CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

CENTRE DE RÉPONSE AUX INCIDENTS CYBER
Nouvelle-Aquitaine

RFC2350

Vie du document :

Historique des versions			
Version	**Date**	**Auteur·e**	**Nature**
V 1.0	25-04-2023	Philippe STEUER	Rédaction
V 1.1	04-03-2024	Philippe STEUER	Modification

Table des matières

1. Information

Ce document contient une description du Campus Régional de Cybersécurité et de confiance numérique de Nouvelle-Aquitaine et plus particulièrement du centre de réponse aux incidents cyber (CRiC) conformément aux spécifications RFC 2350. Il fournit des informations de base, décrit ses responsabilités et services offerts.

1.1. Version du document

La version de ce document est la 1.0 publiée le 25/04/2023.

1.2. Liste de distribution

Les modifications apportées à ce document sont notifiées par courriel à :

InterCERT-FR / réseau des CSIRT Français - http://www.cert.ssi.gouv.fr/csirt/intercert-fr

Veuillez envoyer des questions sur les mises à jour à l'adresse e-mail du CSIRT du Campus csirt@campuscyber-na.fr

1.3. Lieu de publication du document

La dernière version de ce document est disponible sur le site du campus : www.campuscyber-na/RFC2350

1.4. Authenticité du document

Ce document a été signé à l'aide de la clé PGP du Campus.

L'empreinte et son ID sont disponibles dans la section **2.8 et informations de chiffrement .** La clé publique PGP est disponible en **Annexe 1 : Clé publique**.

1.5. Identité du document

Titre : « RFC2350 C3-NA»

Version : 1.0

Date : 25/04/2023

SHA-256

Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure.

2. Introduction et dénomination

2.1 Le Campus Régional de Cybersécurité et de Confiance numérique

Le Campus Régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine est en charge d'assurer un support auprès des entreprises de la région Nouvelle-Aquitaine dans le domaine de la lutte informatique défensive (cyberdéfense) en liaison avec les organismes d'État en charge de ces sujets. Les missions du C3-NA sont :

- Assurer une veille à partir de l'écosystème sécurité informatique régional et national sur les menaces et les vulnérabilités.
- Sensibiliser les entreprises de la région de manière permanente en relayant par mail les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.
- Alerter par mail ses adhérents à partir d'un maillage des organismes en charge de cybersécurité et des remontées d'informations des entreprises de la région Nouvelle-Aquitaine sur des menaces et vulnérabilités.

Le Centre de Réponse à incident est une entité hébergé par le campus régional de cybersécurité et de confiance numérique.

2.2 Dénomination

Dans la suite du document :

- Le diminutif ***C3-NA*** désigne le Campus Régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine.
- Le diminutif ***CriC-NA*** désigne le Centre de Réponse à incident Cyber de la région Nouvelle-Aquitaine.
- Le mot ***bénéficiaire*** désigne les collectivités (mairies, communautés de communes…) , les organismes publics, les PME, les ETI, ou les associations nationales à ancrage régional qui bénéficient des services de réponse à incident du CriC-NA.
- Le mot ***bénéficiaire***++ désigne les bénéficiaires qui ont souscrit (gratuitement) aux offres complètes du CriC-NA.

3. Contacts

3.1. Nom de l'équipe

Nom officiel : Centre de Réponse aux Incidents Cyber.

Diminutif : CRiC.

3.2. Adresse

Campus Régional de Cybersécurité et de confiance numérique Nouvelle-Aquitaine

Service CRiC-NA

4 rue Adrienne Bolland

33600 PESSAC

3.3. Fuseau horaire

Heure normale d'Europe Centrale (HNEC) (Central European Time, UTC+1) et heure d'été d'Europe centrale (UTC+2).

3.4. Numéro de téléphone

(+33) 07 56 42 69 18

3.5. Numéro de FAX

Non disponible

3.6. Adresse de courrier électronique

L'adresse électronique du Campus est cric-na@campuscyber-na.fr

3.7. Autre canal de communication

Non disponible

3.8 Clé publique et informations de chiffrement

Le campus utilise une clé publique PGP :

- ID utilisateur : CSIRT-NA <csirt@campuscyber-na.fr>
- ID clé : 758A441B05B37CEA
- Empreinte : 805A 1E05 6E07 1E16 30E4 A3B9 758A 441B 05B3 7CEA

3.9. Membres de l'équipe

L'équipe est constituée d'analystes en cybersécurité.

Aucune information nominative relative aux membres du CRiC n'est diffusée dans ce document.

3.10. Horaires de fonctionnement

Les heures ouvrées concernant le CRiC sont du Lundi au Vendredi de 9h00 à 12h30 et de 13h30 à 17h00. En dehors de ces heures les bénéficiaires peuvent signaler leur incident sur le site du campus, répondre au questionnaire inclus dans le message vocal et/ou auprès de l'Agence Nationale de la sécurité des Systèmes d'Informations (ANSSI) dont les coordonnées figurent à l'adresse suivante : http://www.cert.ssi.gouv.fr/contact

3.11. Points de contact

Il est préférable de contacter le CRiC à l'adresse cric-na@campuscyber-na.fr.

En cas d'impossibilité d'envoyer un courrier électronique il est possible de contacter le CRiC par téléphone au 0805 29 29 40 aux horaires indiqués précédemment.

4. Charte

4.1. Missions

Le CRiC est un service gratuit d'intérêt public qui permet :

- d'accompagner les victimes d'un incident cyber avéré ou redouté, de les accompagner dans le dépôt de plainte et/ou la notification à la CNIL et de les orienter vers des prestataires en sécurité informatique référencés de la région.
- de porter conseil aux entreprises, collectivités et associations de Nouvelle-Aquitaine dans les domaines de la cyber.

4.2. Offre bénéficiaires++

L'offre ***bénéficiaires***++ est une offre proposée gratuitement par le C3-NA et qui permet aux souscrivants de :

- Disposer d'un scan de surface léger.
- Accélérer la réponse à incident.
- Demander un diagnostique de maturité cyber et disposer de conseil personnalisé.
- Effectuer une évaluation de la sécurité du site internet...

4.3. Circonscription

La circonscription est composée des collectivités, des associations nationales ainsi que de l'ensemble PME et ETI dont le siège social ou un établissement est basé dans un des départements de la région Nouvelle-Aquitaine. Il est conseillé d'adhérer préalablement aux services du CRiC pour bénéficier de l'entièreté des services offerts par le CRiC. Un formulaire de contact est disponible sur le site du campus pour en faire la demande. Les actions suivantes sont nécessaires à l'adhésion :

- La nomination d'un correspondant Cyber au sein de l'entreprise/association bénéficiaire.
- La réponse à un questionnaire d'identification des composants du Système d'Information de l'entreprise/association bénéficiaire.

Le CRiC pourra ainsi optimiser les services d'alerte et de réponse à l'incident pour l'ensemble des entreprises qui auront préalablement adhéré au Campus.

4.4. Parrainage

Le CRiC est un CSIRT public. Il maintient des relations avec les différents CERT et CSIRT en France et en Europe.

4.5. Autorité

Le C3-NA est placé sous l'autorité de l'association loi 1901.

5. Politiques

5.1. Types d'incidents et niveau de support

Le CRiC-NA est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses bénéficiaires. En fonction de la nature de l'incident, le Campus propose une liste de prestataires en Cybersécurité, susceptibles d'aider l'entreprise dans la résolution de l'incident. Un suivi de la résolution de l'incident est assuré dans le but d'établir des statistiques et de capitalisation, et pour améliorer nos capacités de diagnostic.

Le niveau de support offert par le Campus peut varier en fonction du type d'incident, de sa criticité et des ressources disponibles pour le prendre en charge.

5.2. Coopération, échanges et confidentialité de l'information

Le Campus échangera toutes les informations nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître. Le partage d'informations se fera dans le respect des différentes réglementations de protection existantes et respectera le CSIRT Code of Practice http://www.trusted-introducer.org/TI-CCoP.pdf

Les renseignements généraux relatifs aux incidents, tels que les noms et les détails techniques ne sont pas publiés sans l'accord des parties désignées. S'il n'est pas convenu autrement, les renseignements fournis restent confidentiels. Le Campus ne transmets jamais d'informations à des tiers à moins que la loi ne l'exige.

Par conséquent, ces informations peuvent être transmises partiellement à des entités telles que :

- Les groupes concernés dans notre circonscription.
- Nos partenaires.
- Les groupes de coopération CERT/CSIRT.

Toutes les informations sont transmises en fonction de leur classifications et du principe du besoin de savoir. Seuls les extraits spécifiquement pertinents et anonymisés sont transmis. Le Campus traite l'information dans des environnements physiques et techniques sécurisés conformément aux réglementations existantes en manière de protection de l'information.

5.3. Communication

Notre méthode de communication principale est le courrier électronique. Lors de l'échange d'informations sensibles, le chiffrage du mail via PGP est requis.

6. Services

6.1. Réponse à l'incident

Le Campus propose les services suivants dans le cadre de la réponse à l'incident de sécurité informatique :

- Réception des signalements d'incident.
- Diagnostic de l'incident.
- Accompagnement dans le dépôt de plainte et la notification à la CNIL
- Mise en relation vers des prestataires spécialisés.
- Compte rendu d'intervention concernant le traitement de l'incident.
- Capitalisation de la connaissance.
- Suivi et clôture de l'incident.

6.2. Alertes et Cyberthreat Intelligence

Afin d'adapter ses capacités de diagnostic et d'anticipation de la menace, le Campus réalise une veille active sur :

- La collecte de connaissances sur les acteurs de la cybermenace.
- Les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires.

Le C3-NA assure aussi une sensibilisation et une communication de ces informations, par courriel et publication sur son site Web, sous une forme appropriée à la compréhension des entreprises.

7. Formulaire de déclaration d'incident

Nous vous remercions de signaler l'incident via notre site Web à l'adresse campuscyber-na.fr ou en nous contactant par téléphone aux horaires d'activité.

Les bénéficiaires des services du Campus pourront fournir un certain nombre d'informations selon leur niveau de compréhension de celles-ci. Ils seront par la suite recontactés par le Campus.

8. Avertissements

Bien que les informations transmises dans le document aient été vérifiées, le C3-NA refuse toute responsabilité en cas d'erreur ou d'omission ou pour tout préjudice résultant d'information contenues dans ce document.

Si vous constatez une erreur dans ce document merci de nous le signaler par mail. Nous tâcherons de rectifier les informations au plus vite.

Annexe 1 : Clé publique

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGOYRtoBDADMCTfZJKv7pfxkAHvHbYq2j/ShHLFXMJCbX4G2uRh5ekzUUZEs
bmihDMjcsYlJULy/Tf3irf1uhkTUIzUbHAscbn+Loso5eJuAeyaAd3hZBpMvq6Yf
xtjYnqigC+3jPIltq5k1ib+pp3VID//cZ3kOArgF3u+rGqpwVZzNbRsnpsKQHKoe
opYRsrlXL7z6KN37SVKzLBj1Agyu2wzJDI61Xw3EsxHvfsdlMDDb5aG0CJ6gWMrq
hWMbZYvXhGcwRT3AfWCJfeWQdacFp1Sv8pUEf7A9p1frG7TE87fDTh4UeZ1FhdIk
PHXIHaZUJiR4bhkTS6Zpt3cc2LArFc5Hc6SZEPk/RLdIaZlZ7twRM84sex7XpOSh
ZEpj5LfTx8bY46cKboM4uk9KufZvbdSkCFMxtP0iNJ2NLw3PygcLrzCLaML7I6a+
7kIC9FXLlxQMLUyPzo4+QaeVxGBjLpKRtqjBhviJhCCvL/SG4bnNgNP3BPYCbEpH
hTDE1+ZDNZv0nSEAEQEAAbQiQ1NJUlQtTkEgPGNzaXJ0QGNhbXB1c2N5YmVyLW5h
LmZyPokB1AQTAQoAPhYhBIBaHgVuBx4WMOSjuXWKRBsFs3zqBQJjmEbaAhsDBQkB
+lRWBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEHWKRBsFs3zqIDEL/AxXnG0O
gyIz+TUrpEj1s+xeRduCKFkmrDRgRL8Cd8q0Sw8tPKJMs/P0HxmCm73XKQQT5wZK
X6cRLuggyiprU+wCdhARL96qySSBRYj+njFJfcZ5TmwrkBLDMjIWewBbxpa8pw3O
PgfnSQnrnfPdmSxcSVh7m6KmNeUubiFD2ZrhtZZGD2kTE5RBZmz2mTvIcEuoIv3b
VFmYE3X9CG10l2mQD1Nc4G22hVfGTXheQ3DiKFlvcBWthI8JX9mGxWYySU4CrLOt
3foIsKBDI9b1KIqbyWxqX2WJlGjd8aAjBb7L5RN3qrKfPhAL74WFL+EP3ia/a1He
64flqSuti6b4Yu9Mttz2Aqi0PqlCRT7OflMdAELg5lzddekeFG/pjoF6156NMhyi
SJYXYpxPHE3++Sn1qAWu2zhQOQSYPvq/ypyz/xlHdtAPX6QnkjV1KyIb8BHdPiRE
sj6uSBfMU5h9xrpC1Dy0rOJUnyjAiiON6QiRA6y+t2pH3J9hvBjcZovsnLkBjQRj
mEbaAQwA13KD4nu0vMPQSb4Ii4fljv3KThQnhQxfAOz5RMQQvM777vlwCPgCRjTj
eurj/59HcjUvDgk0KWar0pbrDfVwp/3ORRuwJ/JLcN3x7DFTaRbvVdWSJsp88Vs0
2aryxKRiuA6gDF3pYpMeuflSHupxiNjrLfVrIN0jxuT0BR8vCE985h6JUTyuNCSX
DsoQZZP0hJf/6auwGLYJeJF37oipGpsqbzU+wy+xlvJapWmIuRI5HYMEiSmGl6H5
g3Wt9ywkV0Vub1WwtgR9vF2sR3osSPNRQIZ6QXF948iDmSVWIUsgnOFNnRgs3zv7
gtD6G/0qE+88Z4PsKwoti0onkm0Ezx2MntvVtzFFPhQ2J3RLJVtZWEgwqYkDGR0w
DGiCWP7sAX952NQyh+3dexy9vxa3BMSECyuBmRFJuS/22KG/Bfbps7z2oU6lyZpZ
xqSEkAZsiBJOpLFOLPPWZntKSIFuhsPpr1puHaLuHFWmPfLEVGClyutZ4igc2QQC
ezjUkQa/ABEBAAGJAbwEGAEKACYWIQSAWh4FbgceFjDko7l1ikQbBbN86gUCY5hG
2gIbDAUJAfpUVgAKCRB1ikQbBbN86jf2DAC1v+Sw8nPEcttv3vQbmcL6txeKMPXP
bdaVoumGgPlpqfxYOrTzWLXK107HOjsOkgS9Jfg3AUnKFfTVYEasg2otBax6gE8v
pAfD+FA/Xa7ZSLkJRZWs3kgj4o1kVcgDPkvt4mSZqbMzqEiFN4ibiRoiHI4psUqv
wUG0ud6/4RyX/z2bDyZutBnIStdPwJsXxP+Hk0CxSvKXxAIpBUOB0A+ahFSoaEJv
THzJOsrwkjsmoJ2hkOZRqBJEHS6wRRp8w4OcUazp6n8PqdOWAFnjluA99qEezOBW
C+8HEd2MfGBMHK7uAcVc/nZJhBgoccg5GSZB3DSrRHc6q6smc3V1zNTYEbkLeDER
ssTvzBvuJAO2p9DTRkOt97mP1fRjcEhSfd1JFvnZXZzWOmmVjzJDlKcm9PPTtiO/
3fWCrvCTFUz4z5DPOtZ1VXNaLO1XAgTSdQROH5ay34Whkllk7OYpWIz0DEnbleGl
cK+f4NvRfP6BW5LT3kfrWHSQiVw6Fpg83cY=
=hYcH
-----END PGP PUBLIC KEY BLOCK-----