Comment élever et maintenir la posture de sécurité de ma PME ?

WEBINAR

Mardi 26 novembre 2024

blue soft GROUP
Empower

Sommaire

01. Présentation de Blue Soft Empower

02. Contexte de la Cybersécurité pour les PME

03. Nos offres de sécurité

04. Accompagnement et Conformité

05. Session de Questions et Réponses avec nos experts

Evina Burnaz
Sales Development Representative

Jean-François BERENGUER
Directeur des pôles Cyber Sécurité, architecture et intégration

Cédric Saint-Lager
Directeur Commercial Nord Est

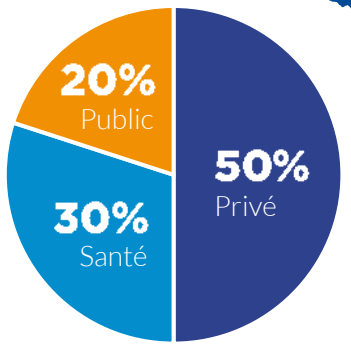
01. Présentation Blue Soft Empower

blue soft Empower

Ultra-spécialiste des solutions Microsoft

107 M€ de CA groupe Blue Soft

18 M€ de CA Blue Soft Empower



100 Talents Bleus

Microsoft

4 Agences

13 Spécialisations avancées

350 Certifications individuelles

Domaines d'intervention

- Collaboratif Microsoft 365
- Poste de travail et mobilité
- Eco-énergie
- Cloud Azure & infra
- Sécurité et identité
- Power Platform
- Intranet et GED
- Data & IA

- Revendeur CSP Tier 1
- FastTrack Ready

Savoir-faire

- Intégration et déploiement
- Gestion du changement & adoption
- Pilotage de projet
- Conseil

Modalités d'engagement

- Projet
- Régie
- Contrat de conseil et support

Récompenses

Microsoft — Partenaire Santé 2023

Powell Software — Partenaire Europe 2023

Nos petits plus

- Prosci
- Prince 2
- PMP

Sondage

Comment évaluez-vous la posture de sécurité actuelle de votre organisation ?

Forteresse imprenable 🌟

Très solide, avec des mesures strictes en place 💪

Bastion en consolidation 🛠️

Moyenne, quelques vulnérabilités connues

Terrain à renforcer 🔍

Faible, en amélioration

Alerte rouge : Danger imminent 🚨

Risquée, nécessitant des mesures urgentes

blue soft Empower

02.
Contexte de la cybersécurité pour les PME

blue soft
Empower

Pourquoi améliorer et maintenir sa posture en Cyber Sécurité?

PROTECTION DES RISQUES

Protéger son informatique des cyber-attaques de plus en plus nombreuses

Protéger les données des clients, des salariés et contractants

Se conformer aux régulations cyber (NIS2)

Développer une culture interne de protection des risques cyber

Continuer d'innover et se protéger des risques associés

AVANTAGES ECONOMIQUES

Eviter les risques d'interruption de travail et de coûts associés aux dommages matériels et immatériels causés par les cyberattaques

Optimiser les investissements liés à la protection informatique en supprimant les coûts redondants

Réduire les primes de cyber assurance en démontrant un haut standard de protection

Bénéficier de subventions publiques liées à la protection numérique

En 2023, les PME ont été la cible de 43% des cyberattaques

blue soft Empower

Les conséquences d'une attaque

- Pertes de données sensibles et indispensables
- Vol de données et risque d'espionnage industriel
- Coûts imprévus pour la remédiation
- Perte financière
- Dégradation de la réputation de l'entreprise
- Problèmes légaux

Et cela peut aller jusqu'à la cessation d'activité

Sondage

Votre organisation a-t-elle déjà fait face à une cyberattaque ?

- ❑ Non
- ❑ Oui, mais on a su rebondir
- ❑ Oui, quelques ajustements nécessaires après coup
- ❑ Oui, et cela a eu de fortes répercussions

En matière de Cyber Sécurité, la posture est essentielle

Analyse des attaques par ransomware. Sources : Microsoft Digital Defense Report 2022

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

88 % des clients concernés n'ont pas utilisé les bonnes pratiques de sécurité AD et Azure AD

Dans **88 %** des cas, l'authentification multifacteur n'a pas été mise en œuvre pour les comptes sensibles et à privilèges élevés

68 % des organisations touchées ne disposaient pas d'un processus efficace de gestion des vulnérabilités et des correctifs

L'absence d'un plan d'intervention efficace était un domaine critique observé dans **76 %** des organisations touchées

44 % des entreprises ne disposaient pas de sauvegardes immuables pour les systèmes touchés

92 % des organisations touchées n'ont pas mis en œuvre de contrôles efficaces de prévention des pertes de données pour atténuer ces risques

blue soft Empower

Une posture doit être complète

Protection

Protection des appareils numériques de l'entreprise (ordinateurs, mobiles)

Conformité et niveau d'exposition

Conformité aux réglementations actuelles et à venir

Audit de la posture, définition et suivi de la feuille de route

Analyse de la surface d'exposition externe

Sécurisation

Sécurisation des accès pour éviter les intrusions

Surveillance

Surveillance permanente des tentatives d'intrusion

Sensibilisation

Formation des utilisateurs à la prévention des risques

Trois axes essentiels

Tous les accès reposent sur les identités

Identités

Le maillon faible. Quels que soient les solutions techniques déployées, elles se seront efficace que si les utilisateurs sont sensibilisés

Utilisateurs

Postes et périphériques

Dans une très grande majorité de cas d'attaque , les premières actions cibles les postes

Tout dispositif visant à améliorer sa posture de sécurité et protéger son système d'information doit à minima prendre en compte ces trois composantes

blue soft Empower

03.
Nos offres Empower CYRENE

blue soft
Empower

4 niveaux

Objectif

Elever et maintenir la posture de sécurité des clients SMB.

Mode réactif

Bronze

M365 Business Standard
+ Defender for Business

Silver

M365
Business Premium

Mode proactif

Gold

M365 Business Premium
Monitoring 8/5

Platinium

M365 Business Premium
Monitoring 24/7

Contenu

- Vente de licences en CSP
- Setup & configuration
- Remédiation

Partenaires

Mantra
Sensibilisation à la cybersécurité

visiativ
Pour le CyberPilot

devensys CYBERSECURITY
Pour le CSIRT

blue soft Empower

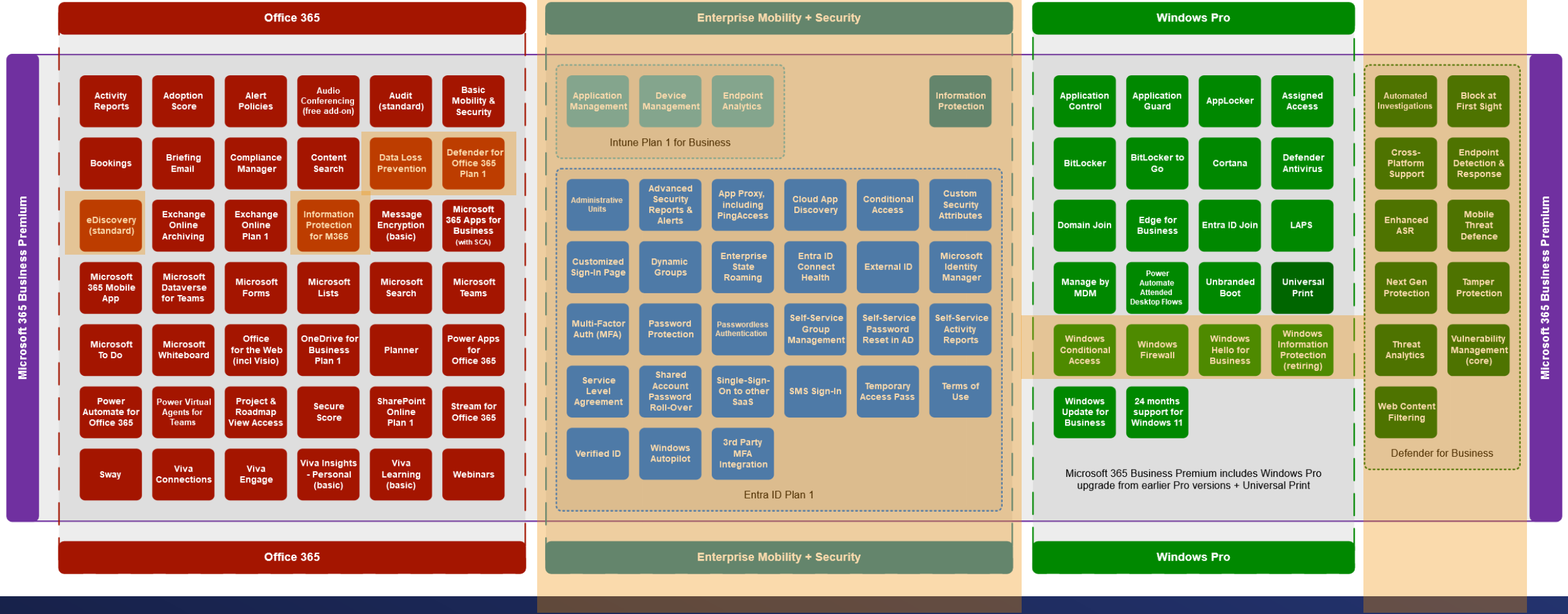
Listing	Bronze	Silver	Gold	Platinium
Licences Microsoft incluses	M365 Business Standard Defender for Business	M365 Business Premium	M365 Business Premium	M365 Business Premium
Monitoring alertes/incidents M365	8/5	8/5	8/5	24/7
Audit/Assessment annuel	✓	✓	✓	✓
Protection des ordinateurs et mobiles	✓	✓	✓	✓
Sécurisation des identités et des accès	✓	✓	✓	✓
Sensibilisation des utilisateurs	✓	✓	✓	✓
E-learning sensibilisation + campagne phishing	Option (5€)	Option (5€)	✓	✓
Gouvernance et protection des données		Option (2€)	✓	✓
Gestion des mises à jour et réduction surface d'attaque		Option (2€)	✓	✓
Posture et conformité, Analyse exposition externe, Daily Report		Option (5€)	✓	✓
Sauvegarde des données : setup, monitoring et tests restauration	Option (3,5€)	Option (3,5€)	Option (3,5€)	Option (3,5€)
	19,90€*	29,90€**	39,90€**	49,90€**

(*) Prix HT par utilisateur et par mois, Engagement annuel, offre accessible à partir de 50 licences
(**) Prix HT par utilisateur et par mois, Engagement annuel, offre accessible à partir de 100 licences

Microsoft 365 Business Premium

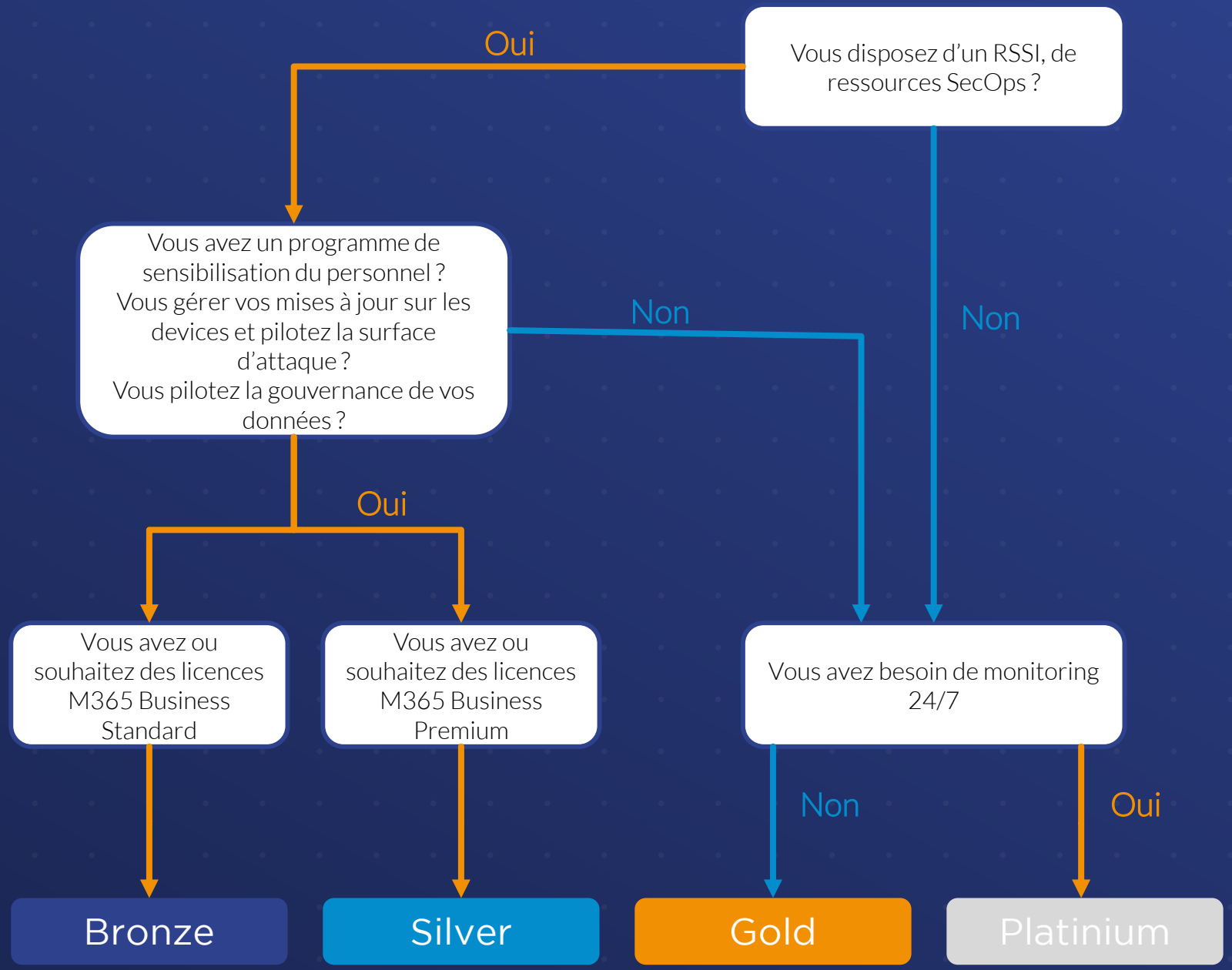
July 2023

m365maps.com

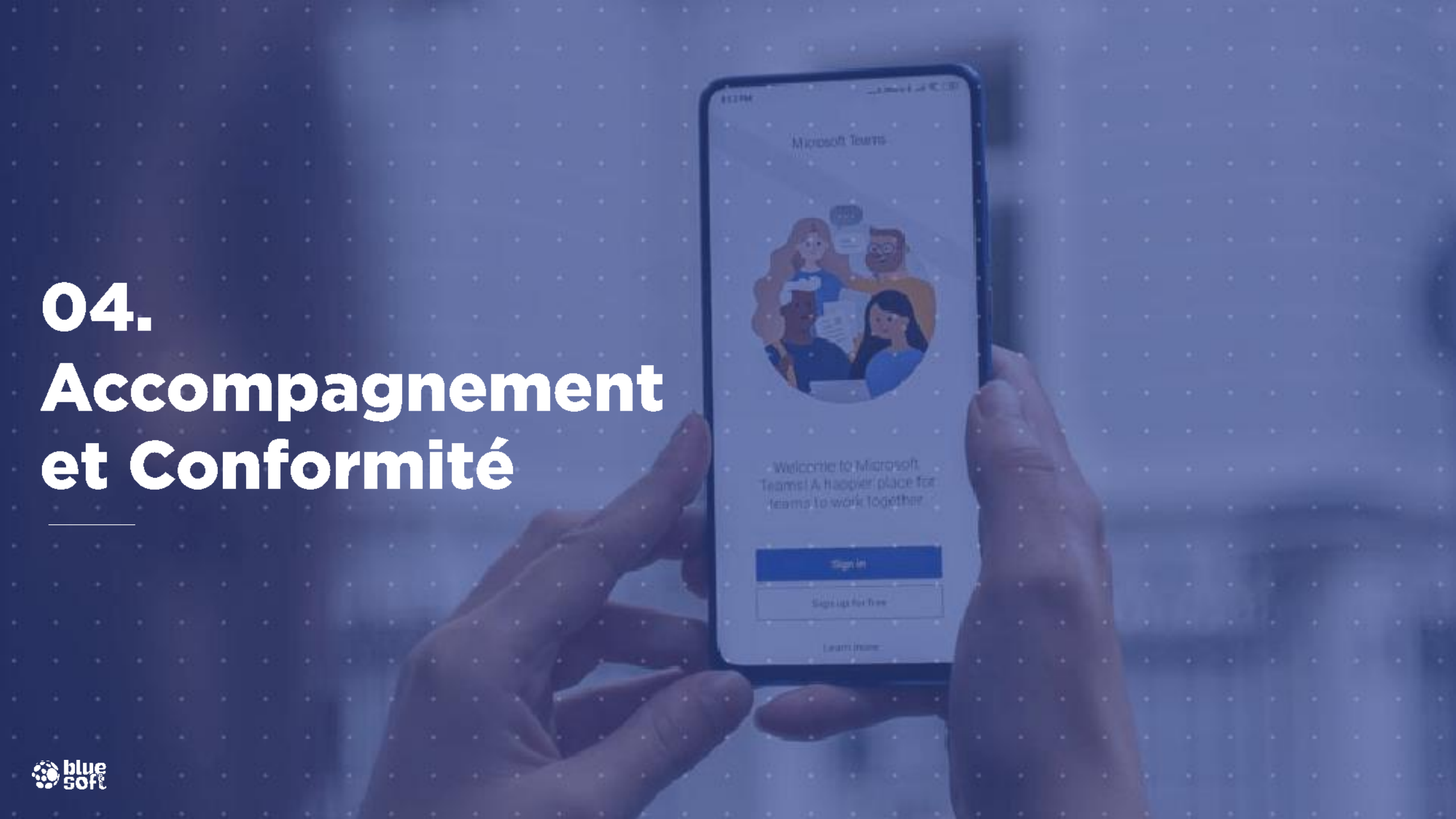


Quelle offre est la plus adaptée à votre contexte ?

Cela dépend de votre niveau de maturité en matière de SMSI sur M365 et du niveau d'accompagnement



04.
Accompagnement et Conformité

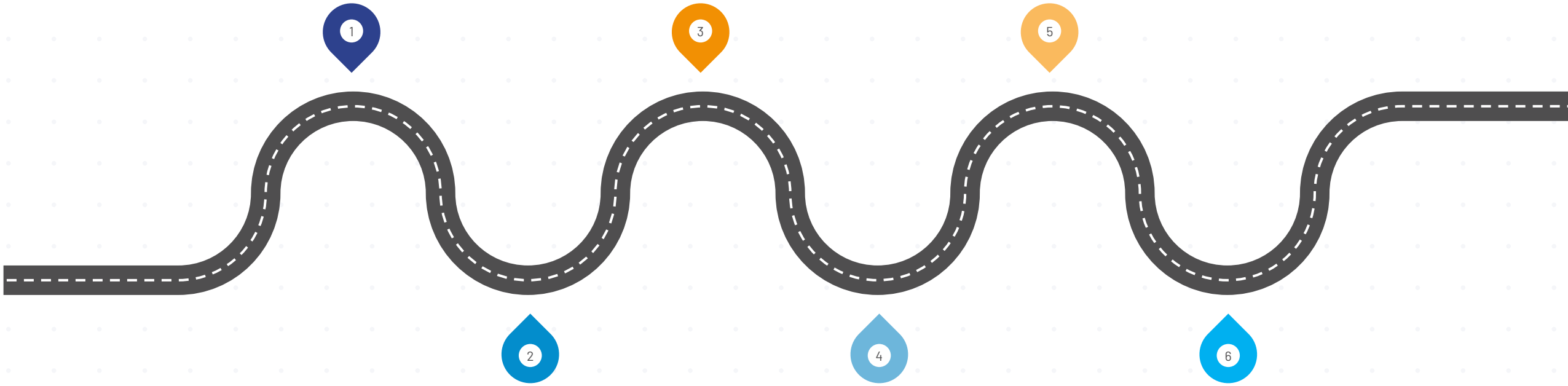


Notre accompagnement

Diagnostic de posture de sécurité et analyse des écarts vs ligne de base

Implémentation de la ligne de base de sécurité dans Microsoft 365
Option sauvegarde Microsoft 365

Programme de sensibilisation des utilisateurs et utilisatrices



Diagnostic 360°
Analyse de la conformité vis-à-vis des règlementations européennes dont NIS2
Analyse de la surface d'exposition externe

Elaboration de la feuille de route

Mise en place du processus de surveillance permanente

Daily report

Option Cyber Coach
Options journées d'expertise
Option CSIRT

Pilotage via SDM

Audit préliminaire

Un premier audit de la posture de sécurité est réalisé lors de l'initialisation du contrat.

Cet audit est renouvelé annuellement. Il porte sur :

- Posture vis-à-vis des bonnes pratiques
- Identification des utilisateurs et données à risques
- Posture vis-à-vis des préconisations du CIS pour les clients disposant déjà d'un environnement M365

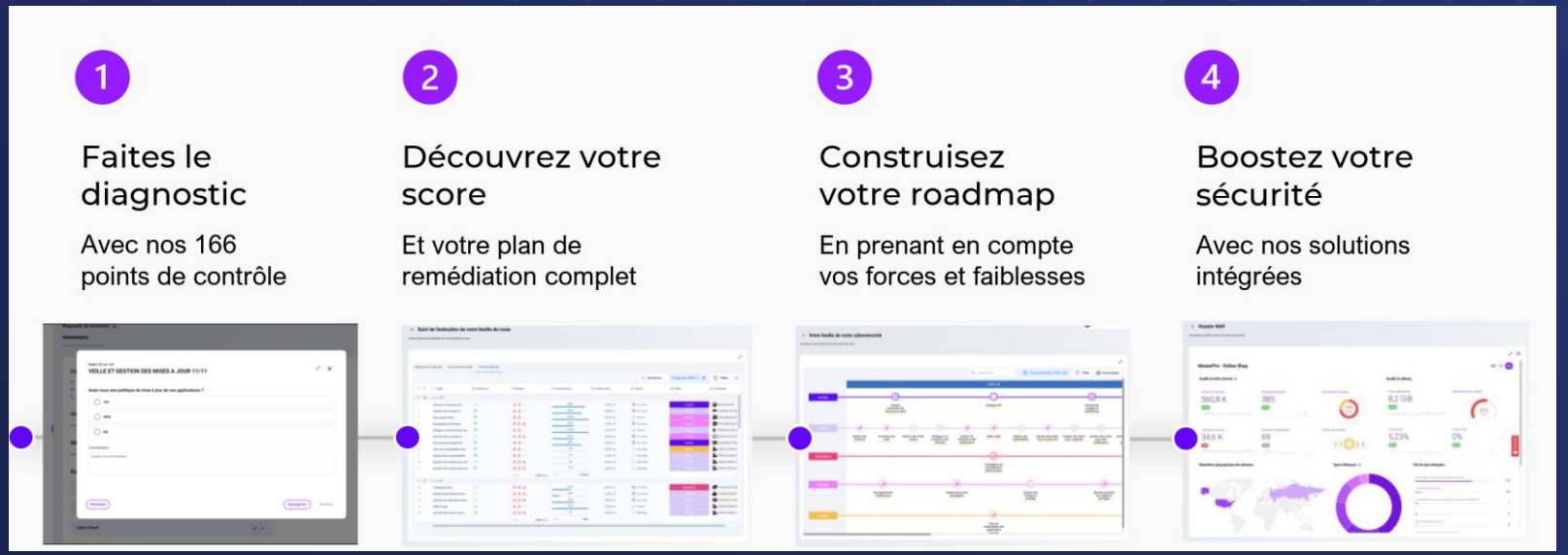
Cet Audit préliminaire permet de mesurer les éventuels écarts avec la ligne de base des configurations qui seront réalisées

Inclus dans Gold et Platinium,
En option pour Silver

Posture et Conformité

Via la solution CyberPilot :

- Diagnostic 360 ° : réalisation d'un état des lieux pour comprendre le niveau de maturité et d'exposition aux risques
- Elaboration et suivi de la feuille de route
- Analyse de la conformité vis-à-vis des règlementations européennes dont NIS2
- Analyse de la surface d'exposition externe
- Guides : PSSI, Charte, gestion de crise, RGPD, …



visiativ
CYBER PILOT

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

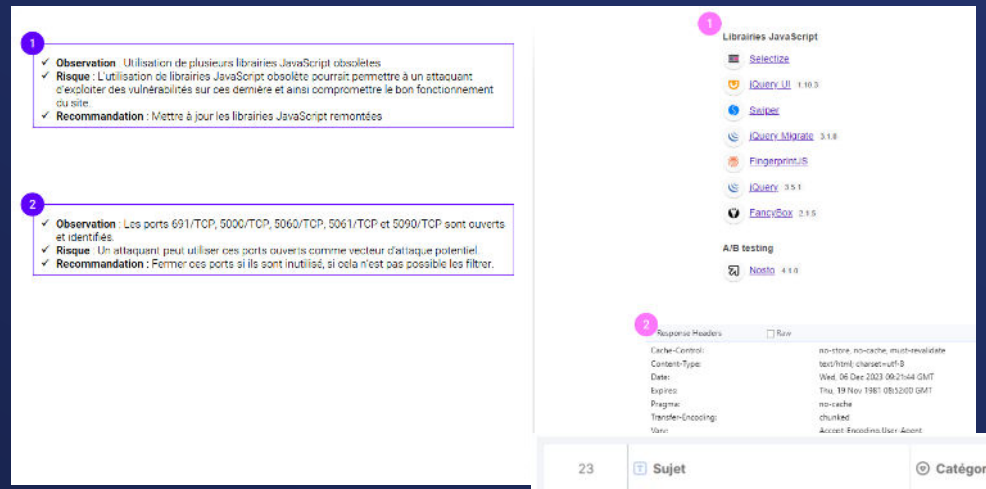
NIS 2

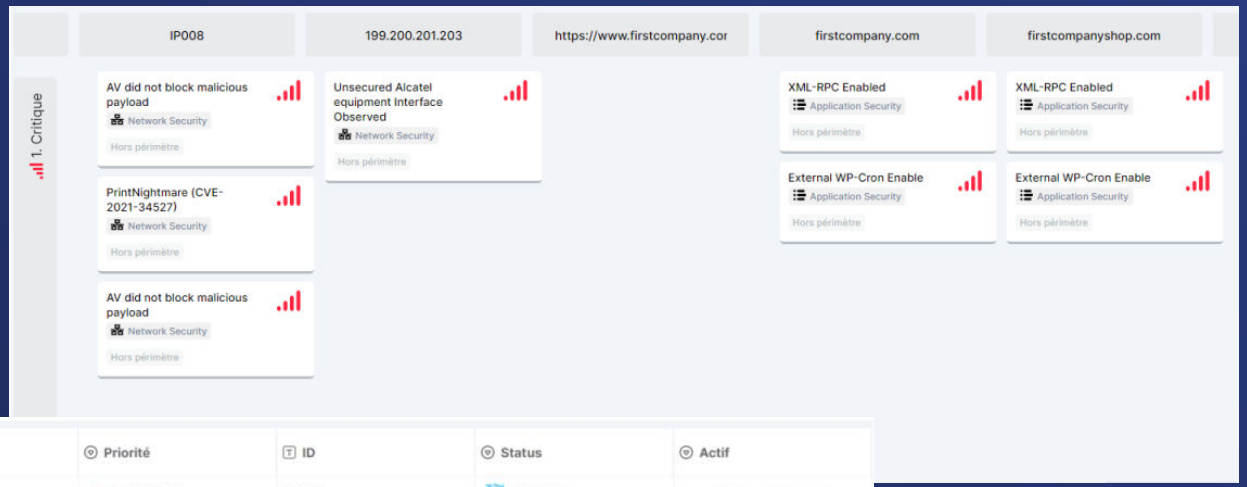
blue soft Empower

Inclus dans Gold et Platinium,
En option pour Silver

Analyse de la surface d'exposition externe

Réalisé 1 fois par an maximum en début de cycle d'un scan de votre surface d'attaque externe et analyse les vulnérabilités détectées de votre surface d'exposition (domaines, IP publiques, ports, protocoles). Cette analyse s'organise via l'utilisation de la solution SAAS SecurityScoreCard pour détecter les vulnérabilités et faiblesses de configuration publiquement accessibles. Elle est augmentée au travers d'une analyse humaine et intégrée dans le tableau de bord de CyberPilot





23	Sujet	Catégorie	QuickWin	Priorité	ID	Status	Actif
1	Site does not enforce HTTPS	Application Security	Oui	Importante	25599	Nouveau	demo-pole-expert-
2	Site does not enforce HTTPS	Application Security	Oui	Importante	25600	Nouveau	demopec.fr
3	Site does not enforce HTTPS	Application Security	Oui	Importante	25601	Nouveau	demo-pec.fr
4	Website Does Not Implement HSTS Best...	Application Security	Oui	Normal	25602	Nouveau	demopec.fr
5	SPF Record Missing	Dns Health	Oui	Normal	25604	Nouveau	
6	SPF Record Contains a Softfail without...	Dns Health	Oui	Faible	25605	Nouveau	
7	SPF Record Contains a Softfail without...	Dns Health	Oui	Faible	25606	Nouveau	
8	TLS Service Supports Weak Cipher Suite	Network Security	Oui	Normal	25607	Nouveau	
9	Website does not implement X-Content-...	Application Security	Oui	Faible	25610	Nouveau	demo-pole-expert-
10	Website does not implement X-Content-...	Application Security	Oui	Faible	25611	Nouveau	demo-pec.fr

Mise en œuvre des lignes de bases

Configuration du tenant

Protection des identités et des accès

Protection des devices sur MDE

Protection des solutions de collaboration dans MDO

Option : Protection des documents via Purview

Option : Protection des devices sur Intune (si onboarding)

blue soft Empower

Inclus dans Gold et Platinium,
En option pour Silver

Surveillance des alertes et incidents

Alertes

- Surveillances des alertes en heures et jours ouvrés
- Notification par mail 24/7 pour les alertes de niveau élevé
- Actions de remédiation de premier niveau suivant convention de service
- Investigations et diagnostics + Préconisation de plan de remédiation

Incidents

- Notification par mail 24/7 pour les alertes de niveau élevé
- Actions de coupure de l'attaque suivant convention de service
- Investigations et diagnostics + Préconisation de plan de remédiation
- En fonction de la gravité : initiation de la gestion de crise + mise en relation avec CSIRT

Un SDM est en charge du pilotage de votre contrat et fera des points trimestriels sur les alertes et incidents et le suivi des mesures correctives et évolution proposées

blue soft Empower

Inclus dans Gold et Platinium,
En option pour Silver

Daily Report

Points de contrôle

- Evènements (alertes) et incidents
- Utilisateurs à risque
- Postes et périphériques non conformes et /ou présentant un niveau de risque
- Evolution du niveau d'exposition
- Etats des jobs de Sauvegardes

Rapport d'analyse et préconisation

- Rapport quotidien
- Tendances sur le mois
- Description des évènements
- Qualification des incidents de sécurité

blue soft Empower

Sensibilisation à la cybersécurité

Kit de communication comprenant

Deux mails rappelant les enjeux de la cybersécurité et incluant les rendez-vous pour les webinaires

Un document sur les bonnes pratiques à avoir face à une tentative de phishing

Deux webinaires

Présentation des enjeux et du setup de sécurité mis en place au sein de l'organisation

Bonnes pratiques et reflexes en matière de sécurité informatique

blue soft Empower

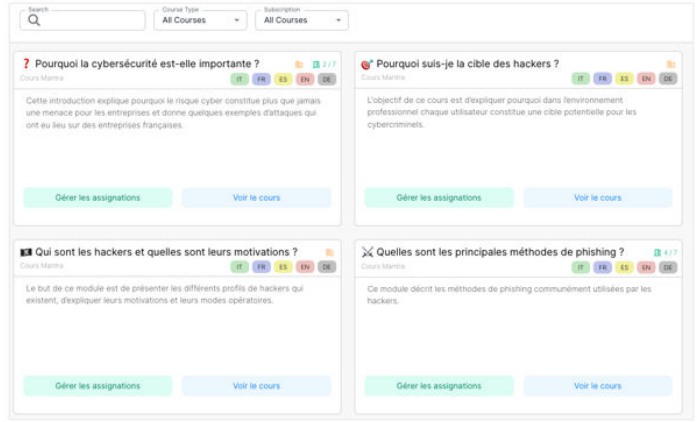
Inclus dans Gold et Platinium,
En option pour Silver

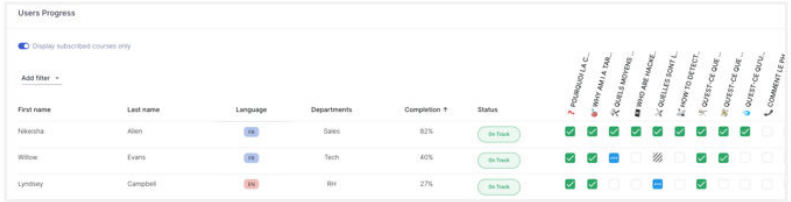
E-learning sensibilisation

Programmes d'E-learning accessible en ligne et sous forme d'un assistant dans Teams qui propose régulièrement de sessions de quelques minutes afin de sensibiliser le personnel de l'entreprise

Cyber Awareness

Formez vos collaborateurs à la cybersécurité





Principales fonctionnalités

- Base de 25 tutoriels & 1 nouveau tutoriel tous les mois
- Approche conversationnelle
- Système de relance automatique
- Contenu des tutoriels 100% éditable
- Suivi avancement via tableaux de bord

Mantra

Mantra

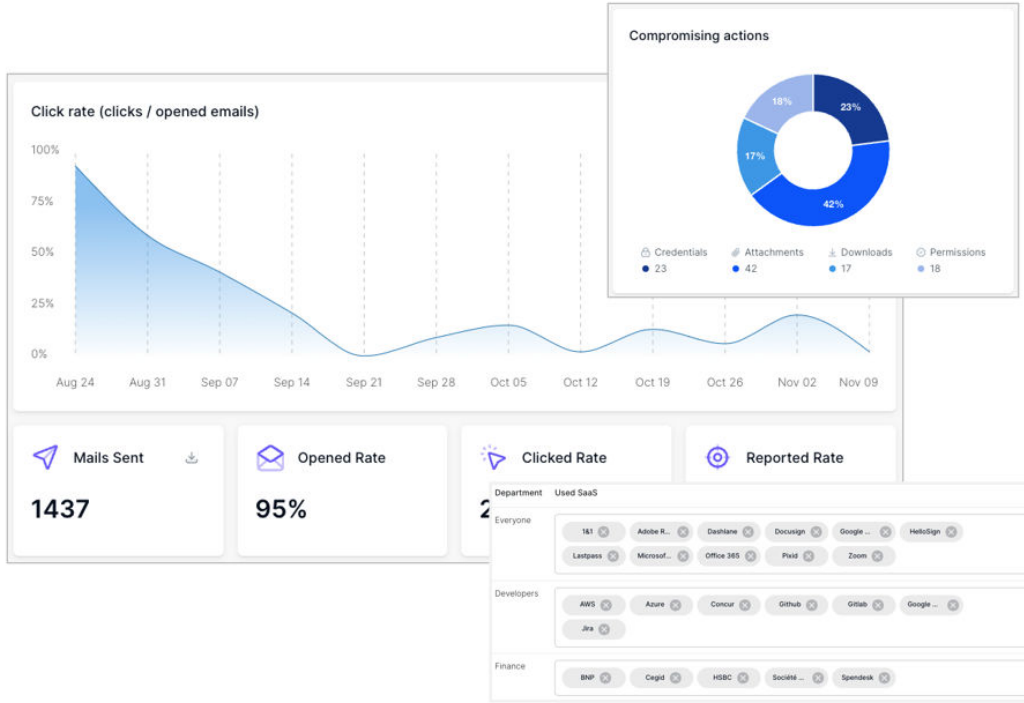
Inclus dans Gold et Platinium,
En option pour Silver

Campagne de test de phishing

Campagnes de simulation de phishing personnalisées au profil de votre entreprise

Phishing Simulation

Entraînez vos utilisateurs en situation réelle



Principales fonctionnalités

- Base de 500 templates
- Simulation d'attaques de spear-phishing
- Parcours gamifié
- Solution 100% automatsée
- Synchronisation annuaire Google Workspace / O365
- Campagnes sur-mesure

Mantra

Mantra

Pilotage du contrat via SDM

Echanges réguliers

(Trimestre ou semestre)

Suivi des indicateurs

Utilisation des licences
Nombre d'alertes et incidents
Exposition des postes et périphériques
Secure Score
Niveaux d'usages

Suivi du plan d'évolution

Mise à disposition de ressources

Des options pour augmenter votre sécurité

RSSI As A Service

Journées d'expertise

CSIRT

blue soft Empower

Option – RSSI as a Service

Le service RSSI en temps partagé fonctionne de pair avec la plate-forme Cyber Pilot, sur des cycles d'un an avec une structure et un calendrier bien définis pour assurer une gestion efficace de la cybersécurité.

Une intervention mensuelle pour

- Faire un diagnostic annuel puis définir les politiques de sécurité et suivre leur mise en œuvre
- Suivre la conformité réglementaire, rédiger les livrables du plan Cyber et organiser la sensibilisation du personnel
- Animer un comité de suivi (avancement opérationnel, priorisation, lever les freins et validation des mesures)

Tous les trimestres : un comité de pilotage remplace le comité de suivi pour réaliser

- Un point avec la direction pour mettre en avant les réalisations et présenter les indicateurs clés
- Un diagnostic annuel puis définir les politiques de sécurité et suivre leur mise en œuvre

blue soft Empower

En complément : Périmètre des missions du RSSI en temps partagé

Evaluation des risques, définition des politiques de sécurité et suivi de leur mise en place, accompagnement à la mise en œuvre d'un SMSI

Suivi de la conformité réglementaire (RGPD, NIS2, DORA, ISO 27001, …)

Accompagnement à la conception et mise en œuvre des opérations de sécurité (gestion des incidents de sécurité, mise en œuvre du SOC, surveillance, …)

Accompagnement à la préparation de gestion de crise

Organisation de la sensibilisation du personnel à la Cybersécurité

Accompagnement à la rédaction de la bibliothèque documentaire du SMSI : PGSSI,

Un accompagnement pour NIS2 et DORA

Dans le cadre de ses journées planifiées, le RSSI en temps partagé pourra vous accompagner pour la mise en conformité avec les nouvelles directives et nouveaux règlements via l'identification des écarts, l'ajout des actions de mise en conformité dans feuille de route et le suivi des actions

NIS2

- Directive Européenne : transposée dans le droit national de chaque pays
- Octobre 2024
- Homogénéité du niveau de Cyber Sécurité à travers l'EU
- Concerne les organisations essentielles et importantes (critères CA, Bilan et Nb employés)

- Les acteurs de la chaîne d'approvisionnement, dont les acteurs du numérique, seront soumis au dispositif -> sous-traitants
- Sanctions financières

DORA

- Règlement Européen applicable tel quel par les états membres
- Janvier 2025
- Résilience opérationnelle numérique du secteur financier
- Concerne 21 types d'entités incluant les partenaires tiers TIC

- Cadre de gestion des risques lié aux TIC
- Programme de tests de résilience
- Processus de notification

blue soft Empower

Option - CSIRT sur demande

Forfait de réponse sur Incident majeur – gestion de crise

Intervention à distance. Sur site possible selon les besoins avec frais de déplacement en supplément

Inclus jusqu'à 35 heures-hommes (HO et HNO) d'intervention

Profils mis à disposition :

- Un gestionnaire de crise (obligatoire)
- Un expert forensique (obligatoire), plusieurs selon la situation
- Un expert en reconstruction / durcissement / remédiation (selon la situation)

Rédaction d'un rapport forensique préliminaire avec les éléments découverts durant l'investigation

devensys CYBERSECURITY

blue soft Empower

Option - Sauvegarde des données

Fournitures de licences

+

Déploiement et configuration de la solution de sauvegarde des données de Microsoft 365

En semaine : Surveillance journalière de la bonne exécution des jobs de sauvegarde

Tests semestriels de restauration d'items

(Mails, Fichiers, Items OneDrive, Equipe Teams)

Questions ?

Merci !

POUR PRENDRE RENDEZ-VOUS AVEC UN EXPERT :

https://outlook.office365.com/book/Prendreunrendezvous@bluesoft-group.com/

04 28 38 51 03

www.bluesoft-group.com