribuer aux choix des plans ainsi qu'à l'élaboration de modes dégradé métiers sans SI ou avec des solutions SI alternatives ;
- Les **équipes IT** (applications et infrastructures) qui vont documenter, mettre en œuvre et tester les plans de reprise du SI ;
- Un "**pilote**" qui va assurer la coordination et le suivi des actions liées à la préparation de ces plans et à leur entretien et tests ;
- Des **Correspondants externes** (ex : correspondant infogérant, fournisseur de service cloud).

ÉVALUATION JURIDIQUE / RESPECT DES SLA

L'évaluation juridique est une étape cruciale dans la gestion globale des vulnérabilités, car elle garantit que toutes les actions réalisées par les entreprises pour remédier à une vulnérabilité sont conformes aux réglementations et aux obligations contractuelles en vigueur.
Il est essentiel de veiller au respect des accords de niveau de service (SLA) établis avec les clients ou les partenaires tout au long du processus de remédiation. Pour assurer une conformité adéquate et une gestion efficace des aspects légaux liés à la vulnérabilité, des consultations juridiques et des échanges avec les parties prenantes appropriées sont indispensables.
En matière de gestion des vulnérabilités, tant du point de vue du fournisseur que du consommateur de services/solutions/produits, le respect des réglementations est un enjeu important. Les non-conformités à des réglementations et directives peuvent dans certains cas entraîner des sanctions financières importantes, des poursuites judiciaires, la perte de confiance des clients et des répercussions négatives sur la réputation de l'entreprise.

PRINCIPES

Phase de préparation :
Indépendamment du processus décrit dans ce document, il est primordial pour une entreprise de réaliser les activités suivantes afin d'opérer d'une manière efficace lors du traitement d'une vulnérabilité :

1. **Réaliser une identification des différents enjeux juridiques :** il est important d'identifier les réglementations, lois et directives en matière de sécurité qui s'applique à l'entreprise et aux systèmes concernés. Il est également nécessaire de déterminer les conséquences potentielles en cas de non-respect des obligations légales et réglementaires. Cette phase permet de lister notamment les solutions à surveiller d'une manière régulière et proche lors de l'application d'un processus de gestion de vulnérabilité ;

2. **Consultation juridique :** si l'organisation ne dispose pas d'un département juridique / conformité, il est fortement recommandé de procéder à des consultations juridiques externes pour bénéficier de conseils avisés dans ces situations.

Phase de vulnérabilité identifiée
Lorsqu'une vulnérabilité est identifiée au niveau d'une organisation qui fournit un service, solution ou produit, il est essentiel de suivre des étapes juridiques spécifiques pour assurer une gestion appropriée des risques et une conformité légale adaptée à l'entreprise. Voici les principales étapes à suivre :

1. **Identification et documentation de la vulnérabilité** : la première étape serait d'identifier et de documenter de manière précise la vulnérabilité pour la rendre compréhensible à l'équipe juridique incluant son impact potentiel sur le service, ainsi que les systèmes ou les données qui pourraient être affectés.

Exemple : vulnérabilité de type injection SQL sur le serveur XX avec une possibilité de récupérer des informations liées à tous les utilisateurs, telles que les noms, prénoms et adresses e-mail et les mots de passe.

2. **Implication des équipes juridiques** : lors de l'identification d'une vulnérabilité, il est nécessaire d'impliquer au plus tôt le département juridiques/ou consultant juriste pour évaluer les implications juridiques nécessaires.

Exemple: si la vulnérabilité impacte un service essentiel pour la nation, ceci pourra impliquer des actions spécifiques dans le cadre de la LPM.

3. **Analyse de la conformité aux réglementations** : selon la nécessité, le département juridique / consultant juriste devrait mener une analyse approfondie pour déterminer si la vulnérabilité identifiée entraîne des violations de réglementations spécifiques liées à la sécurité de l'information, à la protection des données personnelles ou à d'autres obligations légales. *Cette analyse permettra de comprendre les risques juridiques potentiels et d'élaborer une approche appropriée pour la remédiation.*

Cette phase dépend du secteur d'activité et de la localisation géographique de l'entreprise, il peut exister des normes, des réglementations ou des Framework de sécurité spécifiques qui doivent être pris en compte dans le processus de remédiation.
Exemple : GDPR, LPM, etc.

4. **Contrats et SLA avec les clients** : dans le cas où l'entreprise fournit des services/solutions/produits à des clients, il est important de vérifier les contrats et les accords de niveau de service (SLA) en place pour s'assurer que les actions de remédiation sont en ligne avec les engagements pris envers les clients en termes de sécurité et de disponibilité des services.

Exemple : notification d'un client dans les 48h dans le cas d'une vulnérabilité critique conformément à une clause juridique dans le contrat.

5. **Notifications aux partie prenantes concernées** : selon la nature et l'ampleur de la vulnérabilité, il peut être nécessaire de notifier les parties prenantes concernées, telles que les clients, les utilisateurs ou mêmes dans certains cas, les autorités de régulation et/ou de certification tel que l'ANSSI (Agence Nationale de la sécurité des Système d'Information) ou l'ENISA (Agence de l'Union européenne pour la cybersécurité).

Exemple : dans le cadre d'une violation liée à la GDPR en France, en cas de la confirmation de l'exploitation d'une vulnérabilité permettant de récupérer des données personnelles, ceci pourra impliquer des actions spécifiques telles que la notification de la CNIL (Commission nationale de l'informatique et des libertés) dans les 72 heures.

6. **Élaboration d'un plan de remédiation** : En collaboration avec le département juridique, l'entreprise élabore un plan de remédiation qui tient compte à la fois des aspects techniques et juridiques. Le plan devrait inclure des mesures spécifiques pour corriger la vulnérabilité, ainsi que des actions pour se conformer aux réglementations applicables.

7. **Communication interne** : selon le plan de remédiation juridique, les responsables informent les équipes internes concernées, telles que l'équipe technique, les responsables de la sécurité et les parties prenantes clés, des mesures de remédiation envisagées. Selon les cas, les parties impliquées peuvent avoir un rôle différent dans le processus de résolution de la vulnérabilité et de mise en conformité légale.

8. **Mise en œuvre des mesures de remédiation** : l'entreprise doit s'assurer que les mesures de remédiation convenues sont mises en œuvre d'une manière conformes aux exigences légales et qu'elles sont effectives pour corriger la vulnérabilité.

9. **Suivi et documentation** : La traçabilité est une activité clé d'un point de vue juridique. L'entreprise doit s'assurer que toutes les actions prises pour remédier à la vulnérabilité, ainsi que les discussions et décisions prises en collaboration avec le département juridique sont suivies, documentées et auditables.

Exemple : confirmation par mail de l'équipe technique de la reprise d'un service soumis à des clauses strictes de reprise d'activité dans les contrats.

ACTEURS / ÉQUIPES CONCERNÉS

- **Département juridique et conformité** : sont les principaux acteurs impliqués dans l'évaluation juridique de la vulnérabilité, l'analyse des risques juridiques, l'identification des obligations réglementaires et légales, les impacts potentiels sur l'entreprise d'un point vue juridiques et conformité, la définition des mesures de remédiations prévues par rapport aux réglementations et directives.
- **Équipe sécurité informatique / opérationnelles** : ces équipes fournissent des informations techniques sur la vulnérabilité, telles que son impact et les mesures de remédiation possibles d'un point de vue opérationnel. Cette collaboration est essentielle pour comprendre la nature de la vulnérabilité et son contexte technique.

- **Services juridiques des clients ou partenaire**: dans le cas où la vulnérabilité a un impact direct sur les clients ou les partenaires, leurs équipes juridiques peuvent être impliquées pour évaluer l'impact sur leur propres obligations contractuelles et SLA.

- **Direction de l'entreprise**: la direction de l'entreprise est généralement tenue informée des aspects juridiques importants liés à la vulnérabilité et aux SLA pour prendre des décisions stratégiques.

- **Equipe communication**: l'équipe de communication doit être tenue informée des implications juridiques liées à la vulnérabilité afin de gérer efficacement la communication externe et interne en cas de besoin.

- **Auditeurs et régulateurs**: en fonction de la nature de l'entreprise et de ses obligations réglementaires, des auditeurs internes ou externes, ainsi que des régulateurs, peuvent être impliqués pour évaluer la conformité de l'entreprise aux réglementations en matière de sécurité de l'information.

ACTUALISATION DE LA COMMUNICATION

Cette étape du processus consiste en la mise à jour des communications relatives à la vulnérabilité et à la remédiation qui ont déjà été initiées. Une communication claire, proactive et régulière contribue à maintenir la confiance et à assurer une coordination efficace pendant tout le processus de remédiation.

PRINCIPES

L'actualisation de la communication reposent principalement sur les activités suivantes :

1. **Fréquence de communication** : détermination de la fréquence à laquelle les mises à jour de communication seront fournies. Cela peut varier en fonction du niveau de criticité des vulnérabilités et des délais de remédiations. Certaines règlementations peuvent également dicter des exigences sur les délais et les fréquences de communication à respecter.

Exemple: lorsqu'une vulnérabilité critique est confirmée, l'entreprise devrait communiquer à minima une fois par semaine sur l'état d'avancement du plan de remédiation au client afin de respecter un contrat spécifique.

2. **Contenu de la communication** : les évolutions éventuelles du plan d'action, les progrès réalisés et les résultats obtenus.
3. **Communication en cas de retard ou de changement** : il est conseillé de prévoir un processus de communication spécifique en cas de retard dans la remédiation ou de changement dans les plans initiaux pour informer rapidement les parties prenantes concernées, fournir des explications claires et proposer des solutions alternatives si nécessaire.
4. **Rapport d'incident et d'analyse post-remédiation** : il est conseillé, pour toute vulnérabilité identifiée, pouvant être associée à une crise et finalement corrigée, de réaliser un rapport à minima d'analyse post-remédiation. Ces rapports détaillent les leçons apprises, les améliorations apportées au processus de gestion des vulnérabilités et les mesures de prévention pour l'avenir. Ce contenu pourra être utilisé lors de certaines communications afin de sensibiliser les acteurs et construire des bonnes habitudes.

ACTUALISATION DU PLAN DE REMÉDIATION

L' actualisation du plan de remédiation se fait par itérations jusqu'à constatation de :

- L'absence de risque résiduel ;
- Risque résiduel durablement acceptable (acceptation du risque) ;
- Traitement du risque résiduel vers un mode projet avec une planification établie.

A ce stade du processus, le choix arrêté pour gérer la vulnérabilité va nécessairement engendrer des impacts sur le fonctionnement nominal du système considéré que ce soit par la mise en place de nouvelles mesures, par la désactivation de fonctions ou par l'application des procédures de continuité ou de reprise d'activité.

Le niveau de risque initialement évalué doit alors être recalculé dans tous les cas (y compris s'il a été initialement accepté) sur la base de l'efficacité des mesures retenues ou au regard des conséquences de la désactivation de fonctions ou du recours aux plans de continuité et de reprise d'activité. Le risque ainsi réévalué est appelé risque résiduel. En ce sens, le risque résiduel s'entend comme la partie du risque original (initial ou brut) qui n'est traitée par la remédiation

Plusieurs postures sont possibles. Si le risque résiduel (initial ou brut) est :

- Au-dessus du seuil d'acceptabilité : il faut continuer les travaux pour réduire le risque en complémentant ou modifiant le plan d'action, et itérer sur ce processus ;
- En dessous du seuil d'acceptabilité : le composant impacté a retrouvé un fonctionnement nominal d'un point de vue disponibilité, performance et sécurité, conformément aux SLA éventuellement définis. Le risque résiduel doit être matérialisé dans le Plan de Traitement des Risques et accepté comme tel par la Direction et le propriétaire défini. Les travaux peuvent se poursuivre pour diminuer / annuler totalement le risque si cela est possible, mais cela peut se dérouler en dehors de l'organisation exceptionnelle (gestion de crise, etc) qui a été initialement mise en place lorsque le risque dépassait le seuil d'acceptabilité.

RETOUR D'EXPÉRIENCE (RETEX)

En fin de phase d'éradication ou plus généralement lorsque l'incident est considéré sous contrôle et traité à nouveau dans un contexte nominal (hors dispositif de crise / suivi renforcé), il est intéressant de poursuivre systématiquement le traitement par une phase de retour d'expérience (RETEX). En effet, les traitements mobilisent des ressources et réclament du temps. A ce titre, il importe de capitaliser sur les investissements consentis. La capitalisation s'entend en termes de qualification de l'événement, de prise en charge et d'escalade, de traitement, de réactivité et de reproductibilité de l'événement.

Cette phase s'appuie sur un rapport rédigé par le pilote de l'incident, et comportant généralement une synthèse managériale, la liste des points positifs et des pistes d'amélioration consignées, si possible, au fil de l'eau du traitement de l'incident ainsi qu'un chronogramme des actions et temps forts majeurs, extrait si possible de la main courante de pilotage de l'incident qui consigne l'historique des événements, des actions, des décisions, des résultats et des échecs.

Ce rapport est présenté à l'occasion d'une réunion de RETEX à chaud et planifiée dans les jours qui suivent afin d'avoir encore une mémoire très détaillée des évènements. Si nécessaire, le pilote de l'incident peut réaliser des réunions d'interview avec tout ou partie des protagonistes pour compléter le rapport et préparer la réunion.

Cette réunion doit rassembler tous les protagonistes de l'incident et permettre de consigner leurs remarques et mettre collectivement à jour le rapport. En finalité, cette réunion vise à rédiger le plan d'action et d'amélioration, avec des actions unitaires attribuées à un porteur, une échéance souhaitée et convenue conjointement et un suivi global de ces actions par une équipe de gouvernance dans la durée.
Une réunion à froid peut également être organisée à la clôture complète de l'incident pour consigner d'éventuels éléments complémentaires ou procéder à des ajustements dans les observations déjà réalisées à chaud et dans le plan d'action.
L'ensemble de ce processus de RETEX contribue à l'amélioration continue des processus et actions de qualification et traitement et boucle sur une nouvelle phase de préparation à la survenance d'un évènement du même type, via le traitement du plan d'action et l'enrichissement d'une base de connaissances. La démarche est conforme à de nombreux référentiels (exemple : ISO27001, ISO22301).

Ces RETEX peuvent aussi servir à la formation :

- Des personnels à la survenue d'une crise soit sous la forme d'exercices sur table soit via le rejeu de la vulnérabilité sous forme de simulations de cellules de crise.
- Des équipes techniques en termes de cas d'espèces servant au transfert de compétences.

<GLOSSAIRE>

LOGICIELS : Ce qui est développé.

PROGICIELS : Ce qui est acheté à un éditeur et intégré. Le terme de «logiciel sur étagère» est parfois employé.

0-DAY : Erreur dans un logiciel, ayant une portée sécurité (une faille), découverte et connue uniquement du découvreur ainsi que d'un cercle limité de personnes ou entités avec qui il l'a partagé. En général, l'éditeur du logiciel est exclu de ces sachants. Le terme peut également être employé, par abus de langage, pour décrire des vulnérabilités connues publiquement mais ne disposant pas de correctif https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043228194 .

BLUE TEAM : La Blue Team comporte un SOC et/ou un CERT .

BUG BOUNTY (PRIME À LA VULNÉRABILITÉ) : Démarche consistant à mettre en place un programme de récompense lors de la découverte de vulnérabilité, avec ou sans passer par un intermédiaire. Il s'agit de proposer un périmètre à évaluer (tout ou partie des applications, services…), publiquement ou en privé, à tout le monde ou à une sélection de professionnels de la cybersécurité, avec les montants des primes associées aux catégories des vulnérabilités (le montant total des primes doit être plafonné mais présente le risque de s'arrêter en cours s'il est atteint).

CERT (COMPUTER EMERGENCY RESPONSE TEAM) OU CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM) : Équipe de réponse et coordination de la réponse aux incidents de cybersécurité. Selon les organisations, le CERT peut également être en charge de la veille.

CERT-FR : Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques français, il est opéré au sein de la Sous-Direction Opérations (anciennement COSSI / Centre Opérationnel de la Sécurité des Systèmes d'Information) de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

CESIN (CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION ET DU NUMÉRIQUE) : Association favorisant les retours d'expérience entre professionnels de la sécurité de l'information et du numériques.

CLUSIF (CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS) : Association d'intérêt public regroupant les professionnels de la sécurité de l'information (utilisateurs, RSSI et offreurs) au sein de groupes de travail, publications et conférences, depuis 1982.

CLUSIR : Associations régionales décentralisées liées au Clusif.

CMDB (CONFIGURATION MANAGEMENT DATABASE) : Une base de données qui contient toutes les informations pertinentes sur les composants informatiques d'une organisation et les relations entre eux, utilisée principalement pour la gestion des services IT.

< GLOSSAIRE >

CVSS (COMMON VULNERABILITY SCORING SYSTEM) : Système standardisé d'évaluation de la criticité des vulnérabilités selon des critères objectifs et mesurables.

COMEX (COMITÉ EXÉCUTIF) : Un terme généralement utilisé pour désigner le comité exécutif d'une entreprise, qui est le groupe de hauts dirigeants chargés de prendre des décisions stratégiques.

COORDINATED DISCLOSURE : Une approche en matière de cybersécurité où la découverte d'une vulnérabilité est partagée de manière confidentielle avec l'entité affectée avant d'être divulguée publiquement, permettant le développement et la distribution d'un correctif.

CVE (COMMON VULNERABILITIES AND EXPOSURES) : Un système de référencement public pour les vulnérabilités de sécurité informatique connues, offrant une méthode standardisée pour identifier chaque vulnérabilité unique.

CWE (COMMON WEAKNESS ENUMERATION) : Un système de classification et de référencement pour les types de vulnérabilités logicielles, destiné à aider à la sensibilisation et à la prévention des faiblesses dans le code qui peuvent conduire à des vulnérabilités de sécurité.

DAST (DYNAMIC APPLICATION SECURITY TESTING) : Solution de tests dynamiques de sécurité des applications permettant de détecter des vulnérabilités et des faiblesses dans la sécurité d'une application au cours de son exécution.

DENIAL OF SERVICE / DOS (DÉNI DE SERVICE) : Attaque visant à rendre un service indisponible soit par l'exploitation d'une vulnérabilité bloquante, soit par la saturation de ses ressources (CPU, mémoire…)

DISTRIBUTED DENIAL OF SERVICE / DDOS (DÉNI DE SERVICE DISTRIBUÉ) : Attaque réseau visant à rendre un service indisponible par l'envoi de très nombreuses requêtes par de très nombreuses sources en saturant soit sa bande passante (attaque volumétrique) soit ses ressources (attaque applicative).

EBIOS RISK MANAGER : Méthode d'appréciation et de traitement des risques numériques publiée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) avec le soutien du club EBIOS.

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS) : Une association internationale de professionnels de la réponse aux incidents et de la sécurité, qui vise à favoriser la coopération et la coordination dans la gestion des incidents de sécurité informatique.

< GLOSSAIRE >

IAST (INTERACTIVE APPLICATION SECURITY TESTING) : Le nommage interactif, vient du fait que cet outil va permettre de tester l'application à son utilisation lors de tests de recette automatisés ou humains ou lors d'une interaction technique.

LIBRAIRIES / BIBLIOTHÈQUE LOGICIELLE : Collection de routines, qui peuvent être déjà compilées et prêtes à être utilisées par des programmes.

LOCAL CODE EXÉCUTION (EXÉCUTION DE CODE EN LOCAL) : Attaque permettant d'injecter du code arbitraire et non contrôlé dans un système vulnérable en étant connecté localement à ce système

LOCAL PRIVILEGE ESCALATION (ELEVATION LOCALE DE PRIVILÈGES) : Attaque permettant d'élever localement ses privilèges sur un système vulnérable afin de pouvoir réaliser des actions qui ne serait normalement pas autorisées.

LOI DE PROGRAMMATION MILITAIRE (LPM) : Loi française qui fixe les orientations et les moyens financiers alloués à la défense nationale sur une période pluriannuelle.

MENU CONTEXTUEL : Liste de commandes ou d'options apparaissant à l'écran lorsque l'utilisateur clique avec le bouton droit de la souris ou appuie sur un bouton de menu contextuel. Il peut varier en fonction de l'endroit où l'utilisateur se trouve, du programme utilisé ou de certaines autres variables.

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) : Organisme gouvernemental des États-Unis chargé du développement et de la promotion de normes et de technologies de pointe pour de nombreux domaines, y compris la cybersécurité.

NVD (NATIONAL VULNERABILITY DATABASE) : Base de données gérée par le NIST qui fournit des informations détaillées sur les vulnérabilités de sécurité connues dans les IT.

OSSIR (OBSERVATOIRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX) : Association regroupant les professionnels de la sécurité de l'information autour d'ateliers mensuels avec deux présentations techniques et une revue d'actualité sécurité dont des vulnérabilités. Toutes les présentations sont publiquement disponibles https://www.youtube.com/c/ossirFrance

RSSI (RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION) : Poste clé dans les entreprises et les organisations qui ont besoin de protéger leurs systèmes d'information et leurs données sensibles contre les menaces internes et externes.

SAST (STATIC APPLICATION SECURITY TESTING) : Outil de tests statiques de sécurité des applications permet aux développeurs de rechercher directement de potentielles vulnérabilités dans le code source de l'application au plus tôt dans le cycle de vie du développement logiciel.

< GLOSSAIRE >

SCA (SOFTWARE COMPONENT ANALYSIS) : Outil qui permet de vérifier la composition d'une application en termes de dépendances tierces et de licences. Comme les applications embarquent généralement des cadriciels (frameworks), des librairies Open Source ou propriétaires entre autres, il est nécessaire de vérifier que l'artefact résultant n'embarque pas des composants connus comme vulnérables ou obsolètes mais également qu'il n'y ait pas de défaut de compatibilité de licences.

SBOM (SOFTWARE BILL OF MATERIALS) : Liste des composants logiciels rencontrés dans un système en particulier. Cette liste est essentielle pour comprendre les vulnérabilités potentielles et les risques de cybersécurité.

SHADOW IT : Utilisation de logiciels, d'appareils ou de services en dehors du contrôle officiel et de la gouvernance de l'entreprise, souvent liée à des préoccupations de commodité ou de coût.

RED TEAM : Personnes autorisées et organisées pour simuler les capacités d'attaque ou d'exploitation d'un adversaire potentiel contre la posture de sécurité d'une entreprise. L'objectif de la Red Team est d'améliorer la cybersécurité de l'entreprise selon des scénarios prédéfinis.

REMOTE CODE EXECUTION (EXÉCUTION DE CODE À DISTANCE) : Attaque permettant d'injecter du code arbitraire à distance dans un système vulnérable (via le réseau, local ou Internet) et d'en prendre le contrôle.

RPO (RECOVERY POINT OBJECTIVE) : Selon l'ISO 22301, le RPO est défini comme l'objectif en termes de durée de la période pendant laquelle les données peuvent être perdues suite à un incident ou une perturbation.

SOC (SECURITY OPERATION CENTER) : Ensemble de moyens humains et techniques chargés de surveiller et d'analyser en permanence le dispositif de sécurité d'une entreprise, puis de réagir en cas d'alerte. Suivant les organisations, la réponse à l'incident de sécurité peut être traitée par le CERT ou par le SOC.

VDP, POLITIQUE DE DIVULGATION DE VULNÉRABILITÉS : Le cadrage interne consiste à définir une Politique de Divulgation de Vulnérabilités ou Vulnerability Disclosure Policy (VDP) en anglais. Une VDP est une organisation mise en place pour permettre le recueil légal de vulnérabilités remontées par des sources externes à l'entreprise, en toute sécurité.

VOC (VULNERABILITY OPERATION CENTER) : ensemble de moyens humains et techniques chargés de surveiller et de piloter le traitement des vulnérabilités techniques. A noter que ce terme est une invention française et n'existe pas dans le monde anglo-saxon qui lui préfère « vulnerability management ».*

ZERO DAY / 0-DAY : Ce terme fait référence à une vulnérabilité de sécurité dans un logiciel ou un système d'information qui est exploitable par des hackers avant que les fournisseurs ou les développeurs aient pu créer et publier un correctif.

< RÉFÉRENCES >

Guide gestion de crise publié par l'ANSSI : https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/

Guide de la méthodologie d'analyse de risque EBIOS RM : https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
ADRESSE MAIL DE CONTACT : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX