

Répondre aux attaques avancées

lundi 9 août 2021



Répondre aux attaques avancées

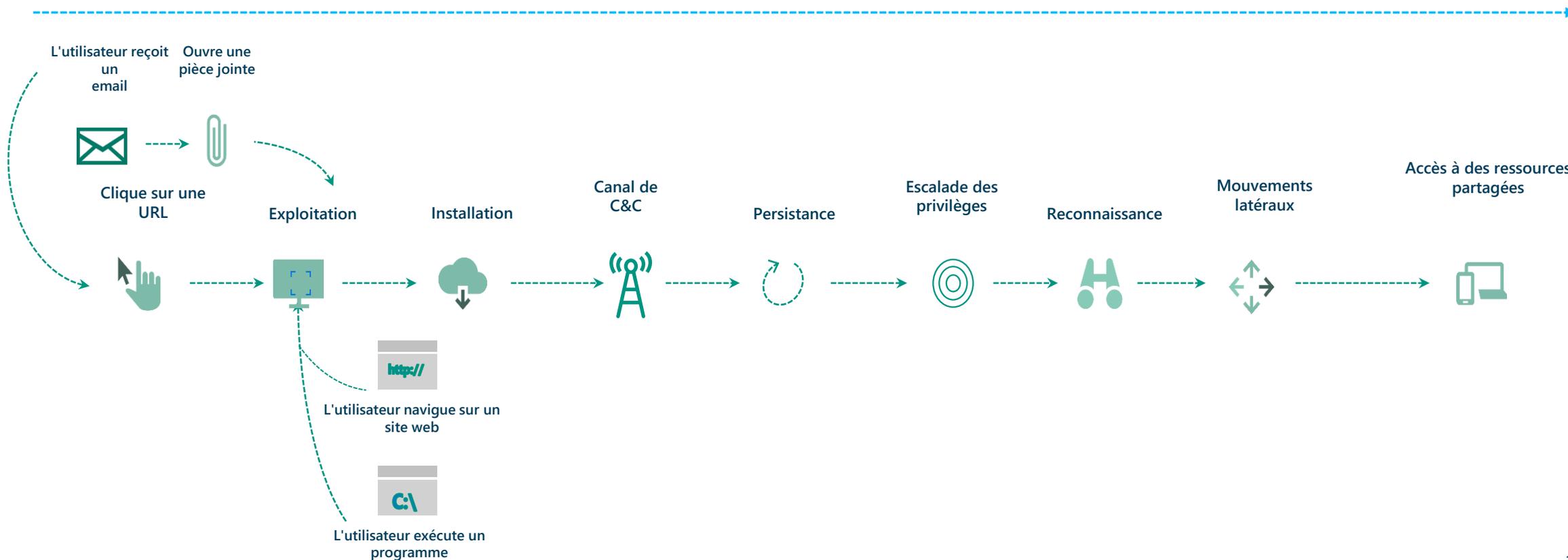
Présentation des scénarios type d'attaques

Applications

Périphériques

Identité

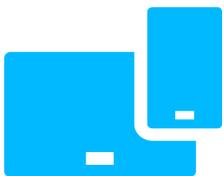
Données





Différentes solutions pour répondre aux attaques avancées

Définir les mécanismes de protection de votre environnement



Terminaux



Identité



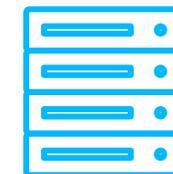
Apps Cloud



Apps



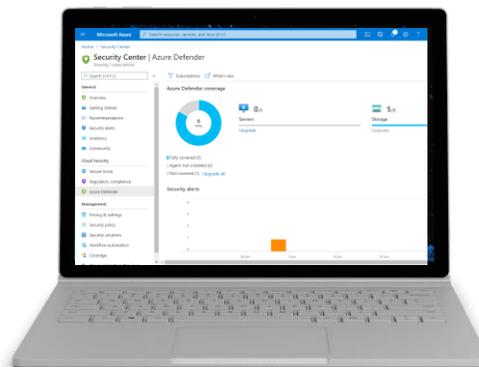
Cloud



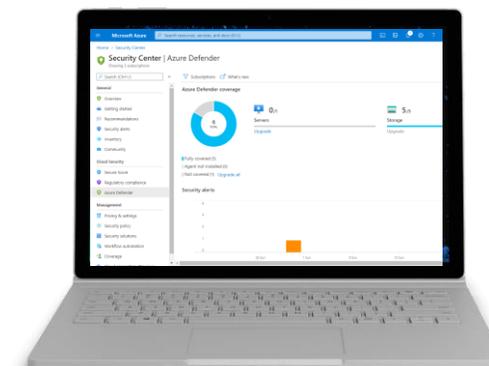
Autres infrastructures



Microsoft 365 Defender



Azure Sentinel



Azure Defender

Solution **SIEM** et **XDR**



Les bénéfices de notre offre par Exakis Nelite

Donner une vision et accompagner l'intégration des mécanismes permettant la réponse aux attaques avancées selon les bonnes pratiques et retours d'expérience.

Notre objectif

- ✓ Répondre à toutes les problématiques de sécurité
- ✓ Identifier les chantiers autour de la protection du système d'information.
- ✓ Implémenter les mécanismes selon les bonnes pratiques et nos retours d'expériences
- ✓ Suivre les évolutions de sécurité dans le temps



Valider les services et les cas d'usage prioritaires et configurer les périphériques en fonction des règles et usages définis



Déploiement des solutions et personnalisation de l'environnement



Suivi des évolutions de sécurité et recommandations pour des améliorations



Identifier les chantiers clés de la sécurisation



Intégration du service selon les besoins



Répondre à des besoins de sécurité et surveillance



Les étapes de mise en œuvre

Une démarche accélérée pour une sécurisation rapide

MISE EN ŒUVRE & DÉPLOIEMENT

AMÉLIORATION CONTINUE (2 ITÉRATIONS)



ACCOMPAGNEMENT



Ce que comprend notre offre

Mise en œuvre & déploiement rapide de mécanisme de protection des périphériques



1

INITIALISATION & DÉFINITION

- Kick-off
- Revue de l'existant et des prérequis
- Elaboration de la feuille de route sur la réponse aux menaces
- Ateliers techniques
- Définition des Uses Cases
- Restitution de la feuille de route
- Définition de l'architecture
- Livrables : Feuille de route, Spécifications

2

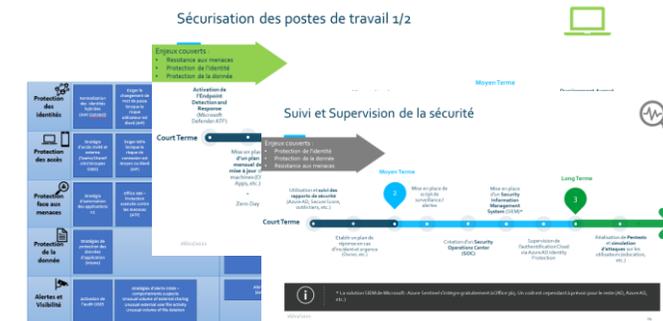
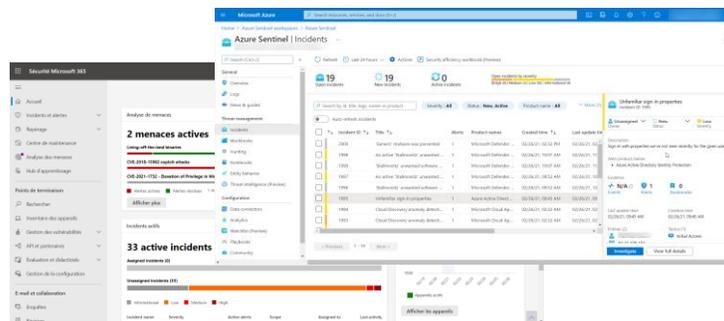
CONFIGURATION & DÉPLOIEMENT

- Configuration des mécanismes de protection avancés identifiés :
- Microsoft 365 Defender
- Azure Defender
- Azure Sentinel
- Mise en place des processus, de la gouvernance et des réponses sur incidents.
- Livrables : Cahier de recette des infrastructures, Guide opérationnel

3

AMÉLIORATION CONTINUE

- Evaluation des chantiers, de l'adoption des solutions
- Evaluation des nouveautés proposées par les services
- Mise à jour de la feuille de route de sécurité avec les nouveaux enjeux
- Livrables : Feuille de route mise à jour





Ce que comprend notre offre

Mise en œuvre & déploiement de mécanismes de réponse aux menaces avancées

Accompagnement des acteurs

Rapide

- Accompagnement permettant de prendre en compte l'état de l'art et présenter les solutions proposées par Microsoft afin de définir la feuille de route des chantiers de sécurisation et de protection.

€ Budget

A partir de 20 000 € HT

Accompagnement des acteurs

Complet

- Accompagnement complet offrant :
- Un état de l'art
- La feuille de route de sécurisation du système d'information
- L'implémentation des solutions de sécurisation identifiées et proposées par Microsoft
- L'accompagnement des populations

€ Budget

A partir de 40 000 € HT

Merci !