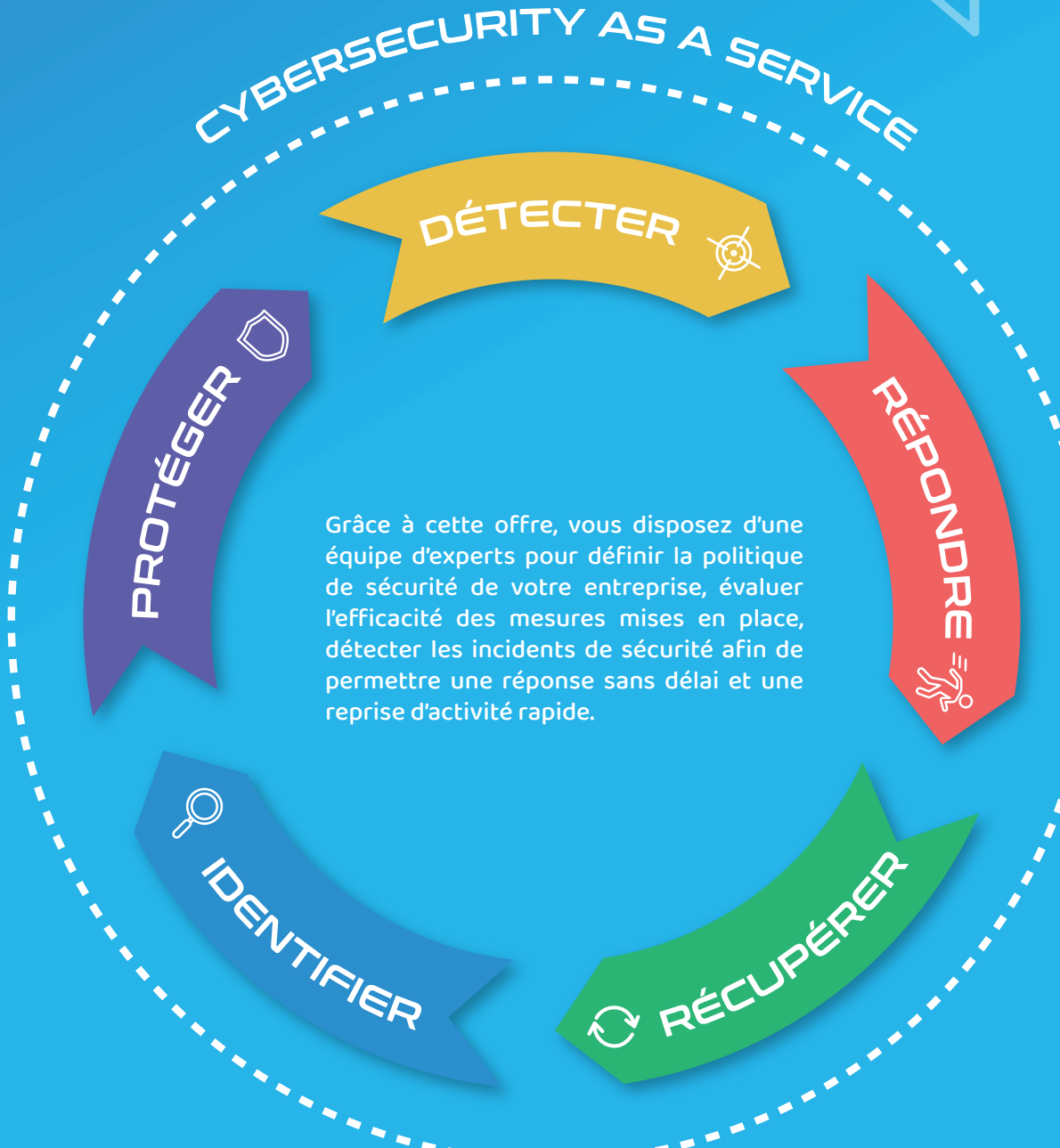
Depuis 2016, Soteria Lab accompagne ses clients pour les aider à protéger leurs activités grâce à la protection de leurs infrastructures numériques.

Pour y parvenir, Soteria Lab s'appuie sur une équipe de passionnés hautement qualifiés et utilise des technologies de pointe.

Notre gamme de services permet de couvrir les 5 fonctions de la cybersécurité :

cybersecurity as a service (CSaaS)

Une prestation clés en main, adaptée aux entreprises de toutes tailles et de tous secteurs d'activité, qui consiste à externaliser l'ensemble de la gestion de la cybersécurité et à la confier aux équipes d'experts de Soteria Lab.



Grâce à cette offre, vous disposez d'une équipe d'experts pour définir la politique de sécurité de votre entreprise, évaluer l'efficacité des mesures mises en place, détecter les incidents de sécurité afin de permettre une réponse sans délai et une reprise d'activité rapide.

DÉTAILS DES SERVICES

01 IDENTIFIER

Pour pouvoir protéger les systèmes d'informations, il faut avant tout être capable d'identifier les menaces et vulnérabilités.

Nous proposons une large gamme de contrôles couvrant les aspects gouvernance (identification des risques et des processus mis en place pour les réduire), mais aussi techniques (identification des choix technologiques et contrôle de leur mise en oeuvre) et humains (identification des cibles potentielles et contrôle du niveau de vigilance).

Ces audits permettent de construire un plan d'action personnalisé définissant les moyens à mettre en œuvre et les mesures de sécurité les plus adaptées aux besoins de votre organisation.

02 PROTÉGER

La protection consiste en la mise en application du plan de sécurisation établi lors de l'étape précédente.

RSSIaaS

Le RSSI externe est le garant de la sécurité des Systèmes d'information. Sa mission première est de définir la politique de sécurité du SI et de veiller à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.

03 DÉTECTER

Pour permettre la sécurisation de vos systèmes d'informations, il est important d'avoir le bon outil pour détecter les actions malveillantes qui pourraient se produire dans votre entreprise.

SOCaaS

Il désigne le Centre Opérationnel de Sécurité (Security Operations Center en anglais). Le SOC comprend :

Des moyens humains : une équipe d'analystes chargée d'analyser les évènements de sécurité et de détecter les incidents de sécurité, c'est-à-dire les évènements pouvant avoir un effet négatif sur les activités de l'entreprise.

Des moyens techniques : les analystes s'appuient sur des sondes permettant de récolter les informations pertinentes sur l'ensemble des équipements du système d'information, mais également des outils d'analyse et de corrélation de données afin de détecter les incidents de sécurité.

04 RÉPONDRE

Lorsque l'on a détecté un incident de sécurité, il est nécessaire de réagir rapidement afin d'éviter que les dégâts ne soient trop importants.

CSIRT

Notre équipe de réponse aux incidents de sécurité informatique (anglais CSIRT) est chargée de gérer les crises d'origine cyber et d'assurer une veille continue autour des cybermenaces. Ses missions sont diverses, et sont réalisées en étroite collaboration avec les équipes SOC et d'audit :

- Préparation du plan de réponse aux incidents
- Exercices de gestion de crise cyber
- Levée de doute
- Réponse à incidents

05 RÉCUPÉRER

Notre équipe CSIRT vous aide lors de la phase de récupération en vous accompagnant lors de la mise en œuvre de votre Plan de Reprise d'Activité et en vous guidant dans la priorisation des services à équipements à restaurer. Nous réalisons également des opérations de nettoyage et de « sanity check » pour s'assurer que l'infrastructure remontée est saine.

FORMATIONS

SENSIBILISATION

Pour accompagner vos équipes, nous proposons une large gamme de formations destinées à apporter une culture de la sécurité à l'ensemble de vos personnels, afin qu'ils deviennent acteurs de la sécurité de vos systèmes d'informations :

E-LEARNING
La formation sur la durée, avec une plateforme permettant d'améliorer l'engagement et la participation de vos collaborateurs.

SERIOUS GAME
L'apprentissage par le jeu, permettant d'intéresser et d'impliquer vos salariés dans différents scénarios pour leur permettre de prendre conscience des risques informatiques et d'assimiler davantage les thématiques.

LES CONFÉRENCES CYBERSÉCURITÉ
Que ce soit pour une conférence à destination de vos clients ou lors d'un événement interne dédié à vos collaborateurs, nous intervenons afin de vous exposer les enjeux de la cybersécurité et de présenter un état de la menace et des bonnes pratiques associées. La présentation est accompagnée de démonstrations techniques permettant d'appuyer le propos.

ATELIERS THÉMATIQUES
approfondissements autour d'un sujet afin de mieux l'appréhender, de partager les bonnes pratiques associées et d'échanger sur les expériences de chacun.

FORMATIONS TECHNIQUES

Ethical Hacking

Formation spécialisée dans la sécurité offensive afin de vous aider à mieux comprendre et à pratiquer les techniques d'attaques. Cela vous permettra d'acquérir les compétences nécessaires pour protéger vos systèmes contre les menaces les plus récentes.

Cyber Range

Le Cyber Range est une plateforme d'entraînement aux attaques, à la défense et à la gestion de crise cyber. Il est destiné aux entreprises souhaitant former leurs employés à la cybersécurité. Ils permettent de revoir les bases, de travailler sur des technologies connues ou inconnues, et de tester des attaques en toute sérénité pour acquérir les compétences nécessaires à la sécurisation des organisations.

Cette solution s'adresse également aux écoles et universités ayant la volonté de former leurs étudiants sur des infrastructures réalistes.

Les scénarios proposés conviendront aussi bien aux débutants souhaitant s'initier aux fondamentaux de la cybersécurité qu'aux professionnels souhaitant s'aguerrir.

contact@soteria-lab.com

https://soteria-lab.com

+33(3) 72 47 05 27

Soteria Lab
71 rue des Cinq-Piquets
54000 Nancy

REJOIGNEZ-NOUS

@soteria_lab

@soteria-lab