Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

La cyber kill chain*

- Qu'est-ce qu'une cyber kill chain ?
- Le cyber kill chain framework** : les 7 étapes d’une cyber kill chain

*Chaîne d'attaque cybernétique

** Cadre de la chaîne d’attaque cybernétique

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Qu'est-ce qu'une cyber kill chain ?

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

→ Définition

La Cyber Kill Chain est un modèle développé par Lockheed Martin qui décrit le processus et les étapes que les attaquants utilisent pour mener une cyberattaque.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

→ Pourquoi un cadre ?

Le cadre de la Cyber Kill Chain (Cyber kill chain framework) sert à comprendre et à analyser les étapes d'une attaque informatique.

/ En identifiant chaque phase de l'attaque, les professionnels de la sécurité peuvent mettre en place des mesures de défense adaptées à chaque étape pour détecter, prévenir ou atténuer les attaques potentielles.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
La cyber kill chain

Le cyber kill chain framework : 7 étapes pour comprendre et contrer les cyberattaques

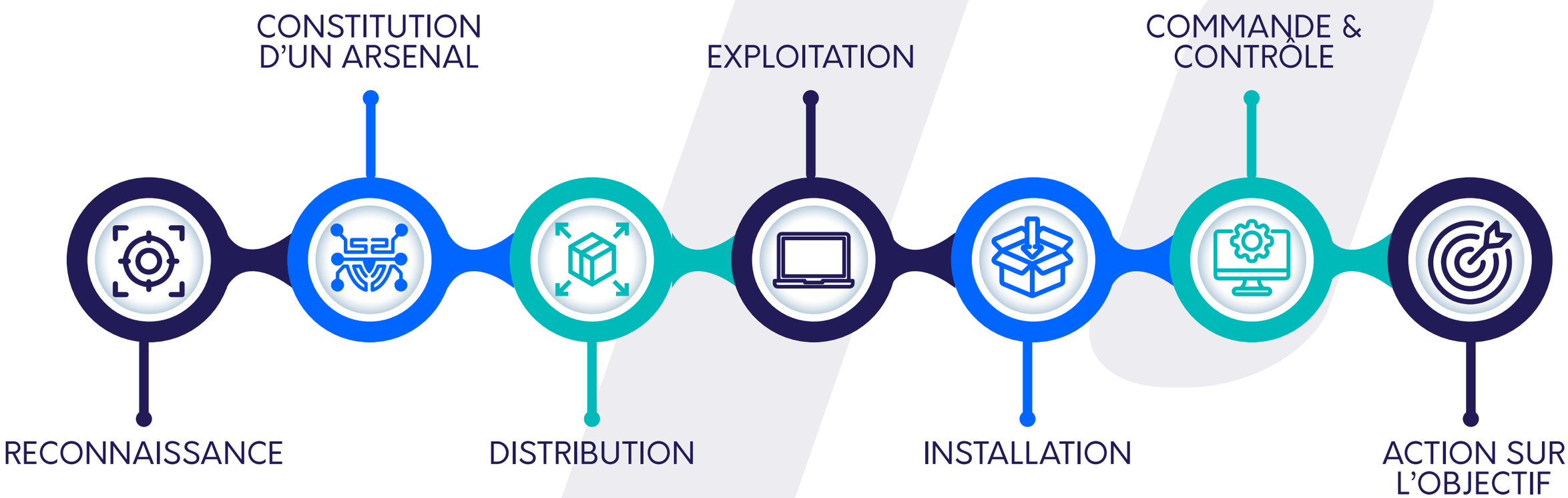
www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
La cyber kill chain

Les phases de Cyber Kill Chain



Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Reconnaissance

La première étape de la Cyber Kill Chain consiste à collecter des informations sur la cible.

Durant cette phase, le cybercriminel commence à identifier et à rechercher des vulnérabilités ainsi que des points faibles à exploiter au sein du réseau de la victime.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Constitution d’un arsenal

Lors de cette phase, l'attaquant se consacre à la préparation des outils spécifiques et des méthodes qu'il utilisera pour mener son attaque. Cela implique notamment la création du logiciel malveillant qui sera déployé dans le cadre de l'attaque.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Distribution

La phase de distribution, dans le cadre de la Cyber Kill Chain, est le moment où un attaquant déploie et transmet le logiciel préparé à la cible.

Utilisation d'e-mails de phishing.

Distribution de clés USB infectées.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Exploitation

C'est l'étape où l'attaquant exploite les vulnérabilités ou les faiblesses identifiées dans le système de la cible, telles qu'identifiées lors des phases précédentes, pour introduire et exécuter le code malveillant qu'il a développé lors de la phase de constitution d'un arsenal (weaponization).

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Installation

Cette phase correspond à l'établissement par l'attaquant d'un accès durable et persistant au système de la cible. Elle intervient après la phase d'exploitation, lorsque l'attaquant a réussi à introduire le code malveillant dans le système ciblé. L'objectif est de permettre à l'attaquant de revenir ultérieurement sans avoir besoin de réexploiter la vulnérabilité initiale.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Commande et contrôle

La phase de commande et contrôle est celle où les attaquants prennent le contrôle à distance d'un terminal ou d'une identité au sein du réseau ciblé. Pendant cette phase, les attaquants se déplacent latéralement dans le réseau, escaladent les privilèges et établissent des canaux de communication sécurisés avec les systèmes compromis. Cela leur permet de diriger à distance des actions spécifiques, de se déplacer à l'intérieur du réseau et de maintenir un accès continu de manière discrète.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

La cyber kill chain

Action sur l’objectif

Dans cette phase, l'attaquant entreprend des actions en vue d'atteindre ses objectifs, qui peuvent consister à voler, détruire, chiffrer ou exfiltrer des données.

Cinalia

Sécurisons votre digitalisation

Vous accompagner dans la maîtrise de vos enjeux de cybersécurité.

Un projet?
Des questions ?
N’hésitez pas à nous contacter.

www.cinalia.com

Synelience GROUP

Smart Connection for Smart Solutions