| | NOM(S) | FONCTION(S) | DATE |
|---|---|---|---|
| REDACTION | Jean-Luc BELET | Responsable des opérations CSIRT | 14/12/2022 |
| VERIFICATION | Jean-Charles RENAUDIN | Responsable Cyber Sécurité & CSIRT | 15/05/2023 |
| VALIDATION | Jean-Charles RENAUDIN | Responsable Cyber Sécurité & CSIRT | 29/08/2023 |
| | | | |

HISTORIQUE :

| Date | Version | Description | Rédacteurs |
|---|---|---|---|
| 14/12/2022 | 1.0 | Création du document | Jean-Luc BELET |
| 15/05/2023 | 1.1 | Mise à jour du document | Jean-Luc BELET |
| 18/07/2023 | 1.2 | Mise à jour du document | Jean-Luc BELET |

## SOMMAIRE

# 1 A propos du document.

Grand Est Cybersécurité est le CSIRT[1] de la région Grand-Est. Grand E-Nov+ est l'opérateur du centre d'assistance régional de réponse aux attaques informatiques, mandaté par la Région Grand-Est.

Ce document contient une description de Grand Est Cybersécurité tel que recommandé par la RFC2350. Il présente des informations sur l'équipe, les services proposés et les moyens pour contacter Grand Est Cybersécurité.

## 1.1 Où trouver ce document.

Ce document est accessible sur le site internet de Grand Est Cybersécurité via l'adresse https://www.cybersecurite.grandest.fr

## 1.2 Authenticité du document.

Ce document a été signé à l'aide de la clé PGP de Grand Est Cybersécurité.

La clé PGP publique, son identifiant et son empreinte sont indiqués dans le paragraphe 2.8 et sont aussi disponibles sur le site internet via l'adresse https://www.cybersecurite.grandest.fr.

# 2 Information de contact.

## 2.1 Nom de l'équipe.

Nom court : Grand Est Cyber
Nom complet : Grand Est Cybersécurité

## 2.2 Adresse.

GrandEnov+ / Grand Est Cybersécurité
10, Viaduc J.F Kennedy
54000 Nancy

## 2.3 Zone horaire.

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

## 2.4 Numéro de téléphone.

0970 51 25 25

## 2.5 Numéro de fax.

Aucun à ce jour.

[1] Computer Security Incident Response Team

## 2.6 Autres moyens de communications.

Aucun à ce jour.

## 2.7 Adresse Courriel.

contact@grandest-cyber.fr

## 2.8 Clé publique et informations liées au chiffrement.

PGP[2] est utilisé pour garantir la confidentialité et l'intégrité des échanges avec Grand Est Cybersécurité.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: ID utilisateur: Contact contact@grandest-cyber.fr
Comment: Empreinte: B2F8223074EAB12A693776414DD713C4EFF7B6FD

mQMuBGPP2mwRCAChm585ZqXKLl+QUBT2/EIBqakgSS1eongOW4jCo++RR5g2y+wr
0QyvoFigX4GGPL6NdzIR7HdMxrB3rOhkbZIYAEgX5SY0tRkSBQAbxTnQAPk7A7kx
sSRReiTAKYj9NaYT3ohIpBniCwYz9uC8rHpTJjsrdBfmatervPSc9XPIcwoIkANl
YVcOD/b8/3XLmGJIPGWHIC1MRaW1AZ6qJi+9cBgBFYiFXtnV8zZzezDG9gSQGT65
MWUaupebQdh0oMcx9Lc3fZQgZRiXdjn8ddNtRyMudQ75RWghUv6VTOWTS5YlN00B
A5vhTeuZt0nbK+KDJm1hfxtwiKBW76Lf+DGrAQD8TYOBsLrqUMOIZbht4NVmrosA
Bnn6qKNo4iMQZZxCKwf8DmUahrd1/LiMzFC3PWgPoVbg6B3H/Uv7B5XeGH2vcDtE
CX/qqx7xwm1fDNFZKdAuyzZhCvNldbfX1fvq4rYpCbPOovL+xV52kWW47p+rXUOG
COAAxWYoQiTKVG97mfCE/U6lLUAxFRhTht2hFnf3fT9Mog9/MbA+kZMFWLAZ3yx2
Y2jCf1oax9ksQyrCpenBoMunkYCIyLTxWn5P1P6zaV20sIjF3k9lbgYP6e6sZyqf
T/hs65OVFFDy8g3t3FzQRsv/Y8fh1ST42fKEJOfl+TFgtdTBQHolQVHO7DjHWA9U
EuHKGTAL5tw6tqY1Ow/ibsOKLZwxRPIazl4EYlni4Qf/e9a2eUtXxDOa3tVrywYp
x6y9d+BWH2WAFKxeqPzzgAMOuHnOF4b0nVgH3s5anxuIuSItFQ3htiMVpC6CfLz4
vxQnEI2AOScF60NwUal8s7uwN6XvQwO0c+TMs4aOjPwoYkJ8PruoeQUsfqAZk+XQ
8OFsusrojg0ZqsoqNw5HL4t01SLDJbnlSM9LssdnJhfaTH9a+UTm7iEUaWXX/ey4
edQITdXgweR3VQtYAeW/SLL0GI3BtreseFmtzrmD9CvFVryxnoSD8lQE2dcr93GW
+WSIgOc+t36xXyy3v4NupcnQAKX6VMSOdMbYETkefwLKY3THBSTQHBUTA4HsvzDo
MLQjQ29udGFjdCA8Y29udGFjdEBncmFuZGVzdC1jeWJlci5mcj6ImQQTEQgAQRYh
BLL4IjB06rEqaTd2QU3XE8Tv97b9BQJjz9psAhsDBQkA7nE0BQsJCAcCAiICBhUK
CQgLAgQWAgMBAh4HAheAAAoJEE3XE8Tv97b9D/YBAMTznineYe92R32Rt4iq5g5C
L3HXO4B5igAmoNj6MX/1AQDfOJuQHCqVx34GYD2wpnm5KR05+dVFqEvfZarM18dk
brkCDQRjz9psEAgAncHfTejeEWH3RkwKr6vVSZc1YVrSVOqvb8dT4/v4ChVWTEA/
9XLS5/Sir7h1/TR2VDDOThA938W7H2B1lydyt6P5F3PzBc1i1J0wEsRaJmypm3ku
tqaJ0oYnQslCP0jABpM4tlJ0rJxMxO20jCEk26yAc4H2XvypLsLhZgaTSPEKB53m
cG8FExEzq1yAET7hsudlQUx82eEWgkba0XMOJSBdG8FmZgj89mIKlg21xcHy9W+N
sx30wWGeZM3iSOkizVj6d3IwAO16/tKcgFQAtT3ad7RHDdDoz8sguQ7sTOQ9srkF
X+FniWu7ilv046Xs8f7s/zoT//WqbXIRgTI+YwADBgf+IfJ07ACEviYqtiuBb2BP
NwXQADdrLBN91Dsn34yS4kJro6U00CtNmNloeOrjbF8v8ggd85ddPXtA1eF9jL9i
x0JeLA5vO6iQHdfe5Ux8TbeIGi0HyoWClo32dvl/xu/vHkOsuvAdgUKdjvyTbCY1
EnmHJJpF5GfAABtKinHhP2MXueG8AbFODjngYatEeL+OFeYB6f3Dhp8jIC6rXcN9
EY6jMKzyekl+z3Xqar1cXbXctJ+Q+rP2OUEVGhxvEjXBN20Ud+zEGiR1JxPboW1n
3TVZcy+97VTxbxfumcoCW2+vSUpRdyYIJC9fzF7rx8Q/LVHJTXJFKpV+saNvVtEe
2Yh+BBgRCAAmFiEEsvgiMHTqsSppN3ZBTdcTxO/3tv0FAmPP2mwCGwwFCQDucTQA
CgkQTdcTxO/3tv1eaAEAnExeGBi8ALX8tP/3RH9G9gC92Wy2EWZQscp2j3caE0cB
AK1iTKdjBpKbVwmuaSz5r8orh4gjhDOWTkR7nPoEVBwK
=LNDP
-----END PGP PUBLIC KEY BLOCK-----

La clé PGP publique est aussi disponible via l'adresse https://www.cybersecurite.grandest.fr.

[2] Pretty Good Privacy

Pour plus de simplicité, vous pouvez aussi nous envoyer les éléments via notre page de dépôt sécurisée BlueFiles en cliquant ICI ou via le QR Code

## 2.9 Membre de l'équipe.

L'équipe est constituée de plusieurs membres :

- Un responsable.
- Un responsable des opérations.
- Plusieurs analystes.

## 2.10 Contact.

Grand Est Cybersécurité est disponible durant les heures ouvrées, soit de 9h00 à 12h30 et de 14h00 à 17h30, du lundi au vendredi (hors jours fériés).

Pour joindre Grand Est Cybersécurité, le moyen de communication privilégié est le téléphone via le numéro 0970 512 525 ou par courriel à l'adresse contact@grandest-cyber.fr.

Nous encourageons le chiffrement des communications en utilisant les références présentées dans le paragraphe 2.8 Clé publique et informations liées au chiffrement de façon à assurer l'intégrité et la confidentialité des échanges.

# 3 Charte.

## 3.1 Ordre de mission.

Grand Est Cybersécurité est le centre de réponse aux incidents de sécurité informatique de la région Grand-Est. Son objectif est d'apporter une assistance aux organisations de son territoire (Décrites dans le paragraphe 3.2 Bénéficiaires) pour répondre aux incidents cyber auxquels elles font face.

## 3.2 Bénéficiaires.

Les entités pouvant bénéficier de l'accompagnement de Grand Est Cybersécurité sont les organisations localisées sur le territoire de la région Grand-Est, comprenant notamment :

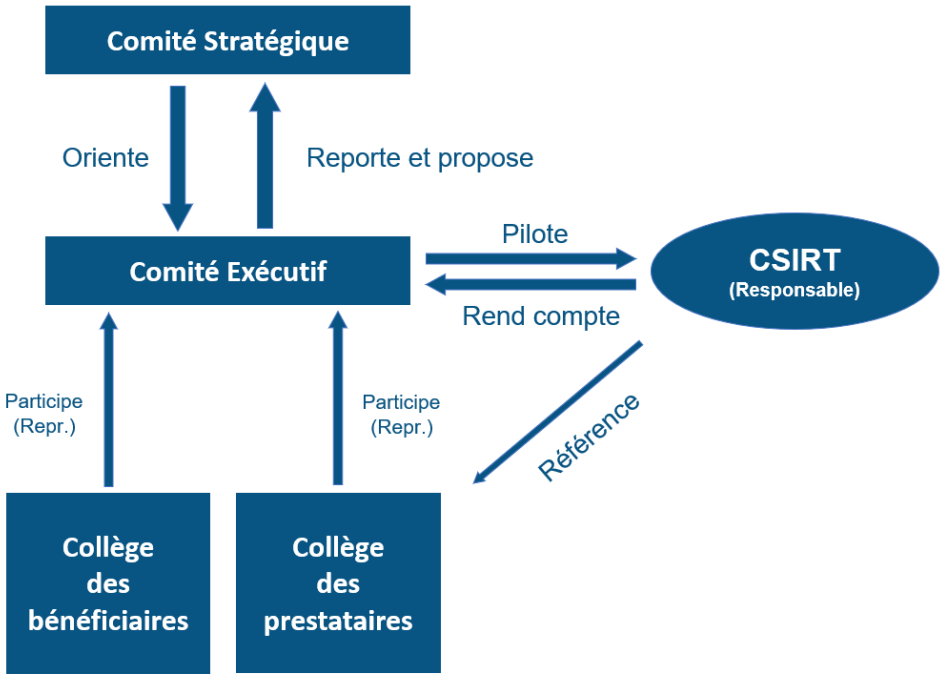
- Les PME.
- Les ETI.
- Les collectivités territoriales et les établissements publiques associés.
- Les associations.

## 3.3 Affiliation.

Grand E-Nov+ est l'opérateur du centre d'assistance régional de réponse aux attaques informatiques, mandaté par la Région Grand-Est.

### 3.4 Autorité.

Une gouvernance de Grand Est Cybersécurité est en place :




# 4 Politique.

## 4.1 Types d'incidents et niveau d'intervention.

Le périmètre d'action de Grand Est Cybersécurité couvre tous les incidents de sécurité informatique touchant les organisations bénéficiaires de son territoire décrites dans le paragraphe 3.2 Bénéficiaires.

Les missions principales de Grand Est Cybersécurité sont :

- ✓ La réception des déclarations d'incident et la coordination des demandes d'aide des bénéficiaires à la suite d'un incident informatique.
- ✓ La prise en compte du 1er niveau de l'incident avec un pré-diagnostic et une évaluation de l'incident.
- ✓ La mise en relation avec un prestataire qualifié et référencé de réponse à un cyber-incident. Cette mise en relation fera obligatoirement l'objet d'une contractualisation, avec émission d'un devis, entre le prestataire qualifié et le bénéficiaire. Le bénéficiaire retient le prestataire de son choix.
- ✓ Le suivi du traitement de l'incident jusqu'à sa clôture.
- ✓ La mise en relation avec les services de police et de gendarmerie pour le dépôt de plainte.
- ✓ La consolidation des statistiques d'incidentologie à l'échelle régionale et nationale.

## 4.2 Coopération, interaction et partage d'information.

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée. Grand Est Cybersécurité peut être amené à communiquer des informations aux autres CSIRT transfrontaliers, régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées à un CSIRT sectoriel (santé, maritime, …) à des fins de capitalisation des incidents propres au secteur concerné. La diffusion d'information sera traitée en accord avec le protocole TLP[3] défini par FIRST[4] (https://www.first.org/tlp).

## 4.3 Communication et authentification.

Grand Est Cybersécurité conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.
Les informations non confidentielles ou peu sensibles peuvent être transmises via des courriels non chiffrés.

# 5 Services proposés.

## 5.1 Réponse aux incidents.

L'activité principale de Grand Est Cybersécurité est de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents. En particulier, il propose les services détaillés dans les paragraphes suivants.

### 5.1.1 Triage.

- Récupération du signalement et prise de contact avec le déclarant.
- Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident.
- Détermination de la sévérité de l'incident (son impact) et de son périmètre (nombre de machines affectés).
- Catégorisation de l'incident.

### 5.1.2 Coordination.

- Identification des meilleurs partenaires au sein du dispositif national de réponse aux incidents pour accompagner le demandeur.
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident. Notamment, mais de manière non exhaustive :
    - A l'ANSSI[5] en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs.
    - A la CNIL[6] en cas de violation de données à caractère personnel.

[3] Traffic Light Protocol
[4] Forum of Incident Response and Security Teams
[5] Agence Nationale de Sécurité des Systèmes d'Information
[6] Commission Nationale de l'Informatique et des Libertés

### 5.1.3 Résolution.

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident.
- Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident.
- Suivi des phases de résolution et de remédiation de l'incident en relation avec le bénéficiaire et le prestataire choisi.
- Compte rendu d'intervention concernant le traitement de l'incident et capitalisation de la connaissance des cybermenaces.

## 5.2 Activités proactives.

Grand Est Cybersécurité délivrera à terme des services proactifs à ses bénéficiaires, tel que :

- Des services de veille.
- Des analyses de menaces.
- Un bulletin de veille à destination d'abonnés.

# 6 Formulaires de notification d'incident.

Un formulaire de notification est disponible en ligne via l'adresse https://www.cybersecurite.grandest.fr.

En cas de déclaration par téléphone ou courriel, les éléments suivants sont à fournir pour faciliter la prise en compte :

- Informations sur l'organisation touchée (Nom, contact de la direction et des équipes techniques, taille, …).
- Informations de contact du demandeur comprenant notamment : nom, fonction et numéro de téléphone.
- Chronologie de l'incident : date et heure du début de l'incident et de sa détection.
- Description de l'incident comprenant notamment l'impact sur l'organisation et le nombre et type de machines touchées.
- Actions effectuées depuis la détection de l'incident.
- Toute autre résultat d'investigations déjà menées.
- Architecture du système d'informations.
- Outils et politiques de défense contre les incidents en place.
- Si le demandeur est déjà en contact avec un prestataire de réponse aux incidents de sécurité informatique.
- Services attendus de la part d'une équipe de réponse aux incidents.

La politique de confidentialité et les traitements de données sont disponibles en ligne via l'adresse https://www.cybersecurite.grandest.fr.

# 7 Décharge de responsabilité.

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, Grand Est Cybersécurité n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation, par le prestataire, des informations contenues.