Sécurité des Systèmes d'Information

Gestion des incidents de sécurité

ECE PARIS
ÉCOLE D'INGÉNIEURS

Sommaire

- Contexte
- Organisation de la gestion des incidents SSI
- Processus de gestion des incidents
- Principes de base
- Exemple d’investigation numérique
- Etapes de réponse à incident

Contexte

APT (Advanced Persistent Threat)

- **Stuxnet** utilise 4 *0-days :*
  - ✓ CVE-2010-2568 exécution d'un code arbitraire lorsque l'utilisateur affiche l'icône du raccourci (fichier .LNK sur la clef USB)
  - ✓ CVE-2010-2729 vulnérabilité dans le spouleur d'impression signé par un certificat valide permettant d'exécuter du code à distance sans authentification

  - ✓ CVE-2010-2772 accès avec des privilèges élevés à des composants d'un système SCADA Siemens (Simatic WinCC et PCS 7)
  - ✓ CVE-2010-3338 élévation de privilèges au sein du planificateur de tâches

Contexte

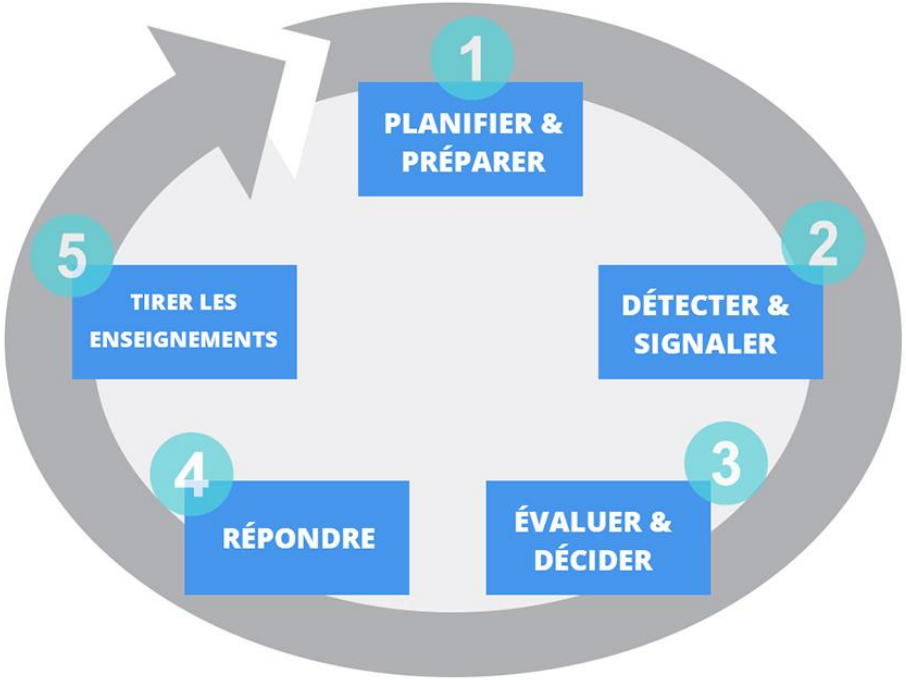
Wannacry (mai 2017)

- Ransomware visant les systèmes Windows
  - ✓ Infection de plus de 300 000 ordinateurs dans 150 pays
  - ✓ Se propage en utilisant EthernalBlue (exploit du protocole SMB Windows) développé par la NSA (National Security Agency) et volé puis diffusé par les Shadow Brokers en avril 2017

  - ✓ C'est un **ver réseau** car il inclut un mécanisme de "transport" pour se propager sur des ordinateurs aléatoirement sur tous les réseaux (local ou Internet)
  - ✓ Renault a été infecté et a dû stopper la production dans de nombreuses usines pour isoler et nettoyer les ordinateurs infectés
  - ✓ Le lendemain suivant l'attaque initiale au mois de mai, Microsoft a sorti un patch d'urgence pour les produits en fin de vie (Windows XP, Windows Server 2003 et Windows 8)

Organisation de la gestion des incidents

- **Objectifs d'une politique de gestion des incidents :**
  - Garantir que le **mode de notification** des incidents permet de réaliser une **correction dans les meilleurs délais**
  - Garantir une **approche cohérente et efficace** pour le traitement des incidents



ECE PARIS ÉCOLE D'INGÉNIEURS

Organisation de la gestion des incidents

- **Moyens pour atteindre ces objectifs :**
  - **Procédures** de signalement, de remontée d'informations et de réponses
  - **Sensibilisation** des utilisateurs des points d'entrée pour le signalement et de leur obligation de signaler tout événement dans les meilleurs délais
  - Le mécanisme de **signalement** doit être le plus **simple**, le plus accessible et le plus disponible possible
  - Mettre en place une **surveillance** des systèmes, des alertes et des vulnérabilités pour détecter les incidents
  - Définir des **priorités** de traitement des incidents
  - Evaluer les incidents après résolution pour **améliorer** les mesures existantes
  - Définir une **procédure** permettant de collecter les éléments de preuve en cas d'action en justice

Organisation de la gestion des incidents

Organisation

- Equipe dédiée à la gestion des incidents
  - ✓ **CERT** (Computer Emergency Response Team)
  - ✓ **CSIRT** (Computer Security Incident Response Team)
- Peut être centralisée, distribuée ou externalisée
- Doit être **visible** en interne et en externe pour être contactée rapidement
- Doit avoir la **légitimité** nécessaire pour pouvoir agir rapidement
- Un **SOC** (Security Operation Center) est une équipe de surveillance des systèmes d'information (sites Web, applications, bases de données, serveurs, réseaux, postes de travail…)
  - ✓ Permet de détecter des anomalies et créer des incidents de sécurité

Organisation de la gestion des incidents

Objectifs de l'équipe de gestion des incidents

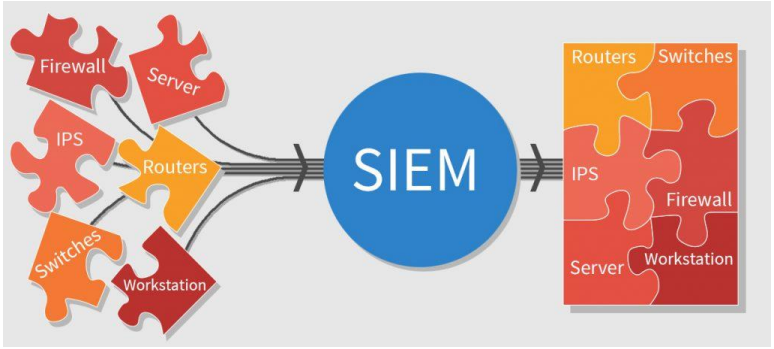
- Rationalisation de la **veille**
- **Traiter** rapidement tout type **d'incident** de sécurité par du personnel qualifié et avec des procédures éprouvées
- Avoir une vue du **risque** d'exposition de l'organisation

Compétences

- Techniques (analyser l'incident et identifier les contre-mesures)
- Connaissance du contexte et des enjeux métier
- Rédactionnelle (formaliser les actions entreprises)
- Aisance relationnelle (échanger avec les acteurs en adaptant le discours)

Outil de détection

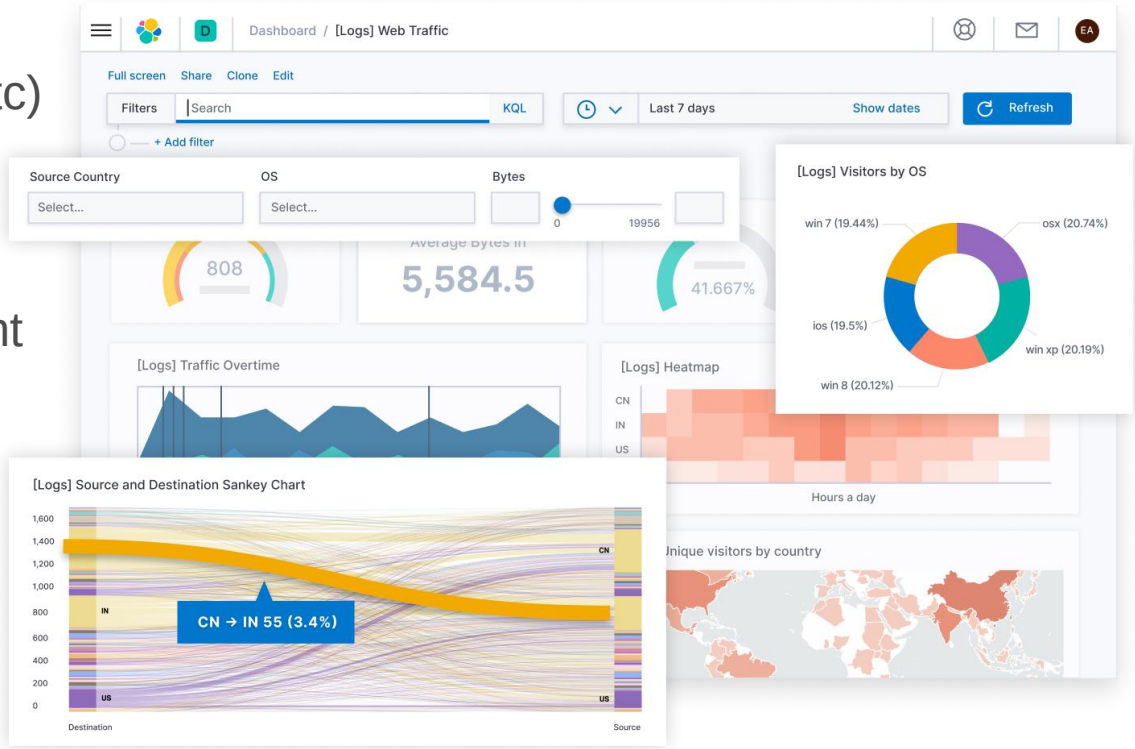
- **Le SOC est généralement équipé d'un SIEM (Security Information and Event Management) pour l'analyse en tant réel des événements de sécurité**
  - Permet de surveiller des applications, des comportements utilisateurs et des accès aux données
  - Analyse les données des événements issus des machines, systèmes et applications :
    - ✓ Pare-feux
    - ✓ IDS/IPS
    - ✓ Equipements réseau
    - ✓ Annuaires (AD), IAM
    - ✓ Serveurs (Système, applications et bases de données)
    - ✓ etc



SIEM

Les fonctions du SIEM sont :

- Collecte (syslog, SNMP, journaux d'événements, etc)
- Normalisation (structuration des logs)
- Agrégation (enrichissement avec d'autres données)
- Corrélation (lien entre les événements ayant lieu sur des éléments différents du SI) pour créer des alertes



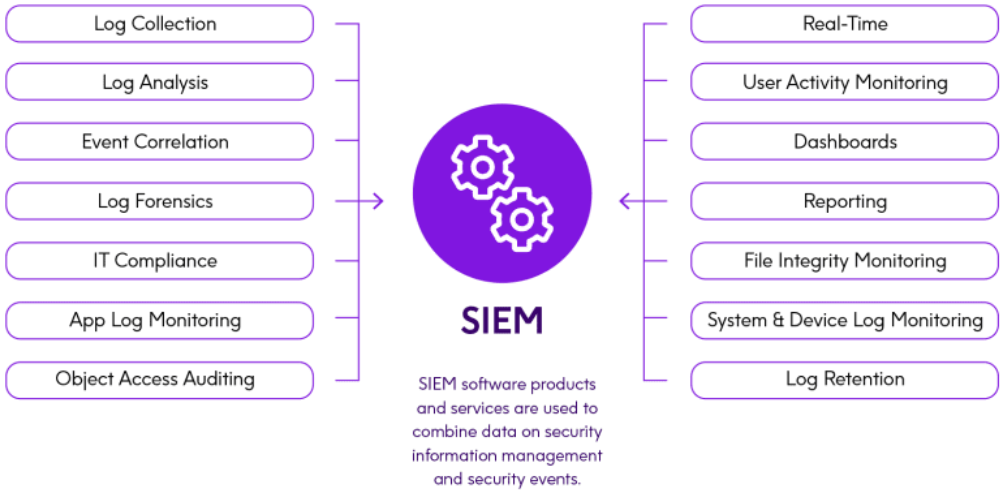
- ✓ Définition des comportements anormaux (difficulté pour ne pas avoir trop d'alertes)

- Rapports (tableaux de bord, conformité)

SIEM

Le principe du SIEM est :

- L'agrégation de données pertinentes provenant de sources différentes
- Identifier les écarts par rapport à la moyenne/norme
- Générer une alerte



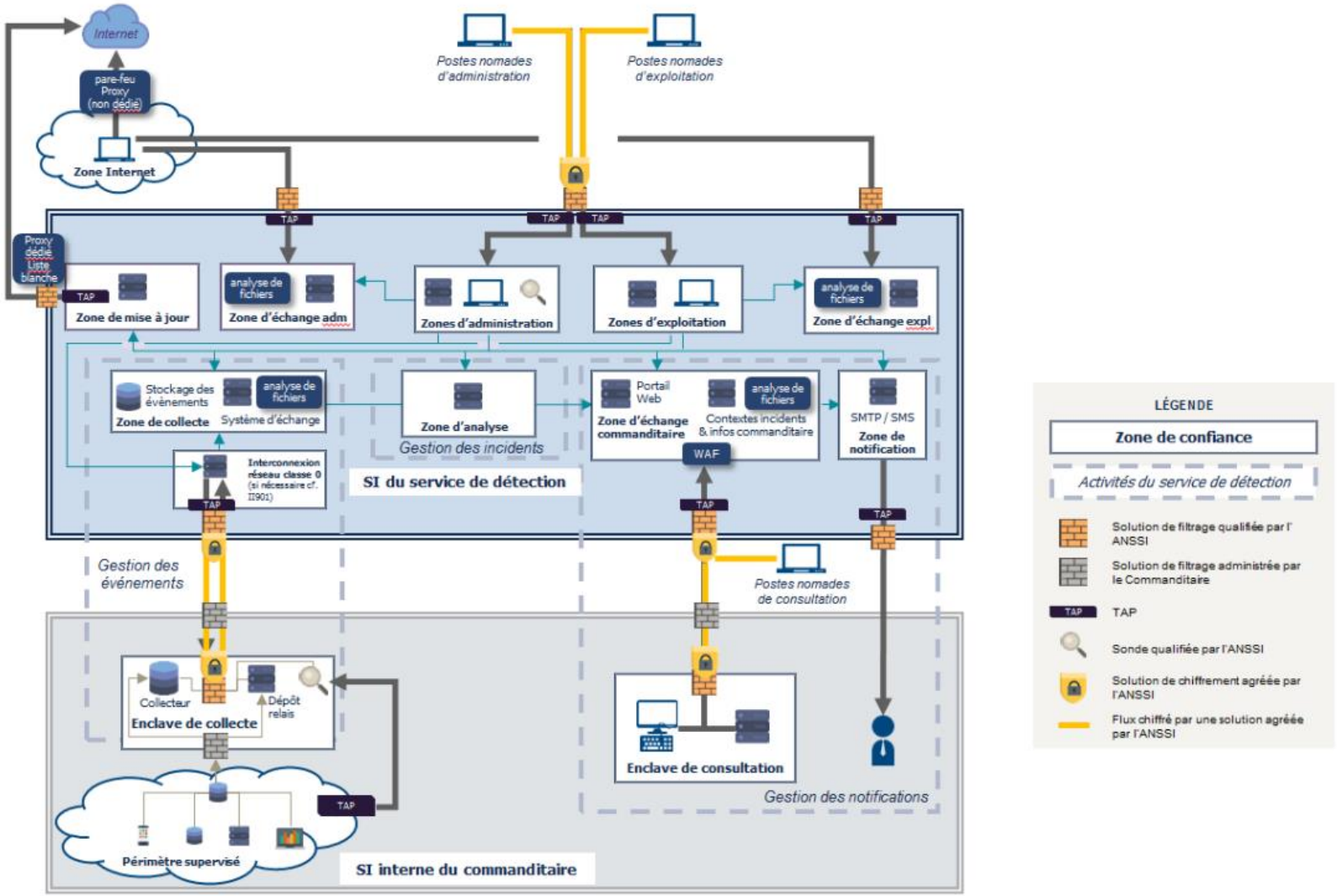
Le SIEM peut être basé sur :

- Des règles statiques définissant les comportements anormaux
- **L'analyse du comportement** des utilisateurs et des entités (UEBA) : utilisation de machine learning pour établir des bases de référence pour chaque entité particulière (utilisateur, document, page web, etc)
- **L'orchestration** de la sécurité et la **réponse automatisée** (SOAR) : réaction aux incidents de sécurité sans intervention humaine

Détection des incidents de sécurité

- **Le service de détection des incidents de sécurité est composé de 3 activités :**
  - Gestion des **évènements** : moyens assurant le **recueil** et le **stockage** des évènements de sécurité
  - Gestion des **incidents** : moyens permettant **d'identifier** et de **qualifier** un incident de sécurité sur la base **d'évènements** collectés
  - Gestion des **notifications** : moyens permettant **d'informer** le commanditaire sur les **incidents de sécurité** détectés et de stocker ces notifications

Exemple d'architecture de collecte



Source : ANSSI

Qualification des incidents de sécurité

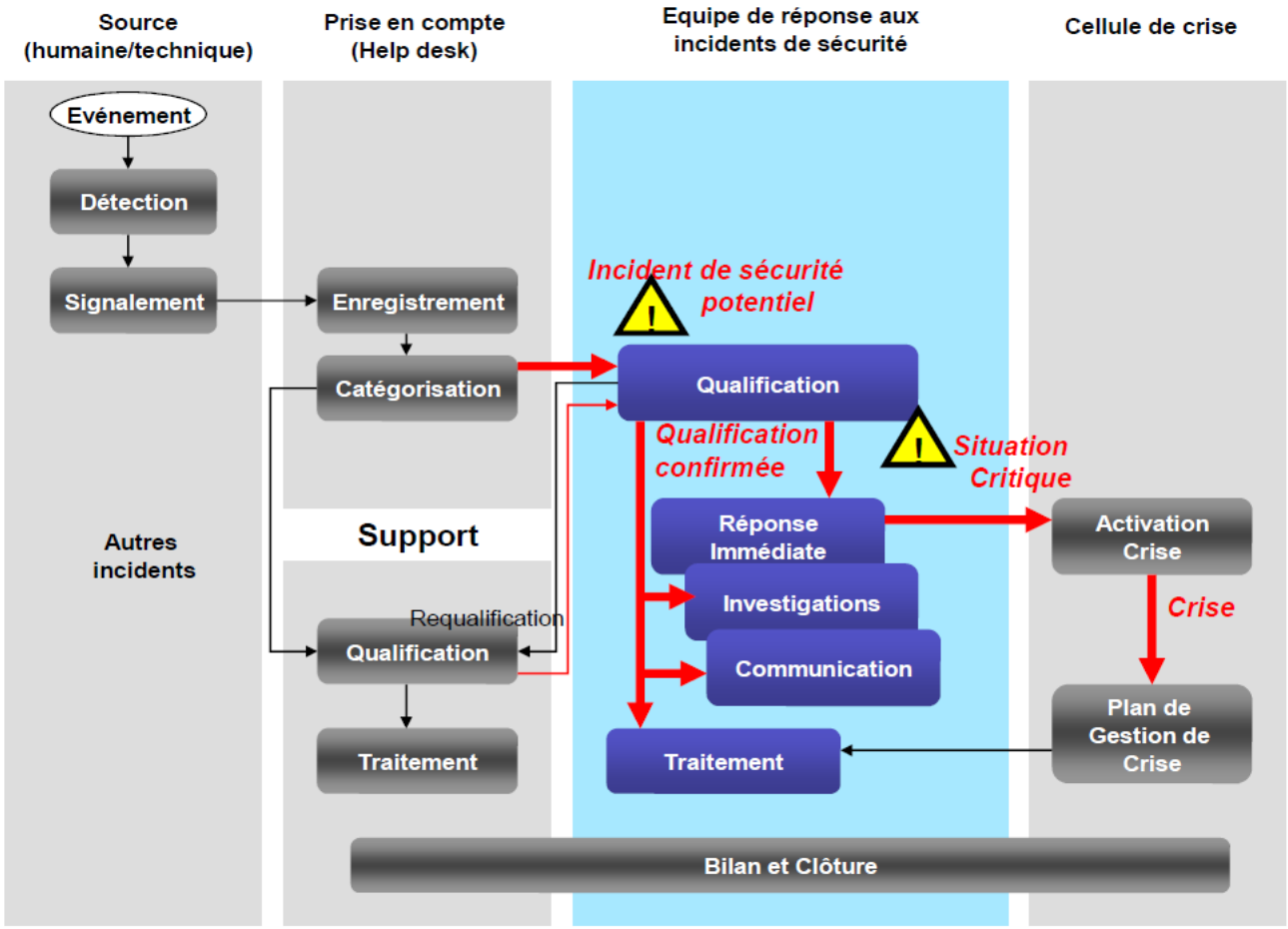
Qualification d'un incident de sécurité

- Réaliser des recherches à partir d'informations collectées ou issues des analyses
  - ✓ Empreintes cryptographiques,
  - ✓ Noms de fichiers ou de codes malveillants,
  - ✓ Chaînes de caractères contenues dans des codes malveillants,
  - ✓ Noms de domaines et adresses IP,
  - ✓ Etc.
- Utiliser des bases d'informations internes (bases RIPE, plateformes antivirales hors ligne, bases de résolution DNS, etc.) pour **limiter au maximum les recherches sur internet**
- Déterminer **la nature et la gravité** de l'incident de sécurité

Détection des incidents de sécurité

- Chaque incident de sécurité **détecté** fait l'objet d'un **ticket d'incident** de sécurité :
  - ✓ **Date de création du ticket** et des différentes opérations réalisées sur celui-ci (**traçabilité des actions**)
  - ✓ **Date et heure de la détection** de l'incident de sécurité
  - ✓ **Date effective de l'évènement** ou des évènements ayant donné lieu à l'incident de sécurité
  - ✓ **Description** de l'incident de sécurité
  - ✓ **Gravité** de l'incident de sécurité
  - ✓ **Description de l'impact** de l'incident de sécurité pour le commanditaire
  - ✓ Identifiants et numéros de version des **règles de détection déclenchées** (contient un ou plusieurs évènements)
  - ✓ **Equipements** ayant généré et collecté les évènements de l'incident
  - ✓ Identifiants des **évènements** ayant permis la détection de l'incident
  - ✓ **Risque** induit par l'incident

Processus de traitement des incidents



Source : Clusif

Gestion des incidents

Détection et signalement

- Toute personne qui a connaissance d'une anomalie

Prise en compte

- Enregistrement de l'incident
- Catégorisation par une équipe de support (fiches par type d'incident)
- Qualification par l'équipe de réponse aux incidents de sécurité

Gestion des incidents

Réponse à l'incident SSI

- Mesures de réponses immédiates
  - ✓ Confinement
  - ✓ Préservation des traces
- Investigations
  - ✓ Nature
  - ✓ Fait générateur
  - ✓ Périmètre concerné
  - ✓ Impact

Gestion des incidents

- Traitement
  - ✓ Mesure pour **éviter l'aggravation** des conséquences (restrictions temporaires et communications ciblées)
  - ✓ Déclarations aux **assurances**
  - ✓ **Résolution** de l'incident (réservation de ressources externes si nécessaire puis réparation ou réinstallation/restauration)
- Revues post-incident
  - ✓ Investigation post-incident (investigations complémentaires pour **comprendre l'origine de l'incident** ou collecte de preuve pour un tribunal)
  - ✓ Rapport de synthèse (éléments techniques, bilan des processus, bilan financier) → alimente une base de connaissance pour **amélioration continue**

Gestion des incidents

- Actions post-incident
  - ✓ Bilan de l'incident adressé aux directions et contenant un plan d'actions
  - ✓ Recours pénal (réunir les faits de manière chronologique, la liste des préjudices subis, les éléments de preuve collectés)
  - ✓ Révision des contrats (assurance ou fournisseur)
  - ✓ Communication interne (sensibilisation)

- **Les enseignements tirés du traitement des incidents de sécurité doivent contribuer à l'amélioration générale des processus**

Principes de base

- **Conserver une copie hors ligne des documents de gestion d'incident**

- **Réaliser des sauvegardes « déconnectées » du système d'information**

- **Conserver les journaux pendant au moins 6 mois**

- **Tenir à jour le plan de réponse en cas d'incident de sécurité**
  - Prendre en compte tous les aspects juridiques lors de la gestion d'un incident de sécurité

- **Documenter chaque étape de l'incident de sécurité**

Exemple d'investigation numérique

- **Observation de ralentissements sur certains serveurs**
  - Détermination de l'étendue du problème
    - ✓ Le problème semble ne concerner qu'un serveur frontal et son serveur de maintenance
  - Récupération des informations
    - ✓ Logs systèmes et réseau, diagrammes de topologie réseau, images systèmes, rapports d'analyse du trafic réseau…
    - ✓ Ne pas éteindre les systèmes → récupération de la mémoire vive
  - Investigations pour identifier quels systèmes, comptes et données ont été compromis
  - Mise en œuvre de mesures correctrices

Exemple d'investigation numérique

Analyses réalisables sur le système

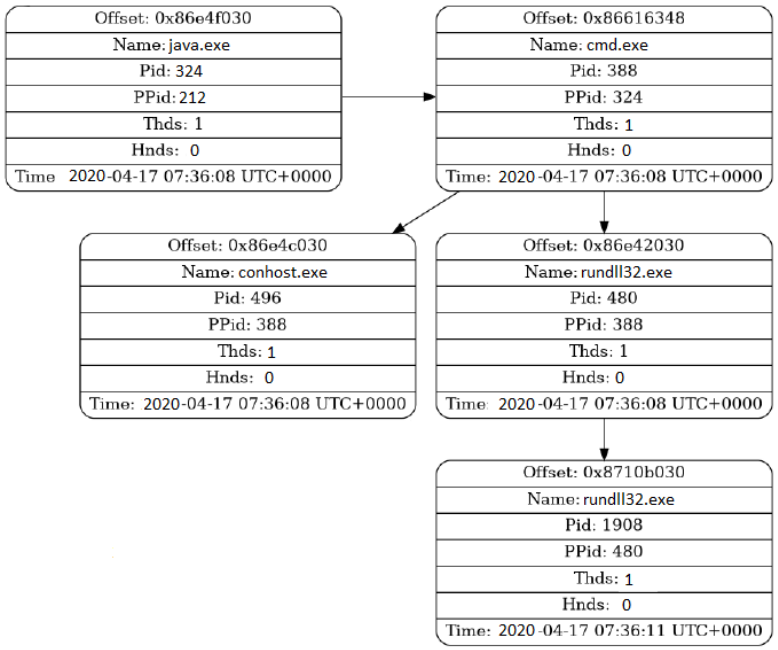
- Analyse du disque dur
  - ✓ Difficulté : grande quantité de données à copier (centaines de Go) pour l'analyse -> nécessite beaucoup de temps

- Analyse de la mémoire vive
  - ✓ Taille plus faible (16 à 32Go) → rapide à copier
  - ✓ Contient l'ensemble des processus en cours d'exécution, les connexions réseau, certaines clés de registre, des mots de passe
  - ✓ Permet de démarrer l'analyse des indicateurs de compromission tout en travaillant à l'obtention d'une image du disque dur

Exemple d'investigation numérique

Analyse de la mémoire vive

- Acquisition de la mémoire vive avec DumpIt ou WinPMEM
- Analyse de la mémoire avec Volatility ou Rekall
  1. Identification du profil (imageinfo)
  2. Lister les processus en mémoire à la recherche d'incohérences (pstree)



- Processus fils de java.exe anormaux (cmd.exe et rundll32.exe)
- Analyse de la mémoire de ces processus

Exemple d'investigation numérique

3. Utilisation du plugin malfind pour rechercher une injection de code malveillant et extractions des sections mémoire pour les analyser plus en détail

```
$ volatility -f memdump.vmem malfind -p 1908

Process: rundll32.exe Pid: 1908 Address: 0x1600000 Vad Tag: VadS Protection:
PAGE_EXECUTE_READWRITE Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1,
Protection: 6

0x01600000 4d 5a e8 00 00 00 00 d7 30 7b b8 91 00 00 00 e9 MZ......0{......
```

4. Scan des fichiers extraits pour mettre en évidence les logiciels malveillants

```
$ clamscan *

Process.0x8710b030.0x1600000.dmp : Win.Tool.MeterPreter-6294292-0 FOUND
```

- L'analyse de Clamav confirme que le processus rundll32.exe comporte un implant meterpreter

Exemple d'investigation numérique

5. Analyse des connexions réseau (netscan)

```
$ volatility -f memdump.vmem netscan

Volatility Foundation Volatility Framework 2.4
Offset(P)  Proto    Local Address                Foreign Address      State          Pid      Owner          Created
[...]
0x1121b7b0 TCPv4    192.168.205.186:8080         192.168.205.180:35132 CLOSED        324      java.exe       2020-04-17 07:34:12
0xfc13770  TCPv4    192.168.205.186:49154        192.168.205.180:445  CLOSED         4        System         2020-04-17 07:34:42
0x17f35240 TCPv4    192.168.205.186:49158        192.168.205.180:443  CLOSED         1908     rundll32.exe   2020-04-17 07:36:24
[...]
```

- La 1ère connexion (java.exe) est la trace de la connexion de l'attaquant à l'application web hébergée sur le serveur
- La 2ème connexion (system) correspond au chargement de la dll par rundll32 sur un partage réseau mis en place par l'attaquant
- La 3ème connexion (rundll32) correspond à l'exécution d'un reverse shell utilisant l'implant meterpreter

Exemple d'investigation numérique

5. Analyse des droits obtenus sur le système (getsids)

```
$ volatility -f memdump.vmem getsids –p 1908

rundll32.exe (1908): S-1-5-18 (Local System)
rundll32.exe (1908): S-1-5-32-544 (Administrators)
rundll32.exe (1908): S-1-1-0 (Everyone)
```

- Le processus avait les droits System, appartenant au groupe Administrators

Conclusion

- Une vulnérabilité de l'application web a permis le déploiement d'un applet java qui a récupéré une DLL chez l'attaquant permettant la création d'un reverse shell

Investigation numérique légale

Investigation numérique légale (*computer forensics*)

- Protocoles d'investigation numériques **respectant les procédures légales** et destinée à **apporter des preuves numériques** à la demande d'une institution judiciaire par réquisition, ordonnance ou jugement
- Les données ne doivent **surtout pas être modifiées** lors d'une acquisition
  - ✓ Copie bit à bit des données à analyser et travail sur une copie de la copie
- Chaîne de contrôle (*chain of custody*) : document permettant **de retracer les accès aux pièces à conviction** et de définir les accréditations permettant ces accès

Etapes de réponse à incident (SANS)

- **SANS (Sysadmin, Audit, Network, Security)**
  - Formations et certifications cybersécurité
    - ✓ Exemple : FOR500 (Windows Forensic Analysis) permettant d'être certifié GCFE (GIAC Certified Forensic Examiner)

- **6 étapes pour le processus de réponse aux incidents**
  - Préparation
  - Identification
  - Cloisonnement
  - Eradication
  - Retour à la normale
  - Retour d'expérience

Etapes de réponse à incident (SANS)

Etape 1 : Préparation

- Politique de sécurité
  - ✓ Définition de l'incident de sécurité
- Plan de réponse aux incidents
  - ✓ Priorisation des incidents en fonction de l'impact pour l'organisation
  - ✓ Description de la manière dont l'équipe gère les incidents
- Communication
  - ✓ Annuaires interne et externe
  - ✓ Notification des autorités (par exemple 72h pour une violation de données personnelles)

Etapes de réponse à incident (SANS)

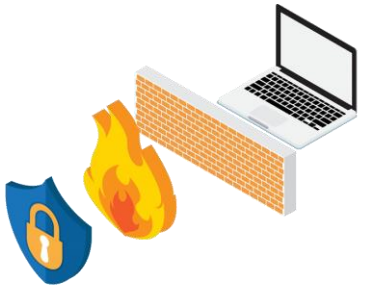
Etape 2 : Identification

- Critère de déclenchement de la réponse
  - ✓ Nécessite de collecter des événements de nombreuses sources
  - ✓ Exemple de critère:
    - Détection de trafic réseau élevé
    - Réception d'un mail de phishing
    - Notification d'une entité externe
    - Disparition d'une clé USB
    - Etc
- Détermination du périmètre de l'incident

Etapes de réponse à incident (SANS)

Etape 3 : Cloisonnement

- Limitation des dégâts et empêchement de survenance de nouveaux dommages
- Cloisonnement à court terme (limitation des dégâts immédiats)
  - ✓ Isolation réseau d'une machine ou d'un ensemble de machines
  - ✓ Sauvegarde des systèmes (permet de garder une image forensic des systèmes affectés avant de réinstaller les systèmes pour une analyse ultérieure)



- Cloisonnement à long terme (remédiation temporaire pour éviter l'interruption de la production)
  - ✓ Suppression des comptes malveillants et/ou backdoors des systèmes
  - ✓ Installation des patches de sécurité

Etapes de réponse à incident (SANS)

Etape 4 : Eradication

- Restauration des systèmes affectés
  - ✓ S'assurer que tout contenu malveillant a bien été nettoyé des systèmes
  - ✓ Généralement, une **réinstallation complète** des systèmes est le seul moyen de s'assurer que tous les contenus malveillants ont été effacés et éviter une réinfection
- Amélioration des défenses après détermination de la cause racine de l'incident et éviter une nouvelle compromission
  - ✓ Mise à jour des systèmes, correction des vulnérabilités, désactivation des services inutilisés

Etapes de réponse à incident (SANS)

Etape 5 : Retour à la normale

- Remise des systèmes en production après avoir vérifié qu'ils sont propres
  - ✓ Test, surveillance, validation des systèmes pour remise en production
- Suppression des outils utilisés pour la réponse à incident
- Empêcher la survenance d'un nouvel incident dû au même problème

Etape 6 : Enseignements tirés

- Objectif : amélioration continue
- Documentation complète de l'incident pour fournir une base de référence dans le cas d'un incident similaire (peut servir de support de formation et de point de comparaison pour des incidents ultérieurs)
- Actualiser le plan de réponse aux incidents

Conclusion

- **La réponse à incident doit être préparée même si tous les incidents sont différents**
  - Exercices de gestion de crise
- **Se découpe en 3 phases :**
  - Observer
  - Analyser les objectifs et les impacts
  - Remédier
- **Le délai moyen écoulé entre une intrusion et sa détection est aujourd'hui de 35 jours (étude 2022)**
  - Temps moyen entre l'accès initial et le déploiement d'un **ransomware** dans le système : minimum 3j pour l'attaque la plus rapide et moyenne 25j