CYBER RÉUNION

TLP: CLEAR

CSIRT LA RÉUNION | COMPUTER SECURITY INCIDENT RESPONSE TEAM

Convention de référencement des Prestataires de réponse aux incidents de cybersécurité (PRICS-RR) avec le CSIRT LA REUNION

Statut : Validé | Classification : PUBLIC |Version : V1.0

ETABLIE

ENTRE

XXX, ayant son siège au XXX

Représenté par XXX

Ci-après dénommée Prestataire de réponse aux incidents de cybersécurité
D'UNE PART

ET

Le CSIRT LA REUNION porté par Réunion THD,

Régie publique à caractère industriel et commercial

Ayant son siège au 1 rue Emile Hugo 97490 Sainte-Clotilde

Représentée par Denis FABREGUE

Ci-après dénommée « Le CSIRT LA REUNION »,

D'AUTRE PART,

Ci-après dénommés collectivement « les Parties » et individuellement une Partie.

Table des matières

Introduction :

Le CSIRT LA REUNION est le centre de réponse aux incidents cyber ou CSIRT (Computer Security Incident Response Team) opéré par Réunion THD pour le compte de la Région Réunion. Ce centre accompagne notamment les entreprises (très petites et moyennes entreprises et entreprises de tailles intermédiaires), les collectivités locales et les associations du territoire réunionnais victimes d'incidents de sécurité.

Ce dispositif est soutenu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans le cadre de la convention de création du CSIRT LA REUNION qui lie le Secrétariat général de la défense et de la sécurité nationale (SGDSN) à la Région Réunion, cette dernière s'est notamment engagée à déployer un service de réponse à incident de premier niveau intégrant la proposition de mise en relation des victimes d'incidents de sécurité avec des Prestataires spécialisés.

Article 1 : Objet de la convention :

La présente convention a pour objet de formaliser les conditions de référencement des Prestataires de réponse aux incidents de cybersécurité – appelés **PRICS-RR** dans la suite de ce document – dans le cadre du service de mise en relation gratuit proposé par le CSIRT LA REUNION à destination des victimes d'un incident d'origine cyber et qui sont situées / dont les actifs sont situés dans le périmètre géographique de l'île de La Réunion.

Nota Bene : l'appellation PRICS-RR bien que syntaxiquement proche du sigle « PRIS »[1] de l'ANSSI est complétement indépendante de la qualification de Prestataires de Réponse aux Incident de Sécurité de l'ANSSI.

La notion de « Prestataire » désigne la personne morale dont l'activité est la prise en compte et la résolution des incidents de cybersécurité.

Article 2 : Conditions de référencement :

Pour être référencé par le CSIRT LA REUNION en tant que Prestataire de réponse aux incidents de cybersécurité sur le périmètre de la Région Réunion (PRICS-RR), deux conditions cumulatives doivent être remplies :

- Le Prestataire doit délivrer des services numériques et de cybersécurité dont l'une des finalités *a minima* doit être la réponse aux incidents de sécurité (qualification, collecte, analyse, endiguement, remédiation, actions post incidents) ou toute activité s'y rapportant ;
- Ces services doivent apparaître dans le catalogue de services du Prestataire et doivent être publiés sur le site internet public du Prestataire, facilement identifiables et accessibles.

Le référencement des Prestataires pour leur inscription dans le référentiel des Prestataires du CSIRT LA REUNION s'appuie sur les services délivrés, les certifications et les qualifications professionnelles, en termes de périmètres couverts, de formation et d'expérience professionnelle, des sociétés ou de leurs personnels. Une liste de références clients susceptible d'attester une expérience avérée en

[1] https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris

matière de prestations de réponses aux incidents et de gestion d'incidents serait la bienvenue. En cas de contraintes liées à la confidentialité, le candidat le signalera afin d'une prise en compte complémentaire et adaptée.

Les qualifications attendues plus particulièrement sont les suivantes : prestataire de réponse à incidents (PRIS) ou d'audit de sécurité des systèmes d'information (PASSI) portées par l'ANSSI, le label Expert Cyber et le référencement des professionnels portés par le GIP ACYMA[2].

Toutefois, ces qualifications, labels ou référencements ne sont pas indispensables pour le référencement, mais des éléments probants seront demandés aux soumissionnaires.

Un fichier tableur sera mis à disposition des candidats, contenant plusieurs champs d'information à compléter pour solliciter le référencement des prestataires.

A l'issue d'une analyse du fichier instruit par le CSIRT LA REUNION et sous réserve que les deux conditions cumulatives citées plus haut soient bien remplies le Prestataire sera officiellement référencé et il pourra faire publicité de son référencement.

Article 3 : Engagements du CSIRT LA REUNION

Le CSIRT LA REUNION s'engage à :

- Conseiller les victimes[3] sur les opérations à mener en fonction de la qualification initiale de l'incident en amont d'une éventuelle prise en charge par un Prestataire de réponse à incident de cybersécurité ;
- Ne pas interférer dans la contractualisation et/ou dans l'exécution d'une prestation entre le (ou les) Prestataire(s) et le Bénéficiaire ;
- Transmettre au Prestataire retenu par un Bénéficiaire les éléments factuels qui auraient pu être déjà collectés auprès du Bénéficiaire lors de la phase de qualification et de triage à la suite de sa sollicitation du CSIRT LA REUNION ;
- Participer aux réunions de suivi et de clôture de l'incident avec le Bénéficiaire final de la prestation de réponse à incident ;
- Apporter un soutien, dans la mesure du possible, en fonction des capacités propres du CSIRT LA REUNION et en coordination avec le Prestataire, en complément des prestations réalisées par le ou les Prestataire(s) ;
- Partager des indicateurs de compromissions (IOCs) anonymisés et des éléments descriptifs des tactiques, techniques et procédures (TTPs) avec la communauté des Prestataires du CSIRT LA REUNION ;
- Assurer la facilitation et la coordination avec les autres CSIRTs français (CERT-FR, autres CSIRTs régionaux, CSIRT sectoriels …) ainsi qu'avec les forces de l'ordre et/ou de justice si nécessaire, et jouer un rôle de facilitateur avec d'autres CSIRTs internationaux ;
- Mettre en avant sur son site internet public la liste des Prestataires référencés avec les niveaux de référencement, de certification et les domaines de compétences ;

2 https://cybermalveillance.gouv.fr/

3 Victime = Bénéficiaire

- Coopérer de manière transparente avec l'ensemble des acteurs de la réponse aux incidents du dispositif national et les communautés dans lesquels ils s'inscrivent ;
- Valoriser le partenariat avec l'ensemble des Prestataires dans ses actions de communication traitant de la cybersécurité à La Réunion et dans l'hexagone ;
- Organiser au minimum, une réunion annuelle avec l'ensemble des Prestataires référencés, au cours de laquelle seront présentées les statistiques liées aux missions de réponse aux incidents de premier niveau. Cette rencontre offrira également l'opportunité d'échanger sur le processus de référencement ainsi que sur les sujets connexes afin de renforcer la collaboration et d'améliorer la qualité des services fournis ;
- Transmettre au Bénéficiaire un questionnaire de satisfaction à l'issue de la prestation ;
- En cas de désaccord entre le Bénéficiaire et le Prestataire, et avec leurs accords respectifs, jouer un rôle de médiation.

Article 4 : Engagements du Prestataire

Le Prestataire s'engage à :

- Fournir toutes les informations nécessaires, visées à l'article 2 de de la présente convention, lors de la phase de référencement de ses prestations de réponse à incidents ou toute activité s'y rapportant auprès du CSIRT LA REUNION, et les mettre à jour au moins une fois par année calendaire ;
- Fournir la liste des services inclus dans ses prestation de réponse à incidents, et préciser ceux réalisés en Jours et Heures Ouvrées (JHO) et Jours et Heures Non Ouvrées (JHNO) ;
- Mettre en œuvre les moyens permettant de répondre aux mises en relations ou sollicitations du CSIRT LA REUNION pour la réalisation de prestations de réponse à incident auprès de Bénéficiaires du CSIRT LA REUNION et toutes les activités s'y rapportant ;
- Faire preuve de transparence auprès du Bénéficiaire sur les actions menées lors d'une prestation de réponse à incident ;
- Tracer et journaliser toutes les opérations réalisées au profit du Bénéficiaire par la tenue d'un journal de bord ou d'une main courante lors de la réalisation d'une prestation de réponse à incidents ;
- Respecter les bonnes pratiques et la réglementation qui s'applique à ses prestations de réponse à incident ainsi que la réglementation sur la protection des données personnelles (RGPD ou autre plus spécifique à un secteur d'activité par exemple) ;
- Respecter en toutes circonstances les protocoles TLP[4] pour le partage d'information et PAP[5] sur l'utilisation des informations ;
- Faire un retour d'expérience a minima documenté et anonymisé au CSIRT LA REUNION de la prestation délivrée au Bénéficiaire dans le cadre de son intervention dans les 30 jours après la fin de la prestation ;
- Partager avec le CSIRT LA REUNION les indicateurs de compromission et des éléments descriptifs des tactiques, techniques et procédures résultant des investigations numériques avec le CSIRT LA REUNION sous réserve de l'accord du Bénéficiaire ;

[4] Traffic Light Protocol : voir https://www.cert.ssi.gouv.fr/csirt/politique-partage/

[5] Permissible Actions Protocol : voir https://www.cert.ssi.gouv.fr/csirt/politique-partage/

- Fournir au CSIRT LA REUNION une synthèse annuelle afin d'alimenter le rapport annuel des incidents de cybersécurité et de l'état de la menace sur la base des opérations menées dans le cadre de la mise en relation par le CSIRT LA REUNION ;
- Fournir au CSIRT LA REUNION toute information et toute documentation de nature à apporter la preuve du respect des engagements cités dans l'article 4 de la présente Convention.

Le CSIRT LA REUNION se réserve la primeur de toute action de communication autour du partenariat, le Prestataire étant libre de toute communication ultérieure, mais devant demander l'accord du CSIRT LA REUNION en cas d'utilisation de son nom, logo, ou de ses références

Sous réserve de son référencement, le Prestataire pourra apposer un macaron distinctif fourni par le CSIRT LA REUNION sur ses supports de communication. Ce macaron attestera de son référencement et renforcera sa crédibilité auprès de ses clients et partenaires.

Article 5 : Respect des valeurs fondamentales du CSIRT LA REUNION

Tous les CSIRT régionaux partagent trois valeurs fondamentales, décrites ci-dessous. Le Prestataire s'engage également au respect scrupuleux de ces valeurs.

5.1. Confiance

La confiance est une composante essentielle dans les domaines de la cybersécurité et de la réponse aux incidents de sécurité. En effet, le CSIRT LA REUNION se doit d'établir et de maintenir une relation de confiance avec les Prestataires.

Dans l'exercice de ses missions, le Prestataire pourra être amené à accéder à des données sensibles, il s'engage sur le fondement de la relation de confiance à n'en divulguer aucune.

5.2. Engagement

L'engagement du CSIRT LA REUNION se traduit par deux notions qui se rejoignent.

D'une part, par le sens du service, essentiel pour accompagner des victimes d'incident dans le cadre du service d'intérêt général gratuit que le CSIRT LA REUNION propose aux Bénéficiaires.

D'autre part, par l'engagement de service et de réactivité que prend le CSIRT LA REUNION pour ne laisser aucune demande sans assistance.

Le Prestataire s'engage à intervenir dans le respect de la continuité de ses deux notions. Il s'engage par ailleurs à intervenir de manière prompt et sérieuse à toute sollicitation de Bénéficiaires.

Le Prestataire s'engage à signaler dans les plus brefs délais toute indisponibilité au Bénéficiaire afin de mettre ce dernier à mesure de consulter un autre Prestataire.

5.3. Coopération

Le Prestataire s'engage à coopérer de manière transparente avec le CSIRT LA REUNION et l'ensemble des acteurs de la réponse aux incidents afin d'instaurer un climat d'entraide et de partage permettant de renforcer la sécurité numérique aux échelles régionales et nationales.

Article 6 : Respect des principes éthiques

6.1. Respect de la règlementation

Le Prestataire est tenu de s'informer sur la législation applicable dans le cadre de son activité afin d'agir dans le respect de celle-ci.

6.2. Conflit d'intérêt

Le Prestataire s'engage à éviter toute situation de conflit d'intérêt dans le cadre de l'exécution de ses missions.

Un conflit d'intérêt se définit comme toute situation dans laquelle les intérêts personnels, financiers ou professionnels du Prestataire pouvant influencer, ou sembler influencer, de manière inappropriée son jugement ou ses actions dans l'exécution de ses obligations.

Le Prestataire s'engage à informer immédiatement le Bénéficiaire et le CSIRT LA REUNION de tout conflit d'intérêt potentiel ou avéré dont il a connaissance.

En amont de toute intervention auprès du Bénéficiaire qui l'aura choisi, le Prestataire s'engage à prendre toutes les mesures raisonnables pour résoudre la situation, y compris le cas échéant se retirer de la situation conflictuelle.

Tout manquement à cette obligation donnera droit au Bénéficiaire de se défaire des services du Prestataire.

6.3. Neutralité : traitement équitable des Bénéficiaires

Le Prestataire s'engage à un traitement équitable des Bénéficiaires.

Ce traitement équitable inclut sans s'y limiter les éléments suivants :

- Egal accès aux services : tous les Bénéficiaires faisant appel au Prestataire doivent avoir un accès égal aux services offerts par le Prestataire sans discrimination fondée sur des critères tels que la taille de l'entité, le secteur d'activité ou la localisation géographique.
- Evaluation des besoins : le Prestataire s'engage à évaluer de manière objective et équitable les besoins spécifiques des Bénéficiaires, afin d'adapter les services fournis en conséquence.
- Réglementation sur la protection des données : le Prestataire s'engage à respecter toutes les lois et réglementations applicables en matière de protection des données.
- Respect du droit de la concurrence : le Prestataire s'engage au respect des règles applicables en matière de concurrence. Il s'engage à éviter toute pratique anticoncurrentielle ainsi que toute situation équivoque pouvant notamment mener à une entente illicite, à la privation d'un concurrent d'une opportunité du fait de ses actions, à des pratiques commerciales déloyales ou à la diffusion de propos infondés et malveillants au sujet d'un concurrent.
- Prévention et lutte anticorruption : le Prestataire s'interdit toute pratique consistant à offrir, donner ou recevoir directement ou indirectement des avantages, incitations financières ou non financières autre que celles prévues dans le cadre de l'exécution de ses prestations.

- Signalement des violations : le Prestataire s'engage à signaler immédiatement au CSIRT LA REUNION toute suspicion ou connaissance d'activité pouvant constituer une violation des principes anti-corruption et anti-concurrence.

Article 7 : Conditions d'exécution des prestations

La présente Convention ne vise pas la réalisation du service par les Prestataires auprès des Bénéficiaires.

Les prestations relèvent de la relation contractuelle qui sera conclue entre les Prestataires et les Bénéficiaires.

Article 8 : Conditions financières

Le référencement du Prestataire, après vérification de sa qualification professionnelle, est gratuit. La mise en relation entre le Prestataire et le Bénéficiaire, ne donne lieu à aucune rémunération du CSIRT LA REUNION et ne constitue ni un marché public ni un contrat de sous-traitance, au sens des articles L.2193-1 et suivants du code de la commande publique.

Article 9 : Conditions de contractualisation

Dans le cadre de la mise en relation au profit d'un Bénéficiaire, le CSIRT LA REUNION se doit, par mesure d'équité, de proposer plusieurs Prestataires aux Bénéficiaires.

Le choix final du Prestataire est du seul ressort du Bénéficiaire et la contractualisation d'une prestation reste l'affaire du Prestataire et du Bénéficiaire.

Article 10 : Enquête de satisfaction auprès des Bénéficiaires

Le Prestataire est informé qu'il pourra faire l'objet d'une enquête de satisfaction dans le cadre de l'évaluation des services fournis.

Cette enquête vise à recueillir des retours d'expérience afin d'améliorer la qualité des prestations.

Le Prestataire s'engage à prendre en compte les résultats des enquêtes effectuées auprès des Bénéficiaires afin d'améliorer le service rendu.

Toutefois, le Prestataire est informé que si trois enquêtes lui sont défavorables, il pourra être sanctionné dans les conditions décrites à l'article 16 de la présente Convention.

Article 11 : Rémunération du Prestataire par le Bénéficiaire

Le Prestataire sera rémunéré par le Bénéficiaire pour les services effectués.

Article 12 : Durée de la Convention

La présente Convention entre en vigueur à la date de sa signature, pour une durée d'un an, reconductible au maximum deux fois par tacite reconduction.

Une nouvelle analyse et évaluation du Prestataire aura lieu tous les ans sur la base de la synthèse annuelle remise par le Prestataire afin de s'assurer de la conformité du Prestataire vis-à-vis du référentiel actualisé.

Article 13 : Résiliation et Déréférencement

Chaque Partie peut résilier la présente Convention, à tout moment, sous réserve du respect d'un préavis d'un mois transmis par courrier électronique signé avec accusé de réception. Les conditions du déréférencement d'un Prestataire sont précisées dans les articles 13, 14 et 15 de la présente Convention.

Article 14 : Mise à jour de la Convention

La présente Convention peut être revue et la version qui fait foi est celle publiée sur le site Internet du CSIRT LA REUNION. Toute modification de la présente Convention donne lieu à une communication aux Prestataires référencés, qui devront en retourner un exemplaire signé dans un délai de 15 jours. Le défaut de retour signé de la nouvelle convention dans le délai de 15 jours entraîne la fin de la convention et donc du référencement.

Article 15 : Engagement de responsabilité

La relation entre le CSIRT LA REUNION et le Prestataire ne relevant pas d'un contrat de service, Le CSIRT LA REUNION ne pourra être tenu responsable ou co-responsable de tout manquement du Prestataire à ses obligations légales ou contractuelles vis-à-vis du Bénéficiaire.

Le CSIRT LA REUNION ne peut pas s'engager sur le nombre de prestations qui seront confiées à un Prestataire.

Le CSIRT LA REUNION ne propose pas de défraiement pour les frais engagés par le Prestataire pour son référencement ou les actions nécessaires au maintien de son référencement.

Article 16 : Sanctions

Tout manquement aux engagements contenus dans la présente Convention ou au moins trois enquêtes de satisfaction défavorables réalisées par le CSIRT LA REUNION auprès de Bénéficiaires pourra conduire à un déréférencement d'un Prestataire par le CSIRT LA REUNION, sous réserve d'un préavis d'un mois notifié par lettre ou courrier électronique signé (e) et recommandé(e) avec accusé de réception.

Article 17 : Litiges

En cas de contestation ou de litige relevant de l'application ou de l'interprétation de la Convention, les Parties conviennent que le Tribunal compétent est le Tribunal administratif de La Réunion dont les coordonnées sont les suivantes :

27, rue Félix Guyon
CS 61107
97404 Saint-Denis Cedex
Téléphone : 02 62 92 43 60
Télécopie : 02 62 92 43 62
Courriel : greffe.ta-reunion@juradm.fr

Point de contact :

Le CSIRT LA REUNION est joignable :

- Par téléphone au 0 262 974 999
- Par courriel à l'adresse : csirt@cyber-reunion.fr
- Par messagerie signée avec la clé PGP dont l'empreinte est disponible à l'adresse : https://www.cyber-reunion.fr/cle-pgp

Signataires de la Convention

Pour le CSIRT LA REUNION	Pour le Prestataire
	Nom de société
Nom, prénom	Nom, prénom
Fonction	Fonction
Signature	Signature
Cachet du CSIRT LA REUNION / Réunion THD	Cachet de la société