

UNIVERSITÉ DE LORRAINE

FACULTÉ D’INFORMATIQUE

MASTER 2 INFORMATIQUE :

SÉCURITÉ DES SYSTÈMES D’INFORMATION

RAPPORT SÉCURITÉ DES SYSTÈMES D’INFORMATION

AUTEURS : PROFESSEUR : Promotion Master SSI 2021-2022 Jean-Marc MISERE

METZ

Octobre 2021

Table des matières

1 Introduction 6

2 SOC / CSIRT / CERT 7 2.1 Définitions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7 2.1.1 SOC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7 2.1.2 CSIRT . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7 2.1.3 CERT . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 2.2 Rôles, Missions et Métiers . . . . . . . . . . . . . . . . . . . . . . . 8 2.2.1 SOC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8 2.2.2 CSIRT / CERT . . . . . . . . . . . . . . . . . . . . . . . . . 11 2.3 Leurs interactions . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18 2.3.1 Couverture Fonctionnelle . . . . . . . . . . . . . . . . . . . . 18 2.3.2 Organisation des CSIRT / CERT . . . . . . . . . . . . . . . 19 2.4 Comment choisir ? . . . . . . . . . . . . . . . . . . . . . . . . . . . 21 2.4.1 Les modèles de déploiement d’un SOC . . . . . . . . . . . . 21 2.4.2 Les défis d’un Security Operation Center (SOC) . . . . . . . 22 2.4.3 Le coût . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23 2.4.4 Les questions à se poser lors de la création d’un SOC . . . . 24 2.4.5 Les modèles organisationnels d’un CSIRT . . . . . . . . . . 25 2.5 Résumé et perspective d’évolution . . . . . . . . . . . . . . . . . . . 26 2.5.1 Les avantages d’un Security Operation Center (SOC) . . . . 26 2.5.2 Les avantages d’un CSIRT . . . . . . . . . . . . . . . . . . . 27 2.5.3 Évolution . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28

3 SOC, procédures et outils 30 3.1 Sources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30 3.2 La détection des menaces . . . . . . . . . . . . . . . . . . . . . . . . 30

3.2.1 Les ressources utilisées par les outils du SOC : les logs . . . 30 3.2.2 LMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33 3.2.3 SIM SEM SIEM . . . . . . . . . . . . . . . . . . . . . . . . . 35

3.3 Réaction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42 3.3.1 SOAR . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42 3.3.2 Prise de contact et neutralisation . . . . . . . . . . . . . . . 44

3.4 Crise . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45 3.4.1 Le CSIRT . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45 3.4.2 Le SIRP (Security Incident Response Plan) . . . . . . . . . 47 3.5 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 48

2

*TABLE DES MATIÈRES* 3

4 Traitement d’une menace 50 4.1 Sources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50 4.2 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50 4.3 Le traitement de la menace avant la réalisation . . . . . . . . . . . . 52

4.3.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 52 4.3.2 Sécurité Basique . . . . . . . . . . . . . . . . . . . . . . . . 52 4.3.3 Sécurité Intermédiaire . . . . . . . . . . . . . . . . . . . . . 53 4.3.4 Sécurité Avancée . . . . . . . . . . . . . . . . . . . . . . . . 54 4.3.5 Se préparer . . . . . . . . . . . . . . . . . . . . . . . . . . . 56

4.4 Le traitement de la menace pendant la réalisation . . . . . . . . . . 57 4.4.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 57 4.4.2 Identification . . . . . . . . . . . . . . . . . . . . . . . . . . 57 4.4.3 Cellule de crise . . . . . . . . . . . . . . . . . . . . . . . . . 60 4.4.4 Logs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 61 4.4.5 Déconnexion . . . . . . . . . . . . . . . . . . . . . . . . . . . 61 4.4.6 Communication . . . . . . . . . . . . . . . . . . . . . . . . . 62 4.4.7 Précaution . . . . . . . . . . . . . . . . . . . . . . . . . . . . 64 4.4.8 Identification avancée . . . . . . . . . . . . . . . . . . . . . . 64 4.4.9 Informations . . . . . . . . . . . . . . . . . . . . . . . . . . . 65

4.5 Le traitement de la menace après la réalisation . . . . . . . . . . . . 67 4.5.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 67 4.5.2 Consignes générales . . . . . . . . . . . . . . . . . . . . . . . 67 4.5.3 Le dossier pour la police . . . . . . . . . . . . . . . . . . . . 68 4.6 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 69

5 Évolution des menaces 70 5.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 70 5.2 Les acteurs intéressés . . . . . . . . . . . . . . . . . . . . . . . . . . 71

5.2.1 Individus isolés . . . . . . . . . . . . . . . . . . . . . . . . . 71 5.2.2 Groupes indépendants . . . . . . . . . . . . . . . . . . . . . 73 5.3 Les APT . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 76 5.3.1 Définitions . . . . . . . . . . . . . . . . . . . . . . . . . . . . 76 5.3.2 Mode Opératoire . . . . . . . . . . . . . . . . . . . . . . . . 76 5.3.3 Rapports sur les APT . . . . . . . . . . . . . . . . . . . . . 77 5.3.4 Prévention . . . . . . . . . . . . . . . . . . . . . . . . . . . . 79 5.4 Les attaques . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 79 5.4.1 Client-side VS Server-side . . . . . . . . . . . . . . . . . . . 80 5.4.2 Attaques Client-side . . . . . . . . . . . . . . . . . . . . . . 81 5.4.3 Attaques Server-side . . . . . . . . . . . . . . . . . . . . . . 84 5.4.4 Mise à niveau d’attaques répandues . . . . . . . . . . . . . . 88 5.4.5 Attaques derniers cris . . . . . . . . . . . . . . . . . . . . . . 94 5.5 Résumé . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99

6 Évolution des Techniques de défense (Concepts et Méthodes) 100 6.1 MITRE ATT&CK . . . . . . . . . . . . . . . . . . . . . . . . . . . 100 6.1.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 100 6.1.2 Matrice MITRE ATT&CK . . . . . . . . . . . . . . . . . . . 100 6.1.3 Outils CALDERA . . . . . . . . . . . . . . . . . . . . . . . 102

*TABLE DES MATIÈRES* 4

6.1.4 Les différentes équipes de CALDERA . . . . . . . . . . . . . 102 6.1.5 Les avantages d’utiliser le framework MITRE ATT&CK avec le SIEM . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 103 6.1.6 ATT&CK ™ Navigator . . . . . . . . . . . . . . . . . . . . 103 6.1.7 Avantages et inconvénients . . . . . . . . . . . . . . . . . . . 104 6.2 Les IOC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 104 6.2.1 Qu’est ce-qu’un IOC ? . . . . . . . . . . . . . . . . . . . . . 104 6.2.2 Comment fonctionnent les IOC ? . . . . . . . . . . . . . . . 105 6.2.3 Exemples d’IOC . . . . . . . . . . . . . . . . . . . . . . . . 106 6.2.4 Outils permettant la mise en oeuvre des IOC . . . . . . . . . 107 6.3 Les CTI . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 109 6.3.1 Définition des CTI . . . . . . . . . . . . . . . . . . . . . . . 109 6.3.2 Le rôle des CTI . . . . . . . . . . . . . . . . . . . . . . . . . 109 6.3.3 Situation de la Threat Intelligence . . . . . . . . . . . . . . . 110 6.3.4 Les entreprises sur le marché des CTI . . . . . . . . . . . . . 110 6.3.5 Le fonctionnement d’un CTI . . . . . . . . . . . . . . . . . . 110 6.3.6 Les types de CTI . . . . . . . . . . . . . . . . . . . . . . . . 111 6.3.7 Les moyens de collecte . . . . . . . . . . . . . . . . . . . . . 112 6.3.8 Les différents outils utilisés . . . . . . . . . . . . . . . . . . . 113 6.3.9 Les obstacles de l’implémentation des CTI . . . . . . . . . . 113 6.3.10 Avantages et inconvénients des CTI . . . . . . . . . . . . . . 114 6.4 Threat Hunting . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 114 6.4.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 114 6.4.2 Sécurité offensive : Le threat Hunting comme une valeur ajou tée liée aux professionnels eux-mêmes . . . . . . . . . . . . . 114 6.4.3 Principales caractéristiques du Threat Hunting . . . . . . . . 115 6.4.4 Techniques courantes de Threat Hunting . . . . . . . . . . . 115 6.4.5 Le threat hunting renforce la protection de l’entreprise . . . 116 6.4.6 Threat hunting ou réponse à incident . . . . . . . . . . . . . 116 6.4.7 Parvenir à un consensus sur le threat hunting . . . . . . . . 117 6.4.8 Processus pour effectuer le Theat Hunting . . . . . . . . . . 117 6.4.9 Outils de Threat Hunting Observer GigaFlow . . . . . . . . 118 6.4.10 Avantages du Threat Hunting . . . . . . . . . . . . . . . . . 118 6.5 Bug Bounty . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 118 6.5.1 Qu’est-ce que le bug bounty ? . . . . . . . . . . . . . . . . . 118 6.5.2 Comment sont réalisés les programmes ? . . . . . . . . . . . 119 6.5.3 Les primes . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120 6.5.4 Auto-héberger vs Plateforme ? . . . . . . . . . . . . . . . . . 120 6.5.5 Pentest ou bug bounty ? . . . . . . . . . . . . . . . . . . . . 121 6.6 La journalisation . . . . . . . . . . . . . . . . . . . . . . . . . . . . 124 6.6.1 Définition de la journalisation . . . . . . . . . . . . . . . . . 124 6.6.2 Le rôle de la journalisation . . . . . . . . . . . . . . . . . . . 124 6.6.3 La centralisation des logs . . . . . . . . . . . . . . . . . . . . 125 6.6.4 Les types de journalisation . . . . . . . . . . . . . . . . . . . 126 6.6.5 Avantages et inconvénients de l’analyse des logs . . . . . . . 127

*TABLE DES MATIÈRES* 5

7 Évolution des Techniques de défense (Outils innovants) 128 7.1 L’intelligence Artificielle . . . . . . . . . . . . . . . . . . . . . . . . 128 7.1.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 128 7.1.2 Définition . . . . . . . . . . . . . . . . . . . . . . . . . . . . 129 7.1.3 L’intelligence Artificielle dans la cyber-sécurité . . . . . . . . 129 7.2 Machine Learning . . . . . . . . . . . . . . . . . . . . . . . . . . . . 131 7.2.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 131 7.2.2 Définitions . . . . . . . . . . . . . . . . . . . . . . . . . . . . 131 7.2.3 Les systèmes d’auto-défense . . . . . . . . . . . . . . . . . . 133 7.3 EDR/XDR/MDR/NDR . . . . . . . . . . . . . . . . . . . . . . . . 135 7.3.1 Limite des Antivirus traditionnels . . . . . . . . . . . . . . . 135 7.3.2 Endpoint Detection and Response . . . . . . . . . . . . . . . 135 7.3.3 Network Detection and Response . . . . . . . . . . . . . . . 137 7.3.4 Extended Detection and Response . . . . . . . . . . . . . . . 138 7.3.5 MDR . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 139 7.3.6 Meilleure solution . . . . . . . . . . . . . . . . . . . . . . . . 140 7.4 Les WAF . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141 7.4.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141 7.4.2 Définition . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141 7.4.3 Architecture . . . . . . . . . . . . . . . . . . . . . . . . . . . 141 7.4.4 WAF exemple de fonctionnement . . . . . . . . . . . . . . . 143 7.4.5 Les limites . . . . . . . . . . . . . . . . . . . . . . . . . . . . 145 7.5 Le Phishing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 146 7.5.1 Contexte . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 146 7.5.2 Qu’est-ce que le Phishing ? . . . . . . . . . . . . . . . . . . . 146 7.5.3 Lutter contre le phishing . . . . . . . . . . . . . . . . . . . . 147

8 Conclusion 148

Chapitre 1

Introduction

Dans ce projet supervisé par Mr Jean-Marc MISERT, nous allons traiter de différentes facettes de la cybersécurité, avec pour objectif de construire un guide sur la cybersécurité. Ce guide s’articulera autour de six points majeurs :

— SOC / CSIRT / CERT

— SOC, procédures et outils

— Traitement d’une menace

— Évolution des menaces

— Évolution des Techniques de défense (Concepts et Méthodes) — Évolution des techniques de défense (outils innovants)

6

Chapitre 2

SOC / CSIRT / CERT

2.1 Définitions

2.1.1 SOC

Un SOC (Security Operation Center) est un centre de commande pour les pro fessionnels de la cybersécurité chargé de surveiller, d’analyser et de protéger une entreprise contre les cyberattaques.

Dans un Security Operation Center, le trafic Internet, l’infrastructure réseau interne, les postes de travail, les serveurs, les endpoints, les bases de données, les applications, les objets connectés (IoT) ainsi que d’autres systèmes sont surveillés en permanence afin de détecter les incidents de sécurité. Ces incidents sont identifiés, analysés, communiqués, actionnés / défendus, enquêtés et signalés par le SOC.

De plus, la surveillance des applications à pour but d’identifier une éventuelle cyberattaque ou intrusion (événement) et de catégoriser la menace (incident) afin de déterminer si elle est réelle et malveillante avec son impact sur l’entreprise. Au sein d’un SOC, le personnel peut travailler avec d’autres équipes ou départements interne ou externe, mais est généralement autonome avec des employés qui ont des compétences en matière de cybersécurité bien particulières.

La plupart des SOC fonctionnent 24h/24 et 7j/7, les employés travaillent en équipes pour surveiller en permanence l’activité du réseau et mitiger les menaces. Le déploiement d’un SOC peut se faire en interne, ou être entièrement, voire par tiellement, sous-traité à des fournisseurs externes.

2.1.2 CSIRT

L’équipe d’un CSIRT est chargée de prévenir et de réagir en cas d’incidents de sécurité informatique. En amont, elle assure notamment une veille pour connaître l’état de la menace et évaluer les propres vulnérabilités de son organisation. En aval, elle analyse et traite les incidents de sécurité en aidant à leur résolution. C’est une équipe qui centralise et sert de relais que ce soit en interne et ou externe de l’entreprise.

7

*CHAPITRE 2. SOC / CSIRT / CERT* 8

2.1.3 CERT

Suite à la première attaque massive sur internet lié au vers de Morris lancé le 2 novembre 1988, La DARPA (Defense Advanced Research Projects Agency) fonde CERT/CC (Computer Emergency Response Team/Coordination Center) considéré comme le premier CSIRT (Computer Security Incident Response Teams) 1.

Le terme CERT est une marque déposée par l’université Carnegie Mellon. Avant, les CSIRT devaient demander l’autorisation d’utiliser le nom de « CERT », désor mais l’université de Carnegie Mellon continue à gérer les demandes pour les CSIRT américains mais ne s’oppose plus à son utilisation en dehors du sol américain 2.

Au sens strict comme définie par l’Université Carnegie Mellon depuis 1997 le terme CERT ne devrait plus définir un acronyme et ne devrait plus non plus définir une fonction dans une organisation mais dans l’usage nous trouvons de nombreuses références qui définissent les CERT comme des services plus orientés sur le thread intelligence avec une vision plus globale et plus éloigné du domaine d’activité de l’entreprise 3.

2.2 Rôles, Missions et Métiers

2.2.1 SOC

Le SOC surveille les données de sécurité générées au niveau de l’ensemble de l’infrastructure IT de l’entreprise, en allant des systèmes hôtes et des applications jusqu’aux périphériques réseau et de sécurité, tels que les pare-feu et les solutions antivirus. En combinant une gamme d’outils avancés et les compétences de pro fessionnels expérimentés en matière de cybersécurité, le SOC remplit les fonctions vitales suivantes :

— Surveillance, détection, investigation et triage des alertes des événements de sécurité.

— Gestion des réponses aux incidents de sécurité, notamment l’analyse des mal wares et les investigations forensiques.

— Gestion des renseignements sur les menaces (ingestion, production, curation et diffusion).

— Gestion des vulnérabilités basée sur les risques (notamment, la priorisation des correctifs).

— Traque des menaces.

— Gestion et maintenance des dispositifs de sécurité.

— Développement de données et d’indicateurs pour le reporting/la gestion de la conformité.

1. https://www.cert.ssi.gouv.fr/csirt

2. https://www.sei.cmu.edu/our-work/cybersecurity-center-development/ authorized-users

3. https://www.sei.cmu.edu/education-outreach/license-sei-materials/ authorization-to-use-cert-mark

*CHAPITRE 2. SOC / CSIRT / CERT* 9 

Figure 2.1 – Schéma explicatif de la composition d’un SOC moderne

Le SOC comprend un ensemble d’outils dans une pile technologique distincte pour aider les analystes en cybersécurité à surveiller en permanence les activités de sécurité dans l’infrastructure IT de l’entreprise. Les membres de l’équipe de sécurité affectés au Security Operation Center utilisent ces outils pour identifier, classer, analyser les incidents et événements, et décider comment réagir face à ces événements.

Les outils essentiels de la pile technologique SOC sont :

— Une solution SIEM (Security Information and Event Management) Les outils de gestion des informations et des événements de sécurité (SIEM) constituent la base du SOC, étant donné leurs capacités à corréler les règles avec des quantités massives de données hétérogènes afin de détecter les me naces. L’intégration des renseignements sur les menaces (Threat Intelligence) ajoute une importante valeur à l’activité SIEM en contextualisant et en prio risant les alertes.

— Une surveillance comportementale

La capacité UEBA (User and Entity Behavioral Analytics), généralement ajoutée dans un deuxième temps à la plateforme SIEM, aide les équipes de sé curité à créer des points de référence en appliquant la modélisation du compor tement ainsi que l’apprentissage automatique afin de faire émerger les risques de sécurité.

— La découverte d’actifs

La découverte d’actifs, aussi appelée répertoire d’actifs, aide à mieux com prendre quels systèmes et outils sont en cours d’exécution dans votre en vironnement. Il permet de déterminer quels sont les systèmes critiques de l’entreprise et comment prioriser les contrôles de sécurité.

— L’évaluation de la vulnérabilité

Détecter les failles qu’un attaquant peut utiliser pour pénétrer au sein des sys tèmes est essentiel pour protéger l’environnement de l’entreprise. Les équipes

*CHAPITRE 2. SOC / CSIRT / CERT* 10

de sécurité doivent rechercher les vulnérabilités des systèmes pour repérer les potentielles brèches et agir en conséquence. Certaines certifications et régle mentations exigent également des évaluations périodiques de la vulnérabilité pour permettre de valider la conformité.

— La détection de l’intrusion

Les systèmes de détection d’intrusion (IDS) sont des outils incontournables permettant aux SOC de détecter les attaques dès les premiers stades. Ils fonc tionnent généralement en identifiant les schémas d’attaque connus à l’aide de signatures d’intrusion.

Les métiers au sein du SOC 4:

— Responsable SOC :

Le responsable du SOC planifie et organise les opérations quotidiennes du SOC afin d’évaluer le niveau de vulnérabilité et de détecter des activités sus pectes ou malveillantes. Il met en place le service de détection des incidents de sécurité. Il valide la bonne exécution des processus de supervision et de gestion des évènements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d’amélioration des services du SOC.

Rôle dans le pilotage des opérations :

— Planifier et organiser les opérations quotidiennes du SOC

— Assurer un appui opérationnel à la gestion de crise de sécurité en cas d’incidents de sécurité majeurs

— Assurer les relations avec les équipes de réponse à incidents CERT ou CSIRT

Rôle stratégique de prévention et de détection :

— Définir la stratégie du SOC avec une cohérence technique

— Définir et mettre en œuvre les outils du SOC pour la collecte des évè nements, l’accès aux plateformes de sécurité, la gestion des alertes, les workflows de suivi d’incidents de sécurité

— Définir les cas d’usages de détection et les intégrer dans les outils de détection

— Mettre en place des outils de notifications et les faire évoluer — Créer des synergies avec les autres équipes de sécurité

Le responsable du SOC doit acquérir une bonne compréhension des besoins de supervision pour les activités métiers critiques

— Opérateur Analyste SOC :

Il assure la supervision du système d’information de l’organisation afin de dé tecter des activités suspectes ou malveillantes. Il identifie, catégorise, analyse et qualifie les événements de sécurité en temps réel ou de manière asynchrone

4. https://www.ssi.gouv.fr/uploads/2015/07/anssi-panorama\_metiers\_ cybersecurite-2020.pdf

*CHAPITRE 2. SOC / CSIRT / CERT* 11

sur la base de rapports d’analyse sur les menaces. Il contribue au traitement des incidents de sécurité avérés en support des équipes opérationnelles.

Rôle de détection :

— Identifier les événements de sécurité en temps réel, les analyser et les qualifier

— Évaluer la gravité des incidents de sécurité

— Notifier les incidents de sécurité, escalader le cas échéant

Activité de réaction :

— Transmettre les plans d’action aux entités en charge du traitement — Faire des recommandations sur les mesures immédiates

— Accompagner le traitement des incidents par les équipes d’investigation Autres activités :

— Contribuer à la mise en place du service de détection (SIEM, etc.) — Contribuer à la définition de la stratégie de collecte et de corrélation des journaux d’évènements

— Collaborer à l’amélioration continue des procédures

— Contribuer à la veille permanente sur les menaces

— Renseigner les tableaux de bord rendant compte de l’activité opération nelle

— Maintenir à jour la documentation

— Activités de recherche de compromissions (threat hunting)

L’opérateur du SOC pourra également être amené à développer des compé tences en machine learning afin de renforcer les capacités de détection.

2.2.2 CSIRT / CERT

L’ANSSI (Agence nationale de la sécurité des systèmes d’information) définie les cinq missions principales suivantes comme étant à la charge des CSIRT 5:

— Centralisation des demandes d’assistance suite aux incidents de sécurité (at taques) sur les réseaux et les systèmes d’informations : réception des de mandes, analyse des symptômes et éventuelle corrélation des incidents.

— Traitement des alertes et réaction aux attaques informatiques : analyse tech nique, échange d’informations avec d’autres CSIRT, contribution à des études techniques spécifiques.

— Établissement et maintenance d’une base de données des vulnérabilités. — Prévention par diffusion d’informations sur les précautions à prendre pour minimiser les risques d’incident ou au pire leurs conséquences.

5. https://www.cert.ssi.gouv.fr/csirt/

*CHAPITRE 2. SOC / CSIRT / CERT* 12

— Coordination éventuelle avec les autres entités (hors du domaine d’action) : centres de compétence réseaux, opérateurs et fournisseurs d’accès à Internet, CSIRT nationaux et internationaux.

La RFC-2350 6 publié en 1998 par IETF (Internet Engineering Task Force) veut standardiser les bonnes pratiques que doivent suivre un CSIRT, et le questionnaire « ENISA Maturity Evaluation Methodology for CSIRTs » dans la version 2.0 a été publié 9 avril 2019 par l’ENISA (European Network and Information Security Agency) pour permettre d’évaluer son CSIRT selon 44 questions répartis sur les thèmes suivants : organisationnel, personnel, outils, processus 7.

L’ENISA 8reprend la liste des services suivants définie par le CERT/CC pour les CSIRT, à priori aucun CSIRT ne fournirait la totalité de ces services : Les services de base sont indiqués en caractères gras et seront détaillés au fur et à mesure sur la base de leurs définitions données par l’ENISA.

— Services réactifs :

Les services réactifs sont conçus pour répondre aux demandes d’assistance, aux signalements d’incidents et à toute menace ou attaque à l’encontre de systèmes.

— Alertes et avertissements

Ce service consiste à diffuser des informations décrivant une attaque, une vulnérabilité de sécurité, une alerte d’intrusion, un virus informatique ou un canular, et à recommander des mesures à court terme pour remédier aux problèmes qui en découlent. Le bulletin d’alerte, d’avertissement ou de sécurité est envoyé en réaction au problème survenu, afin de prévenir ou conseiller.

— Traitement des incidents

Le traitement des incidents consiste à recevoir, trier et répondre aux de mandes et aux signalements, et à analyser les incidents et évènements. Les réponses peuvent être entre autres : filtrer le trafic sur le réseau, res taurer les systèmes, appliquer des correctifs aux systèmes ou les réparer. — Analyse des incidents

L’analyse des incidents consiste essentiellement à examiner toutes les informations disponibles, ainsi que les éléments probants ou artefacts re latifs à un incident ou un événement donné. L’analyse a pour but de déterminer l’ampleur de l’incident, l’étendue du dommage causé, la na ture de l’incident et les stratégies de réponse ou solutions temporaires. Le CSIRT établit des corrélations entre différents incidents, afin d’établir d’éventuelles interactions, des tendances et des profils, voire la signature des intrus. Le CSIRT peut également participer au rassemblement de preuves légales.

— Réponse aux incidents sur place

6. https://www.ietf.org/rfc/rfc2350.txt

7. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/ csirt-maturity/csirt-survey

8. https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-french/ at\_download/fullReport

*CHAPITRE 2. SOC / CSIRT / CERT* 13

— Appui à la réponse aux incidents

Par téléphone, par courriel, par télécopie ou par l’envoi de documen tation, le CSIRT fournit aux victimes d’une attaque l’assistance et les orientations dont elles ont besoin pour restaurer leurs systèmes après un incident.

— Coordination de la réponse aux incidents

Le CSIRT coordonne les actions de réponse menées par toutes les par ties concernées. Le travail de coordination peut comprendre la collecte de coordonnées de contact, la notification aux sites de leur implication éven tuelle (en tant que victime ou source d’une attaque), la compilation de statistiques concernant le nombre de sites concernés, et la facilitation de l’échange et de l’analyse des informations. Le travail de coordination peut également couvrir la notification et la collaboration avec le département juridique, le département des ressources humaines ou le département des relations publiques de l’organisation, de même que la coordination avec des représentants de la loi.

— Traitement des vulnérabilités

— Analyse des vulnérabilités

— Réponse aux vulnérabilités

— Coordination des réponses aux vulnérabilités

— Services proactifs :

Les services proactifs sont destinés à améliorer l’infrastructure et les proces sus sécuritaires des parties prenantes avant qu’un incident ou un événement survienne ou soit détecté. Leur but principal est donc de prévenir les incidents et d’en réduire l’impact et l’étendue s’ils surviennent.

— Annonces

Ce service vise de manière non limitative les alertes d’intrusion, les aver tissements de vulnérabilité et les bulletins de sécurité. Ces annonces informent les parties prenantes de développements nouveaux appelés à avoir un impact de court à moyen terme, tels que les vulnérabilités et outils d’intrusion récemment découverts. Elles permettent donc aux par ties prenantes de protéger leurs systèmes et réseaux contre les problèmes récemment détectés, avant même qu’ils puissent être exploités.

— Veille technologique

— Audits ou évaluations de la sécurité

— Configuration et maintenance de la sécurité

— Développement d’outils de sécurité

— Services de détection des intrusions

— Diffusion d’informations relatives à la sécurité

— Traitement des artefacts :

Un artefact est un fichier ou objet quelconque trouvé dans un système et sus ceptible d’avoir servi à une tentative d’attaque ou à une attaque de systèmes et de réseaux, ou qui sert à contrecarrer les mesures de sécurité. Les artefacts comprennent entre autres les virus informatiques, les chevaux de Troie, les

*CHAPITRE 2. SOC / CSIRT / CERT* 14

vers, les scripts d’exploitation et les boîtes à outils.

Le traitement consiste à recevoir des informations concernant les artefacts, voire des copies de ceux-ci, utilisés pour des intrusions, des reconnaissances et d’autres activités non autorisées ou perturbatrices. À réception, l’artefact fait l’objet d’un examen couvrant sa nature, son fonctionnement, sa version et son utilisation afin d’élaborer une stratégie de réponse en vue de sa détection, de son élimination et de sa prévention. Étant donné que les divers types de CSIRT ont une approche différente du traitement des artefacts, ce service est lui-même divisé en catégories correspondant au type d’activité exercée et au type d’aide fournie.

— Analyse des artefacts

— Réponse aux artefacts

— Coordination des réponses aux artefacts

— Gestion de la qualité de la sécurité :

Les services inclus de cette catégorie ne relèvent pas spécifiquement du trai tement des incidents ou des CSIRT, il s’agit de services bien établis visant à améliorer la sécurité générale d’une organisation. En valorisant les expé riences acquises dans le cadre de la prestation de services réactifs et proactifs, un CSIRT peut ouvrir à l’intention de ces services de gestion de la qualité des perspectives qu’ils n’auraient sans doute pas eues autrement.

— Analyse des risques

— Continuité de l’activité et reprise après sinistre

— Consultance en matière de sécurité

— Sensibilisation

— Éducation/formation

— Évaluation ou certification des produits

Quelques actions concrètes des CSIRT :

Le CERT-FR de l’ANSSI diffuse de manière publique des informations sur les me naces afin de proposer une source d’information en français des failles récemment découvertes ainsi que des manières connues de s’en prémunir.

Figure 2.2 – Informations disponibles en ligne

*CHAPITRE 2. SOC / CSIRT / CERT* 15

Le CERT Santé en coordination avec l’ANSSI est intervenu, en 2020, directement au profit de 9:

— Dix établissements de santé publics, dont quatre OSE (Opérateurs de Services Essentiels). Ces incidents avaient pour origine des attaques par rançongiciel, par déni de service et un dysfonctionnement des équipements de sécurité (faux positifs).

— Deux EHPAD, l’un victime d’un rançongiciel et l’autre pour une compromis sion potentielle.

— D’un prestataire d’un établissement médico-social dans le domaine du handi cap qui a été victime d’un rançongiciel.

Malgré la croissance soutenue de par leur nombre, avoir un CSIRT membre de l’interCERT reste accessible qu’aux grands groupes ayant une forte maturité sur la sécurité des systèmes d’information 10

— Organe National : ANS, ANSSI, Éducation Nationale, Ministère de l’Intérieur, Ministère des Armées, Police nationale. . .

— Banque et assurance : AG2R La Mondiale, AXA, Banque populaire, BNP Paribas, Crédit Agricole, Société Générale. . .

— Fournisseur de service essentiel : EDF, ENGIE, ENEDIS, Le Groupe La Poste, Orange, SNCF, SUEZ, Total SE. . .

— Grands groupes industriels : Airbus, Dassault Aviation, L’Oréal, Michelin, Naval Group, STMicroelectronic, Thales, VINCI. . .

C’est pourquoi il existe des CSIRT comme « CERT Orange Cyberdefense » ou « CERT Sogeti ESEC » qui proposent leurs services auprès d’autres organisa tions dans le cadre de contrat. Cette liste n’est pas exhaustive par exemple l’on peut trouver des société comme THETRIS qui propose leur service de CSIRT sans nécessairement avoir rejoint l’InterCERT.

Métier au sein du CSIRT 11 :

— Responsable du CSIRT :

Il est responsable d’une équipe de réponse aux incidents de sécurité ciblant les systèmes d’information de l’organisation. Il s’assure de la bonne exécution des investigations et de la coordination des parties prenantes lors d’un incident de sécurité. Lors d’incidents à fort impact, le responsable du CSIRT est amené à interagir avec l’équipe de gestion de crise.

Pilotage des opérations :

— Planifier et organiser les opérations quotidiennes du CSIRT. — Assurer un appui opérationnel à la gestion de crise de sécurité en cas d’incidents de sécurité majeurs.

— Organiser les modes de fonctionnement avec le SOC interne ou externe pour assurer la gestion des incidents de sécurité par anticipation.

9. https://esante.gouv.fr/sites/default/files/media\_entity/documents/mss\_ans\_ rapport\_public\_observatoire\_signalements\_issis\_2020\_v0.96\_09042020\_vf.pdf 10. https://www.cert.ssi.gouv.fr/csirt/intercert-fr/

11. https://www.ssi.gouv.fr/uploads/2015/07/anssi-panorama\_metiers\_ cybersecurite-2020.pdf

*CHAPITRE 2. SOC / CSIRT / CERT* 16

Anticipation :

— S’appuyer sur les services de veille sur les menaces (threat intelligence). — Informer les équipes en charge de la sécurité des nouvelles menaces im portantes et recommander des mesures tactiques pour les contrer. — Construire et maintenir des relations de confiance et d’échange avec les réseaux de CSIRT français et étrangers ainsi qu’avec les organismes gou vernementaux.

— Participer aux exercices de préparation à la gestion de crise de cybersé curité.

Réponses aux incidents :

— Élaborer et tenir à jour le processus d’intervention en cas d’incident majeur de sécurité.

— Vérifier que les prérequis techniques et documentaires sont en place et tenus à jour.

— S’assurer que les parties prenantes connaissent leur rôle dans la gestion des incidents de sécurité.

— S’assurer de la bonne exécution du processus de réponse à incident depuis la détection jusqu’à la résolution de l’incident.

— Organiser les retours d’expérience concernant les incidents.

— Analyste Gestion des incidents et des crises de sécurité (CSIRT) : L’analyste réponse aux incidents de sécurité intervient généralement au sein d’un CERT ou CSIRT. En cas de soupçons sur une activité malveillante ou d’attaque au sein du système d’information, l’analyste réponse aux incidents de sécurité analyse les symptômes et réalise les analyses techniques sur le système d’information. Il identifie le mode opératoire de l’attaquant et qualifie l’étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l’assainissement et le durcissement des systèmes attaqués. Anticipation :

— Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles tech nologies et sur les méthodes des attaques.

— Alimenter les bases de renseignement sur les menaces (threat intelli gence).

— Maintenir et développer des outils d’investigation.

Analyse des incidents :

— Collecter les informations techniques d’un large ensemble de systèmes d’information, réaliser la recherche d’indicateurs de compromission. — Analyser les relevés techniques réalisés.

— Rédiger des rapports d’investigation.

Conseil :

— Préconiser des mesures de contournement et de remédiation de l’incident (assainissement et durcissement).

*CHAPITRE 2. SOC / CSIRT / CERT* 17

— Préconiser des mesures d’amélioration des capacités d’analyse (extraction des indicateurs de compromission).

— Préparer des rapports Formation.

L’analyste réponse aux incidents de sécurité peut être spécialisé en tant qu’analyste système, analyste réseau, analyste de codes malveillants. — Gestionnaire de crise de cybersécurité (CSIRT-CERT) : Le gestionnaire de crise de cybersécurité intervient souvent au sein d’un CSIRT ou d’un CERT externe ou interne pour grandes organisations, ou bien dans une équipe dédiée à la gestion de crise travaillant étroitement avec le CSIRT. Il analyse l’ampleur de la crise, met en place les actions nécessaires à sa résolution et coordonne les équipes pour qu’elles appliquent ses recom mandations. Il conseille les directions métiers afin de résoudre les crises de cybersécurité. Il organise la capacité de l’organisation à affronter de nouvelles menaces en matière de cybersécurité.

Anticipation :

— Conseiller l’organisation pour lui permettre de disposer d’une capacité de gestion de crises de cybersécurité majeures.

— Définir les moyens nécessaires à la gestion de crise : plans, procédure, ressources, etc.

— Vérifier que tous les éléments de préparation des crises sont présents. — Assurer la formation et l’entraînement des acteurs métiers ou support susceptibles d’intervenir en cas de crise de cybersécurité ; tester et valider la capacité de l’organisation à réagir à une attaque.

Réaction :

— Organiser la gestion de crise pour agir et traiter la crise de cybersécurité. — Animer la cellule de crise décisionnelle et contribuer aux cellules de crise opérationnelles.

— Coordonner l’action des différentes parties en présence et la diffusion des informations vers les parties prenantes.

— Suivre et coordonner les plans d’actions en matière d’investigation et de remédiation.

— Assurer les relations avec les autorités, les assurances et des experts ex ternes éventuels.

— S’assurer de la cohérence de la stratégie de communication de crise vis à-vis des parties prenantes.

— Organiser les revues post-mortem et la prise en compte des retours d’ex périence.

Au sein des organisations qui ne disposent pas d’une structure de réponse à incidents spécifique, ce métier n’est pas toujours dédié ; ses missions peuvent être assurées par le RSSI ou par d’autres acteurs de l’organisation de gestion de crise.

*CHAPITRE 2. SOC / CSIRT / CERT* 18 2.3 Leurs interactions

2.3.1 Couverture Fonctionnelle

Nous trouvons très classiquement ce schéma pour clarifier les périmètres d’acti vité des SOC, CERT et CSIRT 12.

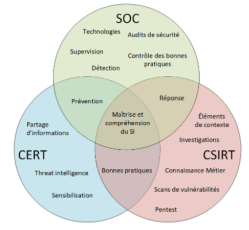


Figure 2.3 – Interactions SOC-CERT-CSIRT

Ce modèle a du sens car il permet de différencier ; les CSIRT qui ont un rôle de cyber pompier en lien avec l’activité, et en cas d’incident avec ils peuvents tenir informé les organes ad hoc : cellule de crise ou relation public ; des CERT qui ont un rôle d’intérêt public sur la recherche et la communication des vulnérabilités.

Le SOC à compte à lui un rôle de cyber vigile qui surveille et défend le SI au quotidien. Cette séparation entre les CSIRT et CERT est dur à suivre dans la pratique car l’emploi du termes CERT est largement utilisé, par exemple, au 26 septembre 2021 ; 75% 13 des CSIRT de l’interCERT utilisaient le sigle CERT ; 49% 14 des CSIRT référencés par l’ENISA utilisaient le sigle CERT.

Dans les faits, le périmètre des CSIRT (CERT) est variable, c’est pourquoi la déclaration de mission est une étape nécessaire et extrêmement importante au moment du démarrage. Elle permet de faire connaître clairement l’existence et le rôle du nouveau CSIRT. Il est recommandé de rédiger une déclaration de mission condensée, mais pas trop étroite, dans la mesure où elle ne subira probablement pas de modification avant plusieurs années. La RFC-2530 donne un modèle qui est lar

12. article “Zero Trust : anti-SOC, tu perds ton sang froid ?” [MISC n° 110 – juillet 2020] par : Jean-Thierry Stephen Avocanh, Étienne Ladent et Thomas Burnouf

13. https://www.cert.ssi.gouv.fr/csirt/intercert-fr/

14. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/ certs-by-country-interactive-map

*CHAPITRE 2. SOC / CSIRT / CERT* 19

gement utilisé. (ANS 15, ANSSI 16, AXA 17, Crédit Agricole 18, Deloitte 19, Enedis 20, ...)

2.3.2 Organisation des CSIRT / CERT

Pour être plus réactifs, les CSIRT ont besoin d’échanger entre eux afin de se tenir informés sur l’évolution de la menace et de mettre en commun leurs constatations pour être plus réactifs. C’est pourquoi il existe des espaces d’échanges entre eux. En France l’ANSSI a organisé l’interCERT. Au niveau international il existe le FIRST (Forum of Incident Response and Security Teams). En octobre 1989, un incident majeur provoqué là encore par un vers (WANK) révéla la nécessité d’un meilleur dialogue entre les diverses CSIRT. En réaction le FIRST fut créé en 1990.

Les buts du FIRST sont les suivants 21 :

— Favoriser la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d’incident de sécurité informatique. — Fournir un moyen de communication commun pour la diffusion de bulletins et d’alertes sur des failles potentielles et les incidents en cours. — Aider au développement des activités de ses membres, en particulier, la re cherche et les activités opérationnelles.

— Faciliter le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques.

Comme il existe l’InterCERT au niveau national ou le First au niveau internatio nal, il existe le TF-CSIRT 22 (Task Force on Computer Security Incident Response Teams) au niveau européen. Ces différents espaces de collaboration sont également des gages de sérieux des CSIRT car l’adhésion est soumise à validation et n’est pas définitive. Par le passé, obtenir l’autorisation d’utiliser le sigle CERT était égale ment une preuve de reconnaissance de la part du CMU.

L’interCERT comme le FIRST utilisent le protocole TLP 23 (Traffic Light Pro tocol). Le respect de ce protocole de classification de document fait partie de la charte de l’interCERT 24. Les documents sont classifiés selon quatre catégories et l’on retrouve ce tag dans l’entête ou le pied de page du document.

TLP : RED = Ne pas divulguer, information restreinte uniquement aux réci piendaires.

TLP : AMBER = Divulgation limitée, information limitée aux organisations et aux parties prenantes des participants sur la base du besoin d’en connaître.

15. https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/CERT\_ Sante\_RFC2350.pdf

16. https://www.cert.ssi.gouv.fr/uploads/CERT-FR\_RFC2350\_EN.pdf 17. https://cert.axa/sources/AXA-CERT-RFC2350.pdf

18. http://cert-ag.com/RFC\_2350\_CERT-AG\_v1.3\_20210825.pdf

19. https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/ csirt-deloitte-france-rfc2350.pdf

20. https://www.enedis.fr/media/1740/download

21. https://www.cert.ssi.gouv.fr/csirt/first/

22. https://www.first.org/resources/papers/conference2004/c12.pdf 23. https://www.first.org/tlp/

24. https://www.cert.ssi.gouv.fr/uploads/Charte-InterCERT-FR-v2.8a.pdf

*CHAPITRE 2. SOC / CSIRT / CERT* 20

TLP : GREEN = Divulgation limitée, information restreinte à la communauté.

TLP : WHITE = La divulgation de l’information n’est pas limitée. Conformément à la RFC-2350, pour assurer leur capacité de confidentialité et d’authentification dans le cadre de leurs échanges, les CSIRT communiquent large ment sur leurs clés PGP (Pretty Good Privacy) 25.

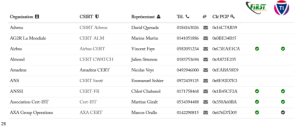


Figure 2.4 – Clés PGP des CSIRT

26

Les CSIRT se multiplient pour répondre à la croissance des cyberattaques. Si nous prenons comme indicateur le nombre de membres du FIRST.

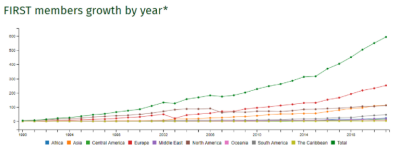


Figure 2.5 – Croissance des membres par année

27

On constate sur ce diagramme un doublement de la croissance du nombre de membres à partir de 2015.Au 26 septembre 2021 ; InterCERT compte 53 CSIRT (ayant souhaités faire apparaître leurs appartenances), dont 14 28 faisant partie du FIRST ; l’ENISA référence 582 CSIRT en Europe dont 41 29 français.

25. https://www.ietf.org/rfc/rfc2350.txt

28. https://www.cert.ssi.gouv.fr/csirt/intercert-fr/

29. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/ certs-by-country-interactive-map

*CHAPITRE 2. SOC / CSIRT / CERT* 21 2.4 Comment choisir ?

2.4.1 Les modèles de déploiement d’un SOC

Il existe plusieurs façons pour une entreprise d’acquérir des capacités SOC. Les modèles de déploiement les plus courants sont les suivants :

— SOC Interne :

La création d’un SOC interne dédié est recommandée pour les entreprises de cybersécurité matures. En effet, celles qui ont tendance à développer des SOC internes ont le budget pour assumer un investissement qui nécessite des efforts 24h/24, 7j/7 et qui s’appuie sur de nombreux relais à l’intérieur et à l’exté rieur de l’infrastructure.

L’un des avantages essentiels de la création d’un SOC interne est une visibilité et une réactivité maximales au niveau de l’ensemble du réseau. Une équipe in terne dédiée aura la capacité de surveiller l’environnement et ses applications, fournissant ainsi une image complète au niveau du paysage des menaces.

Certains inconvénients sont une difficulté pour recruter et retenir les talents et des niveaux d’investissement initiaux élevés. Ce modèle prend généralement un temps considérable à mettre en place et à maintenir pour bénéficier d’un niveau de fonctionnement adapté et pleinement opérationnel.

— SOC, MSSP, et MDR managés :

La sélection d’un SOC géré est recommandée pour les entreprises qui re cherchent l’assistance d’une entreprise externe pour effectuer des opérations de surveillance et de détection de haut niveau.

Certaines d’entre elles peuvent être matures d’un point de vue IT et cyber sécurité. Cependant, les contraintes budgétaires et l’expertise limitée peuvent entraver la capacité de créer un SOC interne 24×7 pleinement fonctionnel. À l’inverse, certaines autres peuvent se trouver à des stades immatures au niveau de la protection de l’entreprise et ont besoin d’une meilleure expertise pour gérer rapidement les efforts de surveillance, de détection et de réponse (MDR : Monitoring, Detection, and Response).

Les avantages de ce modèle sont : une plus grande rapidité, simplicité, scala bilité ainsi qu’une mise en œuvre plus économique. Etant donné la grande va riété de clients et d’industries que les MSSP prennent généralement en charge, l’expertise et la richesse des renseignements supplémentaires peuvent être vé ritablement d’une valeur inestimable.

La différence majeure entre un SOC traditionnel et un SOC intégrant des services MDR est que ces derniers non seulement détectent et analysent les menaces, mais y répondront également. Lorsqu’une menace est détectée, ils vérifieront la criticité tout en y répondant et en informant l’entreprise par la suite de l’incident.

— Hybride : un petit SOC interne et managé :

Un modèle hybride donne accès au meilleur des deux mondes : du personnel interne complété par des experts externes, offrant ainsi une approche sécurisée en matière de détection et de réponse. La plupart des entreprises à ce niveau sont suffisamment grandes pour constituer leur propre petite équipe.

Cependant, elles ne peuvent pas créer un SOC interne 24×7 pleinement fonc tionnel. Cette solution est efficace en raison de la rapidité de la détection et

*CHAPITRE 2. SOC / CSIRT / CERT* 22

du temps de réponse. De plus, le backlog est moins important en raison des analystes supplémentaires (internes et externes) qui travaillent sur les résul tats hautement prioritaires.

En outre, ce modèle offre la meilleure combinaison en termes d’apprentis sage aussi bien pour l’entreprise que pour l’équipe de cybersécurité. Il peut également permettre le transfert de connaissances détenues jusque-là par les experts d’un MSSP.

Les inconvénients importants sont principalement le fait que certaines données seront traitées par un tiers et que ce modèle peut être coûteux à maintenir sur le long terme.

— SOC, MSSP, et MDR managés 30 :

La stratégie Follow the sun consiste en l’application de processus sur différents fuseaux horaires lorsqu’une entreprise possède ses sièges dans plusieurs pays. Une équipe qui commence à traiter une tâche peut alors la relayer à l’équipe suivante une fois son service fermé. La seconde équipe ayant un fuseau ho raire décalé pourra continuer le traitement jusqu’à la fermeture de son propre service et établir un suivi pour une bonne gestion avec l’ensemble des inter venants.

Le processus Follow the sun a plusieurs avantages dont :

— Le traitement rapide et efficace des tâches.

— l’exploitation du potentiel collaboratif.

— La capitalisation et l’exploitation des connaissances.

Ces avantages sont primordiaux pour la compétitivité d’une entreprise, puis qu’ils rendent les équipes bien plus productives et rentabilisent les coûts. Ils permettent d’offrir un bien meilleur service et la satisfaction client en est également améliorée.

2.4.2 Les défis d’un Security Operation Center (SOC)

Le SOC a un rôle de plus en plus complexe, gérant tous les aspects de la sécurité numérique de l’entreprise. Pour de nombreuses organisations, créer et maintenir un SOC pleinement opérationnel peut être difficile.

Les défis classiques sont :

— Le volume

Le défi le plus courant auquel sont confrontées les entreprises est le volume d’alertes de sécurité, dont beaucoup nécessitent à la fois des systèmes avancés et des ressources humaines pour catégoriser, prioriser et répondre correctement aux menaces. Avec un grand nombre d’alertes, certaines menaces peuvent être mal classées ou passées complètement inaperçues. Ce risque souligne le besoin d’outils de surveillance avancés et de capacités d’automatisation ainsi que la nécessité de disposer d’une équipe de professionnels qualifiés en matière de cybersécurité.

— La complexité

La nature de l’entreprise, la flexibilité du lieu de travail, une utilisation accrue 30. https://www.easyvista.com/fr/blog/follow-the-sun-mettre-en-place-des-processus-digitaux-int

*CHAPITRE 2. SOC / CSIRT / CERT* 23

de la technologie Cloud et d’autres problèmes ont augmenté la complexité de la défense d’une entreprise et de la réponse aux menaces. Aujourd’hui, des solutions relativement simples, comme les pare-feu, sont insuffisantes en tant que mesure isolée pour protéger l’entreprise contre ses adversaires numériques. Une sécurité plus efficace nécessite une solution qui combine la technologie, l’humain et les processus, ce qui peut être difficile à organiser, à mettre en place et à faire fonctionner.

2.4.3 Le coût

Bâtir un SOC nécessite beaucoup de temps et de ressources. Sa maintenance peut s’avérer être encore plus exigeante, car le paysage des menaces change constam ment et nécessite des mises à jour et des mises à niveau fréquentes ainsi qu’une for mation continue du personnel de cybersécurité. De plus, peu d’entreprises disposent des talents en interne nécessaires pour comprendre suffisamment le paysage actuel des menaces. De nombreuses entreprises collaborent avec des fournisseurs de ser vices de sécurité tiers (tels que les MSSP : Managed Security Service Provider) pour garantir des résultats fiables sans investissements internes importants en matière de technologie ou de main-d’œuvre.

Un SOC externe coûte nettement moins cher car le matériel, les solutions et les experts sont pour la plupart mutualisés. Pour une surveillance et analyse 24/7 via un SOC externalisé, il faut compter un budget entre 300k€ à 700k€ alors qu’une internalisation du SOC coûte entre 1M€ et 2M€, ce qui inclut le développement et le maintien de la plateforme mais pas les coûts technologiques. Ajoutons qu’il s’agit là d’une dépense d’exploitation (OPEX) et non d’infrastructure, une dépense donc plus facile à intégrer dans le budget.

La pénurie de compétences

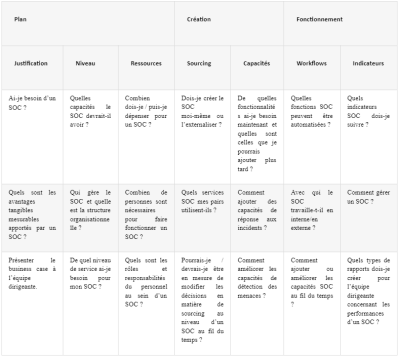
La création d’une solution de sécurité interne est à l’heure actuelle encore plus compliquée étant donné la disponibilité limitée des professionnels qualifiés en cy bersécurité. Ces derniers sont très demandés dans le monde entier, rendant ainsi difficile le recrutement et la rétention des talents. Cette situation signifie que le turnover au sein d’une organisation de cybersécurité peut potentiellement affecter les opérations de sécurité.

Une obligation règlementaire

Pour les OIV (opérateurs d’importance vitale), il est obligatoire qu’une partie de leur système d’information réponde aux exigences de sécurité de la LPM 31 ( Loi de Programmation Militaire). Ainsi, les OIV ont notamment l’obligation de disposer d’un SOC.

31. https://www.ssi.gouv.fr/

*CHAPITRE 2. SOC / CSIRT / CERT* 24 2.4.4 Les questions à se poser lors de la création d’un SOC

Figure 2.6 – Liste des questions à se poser

*CHAPITRE 2. SOC / CSIRT / CERT* 25

2.4.5 Les modèles organisationnels d’un CSIRT

L’ENISA propose les 4 modèles 32 suivants de CSIRT dans son guide de création d’un CSIRT publier en 2006 :

— Le modèle organisationnel indépendant :

Le CSIRT est conçu et agit comme une organisation indépendante, dotée de sa propre direction et de son propre personnel.

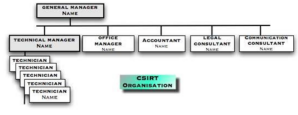


Figure 2.7 – Organisation d’un CSIRT sur un modèle indépendant

— Le modèle organisationnel intégré :

Ce modèle peut être appliqué lorsque un CSIRT est créé au sein d’une organi sation existante en faisant appel à un département informatique déjà en place, par exemple. Le CSIRT est dirigé par un chef d’équipe qui, responsable des activités confiées au CSIRT, réunit les techniciens nécessaires pour résoudre des incidents ou pour mener à bien les tâches qui lui sont assignées, et peut demander une aide spécialisée au sein de l’organisation existante.

Ce modèle convient également lorsque des situations particulières se pré sentent. On attribue alors à l’équipe un nombre déterminé d’ETP (équiva lents temps plein). Le service des abus chez un fournisseur d’accès Internet, par exemple, requiert au minimum un équivalent temps plein, voire (le plus souvent) plusieurs.

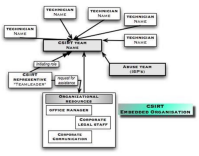


Figure 2.8 – Organisation d’un CSIRT sur un modèle intégré

32. https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-french/ at\_download/fullReport

*CHAPITRE 2. SOC / CSIRT / CERT* 26

— Le modèle «campus» :

Comme son nom le laisse entendre, le modèle «campus» est principalement adopté par des CSIRT du monde universitaire et de la recherche. La plupart des organisations de ce domaine comprennent plusieurs universités et campus disséminés sur un territoire régional, voire sur l’ensemble du territoire natio nal (tel est notamment le cas des réseaux nationaux de recherche ou RNR). Ces organisations fonctionnent le plus souvent indépendamment les unes des autres, et gèrent chacune leur propre CSIRT. Ces équipes sont néanmoins cha peautées par un CSIRT «mère» ou «de base», qui en assure la coordination et constitue le point de contact unique pour le monde extérieur. Il assure en outre, dans la plupart des cas, les services CSIRT essentiels, et la transmis sion des informations relatives aux incidents aux CSIRT «campus» concernés. Certains CSIRT communiquent eux-mêmes leurs services de base aux autres CSIRT «campus», ce qui réduit les frais généraux pour le CSIRT central.

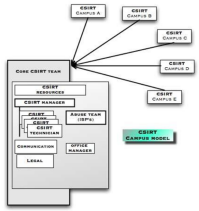


Figure 2.9 – Organisation d’un CSIRT en modèle CAMPUS

— Le modèle volontaire :

Ce modèle organisationnel désigne le regroupement de personnes (spécialistes) en vue d’un échange mutuel – et de la communication vers l’extérieur – de conseils et d’assistance à titre volontaire. Il s’agit d’une communauté peu structurée et largement dépendante de la motivation des participants.

2.5 Résumé et perspective d’évolution

2.5.1 Les avantages d’un Security Operation Center (SOC)

Le principal avantage d’un SOC est l’amélioration de la détection des incidents de sécurité grâce à une surveillance et une analyse continues de l’activité du réseau tout en s’appuyant sur des données de cyber-intelligence. En analysant les activités sur les réseaux de l’entreprise en permanence, les équipes du Security Operations

*CHAPITRE 2. SOC / CSIRT / CERT* 27

Center peuvent détecter et réagir rapidement face aux incidents de sécurité. Cette possibilité est cruciale, car le temps est l’un des éléments les plus critiques lorsqu’il est question de répondre efficacement aux incidents de cybersécurité.

La surveillance du SOC 24/7 donne aux entreprises un avantage significatif dans ce combat pour se protéger contre les incidents et les intrusions, quels que soient la source, l’heure ou le type d’attaque. L’écart entre le moment de la compromission effective et celui de la détection diminue, aidant ainsi les entreprises à rester bien en phase avec les menaces auxquelles leur environnement est confronté et à limiter les risques.

Les principaux avantages d’un SOC sont :

— La surveillance et l’analyse ininterrompues des activités suspectes. — L’amélioration des temps de réponse aux incidents et des pratiques de gestion des incidents.

— La diminution de l’écart entre le moment de la compromission et celui de la détection.

— Des actifs logiciels et matériels centralisés pour permettre la mise en œuvre d’une approche plus holistique de la sécurité.

— Une communication et une collaboration efficaces pour détecter et classer les tactiques et techniques adverses, par exemple en utilisant le framework MITRE ATT&CK.

— La réduction des coûts associés aux incidents de sécurité.

— Plus de transparence et de contrôle sur les opérations de sécurité. — Une traçabilité fiable concernant les données utilisées dans les activités de cybersécurité post-mortem.

2.5.2 Les avantages d’un CSIRT

Depuis plusieurs années déjà la question n’est plus : vais-je subir une cybe rattaque, mais quand ? Il convient de se préparer au sinistre, cela est même une obligation pour certaines organisations. Avoir accès avec un CSIRT ne se résume pas à avoir des cyberpompiers qui interviennent en cas d’indisponibilité du sys tème d’information provoqué par une cyberattaque. Un CSIRT informe les équipes opérationnelles des nouvelles vulnérabilités qui pourraient les concerner et leur com munique des actions à réaliser pour les résorber ou au moins les réduire. Un CSIRT doit également colliger les incidents de sécurité afin d’avoir une vision globale sur les tendances des attaques.

L’autre aspect fondamental d’un CSIRT c’est l’aspect réseau d’échange. La me nace étant globale, les CSIRT doivent échanger entre eux afin de pouvoir capitaliser sur les incidents subis par les autres afin de permettre de capitaliser plus large ment. Ces échanges permettent également de partager les solutions pour réduire les vulnérabilités.

Les processus internes dans les organisations reposant de plus en plus sur le système d’information, un CSIRT peut également être un conseiller de poids auprès

*CHAPITRE 2. SOC / CSIRT / CERT* 28

du service qualité afin d’essayer d’élaborer les meilleures solutions pour assurer la continuité d’activité du core business de l’entreprise.

Construire une relation avec un CSIRT c’est donner les moyens d’être mieux informé, mieux préparer et mieux réagir lors d’un incident informatique lié à une cyberattaque.

2.5.3 Évolution

La transformation numérique massive des entreprises a contribué à une accélé ration de l’expansion du cyberespace qui résulte à une augmentation en parallèle de la surface d’exposition aux menaces et attaques informatiques.

La lutte informatique défensive (LID) a mis en lumière une nécessité fondamen tale de mettre en place des moyens technologiques et humains afin de prévenir, réagir, réduire et anticiper les différentes menaces.

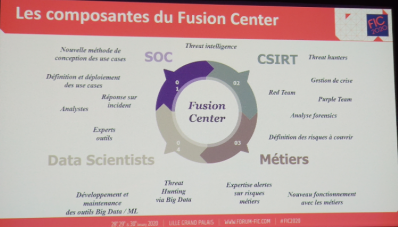
En réponse, les CERT, CSIRT et SOC apparaissent pour faire face aux cybe rattaques, et comme le cyberespace regorge d’attaquants de plus en plus innovant, de groupes organisés et d’associations qui ne connaissent pas de frontière physique, il devient impensable que les outils, les mesures organisationnelles et les partages de ressources liés aux actions de la LID ne puissent pas évoluer eux aussi vers une réponse à incident cybersécurité rapide et efficace.

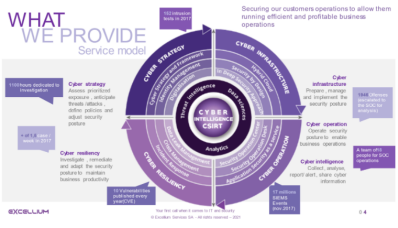
De ce fait, une communication et une collaboration accrue entre les acteurs n’est plus une option. On peut constater qu’après certains déboires d’ordre financier (perte conséquente d’actifs et d’argent), les grandes entreprises s’orientent naturel lement vers une implémentation de plus en plus complexe et complète de solutions interopérables en matière de LID.

Les offres du marché évoluent dans ce sens, par exemple Orange Cyberdéfense propose un interfaçage entre son offre CERT Orange Cyberdefense et les équipes de son offre CyberSOC. Varonis dans son offre de CSIRT intègre la surveillance d’actif alors qu’il s’agit d’une mission dévolu au SOC. On peut également trouver des SOC dans des réseaux de CSIRT par exemple dans le regroupement européen TF-CSIRT on peut trouver SOC-GSE pour l’Italie ou SOC-FDJ pour la France.

Une tendance confirmée lors d’une conférence d’expert cybersécurité au Forum International de la cybersécurité de 2020 33. Au moment même où le besoin d’implé menter un SOC atteint son apogée, on annonce la fin du SOC tel qu’on le connaît. Ce modèle de SOC tendra à disparaître pour évoluer vers un FUSION CENTER afin d’effacer le cloisonnement entre les services et flux d’information des SOC et CSIRT/CERT.

33. https://www.forum-fic.com/

*CHAPITRE 2. SOC / CSIRT / CERT* 29 Figure 2.10 – Composition d’un Fusion Center

Figure 2.11 – Schéma explicatif de la Cyber Intelligence

Chapitre 3

SOC, procédures et outils

3.1 Sources

3.2 La détection des menaces

3.2.1 Les ressources utilisées par les outils du SOC : les logs

De nos jours, la majorité des entreprises et organismes utilisent des systèmes informatisés. Ces systèmes induisent des échanges d’informations ainsi que des com munications entre différentes composantes informatiques, qui peuvent être soit in ternes à l’entreprise soit en dehors des infrastructures de l’entreprise. Dans le cadre de la sécurisation d’un système d’information, il faut pouvoir étudier ces échanges et ces communications. Pour cela nous utilisons des logs. Ce sont des journaux d’évé nements qui relatent toutes les informations concernant l’usage d’une application ou l’échange entre deux équipements.

La plupart des équipements informatiques, tels que les pare-feux, les routeurs, les sondes réseaux ou les antivirus, engendrent des logs 1. Ces derniers proviennent aussi des systèmes d’exploitations de nos machines ainsi que des diverses applica tions présentes sur ces dernières. De ce fait, lorsqu’une entreprise développe une application en interne, elle se doit de prévoir un système de log afin de pouvoir garder en mémoire et retracer les usages de cette dernière.

Comme dit plus haut, on retrouve différents types d’équipements au sein d’un système d’information. Cette diversité entraîne aussi l’existence de plusieurs types de log, tel que :

— Logs applicatifs :

Les types d’informations et le format des messages trouvés dans un journal de log 2 varient selon l’application. En effet, ces variables ne sont pas déterminées par des directives externes ou par le système d’exploitation. Au contraire, les développeurs de l’application logicielle contrôlent ce qui entre dans le fichier journal. Ce sont eux qui décident des événements et des informations qu’il serait utile de consigner et de la manière dont cela doit être fait. De nombreux

1. https://www.ionos.fr/digitalguide/web-marketing/analyse-web/ les-fichiers-log-lenregistrement-des-processus-informatiques/ 2. https://www.xplg.com/application-logs-what-how/

30

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 31

événements seront spécifiques à l’application source. Cependant, il est courant que les événements enregistrés contiennent certaines informations pour les rendre plus utiles.

— Logs systèmes :

Les logs systèmes 3(ou syslog) correspondent aux informations sur le logiciel, le matériel, les processus systèmes et les composants du système. Ils indiquent également si les processus ont été chargés avec succès ou non. Les informations peuvent ensuite être utilisées pour diagnostiquer les sources de problèmes in formatiques, tandis que les avertissements peuvent être utilisés pour prédire les problèmes et problèmes potentiels du système.

Le syslog a des composants standards qui peuvent varier en fonction du sys tème d’exploitation. Cependant, certains composants et informations com muns sont capturés quel que soit le système d’exploitation.

Toutes les entrées sont classées par type, comme par exemple : erreur, infor mation, avertissement, audit de réussite ou audit d’échec pour les systèmes Windows, et urgence, alerte, critique, erreur, avertissement, avis, information ou débogage pour les systèmes Mac OS et Linux.

Toute entrée syslog contient des informations d’en-têtes ainsi qu’une descrip tion des événements. Cette dernière comprend la date et l’heure des événe ments, le nom d’utilisateur connecté et le nom de l’ordinateur au moment de l’événement. Il contient également le numéro d’identification de l’événe ment utilisé pour identifier l’événement et la source de ce dernier , comme par exemple le nom du composant système.

— Logs de base de données :

Aussi appelé journal des transactions 4, il s’agit d’un historique des actions exécutées par un système de gestion de base de données. Il est utilisé pour ga rantir les propriétés ACID (Atomicity, Consistency, Isolation, Durability) en cas de panne matérielle. Physiquement, un journal est un fichier répertoriant les modifications apportées à la base de données, stocké dans un format de stockage stable.

Les propriétés ACID 5 permettent d’assurer que les transactions de bases de données soient traitées de façon fiable. Le terme de transaction fait référence à n’importe quelle opération effectuée au sein d’une base de données. Il peut s’agir par exemple de la création d’un nouvel enregistrement ou d’une mise à jour des données.

La propriété Atomicity vérifie que toutes les modifications ont été effectuées jusqu’au bout. Si durant une modification une erreur ou une interruption se produit, le principe atomicity veut que la base de données annule ladite mo dification.

La propriété Consistency vise à vérifier la cohérence d’une transaction. En d’autres termes, cette propriété s’assure que la transaction ne va pas à l’en contre des contraintes d’intégrité des données.

La propriété Isolation vérifie qu’une transaction est “sérialisable”. Cela signi fie que les transactions surviennent dans un ordre successif, plutôt que d’être

3. https://www.techopedia.com/definition/1858/system-log-syslog 4. https://www.ibm.com/docs/fr/planning-analytics/2.0.0?topic= logs-transactions-log

5. https://datascientest.com/acid

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 32

effectuées en une fois. Toute écriture ou lecture effectuée dans la base de don nées n’impacte pas l’écriture ou la lecture d’autres transactions survenant sur la même database. Un ordre global est créé, et chaque transaction s’ajoute à une file d’attente. Ce n’est que lorsqu’une transaction est totalement complète que les autres débutent.

Cela ne veut pas dire que deux opérations ne peuvent survenir simultanément. Plusieurs transactions peuvent être effectuées en même temps, à condition qu’elles ne puissent pas interférer entre elles.

La propriété Durability permet d’assurer que les changements apportés à la base de données soient permanents, même en cas de panne du système. Ceci a pour but d’éviter que les données soient corrompues ou altérées par une panne de service, un crash ou tout autre problème technique. Pour per mettre cette durabilité, on utilise des ”changelogs” pris pour références chaque fois que la base de données est démarrée.. un changelogs et un versionnage de la base de données. En d’autres termes on utilise un backup de la base de données au démarrage afin de s’assurer de la fiabilité des données et de leurs persistances.

Les logs comprennent les informations concernant les éléments suivants : — Date et heure de la modification

— Nom du client qui a procédé à la modification

— Si les nouvelles données sont des données simples ou des données de chaînes — Valeur avant la modification

— Valeur après la modification

— Nom la table dans laquelle la modification a été apportée

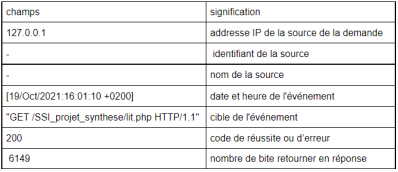
— Éléments qui identifient la cellule qui a été modifiée

Exemple de log : (log http)

Voici un log provenant du fichier acces.log d’un serveur Web :

"127.0.0.1 - - [19/Oct/2021 :16 :01 :10 +0200] "GET /SSI\_projet\_synthese/lit.php HTTP/1.1" 200 6149"

Comme on peut le voir, un log contient beaucoup d’informations , ce qui le rend difficile à lire au premier abord. toutefois en découpant ce log champ par champ on obtient le tableau suivant , qui permet une lecture plus simple de ce dernier.

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 33 Figure 3.1 – Différents champs d’un Log

Le champ IP permet de retrouver la source de l’événement.Le nom de la source permet de savoir le nom de la machine qui déclenche l’événement , ce champ n’est pas obligatoire. On récupère les informations temporelles sur l’évènement, c’est- à dire la date et l’heure système.La cible de l’événement permet de récupérer à la fois la ressource visée , mais aussi la méthode utilisée pour l ’atteindre, ici la méthode utilisée est ‘’Get” . Le code d’erreur permet de savoir si l’action s’est déroulée sans encombre. ici il s’agit d’une requête HTTP, le code de réussite est “200”. Les codes d’erreurs les plus connus sont : 401 en cas d’utilisation non authentifié, 403 en cas d’accès refusé , 404 en cas de ressource non trouvée . Enfin le dernier champ concerne la quantité de données retournée à la source de l’événement.

Les logs sont les sources de données principalement utilisées par le SOC durant leurs investigations.Pour pouvoir utiliser ces données ,le SOC dispose d’outils per mettant la centralisation des logs ainsi que leurs analyses, notamment le LMS , le SIM ,Le SEM et le SIEM.

3.2.2 LMS

Un LMS 6, ou Log Management System, est une solution pour collecter et ana lyser les logs. Le terme équivalent de LMS en français est ‘’outil de gestion des logs”. Un LMS est un système permettant le stockage et la centralisation des logs. L’utilisation d’un LMS aporte des avantages et des fonctionnalité tels que :

— Collecte des données :

Cette fonction permet de recueillir toutes les données de consignation dispo nibles à l’aide de méthodes basées ou non sur la source fournissant les log , voire d’une combinaison des deux.

— Conservation rationnelle :

Même si la collecte et la sauvegarde de logs ne constituent pas un défi tech nique majeur, il n’est pas simple de recueillir efficacement plusieurs gigaoctets, voire téraoctets, de ce type de données. De plus, il faut pouvoir les conserver

6. https://www.netiq.com/fr-fr/docrep/documents/m47h82fbmy/the\_complete\_guide\_ to\_log\_and\_event\_management\_wp\_fr.pdf

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 34

tout en fournissant des fonctions de recherche et d’accès rapides. Cette fonc tion est essentielle aux systèmes de gestion des logs étant donné le nombre de réglementations incluant des conditions spécifiques exigeant la conservation des logs, très souvent pendant plusieurs années.

— La recherche

Cette fonction est le principal moyen d’accéder aux informations contenues dans l’ensemble des logs, y compris ceux issus des applications créées par l’entreprise . En outre, elle est indispensable pour utiliser les logs à des fins d’enquête, mener des analyses d’expertise et identifier les défaillances tout en dépannant les applications à l’aide des logs.

— L’indexation et l’analyse des logs

Tout système de gestion des logs repose essentiellement sur ces deux fonctions. L’indexation permet des recherches cent fois plus rapides. La technologie d’in dexation crée une structure de données appelée un index. Ce dernier permet d’effectuer des recherches très rapides à l’aide de mots-clés ou d’opérateurs logiques sur l’ensemble du système de stockage des logs. Parfois, l’indexa tion permet d’activer d’autres techniques d’analyse sémantique et l’applica tion d’étiquette sur le contenu d’un log. Cependant, tous les outils de gestion des logs ne prennent pas en charge l’indexation et n’indiquent pas les taux de collecte des logs lorsqu’ils ne sont pas pris en compte pour l’indexation.

— La création de rapports standard et planifiée

Ces fonctions concernent toutes les données recueillies par le produit de gestion des logs. Elles sont similaires aux fonctions de création de rapports comprises dans les outils SIEM. La fiabilité des rapports, qu’ils soient créés pour des raisons de sécurité, de conformité ou de fonctionnement, peut confirmer ou détruire la réputation de la solution de gestion des logs concernée. Les rapports doivent être créés rapidement, personnalisables et faciles à utiliser à diverses fins. La distinction entre les recherches et les rapports est parfaitement claire. Le processus de recherche concerne tous les logs collectés disponibles dans leur format brut d’origine,.En revanche, les rapports se fondent sur les logs analysés au sein d’une base de données.

Comme on peut le voir un LMS 7 offre un large panel de fonctionnalités, cepen dant un LMS a un champ d’action limité. En effet, il ne permet qu’une analyse primaire des données des logs , via l’analyse sémantique. De plus, les rapport en gendrés par le LMS sont là pour servir d’historique. enfin un LMS peut déclencher des alertes en cas de lo suspect , toutefois il n’existe qu’un seul niveau d’alerte pour tous les types ce manque de précision empêche d’avoir un feedback concret concernant la gravité et la teneur de l’alerte déclencher. Pour combler ces manques il existe d’autres outils tels que SIEM pour pallier ses faiblesses.

7. https://www.sumologic.com/glossary/siem-log/

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 35

3.2.3 SIM SEM SIEM

Définition

SIM, SEM, SIEM 8, autant d’acronymes qui peuvent sembler confus aux non ini tiés au processus de cyber sécurité tant leurs processus et leurs sens sont similaires. Cependant il existe bel et bien des différences notables entre ces trois procédés. Au cœur du problème se trouve la similitude entre la gestion des événements de sécurité ou SEM, et la gestion des informations de sécurité ou SIM.

Ces deux acronymes désignent des processus de collecte d’information de log (plus particulièrement de log concernant des alertes de sécurité ou de données simi laires) dans un but de stockage à longue durée ou pour analyser l’environnement de sécurité d’un réseau. Leur principale différence se situe dans le traitement des logs récupérés.

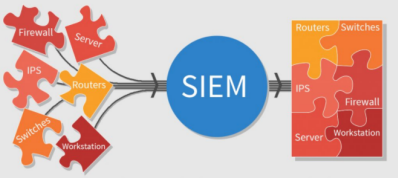
Le rôle du SIM (Security Information Management) est essentiellement de collec ter et stocker des informations tirées des logs(que ce soit à court ou à long terme). Grâce au SIM on passe d’informations sous formes de centaines de lignes de log illisible pour un être humain à des informations regroupées selon des logiques qui permettent de grandement faciliter le travail d’analyse des équipes du SOC.

On peut voir le SIM comme un processus plus à long terme, plus général et sur un domaine plus large que le SEM si l’on veut avoir une vision plus compartimentée.

Le SEM (Security Event Management) quant à lui examine et permet de faire le tri de façon plus pointu des types d’événements spécifiques. On peut par exemple, faire une recherche spécifique sur les évènements ne concernant uniquement les super-utilisateurs d’un SSI. Cela regroupe également les technologies recherchant spécifiquement des authentifications suspectes, des ouvertures de session de compte ou un accès de gestion de haut niveau à des heures spécifiques. Ces événements utilisateurs sont communément appelés des drapeaux rouge (ou red flag puisqu’ils constituent de potentiels problèmes de sécurité).

Enfin, le SIEM (Security Information Event Management) fait référence à des technologies regroupant le SIM et SEM. Ce terme plus générique est le plus cou ramment utilisé pour désigner les outils et ressources de sécurité d’un SOC. Bien, que ce terme puisse sembler un peu "fourre tout” il en est néanmoins pertinent étant donné que les deux aspects cités précédemment (gestion de l’information et des événements) sont utilisés plus ou moins équitablement par les équipes du SOC. Le SIEM est en général placé directement dans les locaux de l’entreprise, les équipes du SOC peuvent difficilement interagir directement avec le SIEM, ils ne peuvent interagir qu’avec les alertes envoyées par ce dernier.

8. https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 36 Figure 3.2 – Illustration du fait que le SIEM est une fusion de plusieurs technologie

Architecture d’un SIEM

Lors de la mise en place d’un SIEM, il est primordial d’adapter ses choix avec l’organisation de la structure de l’entreprise en cas de SOC interne, ou de la struc ture du SOC en cas de SOC externe. Voici quelques exemples de questions qu’une entreprise voulant implémenter un SOC pourrait se poser et comment y répondre ? 9

— Veut-on utiliser le SIEM pour gérer uniquement des incidents de sécurité ou veut-on qu’il soit utilisable par les équipes projet pour accéder aux logs ap plicatifs ou récupérer des métriques métier ?

Le SIEM étant une fusion de nombreuses technologies il est assez courant d’avoir des outils très modulaires et de pouvoir séparer les parties métier, exploitation et sécurité. Dans une entreprise possédant une autre solution de type puit de log (LMS par exemple) il peut être envisageable de se contenter uniquement d’outils de sécurité.

— Quel périmètre veut-on couvrir ?

Il est important de savoir le périmètre que le SOC va couvrir. Parle-t-on SOC interne ou externe ? En cas de SOC interne veut-on couvrir le SI entier d’une entreprise ? seulement un SIIV ? Un datacenter ? Un backbone ?

— Avec quels composants de notre infrastructure le SIEM doit-il s’interfacer ? Étant par nature très modulable, il est possible d’interfacer un SIEM avec tout un tas de plugins qui facilitent la réaction automatique à certains événements ou la lisibilité. De plus, il faut aussi prendre en compte le SI déjà existant dans l’entreprise. En effet, dans le cas d’un SOC interne il est souvent utile d’inter facer le SIEM avec certains outils tels que ceux de récupération d’information tierces sur des annuaires (LDAP ou Active directory par exemple).

— Souhaite-t-on pouvoir personnaliser en détail la solution ou préfère-t-on une solution clé en main ?

Il est important de comprendre qu’il existe des solutions SIEM pour tout type

9. https://docplayer.fr/170242765-Deploiement-d-un-siem-et-enrichissement-des-donnees. html

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 37

de besoin. Si une entreprise veut une solution clef en main qui vise à être utili sable immédiatement il existe des fournisseurs de SIEM déjà tout fait (Qradar d’IBM par exemple). Cela permet un déploiement rapide sans avoir besoin de personnel extrêmement qualifié dans le domaine mais avec un frais fixe assez élevé lors de l’achat et une plus grande difficulté à adapter le SIEM à ses besoins futurs sans repasser par le même fournisseur.

A l’inverse si l’on veut un outil plus personnalisé il existe des solutions com merciales utilisant les briques open source (logstash, elasticsearch) pour per sonnaliser de façon approfondi. Cette seconde méthode possède les qualités et les défauts inverses de la première. Ainsi il faudra compter un déploiement plus long avec des frais plus étendu dans le temps, mais une personnalisation plus grande, et une personnalisation future plus facile.

Centralisation des informations sur les menaces

La centralisation des informations des menaces est indispensable pour aider à les détecter et les contrer. Les CVE 10 (Common Vulnerabilities and Exposures) est une liste publique qui référence toutes les failles informatiques connues. Cette liste sert à aider les professionnels de la sécurité de l’information dans leur lutte contre les cyber-attaques en leur donnant la possibilité d’être mieux informés sur les failles déjà existantes afin qu’ils soient plus coordonnés. Ces CVE sont mainte nues par l’organisme MITRE, soutenu par le département de la Sécurité intérieure des Etats-Unis. On attribue à chaque CVE un identifiant unique dans le but de bien différencier chaque faille connue. Elles sont aussi classées par ordre de dange rosité grâce au CVSS (Common Vulnerability Scoring System) qui est un système d’évaluation standardisé des vulnérabilités informatiques.

Il y a 3 mesures à prendre en compte lors de la notation de la dangerosité d’une faille, et elles sont appelées des métriques :

— La métrique de base est unique et immuable, ce qui signifie qu’elle se base sur un critère qui ne bougera pas dans le temps qui correspond aux qualités intrinsèques de la vulnérabilité.

— La métrique temporelle qui elle aussi est unique et correspond à la capacité pour la faille de durer dans le temps. Ce critère évolue au cours du temps et n’est pas figée dans le marbre pour chaque vulnérabilité.

— La métrique environnementale est multiple cette fois, elle correspond à l’en vironnement touché par la vulnérabilité et comme cet environnement peut évoluer, ce n’est pas non plus une métrique fixée. Elle évoluera si la faille touche de nouveaux environnements ou alors si au contraire elle devient plus limitée en termes de systèmes informatiques dans lesquels elle représente une menace.

Plus la CVE aura une note élevée après avoir passé cette évaluation, plus elle sera considérée comme dangereuse. Et comme cette note peut bouger selon les critères cités au-dessus, il est possible qu’une vulnérabilité peu dangereuse aujourd’hui sera la source principale de nos soucis dans quelques temps.

10. https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 38 Figure 3.3 – Exemple de deux CVE avec leur CVE ID et leur score de dangerosité

Les règles de corrélation

Les règles de corrélation ou use cases 11 sont des règles qui servent à trier les logs arrivants au SIEM afin de ne garder que les logs qui représentent un intérêt à être analysés (cela correspond généralement aux potentiels incidents de sécurité). Ces règles sont soit fournies par divers outils SIEM (dans le SIEM d’IBM par exemple il y a une liste de 300 use cases intégré par défaut), soit prédéfinies pour différents scénarios d’attaque, soit créées et affinées par et/ou pour le client.

Une règle de corrélation définit une séquence spécifique d’événements qui pour raient être révélatrice d’une faille de sécurité. Par exemple, une règle pourrait être créée pour identifier quand plus de x demandes sont envoyées à partir de plages IP et de ports spécifiques dans un certain laps de temps.

Le volume de données enregistrées dans les environnements est énorme. Même les petites et moyennes organisations enverront très probablement des dizaines de Go de données par jour. En fait, les règles aident à condenser ces données en ensembles de données plus faciles à gérer en réduisant le bruit et en mettant en évidence les événements qui pourraient potentiellement avoir un sens.

La plupart des systèmes SIEM fournissent également des mécanismes intégrés pour la production de rapports. Ces rapports peuvent être utiles pour des raisons d’admi nistration, d’audit ou de conformité. Par exemple, un rapport quotidien détaillant les alertes ou les règles déclenchées pourrait être intégré dans un tableau de bord.

Les uses cases sont primordiaux dans l’utilisation d’un SIEM, cependant leur dé veloppement demande énormément de temps (il faut compter des mois de travail d’une équipe pour un seul use case) c’est pourquoi l’offre d’IBM proposant des uses cases dans leurs offres est très attractive.

Il est important de retenir que le nombre de use cases d’un SIEM ne correspond absolument pas à une pseudo “note” du SIEM et que le nombre de use cases n’est absolument pas un critère de bon fonctionnement d’un SIEM. Par exemple, selon le responsable du SOC d’Excellium, leur SIEM comporte une vingtaine de USE CASES qui englobe les 200 par défaut de Qradar d’IBM.

Les uses cases sont systématiquement affinées en fonction soit de l’entreprise dans le cas d’un SOC interne soit de l’entreprise cliente dans le cas d’un SOC externe. En effet, dans une entreprise il peut exister certaines habitudes ou certaines façons de faire qui peuvent rendre des use cases obsolètes ; c’est ce que nous allons voir plus en détails dans la prochaine partie.

11. https://securityintelligence.com/posts/quick-guide-to-siem-use-cases/

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 39

Analyse des données collectées

Dans un SOC, la tâche la plus coûteuse en temps est la distinction entre vrai positif (correspondant à de réels problèmes de sécurités) et faux positif (trafic légal et légitime de l’entreprise). Afin d’affiner et d’automatiser au maximum les alertes du SIEM il est primordial d’enrichir ses données. L’enrichissement des données 12 vise principalement à récupérer des données publiques mises à disposition par la communauté ou des données fournies par les entreprises clientes (ou l’entreprise mère en cas de SOC interne) afin d’augmenter le niveau de confiance des alertes.

On distingue deux grands types d’enrichissement de données différents : — L’enrichissement interne

— L’enrichissement externe

L’enrichissement de données internes concerne uniquement les données des clients du SOC. Elles sont la plupart du temps fournies par l’entreprise cliente afin de faciliter le travail de surveillance du SOC. Cela peut concerner les habi tudes de travail, les outils utilisés ou des enchaînements d’événements communs à l’entreprise. Ces données permettent d’adapter (et potentiellement automatiser) la réponse à apporter lors d’un incident. Lors d’un incident certaines informations tel que savoir si la source de l’événement est interne au GIP ou est ce que la machine mise en cause est une machine de l’entreprise ou le PC d’un employé.

L’enrichissement des données externes concerne quant à elle les données pu bliques le plus souvent partagées par la communauté. Cela comprend deux grands domaines ; dans un premier temps, des informations concernant les IP qui se connectent au SI peuvent être d’une grande aide. Est-ce que l’IP est présente sur des sites de répudiation d’IP ? Fait-elle partie de blacklist publique ? Fait-elle partie d’un réseau de botnets connus ? Autant de critères qui peuvent augmenter la fiabi lité dans la détection d’un incident de sécurité. Deuxièmement, existe-t-il d’autres SOC ou d’autres structures ayant connu des attaques similaires ? Si c’est le cas, la procédure de dépannage sera renseignée dans des bases de données publiques et pourra être utilisée dans de futur cas similaire. Mais pour être utilisé dans le futur, il faut que les équipes se rendent compte que la procédure est connue d’où l’intérêt d’avoir un système d’enrichissement de données compétent.

Outils visuels : Dashboard (SIEM)

La possibilité de visualiser des données et des événements est un autre élément clé des solutions SIEM, car elle permet aux analystes de visualiser facilement les données. Les tableaux de bord contenant des visualisations ou des vues multiples aident à identifier les tendances, les anomalies et à surveiller l’état général de santé ou de sécurité d’un réseau. Certains outils SIEM sont livrés avec des tableaux de bord préétablis 13, tandis que d’autres permettent aux utilisateurs de créer et d’af finer les leurs. Généralement ces données sont projetées sur de grands écrans situés sur un des murs de la pièce du SOC. Les graphiques choisis pouvant changer suivant

12. https://docplayer.fr/170242765-Deploiement-d-un-siem-et-enrichissement-des-donnees. html

13. https://www.logsign.com/blog/what-are-the-types-of-dashboards-in-a-siem-solution/

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 40

l’entreprise nous allons prendre comme exemple le SOC d’Excellium que notre pro motion a visité. Dans le SOC il n’y avait que trois grands écrans muraux contenant des dashboards, en effet, même si sur le papier, avoir le plus d’informations possible peut paraître intéressant, il est impensable pour un employé d’avoir un oeil attentif sur plus de 2 ou 3 écrans à la fois. Ainsi, le choix d’Excellium fut de seulement afficher des données essentielles et généralistes.

Sur l’un des écrans (écran 1) on peut voir la liste des alertes du SIEM par ordre chronologique avec leur niveau d’alerte, l’heure, et l’entreprise qui en était la cible. On y voit aussi le nombre d’alertes en attente ou en cours de traitement. Cette information permet à l’équipe d’avoir une information permanente sur la charge de travail et sur la criticité des alertes en cours.

Sur un autre écran(écran 2) on affiche des statistiques concernant les types d’alertes reçus mis en corrélation avec l’entreprise et l’heure de réception de l’alerte. Ce type de donnée permet au SOC de repérer facilement si pour une raison x ou y une alerte est surreprésenté dans une entreprise ou pendant une période donnée.

Enfin, sur le troisième (écran 3) on pouvait voir la liste des attaques malicieuses avec leur état de traitement. Une attaque peut être :

— En attente de traitement

— En cours de traitement

— Traité

Cet écran permet à l’équipe du SOC d’avoir un point de vue global du traitement des menaces en cours.

Figure 3.4 – Exemple de Dashboard d’un SIEM

Voici un exemple visuel qui permet de s’imaginer à quoi pouvaient ressembler les DashBoard que nous avons eu la chance de voir à excellium. On peut voir que cette exemple de DashBoard est assez semblable à l’écran 2 d’Excellium décrit précédemment ; au niveau du contenu tout du moins. Cependant, bien qu’au niveau du fond ils soient très semblable au niveau de la forme ils n’ont rien à voir, et ce pour une raison très simple, il existe des centaines d’affichages de DashBoard possible et

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 41

donc chaque SOC différent aura un affichage de dashboard adapté à ses méthodes de travail.

Difficultés que l’on peut rencontrer avec les SIEM

Depuis le début de ce document, on a fait l’éloge de l’utilisation d’un SIEM afin de sécuriser un SI, cependant l’achat et la mise en place d’un SIEM comprend son lot de point négatif, il est donc indispensable de bien réfléchir avant de prendre la décision de s’en équiper. Ici nous parlerons uniquement de la mise en place d’un SIEM interne.

Dans un premier temps un SIEM est très coûteux et complexe, surtout pour une PME, en effet le déploiement d’un SIEM peut paraître extrêmement onéreux, cependant selon Frédéric Saulet le Directeur Régional Europe du Sud de LogPoint 14 il est de plus en plus facile d’avoir accès à des licences de SIEM même pour des entreprises ayant un budget limité. En revanche même si la licence de SIEM en elle même est abordable, il faut prendre en compte le côté infrastructure et matériel d’autre part mais surtout le côté technique et connaissances. En effet, le fonction nement d’un SIEM nécessite un niveau élevé dans le domaine de la sécurité IT. Ces outils nécessitent aussi du personnel qui se forme continuellement sur les paysages des menaces, qui sont en constante évolution.

De plus, un SIEM est configuré pour éviter à tout prix les faux négatifs (incidents non détectés) au détriment de la protection contre les faux positifs (événement normal pris à tort comme étant un incident de sécurité). Ainsi, afin de trier les vrai et faux négatifs, en plus de personnel qualifié (sénior), il est nécessaire d’avoir une main d’œuvre (dont le nombre dépend de la taille des données collectées), qui sera certe peut être des juniors donc moins payés, mais cela représente un coût supplémentaire.

Ensuite, certe un SIEM permet de détecter les incidents de sécurité en corrélant et analysant des données, mais ce n’est pas un outil conçu pour identifier les causes des incidents ainsi que les lacunes en matière de sécurité qui en découlent. Ainsi, il est peut être plus intéressant pour une entreprise d’investir dans des mesures de prévention (type certification ISO 27001 sur son SI, stage de consciences numériques pour les employés etc. . .) qui réduisent la surface d’attaque. Évidemment l’idéale, d’un point de vue strictement sécurité, serait de faire les deux (un SIEM et des mesures préventives) mais pour une PME le budget peut être trop faible pour les deux.

14. https://www.globalsecuritymag.fr/SIEM-rumeurs-et-realites,20160831,64798. html

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 42 3.3 Réaction

3.3.1 SOAR

Un SOAR 15 (Security Orchestration, Automation and Response) est un logiciel conçu grâce aux principes de 3 autres solutions dans le domaine de la sécurité :

Figure 3.5 – Les trois outils formant le SOAR

— SAO 16 (Security Automation Orchestration)

Solution permettant d’automatiser et orchestrer les workflows sur plusieurs outils, systèmes et applications. La tâche à automatiser est-elle courante ? fastidieuse ? chronophage ? Si au moins l’une de ces questions est vraie pour une tâche donnée, il est probablement utile de l’automatiser afin de permettre aux équipes de gagner du temps (Selon redhat.com l’automatisation permet de réduire le coût moyen d’une faille d’un maximum de 95%). Le SAO va aussi créer des étapes à suivre afin d’aider le SOC à corriger plus efficacement et plus rapidement les alertes dont il s’occupe. Cela permet de gagner du temps, ce qui est très utile lorsque les logs sont compliqués à analyser ou bien que des alertes graves se présentent.

— SIRP 17 (Security Incident Response Platforms)

Solution permettant de gérer des incidents, et d’y répondre efficacement. Le SIRP va récupérer les alertes directement dans le SIEM et voir s’il peut cor riger l’alerte de lui-même grâce à ce qu’il sait de cette dernière. Le SIRP a

15. https://cyware.com/educational-guides/security-orchestration-automation-and-response 16. https://www.coresecurity.com/blog/sao-vs-siem-not-enemies-security-defending-duo 17. https://www.trustradius.com/incident-response

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 43

aussi la capacité de neutraliser le système d’où provient l’alerte afin d’éviter la propagation de la potentielle attaque.

— TIP 18 (Threat Intelligence Platforms)

Solution permettant d’obtenir des informations sur les indicateurs de compro mission connus (IOC, indicators of compromise) et les tactiques, techniques et procédures (TTP) des attaquants. Pour se faire le TIP va ingérer, analyser et diffuser des données et des renseignements sur les menaces. Ces connaissances que le TIP va acquérir seront ensuite partagées à tous les autres utilisateurs du TIP en question afin d’aider tous les SOC en y apportant notre expérience.

Le SOAR est une version améliorée de chacune de ces fonctionnalités, regroupées entre elles en un seul logiciel. Plutôt qu’avoir énormément d’onglets différents, toutes les solutions sont dans un seul et unique onglet. De plus, le SOAR peut se greffer au SIEM, dont on a parlé au dessus, afin de renforcer les use cases déjà implémentés, en rajouter d’autres, et pouvoir gérer automatiquement certaines alertes, ou au moins découper le travail en plusieurs étapes pour la personne s’en servant. En pratique, le SOAR étant greffé au SIEM ils ne forment qu’une seule entité, ainsi il est possible que certaines des fonctionnalités citées précédemment puissent être associées au deux appareils, dans ce cas il sera évoqué dans la partie respectant le plus les fonctions théoriques de la technologie.

Figure 3.6 – Exemple de page d’analyse d’alerte dans un SOAR (IBM Resilient)

Grâce à tout ça, l’analyste va pouvoir différencier plus facilement les “faux po sitifs” des “vrai positifs”, ce qui est une grosse partie de son travail. Ce concept de faux positif ou vrai négatif est simple : environ 80% des alertes détec tées par les use cases sont des fausses alertes, et les analystes doivent différencier ces fausses alertes des vrais dangers tout ça en analysant les logs. Il y a généralement deux types d’analystes dans un SOC :

18. https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 44

— L1 :

Appelée la ligne 1, ce sont les analystes un peu moins expérimentés, plus jeunes dans le métier, qui vont s’approprier les logs arrivant dans les SIEM, et les analyser. Étant plus jeunes dans le SOC, ils n’ont pas forcément toutes les connaissances nécessaires, et cette L1 souvent composée de quelques stagiaires, le second type d’analyste devient indispensable. Lorsque le SIEM alerte d’une potentielle intrusion leur rôle est de vérifier s’il s’agit d’un vrai positif ou d’un faux positif. Dans le cas où il y aurait un doute, ils laissent la main à la seconde ligne. Malgré tout, la L1 est composée de plus de membres que la L2 et c’est eux qui s’occupent de la majorité des alertes.

— L2 :

Appelée la ligne 2, ce sont les analystes plus expérimentés, avec plus d’an cienneté dans le métier, que la L1 va solliciter lorsqu’ils n’arrivent pas à être sûr de si les logs sur lesquels ils travaillent sont dangereux ou pas. Certains logs sont plus difficiles à juger et en tant que membres plus expérimentés du SOC, ils sont plus facilement capable de voir ce qui cloche ou pas. Les alertes reçues par la seconde ligne étant relativement peu nombreuses par rapport au total des alertes, cela leur laisse le temps d’investiguer plus en profondeur afin de se forger un avis. Pour avoir plus de contexte sur l’alerte, la L2 récupère aussi les analyses faites préalablement par la L1. Ils peuvent aussi chercher des logs en corrélation avec celle ayant causé l’alerte directement dans le SOC pour trouver de potentiels faux négatifs, qui sont des logs dangereux mais non détectés par les use cases du SIEM.

3.3.2 Prise de contact et neutralisation

Une fois qu’un analyste a fini son travail sur une alerte, il doit prendre une décision : Faux positif ? Vrai positif ? S’il a des soupçons ou des doutes, dans le cas d’un SOC externe, l’analyste va faire une prise de contact par appel à l’entreprise d’où provient l’alerte afin de récolter des informations de toutes sortes : Il va essayer de savoir si l’entreprise a remarqué quelque chose de suspect, si ce n’est pas une équipe de pentest qu’ils auraient pu engager sans vous prévenir, s’il y a déjà des dégâts sur leur système d’information. Si le SOC est interne à l’entreprise alors la prise d’information se fera bien plus naturellement mais il sera toujours nécessaire de vérifier même en interne si ce n’est pas une fausse alerte dû à l’erreur humaine en contactant le lieu exact d’où provient l’alerte. Une fois ces informations récupérées, la décision doit être prise.

Dans le cas d’un faux positif alors tout va bien, l’alerte est classée comme cor rigée, et on passe à la suivante. Dans le cas contraire où ce serait un vrai positif et qu’il y a belle et bien une attaque, alors il faut faire quelque chose. Le SOAR permet de neutraliser certains systèmes, ce qui peut aider à contenir l’attaque et c’est ce que le SOC va essayer de faire. Une fois cette tentative de neutralisation effectuée, plus le choix, il faut laisser la main aux équipes se chargeant de la situation de crise qui réagiront en fonction de la criticité de l’attaque.

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 45 3.4 Crise

3.4.1 Le CSIRT

Leur fonction première

Les employés CSIRT 19 sont considérés comme les “pompiers” du SOC. Leur rôle principal est de se rendre sur site lors d’un incident de sécurité détecté par le SOC. Dans le cas d’un SOC externe il est primordial que la société victime soit au courant, en effet il est impensable qu’un employé du CSIRT puisse entrer légalement dans une entreprise sans l’accord de ladite entreprise. Une fois sur site, le principal outil du CSIRT fait ce que l’on appelle une analyse forensique. Cette dernière consiste en un ensemble de procédures permettant de récupérer, extraire, lire et analyser des données provenant soit de la mémoire (vive ou morte) d’un ordinateur infecté, soit directement dans le données d’un SI.

Voici quelques exemples d’outils dans le cas d’une analyse forensique d’un ordi nateur ainsi que leur utilité : 20

— Lace Carver :

Lace Carver est un outil de récupération de données (texte, image ou vidéo), utilisé entre autres par la police judiciaire, sur un disque dur dont les données ont pu être effacées ou partiellement corrompues. Cela est possible grâce à la manière dont un disque dur structure ses données, en effet, un disque dur, en plus de stocker les données d’un fichier, tient un sommaire contenant le nom et l’emplacement sur le disque dur d’un fichier. Lorsqu’on effectue une suppression classique d’un fichier uniquement le sommaire est modifié (les bits correspondant au reste du fichier est toujours présent d’un point de vue transistor mais est considéré comme libre). Ainsi si rien n’a été écrit par-dessus la zone nouvellement libre, une récupération est possible. La récupération des données dans un sens large est primordiale afin de retracer le problème et y remédier le plus rapidement possible.

— Magnet et Cellebrite :

Magnet et Cellebrite sont des outils comparables à Lace Carver mais pour les téléphones mobiles.

— RegRipper :

RegRipper est une solution d’audit qui permet aux équipes de récupérer et d’extraire les paramètres de configuration de Windows depuis les fichiers ruches (SAM Security, Software, System) vers un fichier texte. Cela comprend les données utilisateurs, les services, les pilotes, la configuration réseau etc. . . Ainsi, il est possible de lire les documents récemment ouverts, les utilisateurs ainsi que les groupes par exemple.

— WireShark :

WireShark est un outil d’analyse de réseau ou un outil d’analyse de packet opensource et gratuit avec une interface graphique. L’analyse réseau et la rétro

19. https://www.cyberjobs.fr/Job/Analyste-Reponse-aux-incidents-de-Securite--CSIRT--chez-Bouygu20. https://www.google.com/url?q=https://jafwin.com/2019/04/26/

top-8-des-outils-de-forensique-informatique/&sa=D&source=docs&ust=

1634763069833000&usg=AOvVaw37onRCVW-WnjJF18ofBaWp

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 46

ingénierie ne sont qu’une partie des fonctionnalités de WireShark mais c’est elle que les agents du CSIRT utilisent essentiellement. L’analyse partitionner du réseau en temps réel ou en décalé peut permettre de résoudre des attaques faites essentiellement à distance.

Une fois l’investigation finie, les équipes du CSIRT font un rapport afin que l’en treprise ait une vue plus précise de l’incident et surtout puisse l’utiliser légalement afin de prouver les dommages à l’assureur par exemple.

En dehors d’une intervention

Fort heureusement, il n’y a pas en permanence des incidents de sécurité, pendant qu’ils ne sont pas en intervention il est fréquent que les équipes du CSIRT soit employés afin de :

— Développer et Rechercher :

Cela peut être différent suivant les CSIRT mais les équipes, de par leur travail, doivent posséder de grandes connaissances et de grandes compétences tech niques en général. Ainsi leurs connaissances peuvent être mises à contribution afin de développer des outils notamment pour le SOC. En effet, il n’est pas rare que ce soit le CSIRT qui développe en partie les use cases du SIEM par exemple. En plus de cela, le CSIRT peut aider au développement d’indicateurs de compromission. Un indicateur de compromission (ou IoC pour Indicators of Compromise) est un outil qui va permettre de détecter les traces qu’un malware peut laisser. En effet, même si les auteurs de malwares essayent de mettre en œuvre des logiciels totalement invisibles, c’est fort heureusement impossible, chaque application laisse des traces, même minime, de son exis tence sur le réseau. Familièrement la notion de IoC peut tout autant définir les logiciels permettant de détecter les miettes laissées par un malware mais aussi les miettes en elles-mêmes. Un facteur de compromission est un des as pects des use cases des SIEM expliqué précédemment mais son aspect très technique en fait une tâche adaptée à des employés expérimentés comme ceux du CSIRT. Une partie de leur temps peut aussi être employée à développer ou améliorer des outils forensic comme ceux cités précédemment, bien que la qualité de certains outils (même open source) ne rendent pas cette tâche prioritaire.

— Mise en commun du savoir :

La mise en commun du savoir est une étape très importante de la cyber sécurité en général et le CSIRT ne déroge pas à cette règle. Effectivement, pour répondre le plus rapidement possible à une menace, il est évidemment indispensable d’identifier la menace, mais surtout de connaître les méthodes d’élimination du malware ainsi que les procédures de restauration afin d’an nuler les dommages du virus. Pour la partie identification il faut se référer au CVE (détaillé plus tôt) qui peut être simplement amélioré si une équipe découvre un malware ou une faille inconnue. En revanche, pour ce qui est de la réaction après avoir identifié la menace, il existe des fiches méthodes per mettant d’avoir des informations sur les procédures à effectuer pour éliminer la menace le plus rapidement possible. La rédaction de ces fiches méthodes fait partie du travail du CSIRT.

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 47

3.4.2 Le SIRP (Security Incident Response Plan)

Malgré toutes les mesures mises en place par les équipes de cyber sécurité, il ar rive régulièrement que des entreprises soient ralenties voir totalement arrêtées dans leur travail. Dans certains cas, cela est dû à une erreur humaine interne à l’entre prise mais cela peut être dû à une cyber-attaque ciblée sur une société mais aussi à un désastre plus physique : cela peut être un incendie volontaire ou accidentel par exemple. Il est important de noter que peu importe les raisons qu’elle soit physique, virtuelle, involontaire ou volontaire un plan d’action peut et doit être prévu afin de ne pas stopper son activité sur une trop grande période. Communément appelé SIRP (security incident response plan), ces plans regroupe les moyens à mettre en oeuvre afin de déplacer les postes de travail, les serveurs de travail ainsi que le personnel (même si depuis la crise du COVID et le développement du télétravail ce dernier point est moins primordiale).

Il existe deux grand type de plan distinct suivant si l’entreprise est simplement ralentie par le désastre ou si l’entreprise est à l’arrêt complet. Dans le premier cas, on parle de Plan de Continuité d’Activité (PCA), il a pour but de garantir la survie de l’entreprise en cas de sinistre important touchant le système informatique. Il s’agit de redémarrer l’activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d’une entreprise. Dans le second cas, il s’agit d’un Plan de Reprise d’Activité (PRA), c’est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permet à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d’information en cas de sinistre important ou d’incident critique.

En cas de PCA ou de PRA, il est primordial d’adapter les méthodes aux contextes ainsi qu’aux besoins de l’entreprise. Ainsi ces méthode doivent reposer sur de l’analyse de risque et de l’analyse d’impact :

— L’analyse de risque débute par l’identification des menaces sur de nombreux domaines tels que l’infrastructure, la sécurité du système d’information ou la conscience numérique des équipes de l’entreprise. Concernant l’infrastructure la menace peut être de l’ordre de l’attaque prémédité (intrusion dans les lo caux en usurpant une identité par exemple), de l’ordre de la maladresse d’un employé ou de l’ordre de la catastrophe naturelle (incendie, dégât des eaux . . .). Ensuite, la sécurité du système d’information de l’entreprise est évidem ment primordiale et doit être prise en compte dans l’analyse de risque ; cette dernière peut être externe à l’entreprise ou interne à l’entreprise (employé cor rompu par exemple). Enfin la conscience numérique joue un rôle important, la population étant pour la majorité serviable et peu éduquée à la conscience nu mérique, la majorité des attaques commencent par une défaillance humaine. Que ce soit du phishing, une clé USB trouvée par terre ou tout autre er reur partant d’une bonne intention ou d’une méconnaissance, l’Homme est le premier vecteur d’attaque.

— L’analyse d’impact intervient après l’analyse de risque et consiste en l’impact de ces dits risques s’ils sont avérés et à déterminer à partir de quand cette im pact devient critique, c’est à dire qu’il met en danger les processus essentiels à l’activité de l’entreprise et donc à sa survie dans le temps. Généralement

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 48

l’analyse d’impact se fait dans le pire des cas afin de n’avoir aucune surprise si l’incident se produit : on considère des événements qui peuvent aller d’un inci dent bénin à des accidents dramatiques et improbables (comme la destruction total du bâtiment par exemple), puis on détermine quels impacts financiers, humains, légaux etc . . . ils engendreraient. Une fois que tout cela est fait, on peut en déduire la durée maximum qu’un pôle ou qu’une fonction de l’entre prise peut être hors service sans que cela ait des répercussions irrécupérable sur l’entreprise.

Une fois ces deux étapes faites on peut associer à chaque failles un risque et un impact pour chaque failles, on calcule ensuite la criticité d’une faille correspondant (avec la formule criticité = impact \* risque). Puis pour les failles avec un niveau de criticité suffisamment élevé (ce niveau n’est pas fixe et dépend de l’entreprise) il convient d’implémenter des solutions afin de protéger au maximum l’entreprise de cette faille.

Ces plans d’actions sont généralement organisés par des prestataires externes à l’entreprise, en effet, les savoirs nécessaires à la mise en place des plans d’actions sont des compétences assez peu communes qui ne sont que très rarement présentes au sein de l’entreprise. Ainsi, les entreprises qui signent des contrats avec une sociétée spécialisé dans les plans d’actions, doivent se mettre d’accord sur deux points très précis :

— la Durée Maximale d’Interruption Admissible (DMIA) : Il correspond à la durée maximale avant laquelle l’entreprise doit pouvoir être prête à reprendre son activité.

— la Perte de Donnée Maximale Admissible (PDMA) : Elle correspond à une durée x telle qu’il est jugée acceptable de perdre les données qui datent de moins de x. Ainsi si un entreprise juge que sa PDMA est de 2 heures, elle devra faire une sauvegarde de backups de ses données toutes les 2 heures au maximum.

3.5 Conclusion

Un Soc utilise une très grande quantité d’outils, de procédures et de technolo gies afin de surveiller les systèmes d’informations et de les protéger au mieux des incidents de sécurité. La détection est assurée par un SIEM, fusion d’un SIM et d’un SEM. Basé sur le concept de puit de log, le SIEM y ajoute toutes les notions de tri, de management, de use case, d’interface graphique guidant l’utilisateur et de détection. Afin de faciliter la réaction après une attaque, il est possible de greffer au SIEM un SOAR. Fusion d’un SAO, d’un SIRP et d’un TIP ; le SOAR ajoute au SIEM les notions d’orchestration, d’automatisation et d’alerte.

Il est important de noter que le SOAR est un ad-on du SIEM et que par consé quent il n’est pas totalement faux d’évoquer le SIEM uniquement lorsque l’on parle des outils et des technologies utilisées par le SOC en général (bien que ce soit ,d’un point de vue technique, un abus de langage). Une fois la menace avérée les équipes du CSIRT, un équivalent aux pompiers pour les problèmes de cybersécurité, se dé placent sur place afin d’investiguer plus en détails (les procédures étant plus simples

*CHAPITRE 3. SOC, PROCÉDURES ET OUTILS* 49

lorsque l’on est présent en physique dans les locaux) et résoudre au mieux les inci dents de sécurité afin que les activités du client soient le moins possible impactées.

Ainsi, bien que l’utilisation d’un SOC (qu’il soit interne ou externe) soit un coût relativement conséquent pour une société son utilisation est une étape indispensable afin d’assurer une sécurité correcte du SI d’une entreprise, et donc, réduire les chances d’attaques qui causeraient plus de dégâts que le coût d’installation d’un SOC dans l’entreprise.

Chapitre 4

Traitement d’une menace

4.1 Sources

Dans ce chapitre, la majeure partie des notions présentées sont issues du guide de l’ANSSI ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS 1. Le reste de ces notions provient des cours de Sécurité des Systèmes d’Information de Monsieur Jean-Marc MISERT et de Politique de Sécurité de Monsieur Nicolas MAYER.

4.2 Introduction

En informatique, une menace est une cause potentielle d’incident, qui peut ré sulter en un dommage au système ou à l’organisation. Une menace est commune à une catégorie d’asset (un bien ou un atout). En présence d’une vulnérabilité, la menace devient réalisable et sa criticité augmente. La criticité de la menace dépend du risque de réalisation de cette dernière et de son impact sur l’asset. On en déduit la relation suivante :

Figure 4.1 – La Criticité par rapport à la Fréquence et la Gravité de la Menace

Dans ce chapitre, nous allons détailler les trois étapes du traitement d’une me nace tout en nous concentrant sur les menaces informatiques à but criminel. La première étape concerne la prévention face à la menace. La seconde se concentre sur les réponses utilisées pour contrer la menace. La troisième et dernière étape consiste au rétablissement de l’ensemble du système d’information touché par la menace. La première partie sera générale, dans le sens où les mesures présentées seront utilisées peu importe le type de menace, tandis que les seconde et troisième parties seront explorées à travers un type de menace bien spécifique : les ransom wares.

1. https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques\_par\_ rancongiciels\_tous\_concernes-v1.0.pdf

50

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 51

Qu’est-ce qu’un ransomware (rançongiciel) ?

Un ransomware est un logiciel malveillant dont l’objectif est de prendre en otage les données personnelles de sa ou ses victimes. Afin de parvenir à ses fins, le ran somware va commencer par chiffrer l’ensemble des données personnelles de la cible, puis va demander une rançon (d’où le terme de rançongiciel) en échange de la clé de déchiffrement. La plupart du temps, le rançongiciel va menacer de détruire, ou de publier, les données en cas de défaut de paiement.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 52 4.3 Le traitement de la menace avant la réalisation

4.3.1 Introduction

Dans le cadre du traitement de la menace avant la réalisation, nous allons nous concentrer sur les différentes mesures de prévention existantes, sans être exhaustif. A l’heure actuelle, il existe de nombreuses méthodes et de nombreux outils pouvant être déployés sur la plupart des systèmes. A noter que chaque système est unique et dispose de ses propre spécificités, les éléments qui seront présentés par la suite peuvent ne pas être pertinent en fonction dudit système. De même des mesures complémentaires peuvent s’avérer nécessaire selon les circonstances.

Ces méthodes et outils doivent permettre de limiter les risques de vulnérabilité, car on ne peut se débarrasser d’une menace de manière permanente sauf en cas de suppression de l’asset . Nous allons maintenant traiter des différentes méthodes et outils pouvant permettre de prévenir une menace via la réduction ou la sup pression des vulnérabilités. Ces derniers vont être répartis en trois catégories, selon leur importance et leur complexité de mise en place : Sécurité Basique, Sécurité Intermédiaire et Sécurité Avancée.

4.3.2 Sécurité Basique

En dépit de toutes les technologies à notre disposition pour assurer notre sé curité, il convient de ne pas oublier les étapes simples qui font d’une politique de sécurité une politique efficace. Une des bonnes pratiques de la sécurité est d’utiliser des mots de passe robustes, c’est à dire suffisamment longs, comportant des lettres minuscules et majuscules, des chiffres, des caractères spéciaux et surtout, ne pou vant être facilement déduit par autrui (éviter les dates de naissances et autres mots de passes basés sur des informations personnelles par exemple).

Le déploiement d’Anti-Virus et leur maintien dans le temps permettra égale ment de renforcer la sécurité face aux différents MalWares qui pourraient porter atteinte au système. Ces Anti-Virus, de même que l’ensemble des logiciels du sys tème, devront être régulièrement mis à jour afin que les failles les concernant soient patchées.

Une autre bonne pratique pour renforcer les bases de la sécurité est de faire de la prévention auprès des différents utilisateurs de votre système. Cette prévention leur permettra d’être mieux renseigné face aux différentes menaces pesant sur eux ou sur ledit système. Cette campagne de prévention peut prendre différentes formes et peut comporter de nombreuses thématiques. Parmi ces thématiques, on peut retrouver des campagnes d’alertes contre le phishing ou encore contre le piratage psychologique (social engineering).

Dans un contexte plus global, la sécurité se doit d’être uniforme sur l’ensemble du système. Il est inutile de barricader la porte si la fenêtre reste ouverte. Dans la partie suivante, nous allons détailler différentes méthodes pouvant être déployées afin d’augmenter le niveau de sécurité du système.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 53

4.3.3 Sécurité Intermédiaire

Maintenant que le système de sécurité a atteint un niveau basique, la prochaine étape aura pour but de renforcer les mesures mises en place précédemment. Dans ce but, il est pertinent d’effectuer certains ajouts au système de sécurité.

Dans un premier temps, il est judicieux, voire nécessaire, de segmenter le réseau afin que chaque partie de ce dernier soit indépendante les unes des autres. Ceci permettra une meilleure organisation dudit réseau ainsi que du système de sécurité qui lui est lié. Un bon moyen de segmenter le réseau est de créer différents VLAN (Virtual Local Area Network) afin de simuler des réseaux distincts.

Ensuite, une étape importante consiste à installer des Firewalls (Pares-Feu) aux endroits clés de l’architecture, afin de filtrer le trafic entrant et sortant du système en se basant sur un certain nombre de règles de filtrage. Cet ajout permettrait de limiter les connexions en entrée et en sortie du système à celles strictement autorisées. Une astuce permettant de renforcer la sécurité apportée par un Firewall, mais pouvant se révéler assez coûteuse, est d’installer un second Firewall en complément du premier, de préférence de marque différente, afin que les éventuelles failles présentes sur l’un desdits Firewall soient couvertes par le second.

De plus, un système de gestion des logs est un ajout pertinent. Ce dernier per mettra d’avoir une vision globale des différentes alertes de sécurité passées ou en cours, que ces dernières soient des tentatives d’intrusion logicielles (tentative d’in trusion sur le réseau ou tentative d’action non autorisée) ou matérielles (tentative d’accès dans un lieu non autorisé ou d’utilisation d’un asset non autorisé).

Suite à cela, il convient d’établir une stratégie de gestion des risques. La première étape de cette stratégie est d’établir une matrice d’aversion au risque. Une matrice d’aversion au risque, ou matrice des risques d’accordance, est une table permettant d’évaluer la criticité d’une menace en fonction de sa fréquence et de sa gravité.

Figure 4.2 – Exemple de matrice d’aversion au risque

Cette matrice a pour but d’aider à établir une politique de sécurité efficace du système. Pour ce faire, la matrice va indiquer, de manière distincte, quels sont les assets les plus sensibles grâce à leurs niveaux de criticité. Une fois cette matrice complétée et les assets les plus vulnérables clairement identifiés, la prochaine étape sera de pallier au mieux à ces vulnérabilités.

Enfin, il est important de sécuriser son installation d’un point de vue physique. Cela commence par l’établissement d’une politique de droit stricte et restrictive.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 54

De ce fait, seules les personnes ayant l’autorisation explicite d’accéder à un as set ou de l’utiliser pourront le faire. Ceci permettra d’éviter qu’une personne non digne de confiance, ou n’ayant pas l’autorisation d’accès, ne puisse accéder aux res sources stratégiques. La sécurisation de l’installation comporte également de nom breux points sur la protection face aux menaces dites accidentelles, criminelles ou encore environnementales (inondation, tornade, tremblement de terre, etc. . .).

Une fois ces ajouts effectués, le système de sécurité aura atteint un niveau correct mais loin d’être satisfaisant. Dans la partie suivante, nous allons détailler comment élever le niveau de sécurité du système à un niveau de performance suffisant afin d’atteindre un niveau de risque acceptable.

4.3.4 Sécurité Avancée

Une fois les différents ajouts effectués et le système de sécurité correctement mis en place, il peut être pertinent d’effectuer des scans régulier dudit système afin de détecter d’éventuelles failles.

Un bon moyen de réduire ces failles est de se conformer aux différentes normes ISO relatives à notre système, en l’occurrence les normes ISO 27XXX. Les normes ISO sont des documents mettant en avant les différentes règles en vigueur concernant un produit, un service, un processus ou une personne. Ces règles étant reconnues par un grand nombre d’États, elles font office de normes internationales. Les premières à mettre en place sont les normes ISO 27001, ISO 27002 et ISO 27003, ces dernières se concentreront sur la manière de gérer un système de sécurité, La norme ISO 27001 servira à spécifier les différentes exigences à respecter, la norme ISO 27002 est considéré comme un état de l’art tandis que la norme ISO 27003 se spécialisera sur l’implémentation des précédentes normes. Une autre norme importante de la série ISO 27XXX est la norme ISO 27005 car cette dernière se focalise sur la gestion des risques.

Malgré tous les systèmes de sécurité existants, la menace n’a toujours pas été, et ne sera jamais, complètement éliminée. Afin de pallier les possibles pertes subies lors d’une attaque, la mise en place de BackUps est primordiale. Ces derniers vont permettre de relancer le système sur une sauvegarde précédemment effectuée. Ces sauvegardes peuvent être automatisées et il est conseillé d’en effectuer de manière régulière.

Une fois le système de sécurité déployé, il est conseillé de faire appels à des consultants externes ayant pour mission d’effectuer des tests d’intrusion sur ledit système afin d’en tester la robustesse. Ces consultants étant des hackers éthiques, chaque faille découverte par leurs soins sera présentée et analysée sans le moindre risque pour le système. Chaque faille ainsi découverte pourra, et devra, être corrigée afin de renforcer encore plus la sécurité. Il convient de garder à l’esprit que même si un très grand nombre de failles ont été découvertes, elles ne le seront jamais toutes. Deux options sont possibles pour le test du système : faire appel à une entreprise de Pentest (méthode d’audit consistant à effectuer des tests d’intrusions) ou alors de faire appel à une communauté dont chaque membre sera rémunéré à hauteur des failles découvertes (on parle alors de Bug Bounty).

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 55

Il convient également d’établir un plan de cellule de crise 2. Une cellule de crise est composée des principaux décideurs, des experts au regard de la situation, de professionnels de la communication ainsi que de juristes, d’assureurs et de représen tants des ressources humaines. L’objectif d’une cellule de crise est de se réunir lors d’une crise majeure afin de centraliser les informations, évaluer les risques et leurs évolutions ainsi que d’évaluer l’efficacité des mesures déployées. En général, une cellule de crise se découpe en deux parties : une cellule décisionnelle, composé de l’équipe de direction, de juristes et de responsables des ressources humaines, ainsi qu’une cellule opérationnelle, composé elle des différents ingénieurs et techniciens ainsi que d’experts au regard de la situation. La cellule de crise a également pour objectif de définir la stratégie de communication en temps de crise.

Figure 4.3 – Exemple de composition d’une cellule de crise

L’établissement de différentes stratégies de communication, interne et externe, a pour but de prévoir quelles seront les informations à transmettre aux différentes personnes lors de la réalisation d’une menace. Chaque menace étant différente, il est nécessaire d’établir une stratégie pour chacune d’elle afin que la communication soit la plus efficace possible.

Il est également nécessaire d’établir un Plan de Continuité de l’Activité (PCA) et un Plan de Relance de l’Activité (PRA). Comme spécifié dans le chapitre précédent, le PCA a pour but de garantir la poursuite de l’activité sans interruption et avec une perte de données minimale. Ce dernier se doit d’être spécifique à chaque structure et à chaque situation. Le PRA, quant à lui, est un ensemble de procédures ayant vocation à reconstruire et remettre en route le système en cas d’incident critique. Ce dernier est spécifique à chaque structure et est souvent vu comme une assurance, ce qui conduit les entreprises à le délaisser, à leurs risques et périls.

En lien avec le PCA et le PRA, le Recovery Time Objective (RTO), ou Du rée Maximale d’Interruption Admissible (DMIA) en français, et le Recovery Point Objective (RPO), ou Perte de Données Maximale Admissible (PDMA) en français, sont également d’une grande importance car ce sont eux qui vont définir les ob jectifs de relance de l’activité d’une entreprise. Le RTO va définir la durée pour laquelle le système doit à tout prix être remis en état, que ce soit en état dégradé ou non, sous peine d’interruption d’activité trop longue pour l’entreprise. Le RPO quant à lui définit la perte maximale de données tolérables lors d’un incident. C’est ce dernier qui va influencer la fréquence des sauvegardes effectuées. Ce dernier est généralement exprimé en heures ou en minutes.

2. https://www.cigref.fr/archives/entreprises-et-cultures-numeriques/wp/ wp-content/uploads/2015/08/Rapport-CIGREF-INESJ-2015-cellule-de-crise.pdf

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 56 

Figure 4.4 – Schéma explicatif du RTO et du RPO

4.3.5 Se préparer

La dernière chose à faire pour prévenir une menace est de s’y préparer, car la question qu’il faut se poser n’est pas “Que faire SI je suis attaqué ?” mais “Que faire QUAND je suis attaqué ?”, car aucun système de sécurité n’est infaillible et les assaillants ont toujours un coup d’avance sur les défenseurs. Afin de pallier ce pro blème, une des solutions serait de contracter une assurance, afin que les potentielles pertes soient couvertes par cette dernière.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 57

4.4 Le traitement de la menace pendant la réalisa tion

4.4.1 Introduction

Dans cette partie, nous allons couvrir les différentes actions à entreprendre afin de traiter la menace, à partir du moment ou celle-ci est repérée, jusqu’au moment où l’on se considère hors de la menace, c’est à dire le moment où celle-ci est contenue.

Figure 4.5 – Exemple des étapes à suivre pendant la menace

Comme montré ici, un certain nombre d’étapes sont nécessaires au traitement de la menace, nous allons donc détailler les différentes mesures a mettre en place, durant chacune des ces étapes, tout en axant notre traitement sur un type d’attaque en particulier, le ransomware.

4.4.2 Identification

Comme expliqué dans le chapitre précédent, le SOC ( Security Operation Center) est chargé de la détection et de la réaction face à la menace : la surveillance, les scénarios de détection et la gestion de la cellule de crise.

Le SOC fait partie des équipes qui permettent de gérer la menace dans un SI. Une menace peut se manifester de différentes manières et il en existe beaucoup. Verizon, une entreprise américaine de télécommunication, a analysé ses données portant sur plus de 10 000 incidents et sur une période de 10 ans 3et a établi 9 types de menaces. 96% des attaques ont pu être réparties dans ces neufs types, que voici :

— Les pertes ou vol d’appareil

— Les attaques DDos, donc les attaques par déni de service

— Les arnaques à la carte bancaire

— Les attaques d’application web

— Le cyber-espionnage

— Les intrusions

— Le vol interne

— Les erreures humaines

— Les malwares

Parmi cette dernière catégorie, on retrouve les ransomwares. La suite traitement de la menace sera axée plus précisément sur les ransomware, déjà défini précédem ment.

3. https://www.verizon.com/about/news/verizon-2015-data-breach-investigations-report

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 58

Un ransomware, rappelons-le, est un malware qui va chiffrer les données de sa victime en échange d’une rançon. Traditionnellement un ransomware supprime les fichiers en cas de non paiement. Cependant depuis 2019, il existe des ransomware à double extorsion : en plus de chiffrer les données, le ransomware exfiltre les données, ces informations pourront être publiées ou vendues. La première attaque connue de ce type est le ransomware Maze apparu fin 2019. Aujourd’hui il existe même une extension de cette double extorsion : la triple extorsion : les attaquants demandent en plus une rançon aux victimes collatérales.

On a pu remarquer qu’il existe beaucoup de menaces différentes, et c’est pour quoi il est parfois difficile de les repérer. Il peut-être utile de faire appel à des outils d’analyse des log qui vont signaler des alertes, comme des IDS, des IPS ou des outils d’analyse comportementale (UBA, User Behavior Analytics). Ces derniers sont basés sur des règles et/ou de l’analyse comportementale des assets, des utilisa teurs ou du réseau. Ils permettent d’analyser le nombre important d’informations générées continuellement de manière automatisée et d’aider les personnes en charge d’analyser les alertes.

Ces alertes permettent de repérer de potentielles attaques ou des potentiels patterns d’attaque. Un exemple de pattern est la chaîne cybercriminelle (ou cyber kill chain en anglais) qui définit certaines étapes par laquelle passerait des hackers dans le cadre de leurs attaques. Notre exemple de pattern est celui de la société Varonis 4. Il faut savoir que d’une société à l’autre ces patterns sont légèrement différents. Voici les 8 étapes proposées par Varonis :

— La reconnaissance :

C’est la première étape, il s’agit de repérer et effectuer une reconnaissance des lieux, une reconnaissance des lieux, et ce repérage doit être fait au niveau physique et informatique. Cela peut concerner le réseau avec des scan par exemple. L’attaquant fait aussi de la recherche d’informations sur les failles ou les vulnérabilités qu’il pourrait exploiter pour pénétrer le SI.

— Intrusion :

Une fois l’étape de renseignement faite, le cybercriminel s’infiltre grâce à ses renseignements précédemment trouvés. C’est à cette étape que l’attaque de vient active.

— Exploitation :

Le hacker a accès au système, il y apporte des modifications et l’exploite : il peut créer de nouveaux scripts, installer des outils supplémentaires pour sa future ascension dans les privilèges. Il peut également modifier les certificats de sécurité pour favoriser son élévation.

— L’escalade de privilèges :

Le but de l’attaquant est à présent d’ élever ses autorisations sur l’asset dont il a déjoué la sécurité. Son objectif est d’avoir plus d’accès à plus de ressources, aux fichiers de configurations et aux permissions.

— Mouvement latéral :

Suite à son ascension sur un asset, le hacker se déplace de système en sys tème en vue d’obtenir plus d’accès et de ressources, c’est une exploration plus avancée que la précédente.

4. https://www.varonis.com/blog/cyber-kill-chain/

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 59

— Le camouflage :

L’attaquant masque sa présence pour passer inaperçu et cache ses traces afin de ne pas être repéré.

— Déni de service :

Pour cette partie son ambition est de perturber, interrompre les accès. Cela aura pour résultat d’empêcher les utilisateurs légitimes d’avoir accès à ce dont ils ont besoin, cela peut entraîner une panne des systèmes et saturer les services.

— Exfiltration :

Le hacker va copier, transférer, déplacer les informations vers un emplacement sous son contrôle.

Figure 4.6 – Schéma explicatif de la Cyber Kill Chain

Dans ces situations certains outils comme les UBA permettent de lancer des alertes en donnant des hypothèses sur les attaquants qui seront traités par l’équipe chargée de la détection et réaction face à la menace .

Une fois ces alertes données, elles passent par un tri puis leur gravité est déterminée. Selon la gravité de la menace, certaines actions seront entreprises en accord avec son niveau de criticité.

Certaines de ces alertes ont un niveau de gravité élevé et peuvent donner lieu à la mise en place d’une cellule de crise.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 60

4.4.3 Cellule de crise

Étant donné que certaines attaques ne vont pas juste entraîner une perte d’argent ou de données (réputation, confiance des clients par exemple), il est recommandé de mettre en place une cellule de crise. Celle-ci sera au plus haut niveau organisationnel, sera indépendante des groupes de travail existants. Son rôle sera de coordonner et d’exécuter les procédures écrites au préalable.

Parmi les rôles de cette cellule, on retrouve par exemple la gestion de la stratégie de communication interne et externe, la gestion des informations à collecter et l’organisation pour entreprendre une poursuite pénale (via la CNIL pour la France). Dans le dernier cas, avec l’aide du DPO, la cellule va avoir pour but d’identifier les risques occasionnées par la perte/le vol de données auprès des personnes concernées (clients, employés, membres).

De manière plus générale, cette cellule va devoir aussi identifier les impacts de l’attaque sur le fonctionnement de la compagnie, et proposer des solutions afin de réduire l’importance de ces impacts, avec pour objectif final de les faire disparaître.

La cellule de crise est donc un élément capital du traitement de la menace, car le fonctionnement classique de l’entreprise est modifié en cas d’attaque, et suit des procédures établies au préalable, mais aussi des nouvelles créées par la cellule de crise. Ces procédures vont englober les divers aspects dépendants de la cellule de crise mentionnés plus tôt. Les actions et procédures mises en place par cette cellule de crise devront prendre en compte le type général de la menace, comme mentionné dans la partie d’identification, mais aussi son type plus précis (dans le cas d’un malware, s’il s’agit d’un ransomware, par exemple), car en fonction du type de menace, les actions de la cellule de crise pourront changer du tout au tout.

La cellule de crise étant en charge de toutes les décisions, elle doit prendre en compte l’ensemble des acteurs et des éléments qui seront sollicités, et c’est pour cela qu’elle se découpe en plusieurs sous-cellule de crise, chacune ayant sa spécificité, comme mentionné dans la partie “Cellule de Crise” évoquée dans “Le Traitement de la menace avant la réalisation”.

Figure 4.7 – Schéma explicatif de la prise de décision d’une cellule de crise

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 61

4.4.4 Logs

Surveiller les logs et les récupérer est important pour comprendre une attaque et y réagir au mieux. Il faut pouvoir avoir accès à certaines informations pour comprendre la suite d’évènement se déroulant :

— Date et horodatage de l’action ou événement considéré comme première ob servation de la menace

— Nom de la personne ayant remarqué la menace ou de la personne ayant effectué la première action

— Description de l’événement

Ces informations permettront de décider des différentes actions à entreprendre durant la cellule de crise. Un suivi précis des logs sera utile à maintenir durant l’ensemble de la menace, afin de savoir quelles actions ont entraînées quelles consé quences, et permettra de constituer un dossier de dépôt de plainte. Cela permet aussi de reconnaître le type de menace auquel la compagnie est exposée, et par conséquent savoir quelle stratégie adopter par rapport aux mesures mises en place.

L’ensemble des logs en lien avec la menace qui seront récupérés devront être gardés précieusement. En effet, ces logs seront utiles pour effectuer une identification plus poussée de la menace, mais aussi pour monter le dossier nécessaire au dépôt de la plainte et au dossier de signalisation de la compromission des données du SI.

4.4.5 Déconnexion

Une fois la cellule de crise en place, il est nécessaire, en s’appuyant sur l’analyse des logs, de traiter la menace de manière plus directe, et pour cela, il faut la confiner. Cela peut prendre plusieurs aspects en fonction de la menace, mais ,comme précisé précédemment dans ce rapport, nous allons nous concentrer sur les menaces de type malware, et plus précisément les ransomwares. Dans le cas de ces virus, il est important d’empêcher la propagation, et pour cela, il est impératif de déconnecter les machines infectés du réseau local. Toutefois, cela ne passe qu’au second plan. En effet, le BackUp étant le conteneur de l’ensemble de notre système sain, il faut le préserver à tout prix, et pour cela, le déconnecter est nécessaire. Si le BackUp est touché, il peut subir le même sort que n’importe quel machine infectée, c’est à dire que les données sur celui ci peuvent se retrouver volées, supprimées ou détériorées. Pour éviter cela, il est fortement conseillé de posséder plusieurs BackUps, afin de pouvoir avoir toujours un BackUp non infecté pour la phase de réinstallation du système.

Une fois les BackUps déconnectés, il est temps de repérer et déconnecter l’en semble des machines infectées. Cette action sera à effectuer en permanence, tant que l’attaque sera considérée en cours, car ne le faire qu’une fois, c’est risquer de passer à coté d’une machine infecté, ce qui rendrait donc l’entièreté de l’action in utile. De plus, il est pertinent de vérifier que les éléments reconnus comme infectés ne possèdent pas de connexion sans fil, et si ils en possèdent, de les désactiver (une fois de plus dans un esprit de confinement de la menace).

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 62

L’une des autres déconnexion importante est celle du système d’information à internet. En effet, cette connexion internet présente de nombreux désavantages en cas d’attaque :

— L’attaquant peut communiquer à son malware des consignes à distance, et lui permettre d’être plus imprévisible, ou dans le cas d’un ransomware, changer de méthode d’encryption des données.

— Le virus peut communiquer à l’attaquant, ce qui entraîne un problème majeur depuis quelques années dans le cas du ransomware, via l’arrivée des ransom wares à double extorsion 5 dont le but est de crypter les données de la victime après les avoir exporté vers l’attaquant, dans le but d’obtenir une rançon via la menace de publication des données.

— L’accès à internet a aussi le défaut de laisser le système ouvert à d’autres attaques, et lorsque le SI est ciblé par une attaque de grande envergure, la dernière chose souhaitée est de se faire attaquer par d’autres moyens au même moment.

Bien que nécessaires à la bonne survie du réseau, ces actions vont entraîner un certain ralentissement de l’activité du SI, et il est du ressort de la cellule de crise de prendre les décisions adéquates en terme de temporalité et d’actions afin de restreindre la menace tout en continuant l’activité.

4.4.6 Communication

L’une des tâches importantes de la cellule de crise, qui va être dirigé principa lement par la sous-cellule décisionnelle, est la création et la gestion des plans de communications internes et externes durant le traitement de la menace. Ces deux aspects de la communication sont importants, car ce sont eux qui vont permettre une bonne conclusion au traitement de la menace (sauver ses données et son SI mais perdre sa réputation et ses clients n’est le but d’aucune entreprise). Ces plans ont pour but de s’assurer une cohésion quand à la position de l’entreprise par rap port aux autres acteurs, tout en s’assurant que les communications internes soient maintenues et fluides, mais en restant sécurisées sachant qu’il y a une infiltration sur le réseau.

Communication interne

La communication dite interne est la communication qui se déroule à l’intérieur de l’entreprise, entre les services et les personnes. Cette communication est impor tante car c’est elle qui va permettre la communication du protocole à mettre en place pour traiter la menace. par conséquent, s’il y a un manque de sécurité au niveau de ce canal de communication, cela laisse la porte ouverte pour l’attaquant, lui permettant de connaître les plans de l’entreprise pour réagir à son attaque, et lui permettre d’agir en conséquence.

5. https://www.darktrace.com/en/blog/double-extortion-ransomware/

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 63

Il est aussi bénéfique de rappeler aux employés que ceux-ci ont signé une clause de confidentialité lorsqu’ils ont été embauchés (et si ce n’est pas le cas, il est vital de la rajouter. Cette clause régi ce que les employés ont le droit de divulguer dans certaines situations, et dans le cas d’une attaque, ils ne doivent rien divulguer, ce qui nous amène au plan de communication externe.

Communication externe

La communication externe est la communication depuis l’intérieur de l’entreprise vers toute autre source extérieur, que ce soit les actionnaires, les média ou les clients. Dans le cas d’une attaque, il est bien évidemment nécessaire de prévenir le client et les actionnaires, ceux-ci pouvant être impactés par l’attaque que l’entreprise est en train de subir. Mais il est aussi vital de prévoir une réponse dans le cas ou une information quand à cette attaque viendrait à fuiter, nécessitant la communication avec les médias.

Comme mentionné plus tôt, la clause de confidentialité est plus qu’importante, surtout dans le cas d’un ransomware. En effet, ces virus laissent des traces indiquant que la machine a été infectée, tel que :

— Une note de rançon qui s’affiche sur l’écran

— Un compte à rebours

Le problème est que cela peut impacter la machine de n’importe quel employé, et que si ce dernier n’a pas été assez entraîné et sensibilisé, ou que le rappel de la clause de confidentialité n’a pas été fait, il pourrait se permettre de divulguer l’information de l’attaque sur les réseaux, ce qui alerterait énormément de monde, et en fonction de la compagnie, causer des dégâts de réputation énorme.

Il faut donc, en plus du rappel de la clause, prévenir les employés de ne pas commu niquer vers l’extérieur, à qui que ce soit, mais aussi les prévenir qu’en cas de contact avec une entité externe (média ou autre), ils doivent rediriger la requête vers le ser vice de communication, si l’entreprise en possède un, ou vers leur responsable.

Ces actions peuvent sembler non nécessaires ou non vitales au premier abord pour certains, mais elles sont d’une importance majeur, car le but est de remettre en place le SI comme avant l’attaque, certes, mais surtout sans ternir la réputation de l’entreprise auprès des clients et des actionnaires, et sans que la compagnie perde en valeur.

Un autre point important dans le cas français, s’il y a eu violation de données, il est nécessaire d’en informer la CNIL 6, c’est une obligation légale, définie dans l’article 33 7 du règlement européen de protection des données 8.

6. https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles 7. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4 8. https://www.cnil.fr/fr/reglement-europeen-protection-donnees

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 64

4.4.7 Précaution

Bien que les communications et les déconnexions aient été gérées, il reste le traitement des éléments du SI à effectuer. En premier lieu, il va falloir gérer les appareils qui étaient allumés. S’ensuit les appareils qui étaient éteints, puis les éléments de stockage externe qu’il faut traiter avec un soin tout particulier.

Les premiers éléments, qui sont ceux infectés, ont la particularité de ne pas être un nombre précis, car une nouvelle machine peut se faire infecter à tout moment. Pour éviter cette propagation, et éviter aussi la perte des données sur chaque ma chine, il est nécessaire, lorsqu’une machine a été identifiée comme infecté, de ne surtout pas l’éteindre, ce qui pourrait être le premier réflexe de bon nombre de personnes. Le problème principal avec l’extinction de la machine, malgré le ralen tissement de la propagation du virus qui en découle en lui enlevant une possibilité d’infection, est la perte des traces laissées par le virus, traces qui permettraient de l’identifier plus précisément ou d’avoir des information sur l’attaquant. De plus, pour monter le dossier final pour la police, il est nécessaire d’avoir le plus d’informa tions possibles. De ce fait, il est fortement conseillé de mettre la machine en veille et non de l’éteindre.

La deuxième précaution concerne les machines qui étaient éteintes lors de l’at taque. Celles ci étant éteintes, elles ne sont pas des vecteurs possibles d’attaques, et doivent donc rester ainsi afin de neutraliser la menace. Le plan de communication interne prend ici une autre importance, car il va permettre de notifier les employés non présents lors de l’attaque qu’ils ne doivent pas démarrer leurs machines si celles-ci étaient éteintes lors de l’attaque.

La troisième précaution est liée aux dispositifs de stockage externe de données (disque dur, clé usb, disquette ou autre), qui ont l’avantage d’être portatif, mais le désavantage d’être portatif. En effet, si l’un de ces supports se retrouve infecté, et que le propriétaire dudit support décide de le brancher chez lui, alors sa ma chine personnelle sera infectée et pourra contaminer d’autres machines. Ce n’est toutefois pas le seul problème, car cette clé reste contaminée, donc si l’employé re vient au travail et utilise sa clé, il re-contaminera le SI, augmentant la charge de travail nécessaire pour remettre en place le système. Il faut donc une fois de plus communiquer en interne afin d’expliquer aux employés qu’il ne faut pas utiliser ces dispositifs pendant une certaine période de temps, mais aussi installer un contrôle de ces dispositifs à la sortie des locaux, pour vérifier qu’aucun employé ne sorte avec le virus présent sur lui.

4.4.8 Identification avancée

Une fois ces différentes étapes réalisées, il va être utile de procéder à une nouvelle identification, mais cette fois bien plus poussée. Le but de cette identification va être d’identifier clairement la menace, et de pouvoir commencer à travailler à sa résolution.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 65

Pour ceci, un certain nombre d’informations vont être nécessaires : — L’URL utilisé par le virus pour communiquer avec les attaquants — Le nom du fichier contenant le virus

— La structure du virus

— L’adresse IP de provenance

D’autres informations, plus spécifiques en fonction du type de l’attaque (dont l’identification à été faite précédemment), peuvent s’avérer nécessaire.. Dans le cas du ransomware, il est utile de récupérer les informations suivantes : — La méthode d’encryption utilisée par le virus

— Le mail de phishing possiblement utiliser pour transmettre le virus

Tout ces éléments vont servir à identifier le virus, voir à mettre un nom sur le virus, si celui ci a déjà été utilisé, mais aussi permettre de mettre à jour les politiques de sécurité. En effet, si l’adresse IP est récupérée lors de l’action, il est possible de mettre à jour les firewalls afin que ceux-ci bloquent cette adresse, pour empêcher toute communication entrante et sortante vers celle-ci. L’acquisition de cette adresse IP et la mise à jour de la politique de sécurité ne va toutefois pas garantir la sécurité totale du SI, mais cela va tout de même l’augmenter .

4.4.9 Informations

Quelques informations s’avèrent utiles pour traiter les menaces. Les premières informations traiteront des ransomwares, les secondes des aides possibles pour trai ter la menace, et les dernières traitent des raisons pour lesquelles payer la rançon lors d’un ransomware est une mauvaise idée.

Comme explicité plutôt, l’information traitée maintenant concerne les ransom wares, et plus précisément, un site internet d’aide au traitement des ransomwares. Ce site internet s’appelle NoMoreRansom.org 9. Ce site est un projet initialisé par Europol, la National High Tech Crime Unit de la police allemande, ainsi que McAfee, et il permet de trouver des informations de décryptement de bon nombre de ransomware existant, dont certains assez récents (REvil/Sodinokibi 10, RAGNA ROK 11, Darkside 12), et possiblement encore en activité. Cela renforce l’utilité de l’identification avancée, car si le ransomware identifié est renseigné sur le site No MoreRansom.org, alors plusieurs solutions seront disponibles pour s’en débaras ser.

La deuxième information concerne les personnes à contacter en cas d’attaque. Pour les grosses entreprises, la cellule de crise est en charge et est donc l’entité à contacter pour gérer l’attaque. Mais dans le cas des PME, ou d’auto-entrepreneurs, lorsque ceux-ci sont victimes d’une attaque quelconque, ils ne disposent pas de service de cybersécurité, ou de cellule de crise. De ce fait, ces petites entreprises sont d’autant plus vulnérables aux cyber attaques, et doivent donc reposer sur des

9. https://www.nomoreransom.org/fr/index.html

10. https://www.nomoreransom.org/fr/decryption-tools.html#REvilSodinokibi 11. https://www.nomoreransom.org/fr/decryption-tools.html#RAGNAROK 12. https://www.nomoreransom.org/fr/decryption-tools.html#Darkside

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 66

moyens extérieurs. Certaines entreprises auront anticiper la chose, et souscrit à des assurances, ou délégué la gestion de leur SI à des entreprises extérieur, et dans ce cas, ce sont ces dernières qui géreront le traitement.

Toutefois, certaines entreprises n’auront pas penser à cela, et se retrouveront ciblée par une attaque, sans aucun moyen de défense. Dans ce cas, le gouvernement français à mis en place une plateforme en ligne, cybermalveillance.gouv.fr 13, qui permet de trouver les spécialistes et les compagnies de service locales spécialisées dans ce type d’intervention.

Le dernier point de cette partie informative concerne une fois de plus les ran somwares, mais se focalise sur pourquoi il ne faut pas payer la rançon. Parmi les raisons mentionnées par les experts, on peut trouver :

— Augmentation des fonds pour les attaquants

Via la somme reçu par le paiement de la rançon, les attaquants peuvent aug menter leurs possibilités d’attaque, augmenter leur nombre d’adeptes, avoir une force de frappe plus élevée, et l’ensemble de ces conséquences ne fera que renforcer les prochaines attaques possibles du groupe attaquant, dont l’entre prise peut-être victime à nouveau.

— Aucune garantie de recevoir la clé de désencryption Même si la rançon est payée, il n’y a aucune garantie que les attaquants four nissent la clé de désencryption des données, ou qu’ils ne rendent les données acquises. Il est en effet possible de douter qu’ils ne la fournissent pas, étant donné que cela finirait par être connu, et le groupe ne serait plus crédible, incitant leurs autres victimes à ne pas payer la rançon, mais cela ne constitue en rien une garantie.

— Aucune garantie de pouvoir récupérer ses données

Étant donné que l’encryption des fichiers se fait lorsque les services sont en ligne, il y a de grandes chances que certains fichiers ou les bases de données soient édités par des applications ou des personnes au moment de l’encryption, ce qui résulterait en des fichiers corrompus, et donc des pertes de données.

— Aucune garantie de ne plus se faire attaquer

Même si la rançon est payée, que l’on reçoit la clé de désencryption et qu’aucun fichier n’est corrompu, il n’y a aucune garantie que l’entreprise sera à l’abri de futures attaques, car se faire attaquer une fois par un ransomware et payer une rançon ne permet pas de bénéficier d’une immunité face à ce groupe. De plus, les attaquants peuvent connaître d’autres groupes, ou divulguer sur leur blog que l’entreprise a cédé, et qu’elle a payé la rançon, faisant de l’entreprise une poule aux oeufs d’or pour les attaquants, car ceux-ci sauront qu’opérer une attaque sur l’entreprise peut amener à une rançon payée, la ou une autre entreprise serait peut-être plus encline à ne pas payer, ou mieux renseigner.

Ces raisons font partie des principales mentionées par les experts sur pourquoi il ne faut pas payer la rançon.

Nous avons maintenant vu les différentes étapes majeures à suivre pour traiter une menace, du moment de sa reconnaissance, jusqu’au moment ou celle-ci est confinée.

13. https://www.cybermalveillance.gouv.fr/

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 67 4.5 Le traitement de la menace après la réalisation

4.5.1 Introduction

Une fois l’attaque confinée, et que l’on a une certaine assurance que celle-ci ne puisse plus se propager, ou plus se propager de manière non contrôlée, il est possible de commencer à opérer les étapes importantes pour remettre le SI sur pied.

Figure 4.8 – Exemple des étapes à suivre après la menace

Comme montré ici, il n’y a pas beaucoup d’étapes à effectuer après l’attaque, mais nous allons voir que cela est en fait faux, car il est important de toujours se considérer en amont d’une attaque.

4.5.2 Consignes générales

La première étape concerne les démarches à effectuer pour remettre en place le SI. Celles-ci ne sont que générales, et dépendront de chaque SI, mais serviront de guide sur certaines actions qui sont nécessaires. Pour remettre en place le système, il va falloir utiliser le BackUp sain ou les BackUps sains que l’on a déconnecté en début d’attaque, et en prenant des moments de sauvegarde antérieur au début de l’attaque, afin de redémarrer un système sain.

Il faut séparer deux cas, le cas des machines infectées, et celui des machines saines :

Machines infectées

Pour traiter les machines infectées, deux étapes sont nécessaires : — Vérifier que le virus identifié ne laisse pas de traces lors d’une réinstallation du système, afin d’assurer que le système soit sain après une réinstallation. — Réinstaller sur un support connu, c’est à dire dont le BackUp est sain. Une fois ces machines traitées, elles sont à nouveau considérées comme des ma chines saines.

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 68

Machines saines

Une fois qu’une machine est déclarée saine, elle va pouvoir recevoir le traitement suivant :

— Correction de la faille de sécurité utilisée pour l’attaque, via des mises à jour de logiciels, de nouvelles règles de firewall ou toute autre action qui permet d’empêcher la faille d’être à nouveau exploitée.

— Changer les mots de passe de tous les éléments du SI, car il n’y a aucun moyen de vérifier que l’attaquant n’a pas volé ces données, ce qui compromettrait la sécurité de l’ensemble du système.

Une fois les machines infectées et saines traitées, il convient de réeffectuer les étapes vues dans la partie "Traitement de la menace avant réalisation". Ces étapes finies, le SI sera à nouveau suffisamment sécurisé pour pouvoir être utilisé de manière fonctionnelle, et la dernière partie propre à la menace correspondra au dépôt de plainte à la police.

4.5.3 Le dossier pour la police

La dernière partie à effectuer lors du traitement d’une menace est de monter le dossier de plainte pour la police, à la BEFTI 14, le SCRC 15, la SDLC 16 ou le C3N 17, qui sont en charge du traitement de ces dossiers. Toutefois, pour effectuer leur investigation, ils ont besoin du maximum d’informations possibles, ce qui justifie la nécessité d’avoir un journal de suivi des actions entreprises par tous les acteurs lors du traitement de la menace. Cela se traduit par :

— La timeline de l’attaque, qui va permettre de garder toutes les informations ainsi que le laps de temps écoulé entre chaque actions.

— La localisation de tous les éléments infectés

— Les logs correspondants à l’attaque

— L’analyse technique de l’attaque

— Les fichiers cryptés par le ransomware

— Garder un élément infecté

— Adresse de cryptomonnaie et mail de rançon

— Texte de note sur la rançon

— Les informations de contact de l’ensemble des personnes impliquées dans la résolution de la menace

14. http://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/ Les-actions-PP/Les-brigades-de-police-judiciaire/La-BEFTI

15. https://www.gendarmerie.interieur.gouv.fr/pjgn/scrcgn

16. https://www.police-nationale.interieur.gouv.fr/Organisation/ Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/ Sous-direction-de-lutte-contre-la-cybercriminalite

17. https://c3n-cn.fr/

*CHAPITRE 4. TRAITEMENT D’UNE MENACE* 69

Ces informations sont nécessaires et ne dépendent pas d’une menace en parti culier, mais en cas de rançon payé, d’autres informations s’avèrent nécessaires : — Références du ou des transferts d’argent effectués

— Référence de la ou des personnes contactées :

— Adresse de messagerie ou adresse postale

— Pseudos utilisés

— Numéro de téléphone

— Fax

— Copie des courriels ou courriers échangés

Ces informations sont nécessaires et leur récupération doit donc être planifiée, pour être sur que rien ne manque, permettant d’assurer le meilleur traitement de la part des autorités compétentes.

— Les informations bancaires :

— Numéro complet de la carte bancaire utilisée

— Référence de la banque et du compte utilisé

— Copie du relevé de compte bancaire où la transaction est effectuée — Toutes les informations présentées plus tôt qui peuvent s’avérer utile pour la reconnaissance de l’attaquant

Une fois les informations récoltées et le dossier monté, il suffit d’attendre que la police fasse son travail, et le but de l’entreprise sera de se concentrer sur la sécurisation son SI.

4.6 Conclusion

Pour conclure sur le traitement de la menace, et comme il a été mentionné en amont, le SI est vulnérable aux menaces à partir du moment ou il est créer. De ce fait, le SI se trouve toujours dans la phase de traitement avant le menace, et ce, même lors du traitement d’une autre menace. Il est donc nécessaire, après une attaque, de se préparer à celles qui suivront. Pour ce faire, il est nécessaire de tester et améliorer son système de sécurité en continu.

Chapitre 5

Évolution des menaces

5.1 Introduction

Le domaine de la sécurité des systèmes d’information est un secteur en perpétuel changement. En effet, la démocratisation des équipements informatiques, l’informa tisation des systèmes de traitement de données, la mondialisation du commerce et des échanges, les innovations dans les domaines informatiques et la connexion perpétuelle des machines offrent à la fois son lot de bonnes et de mauvaises choses.

Bien évidemment, l’informatisation et l’automatisation touche en particulier les entreprises, si bien que tous les domaines sont impactés. Il est dur de s’imaginer vivre une journée sans toucher à un système informatisé : nos téléphones, nos ordinateurs, nos véhicules, l’électroménager, les distributeurs de banque, etc. . . Ainsi, la plupart des entreprises dépendent en grande partie de la qualité et de la disponibilité de leurs données et de leurs systèmes de traitement.

La protection de ses données et de ses systèmes devient alors un pivot central de la capacité de production des entreprises. Aussi faut-il, avant de déployer des défenses, réfléchir aux menaces susceptibles de peser sur vos infrastructures. Dans cette partie, nous aborderons, en premier lieu, les individus susceptibles d’attaquer vos systèmes, allant de simples individus à des groupes supportés par de puissantes institutions.

Puis, dans un second temps, nous aborderons les types d’attaques fréquentes, dangereuses, et innovantes, qui nous semblent pertinentes à aborder, car soit d’ac tualité et susceptible de vous toucher, soit innovantes et potentiellement dangereuses à l’avenir. Nous toucherons également quelques mots afin d’expliquer brièvement comment prévenir ces menaces.

70

*CHAPITRE 5. ÉVOLUTION DES MENACES* 71 5.2 Les acteurs intéressés

L’image du hacker est restée et reste encore de nos jours dans l’esprit de la plu part comme une personne isolée, capable à lui tout seul de pénétrer dans n’importe quelle système informatique avec une grande aisance. Voilà le stéréotype du hacker, cependant cette image reflète une période du passé remontant au débuts des sys tèmes informatiques et de l’arrivée d’internet. La réalité est que lors de l’arrivée de nouveaux systèmes d’information, la sécurité de ces nouveaux systèmes dépassent la compréhension de nombreux professionnels laissant le champ libre aux pirates malveillants pour attaquer. Depuis plusieurs années, une prise de conscience à eu lieu et l’apparition de systèmes de plus en plus complexes et sécurisés ont fait leur apparition. La plupart des hackers solitaires ont disparu et ne sont plus capables d’infliger de dégâts considérables à eux seuls.

Malgré cette avancée technologique dans la sécurité des systèmes d’information et ce sentiment de sécurité qui en à découlé, les pirates informatiques continuent d’évoluer et trouvent de nouvelle méthode d’attaque et menacent toujours les sys tèmes des entreprises en travaillant en équipe.

5.2.1 Individus isolés

Un black hat 1est, en argot informatique, un hacker mal intentionné. Ils ont une nette préférence pour les actions illégales. Ils utilisent leur savoir pour découvrir des choses qui leur sont cachées. Ce sont des criminels qui s’introduisent dans les réseaux informatiques avec une intention malveillante. Ils peuvent également diffuser des logiciels malveillants qui détruisent des fichiers, prennent en otage des ordinateurs ou volent des mots de passe, des numéros de carte de crédit et d’autres informations personnelles. Cela va de la création de virus, aux chevaux de Troie en passant par les vers et les logiciels espions.

Le problème de piratage Black Hat est mondial , ce qui le rend extrêmement difficile à arrêter. Peu importe le nombre arrêté de nouveau black feront leurs appa ritions. Les blacks hat sont nombreux, ceux qui rendent leurs méthodes d’attaques et leur motivation personnelle tout aussi nombreuses, on peut tout de même distin guer différents types de black hat suivant leur méthode ou leur motivation.

Script kiddies 2:

Surnommés crashers, lamers ou encore packet monkeys, sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite du fait qu’ils ne comprennent pas ces programmes, afin de vandaliser des systèmes informatiques pour s’amuser. Les scripts kiddies s’attaquent généralement aux sites web mal protégés. Ils exploitent des failles de sécurité connues ou utilisent des logiciels malveillants et des outils d’attaque automatisés tels qu’AutoSploit ou le programme LOIC. Les scripts kiddies peuvent aussi être à l’origine de menaces telles que des attaques par déni de service ou des forçages de mot de passe par force brute. La plupart des black hat commence en tant que script kiddies.

1. https://www.kaspersky.com/resource-center/threats/black-hat-hacker 2. https://fr.wikipedia.org/wiki/Script\_kiddie

*CHAPITRE 5. ÉVOLUTION DES MENACES* 72

Phreakers 3:

Il s’agit de pirates s’intéressant au réseau téléphonique commuté (RTC) Il est difficile de repérer l’intrusion d’un phreaker avant de recevoir une facture de téléphone bien salée. Le fait est que ce sont les entreprises qui sont majoritairement visées par les phreakers.

Une pratique couramment répandue consiste en l’appel de numéros surtaxés. L’entreprise paye ainsi pour les nombreux appels effectués par le pirate. Ce der nier récupère des codes audiotels qu’il peut facilement revendre contre des sommes pécuniaires, importantes selon le volume d’appels effectués.

Le but principal des actes de phreaking est généralement de bloquer des sys tèmes, de détruire des données, d’écouter des conversations ou encore de détourner des lignes, pour réaliser des appels à l’international ou monétiser les appels. Les smartphones se développant, les attaques sont devenues plus dangereuses.

Les PME sont souvent les cibles de ces attaques du fait de l’absence d’un service interne capable de gérer la sécurité de l’entreprise. Les meilleurs moyen pour se protéger de ces attaques sont :

— Orienter sa politique de sécurité sur le réseau téléphonique.

— Installer un firewall et instaurer des règles pour les appels à l’étranger. — Sensibiliser les employés aux attaques type phishing.

Carders 4:

Ils s’attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires). Les informations contenues sur Amazon, Paypal, Netflix, Delive roo. . . sont considérées comme des informations précieuses qui peuvent être utilisées à des fins de blanchiment d’argent. Dès qu’un pirate informatique rencontre ces données, il tente de les utiliser pour des achats illégaux ou d’utiliser des forums de cartes, des sites web malveillants et d’autres points de distribution pour vendre ces informations. Afin de retirer de l’argent à l’insu de la victime, ces criminels effec tuent des virements bancaires ou utilisent d’autres méthodes qui peuvent les aider à obtenir les marchandises sans payer. En général, les personnes qui se trouvent derrière ces activités essaient d’obtenir le plus d’informations possible.

Il existe différentes façons de le faire. À l’origine, il s’agissait d’une carte de crédit volée qui pouvait être utilisée pour faire des achats illégaux jusqu’à ce qu’elle soit annulée. Cependant, la principale méthode actuellement utilisée pour voler des informations sur les cartes de crédit, des informations financières et d’autres données sensibles est directement liée aux logiciels malveillants.

Ce n’est pas la seule méthode utilisée par les groupes de carding. Elles peuvent également voler les informations personnelles d’une victime en utilisant le phishing. Cette méthode de fraude est basée sur de faux sites web se faisant passer pour des institutions légitimes telles que des banques, des universités, des hôtels, des boutiques en ligne et bien d’autres. Le spam et les faux e-mails sont également

3. https://www.monpetitforfait.com/toutes-les-aides/phreaking-piratage-mobile, https://lentreprise.lexpress.fr/high-tech-innovation/fraude-telephonique-comment-se-proteger\_ 1518911.html

4. https://www.oracle.com/fr/security/qu-est-ce-que-carding.html

*CHAPITRE 5. ÉVOLUTION DES MENACES* 73

largement utilisés pour inciter les utilisateurs à révéler des informations personnelles et bancaires, y compris des informations de connexion et des mots de passe.

Pour se prémunir contre ces activités extrêmement dangereuses, les utilisateurs devraient commencer à adopter des habitudes de navigation sûres. Pour protéger vos informations personnelles :

— Utiliser des programmes anti-spyware fiables et de bonne réputation.

— Se tenir à l’écart des sites web illégaux, éviter les redirections de navigateur et les fenêtres publicitaires trompeuses.

— Ignorer les spams ou les courriels provenant d’inconnus.

Vos informations personnelles sont trop importantes pour être divulguées à des tiers malhonnêtes.

Crackers 5:

Ce sont des personnes dont le but est de créer des outils logiciels permettant d’at taquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Leurs motivations sont majoritairement de passer un challenge ou d’éviter de payer pour des services.

5.2.2 Groupes indépendants

Lorsque les individus n’agissent pas de manière isolée, ils peuvent être membres de groupes indépendants. Ces groupes peuvent avoir des objectifs divers et variés, certains chercheront le profit, d’autres à simplement prouver leur compétence, ou agiront à des fins idéologiques et/ou politiques, ces groupes en particulier sont surnommés les “Hacktiviste”.

Les ransomwares de DarkSide 6:

C’est un groupe cybercriminel détecté formellement en 2020 par des entreprises américaines spécialisées dans la cybersécurité. Il est vraisemblablement basé en Russie et cible des victimes ayant des moyens financiers importants, afin d’obtenir de grosses rançons. Selon l’ANSI il s’agit de l’un des groupes cybercriminels disposant des ressources financières et des compétences techniques les plus importants.

Pour mener ses attaques, DarkSide emploie de manière récurrente des ransom wares, et demande une rançon pour la restitution des données (celles-ci oscillent entre 165 000 et 1,65 million d’euros). Il a notamment attaqué Toshiba TFIS, mais il est surtout connu pour la cyberattaque de Colonial Pipeline, un oléoduc améri cain, en mai 2021, qui a poussé le président américain Joe Biden à déclarer l’état d’urgence : c’est à ce jour la plus grande cyberattaque contre une infrastructure pétrolière américaine.

On peut ensuite évoquer les groupes qui agissent à des fins idéologiques et/ou politiques : on les surnomme les groupes “Hacktiviste”. Ce mot est la contraction des mots “ Hack” et “activiste” : on pourrait définir cela comme étant une forme d’activisme numérique qui utilise comme moyen d’action le hacking. Ils peuvent agir

5. https://portail-informatique-et-securite-du-web.over-blog.com/2015/11/ divers-c-est-quoi-un-hacker-et-les-specialites.html

6. https://www.usinenouvelle.com/article/ce-que-l-on-sait-de-darkside-le-groupe-de-cybercriminN1093339

*CHAPITRE 5. ÉVOLUTION DES MENACES* 74

en tant que “lanceur d’alertes” en dérobant notamment des documents confidentiels afin de les rendre publics. Ils pratiquent aussi ce que l’on appelle le Défacement, c’est-à-dire le remplacement du contenu d’un site par un autre contenu, pour y afficher des messages idéologiques.

Il existe une large palette d’Hacktivisme que l’on pourrait découper en différentes catégories :

— L’Hacktivisme “issu de la culture hacker”

Les groupes que l’on classe dans cette catégorie défendent généralement l’idée qu’internet est un espace libre pour tout le monde et que la liberté d’expression doit être garantie à tous. C’est probablement la forme d’Hacktivisme la plus connue du grand public.

L’exemple d’Anonymous 7:

C’est certainement l’un des groupes les plus célèbres du début des années 2010, mais il existe en réalité depuis 2003. Il est notamment connu pour avoir mené des attaques contre des gouvernements arabe entre 2010 et 2011, en soutien au printemps arabe, un ensemble de contestations au moyen orient qui ont provoqué la chute de certains dirigeants ainsi que des guerres civiles. Il a également mené des attaques contre des sites gouvernementaux américains en 2011 pour protester contre les lois SOPA (Stop Online Piracy Act) et PIPA (PROTECT IP Act) concernant les droits d’auteur. Dans la continuité de ces lois, le site Megaupload est fermé par les autorités américaines, en guise de représailles, le groupe attaque de nouveaux des sites gouvernementaux américains, mais aussi le site de l’Elysée et de l’Express en France : le site de ce dernier est attaqué car son rédacteur en chef de l’époque (Christophe Barbier) a publiquement critiqué le groupe et ses actions.

— L’Hacktivisme géopolitique

Les entités qui pratiquent ce genre d’Hacktivisme vont généralement soutenir les intérêts d’états ou de pouvoirs politiques.

L’exemple de l’armée électronique syrienne 8:

C’est une organisation qui a vu le jour au cours de la guerre syrienne en 2011 : elle agit pour soutenir le maintien au pouvoir de Bachar el-Assad. Elle a ciblé principalement des médias, agences de presse et organisations de défense des droits de l’homme qui ont traité de la situation en Syrie : ainsi la BBC, l’AFP ou Human Rights Watch ont été victimes d’attaques DDOS et l’agence américaine Associated Press s’est vu voler son compte Twitter qui a par la suite été utilisé pour diffuser des fausses informations.

— L’Hacktivisme de censure

Cette forme d’Hacktivisme consiste en la censure (suppression) du contenu d’un site que l’individu a jugé comme ne lui convenant pas.

L’exemple d’Antileaks 9:

C’est un groupe qui n’apprécie guère les informations que Julian Assange et Wikileaks divulguent, par conséquent, celui-ci a mené des attaques pour supprimer ce contenu.

7. https://www.lebigdata.fr/anonymous-hebergeur-dark-web

8. https://www.huffingtonpost.fr/thierry-berthier/tactique-armee-syrienne-electronique\_ b\_6661188.html

9. https://www.rt.com/news/ddos-attack-rt-antileaks-178/

*CHAPITRE 5. ÉVOLUTION DES MENACES* 75

— L’Hacktivisme religieux

Enfin, il existe des groupes qui cherchent à promouvoir leur religion et atta quer les personnes critiquant celle-ci.

L’exemple d’Izz ad-Din al Qassam Cyber Fighters 10 :

Ce groupe d’hacktivistes djihadistes, pratique ce que l’on peut appeler le cy berdjihadisme, c’est-à-dire le jihad sous une forme virtuelle. Il a mené une action normée “Operation Ababil” en 2012, qui a consisté à viser des banques américaines avec 135 attaques, en 47 vagues, pour protester contre la diffu sion d’une vidéo, qu’ils ont considérés comme étant anti islam, par le pasteur américain Terry Jones.

Enfin, on pourrait distinguer une dernière catégorie de groupe, celle pratiquant le cyberterrorisme. Il n’y a pas vraiment de définition unanime du terme cyberter rorisme.

Pour certains, ce terme désigne l’activité de perturbation des systèmes d’infor mations réalisée dans le but de créer la panique, par des organisations terroristes connues. Mais pour d’autres, cette définition est limitée car ne couvrant pas toutes les formes de cyberterrorisme. Selon une définition plus large, créée par Kevin G. Coleman, on peut définir le cyberterrorisme comme étant « l’utilisation préméditée des activités perturbatrices, ou la menace de celle-ci, contre des ordinateurs et / ou réseaux, dans l’intention de causer un préjudice de nature sociale, idéologique, religieuse, politique, ou autres objectifs. Ou pour intimider toute personne dans la poursuite de tels objectifs ».

Il n’existe pas d’attaque massive formellement revendiquée par un groupe terro riste. Le 8 avril 2015, le média français Tv5Monde est victime d’une cyberattaque massive. La diffusion des programmes de la chaîne de télévision est interrompue, ses comptes sur les réseaux sociaux sont dérobés et affichent des messages de soutien à l’État islamique. Le groupe “Cybercaliphate” se réclamant de l’État islamqiue revendique l’attaque, à la survenue de celle-ci, les autorités françaises privilégient la piste terroriste. Mais après une enquête plus approfondie, l’auteur de cette at taque serait en réalité une groupe APT Russe, plus précisément le groupe nommé PawnStorm.

Même si à l’heure actuelle le menace ne s’est pas manifestée, elle est très plau sible dans le futur selon l’ANSI, pour certains experts, l’espace numérique pourrait devenir à l’avenir un nouveau terrain d’attaque pour les groupes terroristes.

10. https://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint. html

*CHAPITRE 5. ÉVOLUTION DES MENACES* 76 5.3 Les APT

5.3.1 Définitions

Le terme APT 11 pour “Advanced Persistent Threat”, ou “Menace Persistante Avancée” en français, désigne un type de piratage sophistiqué et persistant :

— Sophistiqué :

Dans le sens où celui-ci est généralement d’un niveau technique avancé, cible des entités conséquentes en employant un ensemble large de techniques et outils.

— Persistant :

Car celui-ci perdure sur une longue période sans être détecté, laissant le temps d’extraire un nombre très important de données dans les systèmes visés.

Une APT cible généralement une organisation pour des motifs d’affaires ou un État pour des motifs politiques. Elle exige un degré élevé de dissimulation sur une longue période de temps. Le but d’une telle attaque est de placer du code malveillant personnalisé sur un ou plusieurs ordinateurs pour effectuer des tâches spécifiques et rester inaperçu pendant la plus longue période possible.

Comme les APT nécessitent des ressources importantes, il est communément admis par les experts que ce type d’attaque relève d’états ou de groupes soute nus par des États, même si pour certains, la démocratisation de ces pratiques a probablement permis l’émergence de groupes APT indépendants.

Cette menace est en plein essor pour différentes raisons :

— Une évolution des compétences et motivations des attaquants. — Des moyens techniques plus avancés.

— Une concurrence entre les firmes plus forte que jamais.

— Une guerre désormais numérique : la cyberguerre.

5.3.2 Mode Opératoire

Les attaques APT suivent toutes un schéma général admis (Trendmicro 12, “APT Attack Sequence") dans leur déroulement. Nous allons ici rapidement vous le dé crire :

— Collecte d’information :

Le groupe APT va choisir leur cible, puis va identifier et s’informer sur les individus ou maillons faibles en utilisant des sources publiques, par exemple les réseaux sociaux, pour préparer une attaque customisée.

— Point d’entrée :

Une compromission initiale va être effectuée, faisant en général usage de faille de type “zero-day” (vulnérabilité informatique n’ayant fait l’objet d’aucune publication ou n’ayant aucun correctif connu) en délivrant un malware via ingénierie sociale (email, téléchargement furtif, . . .).

11. https://fr.wikipedia.org/wiki/Advanced\_Persistent\_Threat

12. https://docs.trendmicro.com/all/ent/ddi/v5.5/en-us/ddi\_5.5\_olh/ APT-Attack-Sequence.html

*CHAPITRE 5. ÉVOLUTION DES MENACES* 77

— Communication de commandes et de contrôles :

Représente les communications utilisées pendant toute la durée d’une attaque pour contrôler et communiquer avec les malwares positionnés dans le réseau de l’entreprise.

— Mouvement latéral :

Une attaque qui a pour but de compromettre des machines additionnelles sur un réseau. Lorsqu’ils sont à l’intérieur du réseau, les attaquants peuvent récolter les informations d’identification, escalader les niveaux de privilèges, bouger à l’intérieur du réseau et exfiltrer des données.

— Découverte d’actifs / de données :

Usage de techniques multiples, comme le port scanning, pour identifier les serveurs et services d’intérêt.

— Exfiltration de données :

Transmission de données non autorisées vers l’extérieur du réseau attaqué. 

Figure 5.1 – Schéma d’illustration du mode opératoire d’attaques de type “APT”

5.3.3 Rapports sur les APT

Les groupes APT sont définis comme étant des groupes d’activités d’intrusion traquées sous un même nom. Ces groupes sont mappés en utilisant les données de l’usage de techniques reportées publiquement. Ainsi, les informations fournies par des sites comme MITRE ATT&CK 13 ou FireEye 14 à propos des groupes APT ne représentent pas toujours toutes les techniques utilisées par ceux-ci, mais celles qui ont été reportées. Les groupes sont également reliés aux logiciels qu’ils utilisent, et les techniques liées à ces logiciels sont également traquées.

De plus, ces organismes surveillant les agissements des groupes APT via les techniques qu’ils utilisent publient régulièrement des rapports 15 sur les groupes les plus actifs du moment.

13. https://attack.mitre.org/groups/

14. https://www.fireeye.fr/current-threats/apt-groups.html

15. https://www.fireeye.com/current-threats/threat-intelligence-reports.html

*CHAPITRE 5. ÉVOLUTION DES MENACES* 78

Voici quelques exemples de groupes APT qui permettent d’illustrer le panel de cibles, d’objectifs et de nationalités qui ont déjà étés touchées :

— APT39 - Supposé être le groupe Chafer :

Groupe soupçonné d’être situé en Iran. Même si leur portée semble globale, il a plutôt tendance à concentrer ses attaques dans le Moyen-Orient. Il attaque en priorité le secteur des télécommunications, ainsi que les secteurs du trans port, de l’IT et de la haute-technologie.

D’après FireEye (), le focus du groupe dans ces secteurs suggère la volonté d’effectuer des opérations de surveillance, d’espionnage ou de traque envers certains individus. Il collecte également des données propriétaires ou clients à but commercial (revente) ou opérationnel (fuites de données).

Le fait qu’il cible des entités gouvernementales suggère qu’une intention se condaire serait de collecter des informations géopolitiques qui pourrait aider l’Etat à prendre des décisions.

— APT1 - UNIT 61398 :

La UNIT 61398 est en réalité une unité de haut rang de l’armée populaire de libération de la Chine. Leurs cibles sont très nombreuses : les technologies de l’information, l’aérospatial, les satellites et télécommunications, la recherche scientifique, les secteurs de l’énergie, du transport, de la construction, de l’in génierie, l’électronique high-tech, les organisations internationales, les médias de services légaux, publicitaires ou de divertissement, la navigation, la chimie, les services financiers, l’agriculture, la santé et l’éducation.

Leur but est le vol systématique de grandes quantités de données, provenant de 141 organisations jusqu’à présent. Toutes ces organisations proviennent de pays parlant anglais. La taille d’infrastructure requise pour de tels vols sug gère qu’APT1 est une organisation de très grande taille, composée de centaines d’opérateurs humains.

— APT38 - Supposé être le Lazarus Group :

Groupe situé en Corée du Nord. Leur cibles sont les institutions financières du monde entier.

Supporté par le régime de son pays, ce groupe est connu pour avoir effectué des attaques parmi les plus larges. Un groupe minutieux, où chaque mouvement est calculé, et qui a pour habitude de rester longtemps dans les systèmes, le temps de bien comprendre la disposition des réseaux, les permissions requises et les technologies utilisées.

Ce groupe prolifique a pour habitude d’utiliser une combinaison de backdoors, de tunnelers, de dataminers et de malwares destructifs pour voler ou détruire les données de leurs cibles. Les vols se concluent, en général, par plusieurs millions de dollars volés, ainsi que des systèmes rendus inopérables.

*CHAPITRE 5. ÉVOLUTION DES MENACES* 79

5.3.4 Prévention

Aucune solution miracle ne peut protéger votre entreprise contre les attaques APT. Une fois infiltrés dans l’organisation, ces menaces, et leurs auteurs, cherchent à rester en place. La clé consiste donc à combiner des technologies capables de re couper les différents journaux et d’identifier les comportements inhabituels au sein du réseau de l’entreprise. La stratégie de défense doit avant tout viser à choisir des solutions de détection de premier plan, capables de fournir de précieux renseigne ments sur les cibles, les méthodes des attaquants, la fréquence de leur activité, la provenance de la menace persistante avancée et les risques associés aux motivations de ces attaquants.

Selon le site Proofpoint 16, 95% des menaces ciblées et persistantes avancées utilisent une forme de phishing en tout début d’attaque. Toute stratégie de défense de l’entreprise contre les attaques APT, appelée advanced persistent threat protection, doit donc inclure une solution de détection capable de repérer les schémas de trafic inhabituel dans les messages électroniques, de réécrire les adresses URL incluses dans les e-mails suspects, puis de surveiller en permanence ces URL dans un sandbox pour détecter tout comportement malveillant. Une telle approche permettra éventuellement à l’entreprise de se protéger et/ou de détecter ce type d’attaques, et savoir quels utilisateurs ont été compromis, à quel moment et depuis quand est un atout majeur pour mieux cerner l’adversaire et ses motivations.

L’organisme Solarwinds propose un logiciel 17 de type SIEM (Security Informa tion and Event Management) nommé “Security Event Manager” capable de regrou per et surveiller les différents journaux de votre réseau d’entreprise et de déceler des comportements suspects afin de spécialement vous protéger contre les attaques APT qui cherchent à se faire discrètes.

5.4 Les attaques

Avec la pandémie et le fait que la majorité des entreprises travaillent à distance. Couplé au fait que les réseaux sont peu, voir pas sécurisé à la maison, les attaques informatiques ont largement augmenté.

En effet, entre 2019 et 2020, les armes DDoS ont plus que doublé, passant de 6 millions en fin 2019 à 12.5 millions au second quadrimestre de 2020. De plus, la plateforme cybermalveillance.gouv.fr a pour mission d’assister les victimes de cybe rattaques et de les informer sur les menaces ainsi que les moyens de s’en protéger. Durant l’année 2020, cette plateforme a connu une forte hausse de sa fréquentation (+155% par rapport à 2019). Plus de 1,2 million de personnes ont visité ses conte nus et ses alertes. Lors des premières semaines de confinement au printemps 2020, les visites ont atteint un pic de près de 600%.

16. https://www.proofpoint.com/fr/threat-reference/advanced-persistent-threat 17. https://www.solarwinds.com/fr/security-event-manager/use-cases/ apt-security-software

*CHAPITRE 5. ÉVOLUTION DES MENACES* 80

5.4.1 Client-side VS Server-side

Nous allons en premier temps, définir Client-side et Server-side : 

Figure 5.2 – Client-Side et Server-Side

— Client-Side :

Dans le développement Web, le terme "côté client" désigne tout ce qui, dans une application Web, est affiché ou se déroule sur le client (appareil de l’uti lisateur final). Cela comprend ce que l’utilisateur voit, comme le texte, les images et le reste de l’interface utilisateur, ainsi que toutes les actions qu’une application exécute dans le navigateur de l’utilisateur. Les langages de bali sage comme HTML et CSS sont interprétés par le navigateur du côté client. En outre, de nombreux développeurs contemporains intègrent des processus côté client dans l’architecture de leurs applications et s’éloignent de l’idée de tout faire côté serveur ; la logique commerciale des pages Web dynamiques\*, par exemple, s’exécute généralement côté client dans une application Web moderne. Les processus web côté client sont presque toujours écrits en JavaS cript.

— Server-Side :

Comme pour le côté client, le terme "côté serveur" désigne tout ce qui se passe sur le serveur, et non sur le client. Par le passé, la quasi-totalité de la logique métier s’exécutait côté serveur, ce qui inclut le rendu de pages web dynamiques, l’interaction avec les bases de données, l’authentification des identités et les notifications push. Le problème de l’hébergement de tous ces processus côté serveur est que chaque requête impliquant l’un d’entre eux doit faire tout le chemin du client au serveur, à chaque fois. Cela introduit une grande latence.

C’est pourquoi les applications contemporaines exécutent davantage de code côté client ; l’un des cas d’utilisation est le rendu de pages web dynamiques en temps réel par l’exécution de scripts dans le navigateur qui apportent des modifications au contenu que voit l’utilisateur. Comme pour les termes "frontend" et "client-side", "backend" est également un terme désignant les processus qui se déroulent sur le serveur, bien que "backend" fasse uniquement référence aux types de processus et que "server-side" fasse référence à l’endroit où les processus sont exécutés.

Source : Cloudflare, “What do client side and server side mean ?” 18

18. https://www.cloudflare.com/fr-fr/learning/serverless/glossary/ client-side-vs-server-side/