CSIRT

Présentation de la force cantonale d'intervention cybersécurité

TLP:CLEAR

(https://www.first.org/tlp/)

CSIRT
CYBERSÉCURITÉ VAUD

canton de vaud
DGNSI

Direction générale du numérique
et des systèmes d'information (DGNSI)

Classification PUBLIC

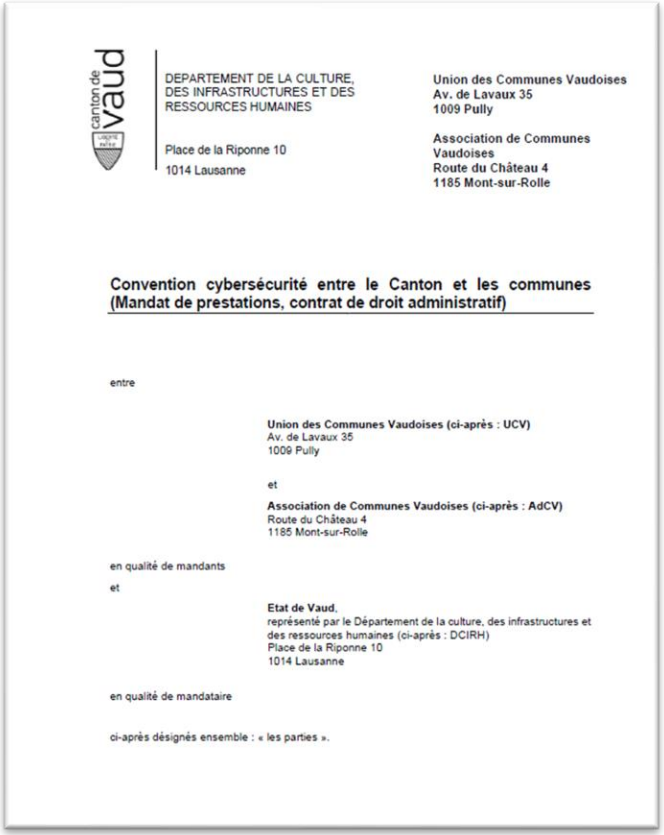
Présentation CSIRT - FPO – V.1.3

Agenda

1. BREF RAPPEL DU CONTEXTE DE LA CONVENTION
2. LA FORCE D'INTERVENTION ET LA GESTION DE CRISE
3. PRÉSENTATION DES ACTIVITÉS DU CSIRT
4. BILAN DU PREMIER SEMESTRE
5. ACTIVITÉS - FIN D'ANNÉE 2024

1/ Bref rappel du contexte

Bref rappel du contexte de la convention



canton de vaud

DEPARTEMENT DE LA CULTURE, DES INFRASTRUCTURES ET DES RESSOURCES HUMAINES

Place de la Riponne 10
1014 Lausanne

Union des Communes Vaudoises
Av. de Lavaux 35
1009 Pully

Association de Communes Vaudoises
Route du Château 4
1185 Mont-sur-Rolle

Convention cybersécurité entre le Canton et les communes (Mandat de prestations, contrat de droit administratif)

entre

Union des Communes Vaudoises (ci-après : UCV)
Av. de Lavaux 35
1009 Pully

et

Association de Communes Vaudoises (ci-après : AdCV)
Route du Château 4
1185 Mont-sur-Rolle

en qualité de mandants

et

Etat de Vaud,
représenté par le Département de la culture, des infrastructures et des ressources humaines (ci-après : DCIRH)
Place de la Riponne 10
1014 Lausanne

en qualité de mandataire

ci-après désignés ensemble : « les parties ».

Signature & entrée en vigueur:
Signée en juillet 2023, pour un démarrage opérationnel au 1er janvier 2024 et jusqu'à fin 2027 (pour le premier cycle)

Champs d'application:
L'ensemble des communes vaudoises et 137 associations intercommunales

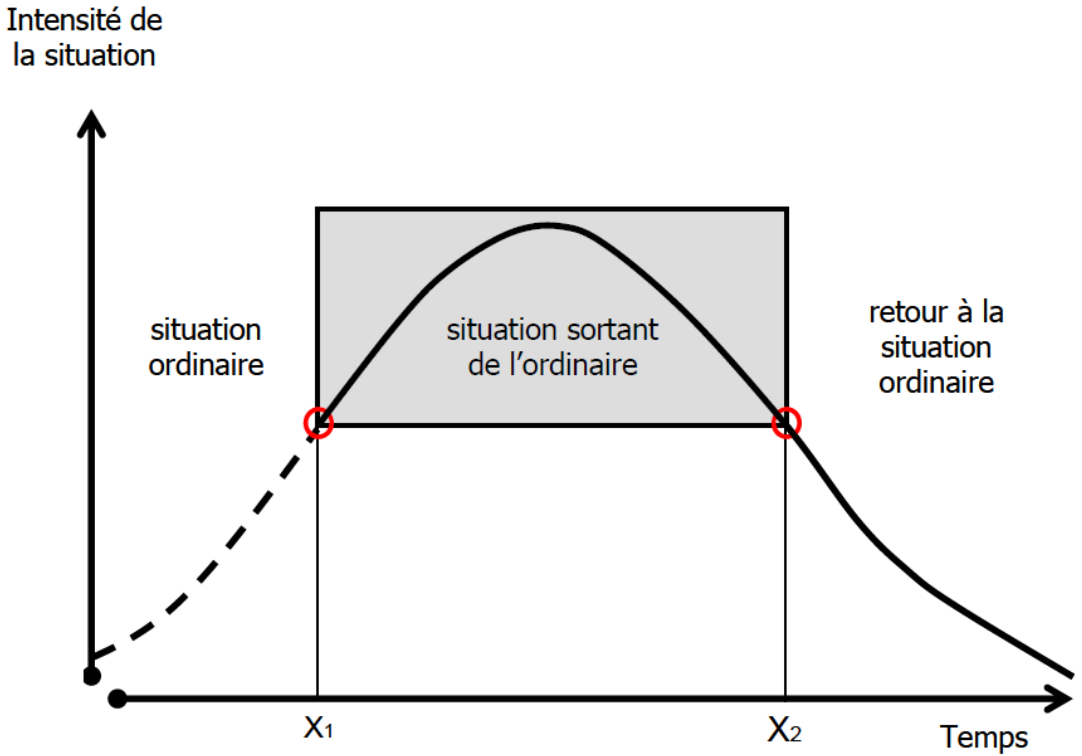
Objet de la convention:
Mise en œuvre d'une force d'intervention cantonale pour défendre les communes et associations intercommunales contre les cyber-risques, contre rémunération de l'Etat (obligation générale de moyens)

Financement:
Couvre les coûts de 2 experts cybersécurité et la mise à disposition d'une réponse technique d'urgence au travers de prestaires privés locaux

Comité de pilotage:
Comité opérationnel avec 4 représentants du Canton (avec présidence à la DGNSI) et 4 représentants des communes

2/ La force d'intervention et la gestion de crise

Une force d'intervention pour les cyberattaques

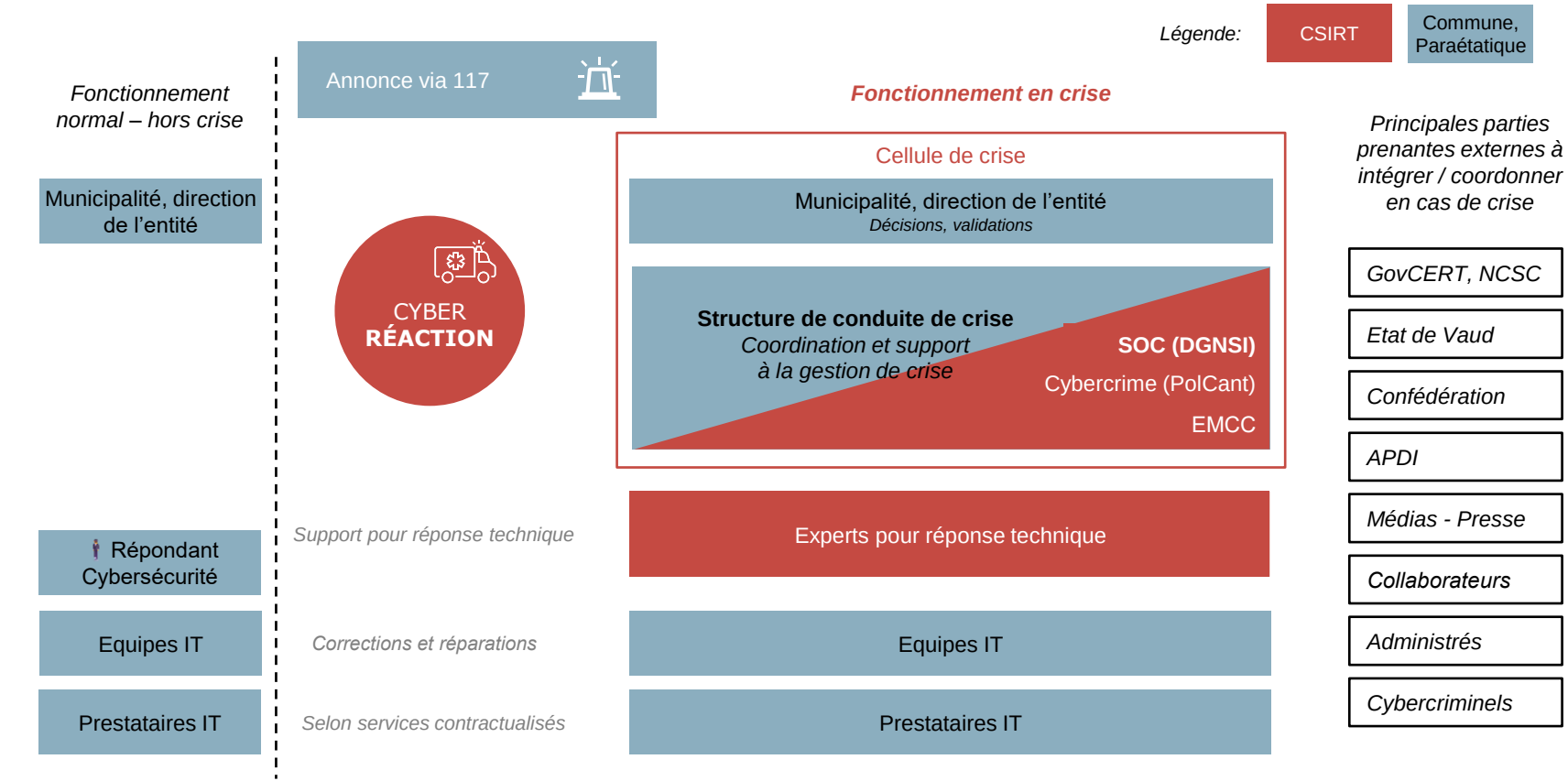


Source : Doctrine EMCC

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



3/ Présentation des activités de la force d'intervention

Périmètre du service CSIRT – édition 2024

Les axes de la Convention

CYBER **RÉACTION**

CYBER **RÉSILIENCE**

CYBER **PRÉVENTION**

Gestion de crise et réponse cyberincident

Renforcement cybersécurité

Formation

Veille

Communauté

Participez à notre prochain exercice de gestion de crise

- Date : **5 décembre 2024**
- Scénario : Simulation de cyberattaques sur plusieurs organisations du Canton exploitant des infrastructures critiques
- Participants: Infrastructures critiques comme communes et associations intercommunales, CHUV, etc…
- Objectifs pour les parties prenantes exercées : Tester leur gestion de crise et leurs plans de continuité ainsi que leur remontée d'information à l'EMCC/CSIRT (PCO)

Les inscriptions sont ouvertes, déjà 60 entités inscrites

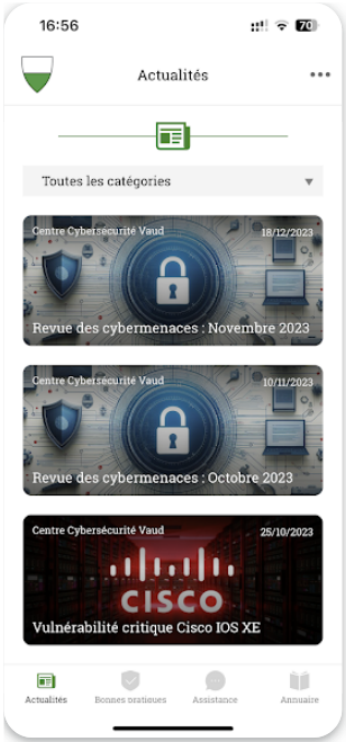
D’autres évènements sont à prévoir !

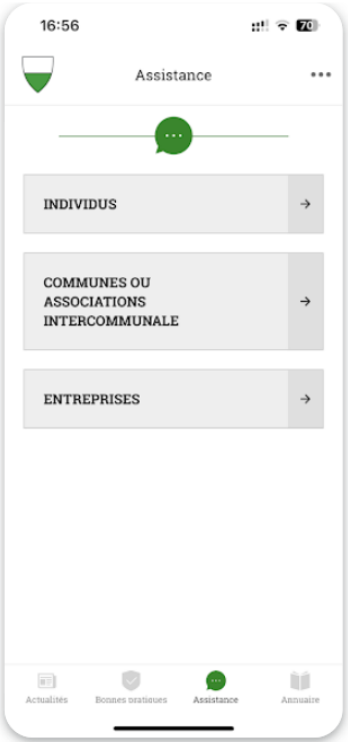
Après le succès du premier évènement Cybersec Connect pour les communes, d’autres événements vont s’organiser

Restez informés grâce à notre application mobile

Restez informés grâce à l'application Cybersécurité Vaud

Cybersécurité Vaud *dans les App-Stores*





Consultez notre page internet vd.ch/cybersecurite

https://www.vd.ch/toutes-les-autorites/departements/departement-de-la-culture-des-infrastructures-et-des-ressources-humaines-dcirh/direction-generale-du-numeri

Ressources de formation

Les ressources de formation visent à acquérir les connaissances et les compétences nécessaires pour se protéger des cyberattaques.

Assurez votre sécurité en ligne

Campagne de sensibilisation à la sécurité en ligne sur les thèmes suivants : protéger ses données ; les sites malveillants ; le phishing ; les mots de passe

eSUSI

Module de sensibilisation et de formation en ligne des utilisateurs à la sécurité de l'information, développé par le groupe latin Sécurité de l'Administration numérique suisse

eCyAd

Formation en ligne sur la sécurité de l'information pour les autorités

4/ Bilan du premier semestre

Présentation des faits marquants

Bilan – Semestre 1/2024

Réponse à incident

- 3 interventions en lien avec des cyberattaques

Renforcement cybersécurité

- Document de gouvernance du service et définition des rôles et responsabilités
- 1 questionnaire « statut initial cybersécurité »

Veille cybersécurité

- 6 bulletins cybermenaces publiés
- Suivi des vulnérabilités avec les communes

Formation

- Nouveau contenu de formation en ligne
- Proposition d'une nouvelle formation cybersécurité UCV

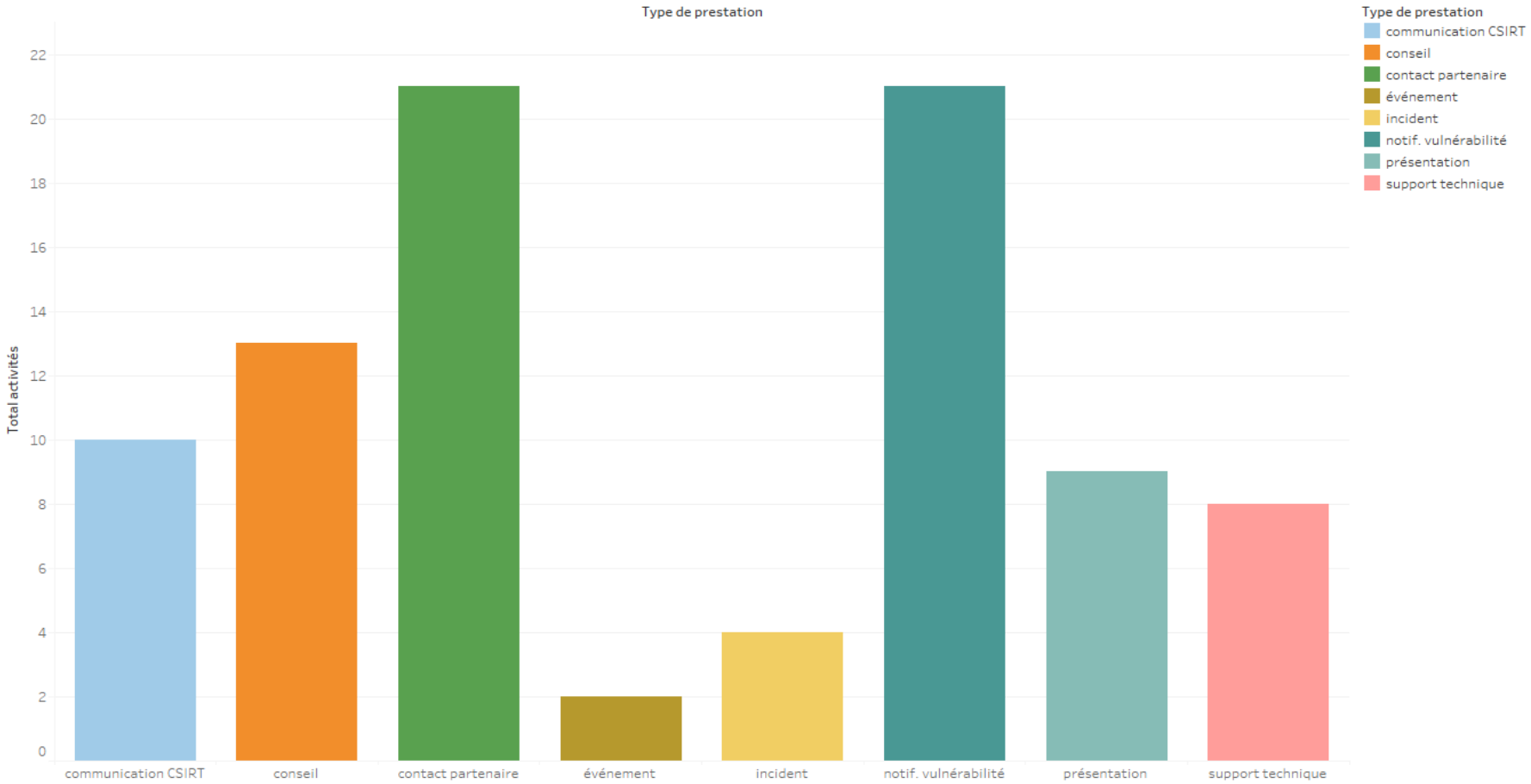
Communauté

- 3 rencontres des syndics (3/10)
- 3 présentations extérieures
- 1 publication dans le journal le PointCommUNE
- 1 évènement « Cybersec Connect »

Pilotage

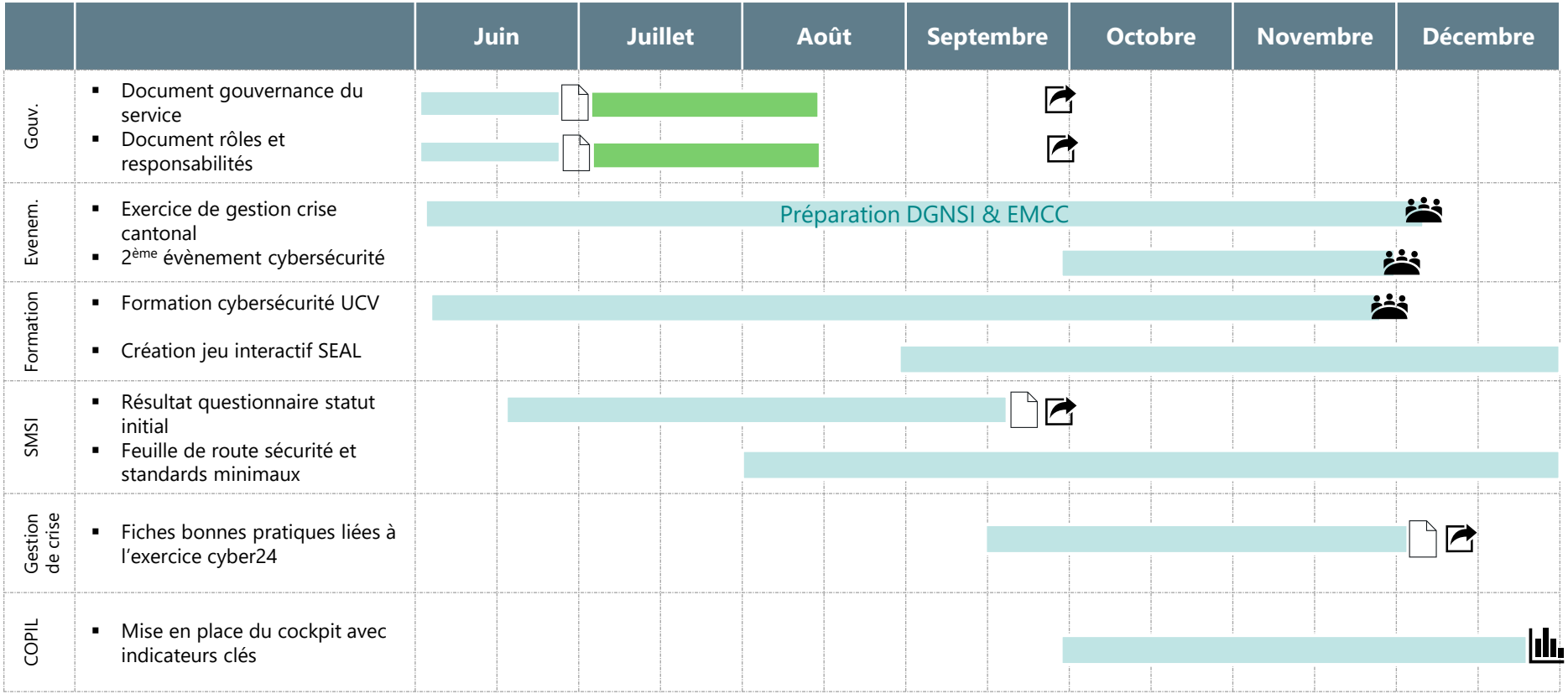
- 1 synchro COPIL
- 1 séance COPIL
- 3 rapports flash

Volumétrie de l'activité par catégorie



6/ Activités fin d'année 2024

Planning 2ème semestre 2024



Les informations à retenir

- Appelez le 117 en cas de suspicion de cyberattaque
- Téléchargez l'application mobile
- Consultez régulièrement notre site internet vd.ch/cybersecurite
- Inscrivez-vous au prochain exercice de crise cantonal
- Prenez contact avec le CSIRT pour toutes vos questions (hors crise) : csirt@vd.ch

ENSEMBLE
POUR UNE SOCIÉTÉ
NUMÉRIQUE RESPONSABLE

canton de vaud

Direction générale du numérique
et des systèmes d'information (DGNSI)

CSIRT
CYBERSÉCURITÉ VAUD

Annexes

Périmètre du service CSIRT – édition 2024

Les axes de la Convention

CYBER **RÉACTION**

Gestion de crise et réponse cyberincident

CYBER **RÉSILIENCE**

Renforcement cybersécurité

Veille

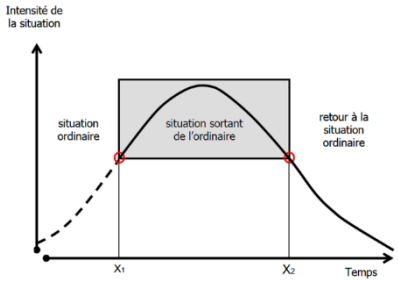
CYBER **PRÉVENTION**

Formation

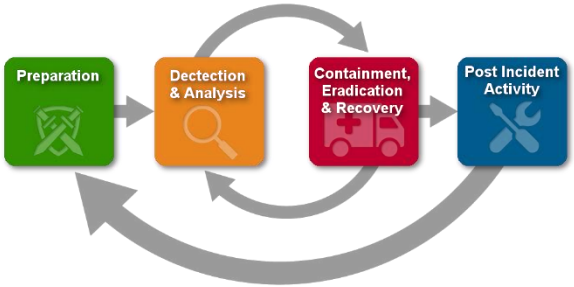
Communauté

Pilier : Gestion de crise et réponse cyberincident

Gestion de crise et communication

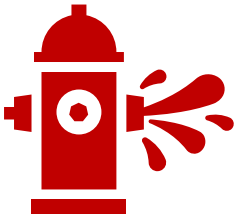


Réponse cyberincident



Gestion de la continuité

Gestion d'une fuite de données



Périmètre du service CSIRT – édition 2024

Les axes de la Convention

CYBER **RÉACTION**

CYBER **RÉSILIENCE**

CYBER **PRÉVENTION**

Gestion de crise et réponse cyberincident

Renforcement cybersécurité

Formation

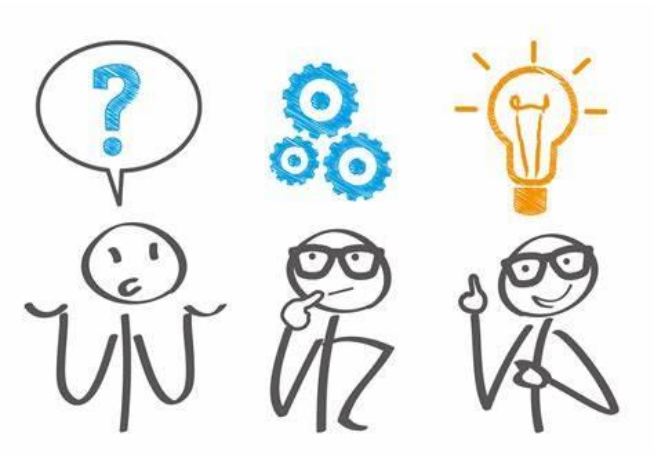
Veille

Communauté

Pilier : Renforcement cybersécurité

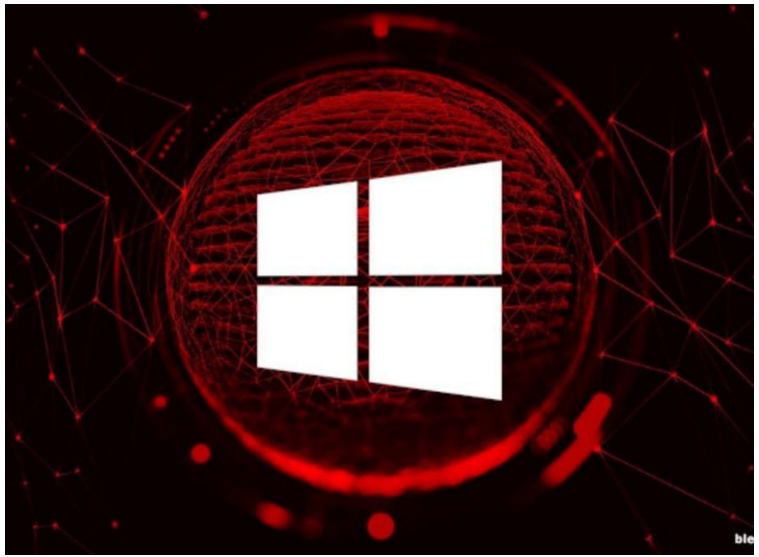
Standards minimaux

Conseils à la demande



Pilier : Veille

Notifications de vulnérabilités critiques



Bulletin cyber mensuel

Téléchargez l'application Cybersécurité Vaud

Périmètre du service CSIRT – édition 2024

Les axes de la Convention

CYBER **RÉACTION**

CYBER **RÉSILIENCE**

CYBER **PRÉVENTION**

Gestion de crise et réponse cyberincident

Renforcement cybersécurité

Formation

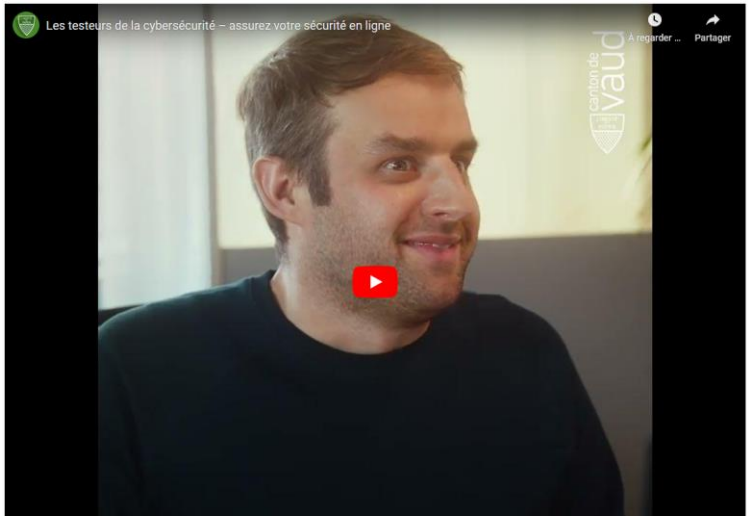
Veille

Communauté

Pilier : Formation

Formation en présentiel

Contenu de formation



Nouvelle formation pour les communes vaudoises

UCV centre de formation

CYBERSÉCURITÉ POUR LES COMMUNES VAUDOISES

21 novembre 2024

Jongny

8h30-16h30

DÉTAILS ET INSCRIPTIONS

ucv.ch/formations

SUJETS TRAITÉS

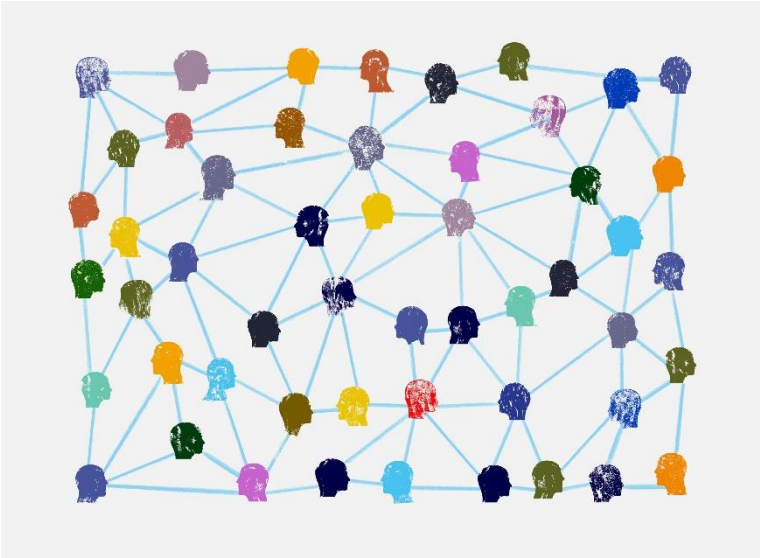
- La sécurité de l'information et le paysage des menaces
- L'environnement réglementaire
- Le système de gestion de la sécurité de l'information (SMSI)
- Les enjeux liés à l'externalisation de l'informatique communale
- La réponse à incident

OBJECTIFS DU COURS

- Comprendre les bases de la sécurité de l'information, identifier les différentes cybermenaces actuelles
- Apprendre les bonnes pratiques d'hygiène informatique
- Savoir évaluer les fournisseurs de services externes pour assurer la sécurité et la conformité
- Apprendre à préparer et répondre efficacement aux incidents

Pilier : Communauté

Réseau des répondants cyber et des partenaires privés



Evènement cybersécurité

Restons en contact

Par email : csirt@vd.ch

Contact Fiona Ponzo :
021 338 07 33 ou
079 547 97 38

En cas d'urgence : **117**