RAPPORT D'ACTIVITÉ 2021

AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

amsn.gouv.mc

RAPPORT D'ACTIVITÉ

DE L'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE

2021

« Ils ne savaient pas que c'était impossible …
Alors, ils l'ont fait »

EDITO

Je tiens particulièrement à remercier les agents de l'AMSN qui, par leurs compétences, leur engagement et leur agilité, ont permis de réaliser tout ce qui vous est présenté dans ce rapport.

Cette année encore, le travail effectué pour la sécurisation des systèmes d'information de l'État et des Opérateurs d'Importance Vitale a été considérable malgré une année perturbée par la crise sanitaire.

L'année 2021 en Principauté a été riche en attaques plus ou moins discrètes, plus ou moins ciblées, mais toujours plus efficaces et malheureusement non sans conséquences pour les victimes. Toutefois, le travail de veille et d'alerte réalisé par l'AMSN a certainement permis d'éviter un certain nombre d'incidents de sécurité.

Au niveau international, l'année 2021 a été marquée par plusieurs opérations policières et judiciaires majeures, ayant permis de mettre fin à des activités de bandes organisées. La coopération internationale coordonnée par Europol et Eurojust, Interpol et le FBI, a joué un rôle central dans l'identification d'acteurs, car les victimes se trouvaient dans différentes zones géographiques du monde.

Une grande partie de l'année 2021 a été consacrée à l'accompagnement de la transition numérique dans de bonnes conditions de sécurité. En cette période de crise sanitaire, la sécurité numérique était encore d'autant plus indispensable que les services numériques devenaient la ligne de vie pour une partie de l'économie, le fonctionnement de la Principauté et la vie des monégasques et des résidents, notamment avec l'essor rapide du télétravail.

Dans ce contexte, comme vous pourrez le lire dans ce rapport, l'AMSN a continué à compléter le cadre réglementaire et étoffer son dispositif opérationnel, tous deux indispensables au développement de la confiance dans le numérique en Principauté.
La maturité de la Principauté en matière de sécurité numérique, évaluée par l'Union Internationale des Télécommunications (UIT), montrait une forte progression en 2018 comparée à 2016. L'évaluation faite en 2020 et publiée en 2021 laisse apparaître une stagnation.

Ce quatrième rapport d'activité effectue le bilan du travail réalisé sur l'année 2021 par l'AMSN mais aussi par les autres entités engagées dans la sécurité numérique. Il propose des orientations issues de l'évaluation de l'UIT qui permettront d'actualiser la stratégie nationale pour la sécurité du numérique. J'espère qu'il vous permettra d'appréhender le volume, le sens et l'intérêt du travail effectué en matière de sécurité numérique.

Frédéric FAUTRIER
Directeur

LES FAITS MARQUANTS DE 2021

3 mars – Attaques massives sur les messageries Exchange

Des acteurs malveillants, dont les méthodes sont attribuées au groupe d'attaquants chinois nommé HAFNIUM, ont exploité des vulnérabilités sur les serveurs de messagerie Exchange de Microsoft. Ces vulnérabilités ont permis aux attaquants d'accéder aux comptes de messagerie et d'installer des portes dérobées pour prendre le contrôle des systèmes d'information. Les attaques ont commencé en janvier, mais l'activité des attaquants s'est intensifiée dès le 2 mars. 32 entités de la Principauté ont été concernées par cette attaque nécessitant, pour 13 d'entre elles, la mobilisation pendant 3 semaines du CERT-MC et des Prestataires d'Audit de la Sécurité de Systèmes d'Information qualifiés.

10 mars – La signature électronique disponible pour les entreprises

Le Gouvernement Princier propose désormais aux professionnels monégasques un nouveau service de remise de certificats électroniques, en partenariat avec l'AMSN. Communément appelée signature électronique, elle est l'équivalent de la signature manuscrite pour un document dématérialisé. Elle a pour objectif de démontrer qu'un document a été signé par une personne identifiée et qu'il n'a pas été modifié. Elle facilite la transition numérique des entreprises.

7 au 9 juin – L'AMSN participe au CTF organisé par le FIRST

Le Forum of Incident Response and Security Teams (FIRST), association qui regroupe 605 équipes de sécurité de 99 pays dont l'AMSN depuis 2018, organise chaque année un exercice « Capture The Flag » (CTF). Le CTF consiste en une série de challenges techniques pour lesquels les participants doivent trouver une solution (Flag). Chaque drapeau soumis contribue au score de l'équipe. L'AMSN a terminé 14ème sur les 50 équipes engagées.

29 juin – Publication de l'indice mondial de cybersécurité 2020

Depuis son lancement en 2015, l'indice mondial de cybersécurité (GCI) a établi une référence de confiance qui mesure l'engagement des pays en matière de cybersécurité suivant cinq axes : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités, et coopération.

12 août – Un nouveau Directeur à l'AMSN

Après 5 années à la tête de l'Agence, Dominique RIBAN passe le témoin ; Frédéric FAUTRIER qui l'a secondé depuis le 5 juillet 2016, est nommé en qualité de Directeur par l'Ordonnance Souveraine n° 8.730 du 1er juillet 2021.
Un clin d'œil au marin, l'équipe de l'AMSN a remis au Contre-Amiral une tape de bouche sur laquelle est inscrit la devise de l'Agence, empruntée à Mark Twain : « Ils ne savaient pas que c'était impossible, alors ils l'ont fait ».

15 octobre – Partenariat avec Thalès

L'AMSN et Thalès ont signé un partenariat concernant la mise en œuvre et les interactions de technologies de pointe en cybersécurité, afin de renforcer la sécurité numérique du Gouvernement et des différentes institutions, entreprises et Opérateurs d'Importance Vitale (OIV) monégasques. Dans le cadre de ce partenariat, Thales fournit « Cybels Sensor », la sonde de confiance et « Cyber Threat Intelligence », le service d'analyse de cybermenaces qui s'intègrent dans « Cybels Analytics », plateforme Big Data de détection d'attaques innovantes.

18 octobre – Monaco Cyber Security Initiative

A l'occasion de la 21ème édition des Assises de la Sécurité, rendez-vous incontournable des experts de la cybersécurité, Monaco Cyber Security Initiative réunit pour la 4ème fois autour de l'Agence Monégasque de Sécurité Numérique 10 entreprises spécialisées dans la sécurité numérique en Principauté. Les Assises sont une véritable institution qui accompagne tous les acteurs de la cyber depuis 20 ans. A cette occasion, le Ministre d'État, accompagné par le Conseiller de Gouvernement-Ministre de l'Intérieur, a pu échanger avec les représentants des entreprises monégasques qui interviennent dans la cybersécurité.

30 novembre – Nouveau partenariat avec Gatewatcher

L'AMSN se réjouit d'annoncer un nouveau partenariat avec l'éditeur français Gatewatcher. Après 4 années d'exploitation de la gamme de sondes de détection Trackwatch®, l'AMSN signe un nouveau partenariat avec Gatewatcher pour l'évaluation de la plateforme de détection et réponse AIONIQ. Gatewatcher met à disposition de l'AMSN son nouveau produit capable de réaliser une analyse cartographique et comportementale de toutes les cybermenaces pour obtenir une visibilité sur les attaques. AIONIQ combine machine learning, analyses statique et dynamique.

5 décembre – L'AMSN de nouveau cooptée par ses pairs

L'AMSN a été à nouveau cooptée pour 3 ans par ses homologues membres du TF-CSIRT. Le TF-CSIRT est un groupe de travail qui promeut la collaboration et la coordination entre ses 445 équipes de réponse à incident (CSIRT) en Europe et les régions voisines, tout en assurant la liaison avec les organisations pertinentes au niveau mondial et dans d'autres régions.

TF-CSIRT
Trusted Introducer

10 décembre – Exploitation importante de la vulnérabilité log4j

THE APACHE® SOFTWARE FOUNDATION
apache.org

Une vulnérabilité critique dans la librairie log4j de la Fondation de logiciel libre Apache, largement utilisé par les sites web, a été dévoilée le 10 décembre. A quelques jours des fêtes de fin d'année, le nombre de tentatives d'exploitation de cette vulnérabilité a explosé, mettant à mal les équipes informatiques. En Principauté, 44628 tentatives ont été enregistrées sur les systèmes d'information de l'État entre le 10 et le 31 décembre 2021.

27 décembre – Destruction des supports de données numériques

Avec le soutien du Commissaire du Gouvernement près la Société Monégasque d'Assainissement (SMA), l'AMSN a initié un projet de destruction des supports de données numériques en Principauté qu'elle finance à hauteur de 50% des investissements nécessaires.
DataDestruction est une prestation entièrement réalisée sur le territoire monégasque par la SMA, par un personnel dédié et avec une traçabilité garantie. Elle consiste en une destruction physique des clés USB, cartes SSD, disques durs, bandes magnétiques LTO et disques optiques selon la norme DIN 66399. Les particules résultantes, totalement inutilisables, suivent ensuite la filière de recyclage des Déchets d'Équipements Électriques et Électroniques (D3E).

LES CHIFFRES CLÉS DE 2021

L'AMSN

2 nouvelles recrues en 2021.
13 personnes au 31 décembre 2021.
23% de femmes qui ont en moyenne 31 ans.
77% d'hommes qui ont en moyenne 42 ans.
39 ans d'âge moyen.
1,59 millions d'euros de budget pour les moyens de l'AMSN.
4,98 millions d'euros de budget sécurité numérique pour les services exécutifs de l'État.
68 Opérateurs d'Importance Vitale.

LA CYBERSÉCURITÉ

588 événements de sécurité ont fait l'objet d'un suivi avec les entités concernées. ↗+52% vs 2020
29 incidents qualifiés nécessitant des actions approfondies de réponse à incident. ↘-15% vs 2020.
415 serveurs ont exposé des protocoles non sécurisés. ↘-14% vs 2020.
622 serveurs ont exposé aux attaquants des vulnérabilités référencées et exploitables.

RÈGLEMENTATION

1 nouvelle Ordonnance Souveraine.
8 nouveaux Arrêtés Ministériels.

FORMATIONS-INFORMATION-SENSIBILISATION

22 formations en ligne et une en présentiel ont été suivies par les Agents de l'AMSN.
18 sensibilisations à l'accès aux informations classifiées ont été dispensées par l'AMSN.
3 sessions de sensibilisation ont été réalisées aux entreprises de la Principauté.
244 « actualités » sur le cyber espace ont été publiées, afin de sensibiliser et informer les acteurs spécialisés de la Principauté.
52 « Les essentiels de la cyber » ont été adressés 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 évènements mondiaux dans le domaine de la cybersécurité.
22 diffusion d'alertes de sécurité ont été émises.
Ces documents sont destinés à prévenir d'un danger immédiat.
991 diffusion d'avis de sécurité documents faisant état de vulnérabilités et des moyens de s'en prémunir, ont été diffusés afin d'éviter la compromission des systèmes d'information, ↗+21% vs 2020.

LA CYBER CRIMINALITÉ[1]

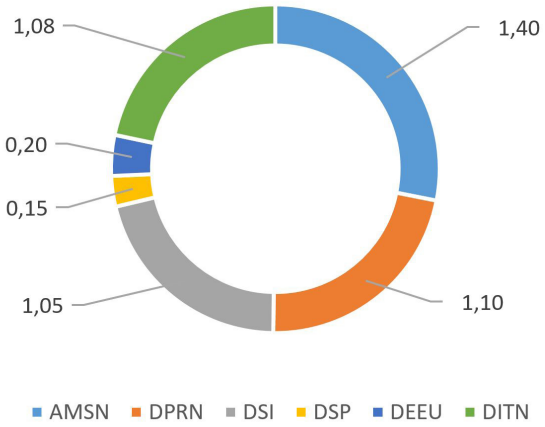
La Direction de la Sûreté Publique contribue à la cybersécurité. Forte d'une unité spécialisée de lutte contre la criminalité technologique, elle a été amenée en 2021 à apporter assistance aux victimes et à intervenir dans le cadre d'instructions de la Justice sur de nombreux dossiers.
3 rançongiciels.
3 intrusions dans des systèmes d'information.
59 escroqueries (tentatives ou commises), usurpations d'identités numériques.
25 hameçonnages.
3 infractions commises sur les réseaux sociaux (usurpation d'identité, harcèlement, diffamation…).
56 assistances techniques aux enquêteurs (extraction de données, analyse et recherches, réquisitions, perquisitions…).

[1] *Chiffres : Unité de lutte contre la criminalité technologique, Division de la police judiciaire*

LE FINANCEMENT DE LA SÉCURITÉ NUMÉRIQUE

La loi n° 1.504 du 23 décembre 2020 portant fixation du budget général primitif de l'exercice 2021, adoptée par le Conseil National dans sa séance du 17 décembre 2020, prévoyait 4,98M€ pour la sécurité numérique à l'article 708.946. Cet article budgétaire, permet de décliner les objectifs stratégiques prioritaires du Gouvernement en matière de sécurité numérique en regroupant les besoins de tous les services exécutifs de l'État ainsi que les participations de l'État dans des opérations de cybersécurité bénéficiant aux entreprises et aux résidents de la Principauté

Article 708 946 : budget 2021 par département/direction en M€



Cet article budgétaire a permis en 2021 les réalisations suivantes :

• L'AMSN a terminé la mise en place de l'Infrastructure de Confiance Nationale pour délivrer des certificats de signature électronique, continué le déploiement de systèmes de détection d'attaques informatiques, mis en service le réseau de sécurité nationale, financé le logiciel Monaco Care Safety pour les internautes de la Principauté.

• La Délégation Interministérielle chargée de la Transition Numérique (DITN) a continué à animer la mise en œuvre des analyses de risques et des audits, prévus par la Politique de Sécurité des Système d'Information de l'État (PSSI-E), pour les nouveaux projets de ses Directions. La Direction des Plateformes et des Ressources Numériques (DPRN) a poursuivi la mise en œuvre du chantier majeur de modernisation et de sécurisation du réseau informatique du Gouvernement. La Direction des Systèmes d'Information (DSI) a renforcé son équipe de sécurité opérationnelle.

• La Direction de la Sûreté Publique (DSP) et le Département de l'Equipement de l'Environnement et de l'Urbanisme (DEEU) ont continué la mise en conformité à la PSSI-E de leurs systèmes d'information.

L'INDICE MONDIAL DE CYBERSÉCURITÉ

Publié tous les deux ans par l'Union Internationale des Télécommunications, agence spécialisée des Nations Unies pour les technologies de l'information et de la communication, l'indice mondial de cybersécurité (GCI) mesure l'engagement des pays en matière de cybersécurité au travers de cinq axes : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération. Cette évaluation, réalisée de façon indépendante par l'UIT, permet à la Principauté d'apprécier régulièrement son niveau de maturité en matière de cybersécurité et contribue à promouvoir de nouvelles actions de développement dans ce domaine.

Les attentes en matière législative couvrent à la fois la cybersécurité, les différents aspects de la cybercriminalité prévus par la convention de Budapest, la protection des informations personnelles et la protection des mineurs sur Internet.

Le positionnement de la Principauté au sein de la communauté internationale

MONACO	2016	2018	2020
SCORE	0,236	0,751	0,725
RANG MONDIAL	102 / 164	43 / 175	69 / 182
RANG EUROPÉEN	38 / 43	26 / 46	36 / 46

Les résultats de l'évaluation 2020

Monaco (Principality of)

Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
72.57	16.00	12.77	12.70	13.75	17.34

Source: ITU Global Cybersecurity Index v4, 2021

Les sujets qui devront être adressés par la Principauté

DES MESURES LÉGISLATIVES

La convention de Budapest est amenée à évoluer au travers d'un deuxième protocole adopté par le Comité des Ministres du Conseil de l'Europe le 17 novembre 2021. Celui-ci prévoit une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaine et pour la coopération directe avec les fournisseurs de services en garantissant la protection des données à caractère personnel. Le texte devrait être ouvert à la signature en mai 2022.

La modernisation du cadre législatif relatif à la protection des données personnelles est un des chantiers nécessaires. En effet, même si la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, permet d'appréhender ce sujet, l'absence d'obligation de notification à l'autorité de protection et à la personne concernée en cas d'incident ou de violation de données a été notée par l'UIT. Ce sujet est abordé par le projet de loi n° 1054 déposé auprès du Conseil National le 20 décembre 2021. Une fois votée, cette loi permettra également d'ouvrir la voie à la reconnaissance par l'Union Européenne de notre signature électronique.

La contrefaçon informatique et l'absence de protection des droits d'auteur de logiciels sont des sujets qui sont pris en compte dans l'évaluation de l'UIT et qui devront donc être adressés dans le calendrier législatif.

DES MESURES TECHNIQUES

- Promouvoir la sensibilisation à la protection des enfants sur Internet : un des axes de progression attendu avec notamment porteur clairement missionné.
- Définir un plan de gestion de crise cyber au niveau national : ce plan devra intégrer aussi bien les préoccupations techniques permettant un retour à un état de sécurité optimal que les aspects stratégiques, qui devront prendre en compte le maintien des activités économiques affectées par la crise.
- Etablir des liens avec ses pairs au niveau régional à date deux organisations européennes coexistent : le CSIRT Network qui regroupe les équipes en charge de la réponse aux incidents de sécurité (CERT) à compétences nationales ou sectorielles des pays membres de l'Union Européenne, et le groupe de travail communautaire européen CSIRT ouvert aux CERT des pays européens et au-delà. Le CERT-MC, CERT de l'AMSN, est référencé auprès du CSIRT mais n'en est pas membre et n'a donc pas toute la reconnaissance nécessaire. Le CERT-MC prendra les mesures nécessaires pour être accrédité auprès du CSIRT en 2022. Dans un second temps, le CERT-MC s'assurera au travers d'audits que le modèle opérationnel utilisé est conforme au modèle SIM-3 communément utilisé par ses pairs. Cette étape lui permettra d'être certifié par le CSIRT et d'en devenir membre à part entière.
- Réaliser régulièrement des exercices de cybersécurité avec les différentes entités en charge de la sécurité numérique en Principauté : l'objectif est de s'assurer de l'existence d'une bonne coordination et des capacités pour travailler ensemble.

DES MESURES ORGANISATIONNELLES

- Revoir régulièrement, au moins tous les 5 ans, la Stratégie Nationale pour la Sécurité Numérique en prenant en considération l'évolution des risques et en y intégrant une feuille de route pour sa mise en œuvre.
- Créer ou désigner une entité chargée de définir une stratégie pour la protection des enfants sur Internet et de superviser au niveau national les initiatives en la matière.

DU RENFORCEMENT DES COMPÉTENCES

Un travail important en matière de formation et de sensibilisation des différentes populations reste à faire : les personnes âgées, les personnels des TPE/PME, le secteur public, la justice, les forces de l'ordre, les enseignants, les élèves.

LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ NUMÉRIQUE BILAN DES RÉALISATIONS DE 2021

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

- La mise en place des mesures de sécurité règlementaires pour les Opérateurs d'Importance Vitale (OIV), débutée en 2018, s'est poursuivie en 2021 et devrait aboutir en 2022.

- Le CERT-MC a traité 29 incidents de sécurité à la suite d'attaques par hameçonnage ou d'exploitations de vulnérabilités des systèmes d'information de l'État et des OIV.
Le traitement de ces incidents a mobilisé 33 jours homme en 2021.

- Au 31 décembre 2021, 6 OIV bénéficient du service de détection des attaques mis en œuvre par l'AMSN et opéré par son entité SOC-MC.

- La protection des établissements, installations ou ouvrages exploités par les OIV est désormais renforcée et fait l'objet d'un plan particulier de protection qui doit être validé par la Direction de la Sûreté Publique, conformément à l'arrêté ministériel n° 2020-902 du 21 décembre 2020. Les OIVs peuvent, afin de délivrer des autorisations d'accès à tout ou partie de leurs établissements, installations ou ouvrages, solliciter la Direction de la Sûreté Publique, laquelle rend alors un avis à la suite d'une enquête administrative.

- 991 avis de sécurité ont été diffusés en 2021 vers les OIV et les services de l'État.
Ce nombre est en augmentation de 21% comparé à 2020. Ces documents font état des vulnérabilités et des moyens de s'en prémunir, afin d'éviter la compromission des systèmes d'information.

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 :

- 32 systèmes d'information de l'État ont fait l'objet d'une démarche d'homologation en 2021 afin de s'assurer de la prise en compte de la sécurité dans leur conception.

- 15 audits ont été effectués par des Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifiés par l'AMSN, afin de vérifier le niveau de sécurité appliqué aux systèmes d'information de l'État.

- L'Infrastructure de Confiance Nationale, qui permet la délivrance de certificats pour les services électroniques (cachet électronique, signature électronique), a été mise en production en mars pour les entreprises et en juin pour les monégasques et résidents ; le processus de qualification a débuté en décembre 2021 et se terminera au premier semestre 2022.

- Monaco Care Safety, service gratuit pour les clients de Monaco Télécom, lancé en juillet 2019, offert par le Gouvernement Princier, qui permet d'obtenir 5 à 10 licences d'antivirus, de contrôle parental pour la navigation sur Internet et de navigation sécurisée sur Internet, compte 1149 clients actifs au 31 décembre 2021. 6162 clients ont souscrit au service mais ne l'ont pas encore activé.

Développer les sensibilisations et les formations initiales et continues :

- Plusieurs actions de sensibilisation ont pu être menées :
  · le 24 mars auprès de l'Association Monégasque des Activités Financières ;
  · le 6 octobre lors d'une conférence-débat organisée par le Monaco Business ;
  · le 7 octobre dans le cadre des ateliers du numérique organisés par le Monaco Economic Board[2] et la Fédération des entreprises de Monaco[3] ;

- Le personnel de l'AMSN a suivi 23 formations spécialisées en présentiel ou à distance, en particulier pour les nouveaux recrutements :
  · 1 stage au CFSSI[4] sur la réponse aux incidents de sécurité ;
  · 4 formations pratiques sur l'investigation post-incident ;
  · 18 formations sur le système de gestion des évènements de sécurité.

Faire de la sécurité du numérique un facteur de compétitivité :

- Pour la quatrième 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 permet aux entreprises monégasques de prendre la place qui leur revient dans le monde de la cybersécurité et de démontrer que la Principauté est aujourd'hui un acteur à part entière dans ce domaine. Les Assises ont réuni 157 entreprises, 120 experts et journalistes, et 1200 invités lors de cette 22ème édition.

- Au 31 décembre 2021, 6 entreprises sont qualifiées « Prestataire d'Audit de la Sécurité des Systèmes d'Information » (PASSI) et 42 auditeurs en sécurité des systèmes d'information ont obtenu leur attestation de compétence pour réaliser des audits en Principauté.

[2] https://www.meb.mc/

[3] https://www.fedem.mc/

[4] Centre de Formation à la Sécurité des Systèmes d'Information de l'Agence Nationale de la Sécurité des Systèmes d'Information

FOCUS
LE SECURITY OPERATIONS CENTER (SOC)

Le Security Operations Center est la première ligne de défense de l'AMSN.

Le SOC effectue une veille opérationnelle en matière de cybersécurité et analyse les alertes qui proviennent des systèmes de détection des cyber menaces, qui sont installés au sein des réseaux informatiques de certains services de l'État et Opérateurs d'Importance Vitale.

Sa création a été validée en octobre 2018 par le Comité Stratégique de la Sécurité du Numérique, institué lui-même par l'Ordonnance Souveraine n° 6.486 du 25 juillet 2017. Il est opérationnel depuis le 18 mars 2020 et ouvert désormais de 07h30 à 21h30 les jours ouvrés.

Au 31 décembre 2021, le SOC de l'AMSN compte 3 ingénieurs et 1 coordinateur. L'équipe est amenée à croître en 2022 pour élargir, dans un premier temps, sa plage horaire d'activité aux week-ends et jours fériés.

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