Microsoft

5 Week Workshop avec Microsoft Sentinel

aDvens

Security for the greater good

Nous existons pour vous protéger des menaces Cyber.

Advens est un leader européen de la Cybersécurité, indépendant et souverain.

Nos 500 experts forment un collectif engagé et solidaire, présents partout en France (Paris, Lille, Lyon, Toulouse, Bordeaux, Nantes et Rennes), ainsi qu'à Madrid, Barcelone, Montréal et Papeete

Notre mission : protéger les organisations publiques et privées, toujours plus dépendantes du numérique et toujours plus exposées à des attaquants nombreux et professionnels.

Identifier les menaces avec Microsoft Sentinel

Enjeux

Protéger son patrimoine numérique quel que soit son origine (On-premises, Cloud, Mobile)

Anticiper l'expansion de son infrastructure vers le Cloud

Découvrir en continu les menaces et bénéficier de la bonne visibilité

Réduire les ressources allouées à l'analyse et à la surveillance en continue

Objectifs

Expérimenter Microsoft Sentinel sur un périmètre identifié

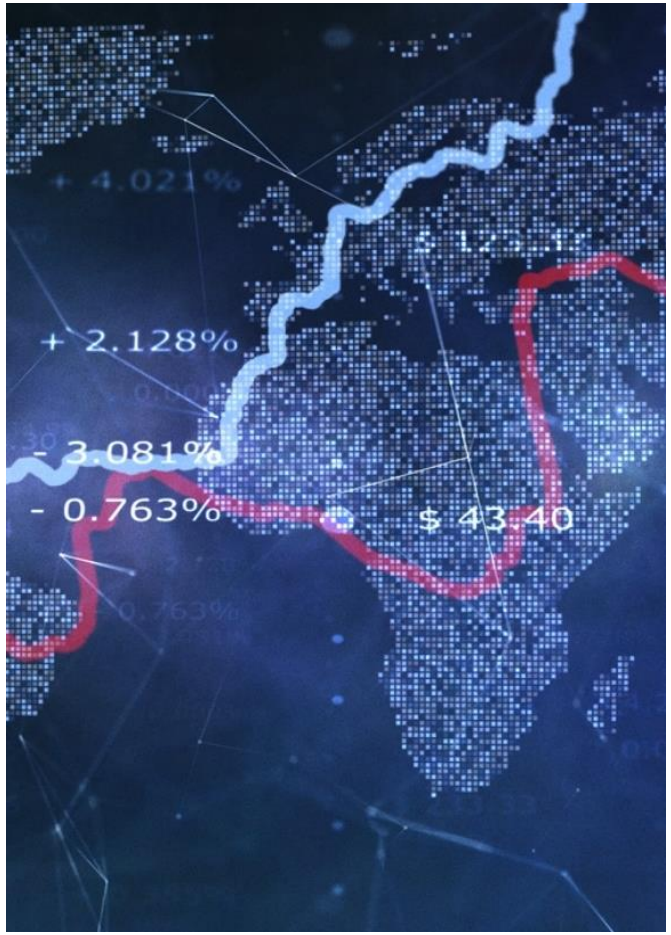
Découvrir et analyser les menaces sur un périmètre Microsoft 365 et On-premises

Automatiser la remédiation des incidents

Disposer d'une vue globale de la sécurité opérationnelle de son SI

Planifier les prochaines étapes

Identifier les menaces avec Microsoft Sentinel



Les usages Cloud sont en pleine croissance et leur protection devient un enjeu de plus en plus majeur pour les organisations. Pour autant, comprendre les risques associés et la manière de construire cette protection dans la durée reste un véritable challenge.

Cet atelier inclut :

- La mise en place d'une surveillance des menaces sur vos environnements Office 365 et Azure AD (endpoints, e-mail, identités…) via votre instance Microsoft Sentinel ou via une instance d'évaluation Microsoft
- L'analyse des situations réelles de menace vous concernant sur la base d'une observation pilote et le partage des axes de sécurisation associées
- La construction d'un plan pour mettre ces menaces sous contrôle avec les services d'Advens et les solutions de Microsoft

Planning : 5 semaines

Hypothèses : tenant Azure déjà existant, réunions et échanges à distance, utilisation des sources natives et incluses en standard dans Microsoft Sentinel (Office 365, activités Azure AD, et selon vos souscriptions existantes Microsoft Defender for Endpoint/Identity/Office/Cloud App/Cloud).

Les coûts associés à l'infrastructure Azure de cette expérimentation sont inclus dans la limite des crédits alloués par Microsoft. Si vous avez déjà déployé une instance Sentinel sur le périmètre de l'atelier, les coûts associés pourront être à votre charge.

Et après ? Suite au workshop, le passage à une offre mySOC complète pourra être étudié (option).

Déroulement du workshop

Echange de qualification

- Introduction
- Attentes du workshop
- Définition du périmètre
- Identification des participants
- Planning prévisionnel
- Alignement sur les attentes et les prochaines étapes
- Communication du questionnaire de qualification

Lancement

- Réunion de lancement
- Objectifs, périmètres, livrables
- Outils de suivi
- Attentes et prochaines étapes

Objectif

- Définition et documentation du périmètre

Configuration Microsoft Sentinel

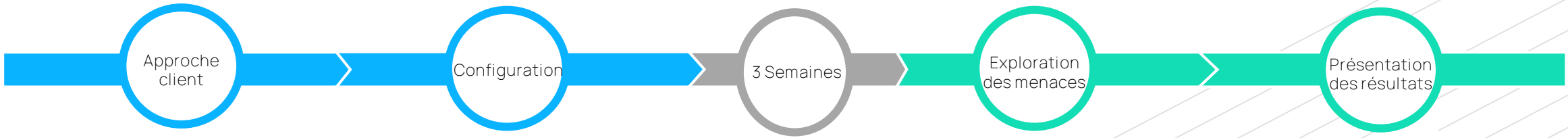
- Mise en place de la licence d'évaluation
- Déploiement et configuration de Microsoft Sentinel

Exploration des menaces et génération de rapports

- Exploration des menaces
- Préparation des rapports d'analyse et recommandations

Présentation des résultats

- Restitution des résultat constatés sur le périmètre d'engagement
- Plan d'actions et prochaines étapes



Et après le workshop…

FUSION CENTER

mySOC PLATFORM

DATA CENTRIC

PORTAIL mySOC

VOUS

ANTICIPER, DÉTECTER ET RÉAGIR AU PLUS VITE

IDENTIFIER VOS VULNÉRABILITÉS

scans de vulnérabilités,

priorisation et pilotage des plans d'action

ALIGNER VOTRE CHAINE DE DÉFENSE À LA MENACE

veille en vulnérabilités contextualisée,

surveillance deep/dark web

DÉTECTER LES MENACES EN TEMPS RÉEL ET PRIORISER LES INCIDENTS

compromission, fuite d'information,

usurpation d'identité…

ASSISTER VOS ÉQUIPES DANS LA RÉACTION

actions de remédiation, réponse incident / gestion crise,

investigation/forensic

Nota : Le service mySOC n'est pas inclus dans le workshop. Son déploiement pourra être étudié après le workshop et fera l'objet d'une contractualisation séparée.

Wavens

Security for the greater good

Paris Lille Lyon Bordeaux Nantes Rennes Toulouse Montréal Madrid Barcelone Papeete