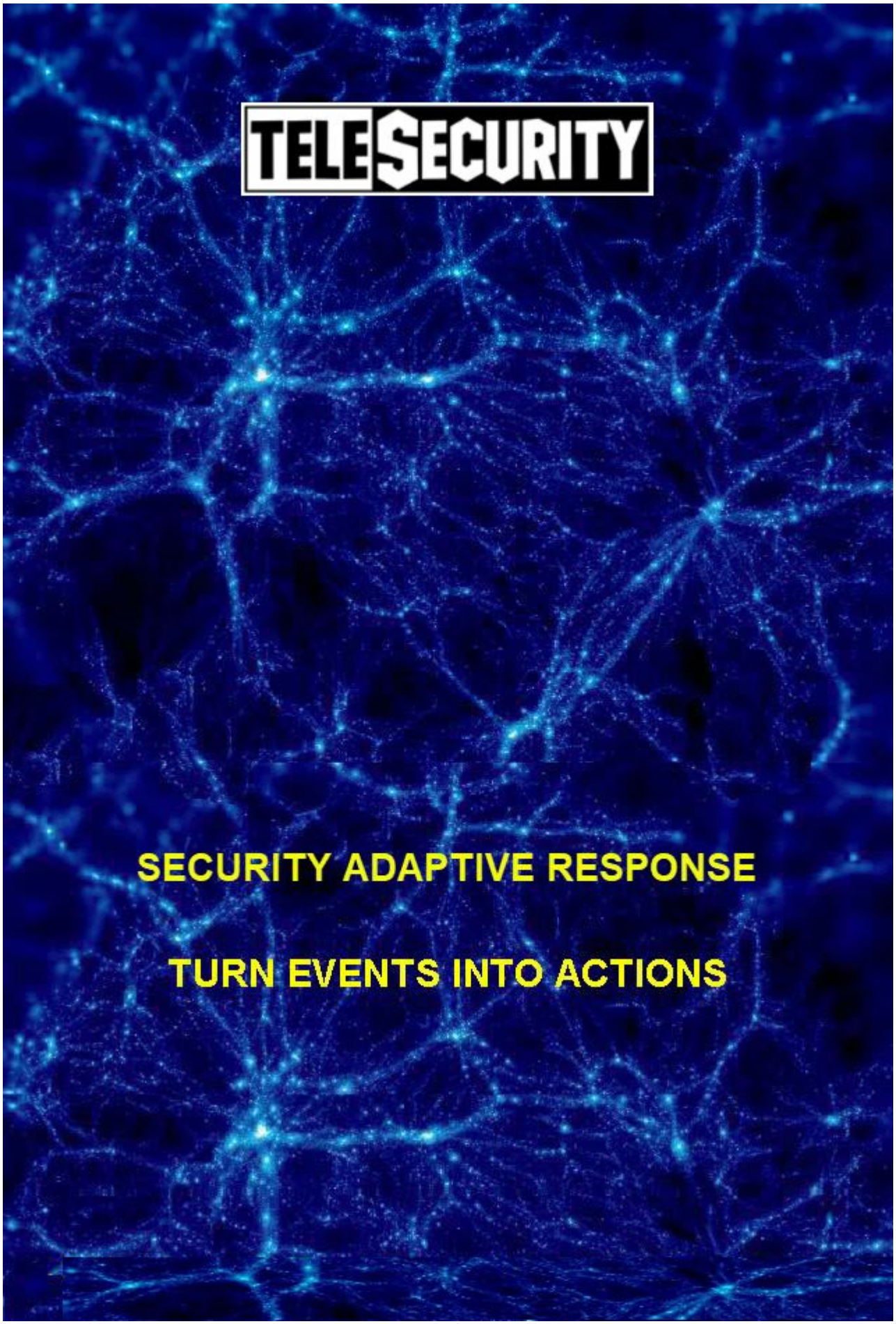

TELESECURITY
SECURITY ADAPTIVE RESPONSE
TURN EVENTS INTO ACTIONS

PRESENTATION DE L'OFFRE TELESECURITY

De nos jours, vos données sont partout, sur vos PCs, vos Smartphones, vos Serveurs, vos Clouds, chez vos Fournisseurs de services, et en transit. Les besoins de Cyber Sécurité des entreprises ont bien évolué.
Il y a nettement plus d'expositions aux risques :

- Accès Internet, Accès Distants, Nomadisme, e-Commerce, SaaS (Software as a Service), Télé-Travail, Cloud Privés, Cloud Publics, IaaS, Hébergement, Remote Control, IoTs, etc.

Il y a nettement plus de menaces chaque jour et ces menaces n'ont pas de contraintes horaires :

- Ransomwares, APT, Phishing, Virus, Malwares, DDOS, Botnet, Clickjacking, Cookie Poisoning, DNS Spoofing, Darkweb, Crypto Lockers, SQL injection, XSS Scripting, Intrusions, Session Hijacking, etc.

Il y a nettement plus de systèmes de protection :

- Firewall, Proxy, Anti-Virus, SandBox, WAF, Authentification, EndPoint Protection, Bastion, CASB, IDS, IPS, Identity Management, Sniffers, Filtrage URLs, Passerelle de Messagerie, DLP, SIEM, etc.

Il y a nettement plus de changements à réaliser, donc plus d'erreurs possibles, et plus de failles de sécurité :

- Migration des VMs, mises à jour des OS, des applications, des browsers, des certificats, des équipements sécurité, des Micro-Services, des IPs réelles et virtuelles, des droits et des privilèges d'accès, etc.

Il y a nettement plus de réglementations à gérer :

- RGPD, LPM (OIV), NIS (OSE), Réquisition Judiciaire, Assurances Professionnelles, ISO-27xxx, PCI-DSS, Conformité Règlementaire Métier, etc.

Il y a nettement plus d'évènements à traiter :

- Incidents utilisateurs, exploitation, alertes systèmes et applicatives, Logs, Vulnérabilités à patcher, etc.

Pour couronner le tout, il y a une pénurie de compétences informatiques :

- Manque criant d'ingénieurs informatiques en général, et encore plus d'ingénieurs en sécurité informatique sans parler des experts... Qui dit pénurie dit inéluctablement ressource quasi impossible à trouver, et si jamais vous la trouvez les coûts pour l'acquérir et pour la garder sont exorbitants.

De nos jours, il est devenu évident que même les technologies de cyber sécurité les plus sophistiquées ne suffisent pas toutes seules à vous protéger. Pour preuves, toutes les attaques destructrices qui ont eu pour cibles en 2020 les Bouygues, Sopra Steria, Orange, Garmin, Spie, Canon, Target, Carlson Wagonlit, MMA, et autres victimes. Il manque clairement des maillons clés qui sont la Surveillance, l'Adaptation, et le Contrôle.

L'ANSSI a publié une étude en 2019 révélant qu'il y a en France 4760 compromissions de sécurité informatiques par jour, lesquelles ne sont découvertes que dans 35% des cas, et qui n'ont pu être découvertes qu'après 167 jours ! Petite cerise sur le gâteau, l'ANSSI indique que ni les très petites entreprises (TPE) ni les entreprises de taille intermédiaire (ETI) ne sont dans les 35% ! C'est-à-dire qu'elles ne s'en aperçoivent même pas…

Devant ce constat clair, la solution parait simple :

- Il faut superviser sa Sécurité en continu.
- Il faut superviser sa Sécurité par des Experts.
- Il faut déléguer cette supervision à une structure mutualisée spécialisée compétente.
- Il faut souscrire une supervision à la carte en fonction des budgets et des risques encourus.

C'est dans cette optique que le service TeleSecurity a été créé.

Grâce à ce service, nous comblons le maillon manquant de la chaine de défense, le MDR (Managed Detection & Response) pour vous offrir la capacité de savoir, comprendre, prévoir, et agir très rapidement, pour éviter et limiter les conséquences, et renforcer votre sécurité et votre défense au fil de l'eau.

La Sécurité Informatique passe d'abord par la nécessité de diminuer au maximum les failles de sécurité. Les failles de sécurité, ce n'est pas seulement des failles techniques sur les OS, les applications, les équipements, ou l'infrastructure réseaux télécoms, mais c'est aussi des mots de passe par défaut, des erreurs humaines dans les configurations, des répertoires partagés qui ne devraient pas l'être, un personnel indiscipliné ou naïf, etc.

Par définition, si vous n'avez pas de failles de sécurité au sens défini plus haut, vous n'êtes pas vulnérables, et donc vous n'avez pas de problèmes de sécurité. Mais, vu les contraintes de tout ordre, nous savons que cela est impossible à réaliser, et surtout à maintenir dans le temps. Il faudra, malgré tout, être capable de contrôler son environnement un minimum.

Grâce à TeleSecurity, nous pouvons vous aider à améliorer votre capacité de contrôler votre environnement.

A côté de cela, vous avez, en face de vous et autour de vous, toutes les menaces potentielles dont la très grande majorité ne sont pas ciblées contre vous, mais plutôt généraliste ou communautaire. Qui s'y frotte s'y pique !
Si vous êtes précisémment la cible d'une attaque, alors c'est grave et c'est très important de la détecter immédiatement et de la contrer très rapidement. C'est pour cela qu'il faut de l'automatisation et de l'expertise.
Si vous n'êtes pas capable de la prévenir, de la contrer et de l'inhiber, il faudra être absolument capable d'en limiter les impacts le plus possible et le plus rapidement possible. C'est là que l'automatisation rentre en jeu.

Grâce à TeleSecurity, nous pouvons réduire votre surface d'attaque, et limiter la propagation d'une attaque.

Nous mettons à disposition de nos Clients, plus de 28 années d'expérience et d'expertise dans la résolution d'incidents de Cyber Sécurité sur les 200 plus grands comptes en France qui sont confrontés quotidiennement aux situations les plus critiques et les plus complexes, avec la pratique de méthodes, de stratégies, et de technologies de Cyber Sécurité les plus abouties et les plus performantes.

TeleSecurity permet aux entreprises de toute taille de déléguer la supervision de leur sécurité, à une équipe de professionnels en la matière capable de les accompagner, de les renseigner, de les conseiller, de les avertir, et de répondre à leurs attentes à chaque étape de leur évolution.

Grâce à son architecture, TeleSecurity récupère, d'un côté tous les événements émis par les équipements cibles du périmètre surveillé, et de l'autre côté tous les référentiels nécessaires de l'entreprise et toutes les bases de connaissances utiles à la prévention des risques, des menaces, et des vulnérabilités.
Il filtre et trie tous les événements significatifs détectés.
Il analyse les informations déduites de ces événements en temps réel.
Il intègre le référentiel de l'entreprise managée.
Il surveille l'évolution des menaces de Cyber Securité dans le monde et instruit les Cyber Feeds.

Il corrèle les évènements avec les bases de connaissances de nos Cyber Feeds mis à jour en temps réel.
Il enrichit les bases de connaissances, et informe les responsables des événements jugés importants.
Il surveille l'activité globale des systèmes cibles, et alerte le Client en cas d'incident ou de risque majeur.
Il agit préventivement et réagit automatiquement selon les process et les directives standards prédéfinies, ainsi que sur la base des directives spécifiques convenues entre nos Experts et le Client dans un contexte donné.

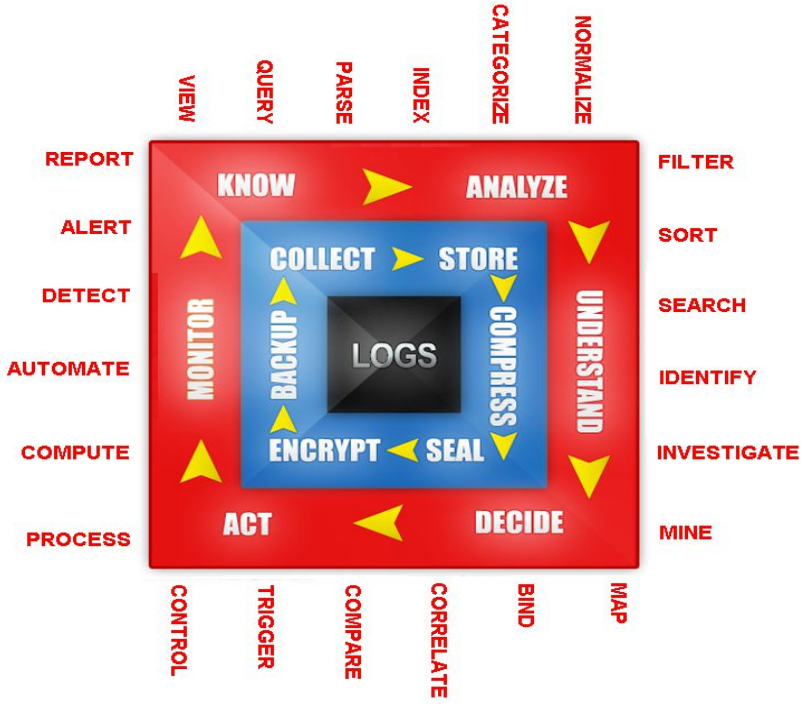
Le service de supervision ne nécessite aucun investissement de la part du Client ni en termes d'achat de matériels, ni en termes d'achat logiciels, ni en termes d'astreinte de personnel. Il n'exige de la part du Client ni formation préalable, ni expertise spécifique, ni intervention spécifique sur ses équipements mis à part la phase initiale de mise en œuvre au cas où le Client souhaiterait des adaptations qui lui seraient propres.

Notre service managé TeleSecurity est une prestation de service récurrente et continue. La prestation est assurée par une équipe d'ingénieurs, d'analystes, et d'experts de la cyber sécurité, alliant compétences et expérience du terrain, capable d'intervenir et d'investiguer sur toutes les couches de sécurisation.

Il permet à nos Clients d'assurer à la fois la supervision de leur sécurité et la gestion de leur système de défense et de le compléter si besoin avec des process et/ou des technologies de sécurité adaptés au contexte.

Le service TeleSecurity est un service de sécurité managé, mutualisé, opéré à distance, disponible en langues française et anglaise, en 24H/24, 7J/7, 365J/an. Ce service peut être étendu avec des prestations à la carte et des interventions spécifiques pour traiter des problématiques plus complexes ou des enjeux spécifiques.

L'organisation des ressources et le périmètre de responsabilité sont revus et adaptés en fonction des besoins du Client et des évolutions des menaces au jour le jour.



Grâce à TeleSecurity, nos équipes techniques sont amenées à :

- collecter, constater, identifier, filtrer, et catégoriser des événements,
- détecter et reporter les anomalies,
- effectuer des investigations poussées suite à un incident,
- enrichir les données brutes et les transformer en informations,
- enrichir les bases de connaissances de référence,
- apprécier des indicateurs et comparer des métriques,
- corréler plusieurs événements ou données de sources différentes,
- auditer des évènements à la lumière des configurations,
- générer des alertes sur événements ou sur seuils,
- prendre des actions préventives en fonction de l'évolution des risques,
- répondre à un événement par une action spécifique appropriée,
- restituer en temps réel les informations,
- produire des tableaux de bord,

- générer des rapports périodiques ou à la demande,
- spécifier des actions de remédiation à une situation,
- activer automatiquement les actions de remédiations,
- ordonnancer automatiquement les travaux,
- etc...

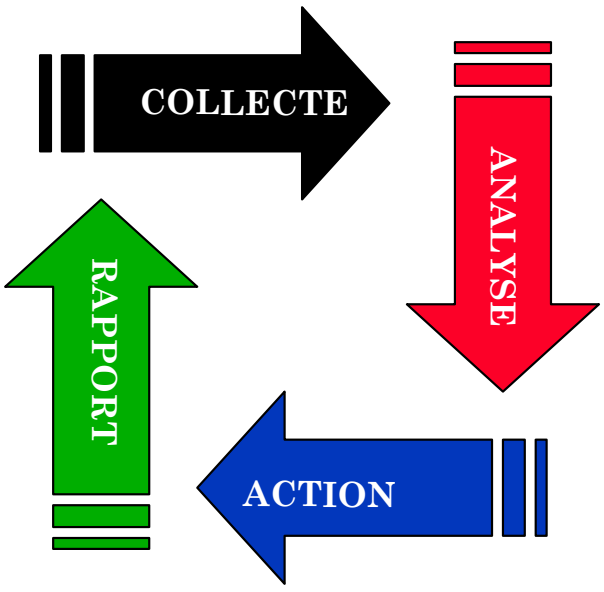
Nos Clients utilisent TeleSecurity pour répondre à plusieurs besoins, à savoir :

- Centralisation et Consolidation des événements
- Conformité Règlementaire
- Gouvernance Métiers
- Gouvernance Informatique
- Gouvernance des Données
- Gestion des traces en temps-réel
- Alerting, Monitoring, & Reporting
- Automatisation des Processus
- Maintien en Condition Opérationnel du SI
- Gestion et Contrôle des Politiques
- Investigations et Corrélations Evènementielles
- Détection des Vulnérabilités, des Risques, et des Menaces
- Gestion et Traitement des Vulnérabilités
- Gestion des Droits et Privilèges des Utilisateurs
- Analyse et Audit des Configurations des Equipements de Sécurité
- Administration et Gestion du cycle de vie des Données
- Audit de l'Activité des Utilisateurs en Temps Réel
- Gestion des Droits et Privilèges des Utilisateurs
- Gestion de l'Intégrité, la Disponibilité, et la Confidentialité des Données
- Qualité de Service et Optimisation des Performances
- Gestion des Evènements et Traitement des Vulnérabilités
- Gestion des Evènements et Traitement des Incidents
- Actions et Réactions sur événements
- Etc.

En tant que prestataire de services de sécurité managés, nous assurons la mise en œuvre, la personnalisation, le déploiement, et le maintien en condition opérationnelle de la supervision des systèmes d'information de nos Clients. Ceci intègre :

- La supervision et la gestion de la Cyber Sécurité, des vulnérabilités, des menaces, et des incidents
- La supervision et la gestion des équipements réseaux data, télécoms, et téléphonie
- La supervision et la gestion des systèmes serveurs, postes de travail, tablettes, et smartphones
- La supervision et la gestion des applications, des sites web, des Clouds Privés et Publics, et des IoTs

Tous les services managés de sécurité sont regroupés sous le nom générique de TeleSecurity.



TeleSecurity est basé sur une automatisation de la quasi-totalité des process et des traitements, allant de la collecte des événements bruts, jusqu'à la génération des actions en bout de chaine soit en prévention soit en réponse à un contexte. On perd tout l'intérêt de la détection si on n'est pas capable de réagir rapidement.

En parallèle à cette automatisation, nous adossons deux services additionnels, à savoir :

- l'expertise technique et l'audit en ligne ou en différé des événements émis par les sources cibles du périmètre client. Cet audit est fait par un pool d'experts qualifiés spécialisés qui vont enrichir et affiner au fil de l'eau les procédures de catégorisation, de détection, et de remédiation des événements remarquables survenus.
- l'exploitation, la gestion, et l'administration à distance des équipements de production du périmètre client qui nécessitent une organisation et des processus spécifiques selon les cas à traiter.

Sur chaque projet TeleSecurity, une équipe de compétences est constituée pour répondre précisément aux exigences spécifiques de l'environnement du Client. A la tête de cette équipe, un responsable de compte est nommé pour assurer l'interface avec les équipes techniques du Client, la gestion complète du projet, et la coordination des équipes contribuant à :

- ✓ l'adaptation de la plate-forme standard pour prendre en compte le périmètre Client
- ✓ la spécification des travaux sur mesure
- ✓ la réalisation des travaux sur mesure
- ✓ l'implémentation des process spécifiques à chaque Client
- ✓ l'activation des services
- ✓ le maintien en condition opérationnelle du service Client
- ✓ la gestion des changements et des évolutions Client
- ✓ la production des rapports et des livrables

Les prestations assurées par nos équipes font l'objet d'engagements formalisés qui s'appuieront sur :

- Un Plan Qualité de Service, pour les conditions organisationnelles et techniques d'exercice des prestations.
- Une Convention de Service, pour la définition des indicateurs de qualité, leurs conditions de mesure et les modes de restitution pour le service continu.
- Une organisation de la relation de type Maîtrise d'Oeuvre/Maîtrise d'Ouvrage qui va permettre au Client de piloter les prestations et de préparer les évolutions.

Le service TeleSecurity est implémenté dans sa version standard après 48H date de commande du Client.
Le service TeleSecurity est facturé à la date de commande pour une durée d'une année renouvelable à sa date d'anniversaire.
Toutes les prestations complémentaires acquises en sus du service TeleSecurity Base Pack sont facturées en sus à la date de commande.

Dans la suite du document vous trouverez la présentation des fonctions TeleSecurity incluses dans le service pack de base ainsi que les options complémentaires que vous pourriez adopter le cas échéant.

THINK FAST

REACT FAST

FONCTIONS DELIVREES PAR LE SERVICE TELESECURITY DE BASE

TeleSecurity Base Pack	Détails	Précisions
CPU Centrale	1	VM Sécurisée Mutualisée
Collecteur Central	1	VM Sécurisée Mutualisée
Nombre de Sources Collectées	10	Configuration des Sources à la charge du Client pour envoyer les traces au point de Collecte. Une source = une @IP.
Types de Sources Supportées	Toutes	Applications, Systèmes, Réseaux, Sécurité, Télécoms, Cloud, Smart Phones, Objets Connectés, Réseaux Sociaux, PABX, etc.
Protocole(s) de Collecte Utilisé(s)	1	Syslog/UDP (18 protocoles disponibles)
Volumétrie Collectée et Traitée	1 To/an	Volume de données non compressées
Stockage des données	1 mois	Standard
Historisation des données	3 mois	Standard
Archivage des données	12 mois	Standard
Conservation de la Preuve	12 mois	Pour un Volume de 1 To/an non compressé
Alertes	10	Alertes définies par le Client ou proposées par nos Experts
Actions & Réactions sur Incidents	5	Actions définies par le Client ou proposées par nos Experts
Corrélations Standard	Oui	Corrélations prédéfinies en Standard sur nos bases de connaissances Threat Intelligence
Corrélations Spécifiques	5	Corrélations définies par le Client ou proposées par nos Experts
Enrichissement par Cyber Feeds	Oui	Accès vers bases de connaissances gratuites intégrées ou renseignées par le Client
Enrichissement statique des données	5	Enrichissements de données définis et renseignés par le Client (données statiques)
Enrichissement dynamique des données	5	Enrichissements de données définis et renseignés par le Client sur fichiers
Rapports Mensuels	10	Un Rapport pour chaque type de source
Jobs Récurrents	5	Standards automatisés
Jobs avec Paramètres Dynamiques	5	Standards paramétrables lancés par l'Utilisateur du Client à la demande
Requête d'Investigations sur Incident	2	Deux requêtes par mois traitées à la demande du Client en HO/JO
Identification Incident Communautaire	100%	Incident défini au sens des RFCs de sécurité sur le périmètre de supervision
Notification d'alerte sur incident	15 minutes	En standard
Demande de Changement	1	Par mois (règle, action, corrélation, rapport)
Accusé de Réception Demande Client	1 heure	Après réception de la demande du Client
Implémentation de la demande	48 heures	Après Accusé de réception (Heures Ouvrées)
Gestion des Restitutions	Standard	Restitutions préconfigurées dans la configuration standard
Gestion des Incidents	Standard	Incidents préconfigurés dans la configuration standard
Accès Portail Web	Permanent	Accès au Portail 24H/24 – 7J/7 - 365J/an
Points de Contacts Client	2	Utilisateurs désignés par le Client
Accès Simultané Utilisateurs	1	Accès au portail Web
Mises à jour du Portail Web	Oui	En temps réel pour les événements et pour les alertes, et Rapports Mensuels sous 48H
Disponibilité des Services Managés	99,5%	Architecture Non Redondée
Disponibilité du Portail Web	99,5%	Architecture Non Redondée
Accompagnement et suivi régulier	Oui	Support Technique Hot Line (Tél.+email)

OPTIONS COMPLEMENTAIRES DISPONIBLES SUR LE SERVICE TELESECURITY

Cryptage des données collectés	Option	DES, 3DES, AES
Intégrité des données collectés	Option	GHOST, MD5, SHA-256, TIGER
Identification d'un incident spécifique	Option	Incident défini au sens du Client sur le périmètre de supervision
Gestion de crise sur incident spécifique	Option	Incident défini au sens du Client sur le périmètre de supervision
Enrichissement par Cyber Feeds Avancées	Option	Accès vers bases de connaissances Editeurs et KDB Professionnelles payantes
Détection des Menaces Avancées	Option	Accès vers bases de connaissances Editeurs et KDB Professionnelles payantes
Rapports circonstanciés	Option	Génération de Rapports d'Audit sur événements remarquables
Détection des Failles de Sécurité	Option	Périmètre cible, durée, contexte à définir
Tests d'Intrusion	Option	Périmètre cible, durée, contexte à définir
Intégration d'un Honey Pot sur site	Option	Pour capturer les flux d'un éventuel attaquant
Gestion des Vulnérabilités	Option	Revues différentielles des Audits, Proposition correctifs, Evaluation des risques, etc.
Gestion des Changements	Option	Détection des changements, Contrôle de cohérence, Maintien en condition opérationnelle, Evolutions, etc.
Analyse des Configurations	Option	Analyse des configurations des sources (Politique de Sécurité)
Audit des Configurations	Option	Audit des configurations des sources (Politique de Sécurité)
Gestion des Configurations	Option	Administration, Exploitation, Modification, Sauvegarde, Restauration, Consignation, Historique, etc.
Expertise sur Evènement ou Incident	Option	Analyse faite par nos Experts dans nos Labs
Rapport d'Expertise Complémentaire	Option	Rapport généré sous 24H sur analyse des événements
Remédiations sur Expertise	Option	Actions correctives jugées nécessaires par nos experts pour éviter, contourner, parer, ou résoudre des incidents potentiels
Formation Audit de Sécurité	Option	Investigations sur Incidents & Attaques
Collecteur sur Site Client	Option	Selon analyse du besoin
Manager sur Site Client	Option	Selon analyse du besoin
Agent de Collecte sur Postes Client	Option	Pull de Traces sur Windows ou Linux
CPU Supplémentaire de Traitement	Option	Selon analyse du besoin
Protocole de Collecte Supplémentaire	Option	Selon analyse du besoin
Augmentation du Périmètre Global	Option	Fonctionnel et Opérationnel (Archivage, Rétention, Volumétrie, Nb de Sources, Agents, Rapports, Alertes, Détections, Audits, etc.)

En fonction des besoins des Clients, des options peuvent être souscrites en sus du Service Pack de Base.
Des critères particuliers sont amendés, complétés, et/ou étendus sur la base d'accords commerciaux spécifiques.

Le service TeleSecurity Pack Base fournit un socle de base de supervision de la Cyber Sécurité pré-paramétré externalisé et mutualisé suffisant pour la plupart des TPE et ETI. Il contient également de base des capacités de personnalisation pour chacun de nos Clients.

Les options complémentaires permettent de personnaliser le service encore d'avantage, de façon agile et maitrisée. Cela peut concerner une extension du périmètre initial de l'environnement à superviser, une extension des capacités fonctionnelles, une adaptation plus forte du service pour répondre aux nécessités du Client, ou même l'acquisition des prestations de services telles que la gestion et l'administration à distance et l'expertise sur site.

☆☆☆☆☆