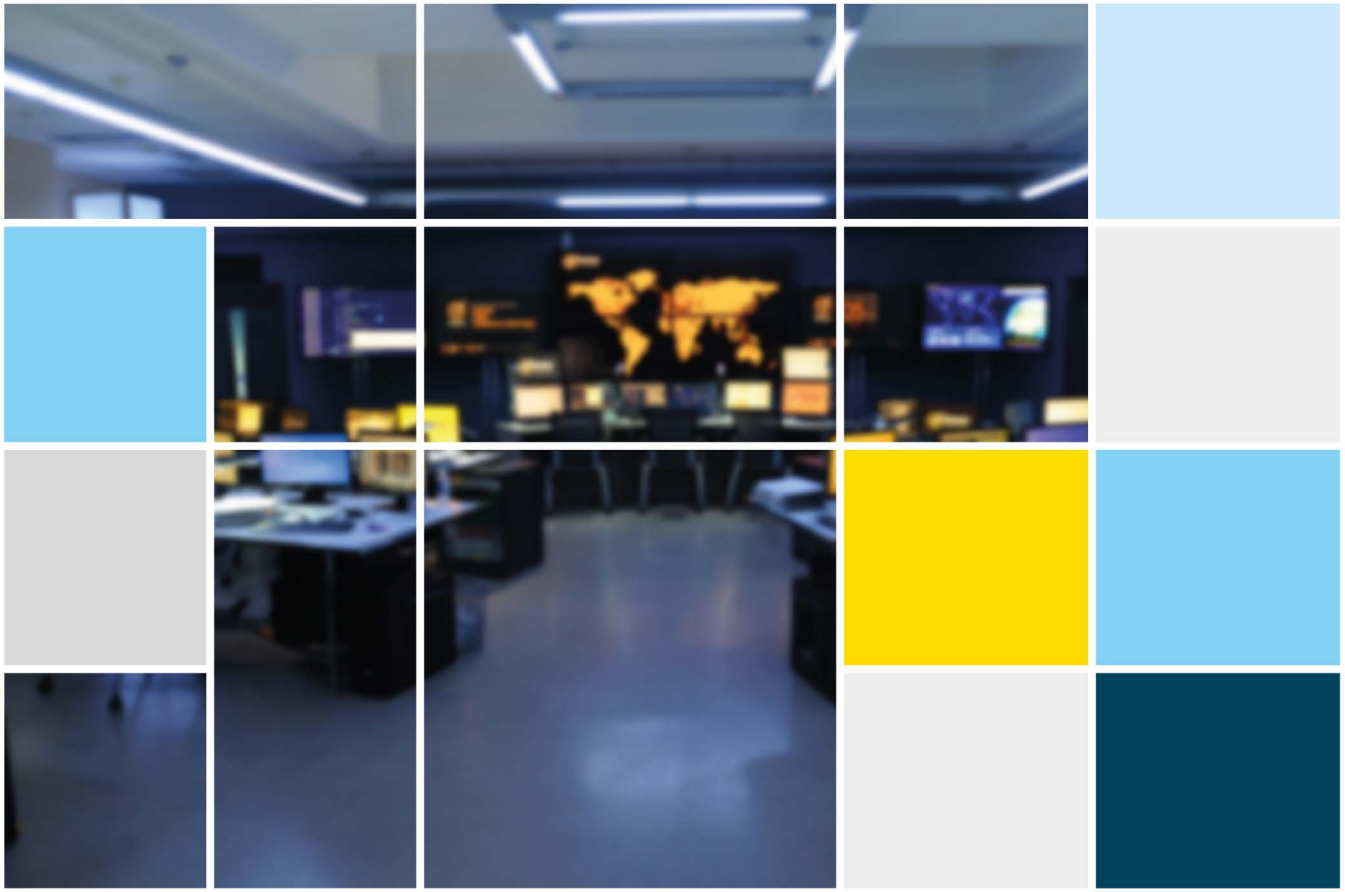
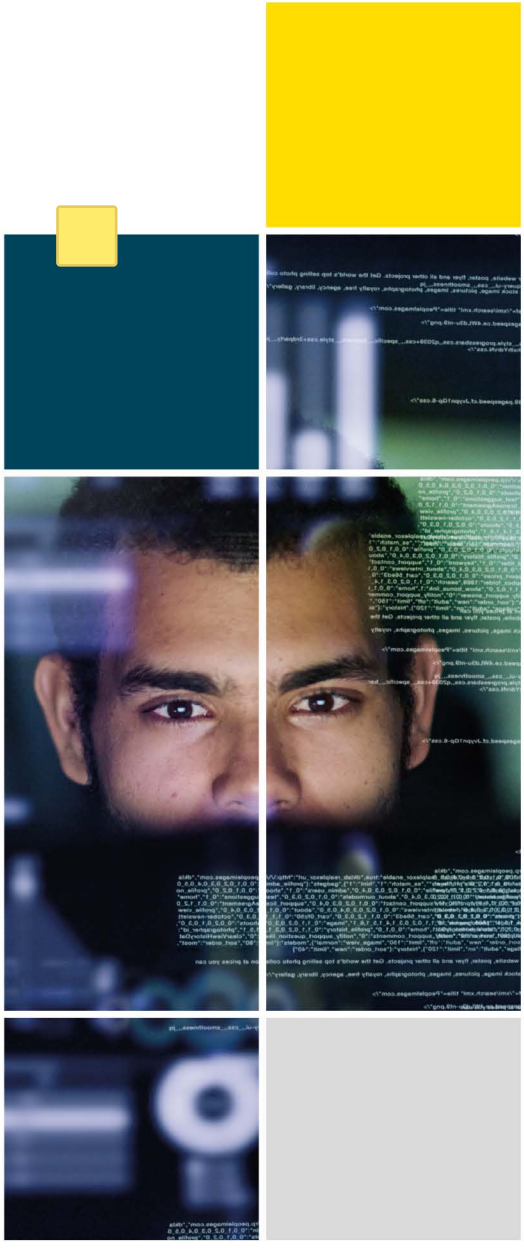
DATAPROTECT
Security is our commitment



SOC | SECURITY OPERATIONS CENTER


DATAPROTECT
Security is our Commitement



CENTRE D'OPERATIONS ET DE SECURITE (SOC)

La sécurité des systèmes d'information (SI) est devenue une des fonctions clé de la bonne gouvernance des organisations. On ne peut plus se contenter de considérer la sécurité comme un simple volet du département des technologies de l'information. La réputation de l'organisation est en jeu, voire même sa survie. Pensons seulement au vol des données personnelles de 500 millions d'usagers de Yahoo en septembre 2016. Ou encore du vol des informations de crédit de 110 millions de clients de la chaine de magasins Target en décembre 2013.

L'intrusion dans les serveurs de Yahoo a ôté 350 millions $ à la valeur de Yahoo qui négociait alors la vente de ses actifs à Verizon. Il s'agit de la plus importante violation des données à caractère personnel de l'histoire. La fuite des données de Target a coûté 162 millions $ à l'entreprise et son président a dû démissionner.

Plus près de nous, celui qu'on a parfois qualifié de « Snowden marocain » a violé en 2014 les serveurs d'un organisme publique marocain et publié la base de données du personnel de cet organisme. La liste de tous les fonctionnaires, diplomates, agents techniques et employés, etc., avec leurs noms, prénoms, date de naissance, état civil, nombre d'enfants, matricules, numéros de la carte d'identité nationale et date de recrutement, a été rendue publique.

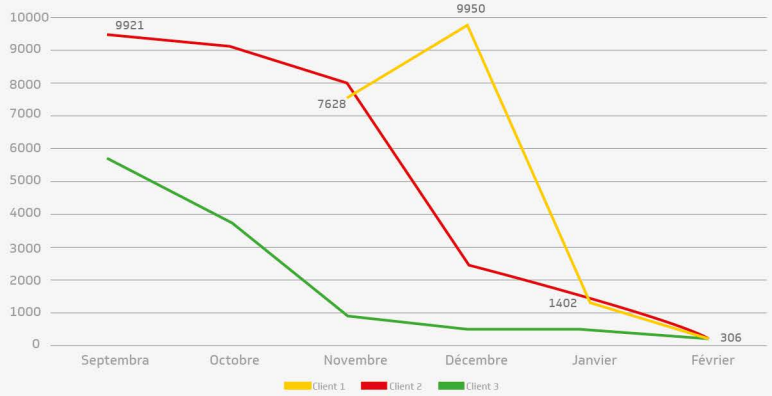
Qu'il s'agisse de hackers agissant pour leur propre compte ou de services de renseignements d'États souverains, ces menaces insidieuses varient sans cesse. Pour s'en prémunir, il ne suffit pas d'investir plus en protection des SI. L'amélioration de la sécurité de l'organisation nécessite de formaliser le traitement des incidents depuis leur détection jusqu'à leur traitement et centraliser les processus de façon à avoir une visibilité globale de la situation en temps réel. L'outil capable de satisfaire à ce double objectif du SOC.

La plupart des SOC sont créés en réponse à un contexte réglementaire, une contrainte légale ou à la suite d'une intrusion dans les systèmes d'information qui aurait pu être prévenue par un dispositif SOC. C'est ainsi que les institutions financières se dotent de structures sécuritaires pour répondre aux exigences réglementaires de plus en plus contraignantes (CSP SWIFT,PCI DSS, ACCORD Bâle III etc.).

Les entreprises commerciales doivent se conformer à la norme PCI-DSS pour protéger les données de crédit de leurs clients. Au Maroc, la Directive Nationale de la sécurité des systèmes d'information (DNSSI) impose des normes très strictes aux opérateurs d'importance vitale en matière de traçabilité et de traitement des incidents.

Grâce au SOC, il est possible de quantifier et de surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume, les coûts associés et leurs impacts sur les processus d'affaires. Son but est de parvenir à diminuer de façon significative le nombre d'incidents en identifiant leurs sources, en les analysant et en remédiant aux défaillances existantes.

LE BUT DU SOC EST DE REDUIRE LE NOMBRE D'INCIDENTS



Exemple d'évolution des événement de sécurité SI traités

DEFINITION DU SOC

Un SOC est composé de trois éléments tous aussi importants les uns que les autres : une équipe d'experts en sécurité, une série de processus formels et une plateforme technologique.

Le SOC a pour fonction d'exercer une surveillance efficace sur un périmètre informatique déterminé et un suivi des incidents de bout en bout. Il transforme les données brutes qui sont générées par l'équipement informatique en incidents et s'il y a lieu en alertes. Le SOC notifie alors le responsable du département des systèmes d'information du danger en cours et, en principe, c'est l'équipe d'intervention de ce département qui procède au traitement de l'alerte et à la restauration du système attaqué.

Dans la pratique, il est souvent difficile de tracer une ligne de démarcation fixe entre le rôle du SOC et celui de l'équipe d'intervention (en anglais Computer Security Incident Response Team ou CSIRT) du département des systèmes d'information de l'organisation cliente. Le SOC est souvent appelé à collaborer au traitement de l'attaque et à la restauration du système.

Éléments de base du SOC

Experts

- Formation certifiante
- Expérience acquise

Technique

- Solution SIEM
- Terminaux
- Surveillance réseau
- Détection incident
- Corrélation
- Archivage

Processus

- Planification
- Identification
- Endiguement
- Notification
- Leçon apprise

SOC

BY **DATAPROTECT**

SECURITY OPERATIONS CENTER

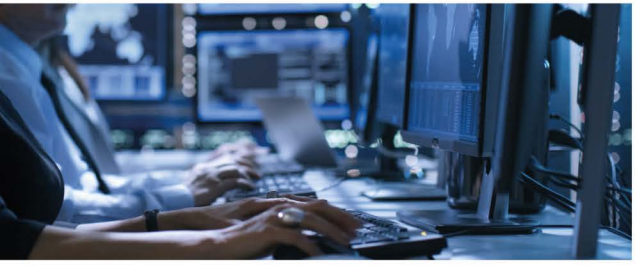
PRÉPARATION • DÉTECTION • INVESTIGATION • ENDIGUEMENT

ÉRADICATION & RECOUVREMENT • REPORTING • ANALYSE POST-INCIDENT • CLÔTURE

Le rôle du SOC n'est pas seulement réactif. Il exerce aussi une activité de veille technologique et un suivi des alertes. La veille technologique peut faire appel à des sources externes, comme le Moroccan Computer Emergency Response Team (maCERT). Toutes les alertes dont l'objet de fiches de retours d'expériences qui sont enregistrées dans un système d'archivage. Il est ainsi possible de procéder à des investigations (forensics) et de réutiliser les solutions trouvées en cas de récidive d'incident similaire.

Déployer un SOC est une œuvre de longue haleine qui doit être soigneusement planifiée. Le centre doit être doté de sa propre charte distincte de l'organisation à laquelle elle appartient. Cette charte définit les responsabilités du SOC, les processus opérationnels et les relations avec le département des systèmes d'information. Seules les grandes organisations qui disposent d'une équipe informatique de plus de 100 personnes, peuvent dégager les ressources nécessaires à la mise sur pied et à l'entretien d'un SOC en interne.

Encore faut-il noter que bien des organisations ont des SOC qui font appel à du personnel dont la tâche principale est étrangère à la sécurité. Ces structures internes donnent une fausse impression de sécurité. Les petites organisations et les grandes organisations qui ne veulent pas taxer indument leurs départements de systèmes d'information ont intérêt à faire appel à un SOC externe géré par un prestataire qualifié.



LES RESSOURCES HUMAINES DU SOC

Un SOC complet doit pouvoir fonctionner 24 heures sur 24 et sept jours sur sept. Cela nécessite au minimum cinq employés à plein temps pour assurer la présence d'un analyste sur toute la période de surveillance. Ces employés doivent avoir une solide formation en applications réseaux et parfois même en rétro-ingénierie (reverse engineering). La grande difficulté est de maintenir le niveau d'attention au niveau indispensable. Pour cela des rotations de personnels sont recommandées. Les jours de congé sont traités comme des jours ordinaires.

Fonction	Tâches	Formation
Niveau 1 (N1) : analyste sécurité	Surveille en permanence la file d'attente des alertes ; tri des alertes ; surveille les capteurs de sécurité et des terminaux ; recueille les données nécessaires pour escalader le travail vers le niveau 2.	Procédures de tri des alertes ; détection d'intrusion ; sécurité des réseaux ; gestion de l'information et des événements de sécurité (SIEM), formation d'enquête basée sur l'organisation cliente, etc.
Niveau 2 (N2) : spécialiste sécurité	Effectue une analyse d'incident en profondeur en corrélant les données de diverses sources ; détermine si un système ou un ensemble de données critiques a été affecté ; conseille sur la restauration ; fournit un support pour de nouvelles méthodes analytiques pour détecter les menaces.	Investigation orientée réseau ; investigation orientée serveur ; procédures de réponse aux incidents ; analyse de logs ; évaluation de base des logiciels malveillants ; évaluation de la menace.
Niveau 3 (N3) : investigateur sécurité	Possède des connaissances approfondies sur les réseaux, les terminaux, l'évaluation de la menace, investigation et rétro-ingénierie des logiciels malveillants. Il peut aussi anticiper les incidents, n'attendant pas qu'ils soient escaladés. Il est responsable de l'analyse de la détection des menaces.	Formation avancée en détection des anomalies ; formation spécifique aux outils pour l'agrégation et l'analyse des données ainsi que l'évaluation de la menace.
Directeur du SOC (Service Delivery Manager)	Gère les ressources (personnel, budget, horaires et technologie) pour respecter les contrats de niveaux de services ; liaison avec la haute direction ; gestion des incidents stratégiques ; orientation globale du SOC.	Gestion de projet ; formation en gestion des réponses aux incidents compétences générales en gestion des ressources humaines.

Source : adapté de SANS Institute

PROCESSUS

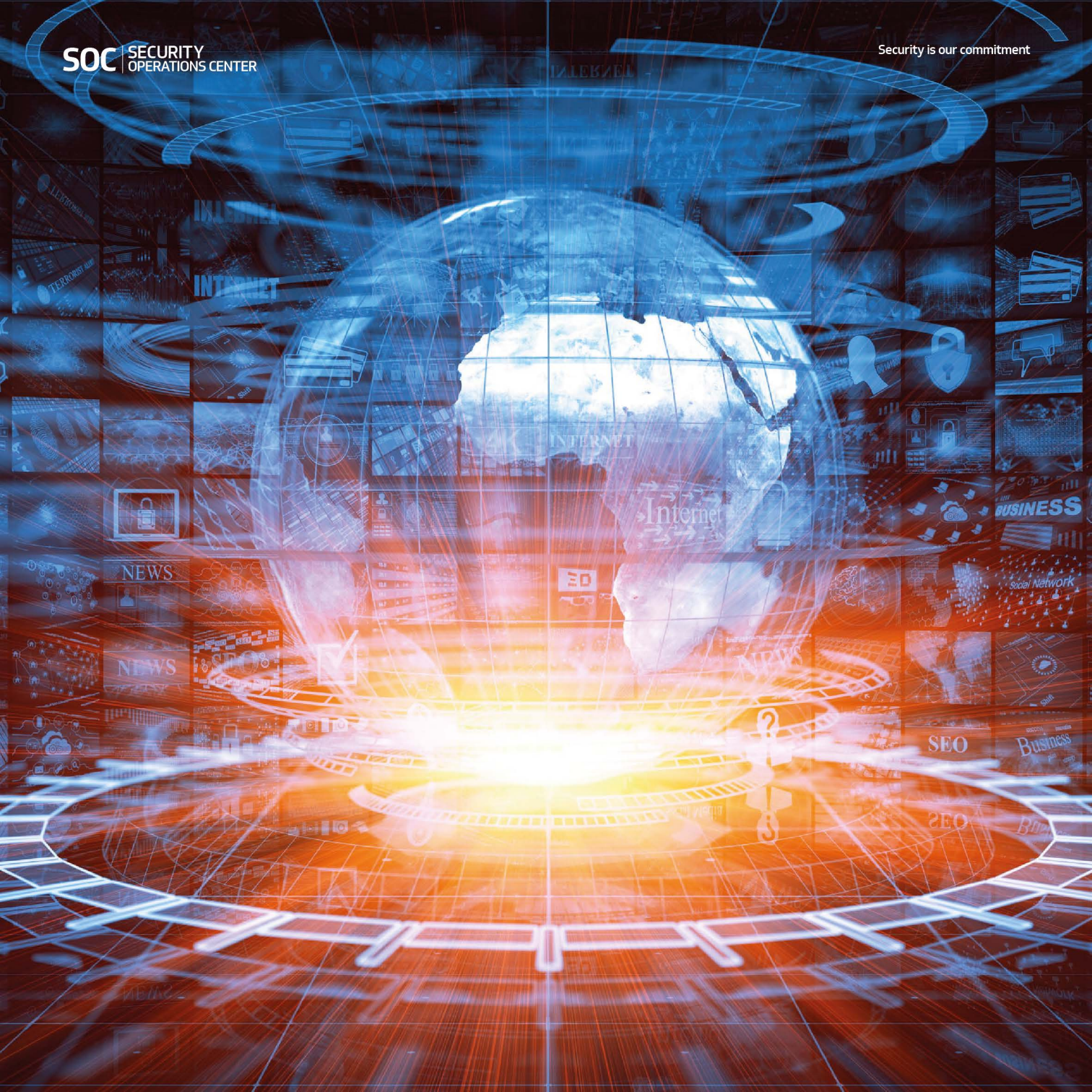
À la base de tout processus de supervision, de réponse et d'investigation se trouve une convention passée entre le SOC et l'organisation cliente. Cela est valable aussi bien pour les SOC internes que pour les SOC appartenant à un prestataire de services de sécurité. Cette convention décrit le périmètre des systèmes d'information à sécuriser, la nature des transactions normalement effectuées par l'organisation et l'engagement du SOC envers le client. Mais le périmètre évolue au fur et à mesure que l'organisation ajoute ou ôte des équipements informatiques à ses systèmes : il faut donc prévoir les modalités de mises à jour de la convention qui doit elle-même être assez flexible.

Pas de surveillance possible sans une bonne connaissance de l'environnement du client. Il est donc indispensable de prévoir au début de chaque mandat de supervision d'un système d'information une étude de cadrage, aussi appelée transition, grâce à laquelle les experts du SOC vont se familiariser avec la plateforme technique du client, son architecture de sécurité ainsi qu'avec ses habitudes de travail. Ce qui peut représenter un événement pour un client peut être considéré comme une pratique courante chez un autre. Une étude de cadrage dure en moyenne trois mois à 6 mois selon la maturité de la documentation existante et les services de réponse existants chez le client.

La matière première de la supervision est constituée par le log sécurité des systèmes d'information à superviser. Comme des dizaines de milliers d'événements sont produits chaque seconde, il est alors indispensable d'établir une série de cas d'utilisation (use cases) qui sont des mini-scénarios qui décrivent les cas qui nécessitent l'intervention des experts du SOC. Un cas d'utilisation standard est une attaque répétée depuis une même source, un excès de trafic entrant, un accès non autorisé à des données confidentielles, etc. D'autres cas d'utilisation peuvent être spécifiques au client.

SOC | SECURITY OPERATIONS CENTER

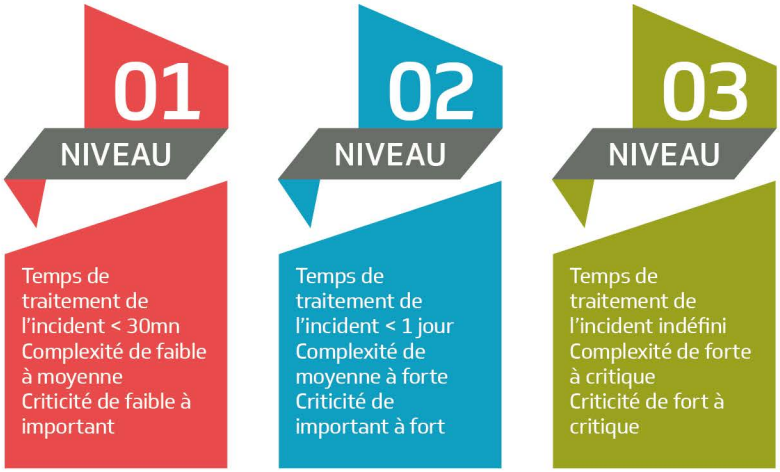
Security is our commitment



Une bonne bibliothèque de cas d'utilisation permet d'automatiser le déclenchement des alertes et libère ainsi l'attention des experts pour les cas complexes qui nécessitent une analyse plus poussée. Plus la bibliothèque des cas d'utilisation est complète, plus on diminue le nombre de faux positifs, c'est-à-dire les événements normaux qui ont été considérés à tort comme défaillants.

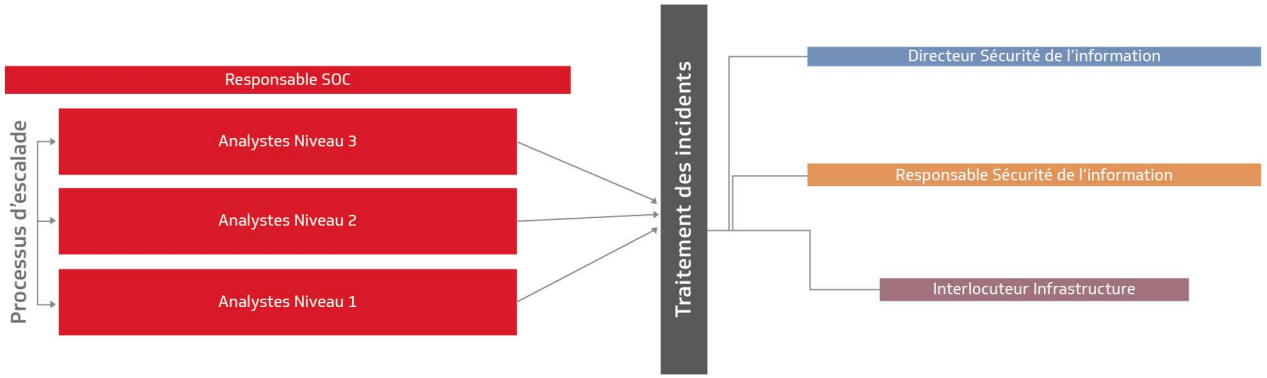
L'expert de niveau 1 a pour fonction d'analyser le trafic quasi-brut qui entre dans le SOC. Il peut aussi recevoir des communications téléphoniques ou autre en provenance du responsable du groupe des systèmes ou d'utilisateurs qui veulent porter une anomalie à l'attention du SOC. Dans un cas comme dans l'autre, son rôle est de résoudre les cas les plus simples dans un laps de temps limité (typiquement moins de 30 minutes). Si l'événement considéré nécessite une intervention plus poussée, il est escaladé vers le niveau 2 qui a plus de temps pour résoudre le problème (typiquement 24 heures). En dernier recours, l'événement est escaladé au niveau 3 qui prendra tout le temps nécessaire pour résoudre ce qui, à ce moment, a toutes les chances d'avoir le potentiel d'une crise grave.

Le processus d'escalade prévoit la mise au courant de l'organisation cliente aux étapes clés. Une notification lui est alors envoyée par courriel ou téléphone détaillant la nature de l'alerte et les moyens à prendre pour remédier à l'intrusion et restaurer le système. En principe, il appartient à l'équipe d'intervention du département des systèmes d'information de procéder, mais comme on l'a déjà vu, il s'agit souvent d'une opération conjointe SOC/CSIRT. Dans tous les cas, le SOC conserve en mémoire les traces de l'intrusion et s'en sert comme outil référentiel.



Source : Atos

Indicateurs de triage



Organigramme du SOC

Grâce à cet outil référentiel, il est ainsi possible de prévenir la répétition d'attaques similaires dans d'autres systèmes d'information. Le grand avantage des SOC appartenant à des prestataires indépendants sur les SOC internes est qu'ils peuvent utiliser l'expérience acquise avec un client pour sécuriser leurs autres clients avec la solution développée. Le SOC devient alors un moyen de prévention.

TECHNOLOGIE

La partie la plus spectaculaire du SOC est constitué par un mur d'images où sont affichés les indicateurs d'activités de manière continue de manière à pouvoir être partagés entre plusieurs experts lors du traitement des incidents. Il s'agit d'une survivance de la sécurité physique quand on avait à surveiller plusieurs caméras de surveillance situées dans les divers emplacements. Les experts du SOC peuvent ainsi travailler en commun sur le même incident.

Le cœur de l'infrastructure du SOC est constitué par une solution de gestion des événements et des informations de sécurité mieux connue sous son sigle anglais SIEM (Security Information and Event Management). Il s'agit d'une application de centralisation et de corrélation des logs. À titre d'exemple, si un inconnu exécute 10 000 ou plus essais d'intrusion sur un serveur, l'ensemble sera traité comme un seul événement. De cette façon, il devient possible pour les experts de niveau 1 du SOC de traiter des centaines de millions d'événements par jour sans être submergés.

La solution choisie par DATAPROTECT pour son infrastructure SIEM est QRadar d'IBM. Cette solution offre une excellente visibilité du réseau, des utilisateurs et de l'activité sur les applications en quasi temps réel. Elle assure la collecte, la normalisation, la corrélation et le stockage sécurisé des événements, des flux, des actifs et des vulnérabilités. Année après année, Gartner Inc. désigne IBM QRadar comme l'un des leaders de son Magic Quadrant pour le SIEM. Comme la solution est évolutive, il est possible de lui ajouter de nouvelles règles chaque fois qu'il y a de nouvelles menaces.

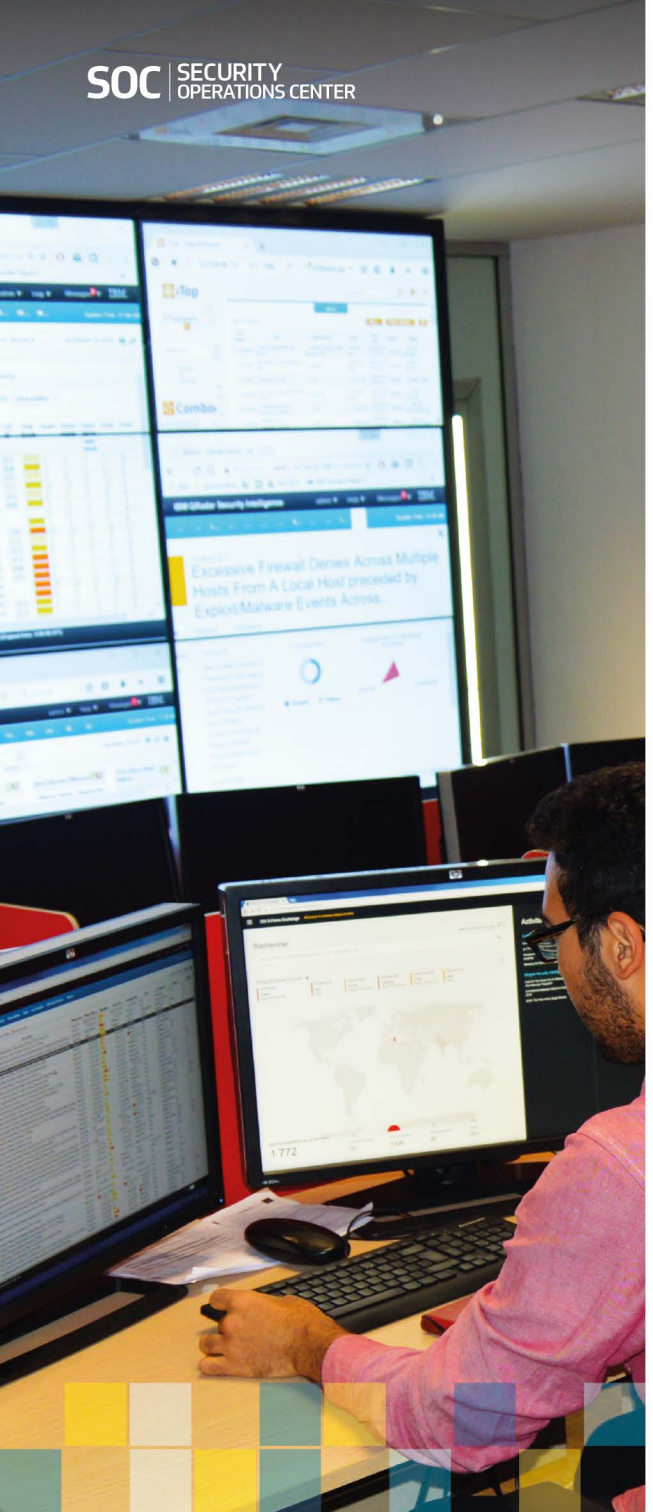
En outre, la connectivité entre le SOC et les systèmes d'information du client est établie par le truchement d'un bastion d'administration (jump host). Cela signifie que le poste de travail du SOC n'est pas en contact immédiat avec les systèmes supervisés, il transite par un poste de travail virtuel qui optimise la connexion SOC-organisation et conserve une trace vidéo de tout le travail effectué. À cet effet, DATAPROTECT utilise la plateforme Citrix qui assure la disponibilité et l'efficacité du service de poste virtuel.

D'une façon générale, le SOC de DATAPROTECT est doté d'outils qui lui permettent d'intervenir dans les systèmes d'information des organisations où qu'elles se trouvent et de traiter les incidents en toute transparence, comme si le périphérique cible était situé dans la même pièce que ses experts en sécurité.

AUTORITE ET COMMUNICATIONS

L'autorité du SOC est définie dans la convention qui le lie à l'organisation cliente. Comme le SOC représente un investissement majeur de la part de l'organisation, il est probable que le SOC bénéficie du soutien du top management. Dans le feu de l'action, toutefois, son autorité est plus virtuelle que réelle. Si le SOC demande la fermeture d'un système en raison d'une attaque en cours, il se heurtera bien souvent aux exigences de service des gens de métier (en particulier, les départements de la production, des ventes, du service à la clientèle, etc.).

L'autorité du SOC dépend des liens permanents qu'il aura tissé avec le responsable du département des systèmes d'information du client et des différents autres intervenants. Voilà pourquoi il est indispensable de prévoir des communications régulières avec l'organisation cliente. Outre les statistiques de performance qui sont transmises au responsable du groupe des systèmes sur une base mensuelle, il est recommandé de rédiger des « success stories » à propos des incidents les plus notoires et de les faire circuler auprès de la haute direction de l'industrie cliente. Ces documents pourront être produits trois ou quatre fois par an afin de rappeler l'utilité du SOC, ses réalisations et son importance – ainsi que l'opportunité de renouveler son budget à la fin de l'année financière !



1 LE PREMIER SOC MAROCAIN

C'est la firme DATAPROTECT qui a ouvert le premier SOC au Maroc en septembre 2014 afin de répondre à une vague d'incidents parmi les opérateurs d'importance vitale. Le centre disposait alors d'une petite salle avec cinq positions de travail et trois employés à plein temps. Il assurait une veille non décalée tous les jours de 8h00 à 19h00 avec astreinte et réponse. Cette première infrastructure a cédé la place en février 2017 à une salle dotée de 12 positions et 15 employés qui assure une veille 24 heures sur 24 et sept jours sur sept.

Au départ, le SOC comptait un seul niveau afin de répondre aux besoins en supervision des organisations clientes. Aujourd'hui, un deuxième niveau a été ajouté pour résoudre les cas plus délicats. Le troisième niveau sera opérationnel en 2018. En attendant, les cas demandant une expertise sectorielle approfondie sont traités par des spécialistes de DATAPROTECT détachés auprès du SOC de façon ponctuelle. Le temps de prise en charge moyen est de moins de 10 minutes dans le SOC de DATAPROTECT et le maximum est de 30 minutes dans 95% des cas.

Depuis 2016, le SOC de DATAPROTECT est certifié ISO 27001 version 2013, qui spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation, quels que soient son type, sa taille et sa nature. Cette norme comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. C'est le seul SOC du Maroc à être certifié ISO 27001.

Le SOC de DATAPROTECT compte actuellement 20 clients, principalement dans le secteur financier (banques et assurances), les services publics (eau et électricité) ainsi que le secteur de la santé (hôpitaux). Il est actuellement en plein expansion et sera bientôt complété par l'ouverture de trois nouveaux SOC : Paris, Dakar et Dubaï. Cette mutualisation de l'infrastructure de sécurité permet de réaliser des économies de gamme (scope economies) et de faire bénéficier tous les clients des expériences acquises à l'occasion du traitement d'un incident particulier.


DATAPROTECT
Security is our Commitement

DATAPROTECT
Security is our commitment

Maroc : Casablanca Nearshore Park, Shore 4, Bd El Qods, Casablanca
Tél.: +212 5 22 21 83 90 / Fax: +212 5 22 21 83 96 / contact@dataprotect.ma / www.dataprotect.ma

France : 9-11 Allée de l'Arche, Faubourg de l'Arche, 92671 Courbevoie Cedex
Tél.: +33 6 48 51 87 97 / contact@dataprotect.fr / www.dataprotect.fr

Maroc | Algérie | Angola | Bénin | Botswana | Burkina Faso | Burundi | Cameroun | Cap-Vert | République centrafricaine | Tchad
Comores | Congo (Brazzaville) | Congo (Kinshasa) | Djibouti | Égypte | Guinée équatoriale | Érythrée | Éthiopie | Gabon | Gambie
Ghana | Guinée | Guinée-Bissau | Côte d'Ivoire | Kenya | Lesotho | Libéria | Madagascar | Malawi | Mali | Mauritanie | Maurice
Mayotte | Mozambique | Namibie | Niger | Nigéria | Réunion | Rwanda | Saint | Helena | Sao Tomé-et-Principe | Sénégal | Seychelles
Sierra Leone | Somalie | Afrique du Sud | Soudan du Sud | Soudan | Swaziland | Tanzanie | Togo | Tunisie | Ouganda | Zambie | Zimbabwe
France | Belgique | Allemagne | Italie | Luxembourg | Pays-Bas | Espagne | Arabie Saoudite | Emirats Arabes Unis