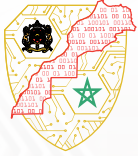


تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Under the High Instructions of His Majesty King Mohammed VI, may God Assist Him

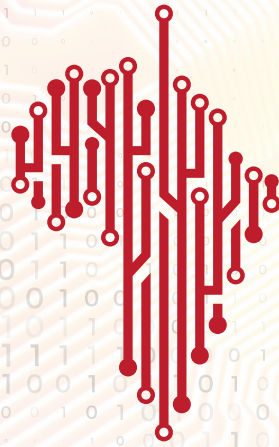


KINGDOM OF MOROCCO
GENERAL DIRECTORATE OF
INFORMATION SYSTEMS SECURITY

DGSSI

Morocco CyberSecurity Week

CyberSecurity at the service of digital transformation and development



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

AFRICA
CYBERSECURITY
FORUM

Rabat - Morocco

AGENDA

من 12 إلى 14 أكتوبر
October, 12th to 14th
2026



FOUR SEASONS
HOTEL
RABAT AT KASR AL BAHR



KINGDOM OF MOROCCO
GENERAL DIRECTORATE OF
INFORMATION SYSTEMS SECURITY

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

www.dgssi.gov.ma

Institutional partners :



ANCA CERT
AFRICAN NETWORK OF CYBERSECURITY AUTHORITIES



تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Under the High Instructions of His Majesty King Mohammed VI, may God Assist Him

Morocco CyberSecurity Week

CyberSecurity at the service of digital transformation and development



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

AFRICA
CYBERSECURITY
FORUM

Rabat - Morocco

من 12 إلى 14 أكتوبر

October, 12th to 14th

2026

DAY 1

NATIONAL STRATEGIES, GOVERNANCE AND CYBER RESILIENCE



08H30 – 09H00 AM

Welcome and Registration

09H00 – 09H30 AM

Official Opening Ceremony

Official opening ceremony with Moroccan authorities and international representatives, marking the collective commitment to security and digital resilience and the launch of the forum's work.



09h30 – 10h20 AM

Ministerial Panel

Facing Cyber Threats :

What resilience to support digital transformation ambitions ?

In a context of accelerating digitalization, this panel will put into perspective the ambitions of digital transformation with the intensification of cyber threats and their impact on digital trust and the pace of digital project implementation. It will take stock of efforts undertaken over the past two decades under national cybersecurity strategies to protect digital ecosystems, secure critical infrastructure, and strengthen resilience. Discussions will highlight key areas of intervention: strategic governance, legal and regulatory framework, capacity building, awareness, public-private and international cooperation, as well as prevention, detection, and incident response. The panel aims to identify concrete action priorities to accelerate a secure and sustainable digital transition.



10h20 – 11h00 AM

Strategic Panel

National Cybersecurity strategies and governance :

Toward more pragmatic and targeted approaches

After years of deployment, national cybersecurity strategies are entering a maturation phase, informed by field realities, lessons learned, and insights gained from resilience efforts. This panel will examine this evolution, marked by more targeted implementation of strategic priorities, building on the structural pillars of governance, legal framework, resilience, capacity building, and cooperation. Discussions will highlight areas of action that are strengthening today, including building a national talent pool, the emergence of a strong and dynamic private cybersecurity ecosystem, promotion of R&D, and strengthening the protection of critical infrastructure and essential services. The objective is to identify how these developments, including in governance models, can increase the impact of cybersecurity policies, support sovereignty, and sustainably strengthen resilience.



11H00 – 11H20 AM

Strategic Keynote

Digital sovereignty and control of technological dependencies – Challenges for States

Keynote exploring the impact of new technologies—artificial intelligence, connected objects, autonomous systems—on digital security. The presentation will show how to anticipate risks related to these innovations while fully leveraging their benefits. It will emphasize the importance of integrating security from the design phase of digital projects to build robust, reliable systems adapted to tomorrow's challenges.



11h20 – 12h00 PM

Break and Exhibition Booth visits by Officials



12H00 – 12H20 PM

Strategic Keynote

The Stuxnet Legacy.

This Keynote revisits the Stuxnet incident through the speaker's perspective, having directly participated in its analysis. It will examine how this foundational event durably transformed the way States and critical operators design, govern, and protect their industrial environments. The presentation will highlight major developments induced by Stuxnet in terms of IT/OT convergence, governance models, and resilience culture, and their resonance with current challenges of secure digital transformation.



12H20 – 01H00 PM

Panel

Cloud-Driven digitalization: What guarantees for a trusted and secure transformation?

The growing use of cloud is redefining digital transformation models, but also imposes new trade-offs in terms of cybersecurity, digital sovereignty, and operational resilience. This session will examine how to build a balanced approach that fully leverages the cloud without compromising the security of data, services, and critical infrastructure. Discussions will highlight issues related to governance, compliance, risk management, securing hybrid and multicloud environments, and sharing responsibilities between clients and providers. The panel aims to develop a clear vision and concrete levers for action to make cloud an accelerator of digitalization based on trust and risk control.



01H00 – 02H20 PM

Official Lunch & Networking



02H20 – 02H40 PM

Panel

Cyber lessons learned – Drawing insights from incidents to better prepare

Through the analysis of recent cyberattacks: DDoS attacks, ransomware, and data breaches, this panel will highlight key lessons learned from real crisis management. Discussions will review the operational, financial, reputational, and regulatory impacts of these incidents on affected entities. They will also showcase best practices in preparation, detection, incident response, crisis communication, and business continuity. The objective is to transform experience from past incidents into levers to strengthen anticipation, resilience, and cyber maturity of entities.



02H40 – 03H20 PM

Panel

Beyond resilience: Why fighting cybercrime is essential to Cybersecurity ?

This panel will put into perspective international efforts aimed at strengthening judicial, police, and technical cooperation to better prosecute perpetrators of cyber offenses and support the overall effectiveness of cybersecurity policies. Discussions will also focus on the new international convention on combating cybercrime, its potential contributions, and expectations raised by broad adoption and effective implementation at the international level. The panel aims to develop an integrated vision where prevention, resilience, attribution, prosecution, and international cooperation mutually reinforce each other.



03H20 – 03H30 PM

Day Summary

Key lessons for national cyber resilience

This closing session will provide a summary of the main lessons and recommendations from the day's panels and Keynote. It will highlight convergences identified in terms of governance, resilience, and secure digital transformation, before opening perspectives on the continental dimension that will be addressed on Day 2.



03H30 – 04H15 PM

Coffee Break, Networking & Exhibition Booth visits

DAY 2

AFRICA CYBER SECURITY FORUM



09H00 – 09H20 AM

Opening Keynote

From continental sovereignty to international cooperation

This Keynote bridges continental ambitions and the sovereign realities of States. It explores how national strategies and regulatory frameworks align with global standards and international partnerships. The presentation will highlight the importance of robust governance and cyberdiplomacy to counter cross-border threats and build trust ecosystems.



09H20 – 10H00 AM

Panel : Cyberdiplomacy

What opportunities for Africa in the new UN permanent mechanism ?

With the establishment, starting this year, of a new permanent mechanism within the United Nations dedicated to digital security and its responsible use, this panel will analyze the opportunities it opens for Africa in terms of influence, cooperation, and capacity building. Discussions will focus on how African countries can fully leverage this framework to make their priorities heard, consolidate their common positions, and better articulate digital diplomacy, cybersecurity, and development. The panel will also highlight the achievements on which the continent can capitalize: skills development, regional dynamics, cooperation frameworks, digital trust initiatives, and resilience efforts, to approach next steps with greater coherence and ambition.



10H00 – 10H20 AM

Keynote

Building high-performance SOC's and CERT's in Africa

Faced with the increase in cyber threats, Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CERT/CSIRT) are today essential pillars of cyber resilience for countries and organizations. This keynote will explore the key success factors for designing, deploying, and evolving high-performance SOC's and CERT's in the African context. It will address issues related to governance, financing, skills development, integration of advanced detection and response technologies, and cooperation between national, regional, and international actors. The speaker will also share lessons learned and best practices in this area.



10H20 – 11H00 AM

Panel

Africa in the era of global Cybersecurity

Building a sovereign, prosperous, and attractive digital market

This panel will analyze the economic opportunities that the rapid growth of the global cybersecurity and digital trust market offers to Africa. Discussions will focus on ways to develop a competitive African cybersecurity ecosystem capable of stimulating innovation, fostering the emergence of specialized startups, supporting the development of local cybersecurity companies, attracting investment, and creating high value-added jobs. The panel will also highlight the role of regional cooperation frameworks, African digital integration, and digital sovereignty initiatives in building a prosperous, attractive African digital market that creates value for the continent.



11H00 – 11H30 AM

Coffee Break & Networking



11H30 – 11H50 AM

Keynote

Africa's financial sector tested by cybercrime

This keynote will analyze the evolution of cyber threats weighing on the African financial ecosystem, from digital fraud to ransomware attacks, including payment system compromises, phishing campaigns, and risks related to digital supply chains. It will highlight the challenges faced by banks, insurance companies, payment operators, and fintechs in securing their operations while maintaining innovation and customer trust. Through concrete examples and lessons learned, this presentation will outline strategies to strengthen the cyber resilience of the financial sector, improve incident detection and response, and develop a collaborative approach among actors.



11H50 – 12H30 PM

Panel

Critical infrastructure in Africa – When legacy systems meet modern threats

This session presents an overview of OT/ICS environments on the continent, addressing themes of systems requiring updates, IT/OT convergence, and international technological partnerships. The presentation will draw on two to three concrete cases in the energy, water, and transport sectors. It will also examine issues related to developing local skills to support the securing of these critical environments by 2030.



12H30 – 12H50 PM

Keynote

Cybersecurity and emerging technologies: Anticipating disruptions to secure Africa's future

This keynote will examine the impact of emerging technologies on the cybersecurity landscape and analyze the new forms of threats they generate, whether AI-assisted cyberattacks, securing connected environments, data protection in cloud architectures, or issues related to post-quantum cryptography. Through a forward-looking approach, this presentation will highlight the technological disruptions that will shape tomorrow's cybersecurity and present strategies enabling States, companies, and critical infrastructure operators to develop an agile, resilient security posture adapted to ongoing digital transformations.



12H50 – 02H00 PM

Official Lunch & Networking



02H00 – 02H40 PM

Panel

Developing cyber human capital: Building skills to secure digital Africa

This panel will address issues related to the entire lifecycle of cyber talent: from identifying and training young professionals to creating attractive career paths, recognition mechanisms, and advancement opportunities to limit brain drain. Speakers will share their experiences on policies and initiatives aimed at strengthening the attractiveness of cybersecurity professions, developing centers of excellence, and creating professional environments that foster engagement and retention of experts. Discussions will also highlight the role of partnerships between governments, universities, and companies in this area.



02H40 – 03H20 PM

Panel

AfCFTA and Cybersecurity: Building a trust infrastructure to secure intra-african trade

The African Continental Free Trade Area (AfCFTA) aims to profoundly transform the continent's economic dynamics by facilitating the circulation of goods, services, and investments between African States. This integration relies on intensifying cross-border exchanges, increasingly supported by digital systems for logistics, customs, payments, traceability, and commercial management. This panel will examine how cybersecurity can concretely support the operationalization of AfCFTA by ensuring trust among economic and institutional actors. It will highlight the mechanisms needed to secure cross-border exchanges, harmonize security practices, strengthen cooperation between competent authorities, and develop common prevention and incident response capabilities.



03H20 – 03H30 PM

Day Summary

03H30 – 04H30 PM

Coffee Break, Networking & Exhibition Booth visits

DAY 3

NEXUS CYBERSECURITY AND ECONOMY



09H00 – 09H20 AM

Opening Remarks

This opening session synthesizes the sovereignty and cooperation issues addressed in previous days, transposing them from the angle of economic performance. It will present the day's objectives: demonstrating how cybersecurity, far from being a simple constraint, constitutes an essential lever for trust, innovation, and sustainable growth.



09H20 – 09H40 AM

Keynote

The Economics of Cybercrime

This Keynote will provide a quantified overview of the underground economy of cybercrime at the global and African levels. It will analyze the economic models of cybercriminals, the direct and indirect costs for businesses and States, as well as money laundering mechanisms and monetization of stolen data. The presentation will highlight the urgency of treating cybercrime no longer as a technical problem, but as a major economic issue requiring coordinated responses at the international level.



09H40 – 10H20 AM

Panel

Financing cyber resilience – From perceived cost to strategic investment

This panel will explore issues related to financing digital security. It will detail mobilizable financing mechanisms (public budgets, private investments, dedicated funds, international partnerships) and demonstrate, through case studies, how the public and private sectors transform cybersecurity into a competitive advantage, optimize return on investment (ROI), and strengthen the valuation of their digital assets. Discussions will aim to identify operational levers for resource allocation aligned with the overall performance of the organization.



10H20 – 11H00 AM

Panel

The Cybersecurity market – Driver of growth and innovation

This panel will propose a strategic analysis of the cybersecurity market as a value creation vector. It will highlight new economic models, dynamics of the startup ecosystem, and priority investment opportunities. The objective is to share a clear vision of the sector's development prospects and its role in the digital transformation of companies.



11H00 – 11H30 AM

Coffee Break & Networking



11H30 – 11H50 AM

Keynote

Cyber Risk Management & Insurance

This Keynote will explore the emergence of the cyber insurance market in Africa and its role in digital risk management. It will analyze risk assessment models, underwriting criteria, and risk transfer mechanisms. The presentation will highlight how cyber insurance can become a maturity lever for African companies, encouraging them to strengthen their resilience and adopt best security practices.



11H50 – 12H30 PM

Strategic Panel

Public-Private partnerships – Co-innovating for shared economic resilience

This panel will analyze the role of public-private partnerships (PPPs) as accelerators of innovation and performance. It will present cooperation frameworks and mechanisms for sharing value and information, essential for anticipating threats. Panelists will propose concrete paths to build sustainable alliances capable of supporting company competitiveness in a changing digital environment.



12H30 – 12H45 PM

Closing Remarks

Commitments for a prosperous and secure digital future

Summary of the day's work and call to action. This final intervention will reaffirm stakeholders' commitment to making cybersecurity an essential pillar of economic development and sustainable digital transformation.



12H45 – 02H00 PM

Lunch Cocktail & Networking

تحت التعليمات السامية لصاحب الجلالة الملك محمد السادس نصره الله
Under the High Instructions of His Majesty King Mohammed VI, may God Assist Him

Morocco CyberSecurity Week

CyberSecurity at the service of digital transformation and development



القمة الإفريقية
للأمن السيبراني

الرباط - المغرب

AFRICA
CYBERSECURITY
FORUM

Rabat - Morocco

من 12 إلى 14 أكتوبر

October, 12th to 14th

2026

www.dgssi.gov.ma



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

**KINGDOM OF MOROCCO
GENERAL DIRECTORATE OF
INFORMATION SYSTEMS SECURITY**

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

