

Rapport d'Activité **2019**



RAPPORT D'ACTIVITÉ

DE L'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE

2019

« Ils ne savaient pas que c'était impossible ...

Alors, ils l'ont fait »

Le mot du Directeur

Voici maintenant trois ans et demi que l'Agence Monégasque de Sécurité Numérique œuvre à la sécurité numérique de la Principauté. Cette année encore, le travail a concerné essentiellement la sécurisation des systèmes d'information de l'État et des Opérateurs d'Importance Vitale. Pour autant quelques initiatives ont été prises en faveur des entreprises et des particuliers.

Un travail très important, nécessitant de nombreuses réunions, a été réalisé avec les OIV. Le dialogue avec les OIV a toujours été constructif et pragmatique. Comme annoncé l'année dernière, l'AMSN a créé une offre de détection qualifiée des incidents de sécurité à destination des OIV encadrée par une convention de service. La mise en œuvre devrait débuter mi 2020.

Sur le plan opérationnel, l'année 2019 a été, dans la lignée des années précédentes, riche en attaques plus ou moins discrètes, plus ou moins ciblées, mais toujours aussi efficaces et malheureusement non pas sans conséquence pour les victimes. Le travail de veille et d'alerte réalisé par l'AMSN est maintenant effectif et efficient; il a permis d'éviter des incidents majeurs et a prouvé que l'AMSN était capable de réagir vite et efficacement en cas d'attaque.

J'écrivais, dans les rapports précédents, qu'il était nécessaire d'aller vers le tout numérique. Une grande partie de l'année 2019 a été consacrée à mettre en place les conditions de sécurité indispensables à l'accompagnement de cette transition. La sécurité numérique est maintenant comprise par l'ensemble de la communauté, comme étant un enjeu majeur de gouvernance et de souveraineté, tant dans les services de l'État que dans les entreprises. Néanmoins, il reste encore un travail important pour passer de la compréhension des enjeux à la mise en place des dispositifs permettant d'assurer la sécurité des systèmes d'information.

Dans ce contexte, l'AMSN a continué de compléter le cadre réglementaire et les moyens techniques indispensables au développement de la confiance numérique et à la protection de la souveraineté de la Principauté dans ce domaine. Le vote par le Conseil National le 4 décembre 2019 de la loi n°1.482, modifiant la loi 1.383, pour une Principauté numérique va permettre d'accélérer cette transition et ouvrira en 2020 de nouvelles perspectives.

La maturité en matière de sécurité numérique de la Principauté, évaluée par l'ONU en 2018, avait fortement progressé. 2020 sera l'occasion de refaire un bilan.


Je tiens à nouveau à souligner la très grande qualité et la disponibilité exceptionnelle du personnel de l'AMSN, les anciens comme les nouveaux arrivés, sans qui rien ne serait possible. La place de l'AMSN dans le paysage monégasque est maintenant connue et reconnue. Le travail au profit des services de l'État ou des OIV concernés par la cybersécurité ou les attaques a prouvé la compétence et l'efficacité de l'agence.

Ce troisième rapport d'activité effectue le bilan du travail réalisé entre janvier 2019 et décembre 2019. Il présente également quelques objectifs pour 2020. J'espère qu'il vous permettra d'appréhender le volume, le sens et l'intérêt du travail de l'AMSN. Je vous affirme à nouveau que la volonté, la détermination, la disponibilité des équipes de l'AMSN sont intactes. Vous pouvez compter sur nous !

Dominique Riban

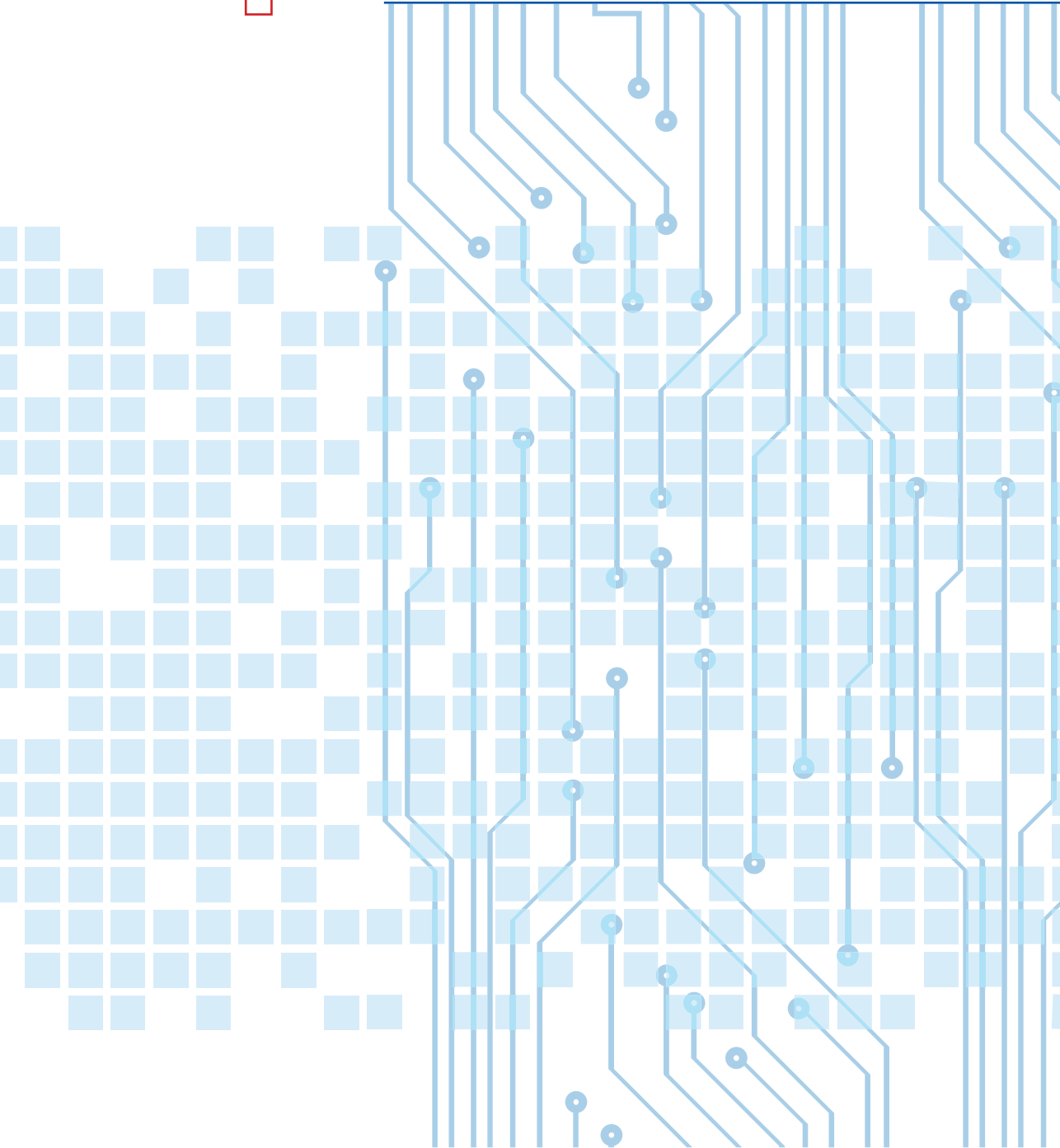


SOMMAIRE

PRÉSENTATION		5
STRATÉGIE		11
CONFIANCE		15
SÉCURISATION		18
RÉALISATIONS		23
COOPÉRATION		28

1

PRESENTATION



Rappel sur les missions de l'AMSN

L'Agence Monégasque de Sécurité Numérique, créée par l'Ordonnance Souveraine n°5.664 du 23 décembre 2015, modifiée, est l'autorité nationale en charge de la sécurité des systèmes d'information. Elle est directement placée sous l'autorité du Ministre d'État. Elle constitue un centre d'expertise, de réponse et de traitement en matière de sécurité et d'attaques numériques et a, à ce titre, en particulier pour missions :

- de prévenir, détecter et traiter les cyberattaques, notamment par l'élaboration de plans, de procédures, de dispositifs de protection et de précaution et, plus généralement, de toutes mesures à proposer au titre de la sécurité numérique ;
- de réagir en situation de crise lors des cyberattaques et de coordonner les actions de réaction ;
- de représenter la Principauté dans les instances internationales de sécurité numérique et auprès des autres centres d'expertise, de réponse et de traitement en matière d'attaques informatiques ;
- de sensibiliser les services publics et les opérateurs d'importance vitale (O.I.V.) aux exigences de la sécurité numérique ;
- de contrôler le niveau de sécurité des O.I.V. ;
- de contrôler les prestataires de services de confiance, afin de s'assurer, à tout moment, que lesdits prestataires et les services qu'ils fournissent satisfont aux exigences fixées par Arrêté Ministériel ;
- de mettre en place, actualiser et publier la liste des prestataires de services de confiance qualifiés ainsi que les informations relatives aux services qu'ils fournissent, dénommée « liste de confiance » ;
- d'évaluer et certifier la sécurité des produits et systèmes des technologies de l'information ;
- de qualifier les prestataires de services de confiance (PSCO) et les services de confiance, les prestataires d'audit de la sécurité des systèmes d'information (PASSI), les prestataires de réponse aux incidents (PRIS), les prestataires de détection d'incidents de sécurité (PDIS) et les prestataires d'informatique en nuage et d'hébergement (PINH) ;
- d'élaborer les fonctions de sécurité prévues au titre IV de l'Ordonnance Souveraine n° 3.413 du 29 août 2011, modifiée, portant diverses mesures relatives à la relation entre l'Administration et l'administré ;
- de mettre en place, si besoin, un service de certification électronique pour les services de l'État .
- L'Agence Monégasque de Sécurité Numérique assure en outre le secrétariat du Comité stratégique de la sécurité numérique créé par l'Ordonnance Souveraine n° 6.486 du 25 juillet 2017.

L'Agence Monégasque de Sécurité Numérique est membre de la Commission d'homologation chargée d'assister les autorités dans l'instruction des demandes d'homologation de systèmes d'information des services exécutifs de l'État, disposition prévu par l'Arrêté Ministériel 2017-56 du 1er février 2017.

Les chiffres de l'année

UNE AGENCE 10 PERSONNES

4 000 heures supplémentaires

1

- Une direction (directeur, directeur adjoint, chef de bureau) ;
- Un pôle expertise avec 2 personnes ;
- Un pôle réglementation et relations internationales (assuré par la Direction) ;
- Un pôle opérationnel avec 3 ingénieurs seniors et 2 ingénieurs juniors ;
- En fin 2019, des travaux importants ont débuté pour accroître la superficie de l'Agence (passage de 120 à 200 M²). Ce nouvel aménagement permettra d'améliorer l'environnement de travail pour mieux servir les services de l'État et les OIV.

OPÉRATIONS DE CYBERDÉFENSE

3

- 65 tickets d'incidents qualifiés ;
- 4 incidents critiques nécessitant des actions approfondies de réponse à incident
- 1,7 milliard d'événements analysés par les outils de détection de l'AMSN ;
- 247 millions de fichiers reconstitués permettant la détection de 3000 logiciels malveillants et 375 fichiers infectés.

DOCUMENTATIONS

2

- Rédaction de 9 textes réglementaires dont une Ordonnance Souveraine et 8 Arrêtés Ministériels avec le support juridique de la Délégation Interministérielle chargée de la Transition Numérique ;
- Rédaction des directives et procédures nécessaires à la certification ISO 27001 pour la gestion du Datacenter de l'AMSN hébergeant :
 - l'Infrastructure de Confiance Nationale (ICN) pour les services de confiance prévus par la loi n°1.383, modifiée, pour une Principauté Numérique ;
 - les systèmes de détection qualifiés prévus par la loi n°1.435 relative à la lutte contre la criminalité technologique.

SENSIBILISATIONS FORMATIONS

4

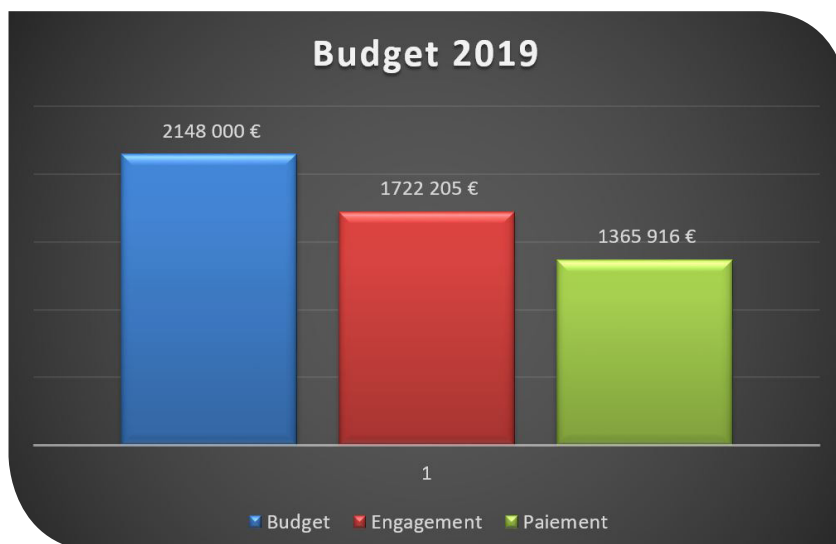
- Plus de 50 entretiens formels avec les autorités, directeurs ou chefs de service de l'État, et responsables d'OIV ;
- 11 formations reçues ;
- Participation à 7 forums de cybersécurité.

FINANCEMENT

5

La loi n° 1.467 du 20 décembre 2018 portant fixation du budget général primitif de l'exercice 2019, adoptée par le Conseil National dans sa séance du 19 décembre 2018, prévoyait les crédits pour la sécurité numérique à l'article 708.946.

Cet article regroupe les besoins de tous les services de l'État en matière de sécurité numérique ; sur les 3,5M€ alloués à cet article, 2,1M€ l'étaient pour l'AMSN.

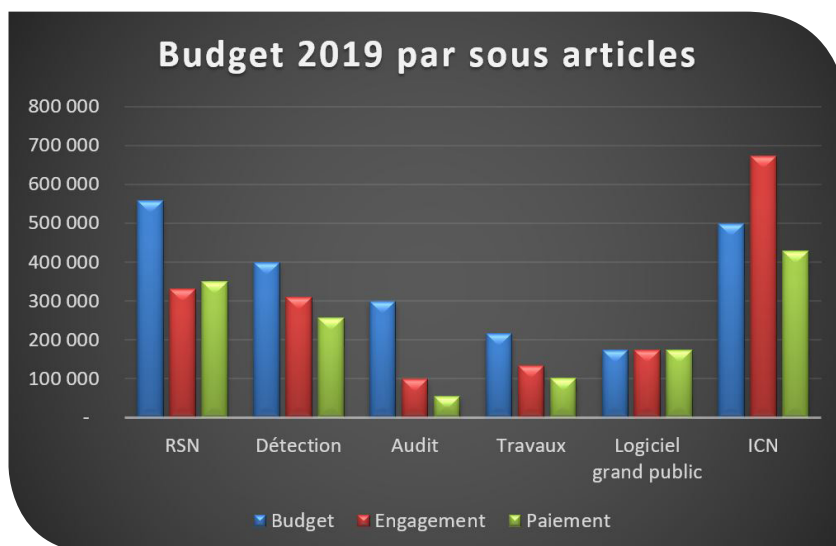


RSN : Réseau de Sécurité National

ICN : Infrastructure de Confiance Nationale

Détection : systèmes de détection qualifiés

Les crédits non engagés ont été reportés sur l'exercice 2020.



L'AMSN en 6 questions

1

QUEL RÔLE AUPRÈS DES AUTORITÉS ET DES ADMINISTRATIONS ?

En collaboration avec les services de l'État et en particulier avec la Délégation Interministérielle pour la Transition Numérique (DITN), l'AMSN instruit et prépare les décisions relatives à la sécurité du numérique et à celles concernant les données sensibles. Elle établit le corpus réglementaire encadrant les activités de sécurité numérique, contribuant à la confiance dans le numérique. Elle participe à l'évolution des systèmes d'information de l'État.

2

QUELLE MISSION AUPRÈS DES OPÉRATEURS D'IMPORTANCE VITALE ?

L'AMSN accompagne les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information critiques, rendue obligatoire par la loi n°1.435 relative à la lutte contre la criminalité technologique. Cette sécurisation passe par l'application de 21 règles de sécurité annexées à l'Arrêté Ministériel n° 2018-1053 définies avec les OIVs. Un calendrier d'application est défini d'un commun accord avec chaque OIV.

3

QUELLES RELATIONS AVEC LES AUTRES ACTEURS DE LA SÉCURITÉ NUMÉRIQUE ?

Parce qu'une agence ne peut à elle seule répondre à tous les besoins en matière de sécurité numérique, l'AMSN se donne les moyens de contribuer au développement d'un écosystème fiable. Pour ce faire, elle s'appuie sur ses propres savoir-faire, sur des coopérations avec des partenaires de confiance par la qualification d'entreprises monégasques et françaises dans le domaine de la sécurité numérique.

Elle apporte également son soutien à la cellule cybercriminalité qui a été créée cette année à la Direction de la Sureté Publique pour mieux prendre en compte les cyber malveillances dont sont victimes les entreprises et les résidents.

4

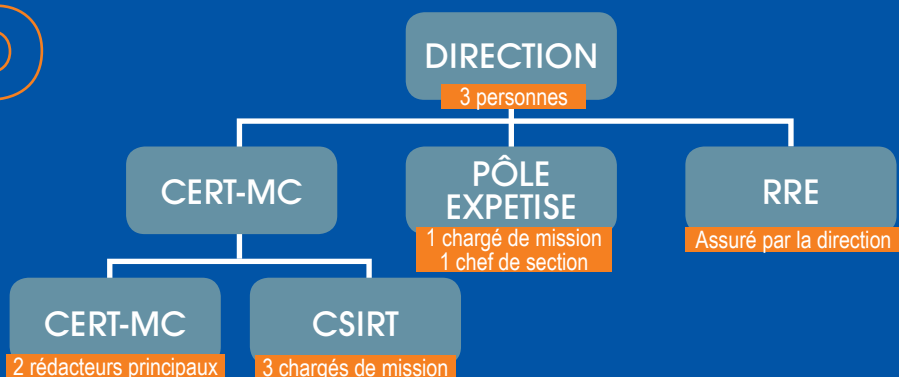
QUELLE PLACE DANS LE CONTEXTE INTERNATIONAL ?

Le cyber espace n'a pas de frontières et nécessite donc pour faire face aux enjeux de ce monde de mettre en place des relations internationales avec des partenaires de confiance. L'agence est membre du TF-CSIRT regroupant 371 centres d'expertise et de réponse à incidents privés et publics principalement européens, ainsi que du FIRST regroupant, quant à lui, 523 structures de même nature dans le monde. L'agence est membre de droit de la réunion annuelle des agences gouvernementales (NatCSIRT), permettant des échanges d'information, améliorant la prévention et le traitement des attaques.

Par ailleurs, elle a établi des relations privilégiées avec l'Agence Nationale de la Sécurité des Systèmes d'Information française et de grandes entreprises internationales.

5

COMMENT EST ORGANISÉE L'AGENCE



La direction de l'agence assure le bon fonctionnement au quotidien de l'Agence, a la charge, la conception, le pilotage et le suivi de la stratégie nationale et de l'agence, et assure la fonction du pôle Règlementation et Relations Extérieures, RRE.

Le CERT-MC, « computer emergency response team », est le pôle opérationnel de l'AMSN. A ce titre il sert les missions principales de prévention, de détection et de traitement des cyber-attaques contre les systèmes d'information de l'État et des opérateurs d'importance vitale. Le « Security Operation Center », SOC, mis en place en 2019, responsable de la veille sur les systèmes de détection qualifiés, est composé d'ingénieurs formés dans le domaine de la sécurité informatique et de l'analyse de la menace. Le « computer security incident response team », CSIRT, est en charge du traitement des incidents de sécurité.

Le pôle Expertise, PEx, porte la mission globale d'expertise et d'assistance technique de l'agence. Il apporte son soutien à l'ensemble des autres pôles de l'AMSN, aux services publics, et aux opérateurs d'importance vitale. Il définit et maintient à jour les référentiels techniques de l'agence. Il porte la mise en place de l'Infrastructure de Confiance Nationale.

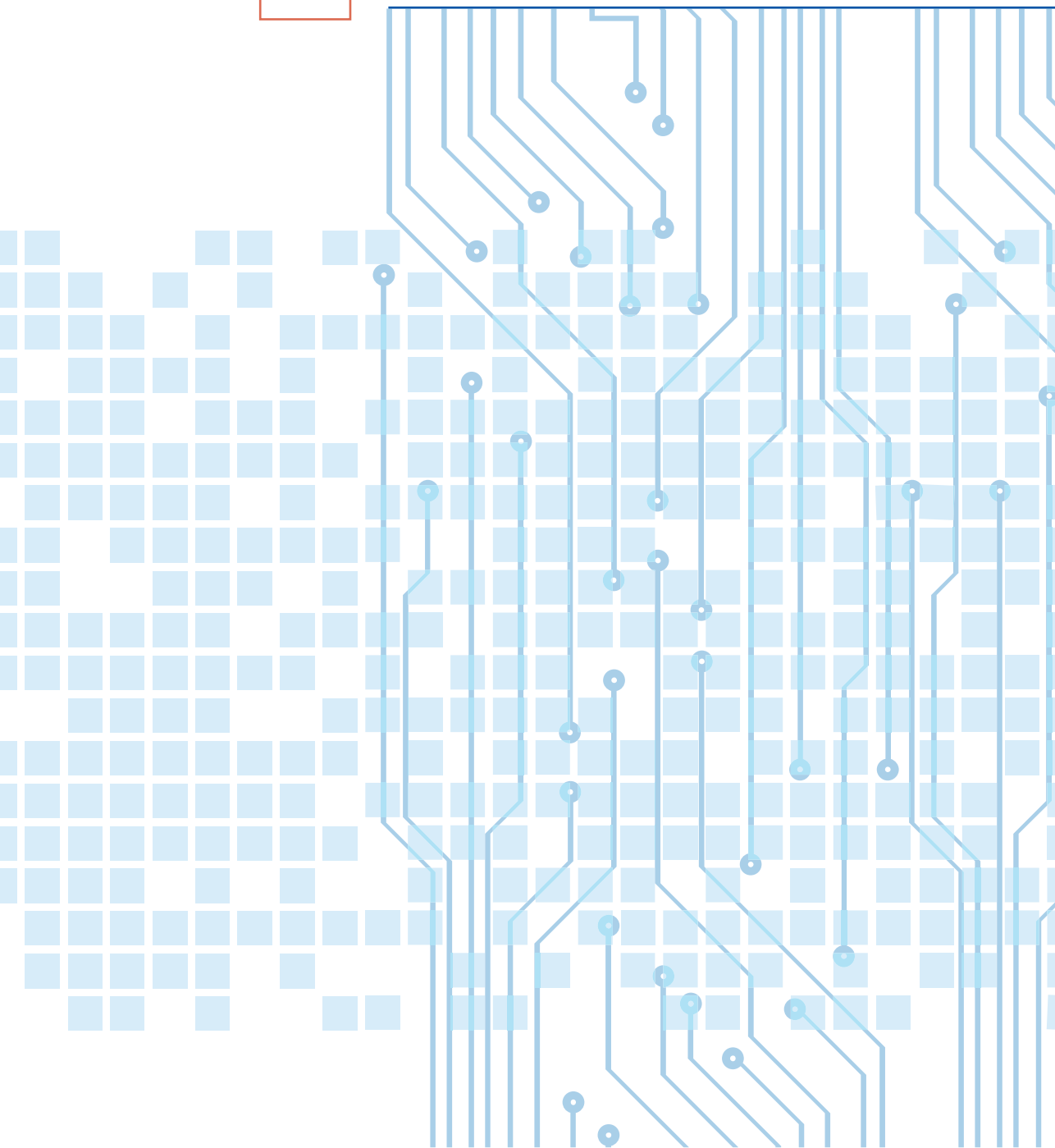
6

ET EN CAS D'ATTAQUE ?

En cas d'attaque avérée, le personnel du CERT-MC assiste la victime pour caractériser l'attaque, définir avec elle un plan de remédiation, et l'accompagner durant toutes les étapes de traitement de l'incident. La victime est invitée à déposer une plainte auprès de la Direction de la Sûreté Publique, Division de Police Judiciaire, Unité de Lutte contre la Criminalité Technologique créée le 12 juin 2019.

Dossiers gérés par l'ULCT	Du 12 juin au 31 décembre 2019
Intrusion et maintien dans un système d'information	1
Ransomwares	1
Phishing	1
Infraction à la protection des informations nominatives	1
Escroquerie / Usurpation d'identité	2
Harcèlement (par voie numérique)	0
Assistance technique	15

2 STRATEGIE



LES ACTIONS DANS LE CADRE DE LA STRATÉGIE POUR LA SÉCURITÉ DU NUMÉRIQUE

1 LE COMITÉ STRATÉGIQUE DE LA SÉCURITÉ NUMÉRIQUE

Le Comité stratégique de la sécurité numérique, institué par l'Ordonnance Souveraine n°6.486 du 25 juillet 2017, a pour rôle :

- de valider et de suivre les plans d'action découlant de la stratégie nationale pour la sécurité du numérique ;
- d'identifier les technologies-clés pour le développement d'un environnement numérique de confiance ;
- d'évaluer les besoins en formation initiale et continue ;
- de suivre les travaux de recherche et d'en accompagner leurs valorisations ;
- d'analyser la veille technologique et économique permettant d'anticiper les évolutions des questions liées au numérique.
- Le Comité s'est réuni 2 fois en 2019. Parmi les sujets abordés, les principaux sont :
- Les séances de sensibilisation des agents de l'État à la sécurité des systèmes d'information ;
- La mise à disposition aux clients de Monaco Telecom d'un antivirus pour leurs ordinateurs et leurs smartphones : « Monaco Care Safety » ;
- L'extension de l'Infrastructure de Confiance Nationale, décidée en 2018 pour générer des certificats électroniques donnant valeur probante aux services de confiance dans le cadre de la relation entre l'Administration et l'administré, aux personnes morales ;
- La décision de mettre en place dans les services du gouvernement des stations de décontamination des supports USB ;
- La mise en place d'une solution sécurisée de partage de fichiers pour les services de l'État ;
- La mise en place d'une messagerie instantanée sécurisée.

2 LES RÉALISATIONS SUR LES 5 OBJECTIFS DE LA STRATÉGIE

Protéger les intérêts fondamentaux, la défense et la sécurité des systèmes d'information des institutions officielles de la Principauté et des infrastructures critiques, ainsi que la gestion des crises informatiques majeures :

- Définition des calendriers d'application des obligations pour les Opérateurs d'Importance Vitale (OIV) avec les intéressés, notification aux OIV de ce calendrier fixant le T0 du projet ;
- Traitement de plusieurs attaques sur des systèmes d'information de l'État et des OIV ;
- Diffusion des alertes et vulnérabilités ;

² Les services électroniques comprennent : la signature, le cachet électronique pour une entité, l'authentification, le chiffrement, l'identification,

Développer la confiance dans le numérique, le respect de la vie privée numérique, la protection des données personnelles et l'appréhension de la cyber malveillance :

- 20 systèmes d'information de l'État ont fait l'objet d'une démarche d'homologation (réalisées ou démarrées en 2018) afin de s'assurer de leur sécurisation ;
- 7 audits ont été effectués, soit par l'AMSN soit par des PASSI, afin de vérifier le niveau de sécurité appliqué aux systèmes d'information
- Déploiement de l'Infrastructure Nationale de Confiance par la société Certinomis, groupe la poste, pour permettre la délivrance de certificats qualifiés pour les services de signature électronique, de cachet électronique pour les monégasques, les résidents, les services exécutifs de l'État et les entreprises monégasques. Les premiers certificats devraient être émis en juin 2020 ;
- Lancement en septembre de l'offre Monaco Care Safety. Ce service gratuit pour les clients de Monaco Télécom, offerte par le Gouvernement Princier, permet d'obtenir 5 à 10 licences à installer sur tous les types d'appareils (PC, tablettes, smartphone iOS et Android), donnant accès à des fonctionnalités d'antivirus, de contrôle parental pour la navigation sur Internet, de navigation sécurisée sur Internet, et de gestionnaire de mots de passe (permettant de stocker et définir des mots de passe différents pour toutes les applications en ne retenant qu'un seul mot de passe).



*Remise de la lettre d'intention par le Ministre d'État
au Directeur Général de Monaco Telecom
pour le financement de la solution Monaco Care Safety, le 16 avril 2019*

Développer les sensibilisations et les formations initiales et continues :

- Une douzième et dernière séance de sensibilisation à la cybersécurité pour les agents de l'État a été réalisée en décembre. Près de 900 agents ont ainsi été sensibilisés depuis le début de la démarche. La sensibilisation des agents de l'État devra se faire dans le futur sur la plateforme de formation en ligne de la DRHFFP ; le contenu des cours en ligne de la plateforme française SecNumacamédie a été mis à disposition à l'AMSN par l'ANSSI, charge à l'AMSN de la mettre en forme et la rendre compatible avec la plateforme de la DRHFFP. Un renfort en communication numérique sera nécessaire pour réaliser cette tâche.
- Le personnel de l'AMSN a suivi 5 formations spécialisées dispensées par le CFSSI . Ces formations se poursuivront en 2020, en particulier pour les nouveaux recrutements.
 - > « Certificats électroniques »
 - > « Homologation de sécurité »
 - > « La méthode EBIOS – outil de gestion des risques »
 - > « Incidents de sécurité – s'y préparer et y répondre »
 - > « Rétro conception de fichiers malveillants »

Faire de la sécurité du numérique un facteur de compétitivité :

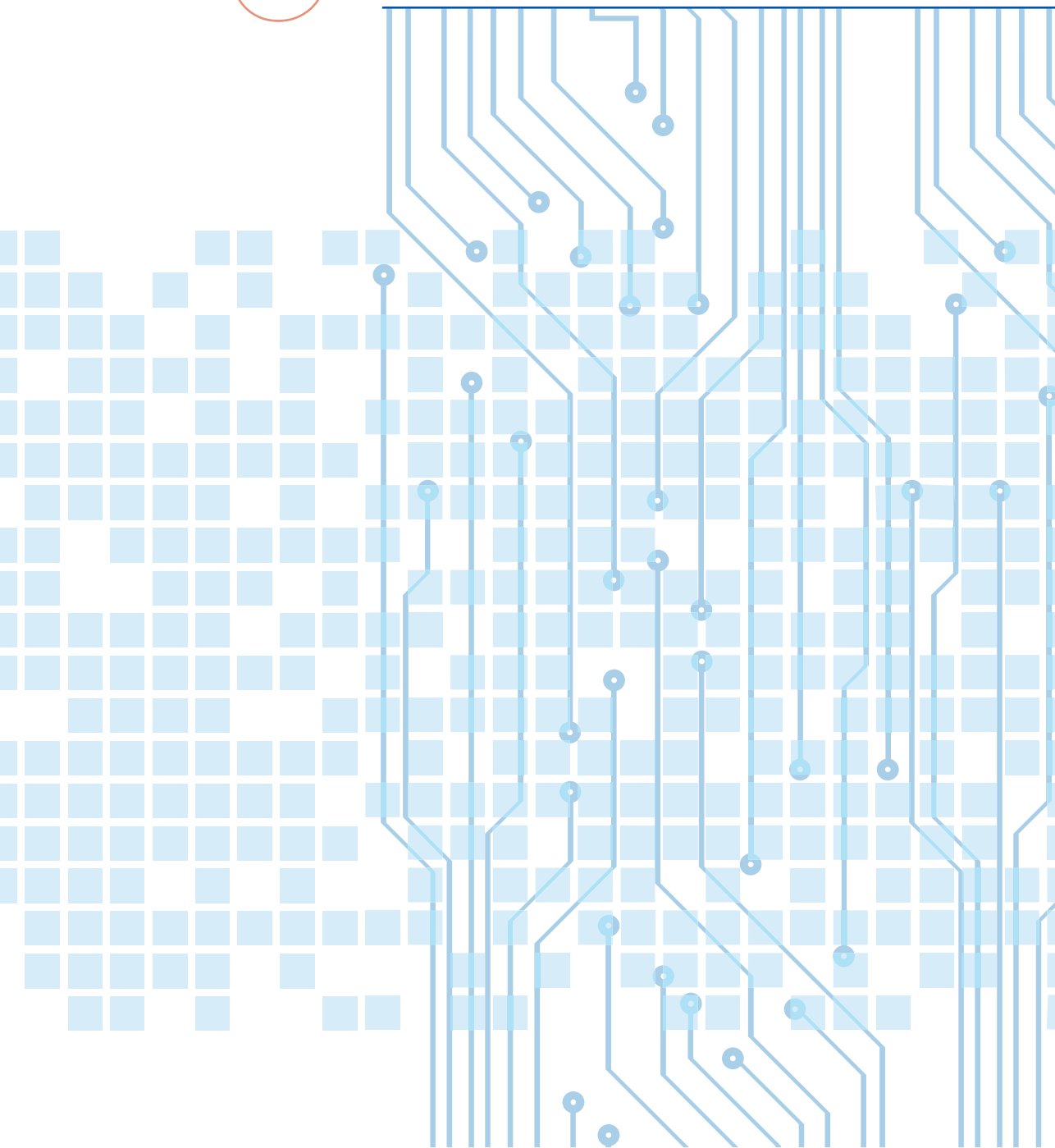
Pour la deuxième année, 10 entreprises monégasques ont pu participer aux « Assises de la Sécurité » autour de l'AMSN sous l'enseigne de « Monaco Cyber Initiative ». Cette participation a permis de montrer l'importance et la place que souhaite prendre la Principauté dans le domaine de la cyber sécurité. Le nombre de visiteurs sur le stand démontre que la Principauté est aujourd'hui un acteur à part entière ;

- La participation aux différents forums a permis de faire connaître l'AMSN. Le nombre et la valeur des candidatures pour nos recrutements montrent que les compétences de l'AMSN et le travail effectué sont maintenant connus dans le milieu de la cyber sécurité ;
- Aujourd'hui, trois acteurs de la Principauté sont qualifiés « Prestataire d'Audit de la Sécurité des Systèmes d'Information » (PASSI) et trois autres sont en cours de qualification.

S'ouvrir à l'international par l'établissement de liens internationaux en matière de sécurité numérique, la contribution de la Principauté à la stabilité du cyber espace :

- L'AMSN a participé à 7 réunions et conférences internationales sur la cybersécurité :
 - > FIC (France) ;
 - > FIRST (Ecosse) ;
 - > TF-CSIRT (Luxembourg) ;
 - > DEFCON (USA) ;
 - > DFRWS (Norvège) ;
 - > HACK.LU (Luxembourg) ;
 - > CORIIN (France).

3 CONFIANCE



L'ENVIRONNEMENT DE CONFIANCE

L'année 2019, par la décision du Gouvernement d'accélérer la transition numérique pour servir les enjeux stratégiques, économiques et sociaux de la Principauté, a été une année décisive dans la mise en place de processus de sécurisation de tous les nouveaux services numériques. L'Agence Monégasque de Sécurité Numérique s'est efforcée d'instaurer un environnement de confiance et de sécurité pour cette transition et de faire prendre les décisions d'arbitrage entre les besoins de sécurité et de souveraineté et le service offert.

1 UN CADRE RÉGLEMENTAIRE ÉVOLUTIF AU SERVICE DE LA TRANSITION NUMÉRIQUE

De nouvelles technologies, de nouveaux usages, de nouvelles applications apparaissent en permanence. Les menaces discrètes et sournoises sont hélas bien présentes. La sécurité numérique est donc un facteur clé de ce changement. La sécurité doit rester proportionnée pour accompagner au mieux la transition numérique.

Le cadre réglementaire de la Principauté doit permettre ces évolutions en toute sécurité, assurer le suivi et l'anticipation de ces changements en offrant aux différents acteurs, publics comme privés, un environnement sécurisé.

En tant qu'autorité nationale, l'AMSN, en 2019, a continué, ou contribué à la mise en place de l'ensemble des textes législatifs et réglementaires en matière de sécurité des systèmes d'information qui garantissent la protection de la souveraineté nationale et favorisent l'attractivité de la Principauté.

L'AMSN participe à l'encadrement des bonnes pratiques en matière de sécurité des systèmes d'information, à l'élaboration de référentiels normatifs en matière de sécurité numérique, à l'intégration des normes juridiques et techniques ainsi qu'à la mise à jour des textes réglementaires. En outre, l'agence assiste les services de l'État et les OIV dans l'élaboration et la mise en œuvre des mesures ou dispositifs issus des textes.

2 L'ACTIVITE DE L'AGENCE DANS LE DOMAINE REGLEMENTAIRE

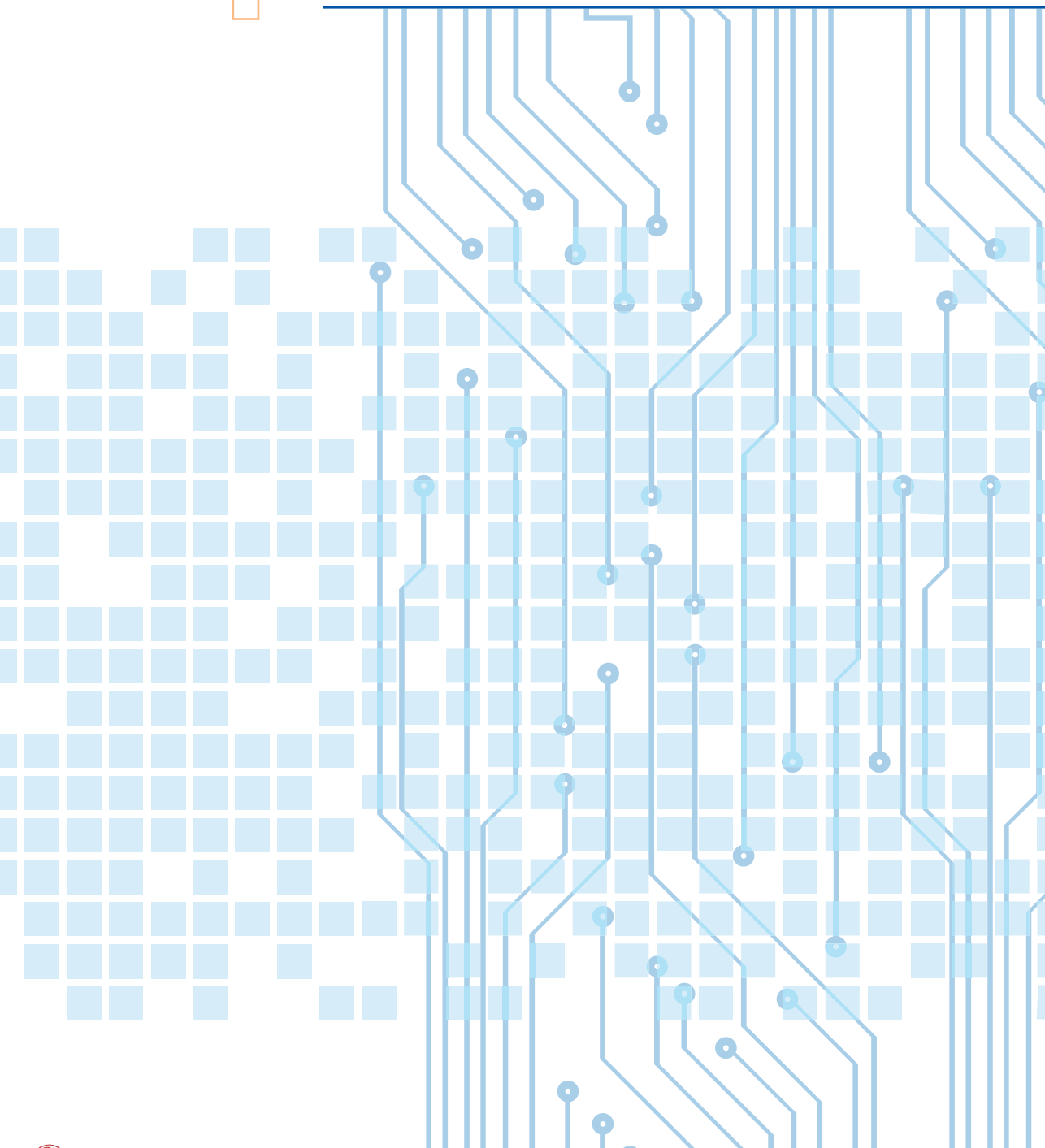
- Ordonnance Souveraine n° 7.680 du 16 septembre 2019 portant application de l'article 25 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique. Elle définit les moyens dont dispose l'Agence Monégasque de Sécurité Numérique, pour caractériser une attaque contre les systèmes d'information de la Principauté ;
- Arrêté Ministériel n° 2019-451 du 16 mai 2019 créant une zone protégée au Centre National de Gestion de Crise ;

² Les services électroniques comprennent : la signature, le cachet électronique pour une entité, l'authentification, le chiffrement, l'identification,

- Arrêté Ministériel n° 2019-452 du 16 mai 2019 créant une zone protégée au Data Center n° 3 de Monaco Telecom ;
- Arrêté Ministériel n° 2019-453 du 16 mai 2019 créant une zone protégée au sein de la Direction des Réseaux et Systèmes d'Information ;
- Arrêté Ministériel n° 2019-454 du 16 mai 2019 créant une zone protégée au sein du Service d'Information et de Contrôle sur les Circuits Financiers ;
- Arrêté Ministériel n° 2019-455 du 16 mai 2019 créant une zone protégée à la caserne du Corps des Carabiniers du Prince ;
- Arrêté Ministériel n° 2019-525 du 18 juin 2019 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée. Il permet de qualifier les Opérateurs d'Importance Vital afin qu'ils puissent, s'ils le souhaitent, exploiter leur propre système de détection qualifié ainsi que leur propre système de gestion des informations et des événements de sécurité ;
- Arrêté Ministériel n° 2019-791 du 17 septembre 2019 portant application de l'article 2, a) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée. Il définit les règles destinées à garantir la sécurité des systèmes d'information sensibles;
- Arrêté Ministériel n° 2019-841 du 8 octobre 2019 portant application de l'article 28 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique. Il a pour objet les contrôles destinés à vérifier le niveau et le respect des règles de sécurité des systèmes d'information des opérateurs d'importance vitale.

4

SECURISATION



SÉCURISATION DES SYSTÈMES D'INFORMATIONS

1 SÉCURISER LES ÉCHANGES

Afin de sécuriser les échanges d'information, la Direction de l'Administration Numérique avec le support de l'AMSN a initié l'installation en Principauté d'une instance de la solution « Cryptobox » de la société «Ercom a Thales company » et devrait être opérationnelle au premier semestre 2020. Installée sur un cloud de la Principauté, elle permettra de simplifier les échanges en garantissant un niveau de confidentialité « Diffusion Restreinte ».

Par ailleurs, une instance de l'application de messagerie instantanée sécurisée « Citadel Team » pour smartphones Android et iOS, PC et MAC, a été mise en place. Ce système, permet des échanges rapides et sécurisés notamment avec les OIV pendant la gestion des incidents de sécurité. Il a prouvé son utilité et son efficacité dans le traitement de plusieurs attaques chez des OIV.

2 LE SECRET DE SÉCURITÉ NATIONALE

Les études pour la mise en place, au sein des services de l'État, d'un réseau permettant le traitement des informations classifiées sont désormais terminées. Ce réseau sera testé fin du premier semestre 2020 pour entrer en service à l'été 2020. En raison des travaux de sécurisation des différents locaux hébergeant les matériels du système, la période de déploiement va s'avérer un peu plus longue que prévue.

Toujours dans ce domaine, l'AMSN a assisté plusieurs services de l'État pour la sécurisation de leurs systèmes d'information et financé une partie des travaux de mise en conformité des locaux.

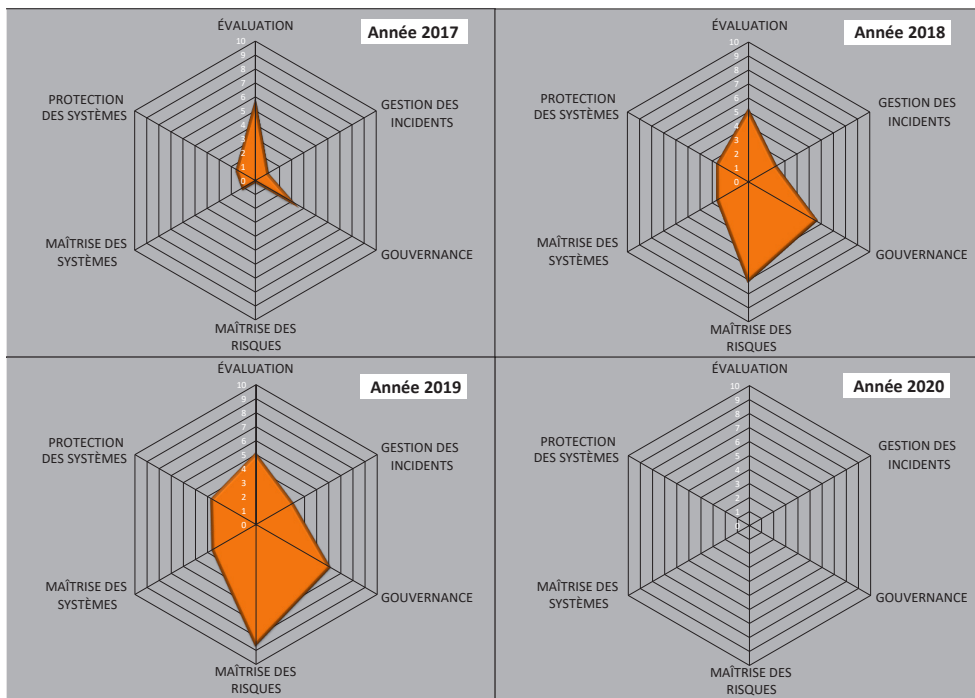
3 LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT

La Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E), publiée par Arrêté Ministériel, fait l'objet d'un suivi annuel avec les services exécutifs de l'État concernés. Pour mémoire, cette politique a pour objectif d'améliorer la protection des informations détenues dans les systèmes d'information. Elle définit 161 mesures, qui s'appuient sur 10 principes stratégiques, applicables aux services exécutifs de l'État et aux établissements publics qui doivent adresser un rapport annuel de progression à l'AMSN.

Sous l'impulsion de la Délégation Interministérielle Chargée de la Transition numérique, la multiplication des projets et la réorganisation des services exécutifs de l'État en charge du numérique nécessaires à une transition numérique volontariste a permis d'instituer une démarche qui prend en compte la mise en conformité à la PSSI-E. Même si l'évolution de la mise en conformité est encore trop lente, la volonté de faire est présente.

L'évolution du niveau de maturité de la sécurité des système d'information est appréciée, à partir des résultats de l'auto-évaluation réalisée par les services exécutifs concernés, suivant 6 axes :

- > Évaluation (suivi de la mise en œuvre de la PSSI-E) ;
- > Gestion des incidents (de sécurité informatique) ;
- > Gouvernance (de la sécurité informatique) ;
- > Maîtrise des risques (informatiques) ;
- > Maîtrise des systèmes (informatiques) ;
- > Protection des systèmes (informatiques).



Evolution du niveau de maturité de la sécurité des systèmes d'information des services exécutifs de l'État 2017-2019.

4

SOUTIENS ET CONSEILS DANS LA CONCEPTION DES SYSTÈMES D'INFORMATION

L'AMSN a continué à apporter son soutien dans la conception des architectures des systèmes d'information de l'État mais également des OIV.

Cette contribution permet de prendre en compte, dès le début des projets, la sécurité des systèmes d'information (Disponibilité, Intégrité, Confidentialité, Traçabilité). Encore trop de projets sont lancés avant d'avoir défini les besoins de sécurité, entraînant, in fine, des retards à l'homologation et donc à la mise en service.

Dans ce cadre de sécurisation des logiciels et systèmes d'information, l'AMSN a, par son concours, aidé différents éditeurs de logiciels et fournisseurs à améliorer la sécurité de leurs solutions.

L'AMSN, en tant que membre de droit de toute commission d'homologation, a participé à de nombreuses réunions pour l'étude et l'homologation des systèmes d'information des différents services exécutifs de l'État. Ainsi, 20 systèmes ont été homologués en 2019. Le nombre de système d'information à homologuer devrait encore augmenter en 2020.

5

DES STATIONS DE DÉCONTAMINATION DES SUPPORTS USB POUR LES SERVICES EXÉCUTIFS DE L'ÉTAT

Un des principaux vecteurs de propagation des virus informatiques est encore aujourd'hui l'utilisation de supports USB non maîtrisés. Plus de 30% des événements de sécurité détectés sur les systèmes d'information du Gouvernement, constatés en 2017 et 2018, avaient comme origine un support USB.

L'AMSN s'est donc efforcée de déployer des stations de décontamination des supports USB. Ces stations sont des ordinateurs sécurisés, équipées d'un écran tactile pour l'interaction avec ses utilisateurs, sur lesquelles sont installés plusieurs antivirus. Elles permettent simplement de vérifier le contenu des supports USB et de s'assurer qu'ils ne contiennent pas de virus informatique avant de les insérer sur les ordinateurs des services exécutifs de l'Etat. Si un virus informatique est détecté, les stations invitent l'utilisateur à effacer le ou les fichiers contaminés.

12 stations ont été déployées dans les services exécutifs de l'État. Au-delà de leur fonction de décontamination, ces stations ont aussi un rôle de sensibilisation.



6

PRESTATAIRES QUALIFIÉS

Le référentiel pour les « Prestataires d'Audit de la Sécurité des Systèmes d'Information » (PASSI) a été publié en 2017. L'année 2018 a vu Monaco Informatique Service devenue Monaco Digital, première société monégasque, obtenir cette qualification. En 2019, les sociétés Digital Security groupe Econocom et PWC ont été qualifiées. L'AMSN a fait passer des examens écrits aux personnels de ces deux sociétés pour l'obtention de la qualification. Trois autres sociétés en cours de qualification devraient obtenir le sésame en 2020.

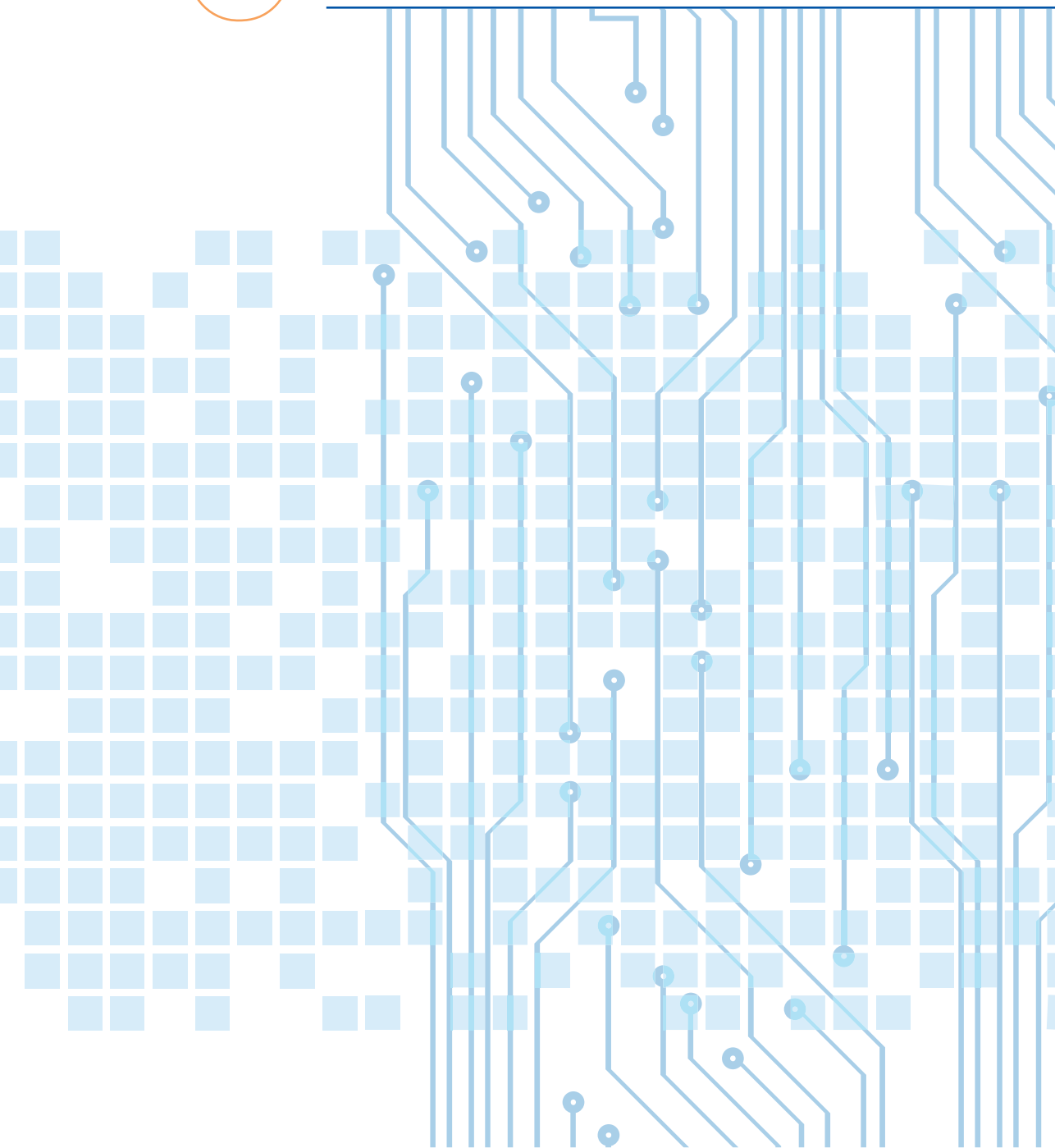


Remise de la qualification par Dominique RIBAN, Directeur de l'AMSN, à Jean-Claude TAPIA, Président de Econocom Digital Security et à Serge BERTOLDO, Consulting Leader PwC France Région Sud & Monaco de PwC Advisory - 10 octobre 2019.

Par ailleurs, une société monégasque a commencé en 2019 le travail pour obtenir la qualification de « Prestataires d'Informatique en Nuage et d'Hébergement » (PINH) annexé à l'Arrêté Ministériel 2018-1108 du 26 novembre 2018. Ce référentiel apporte aux commanditaires d'une prestation d'hébergement informatique ou de solution « Cloud », des garanties quant aux compétences du personnel du prestataire, à la qualité de sa prestation, à la confiance qu'il peut accorder au prestataire et au niveau de sécurité apporté à la prestation. Le respect de ce référentiel est indispensable pour pouvoir prétendre être hébergeur de données de santé.

5

REALISATIONS



ACTIVITÉ OPÉRATIONNELLE

1 VEILLE ET PUBLICATION

Le CERT-MC, avec le concours entre autres du CERT-FR, assure une veille des informations issues de la presse spécialisée, des éditeurs de logiciels, des constructeurs de matériel informatique, des laboratoires de recherche spécialisés en sécurité numérique afin de pouvoir sensibiliser l'ensemble des acteurs de la Principauté, et réagir rapidement à toutes menaces qui pourraient concerner les systèmes d'information de l'État et des OIV.

Ainsi, le CERT-MC a diffusé en 2019 :

249

« actualités » sur le cyber espace,
afin de sensibiliser et informer les acteurs
spécialisés de la Principauté

51

synthèses « Les essentiels de la cyber »
adressées à différentes autorités. Ce document
résume, sans élément technique, les faits les
plus marquants. Ainsi les autorités et les hauts
responsables peuvent être sensibilisés aux
grands événements mondiaux dans le domaine
de la cyber sécurité

15

Alertes de sécurité,
documents destinés à
prévenir d'un danger
immédiat ;

656

avis de sécurité, documents faisant état de
vulnérabilités et des moyens de s'en prémunir,
vers les OIV ou les services de l'État afin
d'éviter la compromission de leurs systèmes
d'information.

Le CERT-MC dispose de systèmes de détection qualifiés qui lui permettent d'identifier les attaques sur les systèmes d'information de l'État. Ces dispositifs, opérationnels depuis novembre 2017, permettent d'assurer la collecte d'informations techniques dans les flux informatiques, et de procéder en temps réel à l'analyse des anomalies et la recherche de menaces.

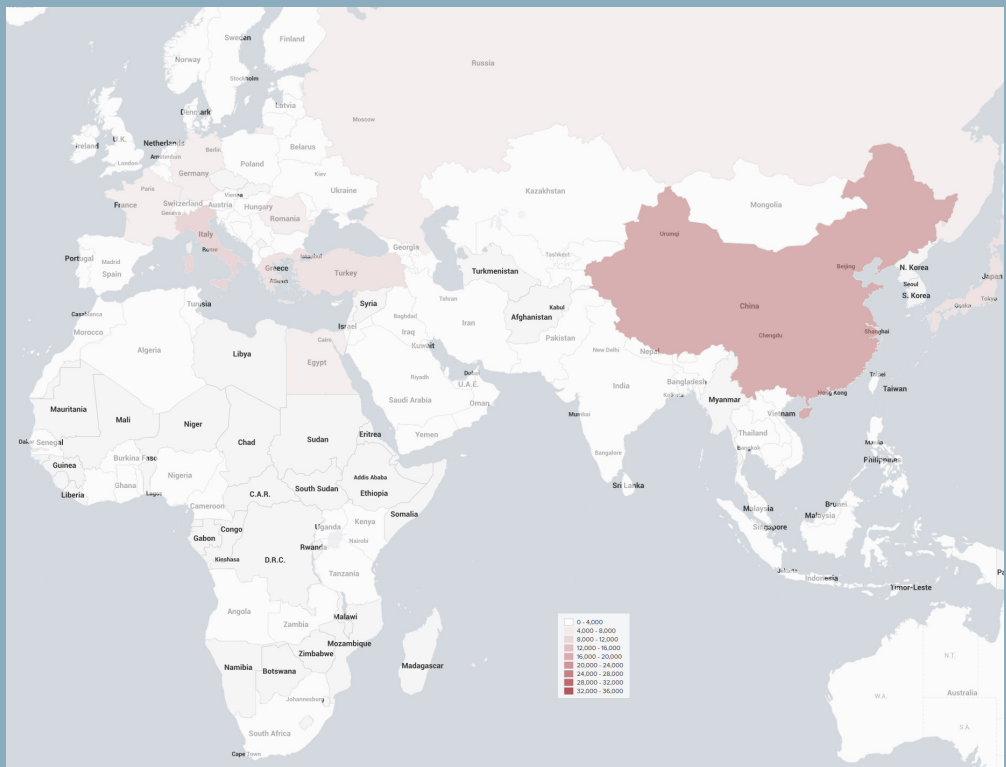
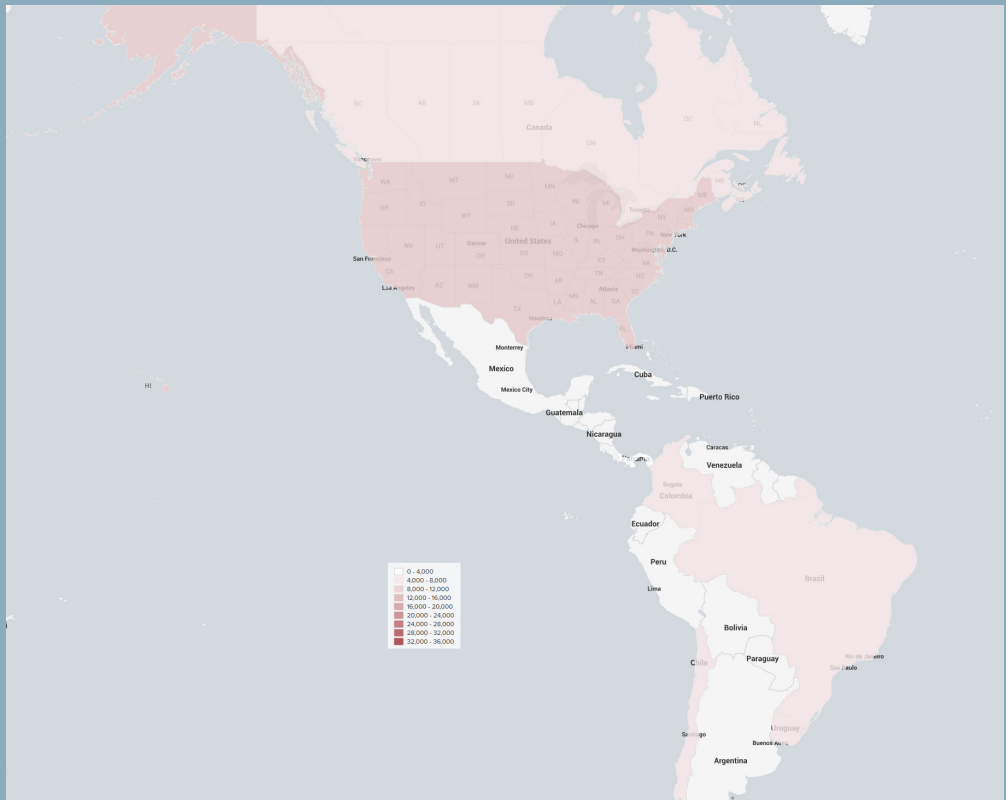
En outre, pour remplir au mieux leur rôle, les ingénieurs du SOC, dont la mission principale est d'opérer une veille sur ces systèmes de détection, conçoivent et développent des tableaux de bord sur mesure en s'appuyant sur un système de gestion des informations et évènement de sécurité. Ces tableaux de bord constituent des outils d'aide à la décision en temps réel en hiérarchisant et en visualisant les détails des attaques ainsi que la relation séquentielle entre divers événements afin de déterminer rapidement les mesures appropriées.

SOC_attacks_detail

parties prenantes: All | minimum severity: 3 | signature: ET EXPLOIT Possib... | dest_ip: All | Hide Filters

_time	dest_ip	alert.severity	alert.signature	Country	stakeholder	http.http_method
1	2020-07-09 15:18:22.783	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
2	2020-07-09 15:08:24.547	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
3	2020-07-09 14:01:25.794	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
4	2020-07-09 13:57:23.908	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
5	2020-07-09 11:54:25.107	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
6	2020-07-09 11:41:23.731	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
7	2020-07-09 11:35:30.573	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
8	2020-07-09 11:25:24.835	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	United States		POST
9	2020-07-09 10:20:27.864	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
10	2020-07-09 06:08:23.902	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
11	2020-07-09 06:05:29.732	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	United States		POST
12	2020-07-09 06:05:29.668	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	United States		POST
13	2020-07-09 05:12:27.792	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Norway		POST
14	2020-07-09 04:17:29.619	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
15	2020-07-09 03:22:25.337	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
16	2020-07-09 02:55:26.908	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Norway		POST
17	2020-07-09 02:39:28.278	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST
18	2020-07-09 02:33:23.999	1	ET EXPLOIT Possible ZYXEL P660HN-T v1 RCE	Colombia		POST

Les deux graphiques ci-dessous illustrent le nombre et l'origine géographique des attaques de type réseau en 2019.



Plusieurs catégories d'attaques peuvent être détectées par ces systèmes :

- Les attaques réseau : tout type d'activité malveillante utilisant le réseau comme vecteur d'attaque (échec d'authentification répétés, tentatives d'injection de paquets malveillants...)
- Les codes informatiques malveillants qui détournent un programme de son exécution normale ;
- Les programmes ou fichiers malveillant développés dans le but de nuire à un système informatique apparaissant sous la forme de programmes ou fichiers ordinaires.

Aujourd'hui, la totalité des systèmes d'information de l'État bénéficient du haut niveau de protection apporté par ces systèmes de détection. Ce service sera également proposé aux OIV de la Principauté en 2020.

Par ailleurs, un système de gestion de tickets permet d'assurer un suivi précis de toutes les actions effectuées et de réaliser un retour d'expérience sur chaque cas, dans une démarche d'amélioration continue.

Depuis janvier 2019, le CERT-MC a qualifié et traité de nombreuses alertes, parmi les détections qu'il a effectuées et les signalements qui lui ont été faits. 65 alertes se sont révélées être de vrais incidents et 4 d'entre elles ont été qualifiées d'incidents majeurs qui ont nécessité plusieurs dizaines d'heures de travail avec les victimes pour rétablir la situation.

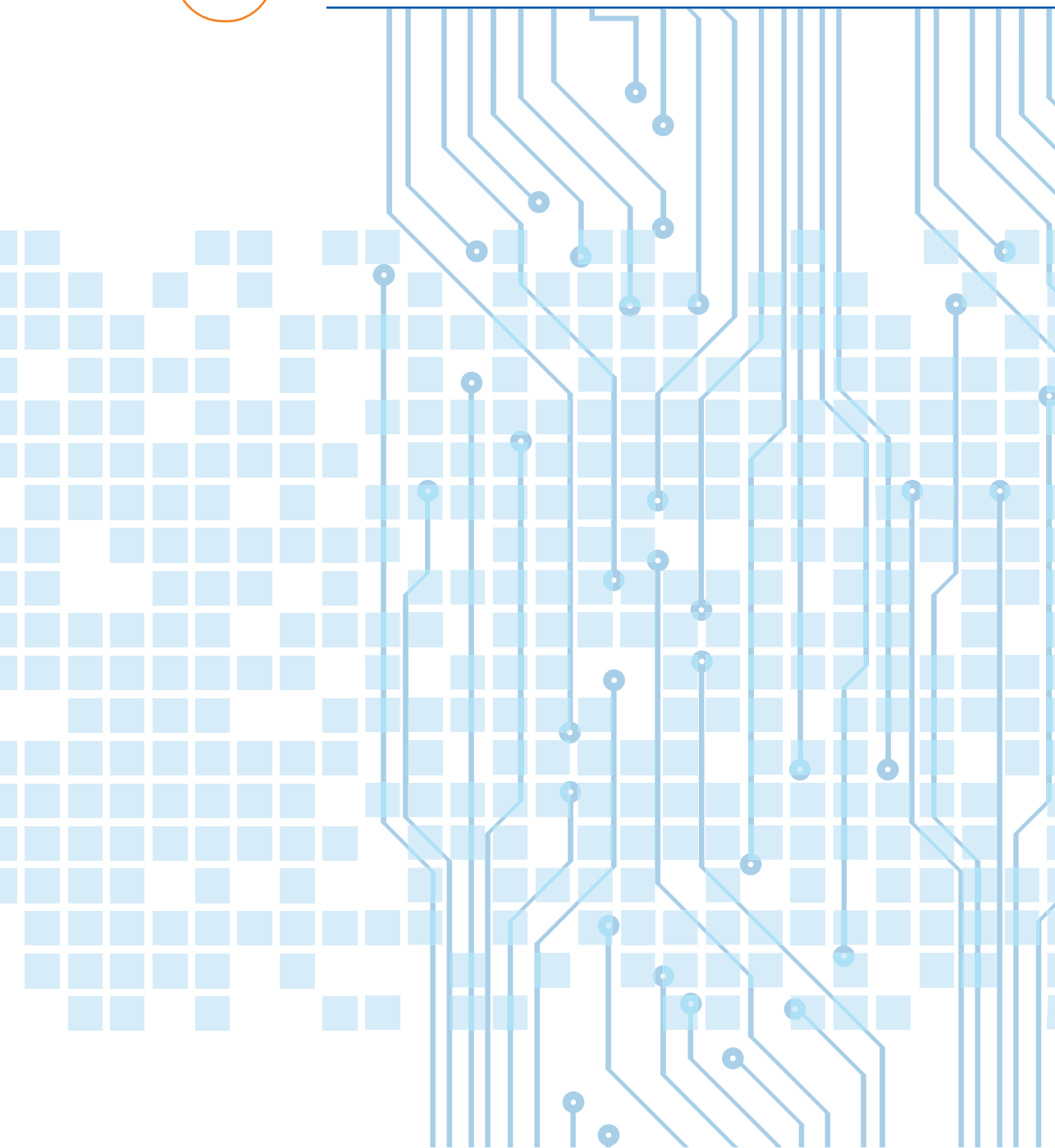
3 LES AUDITS

En 2019, l'AMSN a effectué ou fait réaliser 7 audits, soit dans le cadre des interventions de remédiation d'incidents de sécurité, soit dans le cadre de la prévention ou de démarches d'homologation.

Tous ces audits font l'objet de recommandations afin d'améliorer le niveau de sécurité des systèmes d'information et d'un suivi régulier.

6

COOPERATION



LA COOPÉRATION INTERNATIONALE

Pour être pleinement efficace, une agence comme l'AMSN se doit d'être présente au niveau international afin de tisser des liens privilégiés avec des structures homologues et des partenaires étrangers. L'AMSN prend part chaque année à plusieurs regroupements internationaux qui réunissent la plupart des CERTS dans le monde, et participe à des exercices opérationnels destinés à entraîner les personnels à la gestion et traitement d'incidents cyber

- **DFRWS (Digital Forensics Research Workshop)**

Le DFRWS est une association à but non lucratif qui se consacre à réunir toutes les personnes ayant un intérêt légitime dans l'investigation numérique afin de relever les nouveaux défis dans ce domaine. Le DFRWS organise des conférences numériques dédiées à la criminalistique, aux défis et à la collaboration internationale afin d'orienter la recherche et le développement.

Cet événement comprenait plus de 24 heures de sessions techniques approfondies couvrant les dernières recherches numériques en criminalistique et en sécurité numérique, des démonstrations de nouveaux outils techniques et des ateliers pratiques. A cette occasion, la DFRWS organise un challenge d'investigation numérique autour d'un scénario fictif. Pierre MORLON, en équipe, a terminé à la seconde place sur les 17 participants, confirmant le haut niveau des personnels de l'AMSN.



*Pierre Morlon à la conférence Européenne du DFRWS
24 au 26 avril – Oslo, Kripos (National Criminal Investigation Service)
Norvège.*

- **TF-CSIRT**

L'AMSN est membre « listé » à la TF-CSIRT depuis le 18 décembre 2018, ce qui lui permet d'être présente aux réunions sans toutefois avoir, pour l'heure, de droit de vote. La TF-CSIRT est un groupe de travail pour les CERTs européens.

La TF-CSIRT est rattachée à GÉANT, association technique et scientifique européenne, coordinatrice des projets sur les réseaux et les infrastructures de services connexes au profit de la recherche et de l'éducation, contribuant à la croissance économique et à la compétitivité de l'Europe.



*L'AMSN a participé à la 57ème réunion du TF-CSIRT
24 et 25 mai 2019
Université du Luxembourg, Esch-sur-Alzette.*

- **FIRST** 

Le CERT-MC est, depuis le 22 mai 2018, membre effectif de l'organisation FIRST (Forum of Incident Response and Security Teams). Frédéric FAUTRIER, Directeur adjoint de l'AMSN et Bruno VALENTIN, responsable du CERT-MC ont participé à la 31^{ème} réunion annuelle du FIRST du 16 au 21 juin à Edinbourg.



*Frédéric Fautrier et Bruno Valentin à la 31^{ème} réunion annuelle du FIRST
16 au 21 juin 2019.*

- **NatCSIRT**

En tant que centre national d'expertise, de réponse et de traitement en matière de sécurité et d'attaques numériques, le CERT-MC a participé à la 14^{ème} réunion annuelle du NatCSIRT qui a eu lieu les 21 et 22 juin 2019. Le NatCSIRT regroupe toutes les entités ayant une responsabilité nationale de réponse à incident de sécurité informatique.



*Bruno Valentin et Frédéric Fautrier à la 14^{ème} réunion annuelle du NatCSIRT
21 au 22 juin 2019.*



- **CyberEx2019**

L'AMSN a participé à un exercice international organisé par INCIBE (Institut National Espagnol de la Cybersécurité), l'Organisation des États américains (OEA) et le Centre national pour la protection des infrastructures et de la cybersécurité (CNPIC). La compétition regroupait 80 équipes représentant 24 pays.

Pendant 8 heures, 320 experts en sécurité hautement qualifiés dans le domaine des Technologies de l'Information et de la Communication, ont réalisé un exercice cyber au format CTF (Capture The Flag). Ce type d'exercice permet aux participants d'acquérir de l'expérience dans le domaine de la surveillance des intrusions, ainsi que sur les capacités de réaction à des cyberattaques.

Sur les 80 équipes engagées, l'AMSN s'est classée au 11^{ème} rang.



*L'équipe du CERT-MC pendant l'exercice
11 septembre 2019*

- **ANSSI**



Sur le plan international, l'Agence Monégasque de Sécurité Numérique (AMSN) a de nombreux échanges avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française.



*Visite du Directeur Général de l'ANSSI,
Guillaume POUPARD à l'AMSN – 21 octobre 2019*

Le programme de coopération signé en octobre 2015 entre l'AMSN et l'ANSSI, notamment pour l'échange d'analyses relatives à l'actualité internationale en matière de sécurité des systèmes d'information et aux informations opérationnelles pouvant contribuer au traitement efficace d'incidents liés à la sécurité des systèmes d'information, a été une grande aide pour l'AMSN.

Agence Monégasque de Sécurité Numérique

24 rue du Gabian
MC 98000 Monaco
Tél : +377 98 98 24 93
www.amsn.gouv.mc



Gouvernement Princier
PRINCIPAUTÉ DE MONACO