TOUT CE QUE VOUS AVEZ TOUJOURS VOULU SAVOIR SUR LES SOC

LIVRE BLANC

PREPARED BY
ITRUST
CYBERSECURITY EDITOR

SOMMAIRE

DÉLAI MOYEN DE DÉTECTION D'UNE ATTAQUE : 175 JOURS !

Avec le nombre croissant de failles de sécurité et la sophistication grandissante des cyberattaques, les entreprises doivent aujourd'hui revoir leur approche de la cybersécurité. Il est désormais nécessaire de basculer dans une approche où l'on va privilégier à la fois une analyse complète des données à l'aide d'outils de supervision avancés. Franchir cette étape est indispensable pour sécuriser les infrastructures informatiques existantes.

Illustration de la faiblesse actuelle des protections mises en place par les entreprises européennes, la récente étude M-Trends 2018* menée par Mandiant estime à 175 jours le délai moyen de détection d'une attaque sur une entreprise européenne. La moyenne mondiale est de 101 jours.

Afin de pallier au plus vite ce manque de protection flagrant, la mise en place d'un SOC (Security Operation Center) va permettre à l'entreprise de surveiller en permanence la sécurité informatique de ses actifs IT, mais aussi, et surtout, de réagir sans délai en cas d'attaque avérée ou suspectée.

MAIS QUE SE CACHE-T-IL DERRIÈRE L'ACRONYME " SOC " ?
QUELS SONT LES OUTILS ET LES RESSOURCES À METTRE EN PLACE ?
POUR DISPOSER D'UNE TELLE VIGIE SUR SON SYSTÈME D'INFORMATION ?

*M-Trends 2018 Special Report, Mandiant 2018

QU'EST CE QU'UN SOC ?

UNE ÉQUIPE D'ANALYSTES

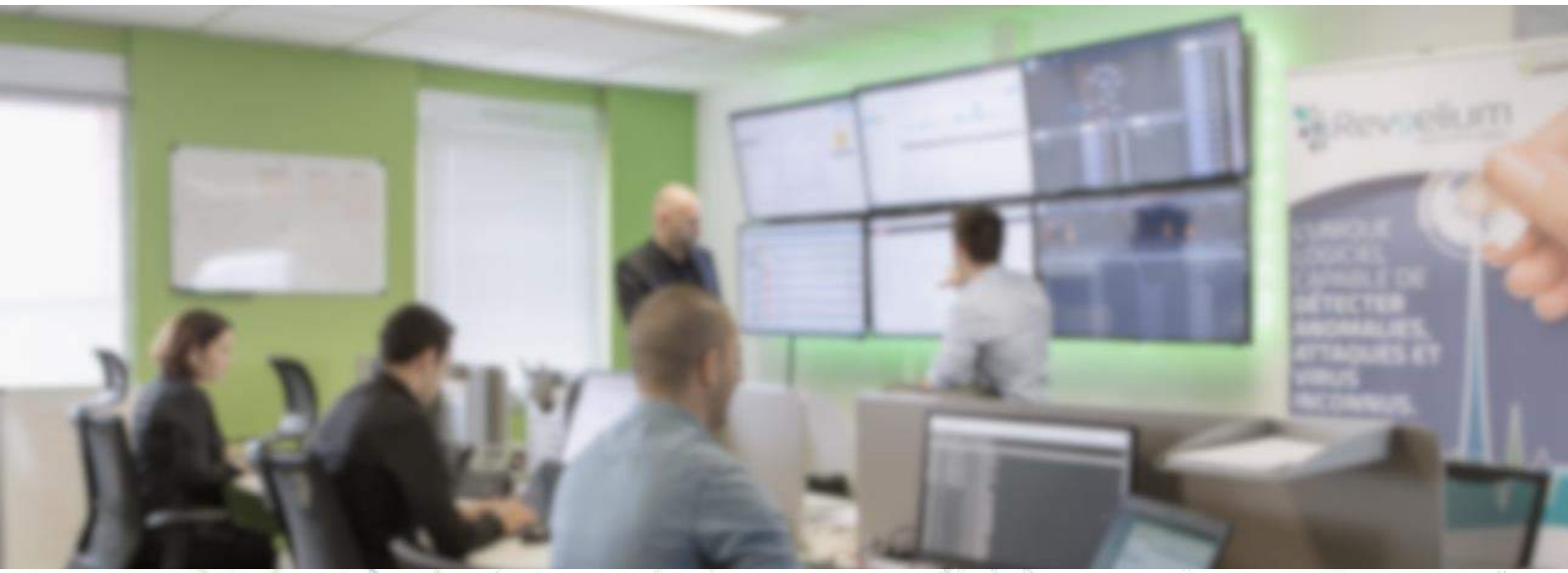
Un SOC est un dispositif de supervision de la sécurité du Système d'Information, ou autrement nommé en anglais Security Operation Center (SOC). À la tête de ce dispositif, une équipe d'analystes dont les principales missions sont de :

- Prévenir, détecter, analyser, évaluer et répondre aux menaces (internes et externes) ;
- Répondre aux incidents de sécurité informatique ;
- Évaluer la conformité réglementaire. Cette équipe se compose d'experts dont les profils sont multiples et les compétences pointues dans leurs domaines.

Les rôles et compétences des équipes qui les composent sont variés :

Par exemple, il existe :

- Des " SOC Specialist " (chargés de l'installation, l'intégration des outils et la maintenance du SIEM) ;
- Des " SOC Analyst " (chargés d'analyser les alertes et incidents) ;
- Des " SOC Support " (accompagnement pour amélioration continue).



GARANTIR LA CONTINUITÉ DES ACTIVITÉS

Le SOC a pour objectif de répondre aux préoccupations principales d'une entreprise quant à sa sécurité informatique. Celui-ci permet de garantir la continuité des activités métiers en s'adaptant au mieux et au plus vite aux menaces et risques liés à l'hyper-connectivité, que ces contraintes soient actuelles ou futures.

C'est d'ailleurs au travers de cet objectif que se trouve un des points forts du SOC : l'utilisation combinée de la machine (outils de gestion et d'analyse) et de l'homme. Ceux-ci permettent de prévenir les attaques de demain, encore inconnues à ce jour.

SOC INTERNE OU MANAGÉ ?

Plusieurs types de SOC cohabitent sur le marché : internes à l'entreprise, managés (prestataire externe), SAAS (externalisé / mutualisé à la demande), hybrides – nous verrons d'ailleurs un cas particulier pour illustrer ce second exemple, à travers de notre propre SOC ITrust.

Chaque modèle de commercialisation présente ses avantages et ses contraintes. Le contexte réglementaire ou la stratégie de l'entreprise, tant vis-à-vis du Cloud et de l'hébergement de leurs données chez des prestataires externes, ainsi que les ressources humaines disponibles orientent vers un modèle commercial.

AU CŒUR DU SOC, LE SIEM

Enfin, impossible d'évoquer le SOC sans parler du SIEM (Security Information Event Managment).

C'est la partie logiciel qui, de par ses fonctionnalités et sa position centrale dans l'architecture du SOC, est considérée comme le cœur de ce dispositif. Les SIEM entrent alors en jeu en permettant la collecte, l'agrégation, la corrélation, le reporting ou encore l'archivage des données récoltées.

En effet, face au nombre d'évènements générés par la multitude des composants d'un Système d'Information, il devient difficile de les traiter progressivement.

LE SIEM EST DONC LA VÉRITABLE CLÉ DE VOÛTE DU BON FONCTIONNEMENT DU SOC ET ASSURE LE BON DÉROULEMENT DE SES MISSIONS.

POURQUOI UN SOC ?

CONTRÔLE

Le SOC permet aux entreprises d'avoir plus de contrôle optimisé sur leurs processus de surveillance.

Il apporte une réponse efficace à la sécurité informatique et des conversations plus éclairées avec les régulateurs. Ces derniers seront continuellement au contact de leurs données, analysant et surveillant tout comportement suspect et facilitant ainsi d'éventuelles investigations.

DÉTECTION / MISE EN CONFORMITÉ

Le SOC permet aux entreprises de structurer le suivi des conformités réglementaires.

L'impact stratégique d'un projet de construction SOC en fait donc une initiative importante pour les organisations dans la mesure où :

- Il améliore le suivi des obligations réglementaires
- Il permet de se préparer à une attaque interne et externe
- Il doit notamment permettre de mettre en place les procédures de réponses aux incidents de sécurité informatique.

Aussi ce dispositif fait partie de la mise en conformité au regard des différentes règlementations (LPM – RGDP…) et améliore la vision globale du parc informatique en termes de sécurité.

LA MISE EN PLACE D'UN SOC MODERNE DOTÉ D'UN OUTIL D'ANALYSE COMPORTEMENTALE RÉDUIT CONSIDÉRABLEMENT LE NOMBRE D'ALERTES DE SÉCURITÉ ET AINSI LE COÛT HUMAIN D'EXPLOITATION DU SOC.
LE TOUT EN AMÉLIORANT LA DÉTECTION DE NOUVELLES MENACES.

LES 8 CRITÈRES D'EFFICACITÉ D'UN SOC

SEUL 20% DES SOC SONT EFFICACES DANS L'ÉTUDE HP*.

RÉUSSIR LA MISE EN PLACE D'UN SOC EFFICACE DANS UNE ORGANISATION PASSE PAR L'APPLICATION DE 8 POINTS FONDAMENTAUX.

1

PRISE EN COMPTE INITIALE DES RÉFÉRENTIELS DE L'ENTREPRISE (SOURCES, MENACES, IMPACTS) ET DE SON ARCHITECTURE (FONCTIONNELLE ET TECHNIQUE).

Cette phase initiale va permettre d'évaluer les paramètres de déploiement et de mise en œuvre du SOC ainsi que les moyens qui lui seront alloués.

Par exemple :

- Faut-il centraliser ou délocaliser la supervision ?
- Quels sont les paramètres fonctionnels à couvrir : zones d'hébergement, mobilité, applications métiers ?
- Quels sont les outils de sécurité à contrôler (pare-feu, anti-virus, anti-spam…) ?
- Quels journaux informatiques doivent-être collectés et analysés ?

Astuce de l'expert

Le réseau d'un e-commercant subit des pics d'activité substantiels dans une année : les soldes, Noël, … lui appliquer des seuils « par défaut » sans les adapter à ses spécificités entraînerait des faux positifs en cascade.

Monsieur DS. Red Team Leader.

2

IMPLICATION DE L'ENSEMBLE DES PARTIES PRENANTES

La mise en place d'un SOC doit être considérée comme un projet stratégique.
Le projet est souvent porté par la direction générale ; c'est un élément clé pour que la sécurité fasse partie de l'ADN de l'entreprise. C'est également un projet où les équipes métiers peuvent être associées, formées et informées au travers d'une méthodologie comprenant retours d'expérience, tableaux de bord métier et d'informations issues de la veille en sécurité.

Astuce de l'expert

Lorsqu'un SOC avertit la direction informatique d'une vulnérabilité sur un actif, des actions doivent être entreprises. Dans le cas contraire, les rapports d'alertes deviennent de plus en plus volumineux (puisqu'ils intègrent les précédentes alertes non traitées) jusqu'à devenir inexploitables. Le SOC doit donc adapter les seuils d'alerte en fonction de ce que l'IT peut traiter pour ne pas créer de sentiment de découragement devant l'ampleur de la tâche, ce qui conduit à un immobilisme.

Monsieur BB. Analyste SOC niveau 2.

* Article réalisé par « lemagit.fr » sur l'étude HP 2015

3

RÉPONSE AUX OBLIGATIONS LÉGALES (RGPD – LPM 2014 -2019)

Le SOC doit bien évidemment pouvoir être utilisé dans le cadre de la conformité et répondre, le cas échéant, aux obligations imposées aux entreprises ou aux OIV (Opérateur d'Importance Vitale).

Dans le cadre du règlement européen 2016/679 du 27 avril 2016 (dit " règlement général sur la protection des données " ou RGPD) ou de la Loi de Programmation Militaire (LPM), il est demandé par exemple la notification d'incidents aux autorités dans les délais extrêmement brefs. Etre capable de détecter et de signaler des incidents de sécurité, parfois complexes, implique la mise en œuvre d'un système de détection d'attaques informatiques performant ainsi que des processus de notification des incidents de sécurité significatifs aux autorités compétentes.

Cela ne s'applique pas uniquement à la RGPD et à la LPM, d'autres réglementations supposent la mise en place d'un SOC : HDS, HIPAA, SOX, Bâle III, PCI/DSS…

Astuce de l'expert

En cas d'attaque informatique, les pirates cherchent généralement à effacer leur traces (les logs essentiellement). Disposer d'un SOC servira notamment de duplicata de ces logs aux personnes qui investigueront l'attaque pour retrouver son origine et son étendue réelle.

Monsieur JV. Redteam malware expert.

4

UNE STRATÉGIE DE SURVEILLANCE ADAPTÉE

L'élaboration d'une stratégie de surveillance permet de formaliser le fonctionnement du socle de cybersécurité et d'en assurer une bonne gestion dans le temps.

Elle se base généralement sur un document définissant le périmètre, l'architecture, les processus de maintien et les différentes règles de détection sur une base de connaissances et sur le suivi du projet.

Si son premier objectif est de garantir la bonne surveillance du parc, la stratégie de sécurité constitue également un excellent moyen de s'assurer de l'efficacité du SOC et de piloter sa montée en puissance.

5

APPRÉCIATION DES RISQUES SCÉNARIOS DE MENACE

Qu'il s'agisse de l'analyse des risques ou d'évaluation des scénarios de menaces, il est humainement impossible de tout couvrir. Il faut donc effectuer des choix :

Quels sont les incidents redoutés par mon entreprise ?
Quels sont les risques acceptables pour mon entreprise ?
Quelles sont les 10 menaces dont je veux impérativement me protéger ?

Astuce de l'expert

La formalisation des risques est un atout substantiel pour une entreprise. En son absence, il arrive souvent que l'IT et la direction n'aient pas la même vision des priorités et que les dépenses soient mal réparties (surinvestissement dans un pare-feu dernier cri pour un gain minime mais lacunes dans la lutte anti spam).

Monsieur BP. Avant vente SOC Reveelium.

6

POLITIQUE DE SUPERVISION

Les choix stratégiques réalisés au moment de l'analyse des risques sont déclinés en une politique de supervision solide, qui intègre entre autres : les éléments nécessaires pour détecter les incidents redoutés (deni de service, élévation de privilèges…), un référentiel qui va formaliser la stratégie d'analyse, l'architecture à mettre en place, le reporting…

Il est souvent nécessaire de disposer d'un reporting spécifique pour le directeur technique ou directeur général.

Astuce de l'expert

En plus de son utilité directe, le reporting permet de constater l'amélioration de la sécurité de l'entreprise au fil du temps. Il permet de construire des indicateurs pertinents pour les boards de direction.

Monsieur CP. Analyste SOC niveau 3.

7

IMPLANTATION / MISE À JOUR

La phase d'implantation du SOC couvre notamment la traduction des éléments de la PSSI (Politique de Sécurité des Systèmes d'Information) en composantes techniques et la mise en place des modèles d'organisation et des processus nécessaires à l'exploitation du SOC.

Cette phase peut également permettre la sensibilisation aux concepts de cyberguerre : il est possible de prévoir une interface dédiée aux démonstrations afin de promouvoir le projet de SOC auprès des directions internes de la même manière qu'un éditeur le ferait auprès d'un client.

Astuce de l'expert

Pour s'assurer d'une bonne implantation et mise à jour, il est indispensable d'avoir une politique de patch management.

Monsieur CP. Expert SOC.

8

MAINTIEN EN CONDITION DE SÉCURITÉ

Au-delà des conditions de sécurité, la phase de maintien en condition de sécurité permet d'assurer que les performances du SOC resteront optimales sur le long terme mais aussi d'analyser les impacts d'une attaque.

Un des meilleurs moyens généralement employés pour évaluer la fiabilité du SOC consiste à mener une simulation de crise.
C'est sans nul doute le meilleur moyen de démontrer concrètement l'efficacité de votre système de protection !

Astuce de l'expert

Faire passer des scripts de hardening permet de vérifier que les serveurs sont bien configurés.

Monsieur GC. Développeur Fullstack Reveelium.

LES CONSEILS DES EXPERTS

PÈRIMETRE DE COLLECTES DES LOGS

Sans logs pertinents, un SIEM est aveugle et le SOC inopérant. C'est pourquoi il est important de collecter un maximum de logs. Cependant tous les logs ne sont pas utiles dans l'analyse. Un SIEM fournit un nombre conséquent d'alertes tout au long de la journée. Les équipes sécurité doivent gérer cette masse importante d'informations et trier les véritables incidents de sécurité, il s'agit de la raison pour laquelle, les organisations doivent se concentrer sur l'analyse des logs de sécurité.

Un travail en amont doit être effectué afin de connaître le périmètre de collecte et d'analyse (Windows, Firewall, Active Directory …).

Pour obtenir un SIEM plus efficace et moins onéreux.

LES OPÉRATEURS SOC SONT UNANIMES POUR DIRE QU'IL EST IMPORTANT DE SE CONCENTRER SUR LA QUALITÉ DES LOGS SÉCURITÉ.

Astuces des experts

La qualité des logs prévaut à la quantité. Ne collectez dans un premier temps que les logs indispensables. En général les firewalls et service d'annuaire sont prioritaires et suffisants pour un réseau d'infrastructure tandis que pour la surveillance web les logs CMS et firewalls/proxys sont prioritaires.

Monsieur DD. Expert SOC Reveelium niveau 1.

75% des attaques complexes (APT, Malware, …) peuvent être détectées avec des sources de logs minimales : les DNS et proxys fournissent quantités d'informations incroyables et utiles.

Madame LB. Datascientist ML Reveelium.

INTÉGRATION RÉGULIÈRE DE NOUVELLES SOURCES DE LOGS

La majorité des offres SOC s'avèrent être incomplètes pour répondre à l'ensemble des besoins. Il est indispensable de veiller à ce que le SIEM intègre régulièrement de nouvelles sources de logs (disposer ainsi de la road map du SIEM). Cependant il ne faut pas se limiter à un SIEM car il ne couvre qu'une partie des attentes. C'est pour cela qu'il est nécessaire d'assembler des solutions complémentaires pour gérer le suivi de la sécurité de son infrastructure de « A à Z ».

Le SIEM est la pierre angulaire du SOC mais il faut le coupler pour l'enrichir à des solutions de détection des vulnérabilités et de surveillance de l'intégrité en continu.

Astuce de l'expert

Pour améliorer la couverture de détection il est pertinent d'intégrer de nouvelles sources comme les IDS/IPS ou analyses Endpoint, mêmes si ces logs ne sont pas indispensables dans un premier temps.

Monsieur CH. Directeur Technique.

SEUILS D'ALERTES PERSONNALISÉS

Le fait de connaître le niveau de risque des différentes cibles et leurs vulnérabilités permet de trier et de prioriser efficacement les alertes remontées par le SIEM. Par exemple, s'il s'agit d'une anomalie sur un serveur sans vulnérabilité connue et non critique, la priorité est réduite et les équipes de sécurité peuvent se concentrer sur des tâches plus importantes.

C'est pourquoi les seuils d'alertes doivent s'adapter à l'entreprise afin d'éviter au maximum les faux positifs.

On observe communément 4 niveaux de maturité dans les capacités de détection d'un SOC :

Alertes unitaires : évènement unique jugé suspect (par rapport à des seuils ou de par sa nature même) : connexion d'un compte administrateur à minuit.

Alertes agrégées : plusieurs évènements dont la somme est jugée suspecte (sur une fenêtre de temps ou pour une même machine) : multiples tentatives de connexions échouées sur 30 machines différentes en 10 minutes.

Alertes corrélées : plusieurs évènements dont l'orchestration laisse penser à une attaque cohérente : Une alerte anti-virale sur un poste suivi d'un scan de ports internes et d'un flux anormalement volumineux de données sortantes = intrusion probable.

Analyse comportementale : apprentissage du comportement usuel du réseau et de ses variations normales (souvent via un outil de machine learning) pour distinguer tout comportement mathématiquement atypique (signaux faibles) ou déviance comportementale pouvant trahir la présence d'un attaquant.

Astuce de l'expert

Un Système d'information est un système vivant, qui évolue. Le SOC doit s'adapter continuellement à l'évolution du système.

Monsieur GC. Développeur Fullstack Reveelium.

RESTITUTION SIMPLE ET ERGONOMIQUE

Dans un contexte où la cybercriminalité ne cesse de se réinventer, il est important de pouvoir réagir rapidement face à une attaque.

Une ergonomie simplifiée, un scoring des alertes, une visualisation simple des problèmes dans le réseau et une exploitation des données rapide faciliteront l'investigation et la rapidité de correction.

DÉTECTION DES MENACES AVANCÉES

SEULEMENT 20% DES MENACES AVANCÉES APT SONT DÉTECTÉES PAR LES SOC ACTUELS

Selon la dernière enquête internationale menée par Kaspersky* auprès des responsables d'entreprises, 91% affirment avoir effectivement été attaqués l'an dernier et 17% confient avoir perdu des données financières à l'occasion de ces attaques. 45% s'estiment insuffisamment préparés à faire face à ces attaques.

En outre, même les entreprises qui disposent déjà d'un SOC sont démunies face au péril des nouvelles attaques ciblées ou APT qui restent invisibles pour 80% des SOC actuels.
Elles ne représentent que 1% des attaques*, mais ce sont indubitablement les plus coûteuses pour les entreprises. Deux raisons expliquent cette cécité des SOC traditionnels. La première n'est pas technique ; c'est essentiellement un problème d'organisation et d'humain.

ATTENTION À VOS CONTACTS

Le succès du Cloud Computing est maintenant avéré sur tous les marchés, y compris en France. Les entreprises ont de plus en plus recours à des applications Saas ou des services Iaas ou Paas. Face à ce phénomène, le SOC choisi devra être capable de s'interfacer avec ces tiers et cela pose le problème de l'accès aux données de fonctionnement de ces services Cloud. En effet, le prestataire Cloud doit accepter de partager ses évènements avec l'opérateur du SOC, que celui-ci soit externalisé ou pas. Quand une entreprise fait le choix d'une technologie Cloud, elle doit absolument s'assurer par contrat d'avoir l'accès à ses données de supervision. Des clauses contractuelles doivent garantir cet accès ainsi que préciser les conditions techniques de celui-ci. L'entreprise qui ne prend pas ces précautions pourrait devoir faire face à des délais supplémentaires dans la mise en place de son SOC, voire même, être contrainte d'utiliser les solutions de son fournisseur de Cloud si celui-ci refuse de partager ses données.

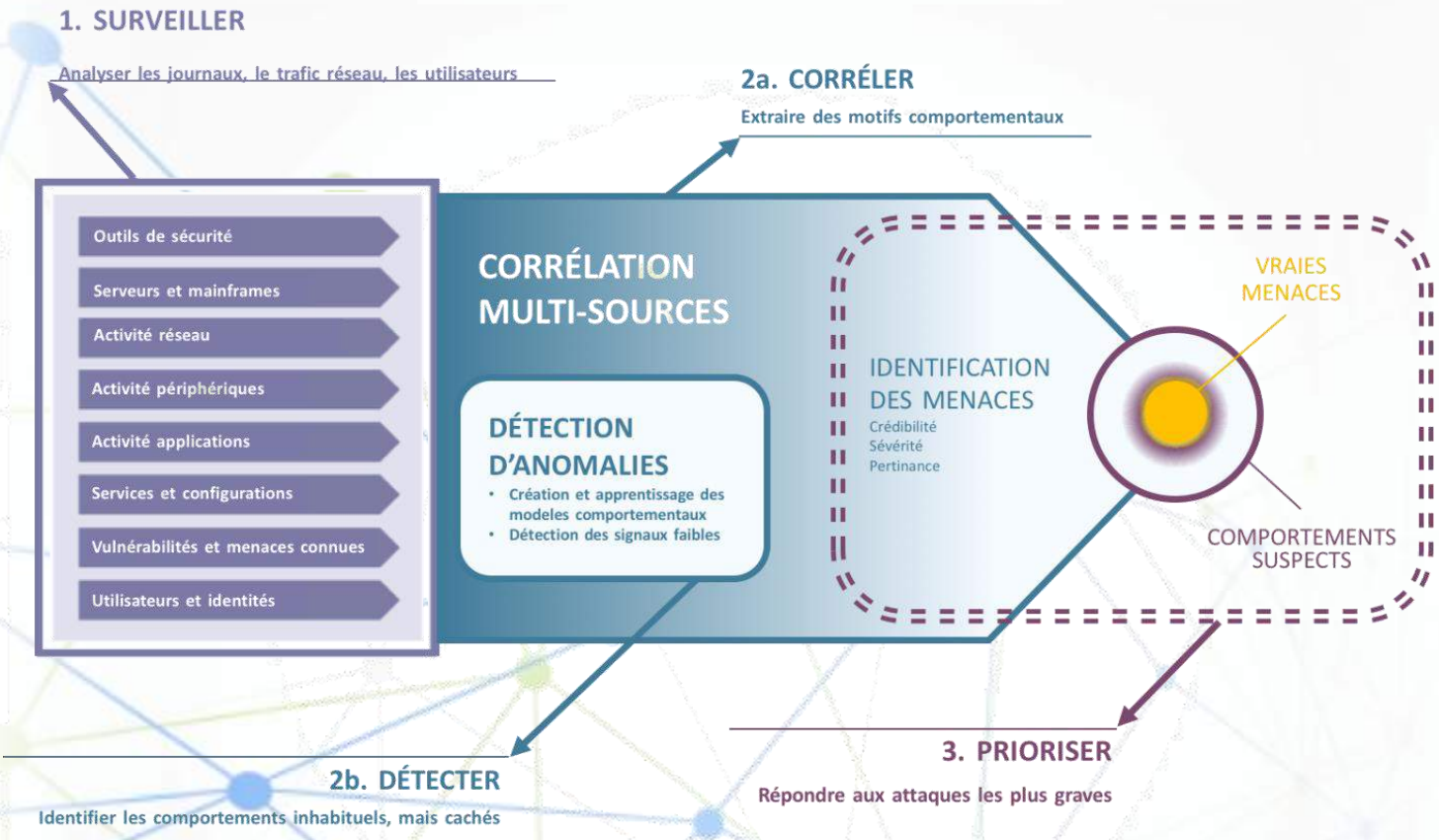
Lorsque des processus de supervision sont en place, ceux-ci sont peu ou mal suivis et présentent des incertitudes : qui prévenir chez le client en cas d'alerte ? Une seconde raison est de nature technologique. Les SIEM actuellement mis en œuvre par les entreprises s'appuient sur la technologie des signatures ou scénarios. Cette approche existe depuis maintenant 20 à 30 ans, une technologie éprouvée mais qui n'est capable de détecter que les attaques déjà connues et reste impuissante face à un nouveau malware, un cryptolocker, une fuite de données ou une attaque ciblée qui exploite des techniques inconnues du grand public.

*The Kaspersky Lab Global IT Risk Report, 2018.
*Corporate IT Security Risks Survey 2016, Kaspersky Lab and B2B International

ANALYSER LES SIGNAUX FAIBLES

Créer de nouvelles règles à chaque nouvelle attaque signalée par une entreprise, c'est aussi prendre le risque qu'il soit déjà trop tard. Il faut être capable de détecter le signal faible dès le moment de l'arrivée du malware ou lorsque celui-ci commence à se propager latéralement. L'important est de le repérer avant qu'il ne s'active. Pour y parvenir, on ne peut s'appuyer sur des motifs, il faut toute l'expérience de l'analyste pour déceler ces signaux ; or les volumes de données à analyser sont tels que l'humain ne suffit plus, une seule solution est possible, c'est l'analyse comportementale via l'intelligence artificielle. Après une phase de profilage des ressources informatiques de l'entreprise, le Machine Learning va être capable de repérer par exemple le poste de travail dont le comportement est anormal. Cette approche permet de détecter ces signaux faibles avec très peu de données au départ.

A partir de ces signaux faibles, il est possible de créer ce que l'on appelle des schémas de menaces, des schémas qui sont aujourd'hui très bien normés à l'image de la base MITRE qui détaille ainsi des schémas de menace à grande échelle. Grâce à cela, lorsqu'on détecte un ensemble de signaux faibles, on est capable de dire par exemple, si on a affaire à une attaque de type cryptolocker ou à une extraction de données.



LES BRIQUES ESSENTIELLES DU SOC

LE SIEM

Le SIEM (Security Information Event and Management) est l'outil central des équipes d'un SOC. C'est cette plateforme vers laquelle convergent toutes les données générées par l'infrastructure informatique. Ce logiciel réalise les corrélations d'événements afin d'identifier d'éventuelles attaques. Néanmoins, si le SIEM est indispensable dans le fonctionnement d'un SOC au quotidien, ce n'est qu'une de ses composantes et les analystes doivent utiliser plusieurs autres outils afin de garantir un niveau de sécurité optimal du système d'information.

Astuce de l'expert

Un bon SOC n'est pas intrusif et impactant, il ne récupère pas l'information, il la collecte.

Monsieur JV. Redteam malware expert.

LA BRIQUE DE MACHINE

« La brique de Machine Learning » devient de plus en plus indispensable dans l'efficacité du travail des équipes d'analystes. Rares sont les opérateurs de SOC à réellement maitriser cette technologie et c'est clairement un critère de choix déterminant dans le choix de son prestataire ou de sa solution SOC.

LA THREAT

La Threat Intelligence va permettre d'aller au delà de la seule corrélation de données captées dans l'infrastructure de l'entreprise. En effet, elle va également s'appuyer sur des données externes, qu'il s'agisse de bases de connaissances internationales telles que celles maintenues par Cisco, Trendmicro, etc. qui centralisent des informations permettant d'affiner et de qualifier une alerte. Ces informations peuvent être issues du Darknet, de Blacklists, etc.

Astuce de l'expert

L'IA et le ML ne fonctionnent pas seuls et de manière autonome, il est indispensable d'avoir une équipe d'expert qui corrèle.

Monsieur CP. Expert SOC ITrust.

LE SCANNER DE VULNÉRABILITÉ

Le scanner de vulnérabilité fait aujourd'hui totalement partie de la panoplie d'outils indispensables dont doit disposer le SOC. C'est cet outil qui va permettre d'auditer régulièrement les différentes briques du SI sur toute sa surface d'attaque et prendre des mesures correctives si des vulnérabilités apparaissent suite à la découverte de nouvelles failles ou lors de l'installation de nouveaux équipements ou logiciels.

LES OUTILS D'ALERTING

Les outils d'alerting doivent être déployés ou directement inclus dans le SIEM.
Ils s'appuient sur un moteur de Workflow et d'orchestration afin de gérer les alertes et les incidents remontés par le SIEM au niveau du prestataire de SOC, mais aussi au sein de l'entreprise, etc. Il est capital de savoir où en est l'analyse et la qualification de l'alerte.

LES DASHBOARDS

Les Dashboards sont souvent intégrés aux plateformes SIEM, de plus en plus personnalisés en fonction des besoins spécifiques de chaque entreprise et notamment pour répondre aux besoins de conformité auxquelles elles sont soumises.
En parallèle à ces tableaux de bord dédiés à la conformité, les smartphones et les tablettes numériques sont de plus en plus exploités tant pour l'alerte immédiate que pour diffuser des données relatives à l'état de sécurité du SI.

EN OPTION

Les IDS (sondes de détection d'intrusion) ainsi que les logiciels de protection Endpoint peuvent eux-aussi alimenter les SOC de données pertinentes. Il est possible, notamment via des agents placés sur les postes de travail, d'élargir le champ de surveillance du SOC. Attention toutefois, l'impact peut être fort sur la production. Cependant certaines entreprises optent pour cette solution pour disposer de données complémentaires afin d'alimenter leur SOC.

ORCHESTRATION
ET
THREAT INTELLIGENCE
L'AVENIR DU SOC

L'orchestration reste un domaine encore peu mature dans les SOC actuels. Rares sont les acteurs à avoir déployé des solutions complètes à l'heure actuelle mais c'est incontestablement un domaine où des innovations vont apparaître au cours des années à venir.
Le volet workflow porte sur la méthodologie de gestion des alertes, l'affectation du traitement aux différents analystes ainsi qu'aux procédures d'escalades en interne ou en externe.

Un deuxième point est de pouvoir définir a priori comment l'architecture applicative et l'infrastructure vont réagir à la détection d'une attaque. Ainsi, l'orchestration va permettre de demander aux firewalls de bloquer l'attaque en fonction des éléments qui ont pu être collectés sur l'incident de sécurité. De même que les WLAN, les switchs vont être reconfigurés par orchestration afin de contenir l'attaque.

C'est un domaine à la fois très porteur en termes de progrès mais très sensible car ce sont des ressources critiques de l'entreprise qui peuvent être concernées. C'est la raison pour laquelle il est absolument nécessaire d'intégrer une intervention humaine dans ce type d'orchestration technique afin de valider la réaction à incident et de ne pas bloquer la production et le fonctionnement de l'entreprise.

Il est absolument nécessaire d'intégrer une intervention humaine dans ce type d'orchestration

Astuce de l'expert

Les principaux problèmes rencontrés dans les SOC sont des problèmes de communications entre les équipes SOC / Clients / Experts / Redteam / Equipes d'infogérance / Direction : Effets tunnels, conflits dus aux intérêts différents, infogérants qui se considèrent surveillés et remis en question, différentes perceptions des priorités entre la direction et les équipes techniques, ...
Aligner tous ces intérêts et traiter ces problèmes de communication résoudront 90 % des problèmes les plus courants.
Monsieur CH. Responsable qualité ITrust.

Actuellement tous les fournisseurs d'équipements réseaux et de briques de sécurité ont implémenté des API dans leurs produits afin de rendre ceux-ci pilotables par logiciel mais l'orchestration de la sécurité n'en est encore qu'à ses prémices.

Une véritable orchestration nécessite de placer l'humain dans la boucle de décision et ne doit pas se limiter à réaliser des appels automatiques à des API. Ce type de framework de communication est encore rarement mis en place.

Il est aujourd'hui difficile d'imaginer comment ces orchestrations vont évoluer à l'avenir, et notamment de savoir si, dans le sillage de l'approche SDWAN (Software Defined Wide Area Network), les entreprises laisseront les logiciels piloter leur sécurité informatique sans intervention humaine. Actuellement bien peu de DSI sont prêts à laisser des algorithmes piloter automatiquement la sécurité de leur système d'information.

DIFFÉRENTS MODES DE COMMERCIALISATIONS

Les entreprises ont à leur disposition toute une gamme de modes de commercialisation afin de mettre en place leur SOC. Le cabinet Gartner en a formalisé 6 grands types. Le SOC peut être déployé non seulement en interne sur un mode on-premise, mais également dans le Cloud sur un mode Saas, ou encore en mode hybride. Certains optent pour un mode externalisé sachant que dans ce dernier mode la plateforme logicielle et les données peuvent être hébergées chez le client, mais la gestion de la plateforme peut être confiée à un prestataire.

LES 6 MODES DE COMMERCIALISATION

Le Gartner a défini 6 grands types de SOC, selon leur mode de commercialisation et leur implémentation technique :

SOC Hybride : *Certaines tâches du SOC sont déléguées. Les entreprises qui disposent de leur propre SOC, assurent elles-mêmes le support de niveau 3. Des équipes externes réalisent les analystes forensic et les tâches de threat intelligence que les organisations ne peuvent pas réaliser elles-mêmes.*

SOC SaaS : *SOC livré en tant que Software*

SOC Virtuel *: SOC ne s'appuyant que sur des ressources IT et humaines mutualisées chez le MSSP (Managed Security Service Provider).*

SOC dédié : *Le SOC est hébergé sur les infrastructures de l'entreprise qui lui dédie des ressources IT et une équipe d'exploitation.*

SOC Intelligent : *SOC qui intègre de nouvelles fonctions telles que la Threat Intelligence, la réponse à incidents.*

SOC Marque Blanche : *SOC utilisé par les distributeurs et commercialisé sous leur propre marque.*

*Security Operations Centers and their Role in Cybersecurity, Communiqué Gartner, 12 octobre 2017

MUTUALISER LES RESSOURCES

On constate fréquemment la nécessité pour les entreprises d'externaliser l'équipe technique car il faut de nombreux profils techniques différents pour opérer efficacement un SOC. Peu d'entreprises peuvent mobiliser un grand nombre de ressources dans un SOC qui, en outre, doit être opéré idéalement en 24/7.

Mutualiser les ressources est donc une solution très fréquente dès lors que l'on veut disposer d'un SOC pour un budget raisonnable.

INTERNE OU À DISTANCE

Une autre tendance forte consiste à maintenir les données dans l'enceinte de l'entreprise. Les données restent dans les limites de son SI et celles-ci sont exploitées à distance par l'équipe du partenaire SOC de l'entreprise ou un mix de l'équipe de l'entreprise et de celle de son partenaire.
Techniquement il n'y a pas véritablement de contrainte à conserver en interne ou exporter les données chez un prestataire de SOC externe. Des tunnels VPN permettent de sécuriser tout les échanges de données. Il s'agit essentiellement d'une décision interne liée à la stratégie de l'entreprise vis-à-vis du Cloud en général ou bien une contrainte réglementaire.

UNE OFFRE COMPLÈTE DE SOC

Quoi de mieux pour illustrer les missions et objectifs d'un SOC que de présenter le SOC d'ITrust, au travers de ses actions quotidiennes.

EXEMPLE DE SOC NOUVELLE GÉNÉRATION

UNE VISION ET UNE SUPERVISION DE VOS SI, …

Le SOC mis en place et/ou opéré par ITrust permet d'optimiser la cyber-protection des entreprises pour leur assurer la continuité de leurs activités quotidiennes. Le cadre de la conformité règlementaire est également pris en compte s'il s'avère nécessaire. Au travers d'une interface graphique claire et personnalisable les utilisateurs peuvent donc avoir une vision précise de la supervision de la sécurité des serveurs, routeurs, applications, bases de données, sites web… L'équipe d'ITrust est composée d'analystes expérimentés possédant des compétences transverses qui surveillent et analysent les alertes des clients.

UN SOC MANAGÉ

Le SOC qu'ITrust met en place peut-être un SOC managé par les clients, l'un de nos partenaires ou par ITrust.

Ce mode de fonctionnement peut être évolutif, voir hybride, permettant la montée en compétence ou le recrutement d'analystes.

DES SOLUTIONS

L'offre SOC d'ITrust repose sur de l'outillage logiciel, des procédures, du reporting et notamment sur les technologies développées par la société : IKare (solution de management des vulnérabilités en continu qui détecte les failles de sécurité de vos applications web, systèmes d'informations, sites internet …) et Reveelium (moteur d'analyse comportementale permettant de détecter tous les comportements malveillants.).

UNE INTELLIGENCE ARTIFICIELLE

La solution Reveelium est un point fort du dispositif : elle permet à ITrust d'enrichir ses scénarios de corrélation et d'être plus pertinente dans ses analyses. L'Intelligence Artificielle permet de détecter les cyberattaques inconnues qui pourraient toucher vos équipements.

DES REPORTING

Les procédures et reporting ont une place centrale dans les tâches d'analystes SOC : elles vont de la classification des alertes, aux procédures d'escalade, notifications du client par mail/SMS/téléphone en cas d'anomalie, procédure d'investigation sur incidents aux rapports d'incidents ou rapports hebdomadaires/mensuels/annuels et aux procédures de veille (CERT, Darknet).

Pour en savoir plus sur les actions mises en place par le SOC d'ITrust, visitez le site internet où tous ces points sont plus amplement développés.

NÉCESSITÉ D'UN SOC INTERNE OU EXTERNE

Face à la montée spectaculaire du risque d'attaques informatiques, la mise en place d'un SOC, qu'il soit en interne ou en externe, est désormais fortement recommandé pour assurer une défense efficace des actifs de l'entreprise.

Il permet de se concentrer sur le cœur de métier avec la mise en place d'une gouvernance de la sécurité, la définition d'une architecture de la sécurité, la surveillance en temps réel de vos actifs, tout en alertant en cas d'incidents.

Astuce de l'expert

L'attaque Wanacry n'a notamment pas été détectée par de nombreux SOC en 2017 en raison du trop grand nombre d'alertes et de faux positifs. Au sein d'ITrust nous avions détecté le malware un jour avant son activation grâce au scoring remonté par l'intelligence artificielle Reveelium. Nous avons eu à traiter 2 menaces scorées au lieu des 233 alertes classiques. Ce qui nous a permis d'intervenir dans un temps record et mettre en quarantaine la malveillance, évitant ainsi l'attaque chez nos clients et partenaires.

Monsieur CH.

ITRUST

Créée en 2007 autour d'un noyau dur d'experts en sécurité informatique, ITrust apporte à ses clients une forte expertise et des solutions innovantes qui permettent d'augmenter de manière significative et continue le niveau de sécurité dans le temps.

Reveelium est une solution unique, au croisement de la cybersécurité, du Big Data et de l'intelligence Artificielle, pour détecter les menaces plus furtives et sophistiquées. Aujourd'hui couplée à son Centre Opérationnel de Sécurité (SOC), Reveelium permet de détecter les menaces avancées en continu.

ITrust et Reveelium ont reçu le label France Cybersecurity, le Trophée de l'innovation décerné lors de la 5e édition de l'IT innovation Forum, le Trophée de l'international du Numérique et le Prix Technology Fast 50 Deloitte. ITrust a également été élue "Start-up à suivre " par GPBulhound dans son rapport Technology Predictions.

Deloitte. Technology Fast50

FRANCE CYBER SECURITY

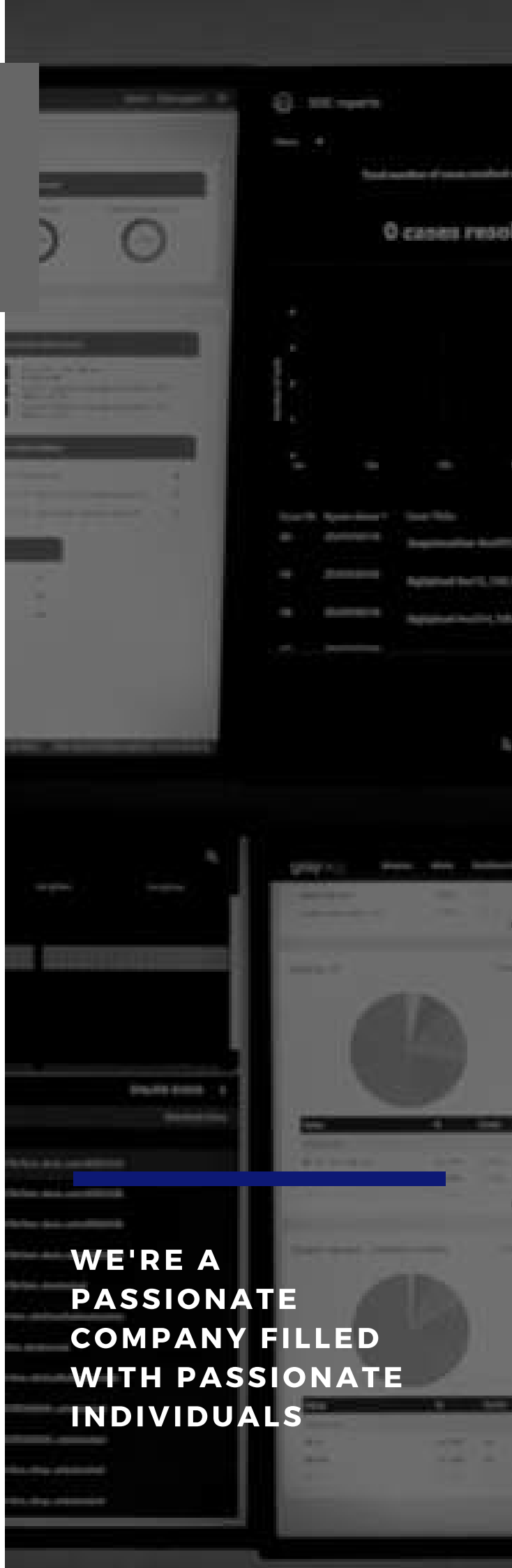
GP. Bullhound

ITrust
CYBERSECURITY AS A SERVICE

SIÈGE SOCIAL
55 AVENUE L'OCCITANE, 31670 LABÈGE, FRANCE

BUREAU INTERNATIONAL
24 RUE FIRMIN GILLOT, 75015 PARIS, FRANCE

TÉL : +33 (0)567.346.781
EMAIL : SALES@ITRUST.FR
WWW.ITRUST.FR



WE'RE A PASSIONATE COMPANY FILLED WITH PASSIONATE INDIVIDUALS