

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

WEBINAR

Mardi 26 novembre 2024



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

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

Savoir-faire

Intégration et déploiement

Gestion du changement & adoption

Pilotage de projet

Conseil

Modalités d'engagement

Projet

Régie

Contrat de conseil et support



107 M€ de CA groupe Blue Soft



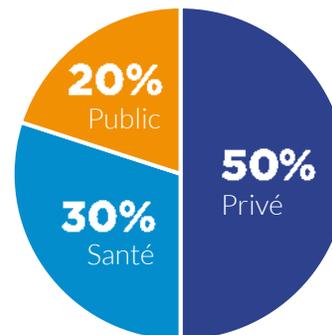
Microsoft

4 Agences

13 Spécialisations avancées

350 Certifications individuelles

18 M€ de CA Blue Soft Empower



100 Talents Bleus



Revendeur CSP Tier 1

FastTrack Ready

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

02.

Contexte de la cybersécurité pour les PME

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

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/RE5bUvw?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

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 ne seront efficaces que si les utilisateurs sont sensibilisés

Utilisateurs

Postes et périphériques

Dans une très grande majorité de cas d'attaque, les premières actions ciblées sont 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

03.

Nos offres Empower CYRENE



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

Contenu

Vente de licences en CSP

Setup & configuration

Remédiation

Mode proactif

Gold

M365 Business Premium
Monitoring 8/5

Platinum

M365 Business Premium
Monitoring 24/7

Partenaires

 **Mantra**

Sensibilisation à la cybersécurité

 **visiativ**

Pour le CyberPilot

 **devenSYS**
CYBERSECURITY

Pour le CSIRT

Listing

Licences Microsoft incluses

Monitoring alertes/incidents M365

Audit/Assessment annuel

Protection des ordinateurs
et mobiles

Sécurisation des identités
et des accès

Sensibilisation des utilisateurs

E-learning sensibilisation
+ campagne phishing

Gouvernance et protection des
données

Gestion des mises à jour et
réduction surface d'attaque

Posture et conformité, Analyse
exposition externe, Daily Report

Sauvegarde des données : setup,
monitoring et tests restauration

Bronze

M365 Business Standard
Defender for Business

8/5



Option (5€)

Option (3,5€)

19,90€*

Silver

M365 Business Premium

8/5



Option (5€)

Option (2€)

Option (2€)

Option (5€)

Option (3,5€)

29,90€**

Gold

M365 Business Premium

8/5



Option (3,5€)

39,90€**

Platinum

M365 Business Premium

24/7



Option (3,5€)

49,90€**

Microsoft 365 Business Premium

July 2023

m365maps.com

Microsoft 365 Business Premium

Microsoft 365 Business Premium

Office 365

Activity Reports	Adoption Score	Alert Policies	Audio Conferencing (free add-on)	Audit (standard)	Basic Mobility & Security
Bookings	Briefing Email	Compliance Manager	Content Search	Data Loss Prevention	Defender for Office 365 Plan 1
eDiscovery (standard)	Exchange Online Archiving	Exchange Online Plan 1	Information Protection for M365	Message Encryption (basic)	Microsoft 365 Apps for Business (with SCA)
Microsoft 365 Mobile App	Microsoft Dataverse for Teams	Microsoft Forms	Microsoft Lists	Microsoft Search	Microsoft Teams
Microsoft To Do	Microsoft Whiteboard	Office for the Web (incl Visio)	OneDrive for Business Plan 1	Planner	Power Apps for Office 365
Power Automate for Office 365	Power Virtual Agents for Teams	Project & Roadmap View Access	Secure Score	SharePoint Online Plan 1	Stream for Office 365
Sway	Viva Connections	Viva Engage	Viva Insights - Personal (basic)	Viva Learning (basic)	Webinars

Office 365

Enterprise Mobility + Security

Application Management Device Management Endpoint Analytics Information Protection

Intune Plan 1 for Business

Administrative Units	Advanced Security Reports & Alerts	App Proxy, including PingAccess	Cloud App Discovery	Conditional Access	Custom Security Attributes
Customized Sign-In Page	Dynamic Groups	Enterprise State Roaming	Entra ID Connect Health	External ID	Microsoft Identity Manager
Multi-Factor Auth (MFA)	Password Protection	Passwordless Authentication	Self-Service Group Management	Self-Service Password Reset in AD	Self-Service Activity Reports
Service Level Agreement	Shared Account Password Roll-Over	Single-Sign-On to other SaaS	SMS Sign-In	Temporary Access Pass	Terms of Use
Verified ID	Windows Autopilot	3rd Party MFA Integration			

Entra ID Plan 1

Enterprise Mobility + Security

Windows Pro

Application Control	Application Guard	AppLocker	Assigned Access
BitLocker	BitLocker to Go	Cortana	Defender Antivirus
Domain Join	Edge for Business	Entra ID Join	LAPS
Manage by MDM	Power Automate Attended Desktop Flows	Unbranded Boot	Universal Print
Windows Conditional Access	Windows Firewall	Windows Hello for Business	Windows Information Protection (retiring)
Windows Update for Business	24 months support for Windows 11		

Microsoft 365 Business Premium includes Windows Pro upgrade from earlier Pro versions + Universal Print

Windows Pro

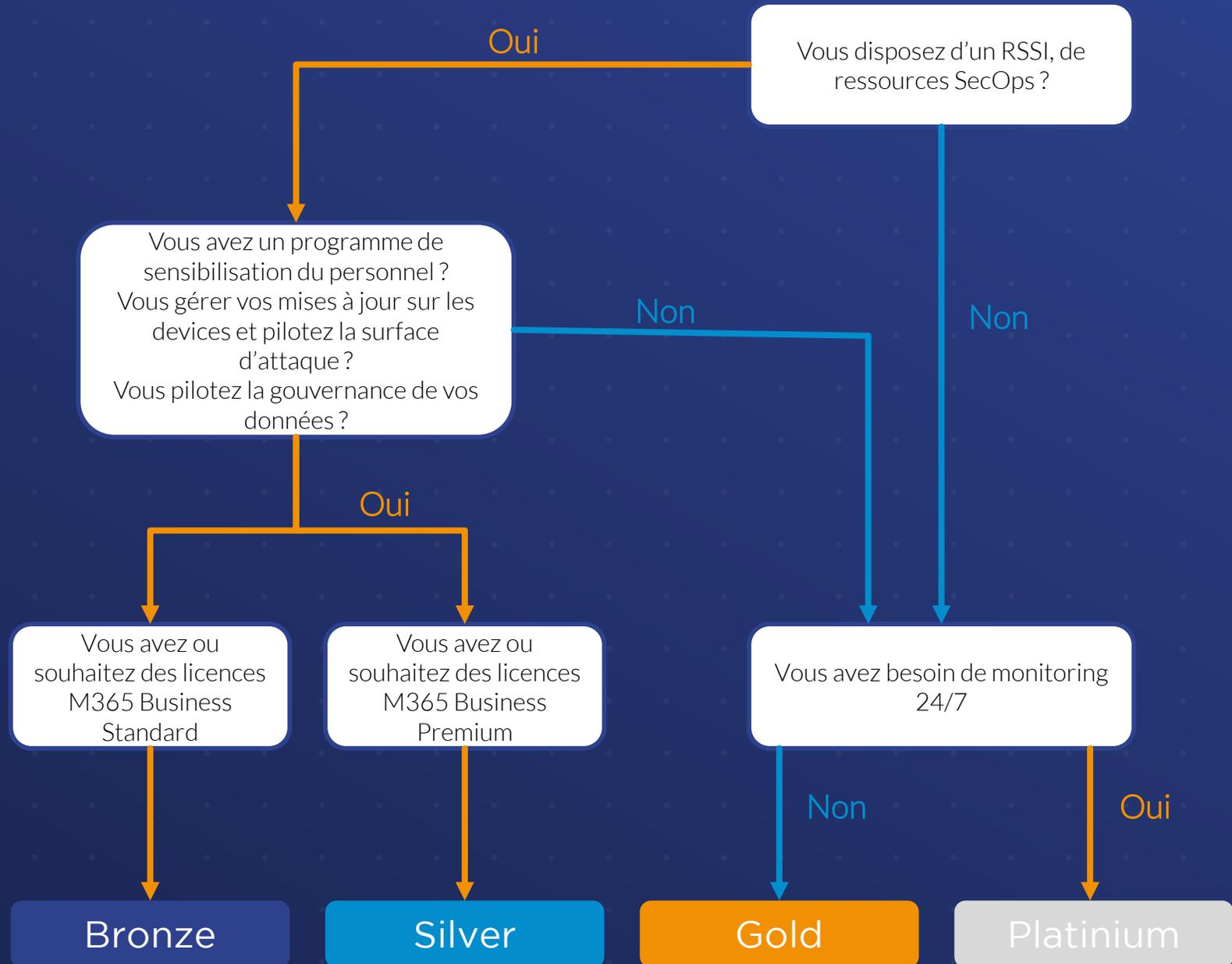
Automated Investigations	Block at First Sight
Cross-Platform Support	Endpoint Detection & Response
Enhanced ASR	Mobile Threat Defence
Next Gen Protection	Tamper Protection
Threat Analytics	Vulnerability Management (core)
Web Content Filtering	

Defender for Business



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 réglementations européennes dont NIS2
Analyse de la surface d'exposition externe



Mise en place du processus de surveillance permanente
Daily report



Option Cyber Coach
Options journées d'expertise
Option CSIRT

Elaboration de la feuille de route

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

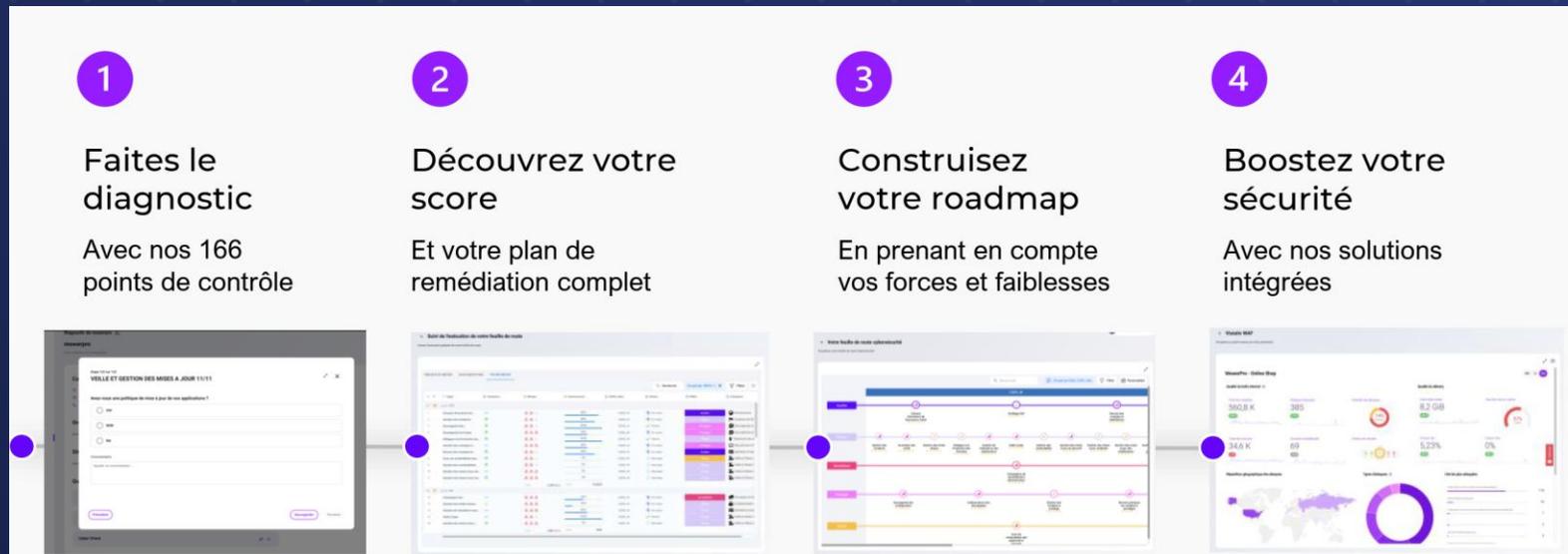
Posture vis-à-vis des
préconisations du
CIS pour les clients
disposant déjà d'un
environnement M365

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

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 réglementations européennes dont NIS2
- Analyse de la surface d'exposition externe
- Guides : PSSI, Charte, gestion de crise, RGPD, ...



Inclus dans Gold et Platinum,
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

1

- ✓ **Observation** : Utilisation de plusieurs bibliothèques JavaScript obsolètes
- ✓ **Risque** : L'utilisation de bibliothèques JavaScript obsolète pourrait permettre à un attaquant d'exploiter des vulnérabilités sur ces dernières et ainsi compromettre le bon fonctionnement du site.
- ✓ **Recommandation** : Mettre à jour les bibliothèques JavaScript remontées

2

- ✓ **Observation** : Les ports 6911/TCP, 5000/TCP, 5060/TCP, 5061/TCP et 5090/TCP sont ouverts et identifiés.
- ✓ **Risque** : Un attaquant peut utiliser ces ports ouverts comme vecteur d'attaque potentiel.
- ✓ **Recommandation** : Fermer ces ports si ils sont inutilisés, si cela n'est pas possible les filtrer.

1

Librairies JavaScript

- Selectize
- jQuery UI 1.10.3
- jQuery 3.1.0
- jQuery Migrate 3.1.0
- FingerprintJS
- jQuery 3.5.1
- FancyBox 2.1.5

A/B testing

- Nosto 4.1.0

2

Response Headers

```
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Wed, 06 Dec 2023 09:21:54 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Vary: Accept-Encoding, User-Agent
```

ID	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)

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

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

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

Inclus dans Gold et Platinum,
En option pour Silver

✓ Cyber Awareness

Formez vos collaborateurs à la cybersécurité

Search: [] Course Type: All Courses Subscription: All Courses

- 1 Pourquoi la cybersécurité est-elle importante ?**
Cours Mantra
Gérer les assignations Voir le cours
- 2 Pourquoi suis-je la cible des hackers ?**
Cours Mantra
Gérer les assignations Voir le cours
- 3 Qui sont les hackers et quelles sont leurs motivations ?**
Cours Mantra
Gérer les assignations Voir le cours
- 4 Quelles sont les principales méthodes de phishing ?**
Cours Mantra
Gérer les assignations Voir le cours

14:01
Alex > Disponible
compléter votre module de cybersécurité (5 min. max)

4

✗ Dommage, la bonne réponse était le phishing

Quel canal les cybercriminels utilisent pour faire du phishing ?

Seulement les appels
Uniquement le mail
Uniquement les SMS
Tous ces canaux

Tous ces canaux

✓ Bravo c'est la bonne réponse

Les cybercriminels sont susceptibles d'utiliser tous ces canaux

Tapez un message

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 ✓

Users Progress

Display subscribed courses only

Add filter

First name	Last name	Language	Departments	Completion %	Status
Nevada	Allen	FR	Sales	82%	On Track
Willow	Evans	FR	Tech	40%	On Track
Lynsey	Campbell	EN	HR	27%	On Track

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

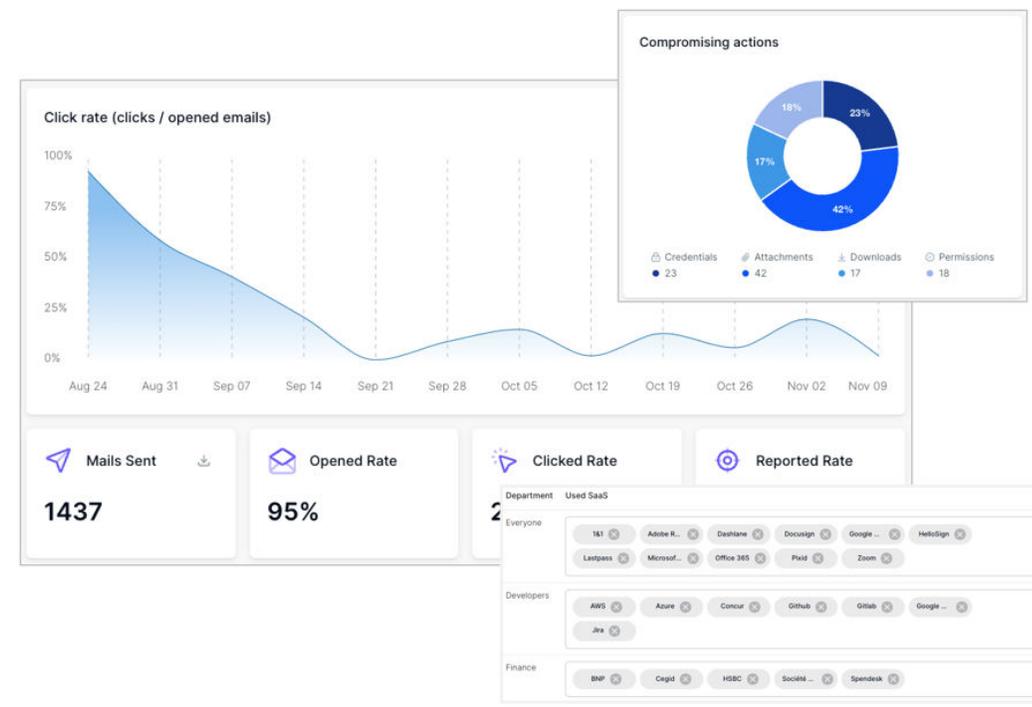
Mantra

Mantra

Inclus dans Gold et Platinum,
En option pour Silver

✓ Phishing Simulation

Entraînez vos utilisateurs en situation réelle



Principales fonctionnalités

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



Campagne de test de phishing

Campagnes de simulation de phishing personnalisées au profil de votre entreprise



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

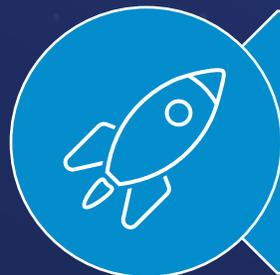


Mise à disposition de ressources

Des options pour augmenter votre sécurité



RSSI As A Service



Journées
d'expertise



CSIRT

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

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

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



UNE ÉQUIPE D'EXPERTS POUR VOUS ACCOMPAGNER.

Grâce à l'expertise de nos équipes, ses outils (SIRP) et sa base de connaissances regroupant l'intégralité des incidents de sécurité, nous serons à même de répondre rapidement à toutes vos problématiques.

- Identifier et catégoriser l'attaque
- Contenir l'attaque pour empêcher la propagation
- Mettre fin aux agissements des attaquants
- Retourner rapidement à un état fonctionnel
- Renforcer la sécurité et la réponse de l'entreprise

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

