

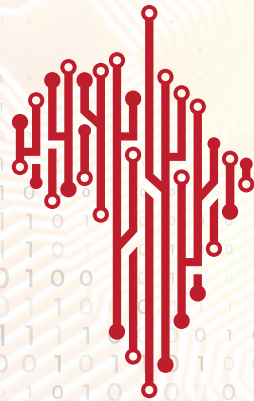
تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Sur Hautes Instructions de Sa Majesté le Roi Mohammed VI, que Dieu L'assiste



ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

Morocco CyberSecurity Week

La cybersécurité au service de la transformation numérique et du développement



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

**AFRICA
CYBERSECURITY
FORUM**

Rabat - Morocco

AGENDA

من 12 إلى 14 أكتوبر
Du 12 au 14 Octobre
2026



FOUR SEASONS
HOTEL
RABAT AT KASR AL BAHR



ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

📍 Avenue Al Melia, Hay Ryad, Rabat 10102
📧 contacts@dgssi.gov.ma

www.dgssi.gov.ma

Partenaires institutionnels :



ANCA CERT
AFRICAN NETWORK OF CYBERSECURITY AUTHORITIES



تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Sur Hautes Instructions de Sa Majesté le Roi Mohammed VI, que Dieu L'assiste

Morocco CyberSecurity Week

La cybersécurité au service de la transformation
numérique et du développement



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

AFRICA
CYBERSECURITY
FORUM

Rabat - Morocco

من 12 إلى 14 أكتوبر

Du 12 au 14 Octobre

2026

JOURNÉE 1

STRATEGIES NATIONALES, GOUVERNANCE ET RESILIENCE CYBER



08H30 – 09H00

Accueil des participants et inscription

09H00 – 09H30

Cérémonie d'Ouverture Officielle

Cérémonie d'ouverture officielle avec les autorités marocaines et représentants internationaux, marquant l'engagement collectif pour la sécurité et la résilience numérique et le lancement des travaux du forum.



09h30 – 10h20

Panel Ministériel

Face aux menaces cyber : quelle résilience pour accompagner les ambitions de la transformation numérique ?

Dans un contexte d'accélération de la digitalisation, ce panel mettra en perspective les ambitions de transformation numérique avec l'intensification des menaces cyber et leur impact sur la confiance numérique et le rythme de mise en œuvre des projets digitaux. Il dressera un état des lieux des efforts engagés ces deux dernières décennies dans le cadre des stratégies nationales de cybersécurité pour protéger les écosystèmes numériques, sécuriser les infrastructures critiques et renforcer la résilience. Les échanges mettront en lumière les principaux axes d'intervention : gouvernance stratégique, cadre juridique et normatif, renforcement des capacités, sensibilisation, coopération public-privé et internationale, ainsi que prévention, détection et réponse aux incidents. Le panel vise à faire émerger des priorités d'action concrètes pour accélérer une transition numérique à la fois sécurisée et durable.



10h20 – 11h00

Panel Stratégique

Stratégies nationales de cybersécurité et gouvernance :
Vers des approches plus pragmatiques et ciblées

Après des années de déploiement, les stratégies nationales de cybersécurité entrent dans une phase de maturation, nourrie par les réalités du terrain, les retours d'expérience et les enseignements tirés des efforts de résilience engagés. Ce panel examinera cette évolution, marquée par une mise en œuvre plus ciblée des priorités stratégiques, dans le prolongement des piliers structurants que sont la gouvernance, le cadre juridique, la résilience, le renforcement des capacités et la coopération.

Les échanges mettront en lumière les zones d'action qui se renforcent aujourd'hui, notamment la constitution d'un vivier national de talents, l'émergence d'un écosystème privé de cybersécurité fort et dynamique, la promotion de la R&D ainsi que le renforcement de la protection des infrastructures critiques et des services essentiels. L'objectif est d'identifier comment ces évolutions, y compris en matière de modèles de gouvernance, peuvent accroître l'impact des politiques de cybersécurité, soutenir la souveraineté et renforcer durablement la résilience.



11H00 – 11H20

Keynote Stratégique

Souveraineté numérique et maîtrise des dépendances technologiques – Enjeux pour les Etats

Keynote explorant l'impact des nouvelles technologies — intelligence artificielle, objets connectés, systèmes autonomes — sur la sécurité numérique. L'intervention montrera comment anticiper les risques liés à ces innovations tout en en tirant pleinement parti. Elle mettra l'accent sur l'importance d'intégrer la sécurité dès la conception des projets numériques, pour bâtir des systèmes robustes, fiables et adaptés aux défis de demain.



11h20 – 12h00

Pause et Visite des Stands d'exposition par les officiels



12H00 – 12H20

Keynote Stratégique

L'héritage de Stuxnet – Comment un incident a redéfini la gouvernance de la cybersécurité industrielle ?

Cette Keynote revient sur l'incident Stuxnet à travers le regard de l'intervenant, qui a directement pris part à son analyse. Elle examinera comment cet événement fondateur a transformé durablement la manière dont les États et les opérateurs critiques conçoivent, gouvernent et protègent leurs environnements industriels. L'intervention mettra en lumière les évolutions majeures induites par Stuxnet en matière de convergence IT/OT, de modèles de gouvernance et de culture de la résilience, et leur résonance avec les enjeux actuels de transformation numérique sécurisée.



12H20 – 13H00

Panel

Digitalisation par le cloud : Quelles garanties pour une transformation de confiance et sécurisée ?

Le recours croissant au cloud redéfinit les modèles de transformation numérique, mais impose également de nouveaux arbitrages en matière de cybersécurité, de souveraineté numérique et de résilience opérationnelle. Cette intervention examinera comment bâtir une approche équilibrée permettant de tirer pleinement parti du cloud sans compromettre la sécurité des données, des services et des infrastructures critiques. Les discussions mettront en lumière les enjeux liés à la gouvernance, à la conformité, à la gestion des risques, à la sécurisation des environnements hybrides et multicloud, ainsi qu'au partage des responsabilités entre clients et fournisseurs. Le panel visera à dégager une vision claire et des leviers d'action concrets pour faire du cloud un accélérateur de digitalisation fondé sur la confiance et la maîtrise des risques.



13H00 – 14H20

Déjeuner Officiel & Networking



14H20 – 14H40

Panel

Retours d'expérience cyber – Tirer les leçons des incidents pour mieux se préparer.

À travers l'analyse des cyberattaques survenues dernièrement : attaques DDoS, rançongiciels et fuites de données. Ce panel mettra en lumière les enseignements clés issus de la gestion de crises réelles. Les échanges permettront de revenir sur les impacts opérationnels, financiers, réputationnels et réglementaires de ces incidents sur les entités touchées.

Ils mettront également en avant les bonnes pratiques en matière de préparation, de détection, de réponse à incident, de communication de crise et de continuité d'activité. L'objectif est de transformer l'expérience des incidents passés en leviers pour renforcer l'anticipation mais aussi la résilience et la maturité cyber des entités.



14H40 – 15H20

Panel

Au-delà de la résilience : pourquoi la lutte contre la cybercriminalité est indispensable à la cybersécurité ?

Ce panel mettra en perspective les efforts internationaux visant à consolider la coopération judiciaire, policière et technique pour mieux poursuivre les auteurs de cyber-infractions et soutenir l'efficacité globale des politiques de cybersécurité.

Les discussions porteront également sur la nouvelle convention internationale de lutte contre la cybercriminalité, ses apports potentiels et les attentes suscitées par une adoption large et une mise en œuvre effective à l'échelle internationale.

Le panel vise à faire émerger une vision intégrée où prévention, résilience, attribution, poursuites et coopération internationale se renforcent mutuellement.



15H20 – 15H30

Synthèse de la journée

Les enseignements clés pour la résilience cyber nationale.

Cette session de clôture proposera une synthèse des principaux enseignements et recommandations issus des panels et Keynote de la journée. Elle mettra en lumière les convergences identifiées en matière de gouvernance, de résilience et de transformation numérique sécurisée, avant d'ouvrir les perspectives sur la dimension continentale qui sera abordée lors du Jour 2.



15H30 – 16H15

Pause-café, Networking & Visite des Stands d'Exposition

JOURNÉE 2

AFRICA CYBER SECURITY FORUM



09H00 – 09H20

Keynote d'ouverture

De la souveraineté continentale à la coopération internationale

Cette Keynote fait le pont entre les ambitions continentales et les réalités souveraines des États. Elle explore comment les stratégies et cadres réglementaires nationaux s'articulent avec les standards globaux et les partenariats internationaux. L'intervention mettra en lumière l'importance d'une gouvernance robuste et de la diplomatie cybernétique pour contrer les menaces transfrontalières et bâtir des écosystèmes de confiance.



09H20 – 10H00

Panel : Cyberdiplomatie

Quelles opportunités pour l'Afrique dans le nouveau mécanisme permanent de l'ONU ?

Avec la mise en place, à compter de cette année, d'un nouveau mécanisme permanent au sein des Nations Unies dédié à la sécurité du numérique et à son usage responsable, ce panel analysera les opportunités qu'il ouvre pour l'Afrique en matière d'influence, de coopération et de renforcement des capacités. Les échanges porteront sur la manière dont les pays africains peuvent tirer pleinement profit de ce cadre pour faire entendre leurs priorités, consolider leurs positions communes et mieux articuler diplomatie numérique, cybersécurité et développement.

Le panel mettra également en lumière les acquis sur lesquels le continent peut capitaliser : montée en compétence, dynamiques régionales, cadres de coopération, initiatives de confiance numérique et efforts de résilience, afin d'aborder les prochaines étapes avec davantage de cohérence et d'ambition.



10H00 – 10H20

Keynote

Construire des SOC et CERT performants en Afrique

Face à l'augmentation des cybermenaces, les Centres Opérationnels de Sécurité (SOC) et les équipes de Réponse aux Incidents de Sécurité Informatique (CERT/CSIRT) constituent aujourd'hui les piliers essentiels de la cyber-résilience des pays et des organisations. Cette keynote explorera les facteurs clés de succès pour concevoir, déployer et faire évoluer des SOC et CERT performants dans le contexte africain. Elle abordera les enjeux liés à la gouvernance, au financement, au développement des compétences, à l'intégration des technologies de détection et de réponse avancées, ainsi qu'à la coopération entre acteurs nationaux, régionaux et internationaux. L'intervenant partagera également des retours d'expérience et les bonnes pratiques en la matière.



10H20 – 11H00

Panel

L'Afrique à l'ère de la cybersécurité mondiale.

Construire un marché numérique souverain, prospère et attractif

Ce panel analysera les opportunités économiques qu'offre à l'Afrique la croissance rapide du marché mondial de la cybersécurité et de la confiance numérique. Les échanges porteront sur les moyens de développer un écosystème africain de cybersécurité compétitif, capable de stimuler l'innovation, favoriser l'émergence de startups spécialisées, soutenir le développement d'entreprises locales de cybersécurité, attirer les investissements et créer des emplois à forte valeur ajoutée. Le panel mettra également en lumière le rôle des cadres de coopération régionaux, de l'intégration numérique africaine et des initiatives de souveraineté numérique dans la construction d'un marché numérique africain prospère, attractif et créateur de valeur pour le continent.



11H00 – 11H30

Pause-café et Networking



11H30 – 11H50

Keynote

Le secteur financier en Afrique à l'épreuve du cybercrime

Cette keynote analysera l'évolution des menaces cyber pesant sur l'écosystème financier africain, des fraudes numériques aux attaques par rançongiciel, en passant par les compromissions de systèmes de paiement, les campagnes d'hameçonnage et les risques liés aux chaînes d'approvisionnement numériques. Elle mettra en lumière les défis auxquels font face les banques, compagnies d'assurance, opérateurs de paiement et fintechs pour sécuriser leurs opérations tout en maintenant l'innovation et la confiance des clients. À travers des exemples concrets et des retours d'expérience, cette intervention présentera les stratégies permettant de renforcer la cyber-résilience du secteur financier, d'améliorer la détection et la réponse aux incidents, et de développer une approche collaborative entre les acteurs.



11H50 – 12H30

Panel

IIV industrielles en Afrique – Quand les systèmes legacy rencontrent les menaces modernes

Cette session présente un état des lieux des environnements OT/ICS sur le continent, en abordant les thématiques des systèmes nécessitant des mises à jour, de la convergence IT/OT et des partenariats technologiques internationaux. L'intervention s'appuiera sur deux à trois cas concrets dans les secteurs de l'énergie, de l'eau et des transports. Elle examinera également les enjeux liés au développement des compétences locales pour accompagner la sécurisation de ces environnements critiques à l'horizon 2030.



12H30 – 12H50

Keynote

Cybersécurité et technologies émergentes : Anticiper les ruptures pour sécuriser l'avenir en Afrique

Cette keynote examinera l'impact des technologies émergentes sur le paysage de la cybersécurité et analysera les nouvelles formes de menaces qu'elles engendrent, qu'il s'agisse de cyberattaques assistées par l'intelligence artificielle, de la sécurisation des environnements connectés, de la protection des données dans les architectures cloud ou encore des enjeux liés à la cryptographie post-quantique. À travers une approche prospective, cette intervention mettra en lumière les ruptures technologiques qui façonneront la cybersécurité de demain et présentera les stratégies permettant aux États, aux entreprises et aux opérateurs d'infrastructures critiques de développer une posture de sécurité agile, résiliente et adaptée aux transformations numériques en cours.



12H50 – 14H00

Déjeuner Officiel & Networking



14H00 – 14H40

Panel

Développer le capital humain cyber : Bâtir les compétences pour sécuriser l'Afrique numérique

Ce panel abordera les enjeux liés à l'ensemble du cycle de vie des talents cyber : de l'identification et de la formation des jeunes professionnels jusqu'à la création de parcours de carrière attractifs, de mécanismes de reconnaissance et d'opportunités d'évolution permettant de limiter la fuite des compétences. Les intervenants partageront leurs expériences sur les politiques et initiatives visant à renforcer l'attractivité des métiers de la cybersécurité, à développer des centres d'excellence et à créer des environnements professionnels favorisant l'engagement et la rétention des experts. Les échanges mettront également en lumière le rôle des partenariats entre gouvernements, universités et entreprises dans ce domaine.



14H40 – 15H20

Panel

ZLECAf et cybersécurité : Bâtir une infrastructure de confiance pour sécuriser le commerce intra-africain

La Zone de libre-échange continentale africaine (ZLECAf) ambitionne de transformer en profondeur les dynamiques économiques du continent en facilitant la circulation des biens, des services et des investissements entre les États africains. Cette intégration repose sur une intensification des échanges transfrontaliers, de plus en plus appuyés par des systèmes numériques pour la logistique, les douanes, les paiements, la traçabilité et la gestion commerciale. Ce panel examinera comment la cybersécurité peut soutenir concrètement l'opérationnalisation de la ZLECAf en garantissant la confiance entre les acteurs économiques et institutionnels. Il mettra en lumière les mécanismes nécessaires pour sécuriser les échanges transfrontaliers, harmoniser les pratiques de sécurité, renforcer la coopération entre autorités compétentes et développer des capacités communes de prévention et de réponse aux incidents.



15H20 – 15H30

Synthèse de la journée

15H30 – 16H30

Pause-café, Networking & Visite des Stands d'Exposition

JOURNÉE 3

NEXUS CYBERSECURITE ET ECONOMIE



09H00 – 09H20

Mot d'ouverture

Cette session d'ouverture fait la synthèse des enjeux de souveraineté et de coopération abordés les jours précédents, pour les transposer sous l'angle de la performance économique. Elle présentera les objectifs de la journée : démontrer comment la cybersécurité, loin d'être une simple contrainte, constitue un levier essentiel de confiance, d'innovation et de croissance durable.



09H20 – 09H40

Keynote

L'économie du cybercrime

Cette Keynote dressera un état des lieux chiffré de l'économie souterraine du cybercrime à l'échelle mondiale et africaine. Elle analysera les modèles économiques des cybercriminels, les coûts directs et indirects pour les entreprises et les États, ainsi que les mécanismes de blanchiment et de monétisation des données volées. L'intervention mettra en lumière l'urgence de traiter la cybercriminalité non plus comme un problème technique, mais comme un enjeu économique majeur nécessitant des réponses coordonnées à l'échelle internationale.



09H40 – 10H20

Panel

Financer la cyber-résilience – Du coût perçu à l'investissement stratégique

Ce panel explorera les enjeux liés au financement de la sécurité numérique. Il détaillera les mécanismes de financement mobilisables (budgets publics, investissements privés, fonds dédiés, partenariats internationaux) et démontrera, à travers des études de cas, comment les secteurs public et privé transforment la cybersécurité en avantage compétitif, optimisent le retour sur investissement (ROI) et renforcent la valorisation de leurs actifs numériques. Les échanges viseront à dégager des leviers opérationnels pour une allocation des ressources alignée sur la performance globale de l'organisation.



10H20 – 11H00

Panel

Le marché de la cybersécurité – Moteur de croissance et d'innovation.

Ce panel proposera une analyse stratégique du marché de la cybersécurité en tant que vecteur de création de valeur. Il mettra en lumière les nouveaux modèles économiques, les dynamiques de l'écosystème des startups et les opportunités d'investissement prioritaires. L'objectif est de partager une vision claire des perspectives de développement du secteur et de son rôle dans la transformation numérique des entreprises.



11H00 – 11H30

Pause-café et Networking



11H30 – 11H50

Keynote

Gestion des risques cyber & Assurances

Cette Keynote explorera l'émergence du marché de l'assurance cyber en Afrique et son rôle dans la gestion des risques numériques. Elle analysera les modèles d'évaluation des risques, les critères de souscription, et les mécanismes de transfert de risques. L'intervention mettra en lumière comment l'assurance cyber peut devenir un levier de maturité pour les entreprises africaines, en les incitant à renforcer leur résilience et à adopter les meilleures pratiques de sécurité.



11H50 – 12H30

Panel stratégique

Partenariats public-privé – Co-innover pour une résilience économique partagée

Ce panel analysera le rôle des partenariats public-privé (PPP) comme accélérateurs de l'innovation et de la performance. Il présentera les cadres de coopération et les mécanismes de partage de la valeur et de l'information, essentiels pour anticiper les menaces. Les panélistes proposeront des pistes concrètes pour bâtir des alliances durables, capables de soutenir la compétitivité des entreprises dans un environnement numérique en mutation.



12H30 – 12H45

Mot de Clôture

Engagements pour un avenir numérique prospère et sécurisé

Synthèse des travaux de la journée et appel à l'action. Cette intervention finale réaffirmera l'engagement des parties prenantes à faire de la cybersécurité un pilier incontournable du développement économique et de la transformation numérique durable.



12H45 – 14H00

Cocktail déjeunatoire & Networking

تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Sur Hautes Instructions de Sa Majesté le Roi Mohammed VI, que Dieu L'assiste

Morocco CyberSecurity Week

La cybersécurité au service de la transformation
numérique et du développement



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

AFRICA
CYBERSECURITY
FORUM

Rabat - Morocco

من 12 إلى 14 أكتوبر

Du 12 au 14 Octobre

2026

www.dgssi.gov.ma



القمة الإفريقية
للأمن السيبراني
الرباط - المغرب
AFRICA
CYBERSECURITY
FORUM
Rabat - Morocco

ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

📍 Avenue Al Melia, Hay Ryad, Rabat 10102
✉ contacts@dgssi.gov.ma

