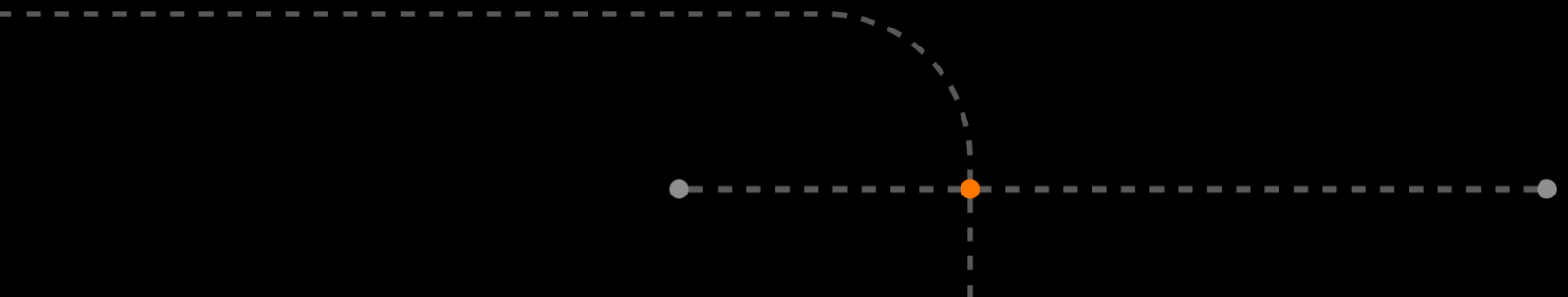
Orange
Cyberdefense

# Xtended SOC 365



orange™

# Les infrastructures de Microsoft privilégiées par les attaquants

**4000**

Attaques par mot de passe par seconde dans le monde*

*Source : Microsoft

# Sécuriser la configuration de Microsoft 365 est un défi de taille

**200+**

Recommandations de sécurité sur un tenant M365

**1000+**

Paramètres pour mettre en place ces recommandations

# Challenge

- Utiliser au maximum les capacités cyber des licences Microsoft 365

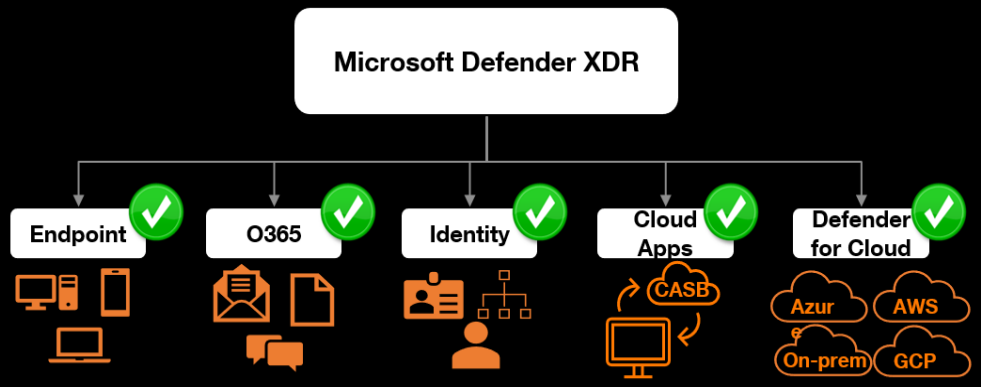
Détecter les menaces sur vos Apps, Devices et Identités

Mettre en œuvre les réponses et les mesures correctives

Améliorer la posture de sécurité

# Dispositif et service

## Tenant Microsoft 365




## Experts Produit

Configuration
Amélioration
Innovation

## Analystes

Détection
Surveillance
Remédiation

API

## Orange Cyberdefense

- Customer Portal
- Ticketing
- Dashboard
- Automation
- Threat intelligence
- Reporting

# Offres de détection, protection et remédiation

## Defender XDR

Defender for **Endpoint**

Defender for **Office**

Defender for **Cloud Apps**

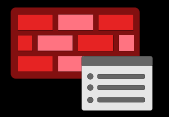
Defender for **Identity**

Microsoft Entra **ID Protection**

## Xtended SOC 365

## Log source (ex) avec Microsoft Sentinel

Firewall



Proxy

ERP

Cloud Service

WAF

## Xtended SOC 365 with Sentinel

# Engagements de service

- Heures et jours ouvrés France métropolitaine de 8H00 à 18H00
- 24/7 en option

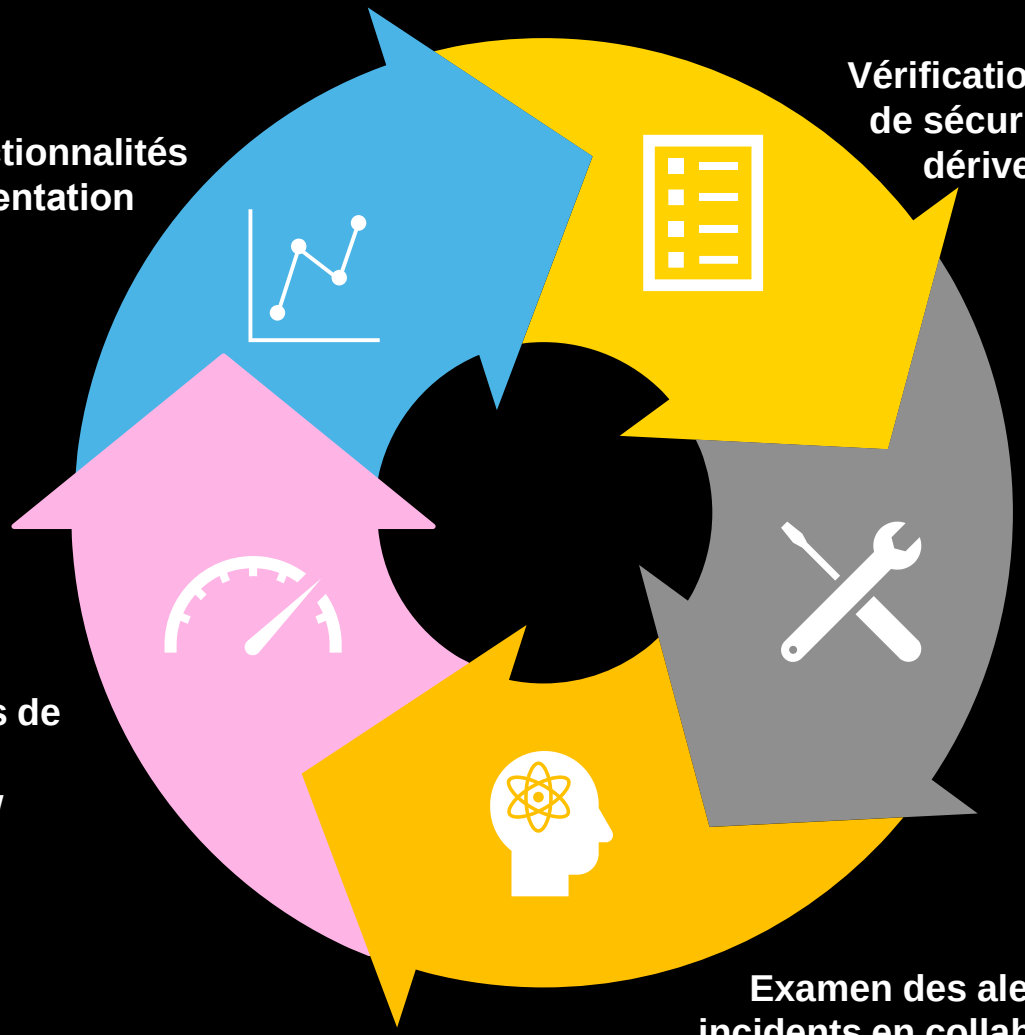
- Incident critique P1: notification sous 30 minutes puis première analyse et action de remédiation sous 2 heures maximum (SLA)
- Incident haut P2 : notification sous 2 heures puis première analyse et action de remédiation sous 8 heures maximum (SLO)

- Threat Hunting régulier des signaux faibles et à partir de nos connaissances des tactiques, et techniques des attaquants (TTP)

- Traitement des actions mises en attente pour favoriser l'apprentissage du machine learning Microsoft

- 1 Réunion de suivi des incidents mensuel
- 1 Point d'amélioration continue mensuel contextualisé

# Maintien en condition de sécurité et innovation



Vérification des +200 paramètres de sécurité et surveillance des dérives de configuration

Proposition d’un plan d’action et accompagnement à la réalisation

Examen des alertes/ incidents en collaboration avec le SOC

Amélioration des capacités de détection pour Defender/Entra/Purview

Suivi des nouvelles fonctionnalités et proposition d’implémentation

# Réponses aux menaces par type d'incident

- Malware, menace web sur les machines
- Exploitation de vulnérabilité

- Mail de Phishing
- Pièce jointe malveillante
- URL de phishing
- Usurpation de domaine

- Découverte
- Exfiltration
- Vol de compte
- Attaque par bruteforce
- Mouvements latéraux
- Attaque par synchronisation de DC
- Augmentation de privilège

- Adresse IP à risque
- Échecs de connexion
- Activité de l'administrateur
- Taux d'activité, Comptes inactifs
- Emplacement, Voyage impossible

## Réponse aux menaces réalisées par OCD

- Isoler un terminal
- Analyser en temps réel via « live response »
- Lancer un scan AV
- Restreindre l'exécution d'une application
- Mettre en quarantaine de fichier

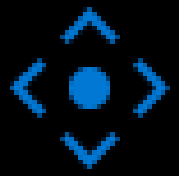
- Stopper une BAL compromise
- Remédier les emails malveillants
- Bloquer un domain ou une URL

- Désactiver un utilisateur dans l'AD
- Suspendre un compte dans Entra ID
- Réinitialiser le mot de passe d'un compte

- Marquer une application comme non approuvée
- Bannir une application

Microsoft 365 Defender for Endpoint

Microsoft 365 Defender for Office



Microsoft 365 Defender for Identity

Microsoft 365 Defender for cloudApps

# Expérience client

## 4 points d’entrée à forte valeur ajoutée

### Portail

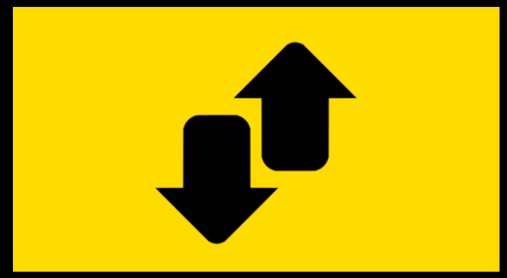
Accès web au client lui permettant de suivre les indicateurs du service et aux incidents en cours sur son périmètre.

### Point de contact

Binôme référent par clients Analyste/Expert Produit Microsoft pour des évolutions majeures ou pour des crises importantes.

### Reporting

Comité de pilotage mensuel avec livraison du support pour mettre en valeur le service et mettre en lumière l’activité cyber dans le SI du client. Permets aussi de piloter l’amélioration continue.



### Synchro incidents

E-bounding entre l’XSOAR d’Orange Cyberdefense et les outils de ticketing du client. Permet au client d’avoir les incidents au plus prêt de sont SI et de ses processus.

# Cas d’usage : tentative de phishing

## 1.Détection

**Détection d’un clic sur une URL suspecte**

(déclenchement d’une règle de détection dans Defender, réception d’une alerte qualifiée, avertissement)

## 2.Investigation

Confirmation de la menace: Analyse du domaine visité

Vérification de la chronologie des actions: Identification de l’origine du clic -> Connexion vers un domaine externe

Identification du vecteur d’infection : Email, Teams, surf Internet, etc

Identification de l’utilisateur connecté à la machine

Vérification si l’incident en cours est déjà existant : rapprochement avec la base d’incident du SOAR

## 3.Remédiation

Prise de contact avec l’utilisateur pour sensibilisation & demande d’action : Nettoyage de la boite mail

Action : Changement de mot de passe en cas de compromission

Vérification si d’autres utilisateurs ont également cliqué : URL similaire sur d’autres postes

## 4.Amélioration

MàJ des actions automatiques : Blocage du domaine dans Defender for Office

MàJ processus : le cas échéant, ajustement du processus lié au traitement de ce type d’alerte

# Option : Implémentation

## Endpoint & Collab Protection

**Assurer la protection et la sécurité de la messagerie et des outils collaboratifs**

**Mise en place de dispositifs de sécurité sur les postes de travail et serveur**


## Data Protection

**Cartographier la donnée présente sur le tenant**
**Labéliser et classifier les données en fonction de leurs cycles de vie**
**Mise en place de contrôle des données sensibles**

## Identity Protection

**Implémentation des bonnes pratiques pour les accès à privilèges**

**Paramétrage des stratégies de protection des identités OnPrem & online**

# Option : Purple Team
# Tenant Microsoft 365


## Périmètre

Réalisation des scénarios d'attaques M365 avancées

Exposition externe uniquement

- Interface d'authentification Office 365
- Système de MFA
- Fichiers OneDrive & SharePoint exposés

## Scénarios couverts

Test de la pertinence des règles de détections face à des attaques standards et avancées

- Scénarios standards :
- Vol et rejeu de session
  - Vol de token, Bypass MFA
- Attaques depuis un compte standard
  - Enumération des ressources et droits
- Abus de droits des applications
  - Mauvaises configurations, Elévation de droits

## Résultats

Echanges avec la Blue Team

Rapport détaillés

- Axes d'améliorations
- Synthèse globale
- Détails des actions offensives

Recommandations sur l'amélioration de la détection

# SOC déroulement de la phase de BUILD

**Initialisation**

**2 semaines**
Kick-off
Rappel des objectifs
Planning
Identification des parties prenantes

**Préparation et conception**

Security Analisys for Microsoft 365
Définition des politiques
Plan implémentation
analyse des paramètres de sécurité MS
**1 mois**

**Déploiement**

1 mois
Installation
Ouverture de flux
Configuration des politiques
Revue sévérité
Mise en place des règles de détection sur Defender
**Test de la pertinence des règles de détection**

**Transition RUN**

Purple team
RACI matrix
Processus
Pre-RUN
Transfert de connaissances
**1 mois**

**1 chef de projet**
**Pour le suivi de l'intégration**

**1 analyste référent + 1 expert produit MS dédié**
**Pour toute la durée du contrat (BUILD & RUN)**

Orange
Cyberdefense

# Merci

Build a safer digital society.

May 23, 2024

www.orangecyberdefense.com