DIRECTION GENERALE DU NUMERIQUE
ET DES SYSTÈMES D'INFORMATION (DGNSI)

Le rôle des secrétaires municipaux dans la cyber-résilience communale

Journées de formation secrétaires municipaux AVSM, le 27 mai et 4 juin 2026

Fiona Ponzo & Nicolas Patthey

Une crise cyber commence souvent comme une matinée ordinaire.

08h17

Plus d'accès à la boite email du greffe et à la GED

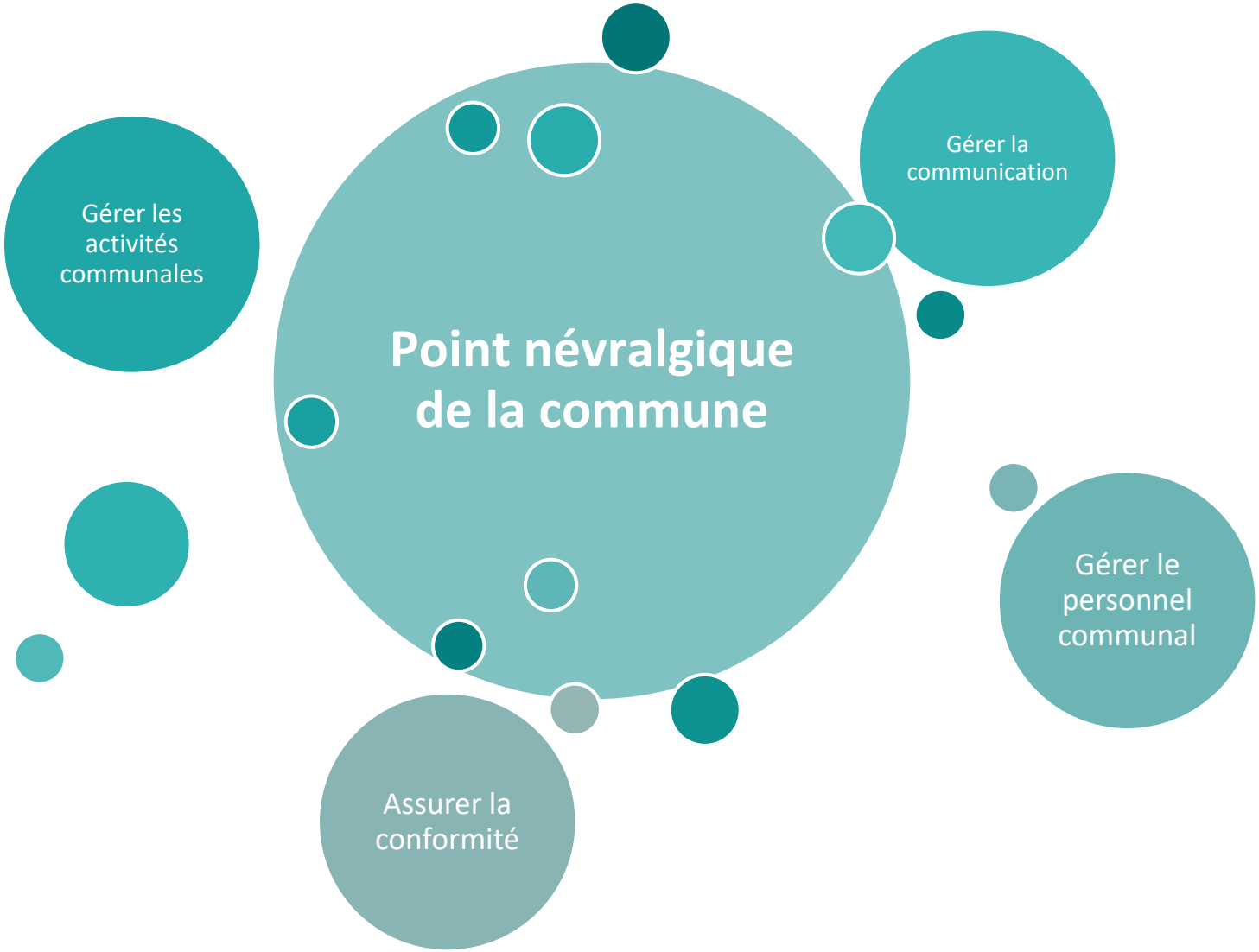
08h22
le syndic vous appelle

08h30
le guichet ouvre

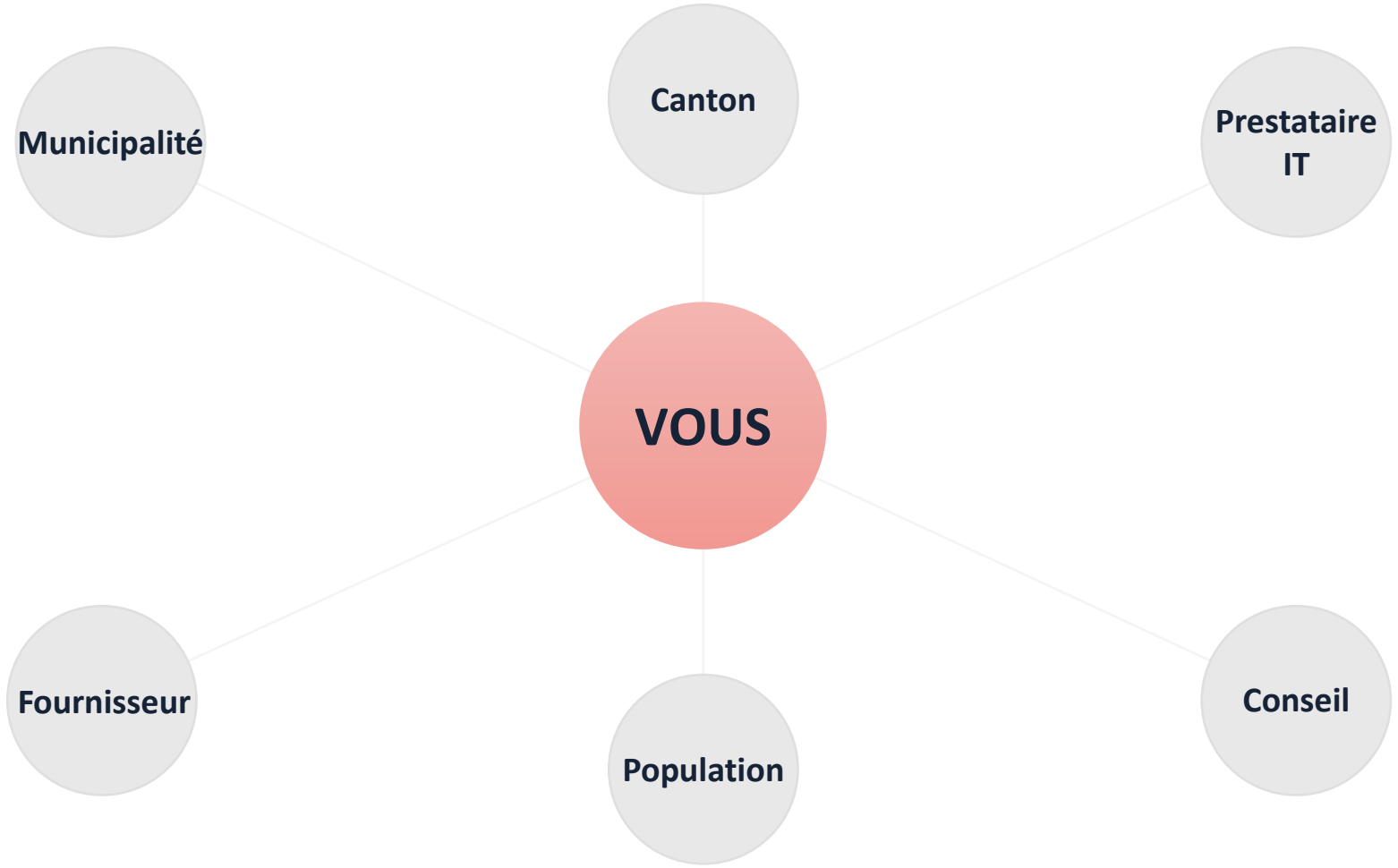
08h35
votre prestataire IT ne répond pas

Votre premier reflexe ?

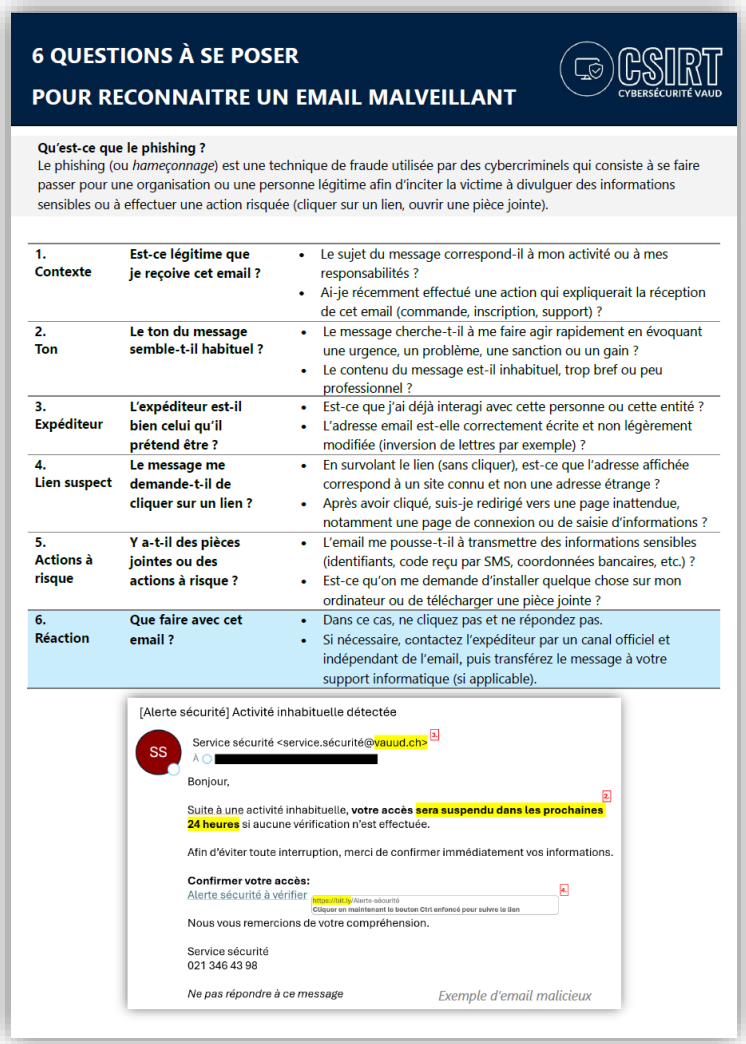
En tant que secrétaire municipal, vous êtes la cible et la solution.



Pourquoi la cible ?



Détecter un email malicieux grâce à notre checklist



6 QUESTIONS À SE POSER
POUR RECONNAITRE UN EMAIL MALVEILLANT

CSIRT CYBERSÉCURITÉ VAUD

Qu'est-ce que le phishing ?
Le phishing (ou *hameçonnage*) est une technique de fraude utilisée par des cybercriminels qui consiste à se faire passer pour une organisation ou une personne légitime afin d'inciter la victime à divulguer des informations sensibles ou à effectuer une action risquée (cliquer sur un lien, ouvrir une pièce jointe).

1. Contexte	**Est-ce légitime que je reçoive cet email ?**	• Le sujet du message correspond-il à mon activité ou à mes responsabilités ? • Ai-je récemment effectué une action qui expliquerait la réception de cet email (commande, inscription, support) ?
2. Ton	**Le ton du message semble-t-il habituel ?**	• Le message cherche-t-il à me faire agir rapidement en évoquant une urgence, un problème, une sanction ou un gain ? • Le contenu du message est-il inhabituel, trop bref ou peu professionnel ?
3. Expéditeur	**L'expéditeur est-il bien celui qu'il prétend être ?**	• Est-ce que j'ai déjà interagi avec cette personne ou cette entité ? • L'adresse email est-elle correctement écrite et non légèrement modifiée (inversion de lettres par exemple) ?
4. Lien suspect	**Le message me demande-t-il de cliquer sur un lien ?**	• En survolant le lien (sans cliquer), est-ce que l'adresse affichée correspond à un site connu et non une adresse étrange ? • Après avoir cliqué, suis-je redirigé vers une page inattendue, notamment une page de connexion ou de saisie d'informations ?
5. Actions à risque	**Y a-t-il des pièces jointes ou des actions à risque ?**	• L'email me pousse-t-il à transmettre des informations sensibles (identifiants, code reçu par SMS, coordonnées bancaires, etc.) ? • Est-ce qu'on me demande d'installer quelque chose sur mon ordinateur ou de télécharger une pièce jointe ?
6. Réaction	**Que faire avec cet email ?**	• Dans ce cas, ne cliquez pas et ne répondez pas. • Si nécessaire, contactez l'expéditeur par un canal officiel et indépendant de l'email, puis transférez le message à votre support informatique (si applicable).

[Alerte sécurité] Activité inhabituelle détectée

SS Service sécurité <service.sécurité@vauud.ch>
À [redacted]

Bonjour,

Suite à une activité inhabituelle, **votre accès sera suspendu dans les prochaines 24 heures** si aucune vérification n'est effectuée.

Afin d'éviter toute interruption, merci de confirmer immédiatement vos informations.

Confirmer votre accès:
Alerte sécurité à vérifier https://bit.ly/Alerte-sécurité Cliquer en maintenant le bouton Ctrl enfoncé pour suivre le lien

Nous vous remercions de votre compréhension.

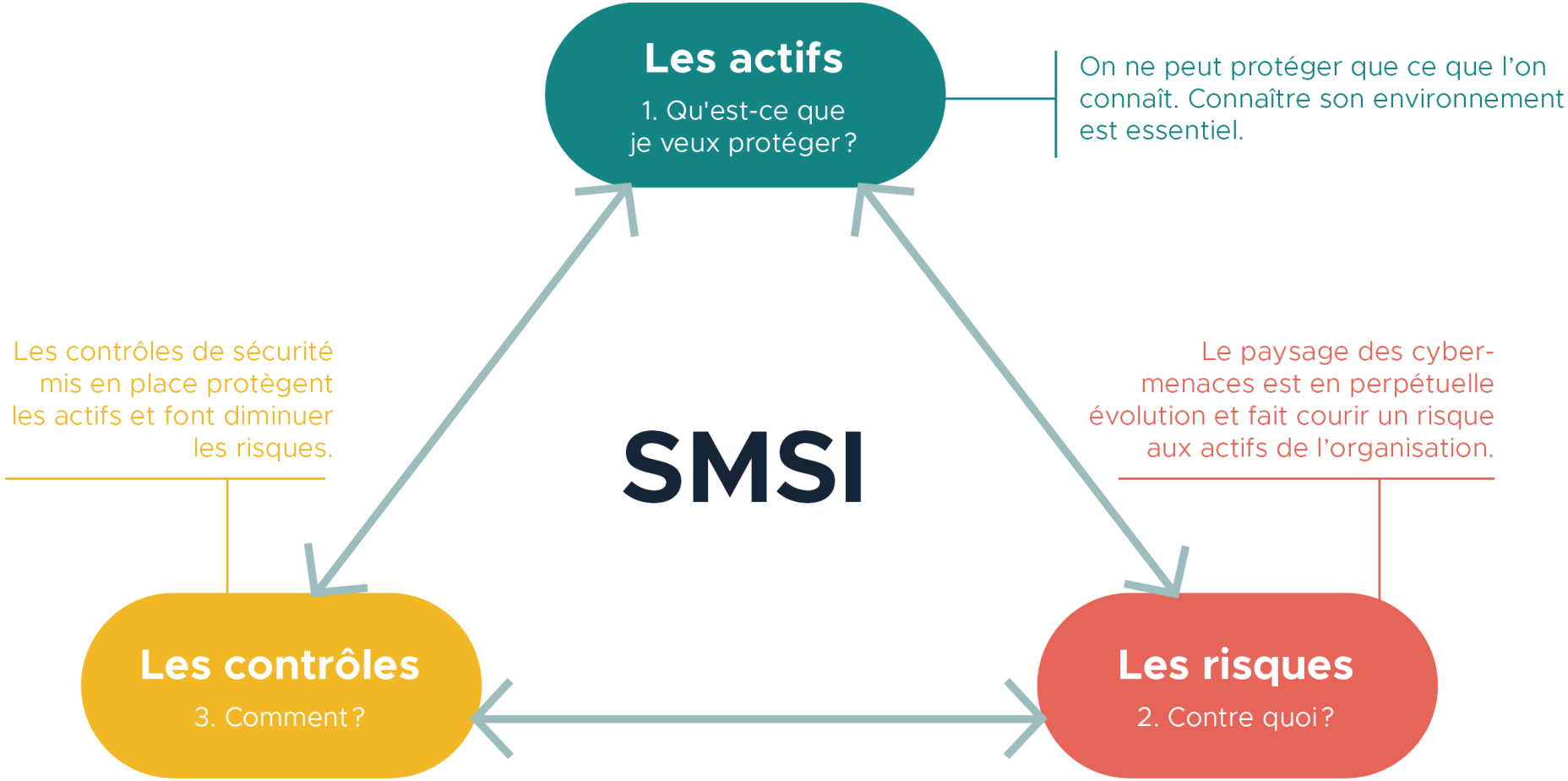
Service sécurité
021 346 43 98

Ne pas répondre à ce message

Exemple d'email malicieux

1. Contexte	**Est-ce légitime que je reçoive cet email ?**	• Le sujet du message correspond-il à mon activité ou à mes responsabilités ? • Ai-je récemment effectué une action qui expliquerait la réception de cet email (commande, inscription, support) ?
2. Ton	**Le ton du message semble-t-il habituel ?**	• Le message cherche-t-il à me faire agir rapidement en évoquant une urgence, un problème, une sanction ou un gain ? • Le contenu du message est-il inhabituel, trop bref ou peu professionnel ?
3. Expéditeur	**L'expéditeur est-il bien celui qu'il prétend être ?**	• Est-ce que j'ai déjà interagi avec cette personne ou cette entité ? • L'adresse email est-elle correctement écrite et non légèrement modifiée (inversion de lettres par exemple) ?
4. Lien suspect	**Le message me demande-t-il de cliquer sur un lien ?**	• En survolant le lien (sans cliquer), est-ce que l'adresse affichée correspond à un site connu et non une adresse étrange ? • Après avoir cliqué, suis-je redirigé vers une page inattendue, notamment une page de connexion ou de saisie d'informations ?
5. Actions à risque	**Y a-t-il des pièces jointes ou des actions à risque ?**	• L'email me pousse-t-il à transmettre des informations sensibles (identifiants, code reçu par SMS, coordonnées bancaires, etc.) ? • Est-ce qu'on me demande d'installer quelque chose sur mon ordinateur ou de télécharger une pièce jointe ?
6. Réaction	**Que faire avec cet email ?**	• Dans ce cas, ne cliquez pas et ne répondez pas. • Si nécessaire, contactez l'expéditeur par un canal officiel et indépendant de l'email, puis transférez le message à votre support informatique (si applicable).

Pourquoi la solution ?



Un document de soutien dans votre démarche de cybersécurité

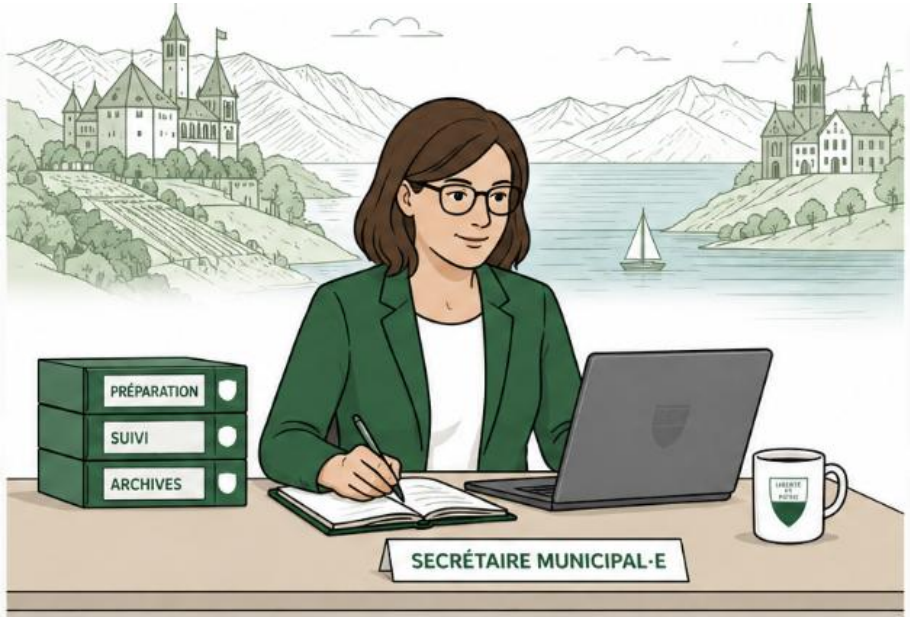
Exemple de contrôles fondamentaux pour votre commune

Niveau de priorité	Gouvernance	Gestion des actifs	Protection des données	Gestion des accès	Infrastructure	Réponse à incidents et continuité
1	**1.1** Former et sensibiliser aux fondamentaux **1.2** Définir une politique de sécurité de l'information	**1.3** Recenser les actifs **1.4** Maintenir les actifs à jour	**1.5** Définir une politique de classification et de gestion de l'information	**1.6** Définir une politique de mots de passe **1.7** Renforcer l'authentification **1.8** Sécuriser les accès à distance **1.9** Gérer les comptes administrateurs **1.10** Définir une politique de gestion des accès et des identités	**1.11** Sécuriser le réseau **1.12** Sécuriser les postes **1.13** Sécuriser le Wi-Fi	**1.14** Sauvegarder les données
2	**2.1** Organiser des programmes de formation et simuler des attaques de phishing	**2.4** Gérer le cycle de vie des actifs	**2.5** Inventorier et classifier les données	**2.7** Contrôler les accès et identités	**2.9** Détecter et gérer les vulnérabilités	**2.12** Préparer la continuité **2.13** Gérer les incidents

Pourquoi la solution ?

Vous avez toutes les compétences métiers pour faire de la cybersécurité :

- Mise en place de processus
- Gestion du personnel
- Coordination entre les acteurs
- Gestion de la communication



Votre rôle pendant une cybercrise

La coordination vaut autant que la technique.

«The more you sweat in peace, the less you bleed in war.»

« Plus vous suez en temps de paix, moins vous saignez en temps de guerre. »

La préparation est la clé.

Qui appeler ?

Contacts
d'urgence

Qui décide ?

Rôles
clarifiés

Quoi maintenir ?

Processus critiques et
planS de continuité

La résilience commence avant la crise.

Le CSIRT est là pour vous éviter de subir un cyberincident.

Veille	**Paysage des cybermenaces**
Renforcement cybersécurité	**Document mesures essentielles de cybersécurité**
Formation	**Site internet et formation UCV**
Communauté	**Exercice de crise CYBER26**

Mais quand est-ce la crise?

Appel au 117 en cas de cyberattaque

L’unité **Cybercrime** de la Police prend contact avec la **force d’intervention**

La gestion des cyberattaques avec le support du Canton

Légende: CSIRT | Commune, Paraétatique

Fonctionnement normal – hors crise

Annonce via 117

Municipalité, direction de l'entité

CYBER **RÉACTION**

Répondant Cybersécurité

Support pour réponse technique

Equipes IT

Corrections et réparations

Prestataires IT

Selon services contractualisés

Fonctionnement en crise

Cellule de crise

Municipalité, direction de l'entité
Décisions, validations

Structure de conduite de crise
Coordination et support à la gestion de crise

SOC (DGNSI)
Cybercrime (PolCant)
EMCC

Experts pour réponse technique

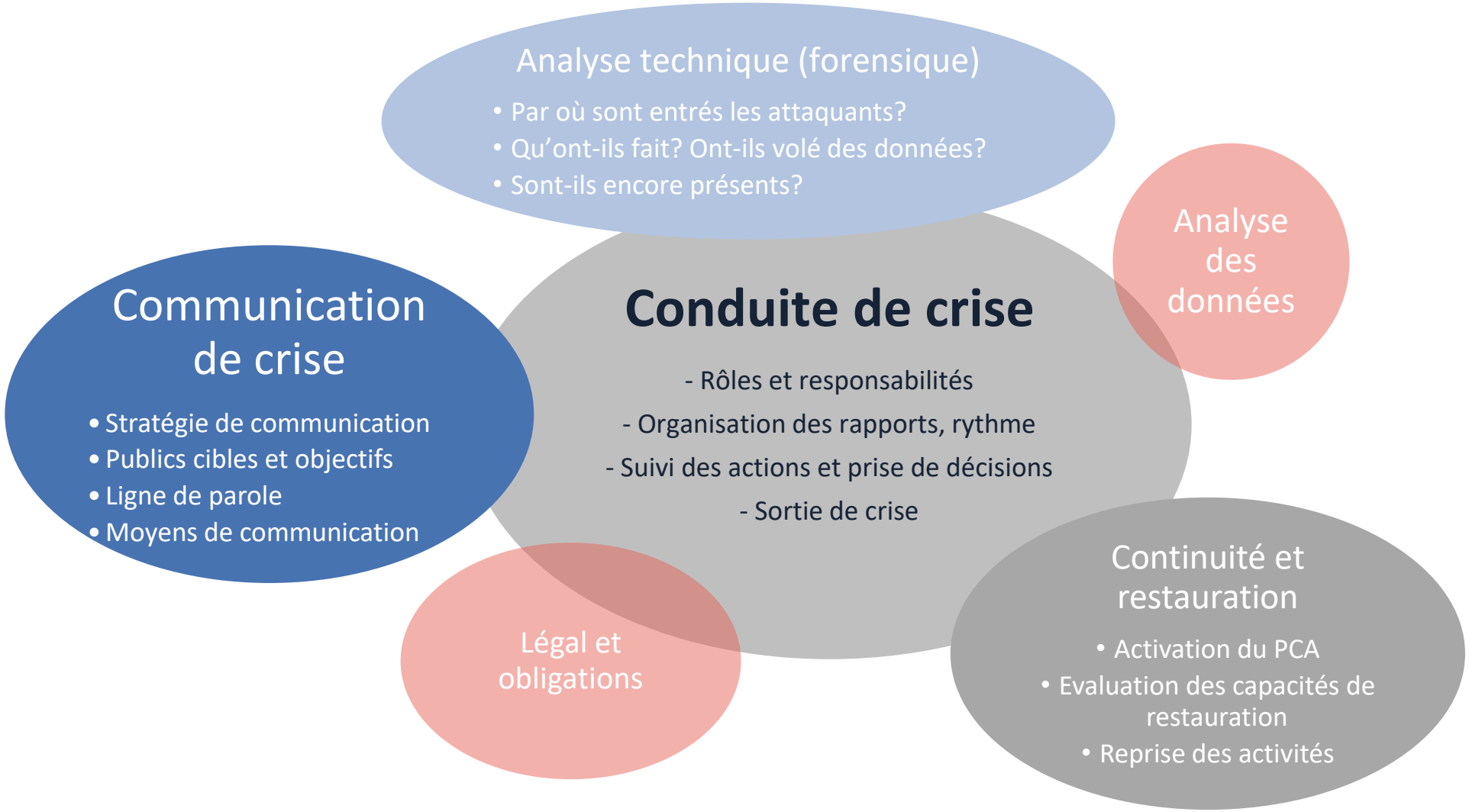
Equipes IT

Prestataires IT

Principales parties prenantes externes à intégrer / coordonner en cas de crise

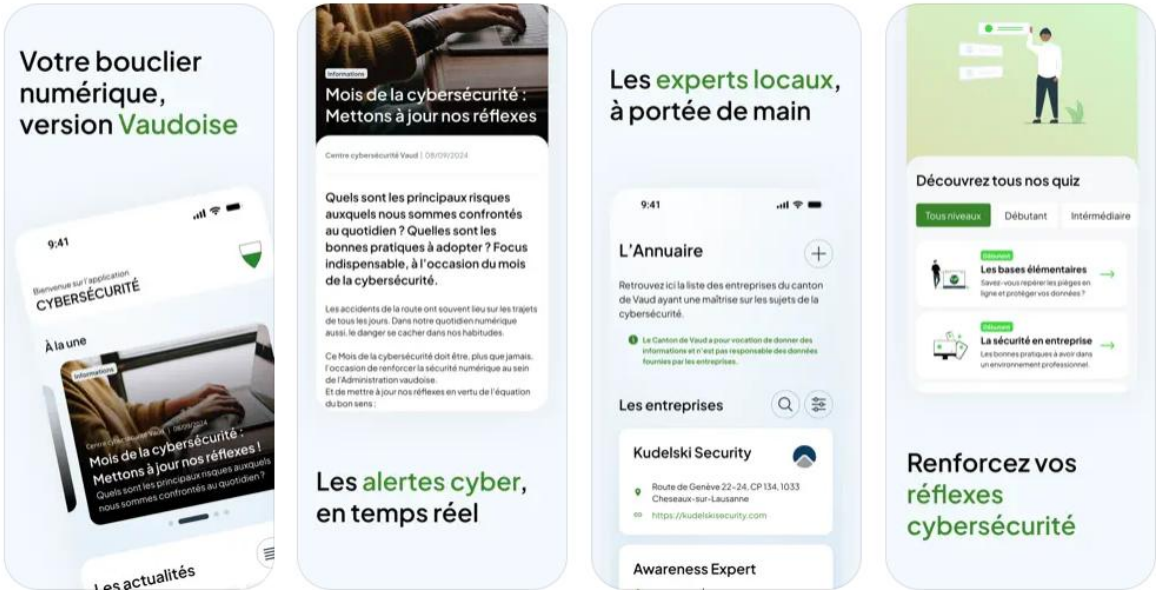
- *GovCERT, NCSC*
- *Etat de Vaud*
- *Confédération*
- *APDI*
- *Médias - Presse*
- *Collaborateurs*
- *Administrés*
- *Cybercriminels*

Accompagnement à la gestion de crise



Les informations utiles

- Consultez régulièrement notre site internet **https://www.vd.ch/cybersecurite**
- Téléchargez l'application mobile **« Cybersécurité Vaud »**
- Prenez contact avec le CSIRT pour toutes vos questions (hors crise): **csirt@vd.ch**
- Appelez le **117** en cas de cyberattaque !



Nos prochains évènements à ne pas manquer…

Séances pour les répondants cybersécurité	• Option 1 : 26 juin de 11h à 12h • Option 2 : 1 juillet de 14h30 à 15h30	En ligne
Evénèment Cybersec Connect	30 juin toute la matinée + apéro lunch	En présentiel à Yverdon (lieu exact à confirmer)
Exercice de crise CYBER26	12 novembre dans la matinée	Dans votre salle de crise

Merci de votre attention

Des questions ?