Orange et CNAM Bretagne, Cybersécurité SEC101, eduf@ction
Notes de cours éditées le 10 janvier 2020

Détecter : de la surveillance à l'évènement de sécurité

Eric DUPUIS[1,2]*

Résumé
Ce document donne les fondamentaux de la gestion de la menace et de sa détection. Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document finale unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Évènements, attaques, détection, SIEM, SOC

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

1. Avant propos

Je vous propose d'aborder ce chapitre liée à la surveillance à l'évènement de sécurité par les quelques points fondamentaux de la gestion de la menace.

Après quelques définitions et positionnement dans l'analyse de menace, de la supervision et de l'analyse comportementale nous aborderons les grandes fonctions nécessaire à la DETECTION.

- **VOIR** : capacité de voir et de capter le comportement d'un système d'information via des sources et capteurs avec le *LOG management* (Systèmes et Applicatifs). En n'oubliant pas l'assurance sécurité des Logs
- **COMPRENDRE - PREVOIR** : Avec le *Threat Management* : Veiller, Surveiller la menace, Modélisation et scénarios redoutés
- **DETECTER** : Surveiller le comportement, évènements, anomalies, incidents . . . menace avancée (APT), avec les SIEM et les SOC

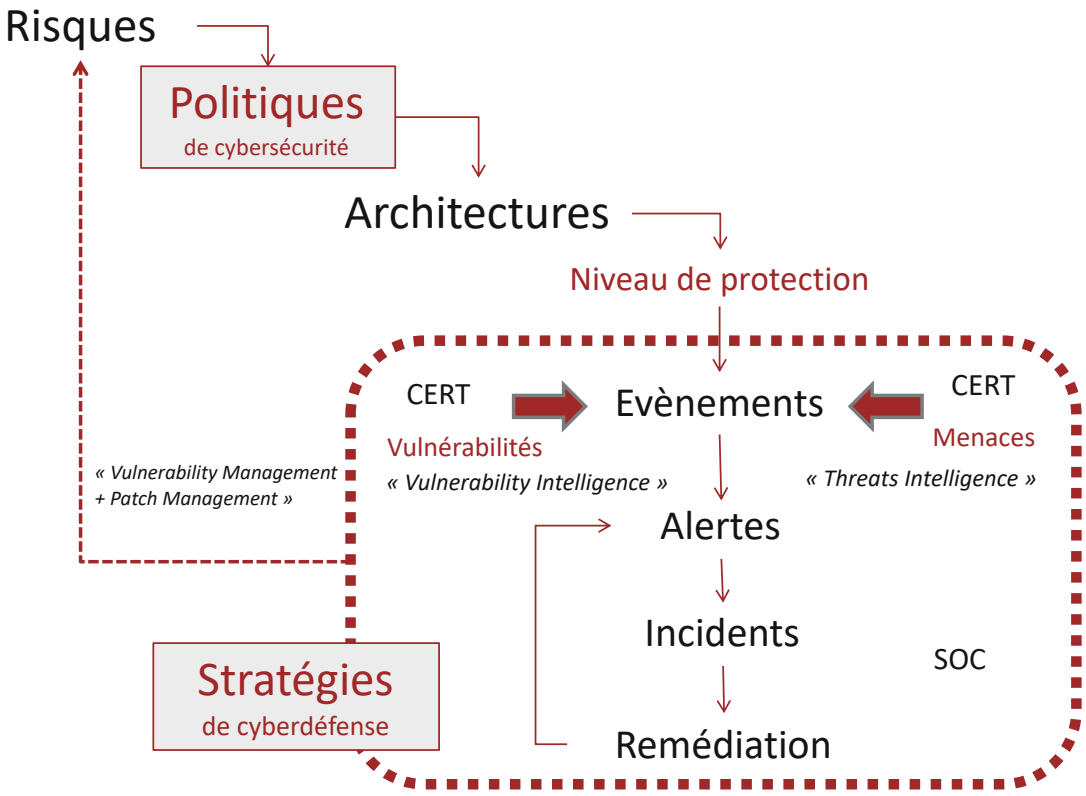


FIGURE 1. lCycle de vie : SEC 101

- **ALERTER** : mettre en place les mécanismes de remontée d'alerte et d'incident.

2. Menaces et définitions

Ce sont généralement les attaques externes et massives qui font l'actualité dans les média. Un grand nombre de risques quotidiens sont issus de l'intérieur même de l'entreprise, fuites de la part de vos employés qui, de façon intentionnelle ou non, révèlent des mots de passe ou des informations sensibles, ou alors d'une opération initiée par des acteurs internes malveillants : des salariés, partenaires, clients qui cherchent à utiliser les informations à leur portée afin d'exploiter ou de porter dommage aux systèmes d'information de l'entreprise, mais plus globalement à l'entreprise dans sa globalité.

Les attaquants externes sont, certes, une menace croissante : ils recherchent sans cesse des failles de sécurité afin d'accéder à vos systèmes.

N'importe quelle entreprise est exposée au risque. De nos jours, les connexions diverses d'une entreprise à l'autre représentent de nombreuses voies pour les

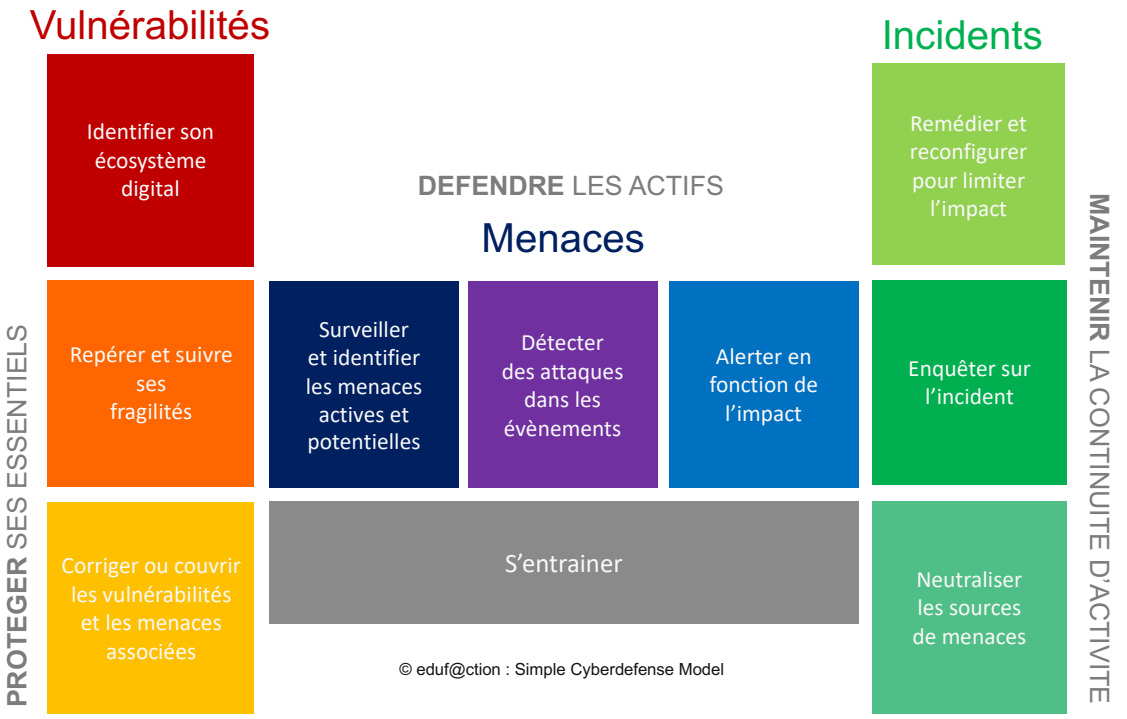
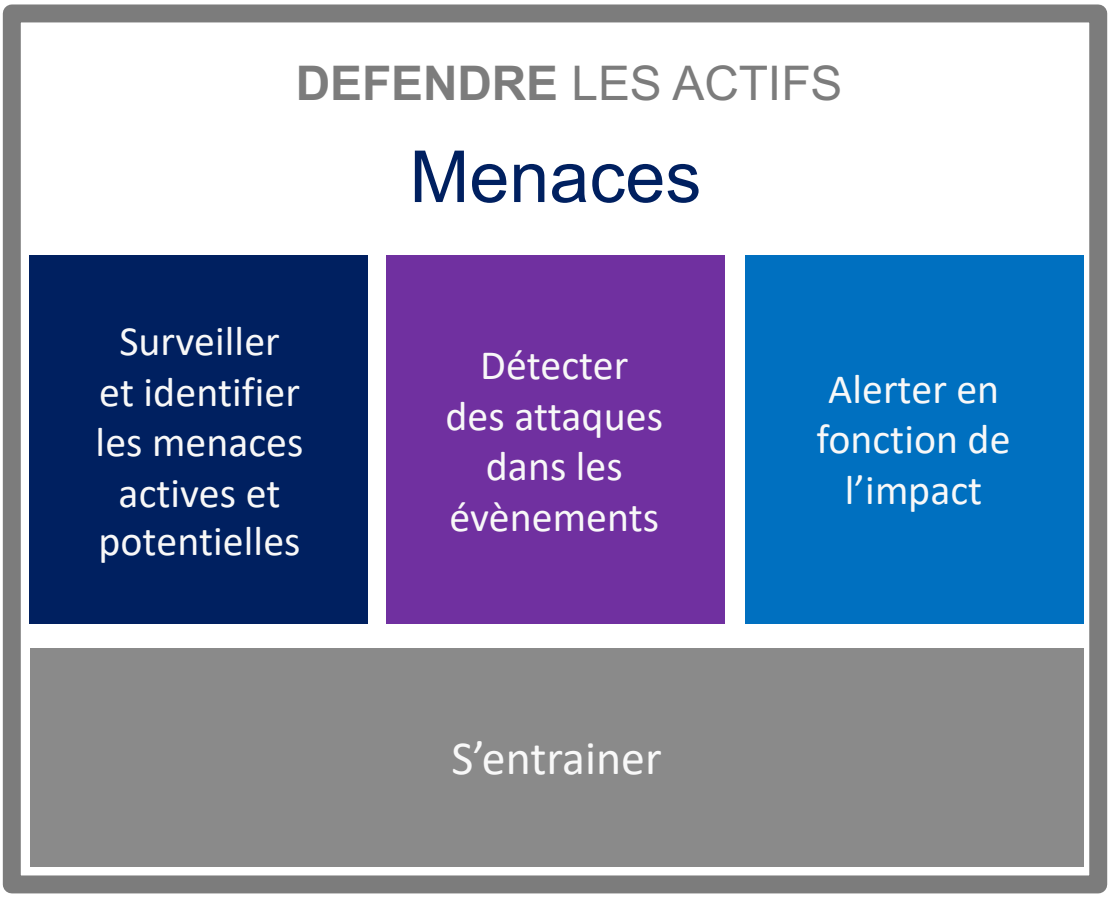


FIGURE 2. Un modèle de gestion cyberdefense

pirates informatiques, qui attaquent souvent les petites entreprises afin d'accéder à leurs plus grands partenaires, clients ou fournisseurs. Les grandes entreprises demandent donc souvent à leurs fournisseurs et partenaires, quelle que soit leur taille, de mettre en place des mesures de cybersécurité.

La nature de ces menaces est en constante évolution. On y trouve les plus courantes :

- Attaques par **déni de service distribuées** (DDoS). Un réseau d'ordinateurs inonde un site Web ou un logiciel avec des informations inutiles. Quand la charge sur les services est important et que le système n'est pas dimensionné ou filtré pour ce type de volume de demande, ce débordement de requêtes provoque une indisponibilité du système inopérant.
- **Codes malveillants** : Bots et virus. Un logiciel malveillant qui s'exécute à l'insu de l'utilisateur ou du propriétaire du système (bots), ou qui est installé par un employé qui pense avoir affaire à un fichier sain (cheval de Troie), afin de contrôler des systèmes informatiques ou de s'emparer de données. La mise à jour des logiciels et des certificats SSL, une forte protection antivirus et une sensibilisation des employés peuvent vous aider à éviter ces types de menace.



© eduf@ction : Simple Cyberdefense Model

FIGURE 3. la gestion de la menace

- **Piratage**. Lorsque des acteurs externes exploitent des failles de sécurité afin de contrôler vos systèmes informatiques et voler des informations. Une mise à jour régulière des mots de passe et des systèmes de sécurité est fondamentale pour déjouer ce type de complot.
- **Hameçonnage** ou dévoiement. Tentative d'obtenir des informations sensibles en se faisant passer frauduleusement pour une entité digne de confiance. Le hameçonnage se fait par e-mail, tandis que le dévoiement utilise des sites ou serveurs fictifs. Une sensibilisation des employés est indispensable afin de ne pas tomber dans ce piège.

2.1 surveiller et anticiper la menace

Dans le domaine spécifique de la menace, veiller sur les menaces nécessite de veiller sur deux choses :

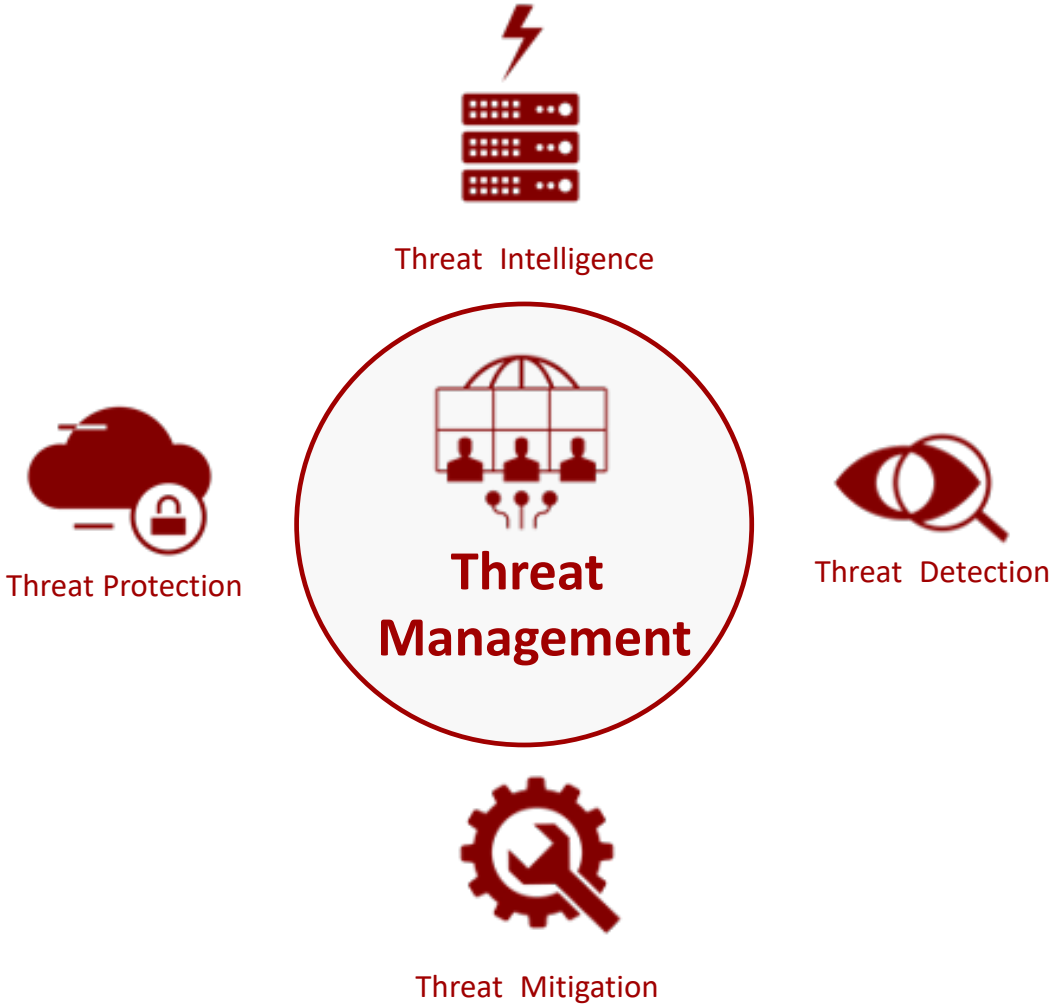


FIGURE 4. les 4 axes de la gestion de la menace

- Les menaces génériques, ou ciblant un domaine particulier (Santé, Industrie, Banque ...) que l'on trouve généralement en utilisant des technologies de « threat Intelligence » permettant
- Les menaces ciblées, dont les indices d'émergence peuvent être détecter en analysant la menace ou en recherchant des indices de compromissions quand ces menaces sont actives dans le périmètre de l'entreprise.

et ceci de deux manières :

- Surveillance de l'écosystème de la menace (IOC, DarkWeb, Threat Intelligence...)

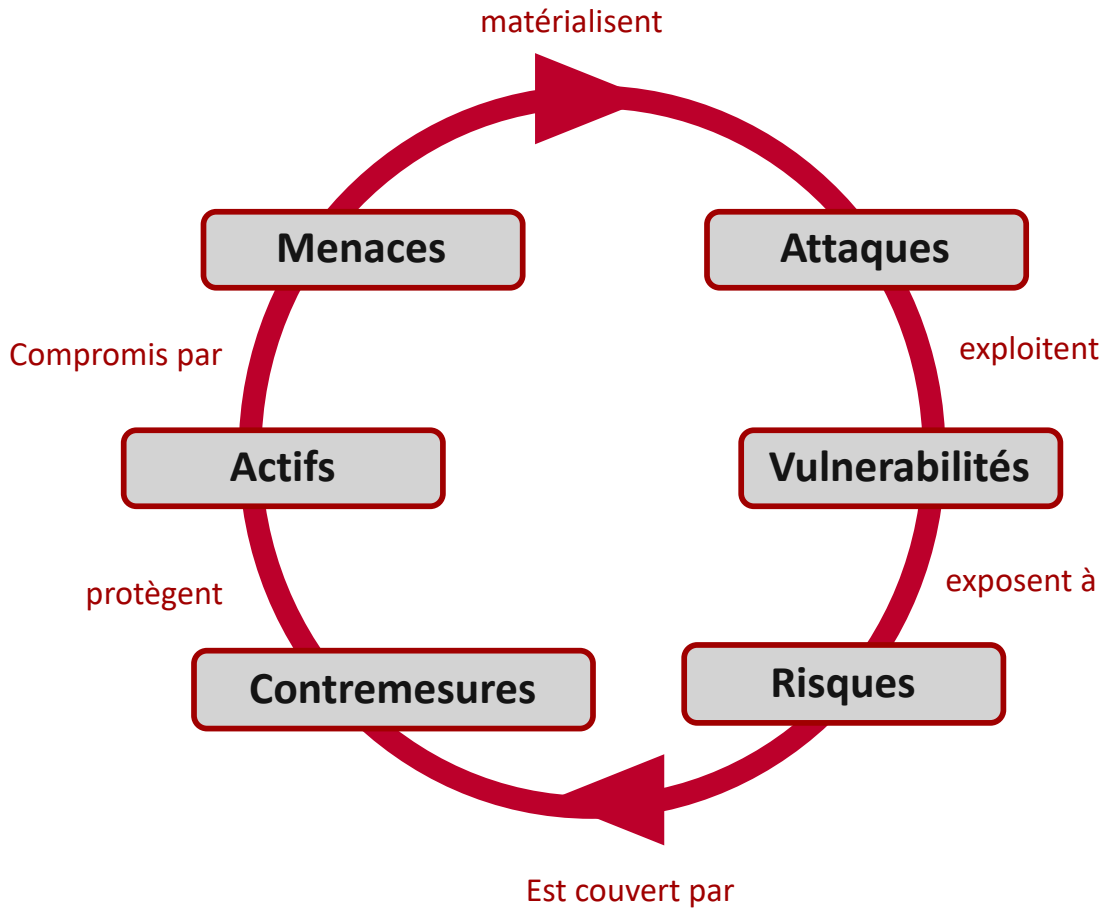


FIGURE 5. la gestion de la menace

- Recherche de compromission, ou d'infection (Threat Hunting, ...)

Ce sont des sujets que nous aborderons dans le processus de gestion de la menace.

2.1.1 Surveillance de la compromission

Un des domaine de la surveillance est donc celui de la compromission. C'est à dire la surveillance dans le fameux Darkweb de l'emergence de données volées, "« perdues »" par une entreprise ou par un particulier.

2.1.2 Surveillance du ciblage

La surveillance du ciblage, que les anglo-saxons appelle le TARGETING est aussi un élément d'anticipation. En effet, ces éléments sont souvent les premiers signaux d'un préparation d'un évènement "« cyber »" qui pourrait toucher l'entreprise.

On y trouve l'émergence de la collecte d'information sur une cible donnée. La mise en oeuvre dans les code malveillant de targetting d'IP spécifique, etc...

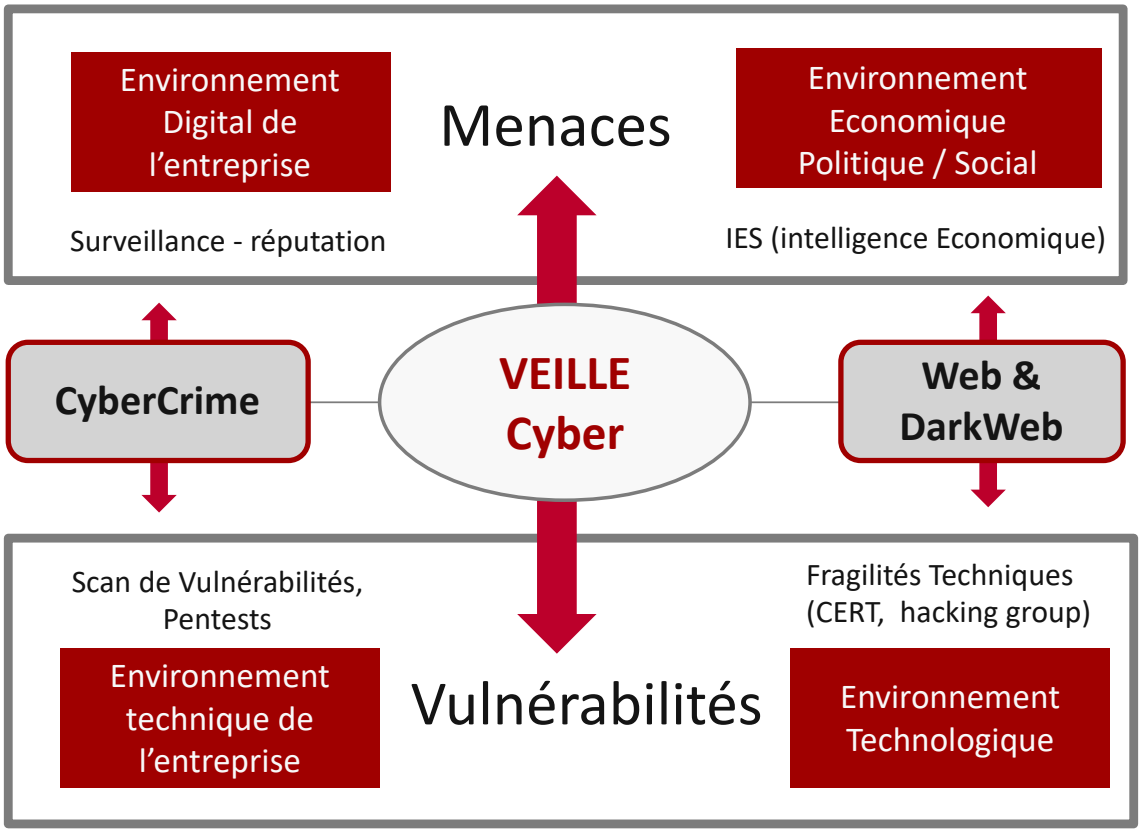


FIGURE 6. Veille cyber, une veille sur les risques

Il y a deux types d'outils pour ce se faire :

- La surveillance classique du web de type « cyberveille », qui permet de découvrir des éléments appartenant à l'entreprise compromis (soient les données, soient des informations permettant de déduire que l'entreprise a été compromise).
- L'analyse en temps réel des codes malveillants qui peut permettre en regardant de manière détaillée l'évolution du code pour comprendre et connaitre les modalités des attaques et les nouvelles cibles.

2.1.3 Que faire des ces informations

Disposer des fragilités de l'entreprise, et connaitre les scénarios potentiels permets d'évaluer un niveau de risque.

2.2 La gestion de la menace

Gérer la menace comporte deux domaines d'activités :

- La veille, au sens renseignement sur la menace (Threat Intelligence)

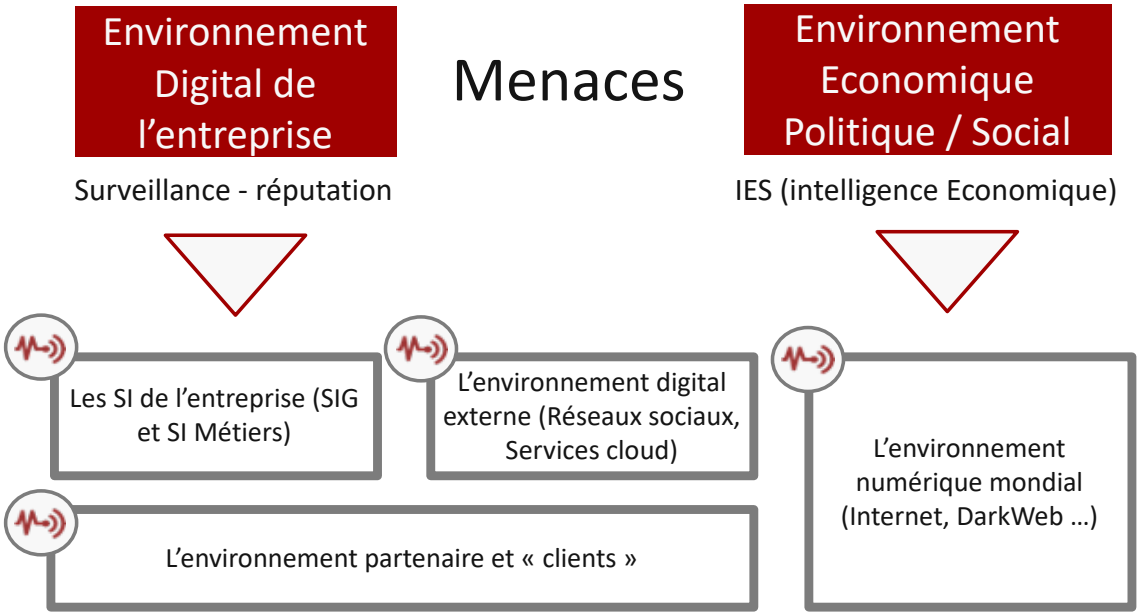


FIGURE 7. Les sources

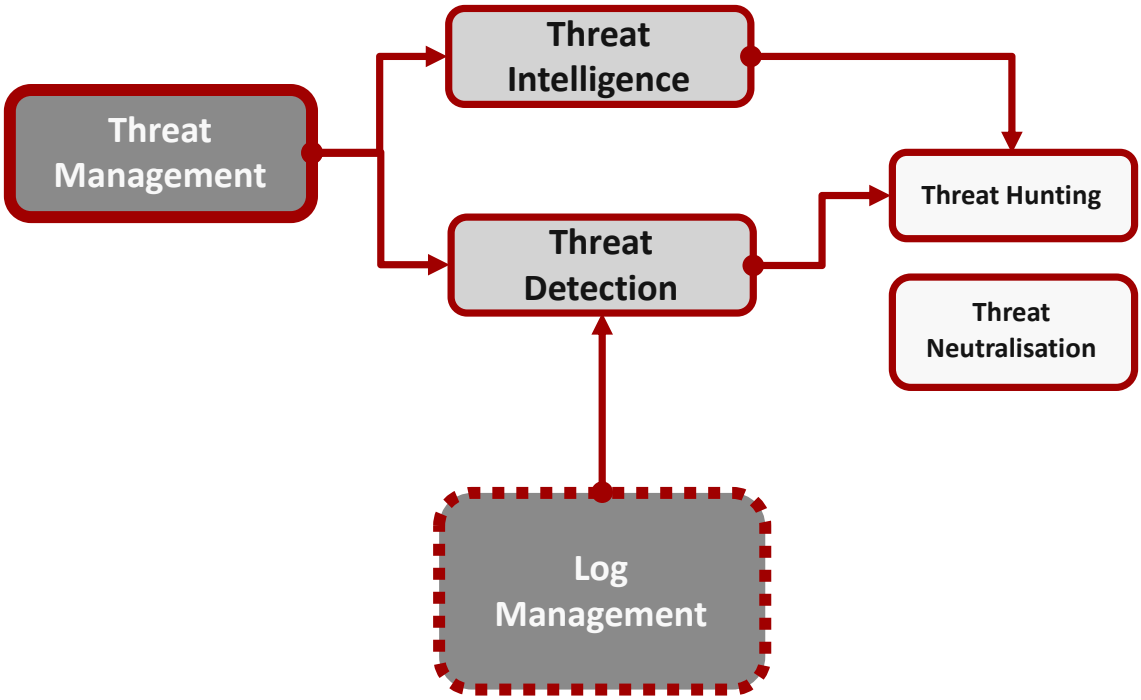


FIGURE 8. la gestion de la menace

- La détection d'attaque, ou de menaces potentielles au sein de l'environnement (Threat Detection)

Ces deux domaines d'activités se base sur la remontée d'information et l'automatisation des détections d'évènements à risques. Le management des LOG des systèmes est au coeur de la détection.

3. Détecter

"« Détecter oui, mais détecter quoi et pourquoi »" est la phrase maitresse de la première étape de réflexion autour de la gestion de la détection d'incident de sécurité. La première question a se poser est qu'est ce qu'un incident de sécurité pour l'entreprise. Si il est vrai qu'il existe un certain nombre de menace "« standard »" que l'on considère très rapidement comme un incident, le déploiement d'outil de gestion d'incident de sécurité ne serait être limite qu'à cette usage standard.

Il y a de nombreuses manières de détecter des tentatives d'attaques dans un système. Les IPS/IDS (Intrusion Prevention System / Intrusion Detection System), Firewall réseaux et firewall applicatif. Toutefois l'imagination des attaquants est suffisamment grande, pour que des attaques complexes ne puisse être détecté par ces seuls outils et produits de sécurité protégeant les flux informationnels.

Nous pouvons en effet considérer par exemple que la détection d'un rançonlogiciel dans l'entreprise est un bien un incident complexe, qu'un IPS/IDS ne détectera pas, qui va par ailleurs nécessiter une alerte et une remédiation rapide si ce n'est immédiate. Toutefois une fuite d'information sur un système métier par des mécanismes discrets sera souvent étudié spécifiquement. Globalement le déploiement d'une fonction d'alerte va nécessiter la définition des "menaces" redoutés par l'entreprise. Ces dernières sont généralement issus des analyses de risque. En effet, il est important au delà des menaces dits standards de revenir au source du déploiement de fonction de sécurité qui sont de gérer et couvrir les risques.

En premier lieu, il convient de chercher à détecter les menaces non couvertes par les mesures de sécurité, les fameuses menaces résiduelles.

Dans l'environnement de l'entreprise, les scénarios complexes issus de l'analyse de risques lors de l'étude des évènements redoutés vont donner les évènements corrélés à détecter. On y trouvera l'application concrète des arbres d'attaques popularisé par une des plus célèbre cyber expert Bruce Schneier (1) qui est présentée de manière un peu plus détaillée dans le chapitre Arbre d'attaques

3.1 Arbre d'attaques

Détecter la menace dans un système d'information c'est aussi connaitre les méthodes, stratégies des attaquants. Ces scénarios d'attaque ou d'opération peuvent être modélisés avec des outils au coeur des analyses de risques. Bien que très largement en arrière plan des méthodes et des outils de gestion de la

menace, les arbres d'attaque restent au coeur des mécanismes de détection.

Les arbres d'attaques sont une représentation des scénarios d'attaques. La racine représente le but final de l'attaque, les différents noeuds sont les buts intermédiaires et les feuilles les actions élémentaires à effectuer. Ces actions seront évaluées par exemple avec les potentiel d'attaque des critères communs (cf.CC et ISO)

Globalement, ces arbres sont basés sur trois types de nœuds :

- Nœud **disjonctif** OR : OU logique. Cela signifie que pour que le nœud soit réalisé, il faut qu'au moins un de ses fils soit réalisé.
- Nœud **conjonctif** AND : ET logique. Pour sa réalisation, il faut que l'ensemble de ses fils soit réalisé.
- Nœud **conjonctif séquentiel** SAND : Pour sa réalisation, il faut que l'ensemble de ses fils soit réalisé dans un ordre séquentiel c'est-à-dire les fils sont effectués les uns après les autres dans l'ordre indiqué.

En fonction de ces noeuds les valeurs des feuilles seront remontées pour obtenir le potentiel d'attaque de la racine. C'est sur la base de ce type de technique que sont construit un certain nombre d'outil de détection.

Gartner, et Lockheed Martin ont dérivé le concept de ces arbres d'attaque dans des modèles dit de « Kill Chain » issus de modèle militaire établis à l'origine pour identifier la cible, préparer l'attaque, engager l'objectif et le détruire.

Ce modèle analyse un fragilité potentielle en dépistant les phases de l'attaque, de la reconnaissance précoce à l'exfiltration des données. Ce modèle de chaine ou processus cybercriminel aide à comprendre et à lutter contre les ransomware, les failles de sécurité et les menaces persistantes avancées (APT). Le modèle a évolué pour mieux anticiper et reconnaître les menaces internes, l'ingénierie sociale, les ransomware avancés et les nouvelles attaques.

3.2 le déploiement d'une menace en 8 étapes

- **Phase 1 : Reconnaissance**. Dans tout « casse », vous devez d'abord repérer les lieux. Le même principe s'applique dans un cyber-casse : c'est la phase préliminaire d'une attaque, la mission de recueil d'informations. Pendant la reconnaissance, le cybercriminel recherche les indications susceptibles de révéler les vulnérabilités et les points faibles du système. Les pare-feu, les dispositifs de prévention des intrusions, les périmètres de sécurité (et même les comptes de médias sociaux) font l'objet de reconnaissance et d'examen. Les outils de repérage analysent les réseaux des entreprises pour y trouver des points d'entrée et des vulnérabilités à exploiter.
- **Phase 2 : Intrusion.** Après avoir obtenu les renseignements, il est temps de s'infiltrer. L'intrusion constitue le moment où l'attaque devient active : les

malware (y compris les ransomware, spyware et adware) peuvent être envoyés vers le système pour forcer l'entrée. C'est la phase de livraison. Celle-ci peut s'effectuer par e-mail de phishing ou prendre la forme d'un site Web compromis ou encore venir du sympathique café au coin de la rue avec sa liaison WiFi, favorable aux pirates. L'intrusion constitue le point d'entrée d'une attaque, le moment où les agresseurs pénètrent dans la place.

- **Phase 3 : Exploitation**. Le hacker se trouve de l'autre côté de la porte et le périmètre est violé. La phase d'exploitation d'une attaque profite des failles du système, à défaut d'un meilleur terme. Les cybercriminels peuvent désormais entrer dans le système, installer des outils supplémentaires, modifier les certificats de sécurité et créer de nouveaux scripts à des fins nuisibles.
- **Phase 4 : Escalade de privilèges**. Quel intérêt y a-t-il à entrer dans un bâtiment si vous restez coincé dans le hall d'accueil ? Les cybercriminels utilisent l'escalade de privilèges pour obtenir des autorisations élevées d'accès aux ressources. Ils modifient les paramètres de sécurité des GPO, les fichiers de configuration, les permissions et essaient d'extraire des informations d'identification.
- **Phase 5 : Mouvement latéral**. Vous avez carte blanche, mais vous devez encore trouver la chambre forte. Les cybercriminels se déplacent de système en système, de manière latérale, afin d'obtenir d'autres accès et de trouver plus de ressources. C'est également une mission avancée d'exploration des données au cours de laquelle les cybercriminels recherchent des données critiques et des informations sensibles, des accès administrateur et des serveurs de messagerie. Ils utilisent souvent les mêmes ressources que le service informatique, tirent parti d'outils intégrés tels que PowerShell et se positionnent de manière à causer le plus de dégâts possible.
- **Phase 6 : Furtivité, camouflage, masquage**. Mettez les caméras de sécurité en boucle et montrez un ascenseur vide pour que personne ne voit ce qui se produit en coulisses. Les cyber-attaquants font la même chose. Ils masquent leur présence et leur activité pour éviter toute détection et déjouer les investigations. Cela peut prendre la forme de fichiers et de métadonnées effacés, de données écrasées au moyen de fausses valeurs d'horodatage (time-stamping) et d'informations trompeuses, ou encore d'informations critiques modifiées pour que les données semblent ne jamais avoir été touchées.
- **Phase 7 : Isolation et Déni de service**. Bloquez les lignes téléphoniques et coupez le courant. C'est là où les cybercriminels ciblent le réseau et l'infrastructure de données pour que les utilisateurs légitimes ne puissent obtenir ce dont ils ont besoin. L'attaque par déni de service (DoS) perturbe et interrompt les accès. Elle peut entraîner la panne des systèmes et saturer les services.

- **Phase 8 : Exfiltration**. Prévoyez toujours une stratégie de sortie. Les cyber-criminels obtiennent les données. Ils copient, transfèrent ou déplacent les données sensibles vers un emplacement sous leur contrôle où ils pourront en faire ce qu'ils veulent : les rendre contre une rançon, les vendre sur eBay ou les envoyer à BuzzFeed. Sortir toutes les données peut prendre des jours entiers, mais une fois qu'elles se trouvent à l'extérieur, elles sont sous leur contrôle.

Différentes techniques de sécurité proposent différentes approches de la chaîne cyber-criminelle. De Gartner à Lockheed Martin, chacun définit les phases de manière légèrement différente.

C'est un modèle souvent critiqué pour l'attention qu'il accorde à la sécurité du périmètre et limité à la prévention des malwares. Cependant, quand elle est combinée à l'analyse avancée et à la modélisation prédictive, la chaîne cyber-criminelle devient essentielle à une sécurité complète.

L'analyse du comportement des utilisateurs (UBA) apporte des informations détaillées sur les menaces liées à chaque phase de la chaîne criminelle. Et elle contribue à prévenir et arrêter les attaques avant que les dommages ne soient causés.

4. Surveiller et anticiper : Threat Detection

La surveillance et le renseignement de la menace au sens général du terme (Threat Intelligence) devrait contenir les 2 niveaux :

- Le renseignement à vocation cyber qui comprend toutes les analyses et information permettant d'anticiper et de caractériser une menace qui pourrait s'exprimer dans le monde numérique,
- Le renseignement d'origine Cyber, dont les données techniques liées à des attaques, menaces qui permettent de configurer des systèmes de détection et de réponse.

Il est vrai qu'encore aujourd'hui parler de « threat intelligence » nous dirige systématiquement sur la deuxième assertion

5. les traces, journaux, logs

Dans le domaine informatique et télécom, le terme log est généralement un fichier, une base de données ou tout autre moyen de stocker des information, ici le stockage d'un historique d'événements qu'un logiciel ou un système souhaite "tracer". Ce mot qui est le diminutif de logging, est traduit en français par "journal". Le log est donc un journal horodaté, qui stocke temporellement les différents

événements qui se sont produits sur un un logiciel, un ordinateur, un serveur, etc. Il permet ainsi d'analyser avec une fréquence programmer (heure par heure, minute par minute, etc) l'activité d'un processus technique.

Une grande majorité des équipements (réseau, serveurs, terminaux (endpoint)), des bases de données ou des applications d'un systèmes d'information peuvent aujourd'hui générer des logs ou traces. Ces fichiers contiennent, pour chaque équipe, la liste de tous évènements "traçable" qui se sont déroulés pendant l'execution : réussite ou échec d'une connexion, redémarrage, utilisation des ressources (mémoire, ...).

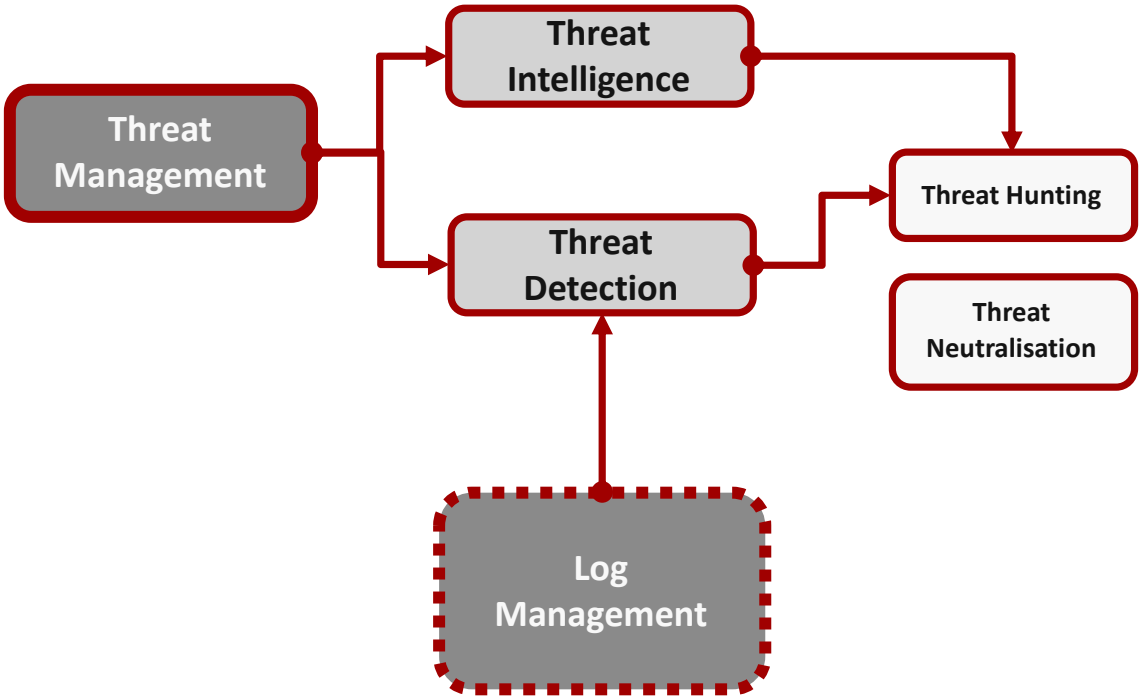


FIGURE 9. Les logs au coeur de la détection

L'exploitation de ces traces est souvent complexe car chaque équipements dispose de ses propre fonctions de gestion des traces. Il faut consulter ces logs équipements par équipements. Heureusement, il existe des outils qui permettent de centraliser et de « normaliser » ces traces. On peut citer par exemple, SYSLOG. C'est un protocole qui définit comment gérer les logs systèmes. Quand un système veut conserver les traces d'un événement), il est possible, d'utiliser syslog pour communiquer les détails de l'événement à un daemon syslog qui va le conserver dans une base de données. L'intérêt d'un serveur Syslog-ng est donc de permettre une centralisation de ces journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances de machines présentes sur un réseau.

6. l'usage des log

- Un complément indispensable au processus de « détection de menace ». La gestion des logs (ou d'événements) s'avère un outil très utile pour les analyses a posteriori, mais peut aussi servir dans la détection en temps reel pour peu que les outils d'analyse puisse le faire ; Nous verront cela dans la partie sur la détection de la menace.
- « Une couverture légale ». Confrontée à une plainte, une entreprise peut utiliser ces traces pour gérer un litige avec un tiers en attestant de la non-implication de son système d'information ou, a contrario, assumer le litige tout en remontant jusqu'à l'utilisateur concerné. La société peut également utiliser ces traces pour fournir des éléments aux services de polices. La fourniture d'élément probant à valeur légale nécessite quelques précautions.
- « Le dépistage des malversations internes ou de comportements déviants ». Les flux illégaux, les flux de données déviants (copies de fichiers en masse avant qu'un salarié quitte l'entreprise par exemple)
-

7. Log Management

8. Puits de logs

La construction d'un « puits de log » est une première brique de réponse : il s'agit de collecter, à l'aide d'un outil automatisé du marché, l'ensemble des journaux d'équipements dans un espace de stockage unique. L'un des critères de sélection de cet outil est justement sa capacité à reconnaître différents formats de logs (syslog, traps SNMP, formats propriétaires...).

Le volume d'information centralisée peut vite exploser : il est important d'éviter la collecte de données inutiles. Par ailleurs, le système peut également être gourmand en puissance de calcul en fonction des périmètres de recherches effectuées.

On parle de log management à partir du moment où les données contenues dans ce puits sont traitées et exploitées, par exemple pour retrouver un élément dangereux (virus, problème de sécurité...), ou un comportement malveillant (fuite d'information, suppression de données...). Il est nécessaire de cadrer en amont les finalités du projet, qui peuvent être multiples :

9. Gestion de la menace

Nous avons évoqué dans le chapitre sur l'anticipation, la veille sur la menace. Opérer la détection d'attaques ou de menaces dormante dans l'environnement

de l'entreprise nécessite une connaissance précise des mécanismes d'exécution oui d'opération de ces menaces. La connaissance de ces mécanismes d'action, de protection, de déploiement, de réplication, de survivabilité, de déplacement des codes malveillants par exemple est la base de leur détection. Il es en de même sur les scénario mixant des actions sur les réseaux ou sur les systèmes informatiques ou numériques. Ces connaissances sont généralement structurés dans des base de connaissances dont les sources sont gratuites ou payantes.

9.1 Cibles de menaces

9.2 Sources de menaces

Nous parlerons ici de sources de menaces comme les indicateurs permettant d'identifier l'origine technique d'une menace. Cela peut être une adresse mail, un serveur/service de mail , une adresse IP de provenance d'un code malveillant, d'une attaque, ou d'un comportement anormal.

On peut citer par exemple Une adresse mail connue pour envoyer un code malveillant. le blacklistage d'adresse IP ou de d'adresse de serveur Mail pour Spam

En face, il des attaquants qui bien entendue vont changer leur position pour émettre ou attaquer d'ailleurs, ou avec une autre forme (furtivité)

Les sources de menace dans l'environnement internet

9.3 Data Lake

9.4 Threats Huntings

La chasse à la menaces dormantes ou aux compromissions mais aussi le maintien du contact entre la défense et les attaquants.

La chasse aux menaces est une tactique permettant de connaître avec plus d'acuité l'environnement de la menance et donc le degré de risque de cyberattaques auquel est soumise une entreprise.

La terminologie threat hunting regroupe plusieurs type de d'action et la définition de n'est pas totalement stabilisée. Globalement on y trouve deux grande classes de threat hunting

Celle travaillant autour de l'environnent, de la surface d'attaque et qui oriente ses actions sur des méthodes de "recherches" permettant de débusquer des menaces latentes ou des menaces dormantes et les réveiller et de les suivre de les comprendre et Pour établir le contact avec l'attaquant.

Et un autres plus active ou proactive dont l'objectif est de rester, conserver le contact avec l'attaquant lors d'une reaction à une alerte.

9.4.1 Etablir le contact

Quand on parle d'établir contact, nous parlons d'aller au contact au sens martial du terme. c'est dire en direct de suivre, caractériser ka sources de la

menace et jouer avec elle.

La méthode de "hunter" consiste en premier à dresser un portrait global de la surface d'attaque, tout en identifiant les attaquants potentiels, leurs motifs et leurs façons de faire. Plus précisément, le « threat hunting » consiste en une analyse détaillée de :

- La position de de l'entreprise, notoriété, popularité sur internet, en analysant en particulier les médias traditionnels et les médias sociaux ;
- l'environnement économique de l'entreprise dont ses fournisseurs, ses clients, ses partenaires, ses employés ;
- le corpus technologiques et physique de l'entreprise, dont les architectures techniques et les mécanismes informatique avec l'environnement économique ainsi l'environnement sécuritaire de ses relations.

Sur la base de cette analyse globale, des SPOF (Sigle Point Of Failure) peuvent être trouvés.

grace à la visualisation globale des lien il sera possible comprendre où, comment, pourquoi et potentiellement par qui (hactivistes, anciens employés, fournisseurs, etc.) la prochaine attaque pourrait être perpétrée. Les « threat hunters », ne sont pas simplement en attente de répondre aux alertes du système de défense, ils cherchent activement des menaces dans leurs propres réseaux afin de prévenir ou de minimiser les dommages. Cette méthode s'avère l'une des plus proactives.

10. SIEM, une technologie

10.1 un peu d'histoire

Le SIEM est aujourd'hui l'aboutissement d'un voeux très anciens des responsable sécurité qui supervise depuis bien des décennies des systèmes de contrôle périmétriques : Corréler tous les évènements arrivants sur l'ensemble de ces équipements. L'acronyme SIEM ou «gestion des informations de sécurité» fait référence à des technologies combinant à la fois la gestion des informations de sécurité et la gestion des événements de sécurité. Comme ils sont déjà très similaires, le terme générique plus large peut être utile pour décrire les outils et les ressources de sécurité modernes. Là encore, il est essentiel de différencier la surveillance des événements de la surveillance des informations générales. Un autre moyen essentiel de distinguer ces deux méthodes consiste à considérer la gestion des informations de sécurité comme une sorte de processus à long terme ou plus large, dans lequel des ensembles de données plus diversifiés peuvent être analysés de manière plus méthodique. En revanche, la gestion des événements de sécurité examine à nouveau les types d'événements utilisateur pouvant constituer des

signaux d'alerte ou indiquer aux administrateurs des informations spécifiques sur l'activité du réseau.

C'est souvent l'usage d'un SIEM dans une ambiguïté de gestion long terme de la sécurité en tant que propriété d'un système d'une part, et la gestion court terme de l'urgence d'une attente à la sécurité qui pose problème dans les projets et dans les opérations.

Ce genre d'outillage est passé par différentes étapes de maturation avec des SIM et SEM et enfin des SIEM. Il s'agit de combiner les fonctions de gestion des informations (SIM, Security Information Management) et des évènements (SEM, Security Event Management) en un seul système de management de sécurité.

- dans la gestion des informations de sécurité (SIM) , la technologie consiste à collecter des informations à partir des journaux d'équipement de sécurité, qui peut consister en différents types de données. Globalement on peut dire qu'un SIM est aimantant important pour des équipes de supervision de la sécurité périmétrique. d'une part pour la traçabilité et le reporting de sécurité.
- technologies spécialement conçues pour rechercher des authentifications suspectes, des ouvertures de session sur un compte ou des accès de gestion de haut niveau à des heures précises du jour ou de la nuit.

Bien qu'outillant des processus très similaires mais distincts, les trois acronymes SEM, SIM et SIEM ont tendance à être confus ou à causer de la confusion chez ceux qui sont relativement peu familiarisés avec les processus de sécurité. La similitude entre la gestion des événements de sécurité ou SEM et la gestion des informations de sécurité ou SIM est au cœur du problème.

Ces deux types de collecte d'informations concernent la collecte d'informations de journal de sécurité ou d'autres données similaires en vue d'un stockage à long terme, ou l'analyse de l'environnement de sécurité d'un réseau.

Plus concrètement, un système de type SEM centralise le stockage et l'interprétation des logs en temps réel et permet une analyse. Les experts en cyber sécurité peuvent ainsi prendre des mesures défensives plus rapidement. Un système de type SIM collecte pour sa part des données et les place dans un référentiel à des fins d'analyse de tendances. Dans ce cas, la génération de rapports de conformité est automatisée et centralisée.

Le SIEM, qui regroupe ces 2 systèmes, accélère donc l'identification et l'analyse des événements de sécurité, atténue les conséquences d'attaques et facilite la restauration qui s'ensuit. Pour y parvenir, il collecte les événements, les stocke (avec normalisation) et agrège des données pertinentes mais non structurées issue de plusieurs sources. L'identification des écarts possibles par rapport à la moyenne

/ norme nourrit la prise de décision. En outre, les tableaux de bord générés contribuent à répondre aux exigences légales de conformité de l'entreprise.

En d'autres termes, avec le SIEM les équipes de sécurité opérationnelle industrialisent la surveillance tout en simplifiant l'analyse de multiples sources d'événements de sécurité (antivirus, proxy, Web Application Firewall. . .). La corrélation des événements provenant d'applications ou d'équipements très variés est aussi facilitée. De quoi détecter des scenarii de menaces avancées.

Dans la pratique, Il existe 3 types de SIEM :

- SIEM déployé
- SIEM basé dans le cloud
- SIEM géré / managé

Reconnaissons-le, s'équiper d'une solution de type SIEM nécessite un investissement conséquent en raison de la complexité de sa mise en œuvre. Toutefois, bien qu'initialement destiné aux grandes entreprises, le SIEM offre des avantages à tous les types d'organisations :

Détection proactive d'incidents Un SIEM s'avère capable de détecter des incidents de sécurité qui seraient passés inaperçus. Pour une raison simple : les nombreux hôtes qui enregistrent des événements de sécurité ne disposent pas de fonctions de détection d'incidents.

Le SIEM dispose de cette faculté de détection grâce à sa capacité de corrélation des événements. Contrairement à un système de prévention d'intrusion qui identifie une attaque isolée, le SIEM regarde au-delà. Les règles de corrélations lui permettent d'identifier un événement ayant causé la génération de plusieurs autres (hack via le réseau, puis manipulation sur un équipement précis. . .).

Dans de tels cas de figure, la plupart des solutions ont la capacité d'agir indirectement sur la menace. Le SIEM communique avec d'autres outils de sécurité mis en place dans l'entreprise (Exemple pare-feu) et pousse une modification afin de bloquer l'activité malveillante. Résultat, des attaques qui n'auraient même pas été remarquées dans l'entreprise sont contrecarrées.

- la premiere fonction d'un SIEM est déjà de corréler les événements provenant des composants de sécurité.
- la deuxième fonction de corréler des événement de comportement du SI
- troisième fonction de corréler avec des événements externes au SI sur la base de capteurs externes (threats intelligence de type renseignement)

Pour aller encore plus loin, une organisation peut choisir d'intégrer à son SIEM une Cyber Threat Intelligence (CTI ou Flux de renseignement sur les menaces).

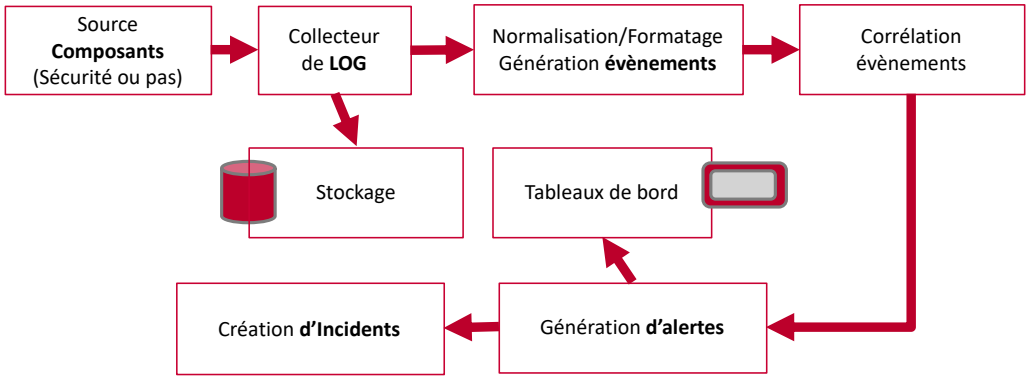


FIGURE 10. architecture d'un SIEM

Selon la définition de Gartner, la Cyber Threat Intelligence (CTI) est la connaissance fondée sur des preuves, y compris le contexte, les mécanismes, les indicateurs, les implications et des conseils concrets, concernant une menace nouvelle ou existante ou un risque pour les actifs d'une organisation qui peuvent être utilisés afin d'éclairer les décisions concernant la réponse du sujet à cette menace ou un danger

La CTI consiste donc à collecter et organiser toutes les informations liées aux menaces et cyber-attaques, afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités visés, les méthodes d'attaque utilisées, etc.). Résultat, une meilleure anticipation des incidents aux prémices d'une attaque d'envergure.

La cyberprotection d'une entreprise est principalement basée sur les outils de protection périmétriques que ceux ci soit des équipements physiques ou qu'ils soient dans le cloud : systèmes de détection d'intrusion (IDS), scanners de vulnérabilités, antivirus ainsi que systèmes de gestion et corrélation d'événements sécurité (SIEM). Lorsqu'il s'agit de superviser un système informatique à grande échelle réparti sur plusieurs sites, il devient vite très difficile de corréler et analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents suffisamment vite pour réagir efficacement. Cette complexité est due à la quantité d'information générée, au manque d'interopérabilité entre les outils ainsi qu'à leurs lacunes en matière de visualisation.

10.2 de l'usage d'un siem pour la gouvernance

À l'heure où les normes et certifications de cyber-sécurité sont de plus en plus nombreuses, le SIEM devient un élément clé de tout système d'information. C'est un moyen relativement simple de répondre à plusieurs exigences de sécurité (Exemple : historisation et suivi des logs, rapports de sécurité, alerting, . . .) et de prouver sa bonne foi aux autorités de certification ou de suivi. D'autant que le SIEM peut générer des rapports hautement personnalisables selon les exigences

des différentes réglementations.

Ce seul bénéfice suffit à convaincre des organisations de déployer un SIEM. Et pour cause : la génération d'un rapport unique traitant tous les événements de sécurité pertinents quelle que soit la source des logs (générés en outre dans des formats propriétaires) fait gagner un temps précieux.

Les contreparties du SIEM Déployer un SIEM ne suffit pas pour autant à sécuriser complètement votre organisation. Les solutions SIEM présentent des limites qui les rendent inefficaces sans un accompagnement à la hauteur et sans solutions tierces. Contrairement à une solution de sécurité de type IDS ou Firewall, un SIEM ne surveille pas les événements de sécurité mais utilise les données de logs enregistrées par ces derniers. Il est donc essentiel de ne pas négliger la mise en place de ces solutions.

Une configuration pointue Les SIEM sont des produits complexes qui appellent un accompagnement pour assurer une intégration réussie avec les contrôles de sécurité de l'entreprise et les nombreux hôtes de son infrastructure.

Il est important de ne pas se contenter d'installer un SIEM avec les configurations du constructeur et/ou par défaut, car elles sont souvent insuffisantes. Les configurations doivent être personnalisées et adaptées aux besoins des utilisateurs. De même concernant les rapports, mieux vaut créer ses propres rapports d'analyse, adaptés aux différentes menaces identifiées. À défaut, le risque est réel de ne pas pouvoir profiter des avantages d'une solution de SIEM.

Des investissements à bien anticiper La collecte, le stockage et l'analyse des événements de sécurité sont des tâches qui semblent relativement simples. Cependant, leur collecte, stockage et l'exécution des rapports de conformité, l'application des correctifs et l'analyse de tous les événements de sécurité se produisant sur le réseau d'une entreprise n'est pas trivial. Taille des supports de stockage, puissance informatique pour le traitement des informations, temps d'intégration des équipements de sécurité, mise en place des alertes... L'investissement initial peut se compter en centaines de milliers d'euros auquel il faut ajouter le support annuel.

Intégrer, configurer et analyser les rapports nécessite la compétence d'experts. Pour cette raison, la plupart des SIEM sont gérés directement au sein d'un SOC souvent externalisé. Porteur de grandes promesses, le SIEM mal configuré peut apporter son lot de déceptions. Selon un sondage réalisé auprès de 234 entreprises (Source LeMagIT), 81 % d'utilisateurs reprochent aux SIEM de produire des rapports contenant trop de bruit de fond et pour 63% les rapports générés sont difficiles à comprendre. Faire appel à des prestataires externes disposant de l'expertise dans le domaine reste souvent la meilleure solution.

Un grand volume d'alertes à réguler Les solutions SIEM s'appuient généralement

sur des règles pour analyser toutes les données enregistrées. Cependant, le réseau d'une entreprise génère un nombre très important d'alertes (en moyenne 10000 par jours) qui peuvent être positives ou non. En conséquence, l'identification de potentiels attaques est compliquée par le volume de logs non pertinents.

La solution consiste à définir des règles précises (en général rédigées par un SOC) et le périmètre à surveiller que faut-il surveiller en priorité ? Le périmétrique ? L'interne ? Réseau/système/application ? Quelle technologie à prioriser ? etc.

Une surveillance à exercer 24h/24 Pour fonctionner correctement, les solutions SIEM nécessitent une surveillance 24h/24 et 7j/7 des journaux et des alertes. Un personnel formé ou une équipe dédiée sont requis pour consulter les journaux, effectuer des examens réguliers et extraire les rapports pertinents.

Voilà pourquoi externaliser cette surveillance auprès d'un fournisseur de services de sécurité tel que SECURIVIEW fait sens. Il s'agit à la fois de disposer des expertises requises, de gagner en lisibilité budgétaire et, aussi, de profiter d'engagements de services. Des conditions à réunir afin que l'investissement dans une solution SIEM marque une étape clé dans la protection de votre organisation contre les menaces avancées.

10.2.1 Analyse d'impact

Un autre problème majeur dans l'usage d'un SIEM est que l'action de comprendre l'impact réel d'une vulnérabilité ou d'une alerte IDS est généralement dévolue à un analyste cybersécurité humain, qui doit lui- même faire le lien entre toutes les informations techniques et sa connaissance de tous les services ou processus liés aux incidents de sécurité détectés sur les composants concernées (serveurs, PC, smartphone, IOT,...) .

Le projet DRA est une étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l'impact réel dû à la situation sécurité globale du système et du réseau. Pour cela une nouvelle méthodologie innovante a été développée en combinant un générateur automatique d'arbres d'attaque (attack trees/graphs) et un moteur d'analyse de risque « traditionnel » similaire à EBIOS.

Les systèmes de gestion des informations et événements de sécurité (SIEM) font régulièrement l'objet de critiques acerbes. Complexité, besoins importants en ressources de conseil externes... de nombreuses entreprises ont été déçues par leur expérience du SIEM pour l'implémentation de la supervision de la sécurité.

Mais la technologie n'est plus, désormais, la raison pour laquelle des entreprises peinent à réussir leurs implémentations de SIEM. Les principales plateformes de SIEM ont reçu de véritables transplantations cérébrales, se transformant en entrepôts de données taillés sur mesure pour fournir les performances et l'élasticité requises. Les connecteurs système et les aggrégateurs de logs, autrefois complexes et peu

fiables, sont aujourd'hui efficaces, rendant la collecte de données relativement simple.

Mais il y a une limite au SIEM, comme à toute technologie s'appuyant sur des règles : le SIEM doit savoir ce qu'il doit chercher. Aucun boîtier SIEM ne pourra identifier automatiquement, comme par magie, une attaque tirant profit d'une méthode ou d'une vulnérabilité inédite.

Le SIEM joue un rôle important dans la détection d'attaques. Mais pour qu'il puisse détecter les attaques connues et inconnues, l'entreprise qui le déploie doit construire des ensembles de règles qui lui permettront d'identifier des conditions d'attaques et des indicateurs spécifiques à son environnement. Et le tout de manière cohérente. Comment donc construire ces règles ?

Tout collecter

Sans disposer de suffisamment de données collectées, le SIEM n'a pas grand chose à analyser. Mais la première étape est de collecter les bonnes données. Et celles-ci sont notamment les logs des équipements réseau, de sécurité et des serveurs. Ces données sont nombreuses et faciles à obtenir. Ensuite, il faut s'intéresser aux logs de l'infrastructure applicative (bases de données, applications). Les experts du SIEM ajoutent à cela les données remontées par de nombreuses autres sources, comme celles des systèmes de gestion des identités et des accès, les flux réseau, les résultats des scans de vulnérabilités et les données de configurations.

Avec les SIEM, plus il y a de données collectées, mieux c'est. Si possible, autant tout collecter. S'il est nécessaire de définir des priorités, alors mieux vaut se concentrer sur les actifs technologiques critiques, à commencer par les équipements installés dans les environnements sensibles et ceux manipulant des données soumises à régulation, ou encore ceux touchant à la propriété intellectuelle.

Construire les règles

Construire une règle pour SIEM est un processus itératif. Cela signifie qu'il est relativement lent et qu'il doit être affiné, précisé au fil du temps. De nombreuses personnes sont atteintes de la « paralysie de l'analyste » en début de processus, parce qu'il existe des millions de règles pouvant être définies. Ainsi, Securosis conseille de se concentrer sur les menaces les plus pressentes pour déterminer les règles à définir en premier.

Dans le cadre du processus de modélisation, il convient de commencer par un actif important. Pour cela, il faut adopter le point de vue de l'attaquant et chercher ce que l'on pourrait vouloir voler.

Modéliser la menace. Il faut se mettre à la place de l'attaquant et imaginer comment entrer et voler les données. C'est la modélisation de l'attaque, avec énumération de chaque vecteur avec le SIEM. Et il convient de ne pas oublier

l'exfiltration car sa modélisation offre une opportunité supplémentaire de détecter l'attaque avant que les données ne se soient envolées. Dans ce processus, il s'agit d'adopter des attentes réalistes car le modèle d'attaque ne peut pas par essence être parfait ni complet. Mais il convient toutefois d'engager le processus de modélisation. Et il n'y a pas de mauvais point de départ.

Affiner les règles. Il convient ensuite de lancer l'attaque contre le SI, telle que modélisée. Les outils pour cela ne manque pas. C'est l'occasion de suivre ce que fait le SIEM. Déclenche-t-il les bonnes alertes ? Au bon moment ? L'alerte fournit-elle suffisamment d'informations pour assister les personnes chargées de la réaction ? Si l'alerte n'est pas adéquate, il convient de revoir le modèle et d'ajuster les règles.

Optimiser les seuils. Avec le temps, il deviendra de plus en plus clair que certaines alertes surviennent trop souvent, et d'autres pas assez. Dès lors, il convient d'ajuster finement les seuils de déclenchement. C'est toujours une question d'équilibre... un équilibre délicat.

Laver, rincer, recommencer. Une fois l'ensemble initial de règles pour ce modèle d'attaque spécifique implémenté et optimisé, il convient de passer au vecteur d'attaque suivant, et ainsi de suite, en répétant le processus en modélisant chaque menace.

Ce processus ne s'arrête jamais. Il y a constamment de nouvelles attaques à modéliser et de nouveaux indicateurs à surveiller. Il est toujours important de suivre les informations de sécurité pour savoir quelles attaques sont en vogue. Les rapports tels que celui de Mandiant sur le groupe APT1 intègrent désormais des indicateurs clairs que chaque organisation peut surveiller avec son SIEM. Armé de ces renseignements sur les menaces et d'un environnement de collecte de données complet, il n'y a plus d'excuse : il est temps de commencer à chercher les attaques avancées qui continuent d'émerger.

Mais avec le temps, il sera nécessaire d'ajouter de nouveaux types de données au SIEM, ce qui impliquera de revoir toutes les règles. Par exemple, le trafic réseau, s'il est capturé et transmis au SIEM, fournira quantité de nouvelles informations à étudier. Mais comment ce regard sur le trafic réseau sera-t-il susceptible d'affecter la manière dont certaines attaques sont traitées ? Quelles autres règles faudrait-il ajouter pour détecter l'attaque plus vite ? Ce ne sont pas des questions triviales : il convient de revoir les règles du SIEM chaque fois qu'est ajoutée une nouvelle source de données (ou retirer, le cas échéant) ; cela peut faire la différence sur la rapidité avec laquelle une attaque est détectée... si elle l'est.

Le plus important aspect de ce processus est la cohérence. Le SIEM n'est pas une technologie du type « installe et oublie ». Il requiert du temps, de l'attention, et d'être alimenté, tout au long de sa vie opérationnelle.

10.3 quelques défits des SIEM

La problématique globale des SIEM est de corréler de l'événement, la question de fond est la collecte de ses évènements. La collecte de LOG est la principale sources d'événements, toutefois, toute les sources d'événements sont susceptible d'enrichir la corrélation, en particulier les vulnérabilités, les IOC, les infos de end-point en gros corrler des inforamtions d'opératione et de renseignements. Cette notion de FUSION de capteurs cher au militaire est un premier pas et nécessite en parrallele aussi de l'information econimoqie, poltiques ou sociale de l'entreprise. Car ces événements peuvent "matcher" avec des attaques complexes.

10.4 l'intelligence artificiel

Le traitement de masse permet

Mais l'important est que l'IA (ex : vectra) puisse explicquer ses propositions et décisions.

11. quelques SIEM

On peut ciert ainssi quelques SIEM non pas pour en faire un publicité particuliers mais simplement pour donner quelques indications sur la provenance ...

12. L'integration dans la gestion des incidents ITIL

13. Le SOC

Les SOC est au coeur du système de Veille Alerte et réponse. C'est la tour de contrôle de l'espace Cyber.

14. le SOC de demain

On peut par ailleurs s'interroger sur le fait qu'un tel système peut et doit opérer d'autres missions que les missions de sécurité pures. Si la supervision des réseaux a été longtemps au outils au services des techniciens, la supervision de l'environnement digital c'est à dire l'environnement informationnel de l'entreprise est un axe fondamental. Le SOC Security Operation Center peut devenir Cyber Operational Center opérant le suivi des risques digitaux au sens large, incluant les réseaux sociaux et leur cohorte de fausse informations et d'information pouvant être des indicateurs de crise à venir pour l'entreprise.

14.1 Evaluation d'un SOC

L'efficacité d'un SOC, et les purples Team.

14.2 Les outils connexes d'un SOC

au dela des SIEM, il semble important d'ajouter à l'outillage dun SOC un ensemble de système permettant de mesurer et d'évaluer l'impact des attaques. Echelle de RICHTER d'une attaque.

https ://observatoire-fic.com/prendre-la-mesure-des-cyberattaques-peut-on-definir-une-echelle-de-richter-dans-le-cyber/

15. surveiller les fuites

J'ai ajouté un chapitre spéciale sur les fuites de données pour deux grandes raisons

- La détection des fuites de données peuvent simplement se révéler par l'apparition de tout ou partie de ces données dans le Darkweb.
- Les fuites de données étant souvent des fuites de données de type "données personnelles", elles impliquent le déroulement de processus de déclaration au titre de la GDPR.

Je ne rentrerai pas ici dans la présentation du RGPD avec son cortège d'exigence et d'organisation à mettre en place Liste de traitement, déclaration, nomination de responsable, etc. Je ne vous propose que de regarder rapidement, la partie détection et partie réponse à incident.

Le terme « fuite de données », ou « data breach » en anglais, est utilisé pour toute situation impliquant la perte, la modification injustifiée ou la publication par accident, par malveillance, de données considérées ou marquées comme confidentielles.

Il est important dans la mise en place de scénario dans les SIEM, et dans le traitement de SOC que l'évènement de fuites de données personnelles puissent être traiter avec un mécanisme précis et documenté, car ces évènements sont très contraint par la réglementation. A titre de remarques, les évènements touchant la fuite de données liées à la protection du secret de défense (Secret Défense) puisse aussi être traité dans un processus particulier car les ces fuites peuvent aussi faire l'objet de procédure au pénal.

Le GDPR prévoit que le responsable du traitement des données à caractère personnel signale**au plus tôt** les fuites de données pouvant constituer une atteinte à la vie privée des personnes concernées. Cette information à la CNIL et aux personnes concernées en cas d'impact important sur ces personnes.

La méthodologie est assez simple pour peu que le constat de l'incident puisse être fait le plus vite possible. Cela peut se faire sur la base d'évènement provenant des équipements de sécurité (via un SIEM par exemple) ou par l'utilisation de services de veille, ou simplement par l'avertissement d'un tiers qui découvre cette fuite.

Détection Enrayer la fuite, Limiter l'impact Analyser les sources

Deuxièmement, vous devez entreprendre dès que possible les démarches pour enrayer l'incident ou en limiter l'impact. Tous les collaborateurs doivent respecter

plusieurs règles. S'ils trouvent des informations à un endroit inapproprié, ils doivent les supprimer ou en informer un responsable. Il peut s'agir de supports physiques, mais aussi de fichiers sur le réseau. Ils doivent également donner l'alerte s'ils rencontrent des étrangers non accompagnés dans une zone sécurisée. Et ainsi de suite. Si des alarmes indiquent un piratage ou une infection des systèmes, les gestionnaires de ces systèmes devront les examiner au plus vite et peut-être les désactiver de manière préventive.

En cas de doute, il est préférable d'arrêter un traitement ou d'empêcher le transport des données traitées jusqu'à ce que vous sachiez clairement s'il y a effectivement un problème, et dans quelle mesure les données traitées sont encore correctes. Cela permet souvent d'éviter qu'un incident ne se transforme en fuite de données. Tant que des données traitées à mauvais escient ne sont pas diffusées ou rendues publiques, il n'y a pas d'infraction, et donc pas d'impact. Au sens strict, il n'est pas encore question d'une fuite de données.

Ensuite, et éventuellement en parallèle, vous pouvez lancer une analyse des faits. D'une part, il faut établir la cause du problème. Vous pourrez ensuite réfléchir aux améliorations dans l'organisation, les systèmes ou les applications, et dans le mode de travail de vos collaborateurs, pour éviter que l'incident ne se reproduise. D'autre part, il faut examiner l'impact réel ou éventuel de l'incident. Y a-t-il des risques pour la confidentialité et l'intégrité des données ? S'agit-il (en partie) de données à caractère personnel ? Quelles peuvent-être les conséquences de cette infraction ? Dans de nombreux cas, il vous faudra du temps pour savoir quelle quantité de données a été impactée et combien de personnes sont concernées. Souvent, vous ne saurez pas non plus d'emblée s'il y a véritablement un risque d'impact, ni quelle peut être l'ampleur des dommages.

Ce n'est que lorsque vous aurez une réponse à toutes ces questions qu'il vous sera possible de faire le bon choix quant à la nécessité de signaler la fuite de données à la Commission de protection de la Vie Privée ou aux personnes concernées. Le quand et le comment de ce signalement seront abordés dans le prochain article.

Par ailleurs, chaque incident doit être consigné dans un registre interne. Qu'il s'agisse d'une véritable infraction ou d'un quasi-accident, il faut toujours analyser l'incident. Ces informations sont importantes pour évaluer les procédures et les directives existantes, et vérifier si les mesures prises offrent une protection suffisante contre les risques éventuels. Les causes d'un incident doivent être consignées, au même titre que les actions visant une amélioration. En assurant un suivi systématique, vous améliorerez systématiquement la sécurité de votre organisation.

Dans les cas extrêmes, une fuite de données peut être catastrophique. Une organisation peut être confrontée à des problèmes de communication dantesques

suite à une fuite de données très sensibles à propos d'un grand nombre de personnes. Il arrive que la fuite de données sorte des murs de l'organisation et que la presse en soit informée. En pareil cas, il est bon de pouvoir retomber sur des scénarios de communication de crise préalablement établis. Si votre organisation est couverte par une assurance couvrant les risques de cyber-sécurité, votre compagnie d'assurance devrait pouvoir vous aider.

Si vous soupçonnez que l'incident est d'origine criminelle, vous devez veiller à constituer un dossier juridique à temps. Il est parfois important de réaliser un back-up rapide des systèmes au moment de la découverte de l'incident ou de conserver les fichiers log, avant que ces informations ne soient perdues ou modifiées par les démarches entreprises pour résoudre l'incident. Il est évident qu'une telle étape ira parfois à l'encontre de ce qu'il convient de faire rapidement pour limiter le problème existant. Si la police ou la justice intervient, ne perdez jamais de vue ce que vous pouvez et ne pouvez pas faire de votre propre chef, surtout si vous êtes en charge du traitement des données. Faites appel au responsable dès que possible. Si les autorités vous obligent à fournir des informations, vous devez toujours veiller à les protéger au mieux et à ne pas exposer de données (par exemple d'autres personnes concernées) si cela n'est pas nécessaire à l'enquête.

Il est judicieux de bien documenter ces démarches successives, afin que chacun dans l'organisation les connaisse et agisse en fonction. Cela peut également s'avérer utile pour démontrer que vous prenez le respect des obligations du GDPR très au sérieux.

Références

(1) Bruce SCHNEIER. « Attack trees ». In : *Dr. Dobb's journal* 24.12 (1999), pages 21-29 (cf. page 9).

16. Contributions

16.1 Comment contribuer

Les notes et les présentations sont réalisées sous LaTeX.

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [1] . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.
Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

16.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

16.2.1 Années 2019

- **François REGIS** (Orange) : CyberHunting

16.2.2 Années 2018

- **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

1. https://github.com/edufaction/CYBERDEF

Table des matières

Table des figures