



WEBFORCE
BE THE CHANGE



RÉSUMÉ THÉORIQUE - FILIÈRE INFRASTRUCTURE DIGITALE

M211 - Analyser les attaques et les incidents de Cybersécurité



42 heures



SOMMAIRE

1. S'APPROPRIER LA NOTION D'UN INCIDENT DE SÉCURITÉ

- Définir un incident de sécurité
- Analyser le Kill Chain

2. APPLIQUER LES PROCÉDURES DE GESTION DES INCIDENTS

- Présenter le processus de gestion des incidents de sécurité
- Appliquer les procédures 800-61 R2 du NIST

3. EFFECTUER LE THREAT HUNTING

- Définir le Threat Hunting
- Identifier les étapes du processus

4. RÉPONDRE À DES INCIDENTS DE CYBERSECURITÉ

- Définir les étapes d'un plan de base de réponse aux incidents
- Automatiser la réponse aux incidents

MODALITÉS PÉDAGOGIQUES



WEBFORCE
BE THE CHANGE



1

LE GUIDE DE SOUTIEN
Il contient le résumé théorique et le manuel des travaux pratiques



2

LA VERSION PDF
Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life



3

DES CONTENUS TÉLÉCHARGEABLES
Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life



4

DU CONTENU INTERACTIF
Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life



5

DES RESSOURCES EN LIGNES
Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage



WEBFORCE
BE THE CHANGE



PARTIE 1

S'APPROPRIER LA NOTION D'UN INCIDENT DE SÉCURITÉ

Dans ce module, vous allez :

- Comprendre les éléments d'un incident de sécurité
- Connaître les étapes du Kill Chain



8 heures



CHAPITRE 1

Définir un incident de sécurité

Ce que vous allez apprendre dans ce chapitre :

- Déterminer les impacts des incidents de sécurité
- Définir et classer les incidents de sécurité
- Apprendre comment réagir devant un incident de sécurité



4 heures

CHAPITRE 1

Définir un incident de sécurité

1. **Impacts possibles d'un incident de sécurité**
2. Qualification d'un incident de sécurité



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

Introduction

- Les entreprises, les organisations et même les individus sont régulièrement attaqués par des cybercriminels et subissent souvent des dommages à long terme.
- L'année 2021 a été marquée par l'augmentation inattendue du nombre de cyberattaques au Maroc. En effet, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a signalé que ses centres de veille ont détecté et analysé environ 400 incidents [*].
- Les principales missions de ces centres sont :
 - ✓ Identifier et traiter les menaces de sécurité
 - ✓ Protéger les données confidentielles et les systèmes d'information contre les attaques externes et internes
 - ✓ Neutraliser les incidents de sécurité



Reference : * https://www.lopinion.ma/Cyber-securite-La-DGSSI-confirme-sa-reponse-a-des-centaines-de-cyberattaques-contre-le-Maroc_a27027.html

01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

C'est quoi un incident de sécurité?

- **Un incident de sécurité** est une occurrence ou un évènement qui compromet le bon fonctionnement, la sécurité d'un système d'information ou bien la modification ou la destruction non autorisés d'informations. Autrement dit, c'est tout incident intentionnel ou non intentionnel qui constitue une menace accrue pour la sécurité informatique. Il peut s'agir d'une menace suspectée, tentée, réussie ou imminente de cet accès non autorisé.
- Cela signifie que quelle que soit la réussite ou la sévérité de l'incident de sécurité, l'exécution des procédures de traçage et de suivi est primordiale pour garantir la confidentialité et la fiabilité des systèmes informatiques et empêcher qu'un événement similaire ne se reproduise à l'avenir.
- Un incident de sécurité peut être isolé ou consister en plusieurs événements qui, ensemble, indiquent que les systèmes ou les données d'une organisation peuvent avoir été compromis ou que les mesures de protection peuvent avoir échoué.
- Voici des exemples d'incidents de sécurité :
 - ✓ Modifications non autorisées des systèmes, des logiciels ou des données
 - ✓ Accès non autorisé ou utilisation de systèmes, de logiciels ou de données
 - ✓ Attaque par déni de service
 - ✓ Comptes d'utilisateurs compromis



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

Exemples :

- Selon une nouvelle étude de la société de sécurité de contenu **IRDETO**, les pirates vendent des centaines d'informations de connexion volées pour des services over-the-top OTT populaires sur les marchés du "**DARK WEB**".
- Pour le mois d'avril 2018, **IRDETO** a découvert 854 listes d'informations d'identification OTT de 69 vendeurs uniques sur plus de 15 marchés du **DARK WEB**. Les noms d'utilisateur et mots de passe volés en vente provenaient de 42 services de streaming différents, dont [Netflix](#), [HBO](#), [DirecTV](#) et [Hulu](#).
- Il n'est pas clair si les informations de compte OTT volées illégalement disponibles à la vente étaient des comptes légitimes et actifs - ou simplement des escroqueries de cybercriminels. (**IRDETO** n'a pas précisé s'il avait testé les informations d'identification volées.) Sur les marchés du **DARK WEB**, masqués à l'aide de protocoles d'accès secrets, un large éventail de produits, comptes et services illicites sont disponibles à l'achat, y compris des informations d'identification de compte pour une gamme de services de télévision payante.



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

Exemples :

- **YAHOO** a une longue histoire de violations de données et de cas où des pirates pénètrent dans les systèmes mais ne prennent rien. Les hacks collectifs ont conduit à un règlement auquel les parties concernées peuvent participer.
- **YAHOO** fournit un avis aux comptes d'utilisateurs supplémentaires affectés par un vol de données d'utilisateurs en août 2013 précédemment annoncé par la société en décembre 2016. Il ne s'agit pas d'un nouveau problème de sécurité. En 2016, Yahoo avait déjà pris des mesures pour protéger tous les comptes d'utilisateurs.



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité



Impacts des incidents :

Les impacts des failles de sécurité tiennent compte des effets immédiats et durables sur les individus et les organisations.

Perte de données : Elles peuvent être détruites ou modifiées au-delà de la récupération.

Domage à l'image publique : Les bonnes réputations sont difficiles à cultiver mais faciles à détruire.

Réduction de la productivité :

- Productivité = dans quelle mesure un employé fait son travail ?
- L'employé doit réagir et se remettre de l'attaque
- les systèmes attaqués peuvent subir des temps d'arrêt, ce qui signifie qu'ils ne sont pas disponibles. Par conséquent :
 1. L'employé ne peut pas utiliser le système.
 2. Les clients ne peuvent pas utiliser le système.

Une action en justice :

- Ne pas protéger correctement les informations personnelles peut entraîner de lourdes amendes en vertu de la **loi sur la protection des données**
- Les victimes concernées peuvent poursuivre l'organisation pour obtenir une **indemnisation**



Remarques

- **PERTE FINANCIÈRE** : Tous ces impacts peuvent entraîner une perte d'argent

01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

Exemple : MAROC

Le Maroc est au 34e rang mondial des cyberattaques, 5,06 millions de menaces

- Entre avril et juin 2019, un total de plus de 5,06 millions d'internautes au Maroc ont été victimes de cyberattaques, principalement des attaques de logiciels malveillants. Les attaques de logiciels malveillants exécutent des actions non autorisées sur le système de la victime.
- Kaspersky a déclaré dans son bulletin trimestriel sur la cybersécurité au Maroc, qu'environ 30,7% des utilisateurs de "Kaspersky Security Network" ont été victimes de menaces basées sur le Web.
- Au deuxième trimestre 2019, les solutions de Kaspersky ont détecté localement plus de 15 166 incidents malveillants sur des ordinateurs utilisant Kaspersky Security Network au Maroc. Les incidents de logiciels malveillants ont été distribués via des clés USB, des CD, des DVD et d'autres méthodes "hors ligne".



<https://www.morocoworldnews.com/2019/10/284120/morocco-cyber-attacks-threats-kaspersky>

CHAPITRE 1

Définir un incident de sécurité

1. Impacts possibles d'un incident de sécurité
2. **Qualification d'un incident de sécurité**



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité

Qualification d'un incident de sécurité :

- Lorsqu'un incident de sécurité se produit, une des premières étapes du processus de réponse aux incidents consiste à répondre à la question : « À quel point est-ce grave ? » ou bien qualifier l'incident. La réponse à cette question est la clé pour bien préciser la stratégie de défense adéquate à chaque situation, en fin de compte, améliorer la sécurité du système informatique.
- En fait, une stratégie efficace de qualification des incidents permet de :
 - ✓ Accélérer la prise de décision : avec les bonnes informations concernant la qualification de l'incident, les responsables de sécurité peuvent se concentrer sur leur rôle dans la réponse à l'événement.
 - ✓ Initier rapidement et efficacement la réponse : les qualifications facilitent la détermination des étapes de réponse spécifiques à suivre et les personnes particulières à notifier.
 - ✓ Prioriser la gestion des incidents : en spécifiant la gravité d'un incident par rapport à d'autres incidents, les responsables de sécurité peuvent se focaliser sur les incidents prioritaires avant de répondre aux événements à faible impact.
 - ✓ Renforcez le plan de réponse : un ensemble standard de qualifications facilite l'identification des points faibles et rend les activités post-incident plus efficaces.



01 – Définir un incident de sécurité

Impacts possibles d'un incident de sécurité



Qualification d'un incident de sécurité:

- **La qualification des incidents** est la démarche d'identification et d'archivage des types et de la gravité d'un incident.
- Généralement, les incidents peuvent être classés à trois niveaux :
 - ✓ Risque majeur (le plus critique et le plus urgent) : fuite de données sur les cartes de paiement, d'informations personnellement identifiables (PII), d'informations de santé protégées (PHI), d'informations classifiées ou d'autres données susceptibles d'aboutir à des dégâts critiques en cas de divulgation ou de corruption.
 - ✓ Risque modéré : exposition des données ou d'informations de nature confidentielles et dont la manipulation ou la divulgation peut entraîner une perte importante, comme : les listes des clients, la rémunération du personnel, les fichiers RH, les propositions commerciales et les rapports financiers.
 - ✓ Risque mineur (le moins critique et le moins urgent) : les seules données exposées ou éventuellement exposées sont accessibles au public ou sans valeur, comme : des communiqués de presse et des horaires de cours, des listes d'adresses e-mail, et des informations techniques des matériels non confidentielles.
- En résumé, la qualification des incidents a un impact direct sur l'efficacité et la précision des processus de réponse aux incidents car elle aide à déterminer les personnes qui doivent être averties et quelles autres étapes selon la sévérité de l'incident.

CHAPITRE 2

Analyser le Kill Chain

Ce que vous allez apprendre dans ce chapitre :

- Découvrir les caractéristiques de la Kill Chain
- Détailler les étapes de la Cyber Kill Chain



4 heures

CHAPITRE 2

Analyser le Kill Chain

1. **Notion du Kill Chain**
2. Etapes du Kill Chain

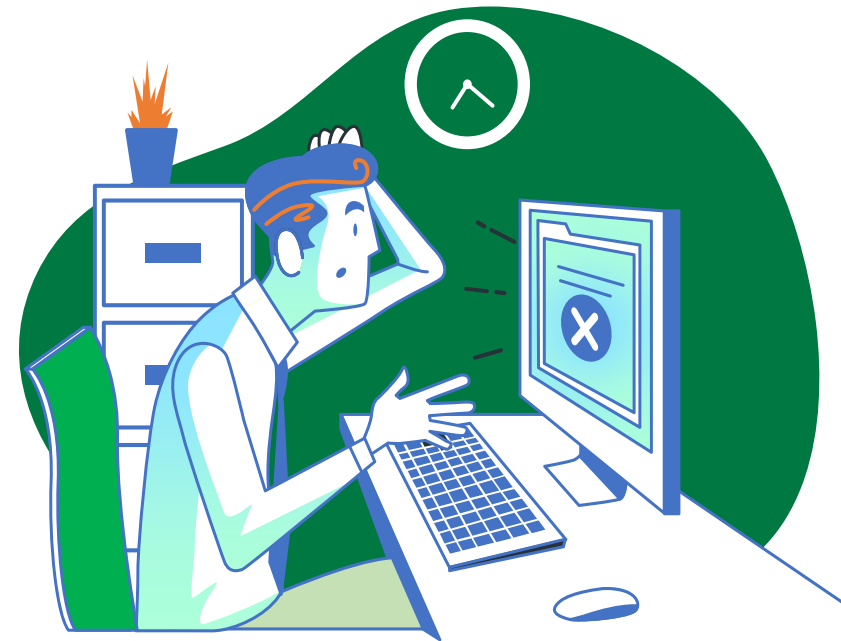


02 – Analyser le Kill Chain

Notion du Kill Chain

Problématique :

- L'un des principaux problèmes auxquels sont confrontées les organisations est l'émergence d'attaques ciblées menées par des adversaires qui ont facilement accès à des outils et à des technologies sophistiqués dans le but d'établir une présence persistante et non détectée dans la cyber infrastructure ciblée.
- Ces attaques en plusieurs étapes deviennent désormais plus complexes, impliquant des mouvements verticaux et horizontaux à travers de multiples éléments de l'organisation.
- La communauté de la recherche en sécurité a donné à cette chaîne d'événements en plusieurs étapes aboutissant au cyber espionnage un nom : la chaîne de cybercriminalité **KILL CHAIN**.

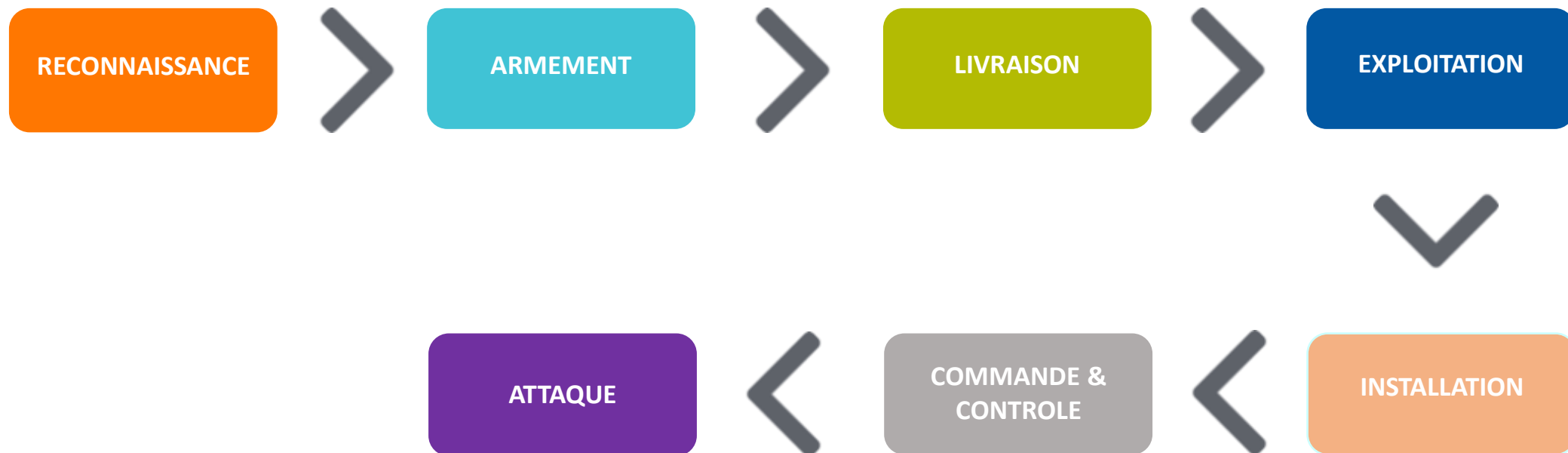


02 – Analyser le Kill Chain

Notion du Kill Chain

C'est quoi Kill Chain ?

- La cyber **KILL CHAIN** est essentiellement un modèle de cyber sécurité créé par Lockheed Martin qui retrace les étapes d'une cyberattaque, identifie les vulnérabilités et aide les équipes de sécurité à stopper les attaques à chaque étape de la chaîne.
- Le terme **KILL CHAIN** est adopté par l'armée, qui utilise ce terme lié à la structure d'une attaque.
- Il consiste en l'identification d'une cible, l'envoi, la décision, l'ordre et enfin la destruction de la cible.

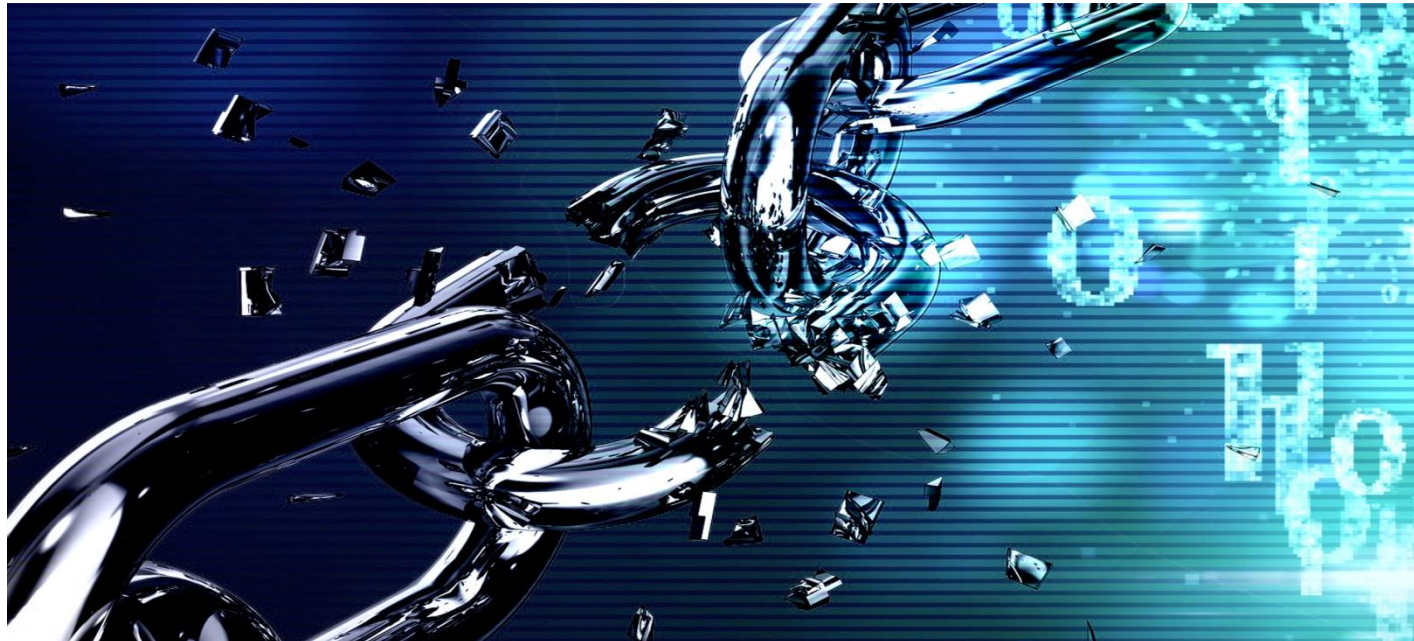


02 – Analyser le Kill Chain

Notion du Kill Chain

Exemple : Lockheed Martin

- Développé par **Lockheed Martin**, le cadre Cyber Kill Chain fait partie du modèle Intelligence Driven Defense pour l'identification et la prévention des activités de cyber-intrusions. Le modèle identifie ce que les adversaires doivent accomplir pour atteindre leur objectif.
- Les sept étapes de la Cyber Kill Chain améliorent la visibilité sur une attaque et enrichissent la compréhension d'un analyste des tactiques, techniques et procédures d'un adversaire.



<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

CHAPITRE 2

Analyser le Kill Chain

1. Notion du Kill Chain
- 2. Etapes du Kill Chain**

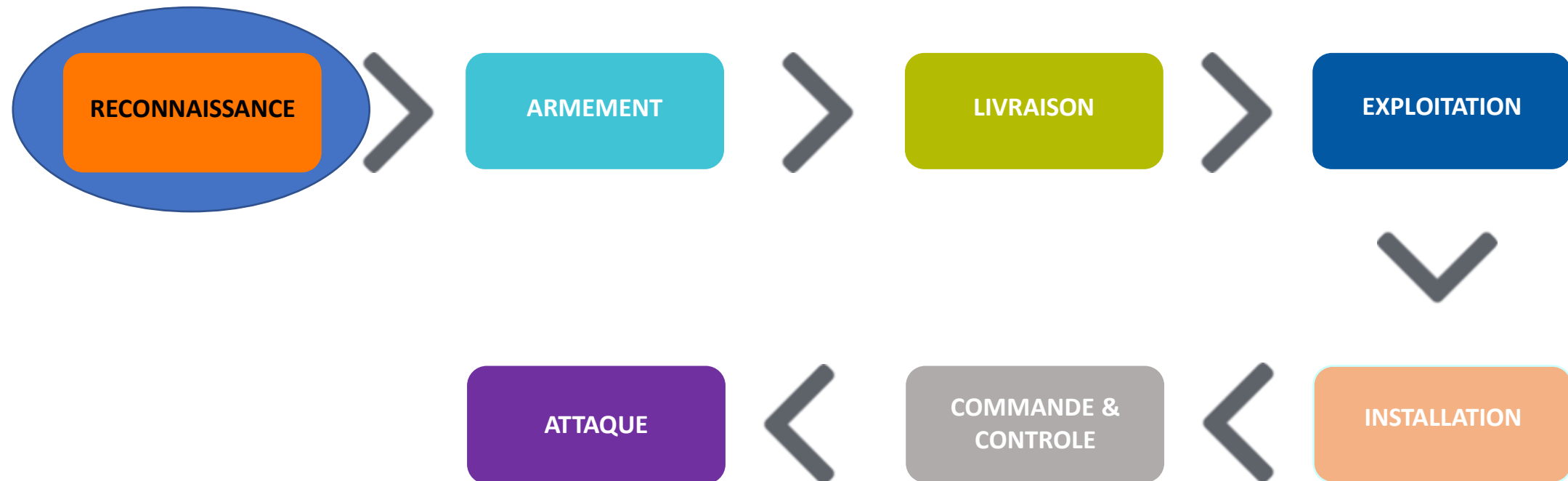


02 – Analyser le Kill Chain

Etapes du Kill Chain

Reconnaissance :

- L'attaquant collecte des données sur la cible et les tactiques de l'attaque. Cela inclut la collecte d'adresses e-mail et la collecte d'autres informations.
- Les scanners automatisés sont utilisés par les intrus pour trouver des points de vulnérabilité dans le système. Cela inclut l'analyse des pare-feu, des systèmes de prévention des intrusions, etc. pour obtenir un point d'entrée pour l'attaque.

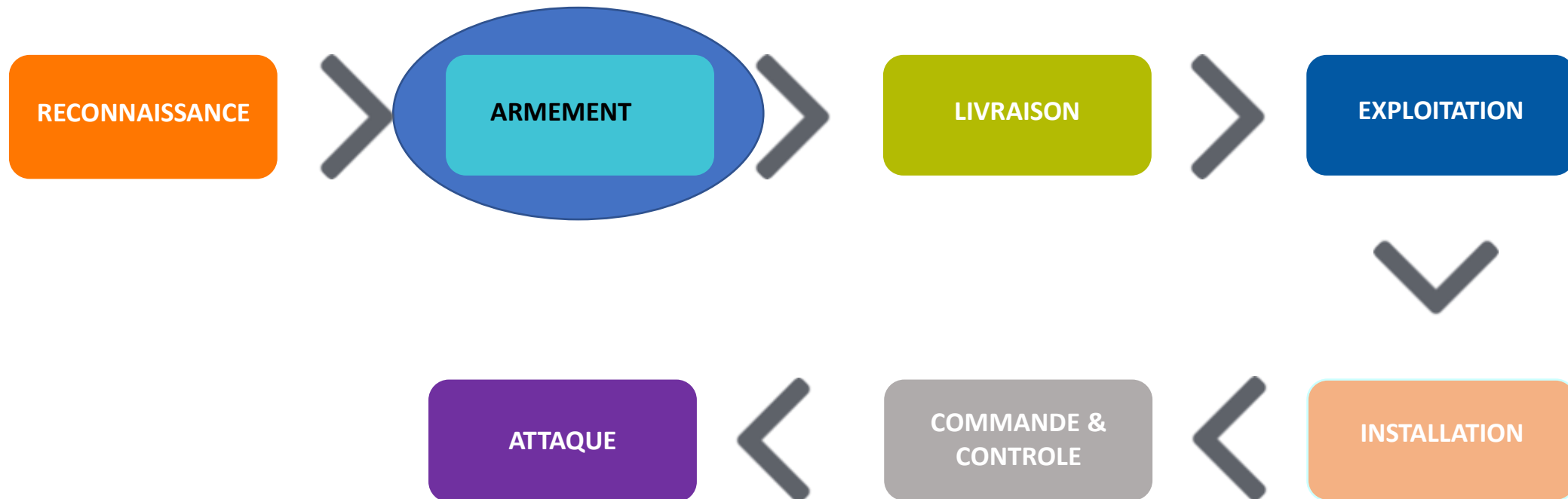


02 – Analyser le Kill Chain

Etapes du Kill Chain

Armement :

- Les informations obtenues de l'étapes précédentes vont permettre de créer un moyen pour infiltrer le système d'information de la victime.
- Pour cela, des logiciels malveillants ou malwares sont utilisés.



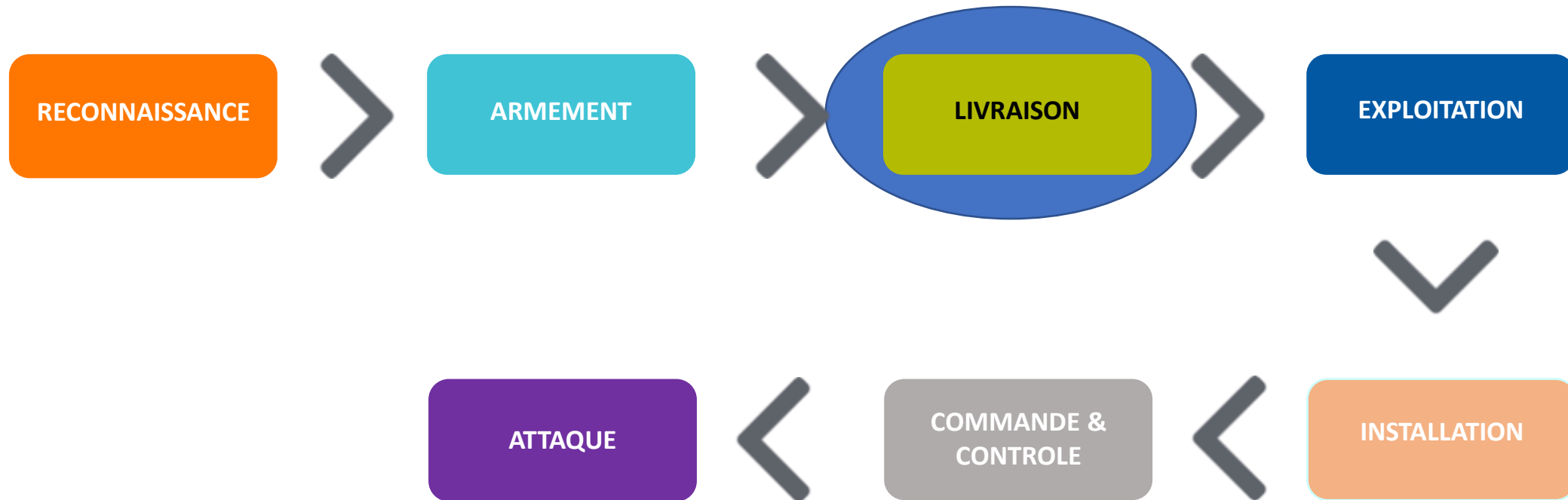
02 – Analyser le Kill Chain

Etapes du Kill Chain



Livraison :

- Dans cette étape, le pirate va livrer (l'arme) qui sera utilisée pour atteindre la cible,
- Par exemple le pirate peut envoyer un email en se faisant passer par la banque de l'utilisateur, cet email contient un lien qui redirige vers une page d'authentification factice. Le but est de collecter les vrais paramètres de l'authentification afin de les utiliser plus tard.
- Les autres moyens de livraison peuvent être l'utilisation d'une clé USB, compromettre un site web ou l'interaction des réseaux sociaux.



02 – Analyser le Kill Chain

Etapes du Kill Chain

Exploitation :

- L'objectif ici est d'exploiter une vulnérabilité afin d'accéder au système d'information de la victime.
- Pour cela plusieurs moyens peuvent être utilisés (faille 0 day, les vulnérabilités, l'ouverture d'une pièce jointe ou le fait de cliquer sur un lien malveillant).



02 – Analyser le Kill Chain

Etapes du Kill Chain



Installation :

- Un Cheval de Troie de porte dérobée ou d'accès à distance est installé par le logiciel malveillant qui permet à l'intrus d'accéder.
- C'est également une autre étape importante où l'attaque peut être stoppée à l'aide de systèmes tels que HIPS (Host-based Intrusion Prevention System).

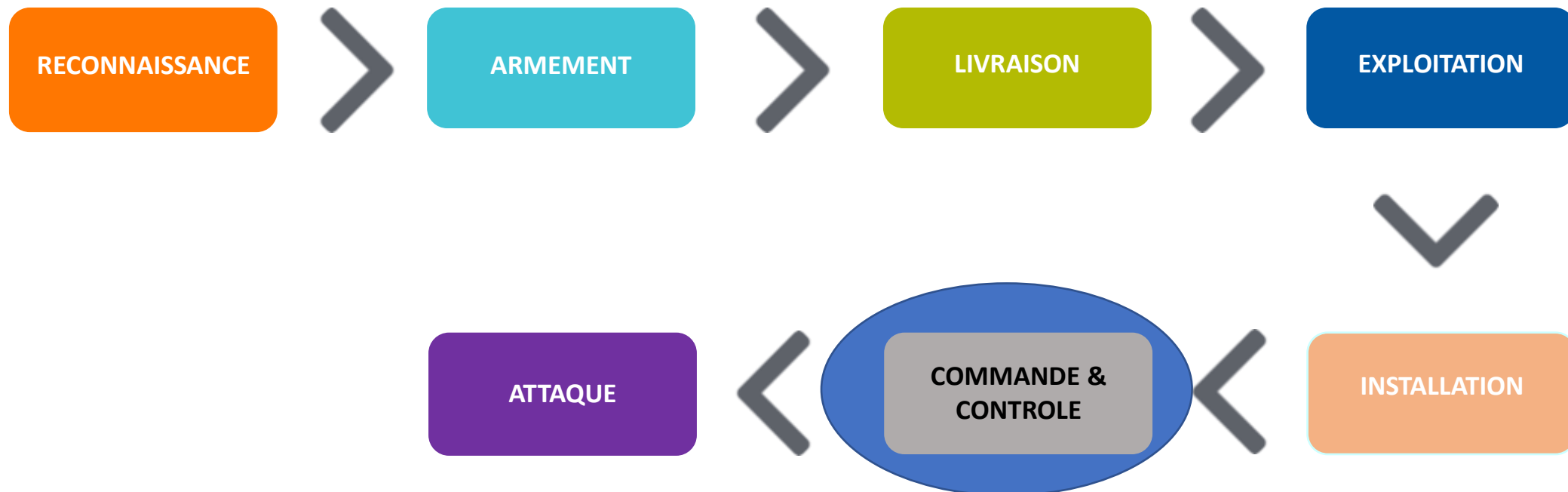


02 – Analyser le Kill Chain

Etapes du Kill Chain

Commande & Contrôle :

- Le logiciel malveillant installé précédemment ouvre un canal de communication vers le pirate informatique. Ce logiciel est à l'entrée, prêt à exécuter les commandes du pirate.
- Les canaux de communications généralement utilisés sont basés sur des protocoles WEB, DNS ou MAIL.



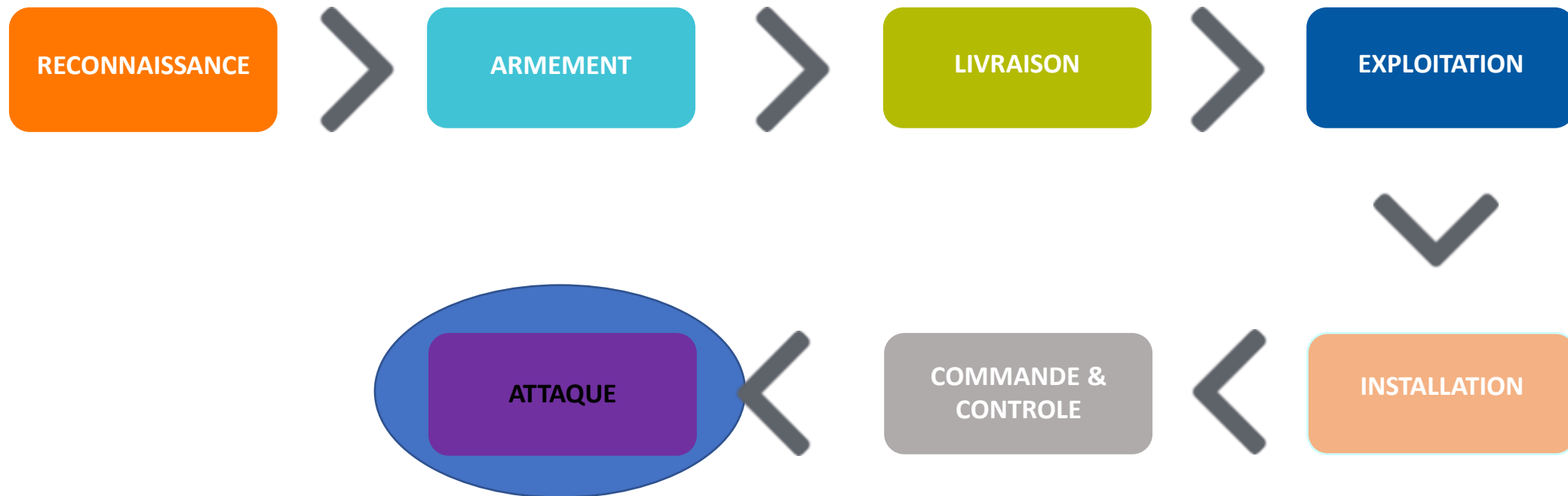
02 – Analyser le Kill Chain

Etapes du Kill Chain



Attaque :

- L'attaquant extrait finalement les données du système.
- L'objectif consiste à collecter, crypter et extraire des informations confidentielles de l'environnement de l'organisation.





PARTIE 2

Appliquer les procédures de gestion des incidents

Dans ce module, vous allez :

- Comprendre l'importance d'utiliser des procédures pour les processus de gestion des incidents
- Maîtriser les moyens pour gérer des incidents de sécurité de l'information



13 heures



CHAPITRE 1

Présenter le processus de gestion des incidents de sécurité

Ce que vous allez apprendre dans ce chapitre :

- Définir le modèle ISO 27035
- Détailler le processus de gestion des incidents



CHAPITRE 1

Présenter le processus de gestion des incidents de sécurité

1. **Modèle de la norme ISO 27035:2011**
2. Détails de chaque étape constituant le processus



01 – Présenter le processus de gestion des incidents de sécurité

Modèle de la norme ISO 27035:2011



Norme ISO 27035:2011

- **ISO/IEC 27035:2011** fournit une approche structurée et planifiée pour :
 1. Détecter, signaler et évaluer les incidents de sécurité de l'information.
 2. Répondre aux incidents de sécurité de l'information et les gérer.
 3. Détecter, évaluer et gérer les vulnérabilités de la sécurité de l'information.
 4. Améliorer en permanence la sécurité de l'information et la gestion des incidents grâce à la gestion des incidents et des vulnérabilités de la sécurité de l'information.
- **ISO/IEC 27035:2011** fournit des lignes directrices sur la gestion des incidents de sécurité de l'information pour les grandes et moyennes entreprises.
- Les organisations plus petites peuvent utiliser un ensemble de bases de documents, de processus et de routines décrits dans la présente norme internationale, en fonction de leur taille et du type d'activité par rapport à la situation de risque pour la sécurité de l'information.
- Il fournit également des conseils aux organisations externes fournissant des services de gestion des incidents de sécurité de l'information.

CHAPITRE 1

Présenter le processus de gestion des incidents de sécurité

1. Modèle de la norme ISO 27035:2011
2. **Détails de chaque étape constituant le processus**



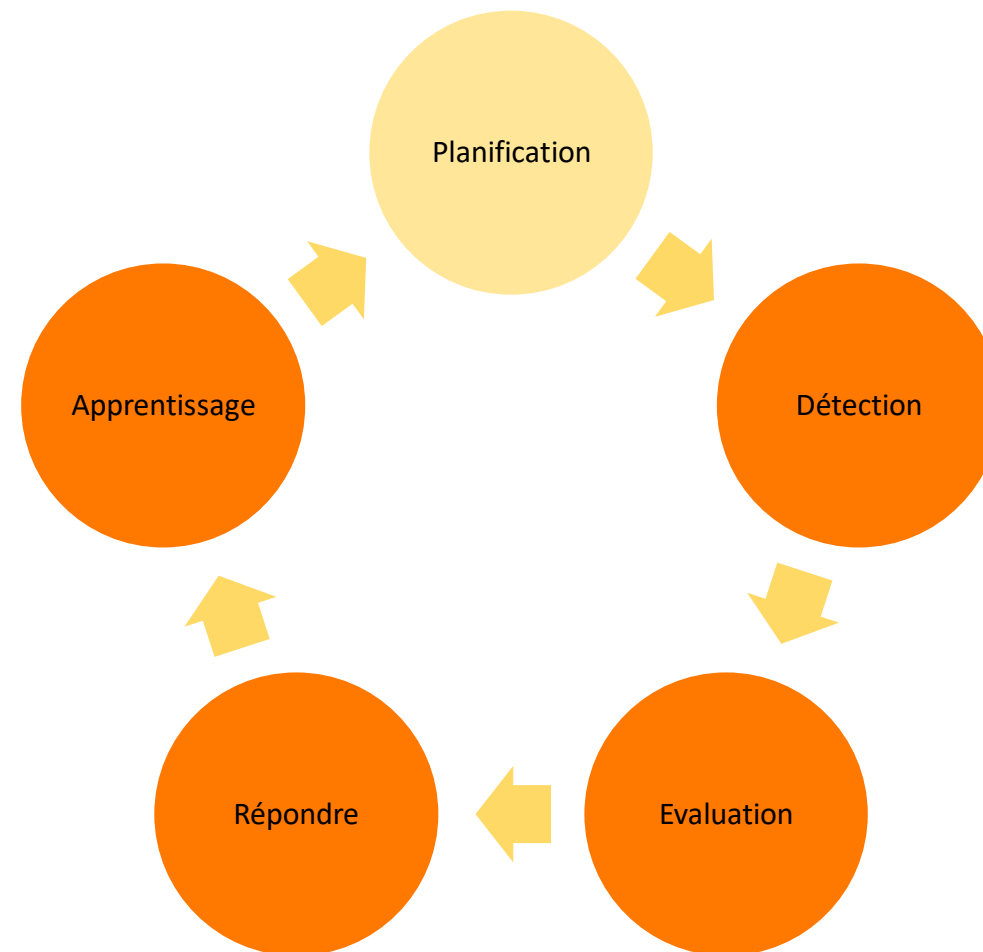
01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :



Planification

- La phase de planification est celle où l'organisation se prépare à détecter, gérer et récupérer des attaques et autres incidents. Il est nécessaire de disposer de plans documentés de gestion des incidents fondés sur une analyse des risques. Le niveau de risque déterminé par l'analyse des risques et les informations externes doit être communiqué à tous les employés concernés, et cela doit inclure des informations sur les incidents indésirables qui se sont produits dans le passé.
- La phase de planification et de préparation de la gestion des incidents de sécurité de l'information se concentre sur la documentation de la politique de signalement et de traitement des événements et des incidents de sécurité de l'information, ainsi que des procédures associées ; mettre en place la structure organisationnelle et le personnel appropriés pour la gestion des incidents ; et la mise en place d'un programme de sensibilisation et de formation.

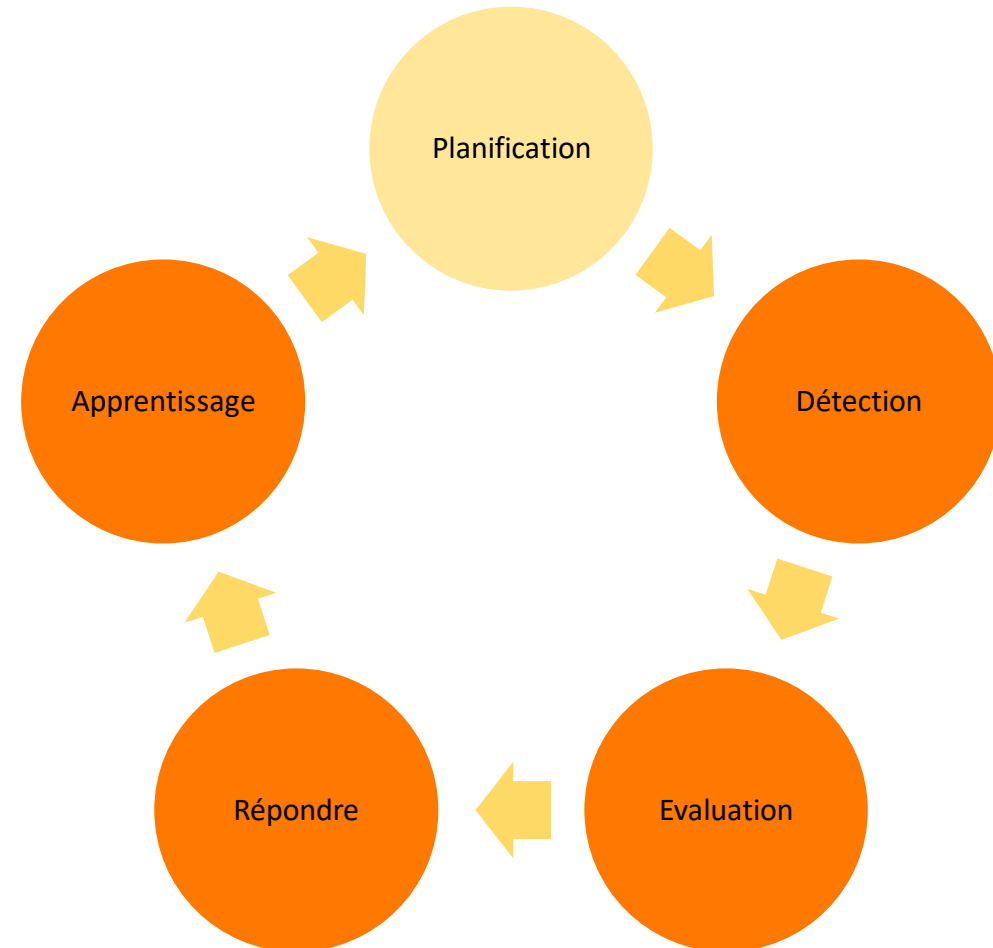


01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

Planification

- Le plan de gestion des incidents doit tenir compte des facteurs organisationnels et humains ainsi que des problèmes techniques, et doit être conçu pour faire face à la situation complexe avec les opérateurs et les multiples sous-traitants. Le plan devrait se concentrer sur :
 - ✓ Qui est responsable des différentes activités.
 - ✓ Quand et comment effectuer les différentes activités.
- Il est important de réaliser qu'il n'est pas possible de décrire tous les incidents possibles et de définir des procédures appropriées. Une capacité fondamentale est donc de former les opérateurs et de les familiariser avec les grands principes de la politique de sécurité. Cela garantit que les décisions sont prises et alignées sur ces objectifs, même lorsque des incidents imprévus se produisent et nécessitent l'application et l'affinement des plans et des rôles.

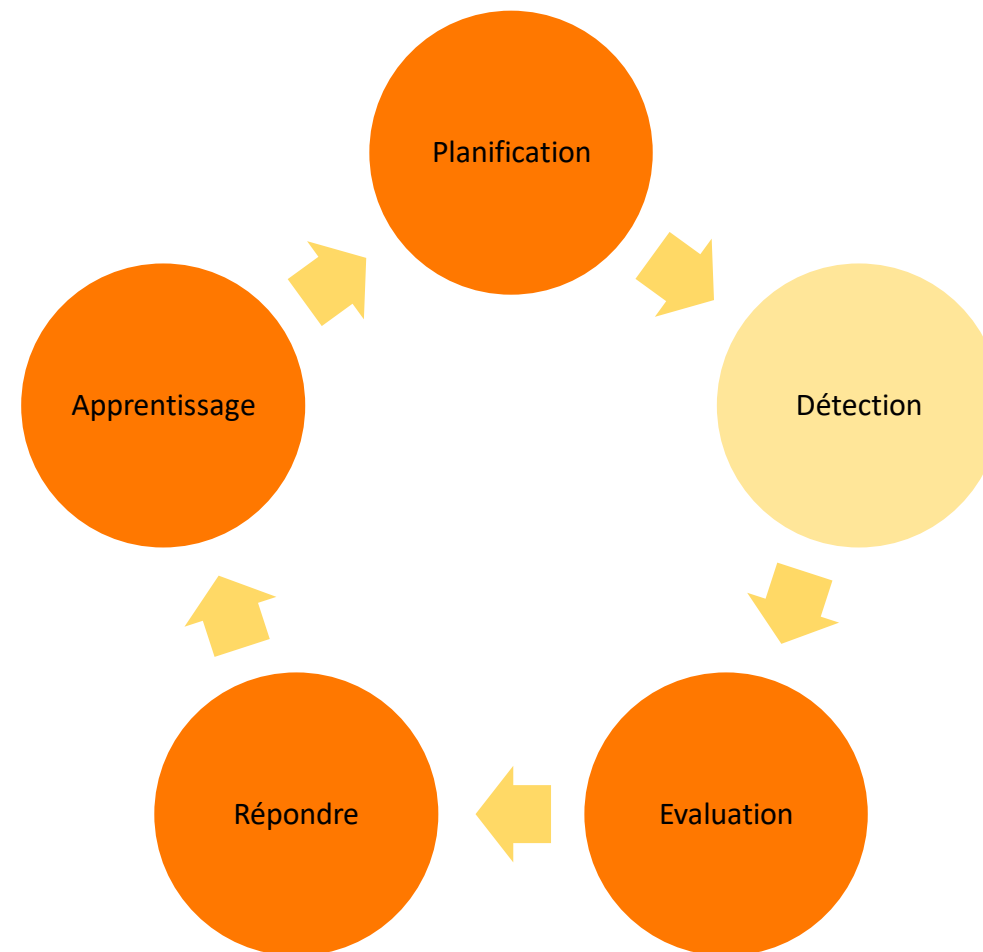


01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

Détection

- Lorsque des incidents surviennent, il est important d'être préparé et d'avoir un plan pour détecter et gérer l'incident. Il est recommandé de créer un plan de réponse aux incidents, qui se compose de trois parties principales :
 1. Un plan sur ce qu'il faut faire en cas de détection ou de suspicion d'un incident : ce plan s'adresse à tous les employés, y compris les sous-traitants et les fournisseurs. Il doit être facilement disponible (par exemple, intranet, affiches) et facile à comprendre. Ce qui signifie qu'il doit être court, précis et suivre une terminologie et des perceptions communes.
 2. Un plan de détection des incidents à l'aide d'outils, de routines et de partage d'informations : ce plan s'adresse aux responsables du travail sur la sécurité.
 3. Un plan détaillé de réponse aux différents types d'incidents : ce plan s'adresse aux responsables de la reprise après incident.



01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

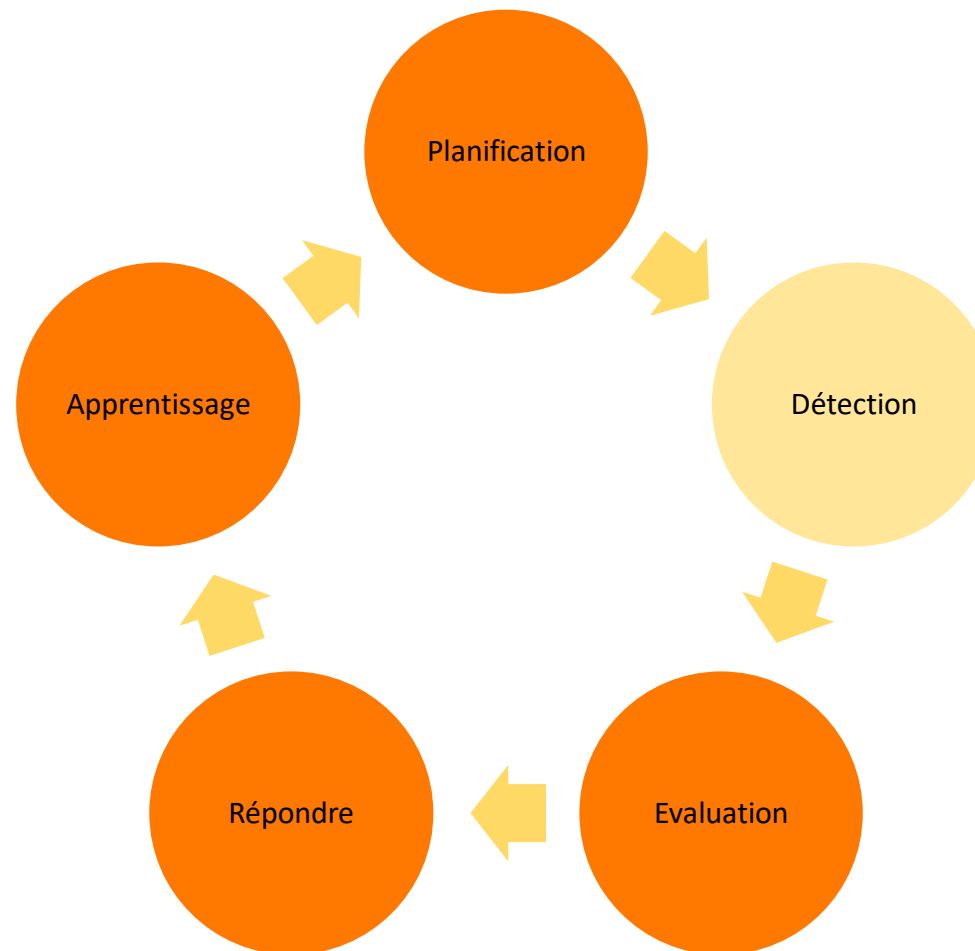


Détection

Un aspect critique de la phase de détection est l'identification de l'incident et le niveau de réponse approprié.

Cela comprend le lancement de procédures (par exemple, alerter le personnel/les collègues, informer les responsables ou les autorités compétentes) ainsi que le lancement d'actions répétées ou préparées (par exemple, la désactivation des nœuds de traitement).

Bien que ce dernier soit affiné dans la phase suivante, il est inhérent de reconnaître qu'une réponse précoce est étroitement liée à une détection réussie.



01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

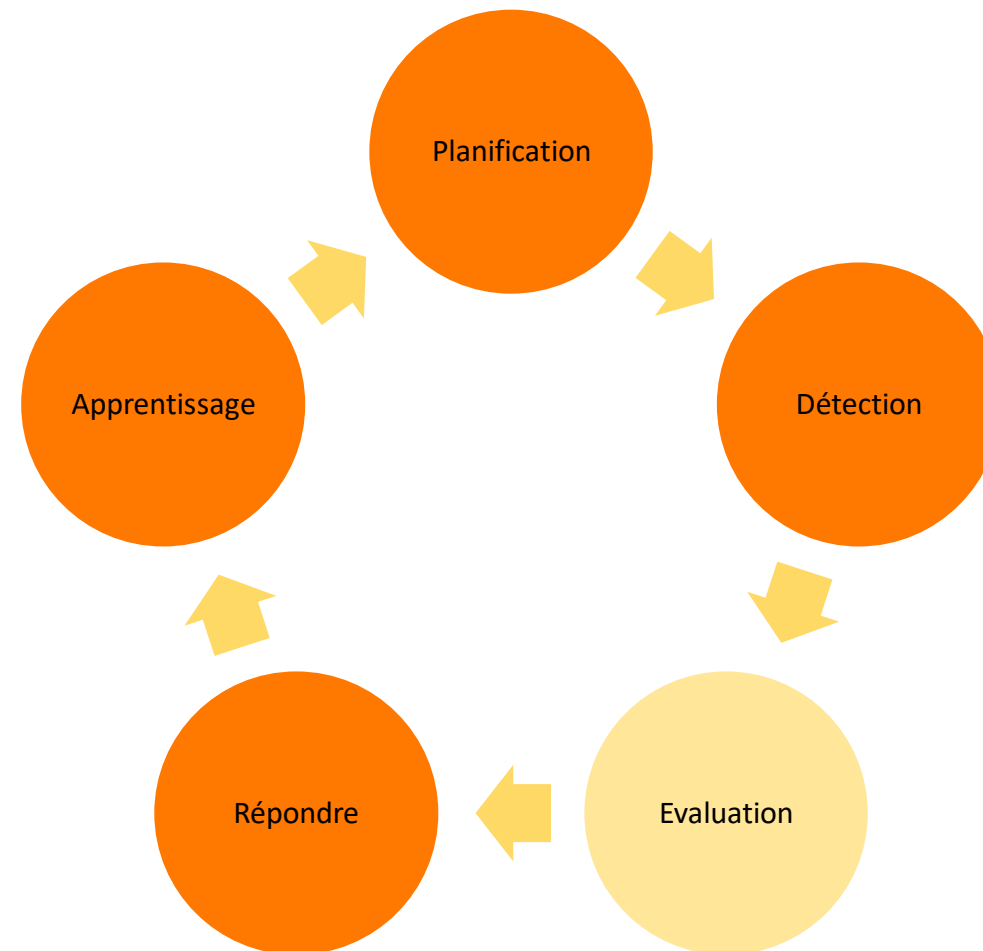
Evaluation

Lorsque l'alerte d'incident parvient à une personne responsable de la gestion de l'incident, ce dernier doit être évalué pour déterminer la gravité de l'incident et la voie à suivre.

Conceptuellement, la phase d'évaluation vise à identifier positivement un incident. Comme mentionné ci-dessus. La phase de détection fournit les preuves sur lesquelles maintenant - pendant la phase d'évaluation - une évaluation appropriée doit être faite. En principe, la phase d'évaluation vise à :

- Déterminer si l'événement est un incident de sécurité réel ou une fausse alerte
- Catégoriser l'incident identifié – par exemple – comme mineur ou majeur
- Déclencher les procédures de réponse respectives compte tenu de la catégorisation.

La phase d'évaluation peut être globalement décrite comme un processus de confirmation d'incident et de sélection de plan. De ce point de vue, la phase d'évaluation est une étape critique dans la réponse opportune et ciblée à un incident. Compte tenu de l'évaluation, des ressources et des procédures sont initiées et qui pourraient elles-mêmes nécessiter des ressources. Il est donc important de fournir des lignes directrices et des modèles de décision clairs pour cette phase. L'évaluation erronée ou l'initiation d'un mauvais plan peut finalement nécessiter de longues mesures de correction.

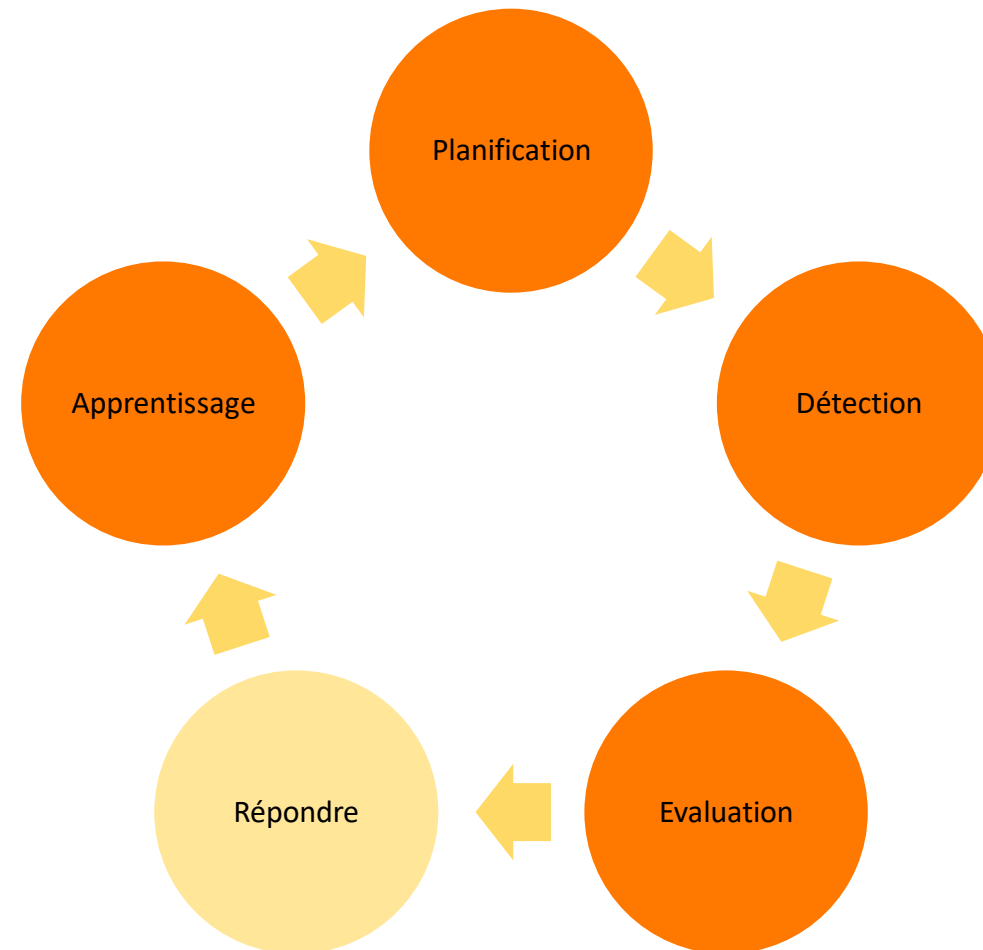


01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

Répondre

- Afin de se remettre avec succès et efficacement d'un incident, il est important d'être bien préparé, ce qui signifie qu'un plan et les compétences nécessaires sont en place. C'est là qu'un travail minutieux dans la phase Plan sera payant. Les facteurs importants sont :
 - Responsabilités claires - répartir la responsabilité des activités de gestion des incidents à travers une hiérarchie appropriée du personnel, avec une prise de décision d'évaluation et des actions impliquant à la fois le personnel de sécurité et de non-sécurité.
 - Procédures claires - fournir des procédures formelles à suivre par chaque personne notifiée, y compris l'examen et la modification du rapport effectué, l'évaluation des dommages et la notification au personnel concerné (avec les actions individuelles en fonction du type et de la gravité de l'incident) ».

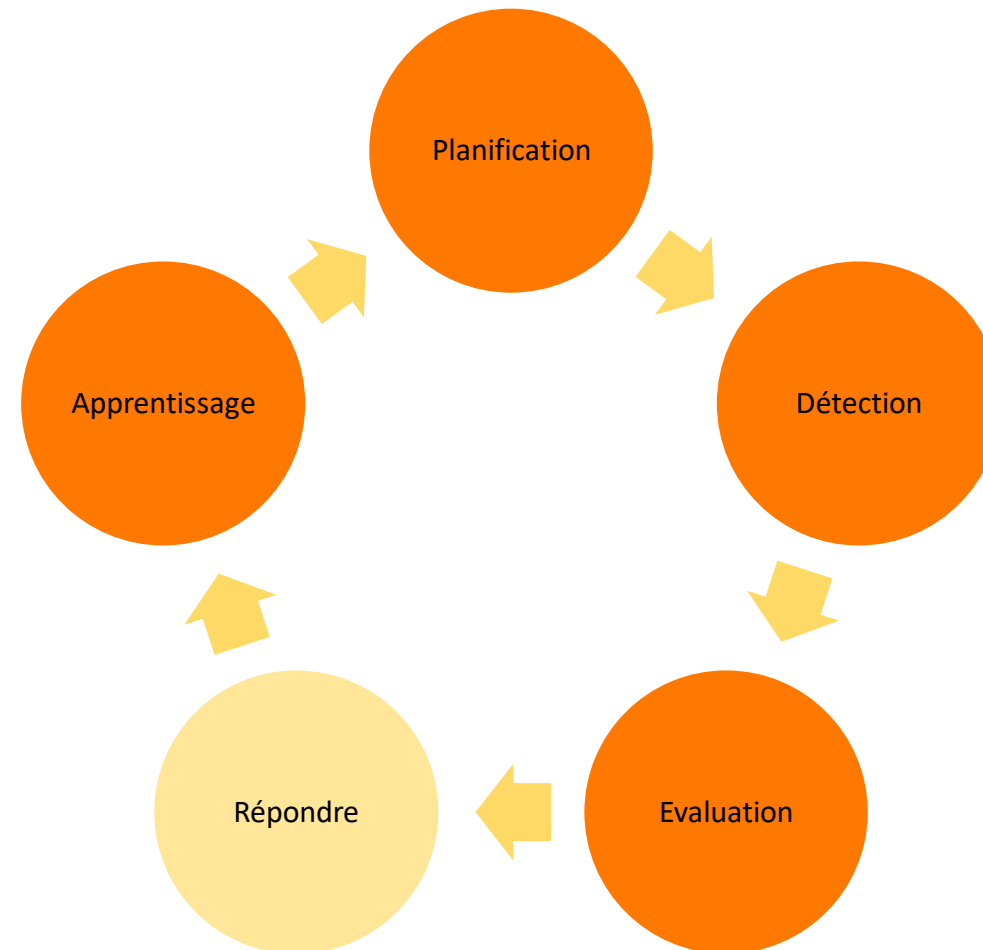


01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :

Répondre

- Lorsqu'un incident est maîtrisé, il convient d'identifier les réponses supplémentaires nécessaires pour ramener le système à un fonctionnement normal. C'est le moment de restaurer les systèmes, de s'assurer qu'ils sont dans un état sûr, de se reconnecter aux réseaux externes, etc. Dans ce processus, il sera souvent nécessaire de :
 - Prendre des mesures immédiates pour réduire la vulnérabilité du système : installer les correctifs nécessaires ou améliorer la configuration du système en modifiant les mots de passe ou en désactivant les services inutilisés.
 - Utiliser des outils : supports d'installation, outils de sauvegarde et de récupération, et éventuellement aussi outils de contrôle d'intégrité et d'investigation.
 - Etre conscient du code malveillant : les Chevaux de Troie, les rootkits et les modules du noyau peuvent être placés de manière malveillante dans le système actuel et sont difficiles à détecter.



01 – Présenter le processus de gestion des incidents de sécurité

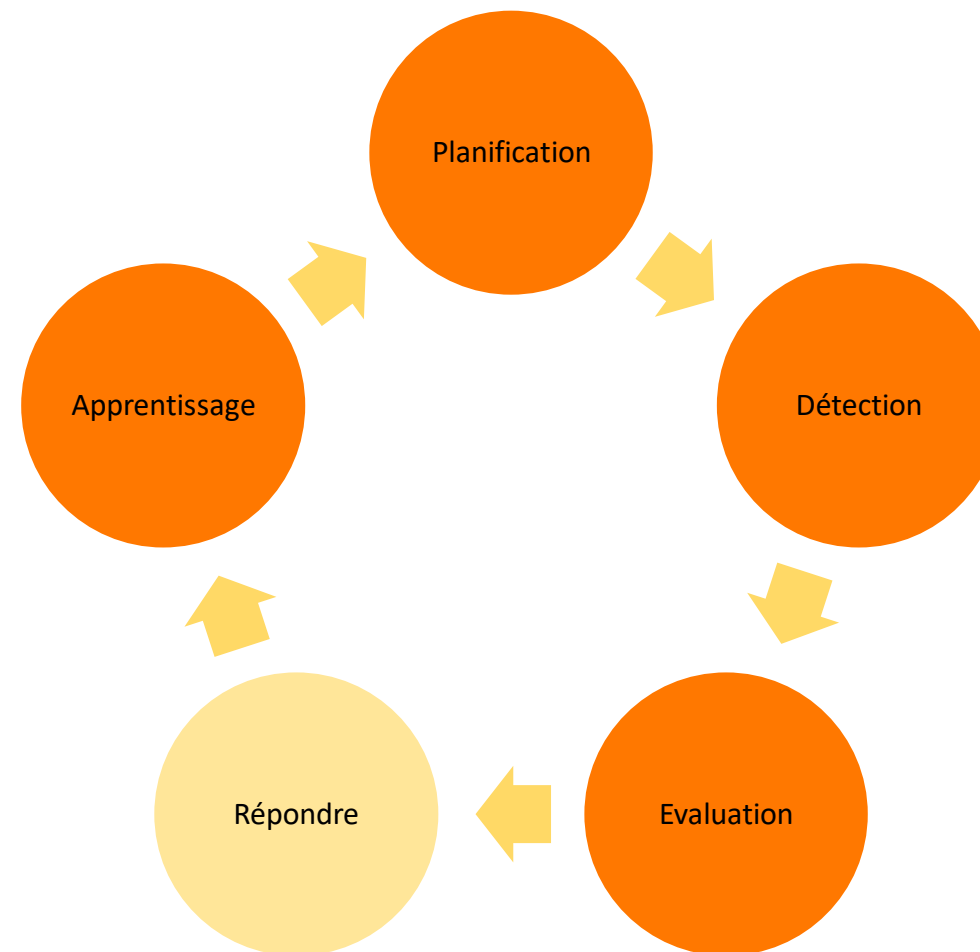
Détails de chaque étape constituant le processus :



Répondre

Exemple

- On considère souvent que la perte de certaines données vaut mieux qu'un système (encore) non sécurisé. Dans un environnement ATM (guichet automatique), il est cependant, important d'équilibrer le besoin d'une sécurité améliorée et la nécessité de maintenir le système opérationnel. Concrètement, on ne peut pas redémarrer un avion dans les airs. Il est donc important que les représentants des acteurs informatiques et ATM (contrôleurs aériens, etc.) soient impliqués dans les décisions qui entraîneront un arrêt du système ou qui pourraient rendre le système instable.
- Lorsque tout est opérationnel et que l'incident est traité, il est important d'utiliser les expériences faites comme une opportunité d'amélioration. La documentation créée lors de la détection et de la récupération de l'incident et les expériences des personnes impliquées dans la gestion de l'incident peuvent être utilisées pour améliorer la préparation de l'organisation à prévenir et à gérer les incidents à l'avenir. C'est l'objet de la phase d'apprentissage. Les activités de la phase d'apprentissage doivent être lancées lorsque l'incident est encore frais dans l'esprit des gens. Mais d'abord, fournir des informations d'état à la personne qui a déclenché une alerte concernant l'incident. Il s'agit d'une partie importante du travail de sensibilisation en matière de gestion des incidents.



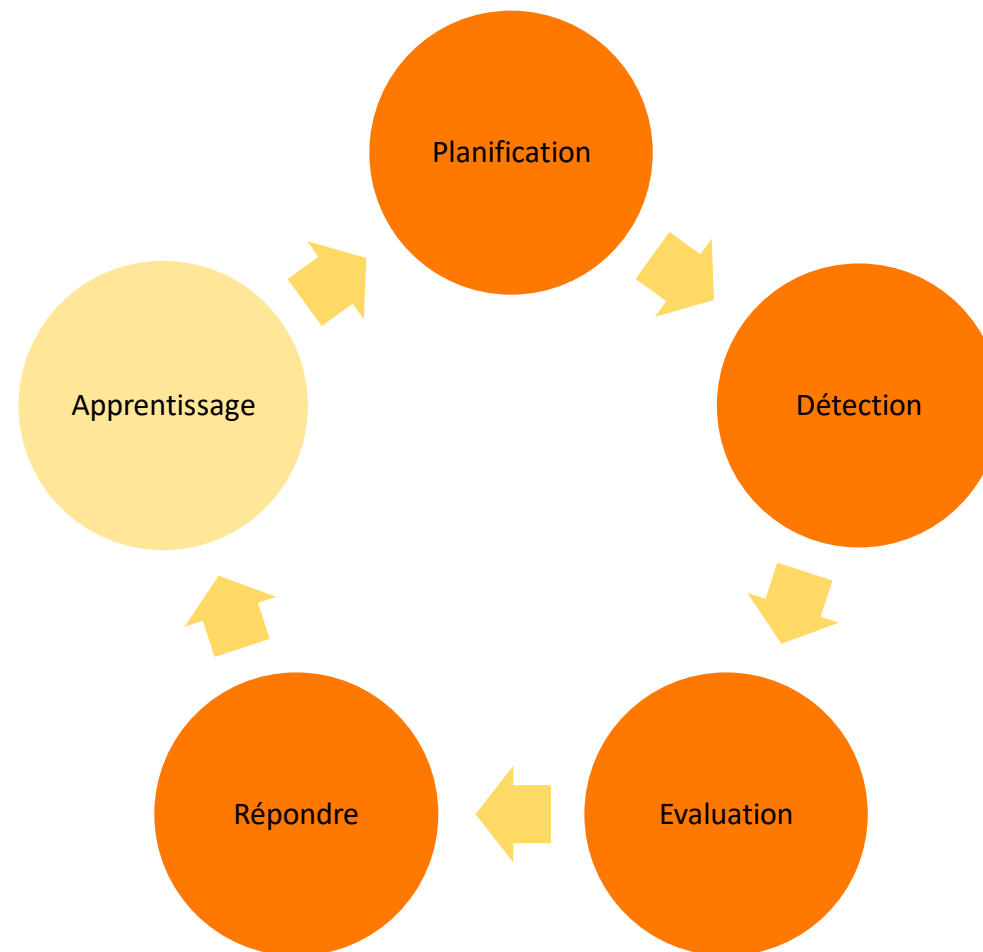
01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :



Apprentissage

- Cette phase couvre le processus d'apprentissage qui suit un incident qui s'est produit.
- L'apprentissage proactif lié à l'anticipation (savoir à quoi s'attendre) est traité dans la phase de planification.
- Les incidents doivent être utilisés comme une opportunité d'apprentissage et d'amélioration.
- Apprendre des incidents devrait être une partie planifiée de la gestion des incidents, et les ressources nécessaires doivent être allouées.
- Le processus d'apprentissage est axé sur l'apprentissage organisationnel.
- L'objectif est de modifier la réponse à l'incident en fonction de la différence entre le résultat attendu et obtenu (apprentissage en boucle unique). De pouvoir, en plus, remettre en question et modifier les variables gouvernantes liées à la technologie, à l'organisation et aux facteurs humains qui conduisent au résultat (apprentissage en double boucle).



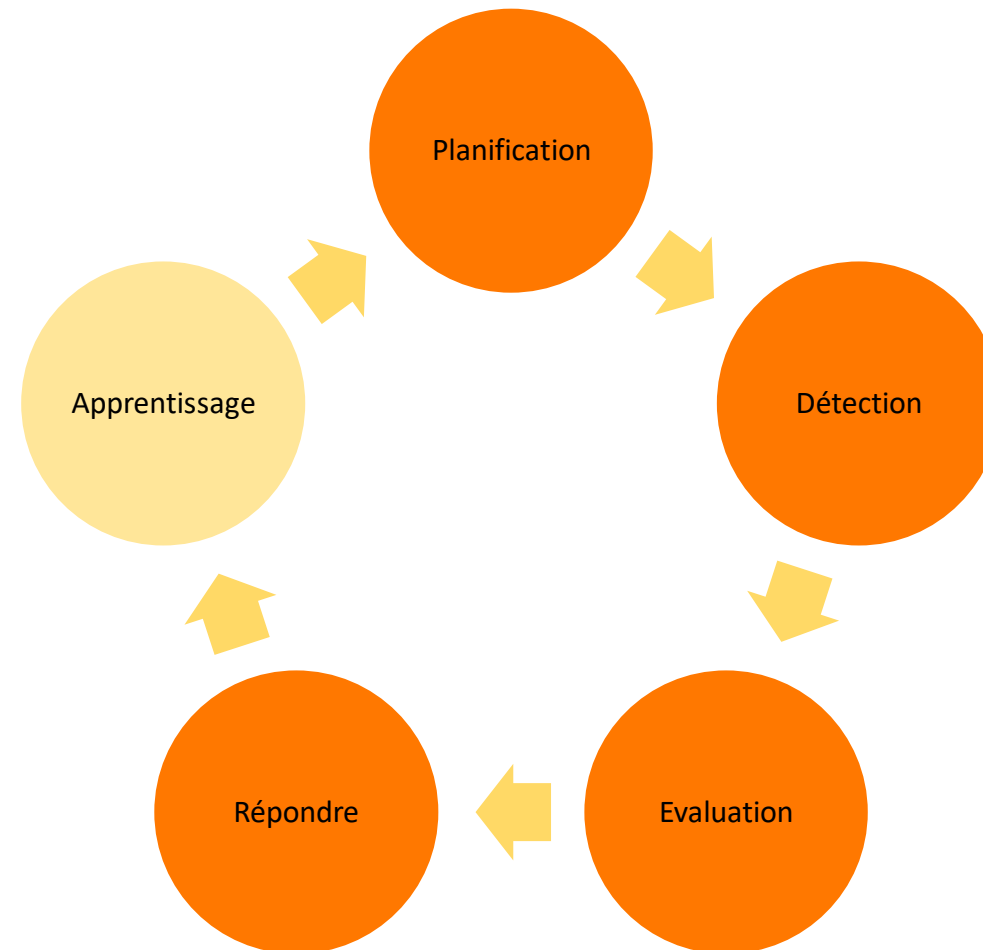
01 – Présenter le processus de gestion des incidents de sécurité

Détails de chaque étape constituant le processus :



Apprentissage

- L'accent est mis sur ce qui a conduit à l'incident, ce qui s'est passé, comment ce dernier a été géré, et de comprendre comment il s'est produit en analysant les obstacles. Enfin proposer les améliorations à l'aide d'une analyse après l'incident.
- Afin d'être en mesure de réussir avec l'apprentissage organisationnel, l'organisation doit être préparée à l'apprentissage. La direction doit décider des ressources à utiliser. La question clé est l'étendue de l'engagement de la direction envers l'apprentissage et la volonté d'utiliser les ressources pour apprendre de ce type d'incidents. Pour chaque incident, il convient de déterminer dans quelle mesure on est capable et désireux d'apprendre de cet incident. Ceci est fortement lié à la gravité de l'incident et déterminera la quantité de ressources qui seront utilisées pour apprendre de l'incident.





CHAPITRE 2

Appliquer les procédures 800-61 R2 du NIST

Ce que vous allez apprendre dans ce chapitre :

- Etablir des capacités de réponse aux incidents de sécurité informatique
- Gérer les incidents de manière efficace et efficiente



6 heures

CHAPITRE 2

Appliquer les procédures 800-61 R2 du NIST

1. **Présentation des quatre phases du processus**
2. Focus sur la partie communication



02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



800-61 R2 du NIST :

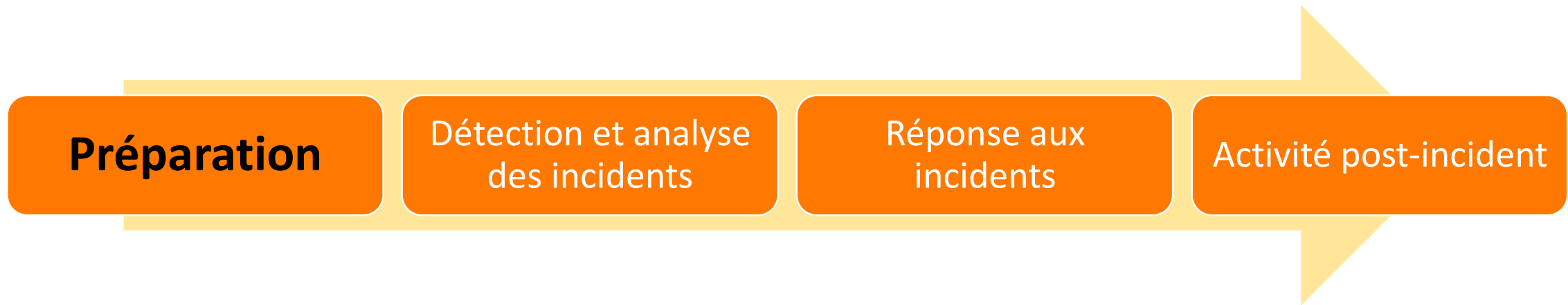
- Dans le "**Computer Security Incident Handling Guide**", également connu sous le nom de **SP 800-61 Rev. 2**, le National Institute of Standards and Technology, généralement connu sous le nom de **NIST**, fournit ses directives de gestion et de réponse aux incidents de cybersécurité.
- Avec la complexité et la fréquence croissante des cyberattaques, des attaques de ransomware et des violations de données dans le monde, la réponse aux incidents de sécurité informatique est devenue une activité d'entreprise essentielle. En conséquence, il est désormais important d'aborder la cybersécurité sous l'angle de la réponse et de la récupération plutôt que de la prévention.
- Le guide de traitement des incidents de cybersécurité du **NIST** vise à aider les organisations, à améliorer leur posture de sécurité et leurs capacités de réponse aux incidents grâce à une planification, une formation à la cybersécurité et une allocation de ressources appropriées.
- Selon le NIST, les principales étapes du processus de réponse aux incidents de cybersécurité sont les suivantes :

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Préparation



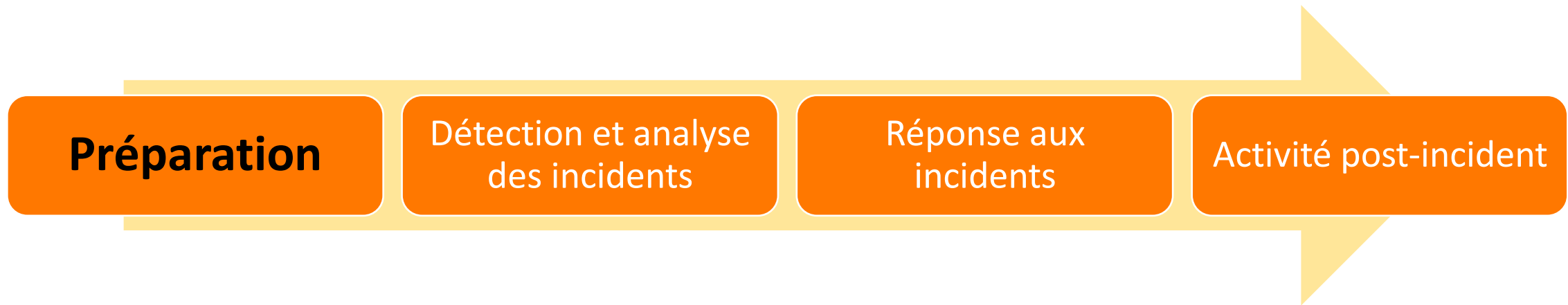
- Dans la phase de préparation, l'organisation doit être prête à minimiser les impacts des incidents de sécurité et à maintenir la continuité des activités (Taylor 2013).
- Le degré de proactivité dans cette phase doit être élevé pour s'assurer que les événements imprévus ou les événements de cygne noir (c'est-à-dire les événements dus à des causes inattendues et hautement imprévisibles) sont bien préparés.
- La gestion de la sécurité de l'information (SI) (par exemple, la culture du SI, la formation, la conformité aux politiques) est une approche populaire dans la préparation pré-incident, qui comprend l'établissement de politiques de sécurité d'entreprise et des mises à jour régulières, le processus de notification des incidents, le développement d'une politique de confinement des incidents, la création des listes de contrôle pour la gestion des incidents, un programme de formation du personnel et l'assurance que le processus d'évaluation des risques de sécurité fonctionne et est actif (Johnson 2014).

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Préparation



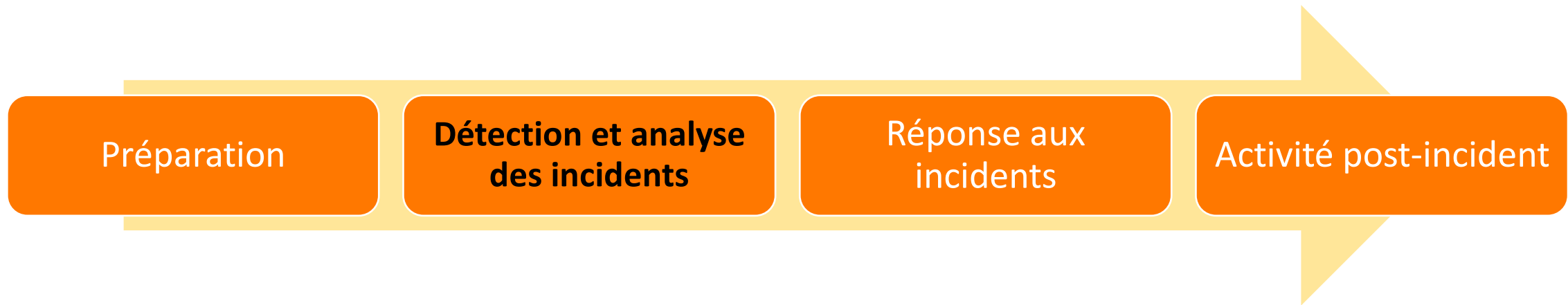
- D'un point de vue technologique, il est crucial d'aborder le contrôle de sécurité logique. Cela comprend, par exemple, la mise en place d'un pare-feu, la protection contre les logiciels malveillants, l'évaluation des vulnérabilités, la surveillance du réseau et la protection de la sécurité des données (comme le système de cryptage, le système d'authentification).
- Un exemple de technologie récente est la gestion des informations et des événements de sécurité (SIEM), qui fournit une surveillance en temps réel et un historique des événements de sécurité capturés par le réseau, le système et les appareils (Anuar et al. 2010).
- La sécurité physique et environnementale complète la protection logique.
- Un autre élément clé de la phase de préparation est la mise en place d'une équipe de réponse aux incidents de sécurité informatique (CSIRT) chargée de déterminer ce qui s'est passé, les actions à entreprendre.

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Détection et analyse des incidents



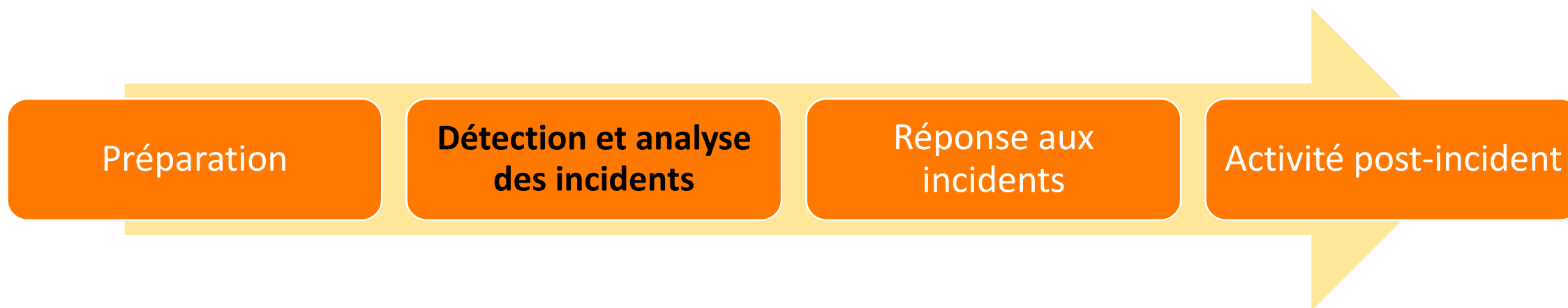
- La préparation vise à minimiser le risque d'incident, mais tous les incidents ne peuvent pas être évités.
- Il est donc nécessaire de détecter et d'analyser rapidement une occurrence d'incident. Le degré de proactivité passe progressivement d'Élevé à Moyen, en fonction de processus particuliers.
- La phase de détection commence dès qu'un événement suspect ou inhabituel est détecté et signalé.
- Certains exemples incluent un nom de fichier inconnu, de nouveaux fichiers inexplicables, un nombre excessif de tentatives de connexion infructueuses et des entrées suspectes dans le compte système du réseau.
- La détection peut provenir d'un outil automatisé (par exemple, un système de détection d'intrusion) et signalée manuellement par des personnes (utilisateurs et employés). Pour organiser systématiquement le flux des rapports, un modèle de rapport d'incident doit être établi dans une organisation.

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Détection et analyse des incidents



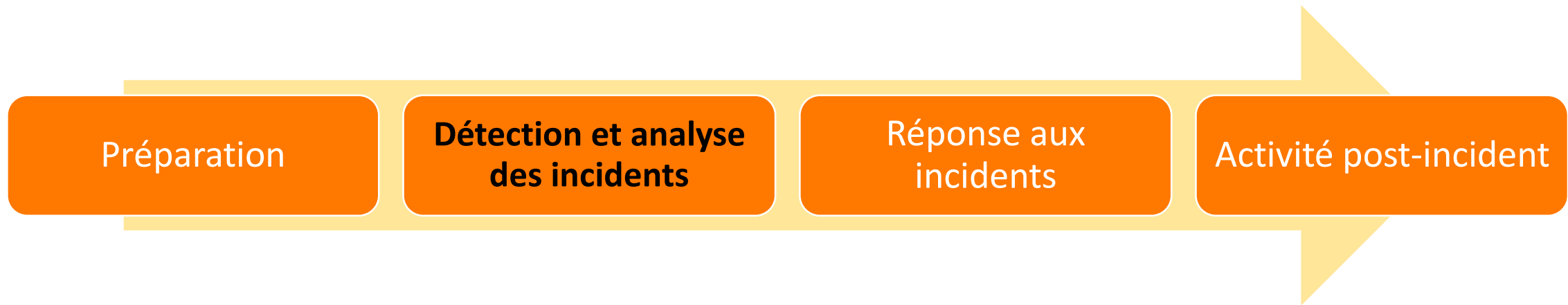
- Une analyse des incidents est ensuite effectuée pour déterminer la validité du rapport (probablement une fausse alerte) ; et le(s) impact(s) potentiel(s) sur les principaux services et actifs de l'organisation. La gestion des risques (y compris l'évaluation des risques et l'atténuation) est la clé pour estimer les dommages que de tels impacts peuvent avoir sur une organisation. De plus, les résultats de l'évaluation des risques sont nécessaires pour déterminer la priorité des incidents (si plusieurs incidents se produisent simultanément).

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus

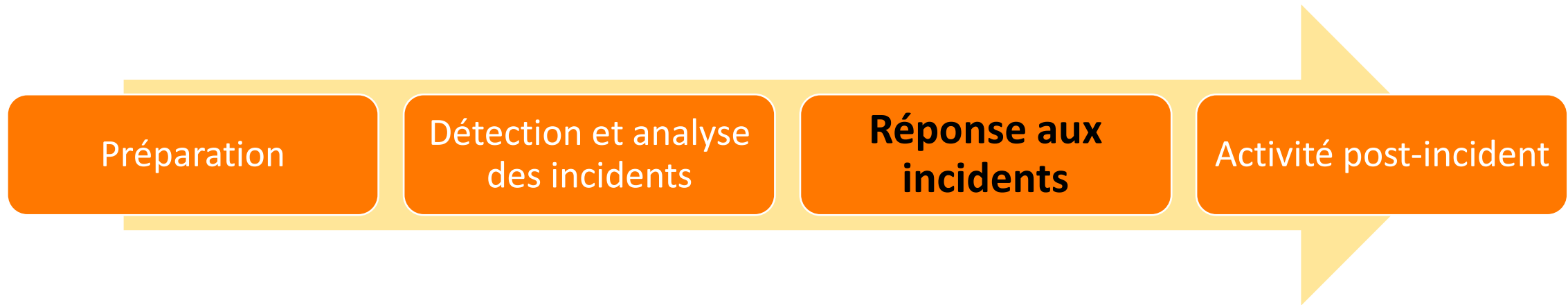


Détection et analyse des incidents



- Étapes du processus :
 - Un événement lié à la sécurité de l'information est identifié et attribué à un gestionnaire d'incidents pour la gestion
 - Le gestionnaire d'incidents effectuera l'analyse de l'incident pour déterminer si un incident de sécurité s'est produit ou non
 - Le gestionnaire d'incidents effectuera une analyse des risques de l'incident conformément au cadre de gestion des risques
 - Le gestionnaire d'incidents détermine la catégorisation et la hiérarchisation des incidents, ainsi que les niveaux de service qui en résultent
 - Pour les incidents majeurs ou significatifs, le dossier est confié au coordinateur de la continuité des services informatiques pour la gestion, conformément au guide de gestion des incidents critiques des STI
 - Les incidents impliquant des violations d'informations personnellement identifiables (PII) ou d'informations de santé protégées (PHI) doivent être signalés au CIO pour renvoi au Bureau de la confidentialité

Réponse aux incidents



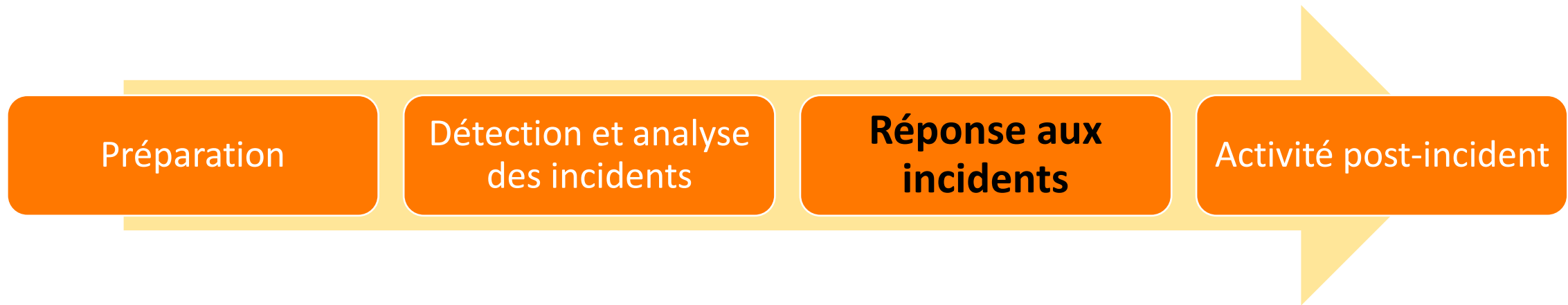
- Cette phase commence une fois que l'événement suspect a été classé comme incident confirmé. Elle consiste à identifier les actions d'intervention immédiate pour faire face à l'incident de sécurité de l'information et, le cas échéant, à informer l'équipe appropriée des actions requises. L'objectif principal est de limiter tout impact négatif sur les opérations, de suivre l'éradication de la menace et du retour des services et systèmes TIC à leur état normal.
- Le gestionnaire d'incidents doit gérer cette phase. Les étapes de confinement, d'éradication et de récupération des incidents peuvent varier en fonction du type d'incident. La responsabilité de la réponse aux incidents peut être répartie entre plusieurs équipes qui seront gérées et coordonnées par le gestionnaire d'incidents.
- Les gestionnaires d'incidents auront besoin d'une expertise en matière d'enquête pour gérer efficacement la réponse à l'incident, ou doivent avoir accès ou avoir des accords avec des tiers ayant les compétences appropriées pour mener des enquêtes.

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Réponse aux incidents

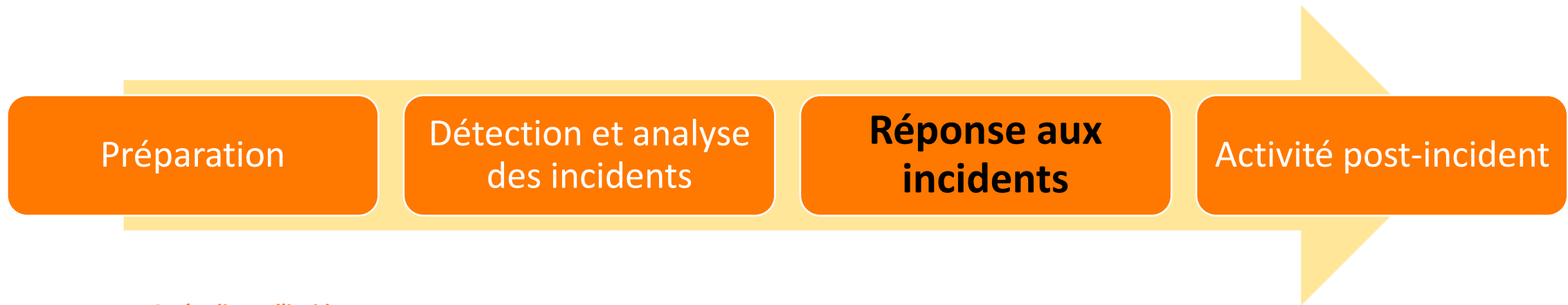


Une combinaison appropriée des actions suivantes doit être utilisée pour terminer cette phase :

1 - Confinement initial de l'incident :

- ✓ Acquérir, conserver, sécuriser et documenter les preuves
- ✓ Confirmer le confinement de l'incident
- ✓ Analyser davantage l'incident et déterminer si le confinement a réussi
- ✓ Mettre en œuvre des mesures de confinement supplémentaires, si nécessaire

Réponse aux incidents



2 - éradiquer l'incident :

- ✓ Identifier et atténuer toutes les vulnérabilités qui ont été exploitées
- ✓ Le gestionnaire d'incidents peut se charger des activités nécessaires pour résoudre le problème et restaurera les services concernés à leur état normal. Si un soutien externe a été demandé, les organismes externes seront également impliqués dans la résolution du problème
- ✓ Supprimer les composants des systèmes à l'origine de l'incident

3 - Récupérer de l'incident :

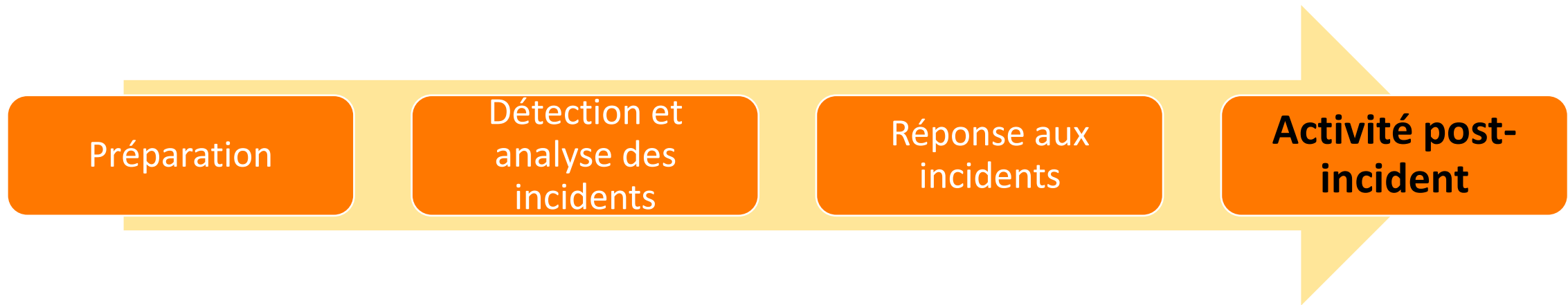
- ✓ Remettre les systèmes et services concernés dans un état prêt à fonctionner
- ✓ Confirmer que les systèmes et services concernés fonctionnent normalement

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Activité post-incident



Cette phase a lieu une fois que l'incident de sécurité de l'information a été résolu ou clôturé.

Compiler un résumé des actions et des résultats

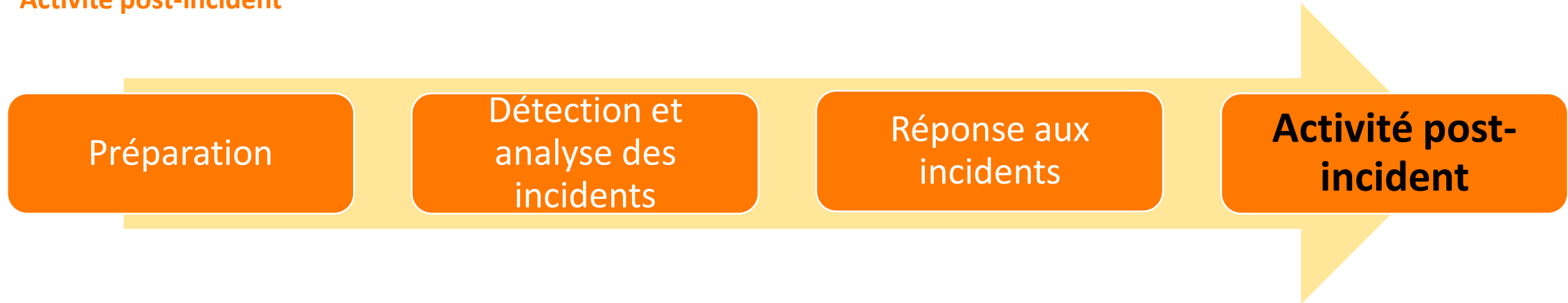
- ✓ Le ou les gestionnaires d'incidents doivent documenter les actions prises au cours du processus. Si l'incident impliquait l'assistance de parties externes telles que AusCERT, CERT Australia ou des consultants en sécurité sous contrat, leurs étapes et leurs rapports doivent également être documentés par le gestionnaire d'incidents.
- ✓ Le gestionnaire d'incidents rassemblera les détails et préparera le rapport de clôture.

02 – Appliquer les procédures 800-61 R2 du NIST

Présentation des quatre phases du processus



Activité post-incident



Le gestionnaire d'incidents est responsable de documenter un rapport de clôture d'incident qui contient (au minimum) les informations suivantes :

- ✓ Résumé de l'incident
- ✓ Acteurs de l'incident
- ✓ Gestionnaires d'incidents
- ✓ Description détaillée de l'incident
- ✓ Preuves pertinentes
- ✓ Détails techniques
- ✓ Actions d'éradication
- ✓ Conclusion
- ✓ Leçons apprises

CHAPITRE 2

Appliquer les procédures 800-61 R2 du NIST

1. Présentation des quatre phases du processus
2. **Focus sur la partie communication**

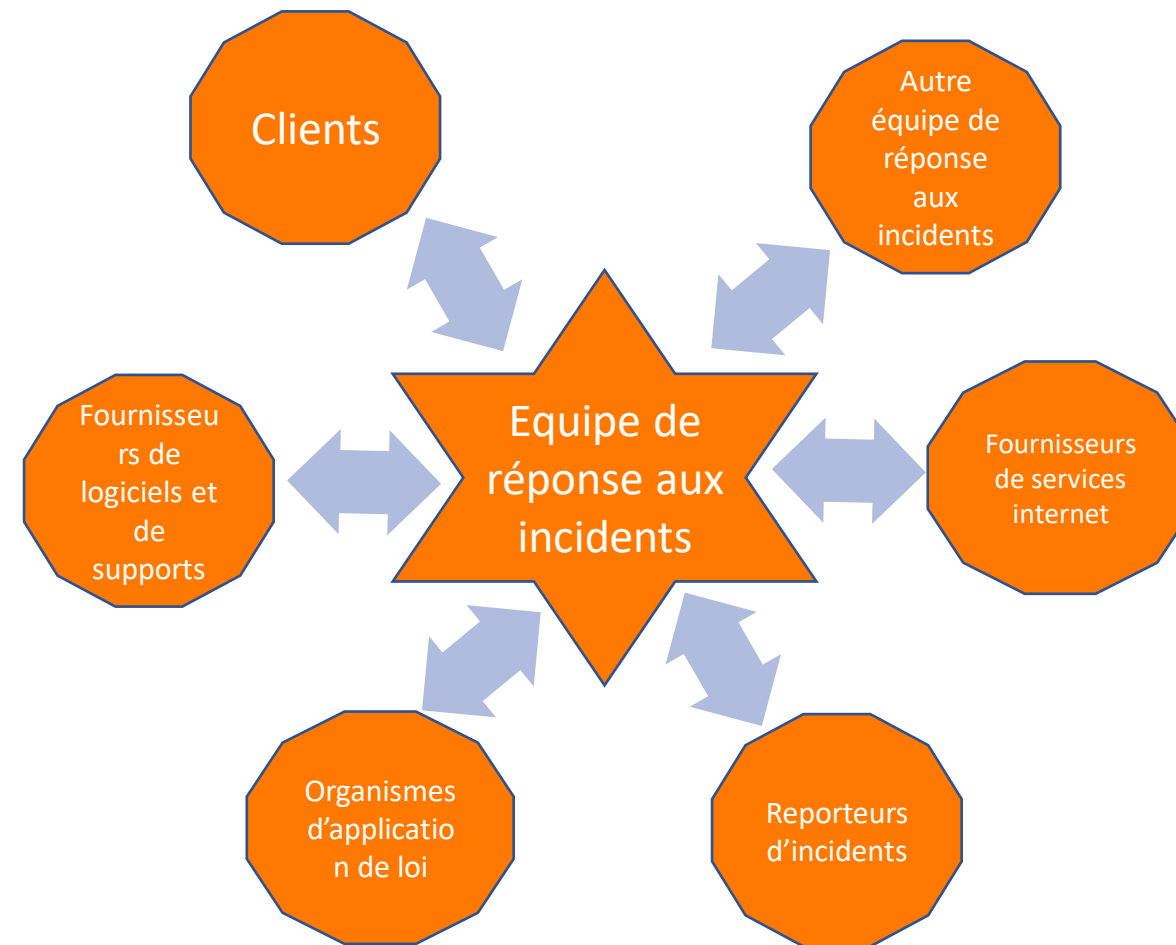


Focus sur la partie communication

- Les organisations ont souvent besoin de communiquer avec des tiers concernant un incident. Elles doivent le faire chaque fois que cela est approprié, par exemple en contactant les forces de l'ordre et en répondant aux demandes des médias.
- Un autre exemple consiste à discuter des incidents avec d'autres parties impliquées, tels que les fournisseurs de services Internet (FAI), le fournisseur de logiciels vulnérables ou d'autres équipes de réponse aux incidents. En cas d'incident, l'équipe d'intervention doit discuter longuement du partage d'informations avec le bureau des affaires publiques, le service juridique et la direction de l'organisation avant qu'un incident ne se produise afin d'établir des politiques et des procédures concernant le partage d'informations.

Sinon, des informations sensibles concernant les incidents peuvent être fournies à des parties non autorisées, ce qui peut entraîner des perturbations supplémentaires et des pertes financières.

- L'équipe doit documenter tous les contacts et communications avec des tiers à des fins de responsabilité et de preuve.
- Les sections suivantes fournissent des directives sur la communication avec plusieurs types de parties externes, comme illustré à la Figure 2-1. Les flèches à double tête indiquent que l'une ou l'autre des parties peut initier des communications.





PARTIE 3

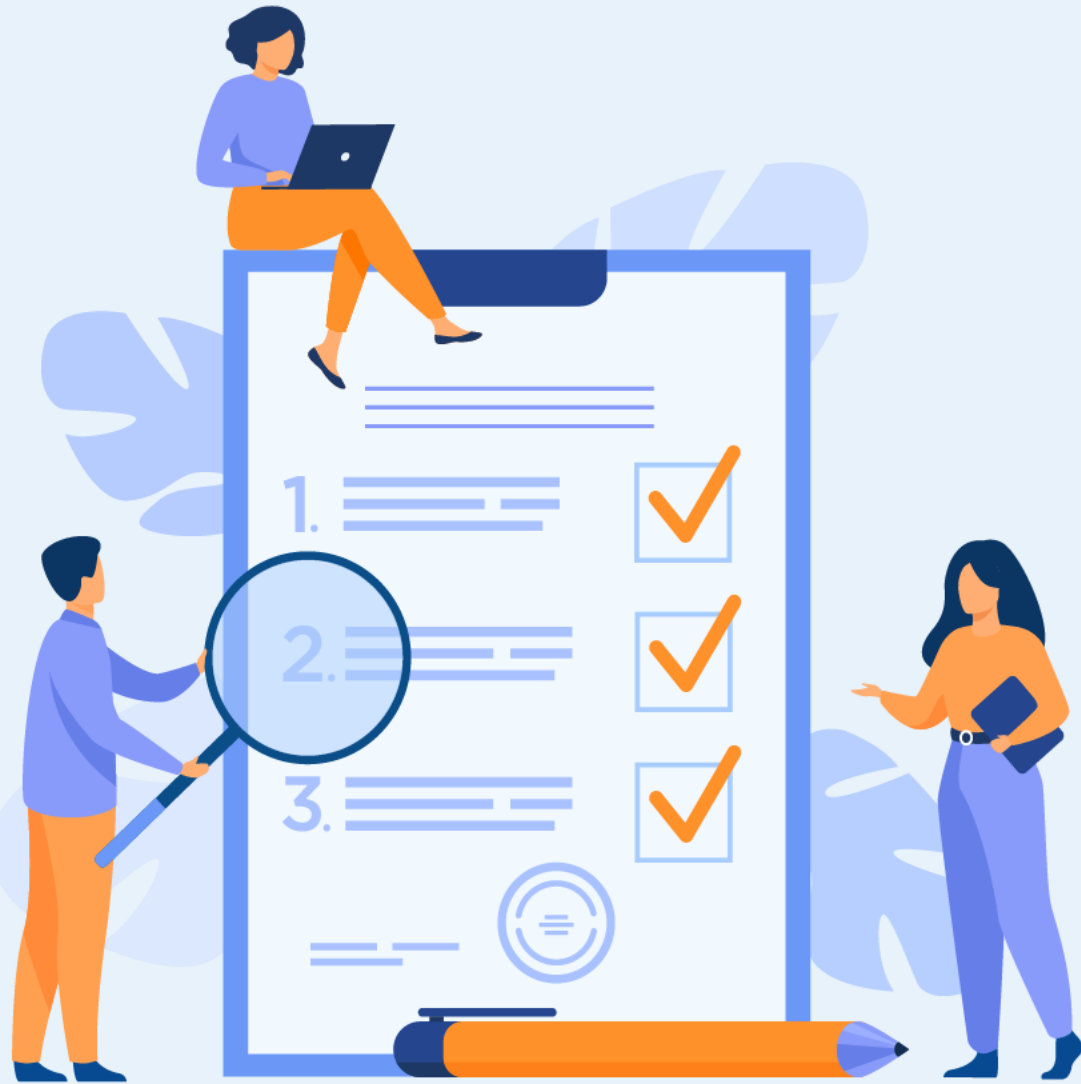
Effectuer le Threat Hunting

Dans ce module, vous allez :

- Définir le terme du « Threat Hunting »
- Décrire les étapes du processus de cette méthode



13 heures



CHAPITRE 1

Définir le Threat Hunting

Ce que vous allez apprendre dans ce chapitre :

- Définir les menaces persistantes avancées (APT)
- Déterminer les caractéristiques des APT
- Connaître les méthodologies de Threat Hunting



6 heures

CHAPITRE 1

Définir le Threat Hunting

1. **Notion de menaces persistantes avancées (APT)**
2. Méthodologies de Threat Hunting



01 – Définir le Threat Hunting

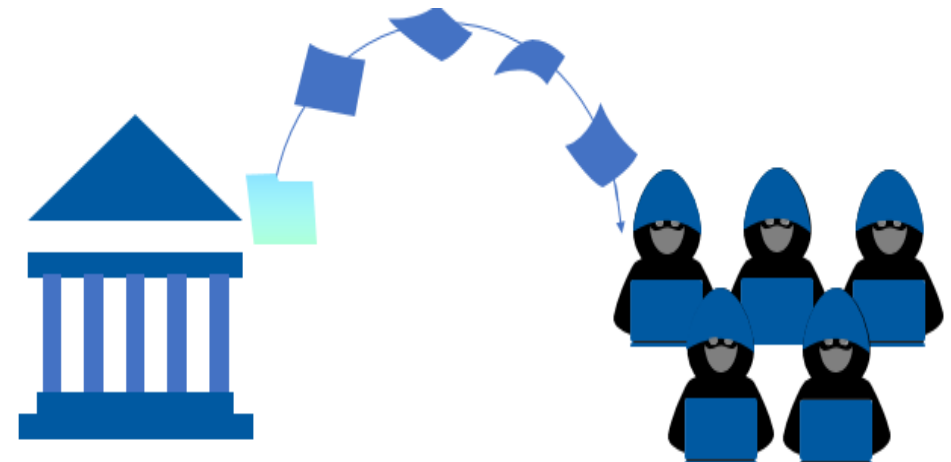
Notion de menaces persistantes avancées (APT)

Définition de menaces persistantes avancées (APT)

- Lorsque la plupart des gens pensent à une cyberattaque, ils y voient un transfert ponctuel. Un attaquant trouve un moyen d'accéder à un système pour un gain financier ou même pour faire ses preuves en ternissant la réputation de l'entreprise. Ensuite, il commence à télécharger des documents et des informations importants, puis s'en va. Dans ce type d'attaques, les attaquants n'essayaient pas de cacher leurs actions.
- Cependant, il existe un autre type d'attaques qui est devenu de plus en plus important au cours des deux dernières décennies. Cette classe d'attaques se caractérise par un mouvement lent et bas d'un groupe d'attaquants pour atteindre leur objectif, qui est généralement de voler les données de la cible sans se faire prendre. Le terme donné à cette classe d'attaques est **Advanced Persistent Threats** (APT) et en français **menaces persistantes avancées**.

Qu'est ce qu' une menace persistante avancée ?

- une menace persistante avancée (APT) une cyberattaque dans laquelle les pirates travaillent ensemble en utilisant des méthodes et outils sophistiqués et avancés pour infiltrer des systèmes et y rester souvent inaperçus pendant une longue période.
- Les APT sont souvent réalisées par un groupe d'attaquants avancés qui sont bien financés par une organisation ou un gouvernement pour obtenir des informations cruciales sur leur organisation cible ou gouvernement.
- Les cibles de ces agressions, qui sont très soigneusement choisies et étudiées, comprennent généralement de grandes entreprises ou des réseaux gouvernementaux.



01 – Définir le Threat Hunting

Notion de menaces persistantes avancées (APT)



Caractéristiques de menaces persistantes avancées (APT)

Parmi les caractéristiques les plus importantes de menaces persistantes avancées, nous citons :

- ✓ Plus dangereux que les menaces traditionnelles car les pirates ont un accès permanent aux données sensibles de l'entreprise,
- ✓ Cibles précises : Les cibles sont généralement de grande valeur, telles que des gouvernements ou des grandes entreprises possédant une valeur de propriété intellectuelle substantielle,
- ✓ Objectifs clairs: les APT recherchent généralement des actifs numériques qui apportent un avantage concurrentiel ou des avantages stratégiques, tels que les données de sécurité nationale, la propriété intellectuelle, les secrets commerciaux, etc.
- ✓ Techniques d'attaque furtives: Les attaques APT sont furtives, possèdent la capacité de ne pas être détectées, se dissimulent dans le trafic réseau de l'entreprise et interagissent juste assez pour atteindre les objectifs définis,
- ✓ Attaque complexe: Les attaques APT sont méticuleusement planifiées et comportent généralement plusieurs étapes,
- ✓ Attaquants bien organisés: Les acteurs derrière les APT sont généralement un groupe de pirates informatiques qualifiés, travaillant de manière coordonnée. Ils disposent de ressources suffisantes tant du point de vue financier que technique,
- ✓ Tentatives répétées: Les acteurs APT attaquent constamment leurs cibles et adaptent à plusieurs reprises leurs efforts pour terminer le travail lorsqu'une tentative précédente échoue.

01 – Définir le Threat Hunting

Notion de menaces persistantes avancées (APT)



Exemples de menaces persistantes avancées (APT)

Le tableau ci-dessous présente trois exemples de menace persistantes avancée appliquer sur des victimes réels.

Nom de APT	Temps actif	Intrusion initiale	Données exfiltrées
Opération Aurora	juin 2009 -décembre 2009	téléchargement furtif (Drive-by download)	télécharger des données sur les serveurs externes
RAS Breach	Inconnu -Mars 2011	Vulnérabilité de xls	compresser, crypter les données en tant que fichiers RAR, utiliser FTP pour la transmission
Opération Ke3chang	Mai 2010 - Décembre 2013	les victimes ouvrent le fichier exécutable	compresser, crypter les données sous forme de fichiers RAR



WEBFORCE
BE THE CHANGE

CHAPITRE 1

Définir le Threat Hunting

1. Notion de menaces persistantes avancées (APT)
2. **Méthodologies de Threat Hunting**



Définition et caractéristiques du Threat Hunting

- Après avoir solidifié les stratégies de sécurité des terminaux et de réponse aux incidents pour atténuer les attaques de logiciels malveillants connus qui sont inévitables aujourd'hui comme les APT, les experts de sécurité peuvent alors passer à l'offensive. Ils sont prêts à creuser profondément et à trouver ce qui n'a pas encore été détecté. C'est exactement le but du **Threat Hunting**.
 - **Threat Hunting** peut être défini comme stratégie proactive conçue pour trouver des menaces inconnues ou des adversaires cachés à l'intérieur d'un réseau avant qu'ils ne puissent exécuter une attaque ou atteindre leurs objectifs.
 - Le processus est une méthode d'*investigation* consistant à tester un ensemble évolutif d'hypothèses à l'aide de kits d'outils de chasse aux menaces qui permettent à la fois un travail de détective créatif et des flux de travail basés sur de nouvelles découvertes.
 - L'objectif du **Threat Hunting** est de surveiller les activités quotidiennes d'un système et le trafic sur le réseau et de chercher les éventuelles anomalies pour détecter toute activité malveillante qui a réussi à contourner les défenses d'une organisation et qui pourrait conduire à une brèche partielle ou complète.
 - Contrairement à la plupart des techniques de sécurité, le **Threat Hunting** va plus loin pour trouver des acteurs malveillants évasifs, en combinant les capacités et les données d'une solution de sécurité avancée avec les solides compétences analytiques et techniques d'un individu ou d'une équipe de professionnels de la chasse aux menaces.



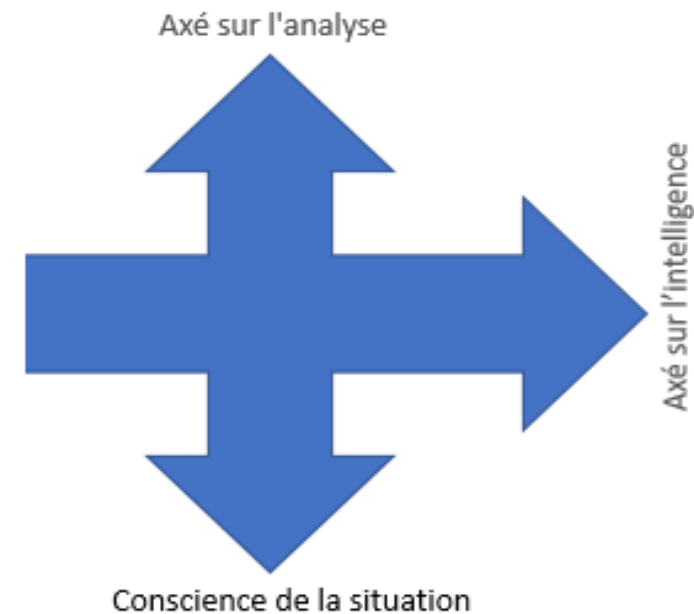
01 – Définir le Threat Hunting

Méthodologies du Threat Hunting

- Les experts du Threat Hunting partent du principe qu'un attaquant est déjà dans le réseau. Ils essaient de rechercher des indicateurs de compromission, de mouvement latéral et d'autres artefacts révélateurs qui peuvent fournir des preuves du comportement d'attaque.
- Selon le point de départ de recherche, le Threat Hunting peut suivre une des trois méthodologies ou techniques suivantes:

1 - Chasse par hypothèses :

- Cette méthodologie de chasse aux menaces consiste à tester trois types d'hypothèses :
 - ✓ Axé sur l'analyse : utilise l'analyse du comportement des utilisateurs et l'apprentissage automatique (ML) pour développer des scores de risque agrégés et formuler des hypothèses.
 - ✓ Axé sur l'intelligence : inclut l'analyse des flux d'intelligence, les analyses de vulnérabilité, les logiciels malveillants et les rapports.
 - ✓ Conscience de la situation : évaluations des risques et identification des actifs numériques qui sont essentiels à l'entreprise ou l'organisation à sécuriser.



01 – Définir le Threat Hunting

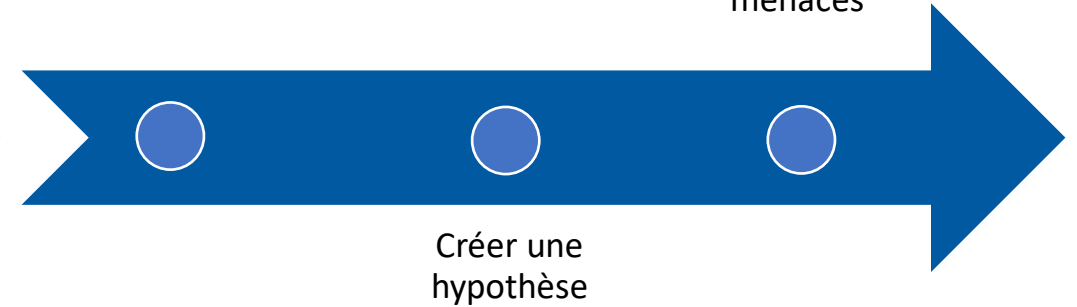
Méthodologies du Threat Hunting

2 - Chasse structurée :

- La chasse structurée est la méthodologie la plus proactive du Threat Hunting.
- Les tâches qui interviennent le plus souvent dans cette méthodologie sont :
 - ✓ Utiliser les indicateurs d'attaque (IoA) et les tactiques, techniques et procédures (TTP) pour déterminer les acteurs de menace,
 - ✓ Le chasseur estime l'environnement, le domaine et les comportements d'attaque pour créer une hypothèse qui s'aligne sur MITRE ATT&CK Framework (MAF)?
 - ✓ Après avoir précisé un comportement, le chasseur essaye de localiser des modèles de menaces en surveillant les activités sur le système.

Déterminer les
acteurs de
menace

Localiser des
modèles de
menaces



Remarque

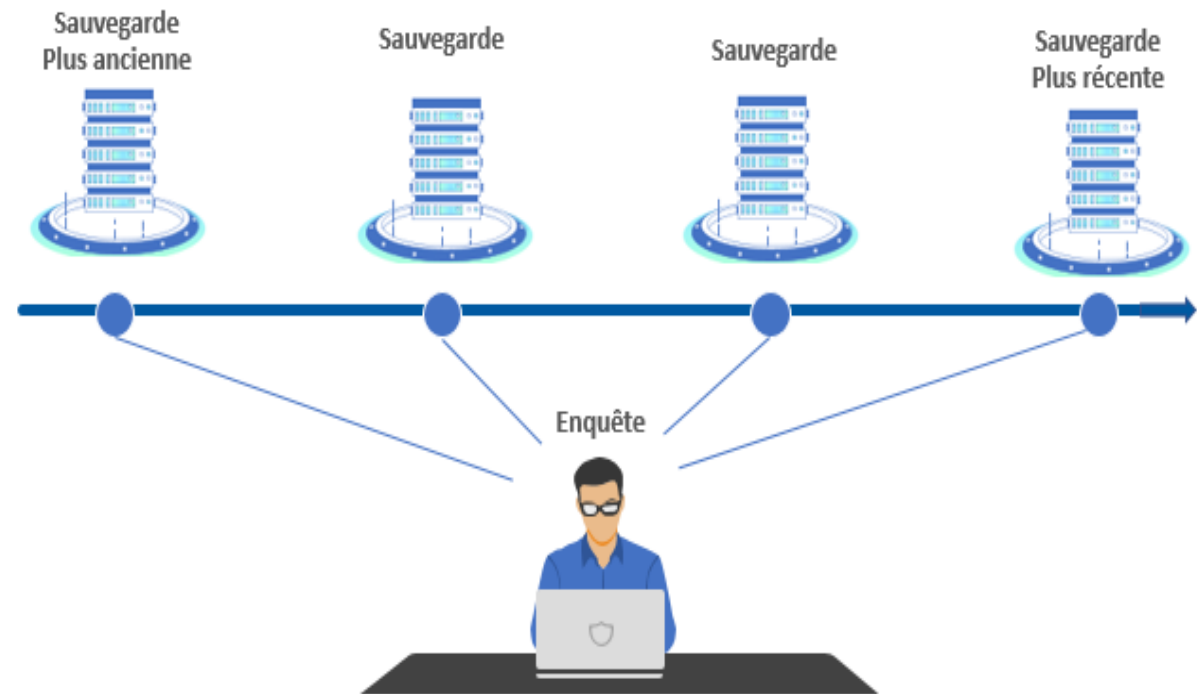
- **MITRE ATT&CK Framework** : fournit une mine d'informations techniques pour les chasseurs en guidant le processus de chasse avec des techniques de détection.

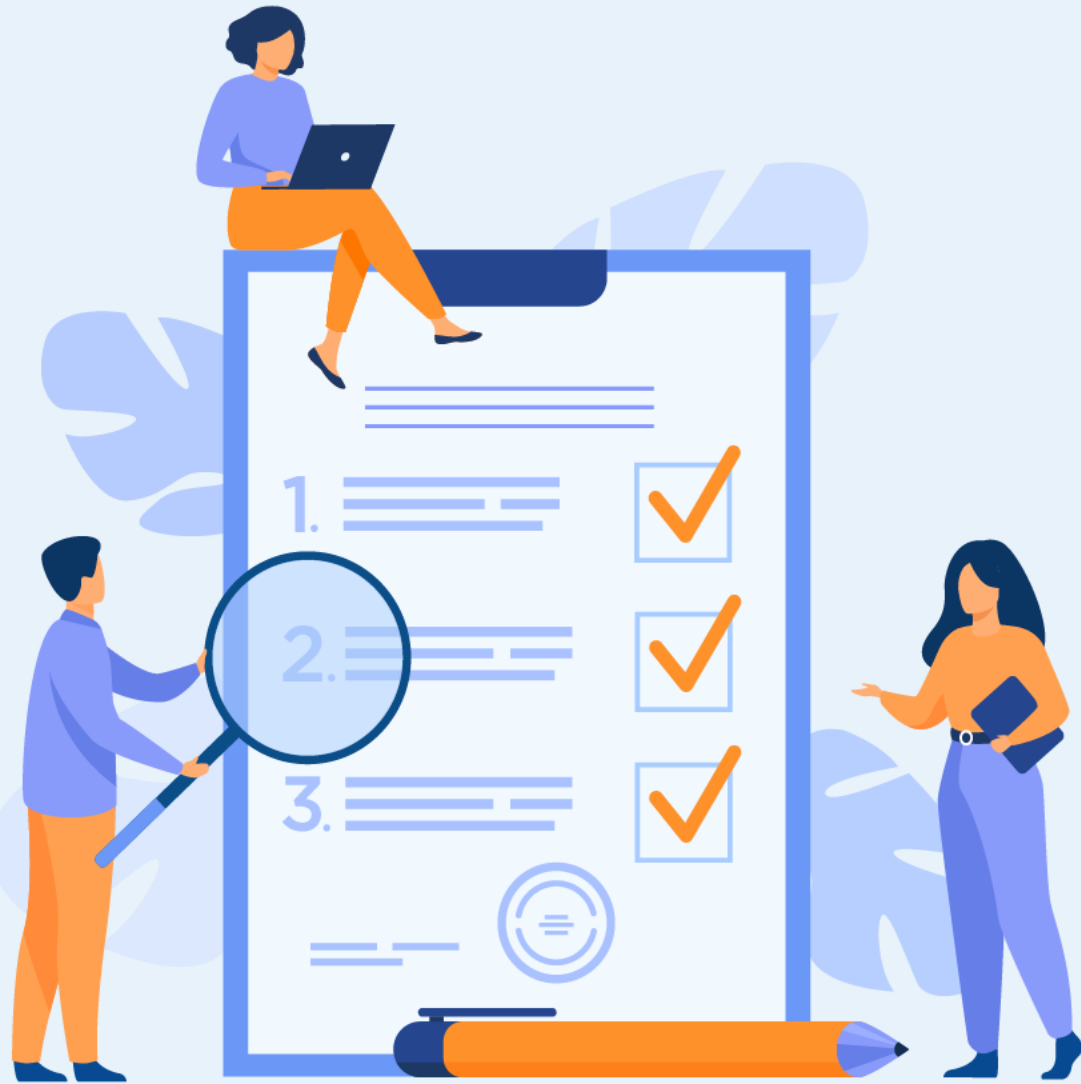
01 – Définir le Threat Hunting

Méthodologies du Threat Hunting

3 - Chasse non structurée :

- La chasse non structurée débute à partir d'un déclencheur ou d'un indicateur de compromission (IoC).
- Ce type de Threat Hunting peut découvrir de nouveaux types de menaces ou de menaces qui ont pénétré l'environnement dans le passé et sont maintenant en sommeil.
- Le chasseur de menaces recherche sur le réseau des modèles malveillants avant et après le déclencheur ou l'IoC.
- Le chasseur de menaces peut enquêter sur les données historiques dans la mesure où les limites de sauvegarde des données le permettent.





CHAPITRE 2

Identifier les étapes du processus

Ce que vous allez apprendre dans ce chapitre :

- Identifier les étapes du Threat Hunting
- Déterminer la Place du Threat Hunting dans la stratégie de sécurité



7 heures

CHAPITRE 1

Identifier les étapes du processus

1. **Identification des étapes**
2. Place du Threat Hunting dans la stratégie de sécurité



02 – Identifier les étapes du processus

Identification des étapes



Identification des étapes

- La création d'un programme efficace de chasse aux menaces fait partie des principales priorités des responsables de la sécurité qui cherchent à devenir plus proactifs et à mettre en place des défenses actives.
- Un processus proactif de chasse aux menaces inclut généralement trois étapes : une étape initiale de déclenchement, suivie d'une enquête approfondie et se terminant par une résolution.



02 – Identifier les étapes du processus

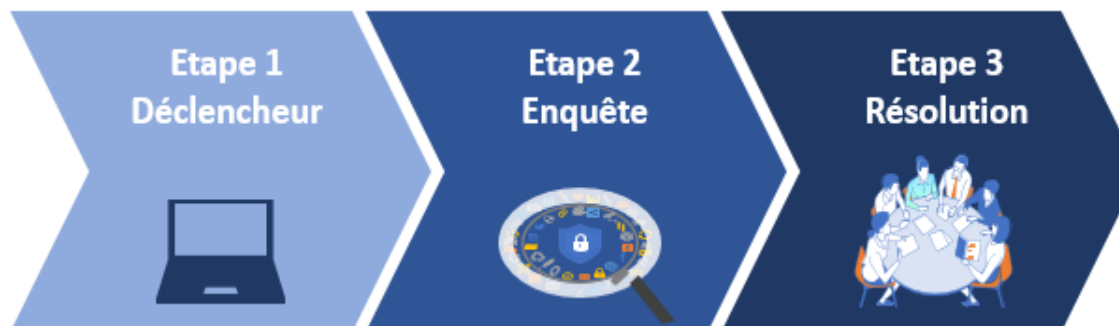
Identification des étapes



Identification des étapes

Étape 1 : Déclencheur

- Le Threat Hunting est généralement un processus ciblé.
- Au début, le chasseur recueille des informations sur l'environnement ciblé puis élabore des hypothèses sur les menaces potentielles.
- Un chasseur de menaces peut utiliser des informations sur les menaces actuelles ou des TTP d'attaquants en plus de ses connaissances, son expérience et ses compétences créatives en résolution de problèmes pour établir une hypothèse de menace et décider de la voie à suivre.
- Ensuite, le chasseur choisit un déclencheur, qui a été identifié généralement dans une applications ou une zone spécifique du réseau, pour une enquête plus approfondie
- Une hypothèse peut servir de déclencheur lorsque des outils de détection avancés incitent les chasseurs de menaces à lancer une enquête sur un système particulier ou une zone spécifique d'un réseau.



Une hypothèse peut servir de déclencheur lorsque des outils de détection avancés incitent les chasseurs de menaces à lancer une enquête sur un système particulier ou une zone spécifique d'un réseau.

02 – Identifier les étapes du processus

Identification des étapes



Identification des étapes

Étape 2 : Enquête

- Une fois un déclencheur choisi, les chasseurs de menaces recherchent en profondeur des anomalies potentiellement malveillantes dans le système ou le réseau.
- Au cours de l'enquête, les chasseurs de menaces utilisent un large éventail de technologies et des outils du Threat Hunting comme **User Entity Behavior Analytics (UEBA)**, **security information and event management (SIEM)** pour les aider à enquêter sur les anomalies, qui peuvent ou non être malveillantes.
- L'enquête se poursuit jusqu'à ce que l'hypothèse soit prouvée ou non.



La technologie d'investigation peut chasser ou rechercher en profondeur des anomalies potentiellement malveillantes dans un système ou un réseau, finalement jugées bénignes ou confirmées comme malveillantes.

02 – Identifier les étapes du processus

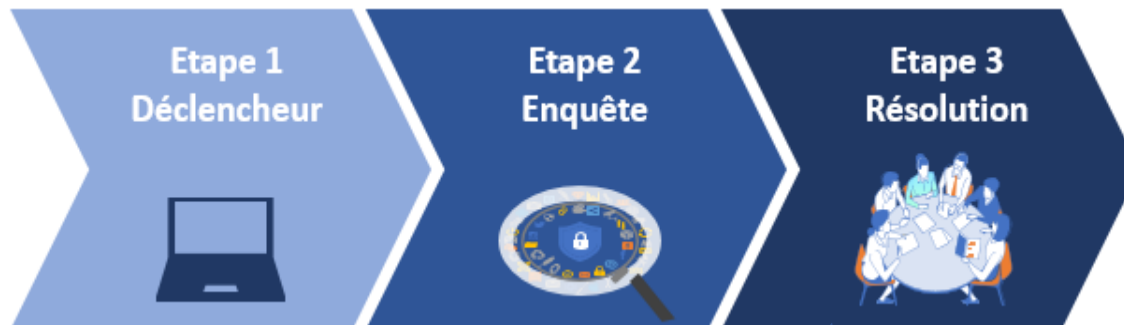
Identification des étapes



Identification des étapes

Étape 3 : Résolution

- Pendant l'étape de résolution, les informations collectées durant l'étape précédant sont communiquées aux équipes de sécurité et d'exploitation pour réagir rapidement et atténuer les menaces
- Les actions à exécuter peuvent inclure :
 - ✓ Mise à jour des règles de pare-feu et IPS
 - ✓ Restauration de fichiers modifiés
 - ✓ Suppression de fichiers malveillants,
 - ✓ Modification des configurations système
 - ✓ Déploiement de correctifs de sécurité
 - ✓ Documentation de méthodes de l'attaquant



Pendant la phase de résolution, ces informations sont communiquées à d'autres équipes et outils qui peuvent répondre, hiérarchiser, analyser ou stocker les informations pour une utilisation future.

CHAPITRE 2

Identifier les étapes du processus

1. Identification des étapes
2. **Place du Threat Hunting dans la stratégie de sécurité**

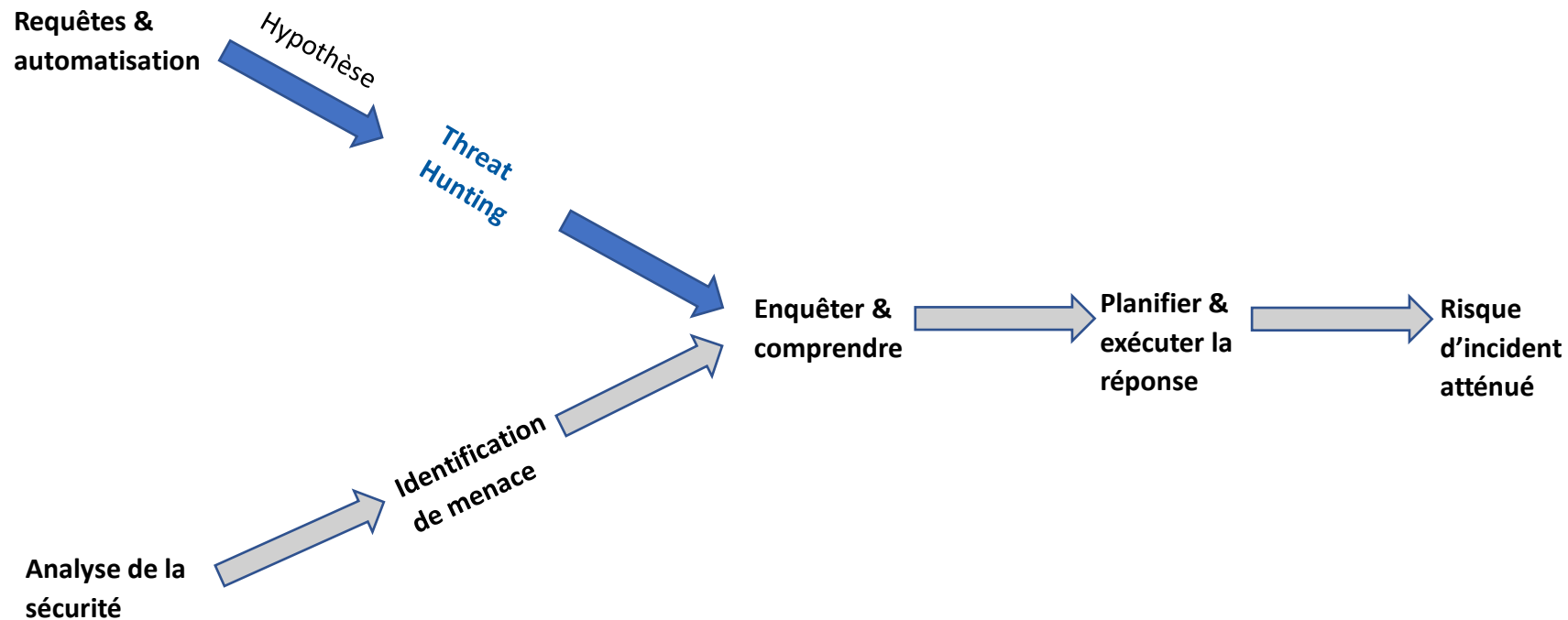


02 – Identifier les étapes du processus

Place du Threat Hunting dans la stratégie de sécurité

Place du Threat Hunting dans la stratégie de sécurité

- Le Threat Hunting est considéré comme un complément essentiel pour renforcer la sécurité d'un système. Il peut être implémenté en parallèle avec la stratégie de défense ordinaire d'une entreprise.
- La figure ci-dessous illustre Place du Threat Hunting dans la stratégie de sécurité :





WEBFORCE
BE THE CHANGE



PARTIE 4

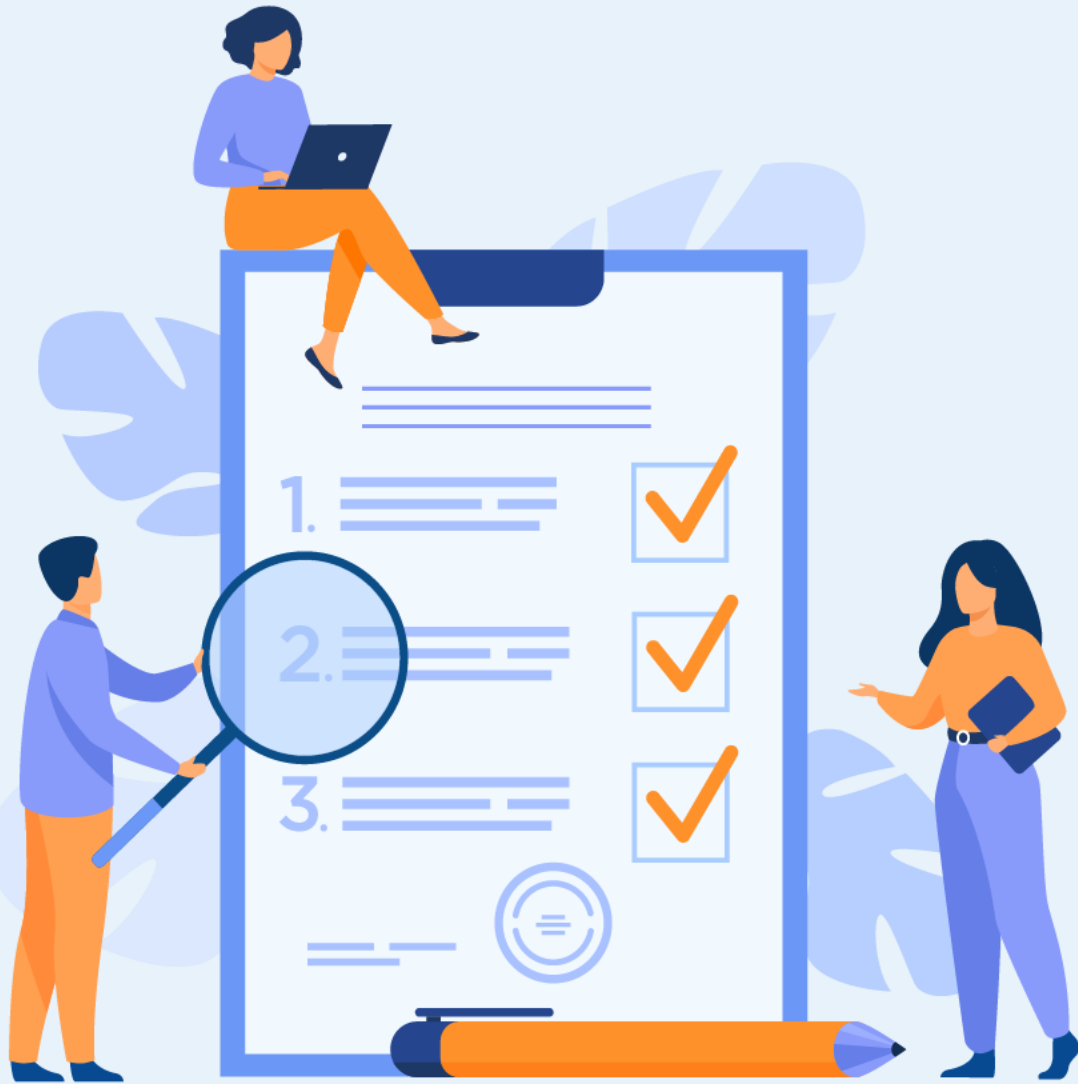
Répondre à des incidents de Cybersécurité

Dans ce module, vous allez :

- Connaître les stratégies et le processus de réponse aux incidents
- Savoir comment automatiser la réponse aux incidents



8 heures



CHAPITRE 1

Définir les étapes d'un plan de base de réponse aux incidents

Ce que vous allez apprendre dans ce chapitre :

- Définir le plan de base de la réponses aux incidents
- Savoir l'importance de la mis en ouvre d'un plan de la réponses aux incidents



4 heures

CHAPITRE 1

Définir les étapes d'un plan de base de réponse aux incidents

1. **Définition d'un plan de réponse aux incidents**
2. Présentation d'un exemple de plan de réponse



01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents



Définition d'un plan de réponse aux incidents :

- Le plan de réponse aux incidents de sécurité de l'information identifie et décrit les objectifs, les attentes, les rôles et les responsabilités en ce qui concerne la préparation, la détection, l'activation/la réponse, le confinement, la correction des notifications, la résolution et l'analyse après action des incidents de sécurité de l'information.
- Les objectifs du plan sont :
 - ✓ Fournir une stratégie de réponse cohérente aux menaces de sécurité de l'information qui mettent en danger les données et les systèmes universitaires.
 - ✓ Protéger la confidentialité, l'intégrité et la disponibilité des systèmes, réseaux et données universitaires.
 - ✓ Protéger le bien-être de la communauté universitaire et minimiser les atteintes à la réputation.
 - ✓ Aider l'université à se rétablir après des incidents de sécurité de l'information.
 - ✓ Mettre en œuvre des actions correctives opportunes et appropriées.
 - ✓ Répondre aux exigences légales ou réglementaires.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents



Pourquoi la planification de la réponse aux incidents est-elle importante ?

Voici les principaux avantages de la planification de la réponse aux incidents :

- **Fournit un processus standard pour la réponse aux incidents**

- ✓ La planification de la réponse aux incidents implique la création d'un plan qui explique comment l'organisation minimise les dommages et la durée des incidents de sécurité.
- ✓ Il permet d'identifier les parties prenantes concernées, de rationaliser l'investigation numérique, de réduire la publicité négative et le taux de désabonnement des clients et d'améliorer le temps de récupération.

- **Aide à répondre rapidement et efficacement**

Tout incident, qu'il soit petit ou important, peut dégénérer en une violation de données, une interruption des opérations commerciales et une perte de données. La planification de la réponse aux incidents aide les organisations à planifier une réponse rapide. Il informe les intervenants sur la façon de corriger les vulnérabilités, de minimiser les pertes, de fermer les vecteurs d'attaque et de restaurer les systèmes affectés.

- **Prépare les équipes pour les scénarios clés**

Les plans de réponse aux incidents incluent des scénarios qui préparent l'organisation à répondre aux menaces connues et inconnues. Il permet d'identifier les causes profondes des incidents de sécurité et d'effectuer une reprise après sinistre (après incident). Il décrit les meilleures pratiques pour la gestion des incidents et fournit un plan de communication pour informer les employés, les forces de l'ordre et les parties prenantes concernées.

- **Protège les informations sensibles**

La planification de la réponse aux incidents aide à prévenir les incidents et à protéger les données. Cela implique l'identification de données importantes, telles que les informations personnellement identifiables (PII), la biométrie, les informations de santé protégées (PHI), les informations financières et les secrets commerciaux. L'identification de ces données permet de les conserver en toute sécurité pour la conformité, la prévention des pertes de données et la continuité des activités.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents



Plan de réponse aux incidents :

- Un **plan de réponse aux incidents** est un plan documenté et rédigé en 6 phases distinctes qui aide les professionnels et le personnel informatique à reconnaître et à gérer un incident de cyber sécurité comme une violation de données ou une cyberattaque.
- Créer et gérer correctement un plan de réponse aux incidents implique des mises à jour et une formation régulières.

Comment créer un plan de réponse aux incidents ?

- Un plan de réponse aux incidents doit être mis en place pour traiter une violation de données suspectée en une série de phases. Dans chaque phase, il y a des domaines spécifiques de besoins qui doivent être pris en compte.
- Plusieurs étapes sont nécessaires pour atténuer complètement l'incident, tout en empêchant la destruction des preuves qui pourraient être nécessaires aux poursuites.

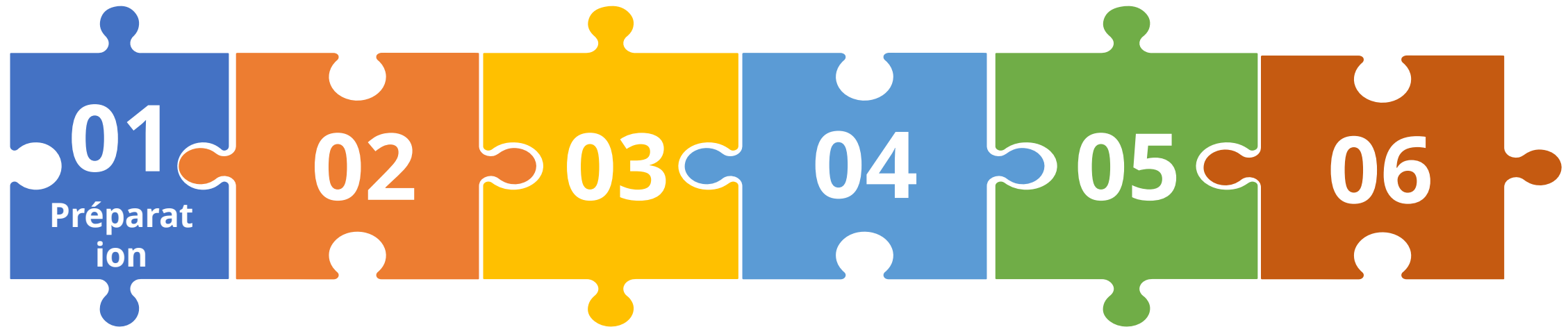
6 étapes de réponse aux incidents

- Selon le manuel des gestionnaires d'incidents du SANS Institute, l'équipe d'intervention en cas d'incident doit suivre six étapes pour gérer efficacement les incidents de sécurité.
- Le plan d'intervention doit aborder et fournir un processus structuré pour chacune de ces étapes.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :



Les plans de réponse aux incidents mettent l'accent sur la phase de préparation car c'est le point de départ pour déterminer les outils et les ressources nécessaires pour bien réagir contre les incidents. Ainsi, elle permet de prévenir les incidents en s'assurant que les systèmes, les réseaux et les applications sont suffisamment sécurisés.

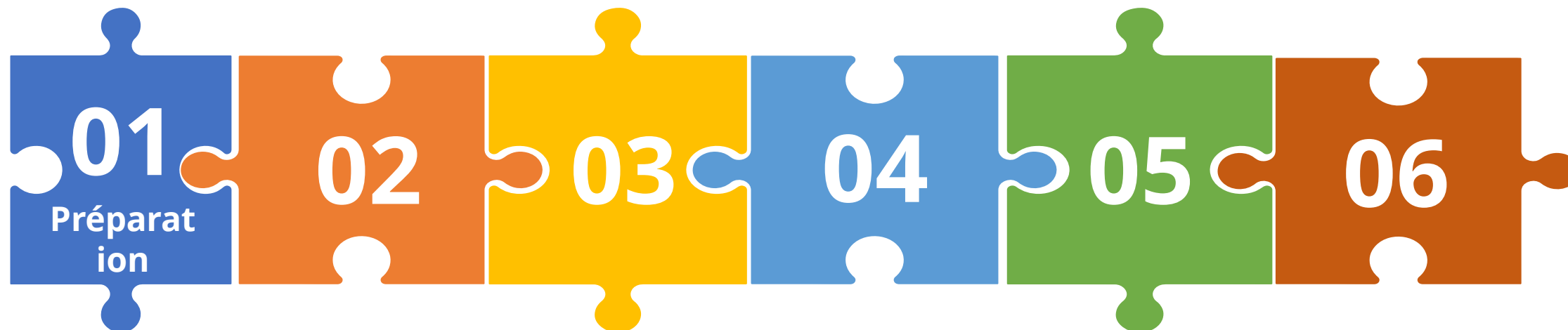
Une liste des tâches primordiales de cette phase comprend :

- ✓ Définir les incidents de sécurité critiques sur lesquels l'équipe doit se concentrer.
- ✓ Examiner et codifier une politique de sécurité organisationnelle.
- ✓ Effectuer une évaluation des risques.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

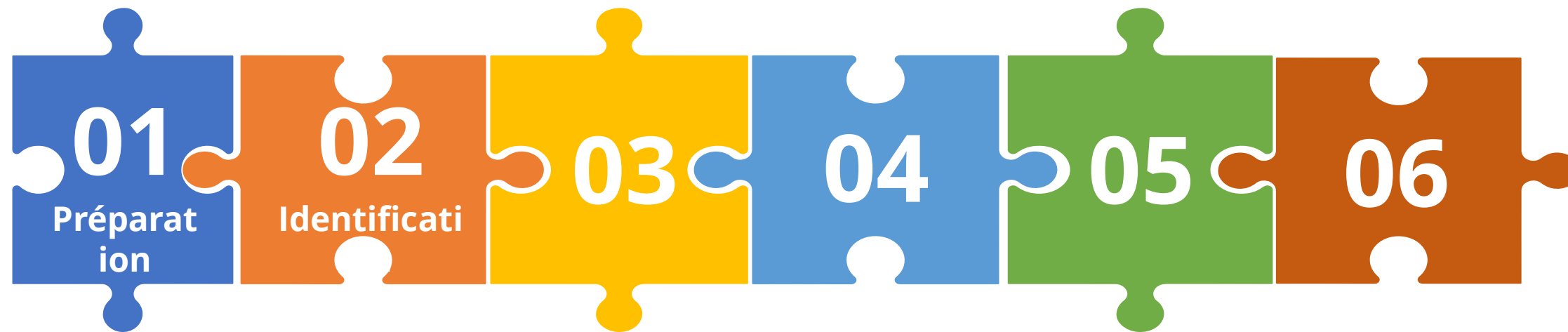


- Tout le monde a-t-il été formé aux politiques de sécurité ?
- Les politiques de sécurité et le plan de réponse aux incidents ont-ils été approuvés par la direction appropriée ?
- En cas d'incident, l'équipe d'intervention connaît-elle ses rôles et les notifications requises à effectuer ?
- En cas d'incident, tous les membres de l'équipe d'intervention ont-ils participé à des simulations d'exercice ?

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

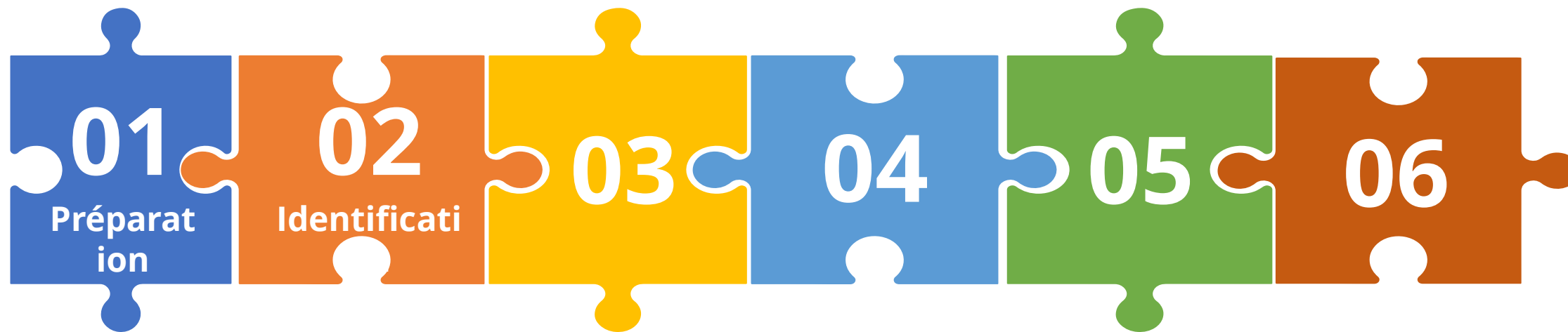


L'identification des incidents s'effectue grâce à la surveillance des réseaux et systèmes informatiques et la détection du moindre écart par rapport aux activités normales. Puis, déterminer s'ils représentent des incidents de sécurité réels ou non.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

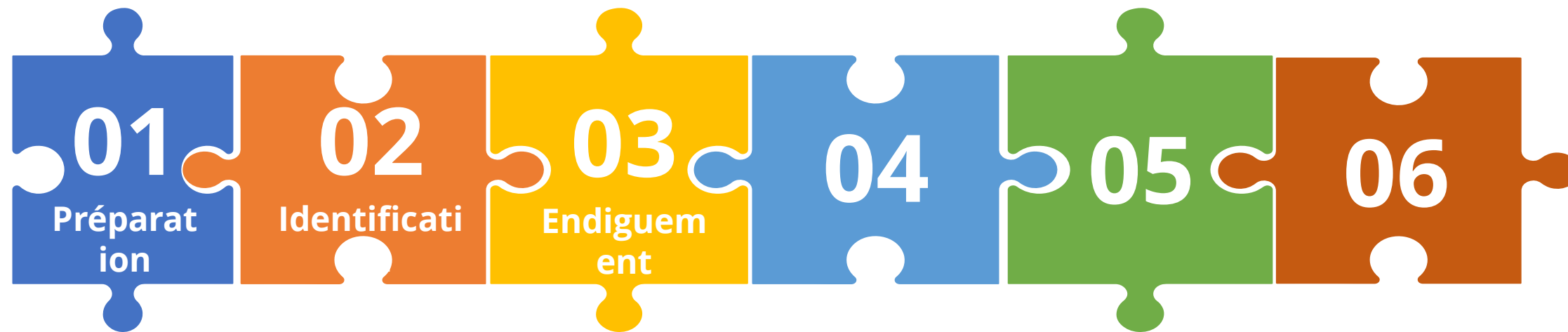


- Quand l'événement s'est-il produit ?
- Comment a-t-il été découvert ?
- Qui l'a découvert ?
- D'autres zones ont-elles été impactées ?
- Quelle est la portée du compromis ?
- Cela affecte-t-il les opérations ?
- La source (point d'entrée) de l'événement a-t-elle été découverte ?

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

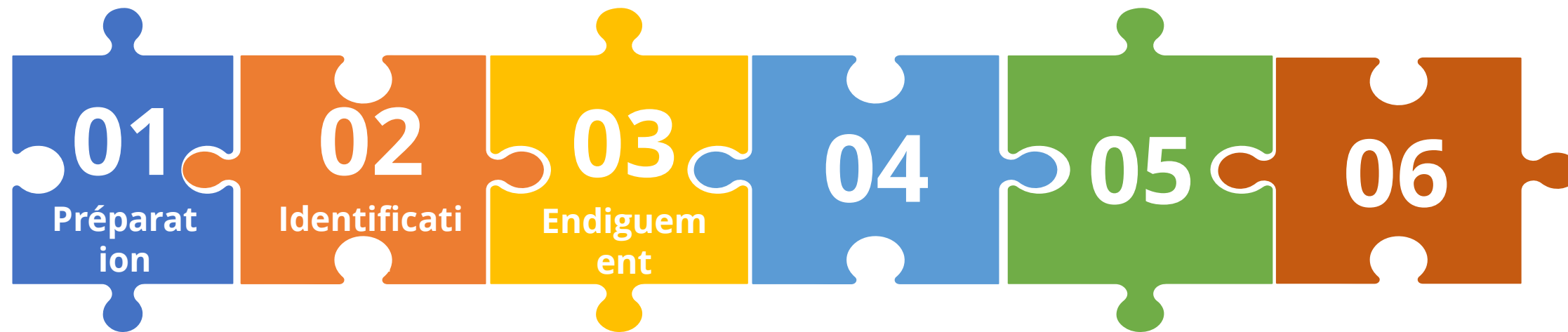


- Lorsqu'un incident est découvert pour la première fois, l'instinct initial est l'application d'un confinement à court terme, par exemple en isolant le segment de réseau qui est attaqué.
- Ensuite, il est nécessaire d'effectuer un confinement à long terme, qui implique des correctifs temporaires pour permettre aux systèmes d'être utilisés en production, tout en reconstruisant des systèmes propres.
- Le but du confinement est de limiter les dommages causés par l'incident de sécurité actuel et d'empêcher tout autre dommage.
- C'est également le bon moment pour modifier tous les identifiants d'accès utilisateur et administratif, revoir les protocoles d'accès à distance, renforcer tous les mots de passe et mettre à jour et corriger le système.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

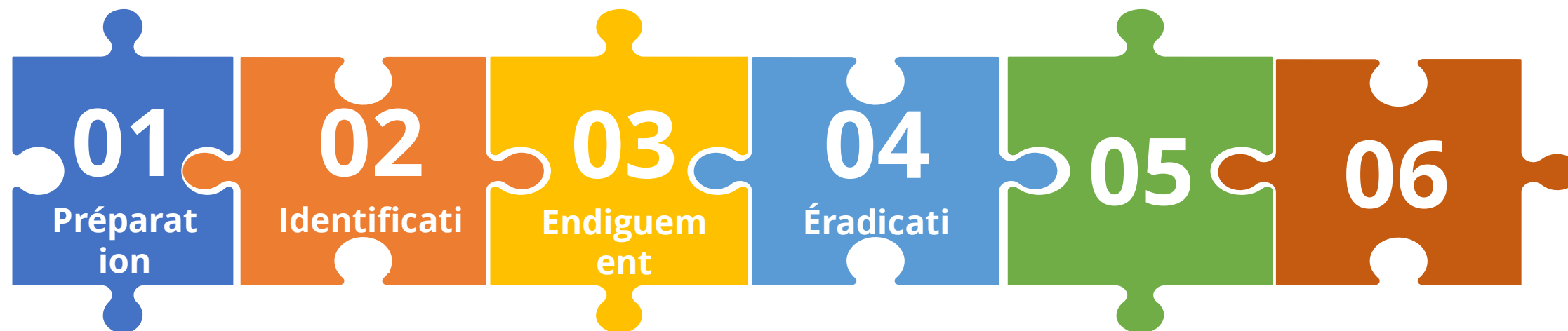


- Qu'est-ce qui a été fait pour contenir la violation à court terme ?
- Qu'est-ce qui a été fait pour contenir la brèche à long terme ?
- Un logiciel malveillant découvert a-t-il été mis en quarantaine du reste de l'environnement ?
- Quel type de sauvegardes mise en place ?
- L'accès à distance nécessite-t-il une véritable authentification multi-facteurs ?
- Toutes les informations d'identification d'accès ont-elles été examinées pour vérifier leur légitimité, renforcées et modifiées ?
- Avez-vous appliqué tous les correctifs et mises à jour de sécurité ?

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

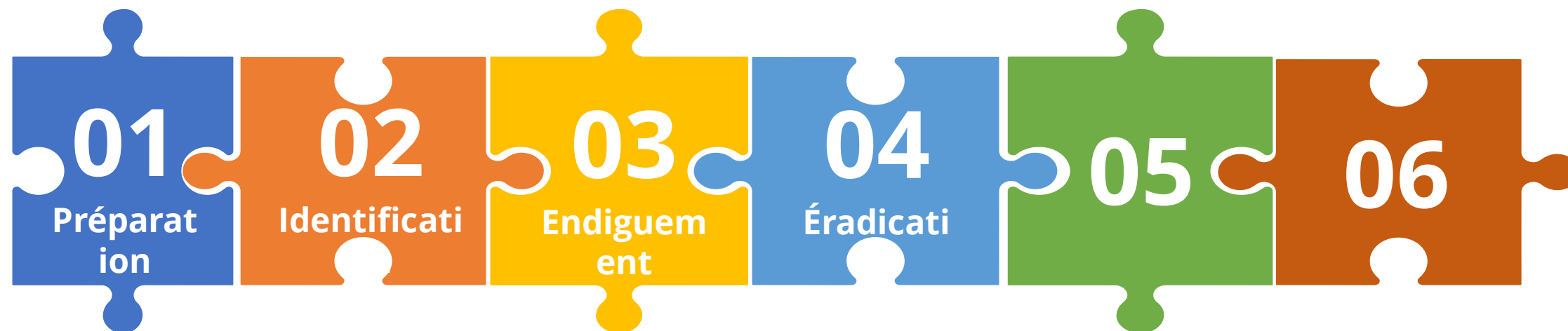


- L'éradication vise à trouver et éliminer la cause profonde de l'incident par la suppression des logiciels malveillants introduits par les attaques puis la restauration de tous les systèmes affectés.
- Les principales tâches de cette phase sont :
 - ✓ Suppression des logiciels malveillants de tous les systèmes affectés.
 - ✓ Identification de la cause première de l'attaque.
 - ✓ Définition des règles pour empêcher des attaques similaires à l'avenir.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

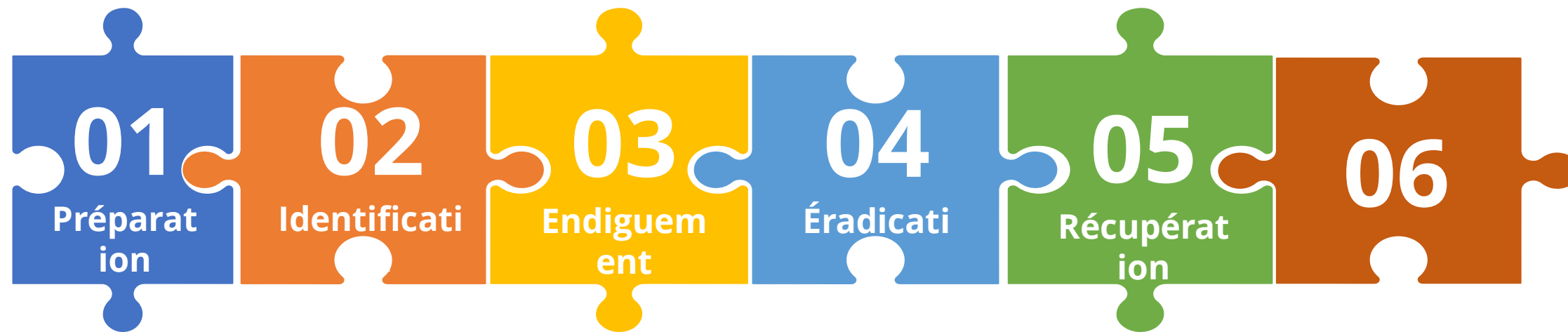


- Les programmes malveillants de l'attaquant ont-ils été supprimés en toute sécurité ?
- Le système a-t-il été renforcé, corrigé et les mises à jour appliquées ?
- Le système peut-il être ré-imaginé ?

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

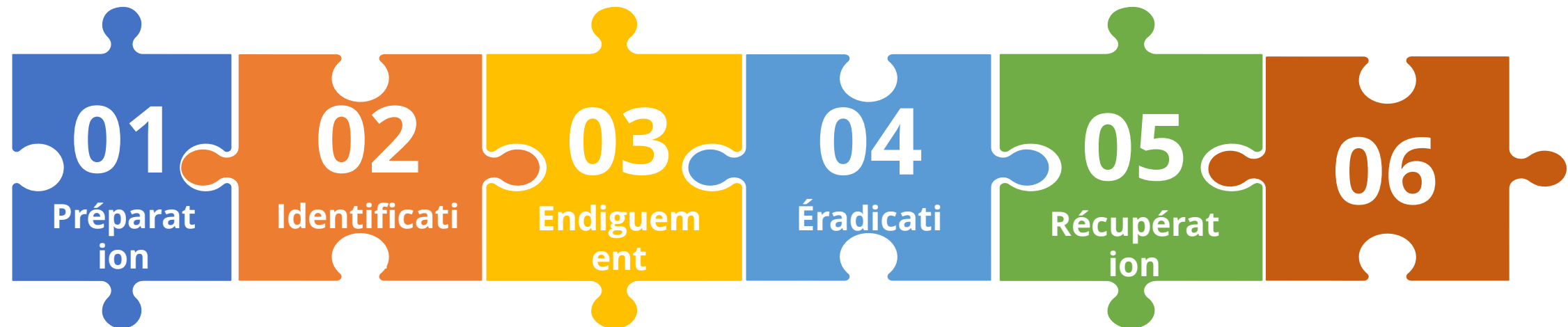


- L'objectif de la récupération est de restaurer et de remettre tous les systèmes et appareils en état de fonctionnement complet, après avoir vérifié qu'ils sont propres et que la menace a été complètement supprimée.
- La procédure de récupération implique :
 - ✓ Définition de l'heure et la date des opérations de restauration.
 - ✓ Vérification que les systèmes sont propres et entièrement fonctionnels au fur et à mesure de leur mise en service.
 - ✓ Surveillance continue pendant un certain temps après l'incident pour observer les opérations et vérifier les comportements anormaux.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :



- Quand les systèmes peuvent-ils être remis en production ?
- Les systèmes ont-ils été corrigés, renforcés et testés ?
- Le système peut-il être restauré à partir d'une sauvegarde de confiance ?
- Combien de temps les systèmes concernés seront-ils surveillés et que recherche-t-on lors de la surveillance ?
- Quels outils garantiront que des attaques similaires ne se reproduiront pas ?

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :

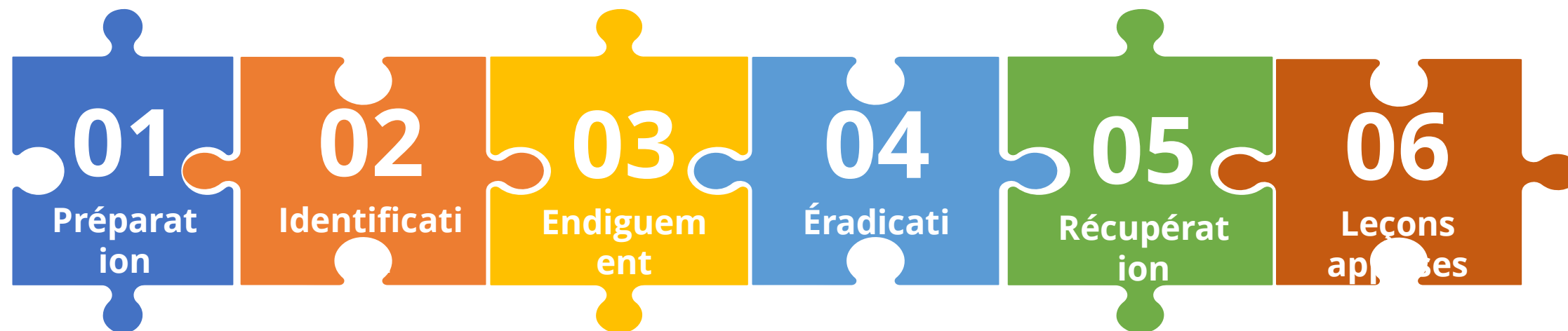


- Au plus tard deux semaines après la fin de l'incident et afin de renforcer la sécurité du système, il est recommandé d'exécuter les tâches suivantes :
 - ✓ Faire une analyse complète de l'incident et ses dégâts.
 - ✓ Documenter tout ce qui concerne l'incident.
 - ✓ Déterminez ce qui a bien fonctionné dans le plan de réponse.
 - ✓ Extraire les leçons qui peuvent aider à améliorer le plan de réponse pour les prochains à l'incident.

01 – Définir les étapes d'un plan de base de réponse aux incidents

Définition d'un plan de réponse aux incidents

Plan de réponse aux incidents :



- Quels changements faut-il apporter à la sécurité ?
- Comment les employés devraient-ils être formés différemment ?
- Quelle faiblesse la brèche a-t-elle exploitée ?
- Comment s'assurer qu'une violation similaire ne se reproduise plus ?

CHAPITRE 1

Définir les étapes d'un plan de base de réponse aux incidents

1. Définition d'un plan de réponse aux incidents
2. **Présentation d'un exemple de plan de réponse**



01 – Définir les étapes d'un plan de base de réponse aux incidents

Présentation d'un exemple de plan de réponse



Exemple de plan de réponse aux incidents :

Ce document décrit les étapes suivies lors d'un plan de réponse aux incidents.

Pour créer le plan, les étapes de l'exemple suivant doivent être remplacées par des informations de contact et des plans d'action spécifiques pour votre organisation.



CHAPITRE 2

Automatiser la réponse aux incidents

Ce que vous allez apprendre dans ce chapitre :

- Déterminer les étapes de l'automatisation de la réponses aux incidents
- Connaître quelques outils de l'automatisation de la réponses aux incidents



4 heures

CHAPITRE 2

Automatiser la réponse aux incidents

1. **Processus à mettre en place**
2. Technologies d'automatisation



02 – Automatiser la réponse aux incidents

Processus à mettre en place



Définition et importance

- Parfois, les organisations découvrent du trafic vers ou depuis un domaine malveillant connu. Ce trafic doit être bloqué pendant l'enquête sur l'intrusion potentielle. Il est plus rapide et plus facile de prendre de telles mesures, puis de passer de la détection à la réponse, grâce à la **réponse automatisée aux incidents**.

Qu'est ce qu'une réponse automatisée aux incidents ?

- La gestion automatisée des incidents est le processus d'automatisation de la réponse aux incidents pour garantir que les incidents critiques sont détectés et traités de la manière la plus efficace et la plus cohérente.

Quelle est l'importance de la réponse automatisée aux incidents ?

- L'avantage fondamental de l'automatisation de la réponse aux incidents est la rapidité. L'automatisation accélère les réponses et les tâches de routine réduisant considérablement le temps de réponse face à une cyber menace. Cela peut faire toute la différence lorsqu'il s'agit de réduire l'impact d'une attaque sur un système.
- Alors que l'intervention humaine est essentielle pour la réponse aux incidents, l'automatisation permet de la minimiser autant que possible. Il aide également les entreprises à mettre en place un système de défense 24h/24 et 7j/7.
- En fin de compte, l'automatisation fonctionne comme un accélérateur pour atteindre l'objectif de répondre intelligemment en un temps record.

02 – Automatiser la réponse aux incidents

Processus à mettre en place



Les étapes de l'automatisation de la réponses aux incidents

L'automatisation est extrêmement importante pour créer un système de réponse aux incidents évolutif et efficace. Ci-après, nous citons les étapes essentielles pour automatiser les réponses aux incidents :

1. Créer le plan de réponse convenable au réseau à sécuriser :

Le responsable de sécurité doit créer le premier plan de réponse à l'aide de tâches manuelles pour répondre à un incident. Il doit également pratiquer ces processus sur des événements réels afin de s'assurer de leur efficacité. Cela ouvre la voie à l'automatisation de ces processus, en partie ou en totalité.

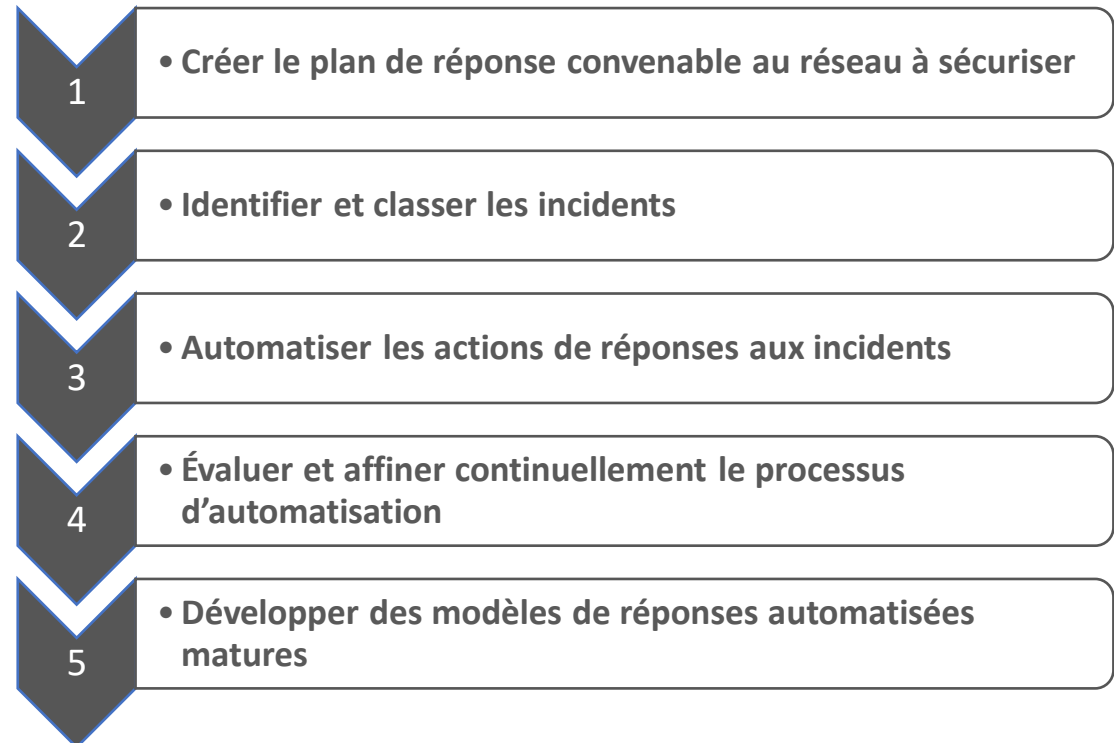
2. Identifier et classer les incidents :

Les incidents sont identifiés par le biais de rapports d'utilisateurs, d'analyses de solutions ou d'une identification manuelle. Une fois identifié, l'incident est enregistré et l'enquête et la catégorisation peuvent commencer pour faciliter ensuite le choix des outils d'automatisation.

3. Automatiser les actions de réponses aux incidents :

Choisir les outils convenables, selon des critères bien définis, est le secret de succès de l'automatisation. Il est aussi important de déterminer les étapes à automatiser surtout pour les systèmes qui adoptent cette méthode pour la première fois.

Évaluer et affiner continuellement le processus d'automatisation.



02 – Automatiser la réponse aux incidents

Processus à mettre en place



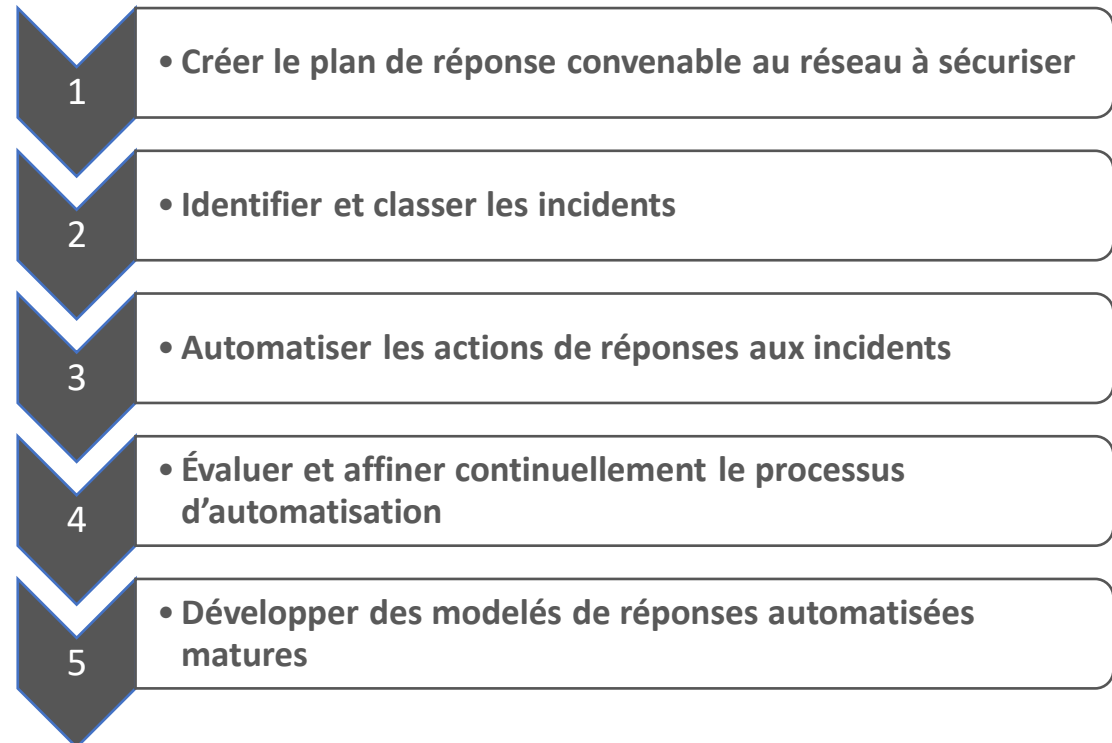
Les étapes de l'automatisation de la réponses aux incidents

4. Évaluer et affiner continuellement le processus d'automatisation :

Après chaque incident de sécurité, le responsable de sécurité examine ce qui a fonctionné et ce qui n'a pas fonctionné, et affine les processus. Progressivement, il identifie les étapes qui peuvent être facilement automatisées à l'aide de la plateforme de réponse aux incidents et des outils intégrés. Au fur et à mesure de l'automatisation des étapes, il est recommandé de surveiller les processus pertinents pour voir qu'ils s'exécutent comme prévu et que les incidents sont efficacement atténués.

5. Développer des modelés de réponses automatisées matures :

Finalement, avec de multiples processus de réponse aux incidents éprouvés et avec un haut degré d'automatisation, le système peut atteindre un haut niveau de maturité. C'est le temps convenable pour créer des modèles de réponses pour des incidents spécifiques, permettant aux analystes de partir d'un modèle et de le personnaliser pour un nouveau type d'incident de sécurité. Cela permet de réutiliser les procédures courantes pour concevoir une réponse efficace et automatisée à tous les incidents courants auxquels le réseau est confrontée.



CHAPITRE 2

Automatiser la réponse aux incidents

1. Processus à mettre en place
2. **Technologies d'automatisation**



02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Les critères pour mieux choisir les technologies d'automatisation

- Maintenant que l'automatisation de la réponse aux incidents a été mise en place, il est très important de garder quelques points à l'esprit avant de choisir les outils appropriés pour le processus d'automatisation.
- Les considérations ci-dessous sont importantes lors du choix des technologies ou des outils de réponse automatisée aux incidents :
 - ✓ Il est important de déterminer la partie du processus qui doit être automatisée. Bien qu'il existe plusieurs outils d'automatisation disponibles, ces outils sont destinés à un objectif spécifique. Peu de ces outils sont utiles lorsque des données doivent être recueillies et analysées, tandis que d'autres outils se chargent d'automatiser l'ensemble du processus de réponse.
 - ✓ S'assurer que l'équipe de sécurité possède les compétences nécessaires pour utiliser ces outils efficacement le plus rapidement possible. Il existe quelques outils, par exemple SANS SIFT, outil extrêmement puissant mais qui nécessite également une connaissance approfondie des principes de la criminalistique.
 - ✓ Il est aussi indispensable de penser au déploiement de ces outils. Il y a l'opportunité d'installer l'outil sur un serveur ou une machine particulière et s'il est nécessaire de déployer des outils supplémentaires, ce qui directement le coût de la solution complète.

02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation

- Choisir le meilleur outil est un défi pour de nombreuses responsables de sécurité. Pour trouver la bonne solution, ci-dessous deux listes d'outils de réponse aux incidents pour identifier, prévenir et répondre aux diverses menaces et attaques de sécurité.
- La première liste contient quelques outils gratuits pour automatiser la réponse aux incidents mais sont limités. Alors que la deuxième liste illustre des outils payants, plus performants et qui sont utilisés par les experts de sécurité.

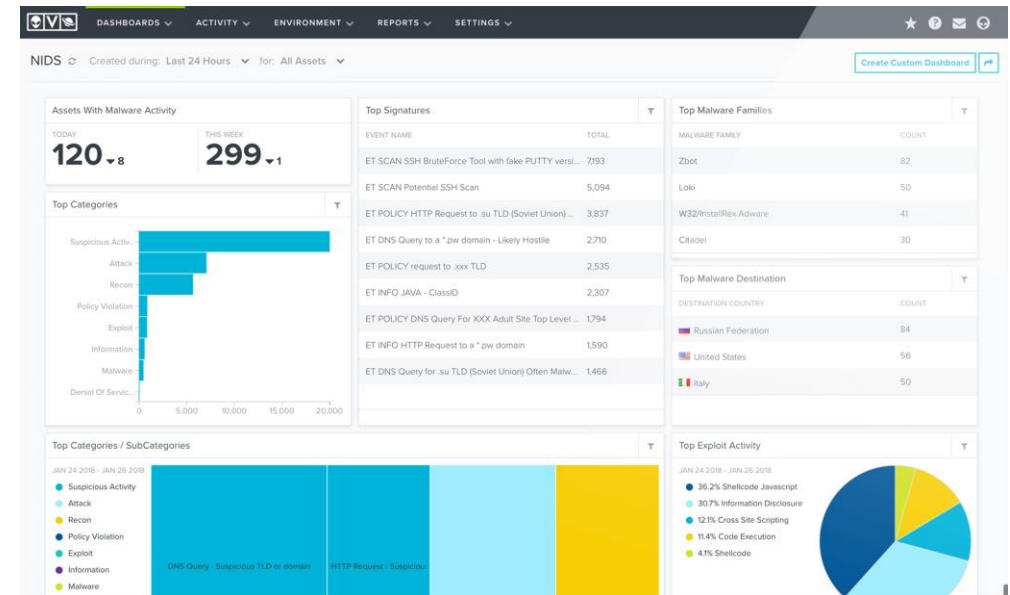
Liste des d'outils de réponse aux incidents gratuits :



est un système open source de gestion des informations et des événements de sécurité (SIEM) qui se connecte aux outils de sécurité et aux systèmes informatiques d'une organisation, rassemble les événements et les données liés à la sécurité et aide les équipes de sécurité à les comprendre pour identifier les incidents de sécurité.

Il permet de faire l'évaluation des vulnérabilités, la détection des intrusions basée sur les données d'événements, l'analyse comportementale et les règles de corrélation des événements.

Site officiel : <https://otx.alienvault.com/>



02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation



Développé par des chercheurs en sécurité de Google, est un framework de réponse aux incidents axé sur la criminalistique en direct à distance.

L'objectif de GRR est de prendre en charge la criminalistique et les enquêtes de manière rapide et évolutive pour permettre aux analystes de trier rapidement les attaques et d'effectuer des analyses à distance.

L'ensemble d'outils comprend des fonctionnalités d'automatisation des tâches telles que la planification automatique des tâches récurrentes. Il fournit des scripts intégrés via une console Python. GRR peut être déployé à grande échelle sur un grand nombre de nœuds.

The screenshot displays the GRR Response Rig interface. On the left, there is a navigation pane with a file system tree showing folders like 'analysis', 'devices', 'memory', 'fs', 'os', 'registry', and 'stats'. The main area shows a table of files with columns for 'Icon', 'Name', 'type', 'size', 'stat_st_size', 'stat_st_mtime', 'stat_st_ctime', and 'Age'. Below the table, there is a 'HexView' section showing the raw hex data of a file, with a search bar and a 'Stats' button.

Icon	Name	type	size	stat_st_size	stat_st_mtime	stat_st_ctime	Age
	\$Recycle Bin	VFSDirectory	0	0	2013-11-14 07:12:36	2008-01-19 10:10:32	2013-11-15 06:32:53
	BOOTSECT.BAK	VFSBiobImage	8192	8192	2009-11-13 12:23:33	2009-11-13 12:23:33	2013-11-18 07:36:16
	Boot	VFSDirectory	0	4096	2009-11-13 12:23:33	2009-11-13 12:23:32	2013-11-15 07:00:31
	Documents and Settings	VFSDirectory	0	0	2012-02-26 02:42:25	2012-02-26 02:42:25	2013-11-15 06:32:53
	PerfLogs	VFSDirectory	0	0	2008-01-19 10:11:20	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files	VFSDirectory	0	4096	2012-12-08 18:33:14	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files (x86)	VFSDirectory	0	4096	2013-09-10 22:43:30	2008-01-19 10:11:20	2013-11-15 06:32:53
	ProgramData	VFSDirectory	0	4096	2012-12-08 18:36:21	2008-01-19 10:11:20	2013-11-15 06:32:53
	System Volume Information	VFSDirectory	0	0	2012-02-26 02:44:46	2012-02-26 02:39:31	2013-11-15 06:32:53
	Users	VFSDirectory	0	4096	2013-11-14 07:12:15	2008-01-19 10:11:20	2013-11-15 06:32:53
	Windows	VFSDirectory	0	16384	2013-11-14 07:06:16	2008-01-19 10:11:21	2013-11-15 06:32:53
	bootmgr	VFSFile	0	333257	2009-04-11 16:13:10	2009-11-13 12:23:33	2013-11-15 06:32:53
	hiberfil.sys	VFSFile	0	644472832	2013-11-14 07:04:20	2013-11-14 06:54:13	2013-11-15 06:32:53

Site officiel: <https://grr-doc.readthedocs.io/en/latest/>

02 – Automatiser la réponse aux incidents

Technologies d'automatisation



WEBFORCE
BE THE CHANGE

Technologies d'automatisation

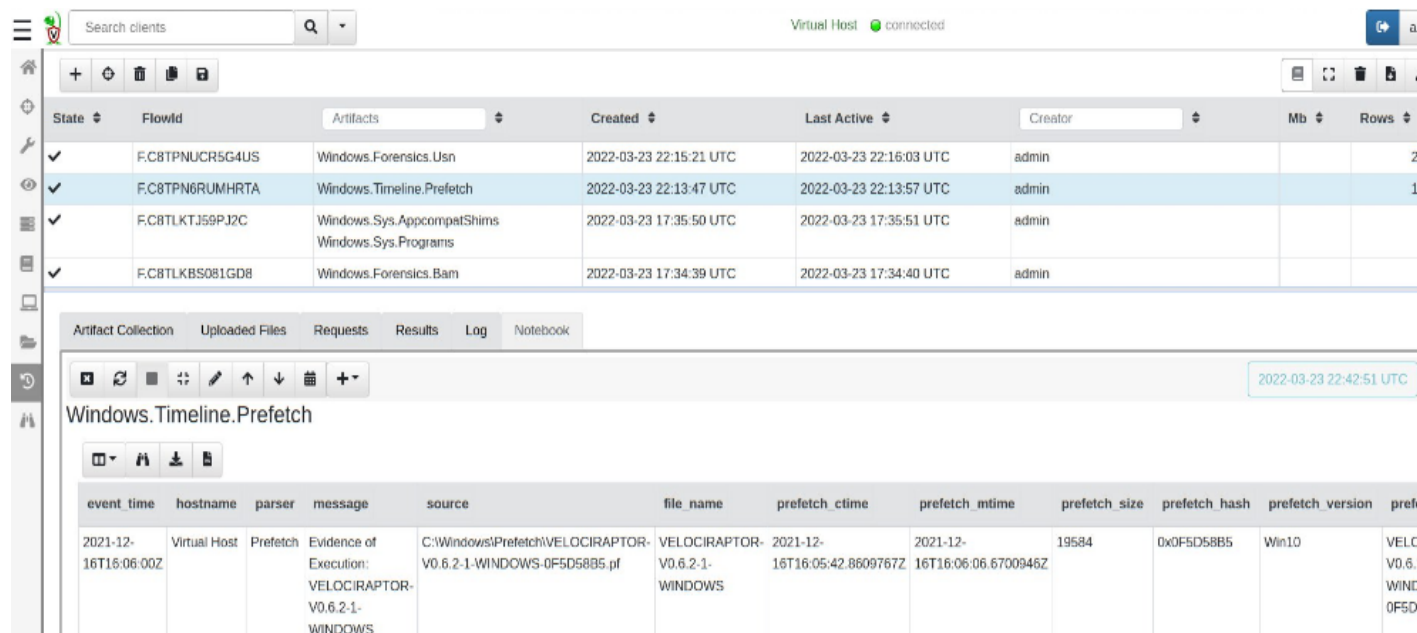
Velociraptor :  **Velociraptor**

est un plateforme open-source avancée de surveillance des terminaux, de criminalistique numérique. C'est un outil qui permet de collecter des informations d'état basées sur l'hôte à l'aide des requêtes Velociraptor Query Language (VQL).

Il a été développé par des professionnels de la criminalistique numérique et de la réponse aux incidents (DFIR) qui avaient besoin d'un moyen puissant et efficace pour rechercher des artefacts spécifiques et surveiller les activités sur des flottes de terminaux.

Il offre la possibilité de répondre plus efficacement à un large éventail d'enquêtes de criminalistique numérique et de réponse aux incidents cybernétiques et aux violations de données comme : chercher des preuves d'adversaires sophistiqués, enquêter sur les traces de logiciels malveillants, et recueillir des données sur les terminaux au fil du temps pour les utiliser dans la chasse aux menaces et les enquêtes futures.

Site officiel : <https://docs.velociraptor.app/>



The screenshot displays the Velociraptor web interface. At the top, there is a search bar for clients and a status indicator for a 'Virtual Host' which is 'connected'. Below this is a table listing artifacts with columns for State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows. The table contains four rows of data, all with a state of 'checked'.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.C8TPNUCR5G4US	Windows.Forensics.Usn	2022-03-23 22:15:21 UTC	2022-03-23 22:16:03 UTC	admin		295
✓	F.C8TPN6RUMHRTA	Windows.Timeline.Prefetch	2022-03-23 22:13:47 UTC	2022-03-23 22:13:57 UTC	admin		163
✓	F.C8TLKJ59PJ2C	Windows.Sys.AppcompatShims Windows.Sys.Programs	2022-03-23 17:35:50 UTC	2022-03-23 17:35:51 UTC	admin		6
✓	F.C8TLKBS081GD8	Windows.Forensics.Bam	2022-03-23 17:34:39 UTC	2022-03-23 17:34:40 UTC	admin		3

Below the table, there are tabs for 'Artifact Collection', 'Uploaded Files', 'Requests', 'Results', 'Log', and 'Notebook'. The 'Results' tab is active, showing a detailed view of the 'Windows.Timeline.Prefetch' artifact. This view includes a table with columns for event time, hostname, parser, message, source, file name, prefetch_ctime, prefetch_mtime, prefetch_size, prefetch_hash, prefetch_version, and prefetch.

event time	hostname	parser	message	source	file name	prefetch_ctime	prefetch_mtime	prefetch_size	prefetch_hash	prefetch_version	prefetch
2021-12-16T16:06:00Z	Virtual Host	Prefetch	Evidence of Execution: VELOCIRAPTOR-V0.6.2-1-WINDOWS	C:\Windows\Prefetch\VELOCIRAPTOR-V0.6.2-1-WINDOWS-0F5D58B5.pf	VELOCIRAPTOR-V0.6.2-1-WINDOWS	2021-12-16T16:05:42.8609767Z	2021-12-16T16:06:06.6700946Z	19584	0x0F5D58B5	Win10	VELO V0.6.2 WIND 0F5D5

02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation

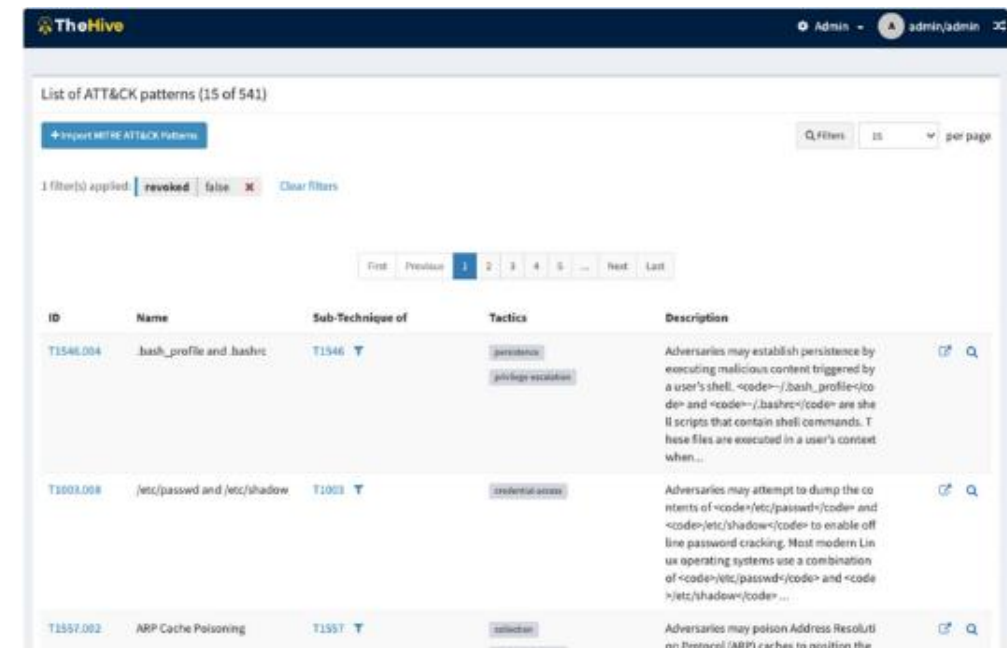
TheHive :  **TheHive**

est d'un système de management du centre des opérations de sécurité (SOC) qui permet aux équipes de collaborer pour effectuer des recherches de qualité, et enquêter sur les incidents de sécurité de qualité et en temps opportun .

Chaque recherche correspond à un scénario, qui peut être décomposé en un ou plusieurs métiers. Ces tâches sont revendiquées par les analystes de sécurité du SOC, qui les examinent simultanément.

TheHive peut également s'intégrer aux systèmes de messagerie électronique, de gestion des informations et des événements de sécurité (SIEM) et à d'autres sources via une API Python.

Site officiel : <https://thehive-project.org/>



Attck Pattern management page

02 – Automatiser la réponse aux incidents

Technologies d'automatisation

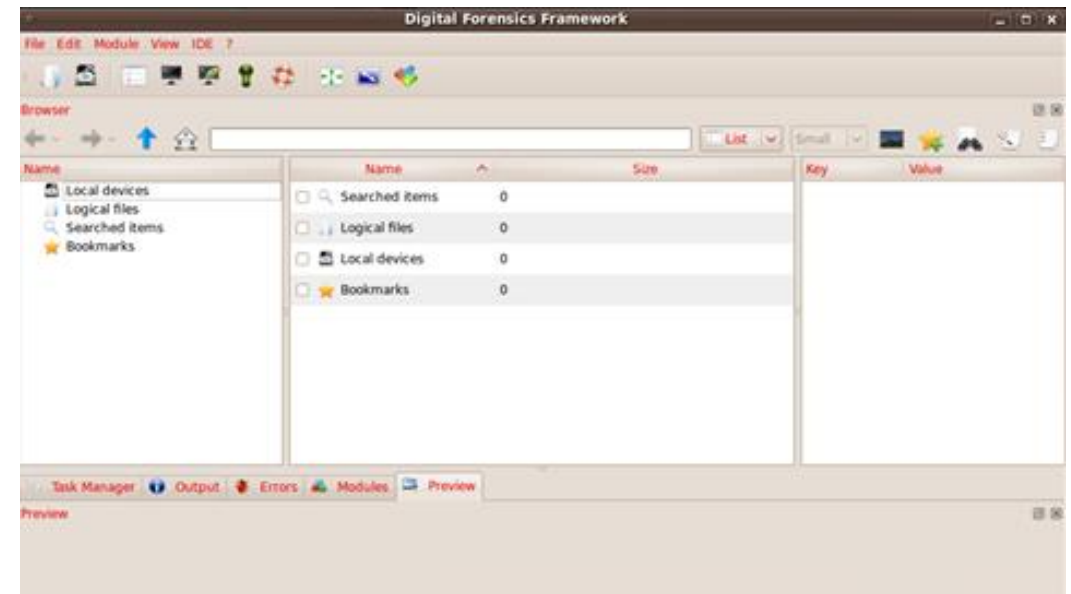
Technologies d'automatisation

SANS Investigative Forensic Toolkit (SIFT) : 

est un outil open source de réponse aux incidents et de criminalistique créée pour fonctionner sur divers paramètres de criminalistique numérique. À l'origine, il est créé par Rob Lee en 2007 pour prendre en charge l'analyse médico-légale dans la classe SANS FOR508.

Il fournit des fonctionnalités telles que la création d'une chronologie à partir des journaux système, la sculpture de fichiers pour extraire des preuves spécifiques et l'analyse de la corbeille.

Il peut être installé sur Linux et Windows.



Site officiel : <https://www.sans.org/tools/sift-workstation/>

02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation

Liste des d'outils de réponse aux incidents payants :

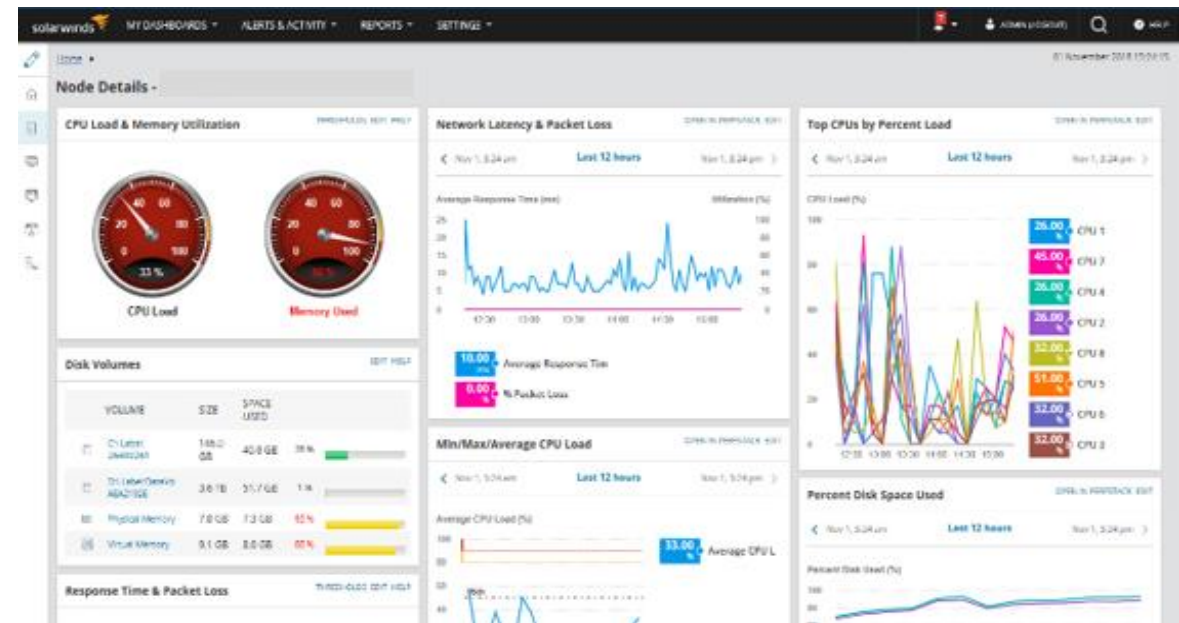
SolarWinds : 

offre à la fois des outils de réponse aux incidents ainsi qu'une résolution et une prévention automatisées.

Bien qu'il soit appelé Security Event Manager (SEM), cet outil est un Security Information Manager (SIM). Il recherche dans les fichiers journaux pour identifier une éventuelle activité malveillante.

Malheureusement, cet outil avancé est conçu pour les professionnels. Par conséquent, il nécessite du temps pour bien maîtriser la plateforme.

Site officiel : <https://www.solarwinds.com/fr/>



02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation

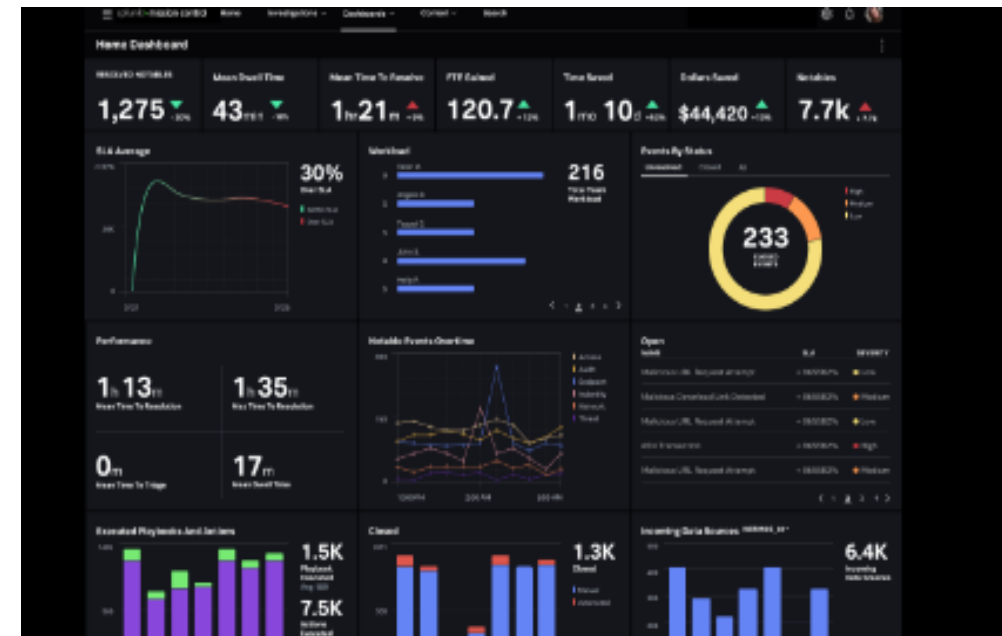
Splunk Phantom : 

est un système de Orchestration, d'automatisation et de réponse aux incidents (SOAR). Il fait partie d'une plate-forme plus large appelée Splunk. La réponse automatisée aux incidents est incluse dans la fonctionnalité Splunk Phantom.

Il contient des processus automatisés qui créent des chaînes d'activités pour détecter les anomalies en déployant une sélection d'outils disponibles.

Les flux de travail incluent des branchements conditionnels qui peuvent conduire au lancement d'actions d'atténuation. Ils peuvent être lancés manuellement ou configurés pour s'exécuter en boucle en continu, à la recherche de problèmes.

Site officiel : https://www.splunk.com/fr_fr?301=/fr_fr.html



02 – Automatiser la réponse aux incidents

Technologies d'automatisation



Technologies d'automatisation

LogRhythm NextGen SIEM : 

est une Platform qui fournit des services pour détecter et arrêter les menaces de sécurité.

Le système comprend des outils de surveillance en direct qui fournissent un service supplémentaire aux utilisateurs tout en collectant des informations pour alimenter le systèmes de gestion des événements et des informations de sécurité (SIEM).

Il s'agit de NetMon pour la surveillance du réseau et de SysMon pour la surveillance des terminaux. SysMon rassemble également les messages de journal à télécharger sur le serveur LogRhythm. Le serveur de journaux de réception s'appelle AnalytiX.

Site officiel : <https://logrhythm.com/solutions/security/siem/>

