SECURITY OPERATION CENTER

PRINCIPE GÉNÉRAL

Le SOC (Security Operation Center) d'ITrust supervise tout ou partie de la sécurité d'une organisation. Ainsi, vous vous concentrez sur votre cœur de métier en confiant la cybersécurité de votre système d'information à des professionnels de la sécurité informatique.

Notre SOC effectue la supervision en continue, cela vous permet de :

- Analyser, stocker et monitorer l'activité de vos systèmes d'information ;
- Assurer pour vous, partiellement ou totalement, l'installation, l'exploitation et l'administration de vos équipements.

Ce centre de contrôle de sécurité vous permet d'optimiser votre cyber-protection tout en vous assurant une disponibilité de vos services aux meilleurs coûts et dans le cadre de conformités réglementaires.

ITrust vous assure une sécurité optimisée sur mesure pour vos cyber-incidents afin de :

1. Prévenir

- Monitoring en continu des vulnérabilités,
- Audit des organisations et des systèmes,
- Formation et sensibilisation des collaborateurs.

2. Détecter

- Assurer les fonctions de surveillance, détection, alerting et reporting,
- Détecter et qualifier les attaques inconnues.

3. Traiter

- Disposer d'une force d'action rapide,
- Assurer un service 24/7/365,
- Analyser et investiguer,
- Préconiser des améliorations.

4. Assurer la maitrise des risques et conformité

- **Légale : CNIL, Bale, SOX, RGS, LPM, HADS, OIV, HIPAA ;**
- Spécifiques Santé : Protection des données personnelles et patients, RGS, HADS ;
- Norme : 27001.

ITrust a mis en place les moyens pour superviser la sécurité des infra-structures informatiques au travers de son propre SOC.

Grâce à son SOC, ITrust mets à la disposition de ses clients un système global de centralisation des journaux entièrement intégré à l'infrastructure.

Cette centralisation permet notamment de visualiser les journaux à partir d'une seule interface. Ceci facilite ainsi l'analyse et l'investigation.

POSITIONNEMENT UNIQUE :

- *Managé ou Non Managé*
- *Souverain Français*
- *Déploiement Rapide*
- *Scalable / à tiroir*
- *Multi-tenant*
- *Technologie de machine learning*

AVANTAGES SOC MANAGE :

- *Equipe d'expert à votre service,*
- *Simplifications de la gestion de la cybersécurité,*
- *Evolutivité et mise à jour intégré,*
- *Réactivité et rapidité de service,*
- *Optimisation des coûts.*

DISTINCTIONS ET LABELS :

EXEMPLES DE RÉFÉRENCES CLIENTS :

ARCHITECTURE DE LA SOLUTION

OFFRE SOC DE NOUVELLE GÉNÉRATION

L'offre SOC d'ITrust repose sur de l'outillages, des équipes expertes, des procédures et du reporting.

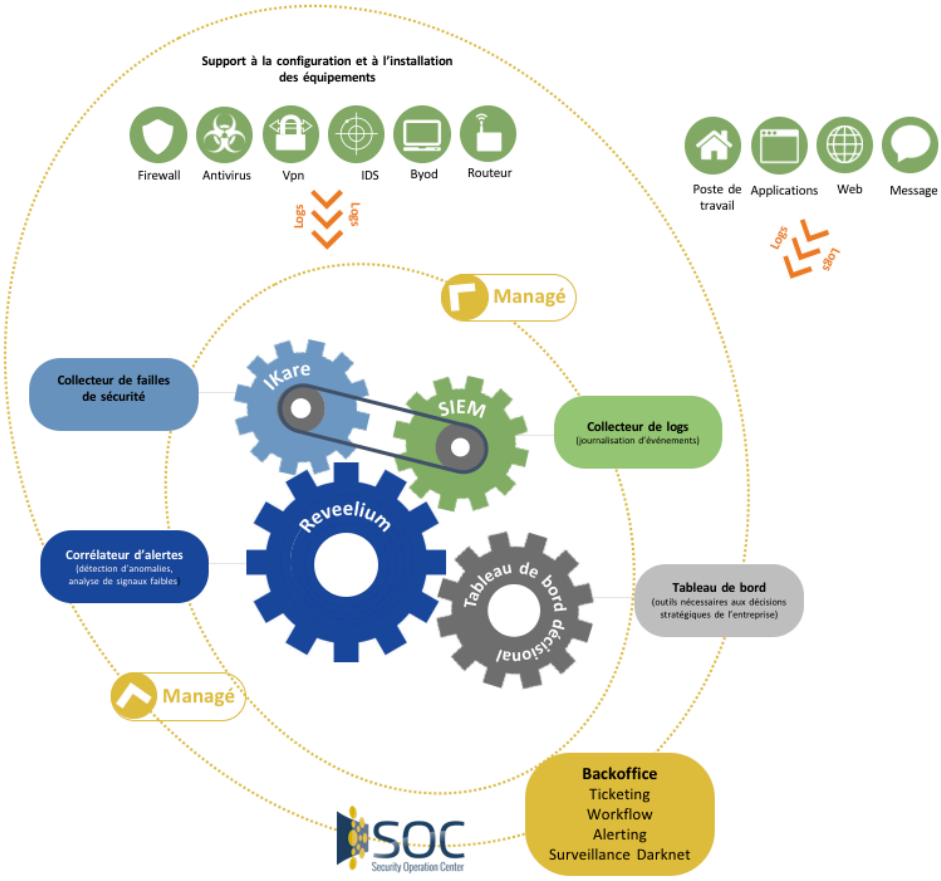
OUTILLAGES

1. IKare

Solution de gestion des vulnérabilités permettant de détecter en temps réel les vulnérabilités des SI, applications web, sites internet. IKare automatise la mise en place de meilleures pratiques de sécurité. Vous augmentez ainsi la sécurité informatique de 90% ; l'outil renforce l'efficacité d'un antivirus ou d'un firewall.

2. SIEM

SIEM (Security Information and Event Management) est une solution permettant de gérer et de corréler des logs en continu. Reveelium peut être facilement ajouté à un SIEM existant, allant plus loin que le simple traitement des journaux.



3. Reveelium

Solution d'analyse comportementale figurant parmi les leader mondiaux et permettant de détecter des APT (menaces avancées persistantes) et des attaques inconnues. Reveelium a été développé pour fournir un système expert de détection d'anomalies basé sur des algorithmes intelligents qu'ITrust a développé depuis 7 ans avec l'appui de trois laboratoires internationaux.

4. Tableau de bord

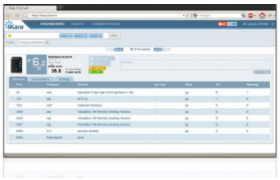
Le tableau de bord automatisé et personnalisé, remonte en temps réel les informations terrain avec IKare Monitoring et permet de croiser les actifs, les vulnérabilités et menaces que rencontre votre structure afin d'établir votre niveau de risque jour après jour.

5. Backoffice

Le Backoffice d'ITrust regroupe l'ensemble des activités de supports, de contrôle et d'administration. Notre backoffice permet une gestion affinée de sécurité avec le ticketing, le workflow, l'alerting et la surveillance darknet.

ARCHITECTURE DE LA SOLUTION

1. IKare



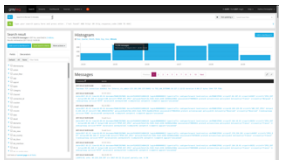
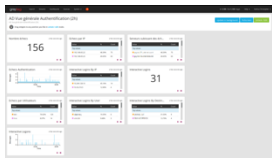

Monitoring de vulnérabilités :

- Identification des vulnérabilités en continu,
- Trending,
- Alerte automatique,
- Veille en sécurité,
- Identification des zones à risques potentiels,
- Recommandations,
- Sécurité des applications,
- Inventaire détaillé des vulnérabilités critiques et non critiques,
- Plan de correction des vulnérabilités critiques.

Managé :

- Étude humaine des alertes et failles,
- Analyse par un ingénieur expert,
- Contact de l'équipe d'exploitation,
- Suivi de gestion de crises,
- Escalade en cas de non traitement d'une alerte critique,
- Intervention en mode jeton de service si nécessaire.

2. SIEM

Corrélation de logs :

- Corrélation intelligente des logs,
- Extraction des données pertinentes,
- Archivage et stockage des événements de sécurité journalisés,
- Alerte en temps réel des anomalies,
- Facilite l'investigation des incidents de sécurité,
- Détection d'intrusions,
- Conformités simplifiées avec les réglementations en vigueur,
- Archivage des données informatiques légales sur 1 ans par défauts et plus sur demande.

Managé :

- Analyse par un ingénieur expert,
- Contact de l'équipe d'exploitation,
- Suivi de l'alerte critique,
- Escalade en cas de non traitement d'une alerte critique,
- Intervention en mode jeton de service si nécessaire.

3. Reveelium


Détection d'anomalies, analyse de signaux faibles :

- Détection des APT, virus et attaques inconnues,
- Détection de comportements déviants au sein des SI,
- Identification de la perte ou l'extraction de données,
- Prévient la saturation de ressources informatiques,
- Alerting automatique,
- Recommandations,
- Plan de correction.

Managé :

- Analyse par un ingénieur expert,
- Intervention en mode jeton de service si nécessaire.

4. Tableau du bord


Maîtrise des risques, conformité à un référentiel :

- Mise en place d'une politique de sécurité,
- Suivi de la mise en place d'une politique de sécurité,
- Inventaire des vulnérabilités et des menaces,
- Contrôle du respect de la politique,
- Aide à la mise en conformité.

Managé :

- Analyse par un ingénieur,
- Intervention en mode jeton de service si nécessaire.

5. Backoffice

- Ticketing
- Workflow
- Alerting
- Surveillance Darknet

FONCTIONS DÉTAILLÉES

EQUIPES & COMPÉTENCES

L'équipe SOC est constituée d'experts hautement qualifiés et dont les compétences sont multiples. Notre équipe met également en place des procédures adaptées afin de réduire les risques de sécurité sur les systèmes d'informations et de faire face aux incidents.

1. Équipe Red Team

- Sécurisation d'assets,
- Analyse de vulnérabilités,
- Audits intrusifs,
- Audits code,
- Audits de configuration,
- Analyse Darknet,
- Analyse malware et attaques,
- Reverse Engineering,
- Investigation et Analyse incident,
- Intervention sur incidents.

2. Équipe Rainbow Team

- Analyse de risque,
- PSSI et compliance,
- Conseil et Accompagnement,
- Formation,
- AMOA, AMOE,
- Architectures de solutions,
- PRA, PCA.

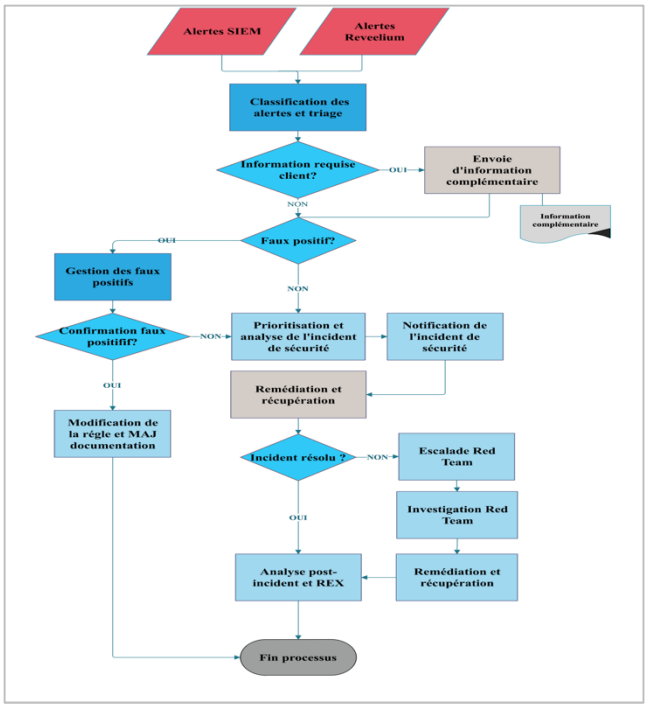
3. Équipe R&D

- Maintenance et mise à jour,
- Développement customisé.

4. Communication & Juridique

Relation avec les institutionnels, états, justice, ANSSI …

PROCÉDURES & REPORTING



Rapport hebdomadaire
Rapport mensuel : indicateurs clés SIEM
Rapport annuel : indicateurs clés (nombres d'incidents, complexité, récurrence …

MODELES LIVRAISON

Le SOC est proposé en mode :

Infrastructure **On Premise** chez le client

En **SaaS** externalisé à la demande

Managé (MSSP) par les équipes ITrust

OFFRES COMPLÉMENTAIRES

SOC OEM : ITrust propose à ses partenaires de commercialiser une offre SOC sous différentes formes.
Le SOC packagé peut être proposé à vos clients en mode supervisé ou non supervisé, utilisable directement par vos équipes.

STRESS TEST SOC : Forte de son expertise en sécurité informatique, la société ITrust est en mesure de tester la capacité de détection des SOC déjà mis en place.

CONTACT

Adresse : ITrust, 55 avenue l'Occitane
31670 Labège Cedex, France

Email : sales@itrust.fr
Tél. : +33 (0)567.346.780

Site : www.itrust.fr