Urgence Cyber région Sud

Soutenu par RÉPUBLIQUE FRANÇAISE

RÉGION SUD PROVENCE ALPES CÔTE D'AZUR

LE LABEL

URGENCE CYBER RÉGION SUD

Un marqueur fort d'engagement pour renforcer la résilience cyber du territoire

Ensemble face à la menace

Dans un monde où les menaces numériques évoluent sans cesse, la sécurité des systèmes d'information est devenue un enjeu stratégique pour les entreprises, les institutions et l'ensemble des acteurs de notre territoire. Le CSIRT Urgence Cyber Région Sud s'inscrit pleinement dans cette dynamique en proposant une réponse collective, structurée et efficace face aux défis croissants de la cybersécurité.

La création du “label Urgence Cyber Région Sud" marque une étape essentielle dans cette ambition commune : renforcer notre écosystème local et promouvoir une approche solidaire et concertée de la sécurité numérique. Ce label n'est pas qu'une simple reconnaissance, c'est avant tout un engagement réciproque.

Pour les prestataires labellisés, c'est l'opportunité d'accéder à une visibilité accrue, de rejoindre un réseau d'acteurs engagés et d'être recommandés auprès de nos adhérents. Pour le CSIRT, c'est la garantie de pouvoir compter sur des partenaires fiables, compétents et impliqués dans la construction d'un territoire cyber résilient.

En adhérant à ce label, nos prestataires deviennent également membres de l'association, avec une voix à l'Assemblée Générale, contribuant ainsi directement aux choix stratégiques du CSIRT et aux grandes orientations en matière de cybersécurité.

SOMMAIRE

A PROPOS DU LABEL URGENCE CYBER RÉGION SUD

RÈGLEMENT ET CAHIER DES CHARGES TECHNIQUE

KIT COMMUNICATION

PLUS QUE JAMAIS,
ENSEMBLE FACE À LA MENACE

A PROPOS DU LABEL URGENCE CYBER RÉGION SUD LES FAQ

En quoi consiste le label Urgence Cyber région Sud ?

Le ***label Urgence Cyber Région Sud*** est une reconnaissance officielle attribuée à des entreprises spécialisées dans la cybersécurité qui s'engagent aux côtés du CSIRT pour renforcer la résilience numérique du territoire. Il atteste du sérieux, de la compétence technique et de l'engagement éthique de ces prestataires, tout en garantissant aux bénéficiaires du CSIRT – entreprises, collectivités, associations – une offre fiable, encadrée et adaptée à leurs besoins.

Contrairement aux partenaires conventionnés, dont la sélection repose avant tout sur une base auto-déclarative, les entreprises labellisées font l'objet d'une évaluation approfondie.

Cette exigence renforcée constitue un gage de fiabilité, de qualité et de transparence. Concrètement, ce label repose sur un processus rigoureux : dépôt de candidature, vérification des pièces administratives, analyse des compétences techniques en commission d'évaluation et engagement formalisé à travers une convention d'usage. Les entreprises labellisées doivent démontrer leur conformité réglementaire (RGPD, assurance, certifications), la solidité de leurs méthodologies, leur capacité d'intervention rapide en cas d'incident et leur volonté de contribuer à l'écosystème régional (actions de sensibilisation, participation aux événements, pratiques tarifaires responsables).

Attribué pour une durée d'un an, le label est renouvelable à condition de satisfaire aux exigences de suivi et de qualité prévues dans le cahier des charges. Il donne accès à de nombreuses contreparties : visibilité dans l'annuaire officiel, valorisation sur les canaux de communication du CSIRT et rôle dans la gouvernance du CSIRT régional en tant qu'adhérent. Il ne s'agit donc pas seulement d'un label technique, mais d'un engagement mutuel autour de valeurs partagées : coopération, transparence, sécurité, et solidarité territoriale.

Pourquoi avoir créer un label territorial, en marge des certifications reconnues (type ISO 27001, NIST...) ?

Loin de suppléer des certifications de type ISO, le "label Urgence Cyber Région Sud » apporte une réponse complémentaire, territorialisée. Il contribue directement à la consolidation de l'écosystème cyber de la région et à sa lisibilité par les différentes parties prenantes.

À l'heure où les écosystèmes locaux sont confrontés à des attaques qui peuvent paralyser des collectivités, des hôpitaux, des TPE ou des associations, il est vital de disposer de relais techniques, facilement identifiables, capables d'intervenir rapidement et efficacement. En labellisant des prestataires ancrés dans le territoire, le CSIRT garantit un niveau opérationnel élevé et cohérent. Cette démarche de labellisation vise à baliser et sécuriser les parcours, à harmoniser les pratiques, à mutualiser les ressources, mais aussi à élever durablement le niveau général de sécurité. En promouvant une logique d'engagement, de transparence et de prix raisonnés, le label favorise une approche équilibrée : la juste solution, au juste besoin.

Créer un label, c'etait pour Urgence Cyber région Sud, affirmer une vision partagée de la cybersécurité comme bien commun; en d'autres termes : engager les acteurs dans un pacte de responsabilité réciproque. Notre label ne se réduit pas à un simple signe distinctif. Il incarne un engagement concret au service de la confiance, de la solidarité et de la qualité dans la réponse aux menaces cyber qui touchent notre territoire.

Le label agit par ailleurs comme un levier de visibilité pour les entreprises qui en bénéficient. Être labellisé par une structure reconnue comme le CSIRT régional, c'est apparaître dans un annuaire officiel diffusé auprès de nombreux donneurs d'ordre, participer à des événements de sensibilisation, accéder à des espaces de publication ou des webinaires, mais aussi se voir reconnu un rôle dans la gouvernance de l'écosystème cyber régional.

Faut-il être labellisé pour que le CSIRT renvoie vers vous dans le cadre de réponses à incident ?

Non. Le CSIRT Urgence Cyber Région Sud adresse, en cas d'incident, une proposition de partenaires conventionnés, sans distinction de statut entre prestataires labellisés et non labellisés. **Le rôle du CSIRT n'est pas de prescrire ou de hiérarchiser les acteurs, mais de fournir aux bénéficiaires une base fiable de professionnels déclarés**, à partir de laquelle chacun reste libre de choisir le prestataire avec lequel il souhaite travailler.

La labellisation ne conditionne donc pas l'accès à la liste diffusée par le CSIRT. Elle constitue en revanche un niveau d'exigence supplémentaire, fondé sur une évaluation plus poussée, qui vient enrichir la relation de confiance avec les bénéficiaires. Il ne s'agit

pas d'un label promotionnel, mais d'un outil de clarification et de reconnaissance, qui permet aux structures accompagnées de savoir que certains prestataires ont accepté d'entrer dans une démarche plus encadrée, plus transparente, plus coopérative.

Ainsi, la labellisation n'est ni exclusive ni obligatoire. Elle s'adresse aux prestataires qui souhaitent formaliser leur engagement aux côtés du CSIRT, tout en apportant aux bénéficiaires un repère de qualité et de fiabilité dans un contexte souvent marqué par l'urgence et l'incertitude.

Quelles sont les étapes pour être labellisé ?

L'obtention du "label Urgence Cyber Région Sud » s'appuie sur un processus complémentaire à la convention de partenariat. Le point de départ est identique : l'entreprise intéressée remplit le formulaire de candidature utilisé également pour les partenaires conventionnés, en y joignant les pièces justificatives requises. Pour entrer dans le processus de labellisation, elle doit cocher la case « Je souhaite être labellisé ».

Dès réception du formulaire, un lien HelloAsso lui est transmis pour régler les frais d'instruction du dossier, qui couvrent l'analyse approfondie et l'organisation de l'entretien.

Une évaluation approfondie est ensuite conduite par l'équipe du CSIRT. Elle porte à la fois sur la complétude administrative, la qualité et la solidité des prestations proposées, la maturité des processus internes, la transparence des engagements (délais, tarifs), et l'implication dans les dynamiques régionales.

Cette instruction est suivie d'un entretien d'évaluation approfondi, au cours duquel sont discutés les cas d'usage concrets, les méthodes de travail, les moyens humains, et les garanties apportées aux bénéficiaires en cas d'intervention.

La décision finale revient au comité de sélection du CSIRT, qui statue sur l'ensemble du dossier. En cas de validation, l'entreprise signe le règlement du label, reçoit un kit de communication personnalisé et intègre l'annuaire officiel des prestataires labellisés.

Qui composent le comité de sélection ?

Le comité de sélection chargé d'attribuer le "label Urgence Cyber Région Sud » est composé de trois membres permanents de l'équipe du CSIRT. Il inclut notamment un analyste cybersécurité, garant de l'évaluation technique des candidatures, ainsi que deux membres impliqués dans le pilotage opérationnel et stratégique du dispositif.
Ce comité est indépendant dans ses délibérations. Il statue sur la base d'un dossier complet, d'un entretien d'évaluation et des critères définis dans le cahier des charges du label. L'objectif : garantir l'équité, la transparence et la cohérence des décisions rendues.

Combien y-a-t-il de commission par an ?

Deux commissions par an (Juillet et décembre)

Quel est le coût du label ?

350 euros TTC (Organisations >500k€ de Chiffres d'Affaires)
750 euros TTC (Organisations de 500k€ à 2M€ de Chiffres d'Affaires)
1500 euros TTC (Organisations >2M€ de Chiffres d'Affaires)

Quels sont les engagements de l'entreprise labellisée ?

Obtenir le "label Urgence Cyber Région Sud » implique pour l'entreprise candidate de souscrire à un ensemble d'engagements clairs, concrets et vérifiables. Il ne s'agit pas d'une simple reconnaissance formelle, mais d'un contrat de confiance réciproque entre le CSIRT et le prestataire, inscrit dans une logique de service public, de responsabilité territoriale et d'exigence professionnelle.

L'entreprise labellisée s'engage tout d'abord à **maintenir en permanence un haut niveau de conformité administrative et réglementaire**. Elle doit notamment justifier d'un statut juridique clair, d'une assurance responsabilité civile professionnelle adaptée, et d'une politique de protection des données conforme au RGPD.

Sur le plan technique, **elle doit démontrer une expertise avérée** en cybersécurité, appuyée par des certifications, des méthodologies reconnues (type ISO 27001, NIST…), des références clients concrètes, et une capacité à intervenir rapidement en cas d'incident. Un engagement formel sur les délais d'intervention (SLA) est exigé.

L'entreprise s'engage également à respecter les principes d'éthique et de déontologie définis par le CSIRT : confidentialité absolue des données manipulées, transparence dans les rapports et interventions, prévention des conflits d'intérêts, et loyauté dans la relation avec les bénéficiaires. Elle doit aussi adopter une politique tarifaire équitable, raisonnable et transparente, en cohérence avec la vocation non lucrative du CSIRT.

Au-delà des aspects techniques et éthiques, l'entreprise labellisée accepte de contribuer activement à l'écosystème régional. Elle s'engage à répondre aux sollicitations de suivi (audit annuel, retour d'expérience, questionnaires…) et à actualiser ses informations dès qu'un changement significatif affecte sa situation.

Enfin, l'entreprise accepte le principe de contrôle : elle autorise le CSIRT à procéder à des vérifications régulières du respect des critères du label, et reconnaît que tout manquement pourra entraîner une suspension, voire un retrait du label. Ce cadre d'exigence garantit que le label reste un marqueur de sérieux et non un simple outil promotionnel.

Quels sont les engagements du CSIRT Urgence Cyber région Sud ?

Dans le cadre du label « Urgence Cyber Région Sud », le CSIRT ne se limite pas à un rôle de certification. Il s'engage lui aussi activement dans la relation partenariale qu'il établit avec les entreprises labellisées, sur la base de principes de transparence, de réciprocité et de reconnaissance.

Le premier engagement du CSIRT est de garantir un processus de labellisation rigoureux, impartial et transparent. Il met à disposition des candidats un cahier des charges clair, un dossier de candidature complet, une grille d'évaluation cohérente, ainsi qu'une procédure de sélection encadrée par une commission dédiée. Ce cadre permet d'assurer l'équité du traitement, la lisibilité des critères et la crédibilité du label sur le long terme.

Le CSIRT s'engage également à accompagner les entreprises labellisées dans la durée. Il leur offre une visibilité renforcée à travers un annuaire officiel, une présence sur l'annuaire de son site web, ainsi qu'une valorisation régulière via ses réseaux sociaux, sa newsletter, ses événements et ses communications institutionnelles. Il fournit à chaque labellisé un kit de communication pour faciliter l'usage du label dans le respect de ses règles d'usage.

En tant qu'animateur de l'écosystème régional de cybersécurité, le CSIRT favorise les échanges entre prestataires, adhérents et institutions afin de créer une communauté de confiance et de monter collectivement en compétence.

Le CSIRT s'engage aussi à assurer un suivi régulier des labellisés. Il met en œuvre un dispositif d'audit ou d'évaluation annuelle, recueille les retours d'expérience des bénéficiaires ayant fait appel aux prestataires, et veille à la qualité continue des services rendus. En cas de manquement avéré, il applique les sanctions prévues dans le règlement d'usage (avertissement, suspension ou retrait du label), dans un esprit de rigueur et de protection de l'intérêt général.

Enfin, le CSIRT garantit une gestion responsable, neutre et non commerciale du label. Il ne joue aucun rôle d'intermédiaire économique ou de courtier d'affaires. Son objectif est de structurer un réseau de confiance, au service de la sécurité collective du territoire, dans le respect de l'équité entre les acteurs.

À travers ces engagements, le CSIRT affirme sa vocation de tiers de confiance public, de facilitateur d'écosystème et de garant d'un haut niveau d'exigence en matière de cybersécurité territoriale.

LE RÈGLEMENT DU LABEL

Article 1 - Objet
Le présent règlement a pour objet de définir les modalités d'attribution, de gestion, de renouvellement et de retrait du "label Urgence Cyber Région Sud », ainsi que les droits et devoirs respectifs des parties prenantes.

Article 2 - Définition du label
Le label constitue une reconnaissance officielle attribuée par le CSIRT Urgence Cyber Région Sud à des entreprises disposant d'une expertise en cybersécurité, engagées dans une démarche éthique, technique et territoriale, et répondant à un ensemble d'exigences définies dans un cahier des charges spécifique.

Article 3 - Durée et validité
Le label est attribué pour une durée d'un an à compter de la signature de ce règlement et de la charte d'usage du kit communication du label. Il peut être renouvelé sur demande expresse du prestataire et après réexamen de la conformité aux exigences du label.

Article 4 - Conditions d'éligibilité
Pour être éligible, l'entreprise candidate doit :

- être établie juridiquement en France,
- exercer une activité dans le champ de la cybersécurité,
- avoir souscrit une assurance responsabilité professionnelle,
- respecter les obligations liées au RGPD,
- remplir le questionnaire technique (voir annexe) et fournir les justificatifs nécessaires.
- s'être acquittée des frais de dossiers (300 euros) et du montant de l'adhésion (50 euros)

Article 5 - Procédure de labellisation
La procédure comprend :

1. La demande de labellisation via un formulaire dédié.
2. Paiement des frais d'instruction du dossier via le lien Helloasso envoyé par mail
3. L'instruction du dossier par l'équipe du CSIRT.
4. Un entretien d'évaluation.
5. La présentation du dossier en commission d'attribution.
6. La signature du règlement du label.

Le CSIRT s'engage à traiter toute demande de réception d'un dossier complet lors de ses commissions annuelles (Juillet et décembre)

Article 6 - Engagements du prestataire labellisé

L'entreprise labellisée s'engage à :

- maintenir à jour ses données administratives et techniques,
- respecter les critères du cahier des charges technique annexé,
- appliquer une politique tarifaire transparente et proportionnée,
- agir en conformité avec la charte éthique du CSIRT,
- se soumettre aux contrôles prévus par le CSIRT.

Article 7 - Engagements du CSIRT

Le CSIRT s'engage à :

- assurer un processus impartial, rigoureux et transparent,
- fournir au prestataire un kit de communication et une charte d'usage,
- valoriser les entreprises labellisées dans ses supports et événements,
- faciliter leur intégration dans les dynamiques collectives de l'écosystème cyber régional,
- maintenir la neutralité dans ses recommandations aux bénéficiaires.

Article 8 - Suivi, retrait et suspension du label

Le CSIRT se réserve le droit de :

- demander une actualisation annuelle du dossier,
- diligenter un contrôle,
- retirer temporairement ou définitivement le label en cas de manquement avéré aux obligations.

Toute décision de retrait est précédée d'une notification écrite et d'un délai raisonnable laissé à l'entreprise pour se mettre en conformité.

Article 9 - Communication et usage du label

L'usage du label est encadré par la charte d'usage remise au prestataire labellisé. Toute communication externe (site, plaquette, appels d'offres) mentionnant le label doit en respecter les conditions de forme et de fond. Le label ne saurait être utilisé pour induire en erreur les bénéficiaires ou usurper une qualité officielle de certification.

Article 10 - Révision du règlement

Le présent règlement peut faire l'objet de modifications à l'initiative du CSIRT. Toute révision substantielle est notifiée aux entreprises labellisées.

Article 11 - En cas de non validation du dossier

La somme de 50 euros correspondant à l'adhésion sera remboursée en cas de non-conformité de la candidature. Les frais de dossier ne seront pas restitués.

Article 12 - Annexe technique obligatoire

Le présent règlement est accompagné d'un cahier des charges technique précisant les prestations attendues, les capacités exigées, les référentiels mobilisables et les éléments à déclarer selon la typologie d'activité.
Voir Annexe 1 : Cahier des charges technique des prestations labellisées.

Fait à Toulon, le 2 juin 2025.

ANNEXE 1 | LE CAHIER DES CHARGES TECHNIQUES

1. Exigences générales

Les entreprises candidates au label doivent remplir les conditions suivantes :

- Être juridiquement établies en France, avec un numéro SIRET actif ;
- Déclarer leur forme juridique, leur effectif et leur rayon d'intervention ;
- Définir un ou plusieurs points de contact référents disponibles ;
- S'engager sur des délais d'intervention cohérents avec leurs moyens ;
- Fournir une description explicite des prestations proposées.

2. Prestations de réponse à incident (RIS)

L'entreprise s'engage, lorsqu'elle se positionne comme prestataire RIS, à pouvoir :

- Collecter, conserver et transmettre des preuves numériques exploitables ;
- Mener des analyses forensiques complètes (origine, propagation, impacts) ;
- Procéder à la remédiation, restauration ou éradication des menaces ;
- Préconiser et mettre en œuvre des mesures de sécurité post-incident ;
- Renseigner ses capacités spécifiques : réponse à rançongiciels, analyse de code malveillant, etc.

3. Prestations de conseil et d'expertise

Les entreprises peuvent proposer, sous réserve de compétence :

- Des prestations de gouvernance cyber : PCA/PRA, BIA, feuille de route SSI, etc. ;
- Un accompagnement à la certification (ISO 27001, HDS, PCI-DSS…) ;
- Une évaluation et une gestion des risques selon des référentiels reconnus (EBIOS, ISO 27005…) ;
- Des audits de conformité réglementaire (NIS2, DORA…).

4. Services externalisés

Les partenaires peuvent proposer les fonctions externalisées suivantes :

- DSI, RSSI, DPO, ou SOC externalisé ;
- Conformité RGPD ;
- Supervision active ou pilotage de projets cyber.

5. Protection et prévention

Sont valorisées les prestations suivantes, selon des modalités précises :

- Sécurité des réseaux : configuration pare-feux, VPN, segmentation, supervision ;
- Sécurité des systèmes : revue des accès, durcissement OS, audit M365… ;
- Tests d'intrusion encadrés (rédaction d'un rapport structuré) ;
- OSINT/CTI : dataleak monitoring, threat intel contextualisée et actualisée.

6. Solutions d'hébergement sécurisé

Les prestataires doivent préciser :

- Le type d'hébergement (cloud public, privé, hybride) ;
- Les garanties de sécurité mises en place (chiffrement, auditabilité, segmentation…) ;
- Les certifications associées (SecNumCloud, HDS…) ;
- La présence d'un PRA et des mécanismes de redondance.

7. Édition de solutions techniques

Les éditeurs peuvent proposer :

- Des solutions EDR/XDR, en vente seule ou avec services managés (MDR) ;
- Des solutions de sauvegarde (on premise ou cloud), avec documentation des procédures de restauration ;
- Des pare-feux avec infogérance ;
- Des solutions d'authentification et de gestion des accès.

8. Formation et sensibilisation

Les entreprises doivent décrire les contenus et formats de :

- Actions de sensibilisation auprès des utilisateurs finaux ;
- Formations techniques destinées aux équipes IT ou SSI.

9. Labels et certifications attendus

Les prestataires peuvent faire valoir tout ou partie des reconnaissances suivantes :

- PASSI, PACS, PRIS, PDIS ;
- Référencement Cybermalveillance.gouv.fr ;
- Label ExpertCyber ou équivalent ;
- Autres certifications reconnues.

LE KIT COMMUNICATION

Les éléments du kit

Une pastille “partenaire labellisé Urgence Cyber région Sud”

Un visuel prêt à l’emploi pour vos réseaux “entreprise labellisée”

Un certificat de labellisation

Urgence Cyber
région Sud

PARTENAIRE LABELLISÉ
Urgence Cyber
région Sud
2025

CERTIFICAT N°LAB25XXXX

LABEL | URGENCE CYBER REGION SUD

Attribué à :

[Nom de l'entreprise]
SIRET : [n° SIRET]
Adresse : [adresse de l'entreprise]

Date d'attribution : [Date complète]

Valable jusqu'au : [Date d'échéance – 1 an après]

Catégorie : [A compléter]

En reconnaissance de :

- son expertise avérée
- son engagement éthique et territorial,
- sa contribution active à la résilience numérique du territoire régional,

l'entreprise ci-dessus est officiellement **labellisée pour l'année 2025-2026 par le CSIRT Urgence Cyber Région Sud**.

Cette labellisation atteste de la conformité de l'entreprise aux critères établis par le règlement et le cahier des charges du label et valide son intégration au réseau de partenaires labellisés.

Fait à Toulon, le [date]
Pour le CSIRT Urgence Cyber région Sud

[Signature et tampon]
Le président du comité de labellisation
CSIRT Urgence Cyber Région Sud

Règlement d'usage du kit communication du label

Préambule

Le présent règlement a pour objet de définir les conditions d'utilisation des éléments visuels et des supports fournis dans le cadre du kit de communication remis aux entreprises labellisées par le CSIRT Urgence Cyber Région Sud. L'usage de ce kit vise à valoriser la reconnaissance obtenue par les prestataires, tout en assurant la cohérence, la lisibilité et la crédibilité du label auprès des bénéficiaires publics et privés.

Article 1 - Contenu du kit de communication

Le kit comprend notamment :

- Des pastilles visuelles millésimées (logo du label avec mention de l'année d'attribution) en plusieurs formats numériques (JPEG, PNG) et coloris,
- Des modèles de mentions types à insérer dans les documents (emails, présentations, plaquettes),
- Un visuel pour les réseaux sociaux,

Article 2 - Conditions d'usage autorisé

L'usage du kit est autorisé pendant la durée de validité du label, soit un an à compter de sa date d'attribution, sauf retrait anticipé. Il est réservé exclusivement à l'entreprise labellisée, pour ses supports internes et externes.

Le kit peut être utilisé notamment dans les documents suivants :

- Site internet institutionnel de l'entreprise,
- Présentations commerciales et techniques,
- Réponses à appels d'offres publics ou privés,
- Cartes de visite, signatures mail, plaquettes imprimées,
- Supports diffusés lors d'événements, salons, webinaires, publications professionnelles,
- Pages officielles de réseaux sociaux.

Article 3 - Mentions obligatoires

Toute utilisation de la pastille doit inclure l'année de labellisation visible et intacte. Il est formellement interdit :

- de modifier la pastille (couleurs, typographie, proportion, cadre),
- de retirer ou masquer la mention de l'année,
- d'utiliser une pastille correspondant à une année non obtenue,
- de présenter le label comme permanent, certifiant ou systématique.

En cas de perte, suspension ou non-renouvellement du label, l'entreprise s'engage à cesser immédiatement l'utilisation du kit et à retirer tout visuel des supports en ligne ou à jour.

Article 4 - Bonnes pratiques de communication

Le label peut être présenté comme une reconnaissance émanant d'un acteur public régional engagé dans la cybersécurité. Il peut être assorti, à titre explicatif, de la mention suivante :

« Label attribué pour l'année [année], par le CSIRT Urgence Cyber Région Sud, reconnaissant les entreprises engagées dans une démarche éthique, technique et territoriale en cybersécurité. »

Toute communication laissant entendre que le CSIRT garantit la qualité ou la performance des prestations, ou qu'il oriente ses bénéficiaires exclusivement vers les labellisés, est interdite.

Article 5 - Contrôle et sanctions

Le CSIRT se réserve le droit de procéder à des vérifications ponctuelles de l'usage du label. En cas de non-respect des présentes dispositions, il pourra :

- adresser une demande de mise en conformité sous 15 jours,
- suspendre temporairement l'usage du kit,
- retirer le droit d'usage du label,
- engager, en cas de présentation trompeuse ou mensongère, une action auprès des autorités compétentes.

Article 6 - Évolutions

Le contenu du kit et les règles de communication associées peuvent faire l'objet de modifications à l'initiative du CSIRT. Les entreprises labellisées seront informées de toute mise à jour, avec transmission des nouvelles versions officielles.

Fait à Toulon, le 2 juin 2025
CSIRT Urgence Cyber Région Sud

Contact :

responsable-ops@urgencecyber-regionsud.fr

04 23 36 09 32

Créé en 2021, dans le cadre du plan France Relance, le CSIRT Urgence Cyber région Sud est un dispositif associatif régional qui a pour but de prévenir, détecter et répondre aux incidents de cybersécurité.
Il s'adresse à tous types d'organisation :
entreprises de toutes tailles, collectivités territoriales et associations.
Urgence Cyber région Sud bénéficie depuis sa création du soutien de la région Sud et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Maison de l'Innovation et du Numérique
Place Georges Pompidou I 83000 TOULON
contact@urgencecyber-regionsud.fr
Tel : 0 805 036 083
www.urgencecyber-regionsud.fr