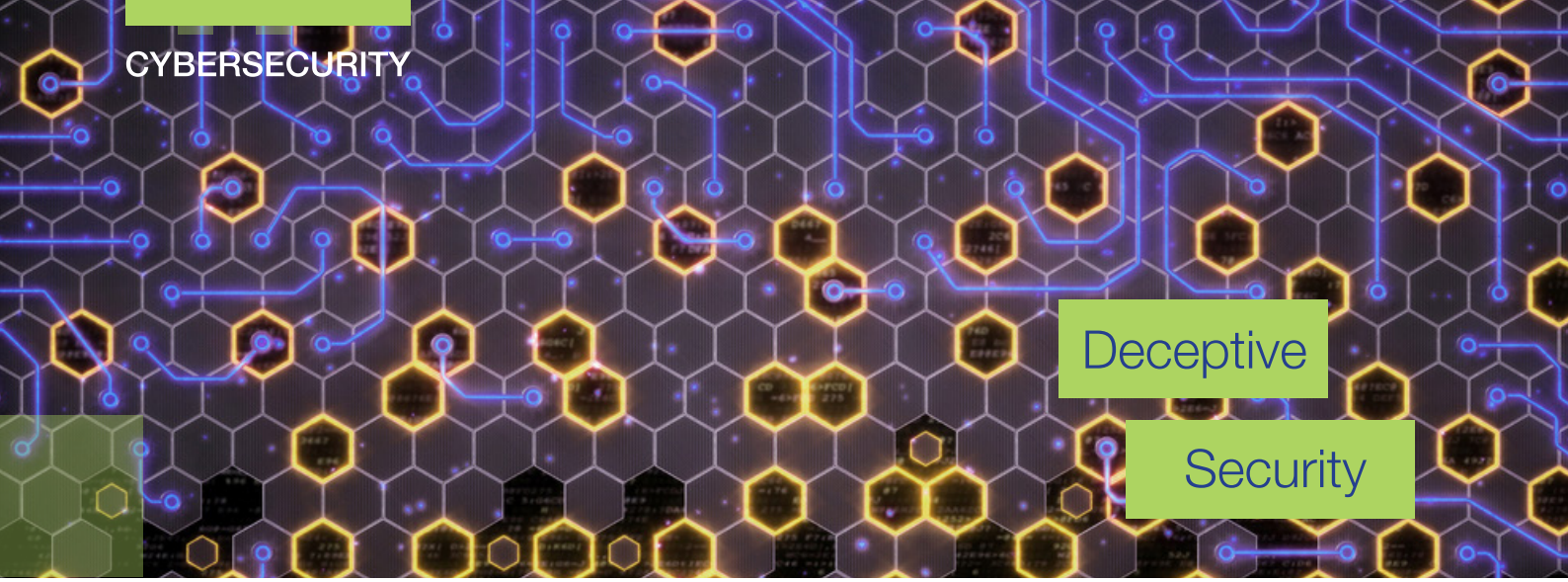


Développez vos capacités de résilience grâce à nos services de Deceptive Security

Les Systèmes d'Informations (SI) des entreprises et institutions font régulièrement face à des tentatives d'intrusion, des cyberattaques et à des malwares de plus en plus sophistiqués. Plutôt que de miser sur un ensemble de solutions complexes, nos services de Deceptive Security permettent de focaliser vos ressources cyber sur des attaques ciblées, difficiles à détecter par des moyens de défense traditionnels.

Un HoneyPot est une réponse pertinente qui permet d'enquêter sur les motivations, outils et méthodes des attaquants tout en préservant la confidentialité, l'intégrité et la disponibilité de vos SI légitimes.

Renforcez vos capacités de détection
Nos services de Deceptive Security ajoutent une couche supplémentaire de cybersécurité grâce à l'utilisation de leurres, pièges et miettes de pain numériques, couplés à une augmentation de la surface d'attaque.

Un HoneyPot permet de faire diversion en attirant un attaquant sur un SI factice afin de le ralentir, d'alerter votre SOC et de collecter des informations. Ces informations peuvent permettre de découvrir des attaques nouvelles et enrichissent les défenses du SI légitime, dans un cycle d'amélioration continue de votre sécurité.

Consolidez vos capacités de réaction
Nos services de Deceptive Security permettent de renforcer vos capacités de réaction face à une intrusion ou une cyberattaque. Ils génèrent une information qualitative et peuvent capturer de nouvelles sortes de menaces qui n'avaient jamais encore été observées.

L'observation des méthodes et outils utilisés par les attaquants sur le HoneyPot permet d'améliorer, à posteriori, les défenses du SI légitime et de maintenir l'activité et les capacités opérationnelles en parallèle.

Nos services de Deceptive Security remplissent trois fonctions essentielles:

PRÉVENTION
en attirant l'attaquant sur les leurres et le HoneyPot

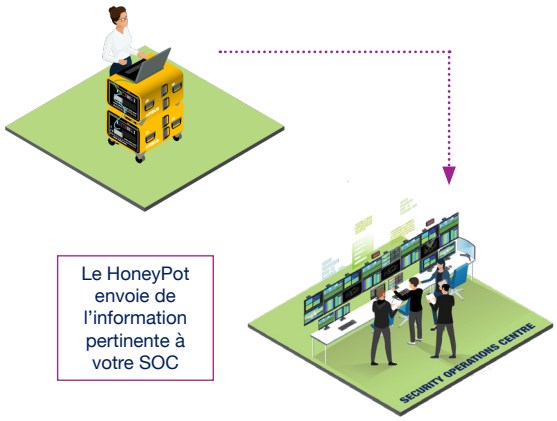
DÉTECTION
en alertant votre SOC en cas d'intrusions ou de menaces

RÉACTION
en collectant de l'information sur l'attaquant pour adapter la réponse

AIRBUS

Une solution de Deceptive Security innovante

- **Attire, détecte et isole** les attaquants menant des opérations ciblées, dont sur des failles encore inconnues
- Intègre un système supplémentaire et interconnecté qui **augmente et accélère la probabilité de détection**
- Déploie des **leurres, pièges et miettes de pain numériques** pour protéger vos systèmes et données
- Permet d'**accroître la compréhension des attaques** observées sur le SI de leurrage puis de répercuter cette connaissance sur le système défensif du SI légitime (amélioration continue)
- Donne la possibilité, en cas de défaillance du système, de revenir, partiellement ou totalement, à la **position nominale de l'architecture**



Qui renforce les capacités de votre SOC

- **Communication simple et rapide** avec votre SOC pour l'alerter directement en cas d'intrusion ou de cyberattaque
- **Améliore la réponse aux incidents** : les leurres sont configurés pour faciliter les enquêtes
- Ajoute une **couche supplémentaire de cybersécurité** à votre SOC

Airbus CyberSecurity fournit des SOC 24/7/365

Des services basés sur la technologie CyberRange

Nos services de Deceptive Security sont rendus efficaces grâce aux **technologies utilisées dans notre plateforme CyberRange** qui permet de **créer un SI de leurrage réaliste et représentatif du SI légitime**. Le HoneyPot CyberRange fait notamment appel à des bots pour simuler de l'activité sur les systèmes dupliqués. Il fait également appel à du machine learning afin de r**enforcer continuellement ses capacités de détection** des menaces potentielles.

- Une topologie informatique avec des services typiques comme l'AD, le pare-feu informatique et les postes utilisateurs
- Des architectures de réseau suivant la norme IEC 62443 et les implémentations réelles

FABRIQUÉ EN FRANCE
MADE IN FRANCE

Contactez nous pour plus d'information

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

ALLEMAGNE
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Allemagne

ROYAUME-UNI
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / Royaume-Uni

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com