bluesecure

NEWSLETTER · 10.2026

Octobre en trois temps forts.

01 · CYBERMOIS 2026

Notre kit de communication, offert à vos équipes.

Télécharger →

02 · ÉVÉNEMENT

Les Assises à Monaco

03 · DÉCRYPTAGE

50 °C

Les frigos pirates

AUSSI : 2 LEARNINGS · MAILWATCH® · 4 SCÉNARIOS

+ NOUVEAUX LEARNINGS

Deux modules, deux publics.

DIRIGEANTS

NIS2

Ce que la directive impose concrètement : gestion des risques, notification des incidents, coopération avec l'ANSSI.

Le module aborde aussi la responsabilité personnelle du dirigeant, pour engager dès maintenant sa gouvernance cyber.

35 MIN · 3 PARTIES

Suivre le module →

TOUS LES COLLABORATEURS

Phishing

Quatre tendances en forte progression : messages rédigés par IA, clonage de voix, invitations d'agenda et pièces jointes SVG détournées, fausses fenêtres de connexion.

Pour chacune, les réflexes concrets pour ne pas se faire piéger.

7 MIN

Suivre le module →

+ PLATEFORME · MAILWATCH®

La vigilance, directement dans la boîte mail.

Intégré à votre environnement Microsoft 365, sans que BlueSecure accède à votre messagerie. Deux briques, pensées pour vos équipes IT.

BANNIÈRE MAILWATCH®

Demande financière sensible. Vérifiez par un autre canal avant d'agir.

Bannières de vigilance

Vous choisissez les situations à signaler : domaine proche du vôtre, nom d'un collègue utilisé depuis l'extérieur, demande financière sensible. Les règles sont créées dans votre tenant : aucun e-mail ne transite par BlueSecure.

Analyse à la demande

Un bouton dans Outlook : le collaborateur soumet un message douteux et reçoit un verdict, avec des indices expliqués en langage courant. IA hébergée en France, contenu non conservé.

UNE BANNIÈRE EST UN POINT DE VIGILANCE, PAS UN VERDICT.

+ PHISHING

6 nouveaux scénarios

Des notifications de compte en ligne, un prétexte classique du phishing. Prêts à intégrer à vos campagnes.

ZOHO **« Réinitialisation de mot de passe »**	BASECAMP **« Ouverture de session »**
BOX **« Compte suspendu »**	DYNATRACE **« Nouvelle connexion détectée »**
WEBFLOW **« Vous avez été invité »**	MY.COREL.GROUP **« Nouvelle publication »**

Tester les scénarios →

+ CYBERMOIS 2026 — KIT GRATUIT +

La sensibilisation ne s'arrête pas en octobre.



Le CyberMois touche à sa fin, les bons réflexes se cultivent toute l'année. Notre kit reste gratuit : trois contenus prêts à partager avec vos équipes.

01 · E-MAIL	02 · AFFICHE	03 · POST
À diffuser en interne, auprès de tous vos collaborateurs.	À imprimer pour vos locaux et espaces communs.	À publier sur votre intranet ou vos réseaux.

Télécharger le kit →

LES ASSISES DE LA CYBERSÉCURITÉ · MONACO · 07-10.10.2026



+ ÉVÉNEMENT

Quatre jours à Monaco.

Quatre jours de rencontres et d'échanges autour des grands enjeux de la cybersécurité. Nous y avons partagé notre vision de la sensibilisation et de l'engagement des collaborateurs.

- **Rencontres** avec clients, partenaires et décideurs cyber
- **Démonstrations de deepfake** sur notre stand
- **Conférence** sur la gamification au service de la sensibilisation

Retour sur les Assises ↗

+ CAS D'ATTAQUE · 11-12.10.2026

50 °C

Des frigos de supermarchés piratés à distance.

Dans la nuit du 11 au 12 octobre, des pirates ont détourné la fonction de dégivrage en passant par d'anciens contrôleurs Danfoss qui ne reçoivent plus de mises à jour. Des produits frais et surgelés ont dû être jetés, et Intermarché parle de plusieurs dizaines de millions d'euros de pertes. Le parquet de Paris a ouvert une enquête et l'ANSSI a alerté les entreprises concernées.

~150	~100	5 %
magasins Intermarché et Netto	magasins U	des Monoprix, plus des E.Leclerc et Carrefour Market

À RETENIR

- **Un équipement connecté est un ordinateur.** Caméra, imprimante, badgeuse ou écran peuvent être piratés comme un PC.
- **Un système sans mises à jour est une porte ouverte.** Avant de brancher un appareil au réseau, prévenez votre équipe IT.
- **Un comportement inhabituel ?** Signalez-le. Mieux vaut un faux positif qu'une attaque qui passe.

SOURCES : LE DAUPHINÉ LIBÉRÉ, AFP, BFMTV

+ LA SUITE · DANS LA PRESSE

Des frigos aux réseaux d'eau, l'OT touche le monde physique.

L'attaque des frigos le rappelle : une menace numérique peut avoir des conséquences très concrètes sur des activités physiques.

JDX

Cybersécurité industrielle : le facteur humain, angle mort des environnements OT

TRIBUNE · JOURNAL DU NET

« Le facteur humain, angle mort des environnements OT »

Jean-Baptiste Arfignan · 12.10.2026

Lire la tribune ↗

Restez informé(e), restez protégé(e).

Un problème technique ? Contactez notre support. Pour une demande fonctionnelle, votre **Customer Success Manager** vous accompagne.

bluesecure