ITU and Cybersecurity

Responding to Cybersecurity incidents and the Global Cybersecurity Index

Pablo Palacios
Programme Officer
ITU Area Office located in Chile
International Telecommunications Union

About ITU

ITU is the United Nations **specialized agency for information and communication technologies** (ICTs)

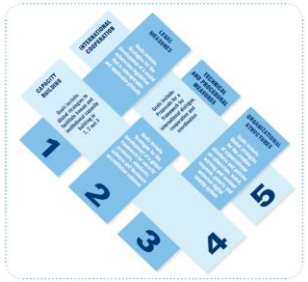
Founded in Paris in 1865 as the International Telegraph Union

More than 150 years of experience and innovation

ITU Mandate on Cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - "**Building Confidence and Security in the use of ICTs**"

world summit on the information society
Geneva 2003 - Tunis 2005



2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

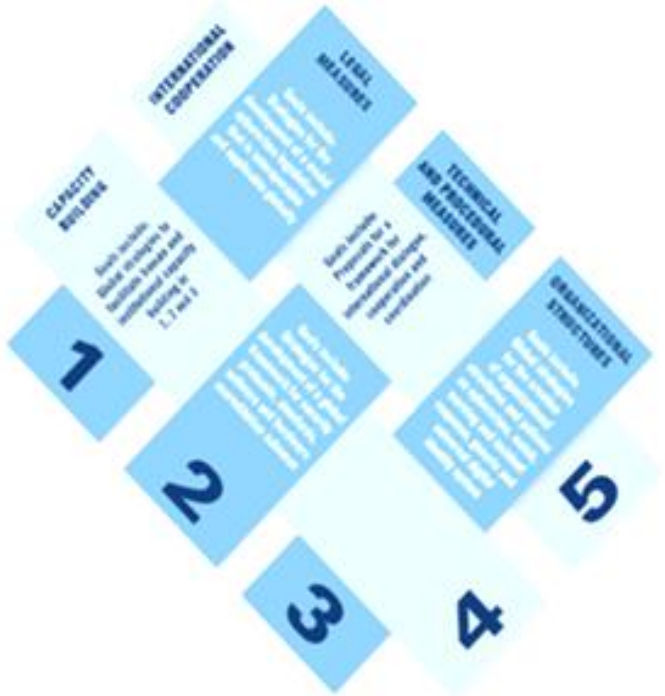
GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

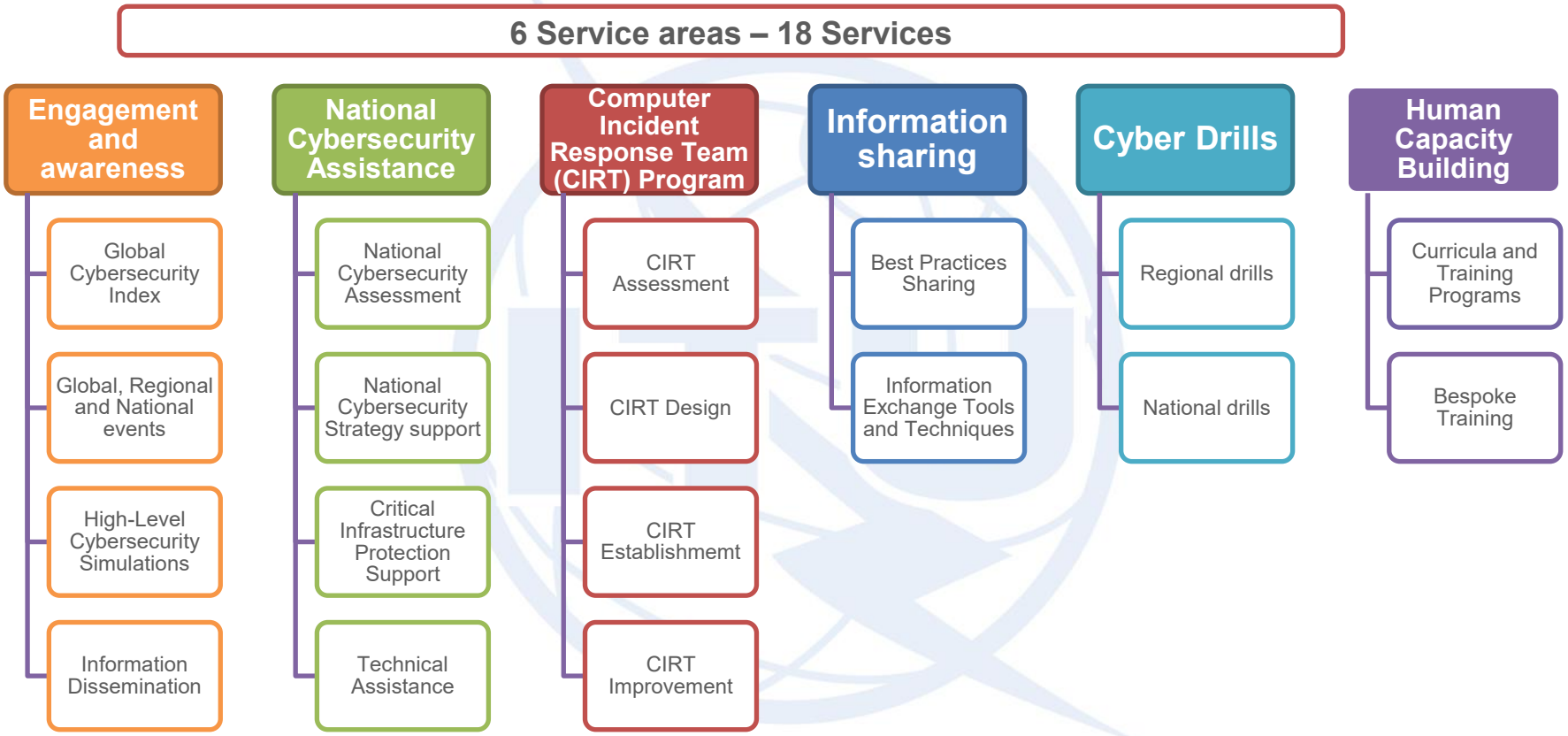
Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
  1. Legal Measures
  2. Technical and Procedural Measures
  3. Organizational Structure
  4. Capacity Building
  5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.



BDT Cybersecurity Program



National CIRTs
The First Line of Cyber-Response

Responsible for:

- Coordinating incident response
- Dissemination of early warnings and alerts
- Facilitating communications and information sharing among stakeholders
- Developing mitigation and response strategies
- Publishing best practices in incident response as well as prevention advice;
- Coordinating international cooperation on cyber incidents;

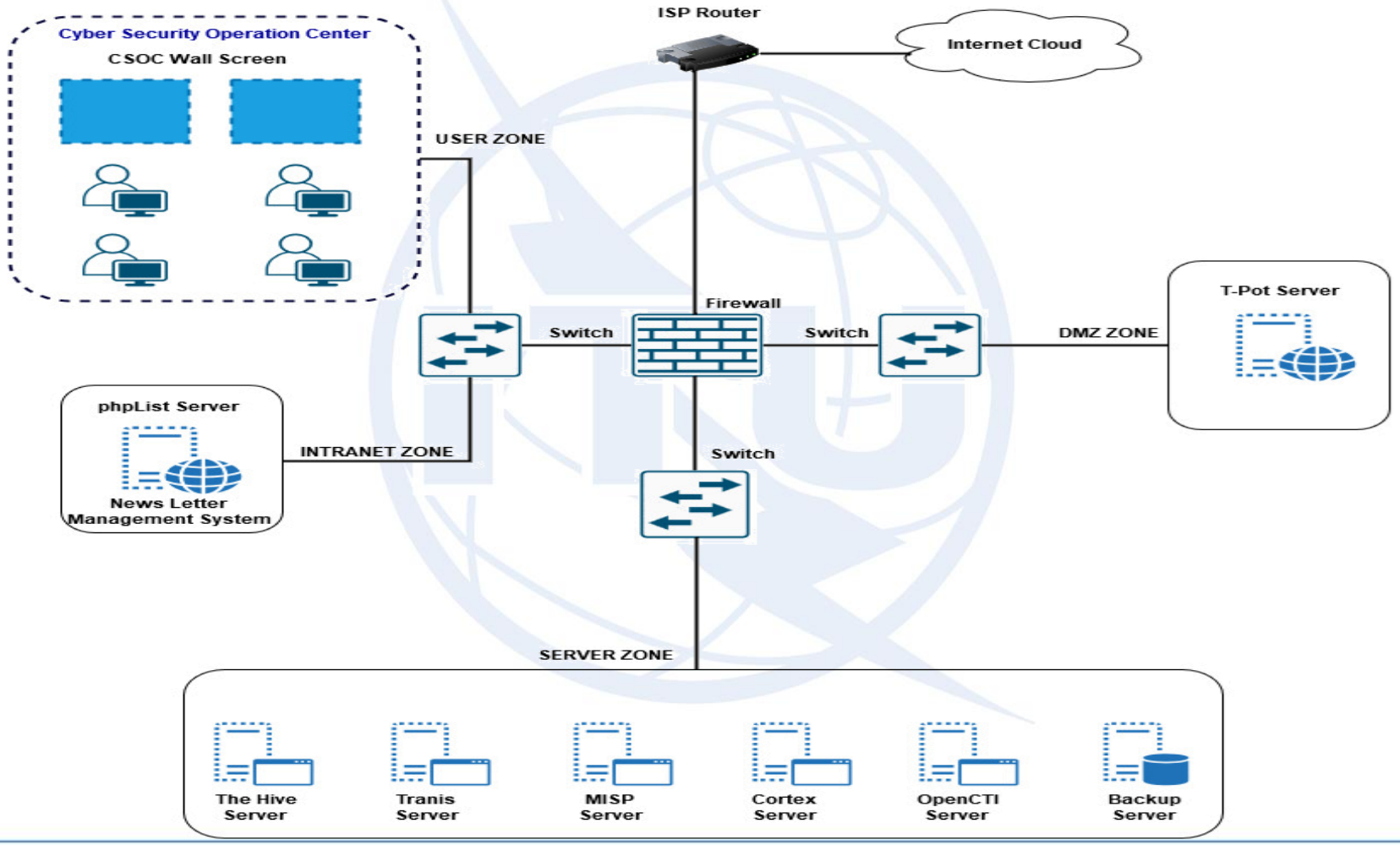
National Incident Response Team

Computer Incident Response Team (CIRT) is a team of cybersecurity experts, security analysts, whose work is focused on developing, recommending, and coordinating the actions necessary to mitigate, eradicate, and recovery, in the shorter time, as a response of an incident of the computer systems. The Computer Incident Response Team (CIRT) is named as Cyber Incident Response Team, or Computer Security Incident Response Team (CSIRT), or, Computer Incident Response Center (CIRC), or Computer Incident Response Capability.

An incident response team has the main objective to be prepared, to handle, to respond, to mitigate, incidents and the impact that they can produce.

* Forrester / ** Silensec

CIRTs - Network Architecture



Benefits of a National Incident Response Team

- Is the national trusted focal point to handle, to coordinate, and to respond to national cyber threats and attacks
- Participate in the protection of the National Critical Infrastructure
- Can help organizations to develop their own incident management capabilities
- Watching functions
- Develop the necessary national capacity and skills for incident handling
- Documentation
- Reporting
- Communications
- Digital Forensics Lab to analyse vulnerabilities
- Development of cybersecurity best practices
- Publicize cybersecurity guidelines
- Deploy awareness campaigns
- Offer cybersecurity trainings
- Collaborate with the national capacity building or educational career

The Cybersecurity Operations Center (CSOC or SOC)

- A CSOC or SOC is basically a team of cybersecurity analysts whose function is the computer network defence (CND), therefore detect, prevent, analyse, react, respond, report, and defend the constituency from cybersecurity incidents.
- A SOC can be a specific unit of, a specific function of, or considered a CERT, CSIRT, CIRT, CIRC, CSIRC, NOSC.
- A SOC can be built with the participation of a small team of five experts, and then grow to be a national coordination centre.
- A SOC can offer prevention of cybersecurity incidents, threat analysis, scanning for vulnerabilities, coordination of countermeasures, contribute to the development of security policies and network architecture, real-time monitor, detection, and analysis of threats and intrusions, triage of alerts, receive claims by phone calls or other means, build historical trends, review relevant data sources, operate technologies to defend the network, use intrusion detection systems, among several others.
- Depending on the and its location, it can have No-Authority, Shared Authority, or Full Authority (not absolute).

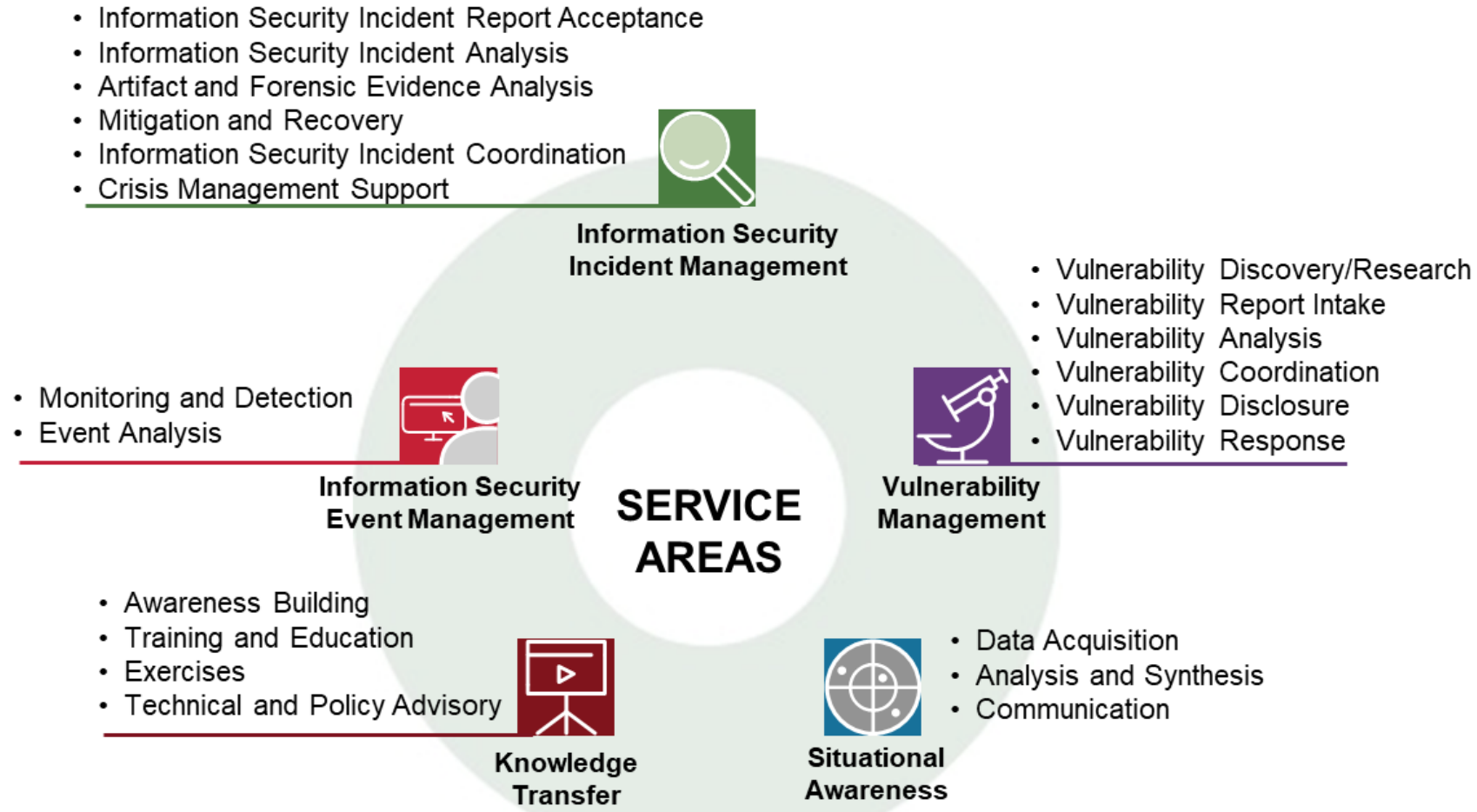
CIRT as part of the National Structure

- Can report to a governmental authority
- Can report to a ministry
- Can report to the regulator
- Can be part of the national defence

- A National CIRT needs to be formally recognized and have clear mandate
- The independency and autonomy is related to its position
- The higher level, the better results - empowered to properly react, respond, handle, coordinate

- ColCERT -> reports to the Ministry of National Defence
- Chilean CSIRT -> at the National Cybersecurity Agency

Basic functions of National Incident Response Teams



Creating a National Incident Response Team

- As considered by the International Telecommunication Union in the ITU CIRT Programme:
- Readiness Assessment:
  - Measuring the readiness of the constituency and government for the deployment of the national CIRT.
  - Cybersecurity situation of the country.
  - National cybersecurity framework.
  - Inclusion of all possible stakeholders -> the regulator, policy makers, health sector, judiciary sector, cybersecurity agencies, Army, ISPs, telecommunications sector, institutions from the critical infrastructure, local industry, banking sector, academia, research institutions, among other relevant national actors.
  - Several local interactive workshops and trainings on basic cybersecurity aspects.
  - Communication of the concept and functions of the National CIRT, the value, the structure, the different models, explanation of all phases. Motivation, further steps, participation of the stakeholders, their expectations, budget.
- Design of the CIRT:
  - Definition of the CIRT, mandate, positioning on the national structure, model of all services, processes, description of the workflow, policies and procedures, roles, responsibilities, strategy for communications, relation with the constituency, resources, technologies to automate the processes, definition and setup of the premises, environmental conditions of the Data Center, hardware, software, deployment of virtual machines, licenses, recruitment of the human resources, skill development, information transfer, trainings, among other activities.

Creating a National Incident Response Team

- Establishment of the CIRT:
  - Deployment of the National CIRT, set up the network, configuration of cybersecurity tools, deployment of internal services for the CIRT, deployment of the services that the CIRT will deliver, configuration of software, installation of servers, development of the internal processes, development of procedures, development of manuals, operating procedures, build up organizational capabilities, customization, and fine tuning, among other activities.
  - Then will start the process of building up experience by handling incidents, building up the relation with the constituency, with other agencies, with other CIRTs.
  - Then start offering services, development of national procedures, participating in the national legal framework, participating in international events, drills, adopting international agreements, participating to conventions, building up relations and programs with the national academia, among several activities and services.
- Improvement:
  - Deployment of more services aligned with the service framework of FIRST.
  - Further work on the technology, including threat intelligent, honeynets, further digital forensic services, further installation of tools and/or development of a digital forensic lab, further vulnerability management, installation of hardware, installation of software, review and deployment of new necessary processes, procedures, guidelines, further work in organizational capabilities, customization and fine tuning.

Event Management

- Service Area: Information Security Event Management -> Monitoring and detection and Event Analysis.
- Identifies information of the security incidents through compilation, correlation, further analysis of the events.
- Assigned to Security Operations Center (SOC) -> first level and second level incident management.
- Service of Monitoring and detection
- For “Log and sensor management” -> tools for automation of the management of events, continuous processing, analyze compiled information, logs, NetFlow, alerts, Intrusion Detection Systems, identify events, violations to policies, attacks, intrusions, breaches, statistical models, machine learning.
- Security Information and Event Management (SIEM), Big Data Platforms, Open-Source Intelligence.
- For “Detection Use Case Management” -> Instructions for event triage, qualification, correlation, as well as the Standard Operating Procedures (SOP).
- For “Contextual Data Management” -> Use of APIs, export data from other systems, Configuration Management Databases (CMDB), Identity and Access Management (IAM), Threat Intelligence systems, manual management through indicators, whitelists, lists of false positives, watchlists, among others.

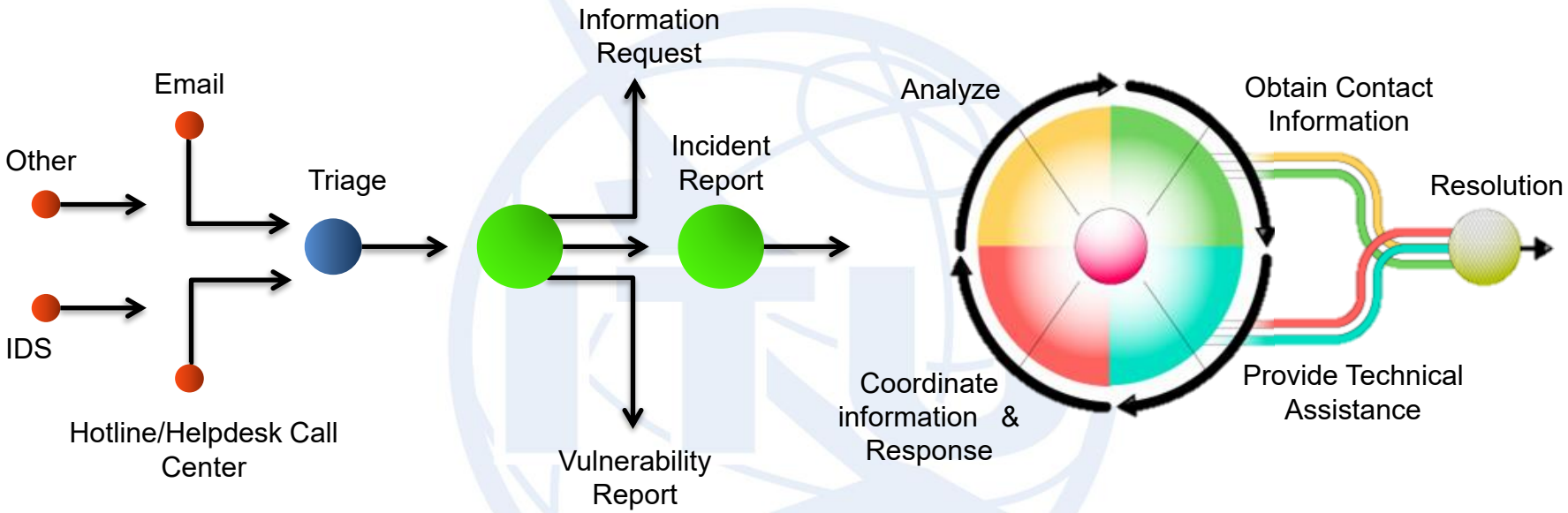
Event Management

- Event Analysis
  - Correlation
  - Qualification
- Triage of incidents to detect the information from potential incidents.
- Qualification to be ready for escalation in case it is necessary or determine as false alarm.
- In some structures: SOC for monitoring and detection -> CSIRT for incident handling.
- SOC teams work in front of a video wall where the alarms are projected.
- Specialists of the CSIRT's team works form workstations using the corresponding tools.
- The tool Security Information and Event Management (SIEM) provides real-time visibility of the information from the security systems and management of event's logs, configure rules, intelligence to be applied to raw data.

Incident Management

- Core critical function of a CSIRT. The major skill and expertise that a CSIRT should have and offer.
- Incident: Start the analysis, classify, categorize, and assign resources, cross incident correlation, determine the root cause, request more information from the source, investigate similar incidents, gather logs from honeynets, request information from partners and from other cybersecurity teams, include a forensics evidence team, properly compile forensics digital evidence, size the equipment, permissions, among others.
- Collection and analysis of the cybersecurity information, and deep comprehension and identification of the incident, how it was performed, the tools that have been used, analysis of the artefacts, the malware, the techniques, the vulnerabilities, the scope of the incident, among several other considerations.
- Then the CSIRT manages the situation, control the damage, recover the systems, document the process, disseminate best practices, apply recommendations, address further crisis, be prepared to similar incidents.
- Receiving reports of incidents, analysis of information, analysis of the whole incident, digital forensics analysis, mitigation, recovery, coordination, crisis management, further learning.
- Established channels for reporting claims with basic data to start the first picture of the incident, triage the received incidents, process alike claims, compile and group information of several sources, maybe massive incident?, among other considerations.
- Implemented mitigation and recovery plan, system restoration, recovery of data, ensure continuity of the business, synchronization of the data and the further full reestablishment of the services.

Incident Handling Lifecycle



Source: CERT/CC Incident Handling Life Cycle in CERT/CC "Handbook for Computer Incident Response Teams (CIRTs)

Incident Handling Lifecycle

Vulnerability Management

- Discovery/Research, Report Intake, Analysis, Coordination, Disclosure, and Response to new and to already known vulnerabilities.
- Implementation of patches to avoid that vulnerabilities are exploited.
- To discovery and research is necessary share information, establish relations between members of vulnerability management services.
- Important are relations with other CSIRTS, explore public sources, premium services and subscriptions, vendors announcements, subscription mailing lists, international organizations, Vulnerability Report Intake services, or as well as through the implementation of fuzz testing.
- Another option is reverse engineering, vulnerability scanning processes, penetration testing.
- As part of the service is included building up a repository, a database of vulnerabilities and the incidents that exploited the vulnerabilities of the network.
- Triage vulnerabilities, further process, reports, classify them by the systems, analysis, among others.
- Understanding potential impacts, root cause, identify remediation strategies, identify patches and solutions all to minimize the possibility that the vulnerability be exploited.
- Disclosure: Deployment of disclosure policies and infrastructure maintenance, policies for announcements, communications, and dissemination, and the further post-vulnerability disclosure feedback.

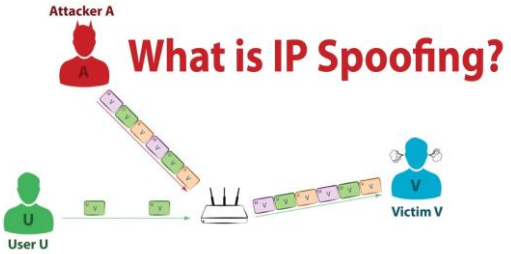
Awareness and Communications

- The National CSIRTs offer several services that demand continuous building technical knowledge, collect unique information, and have a detailed view of the national and international security.
- The National CIRT is one key source of knowledge, technical expertise, and unique cybersecurity skills. It is highly important that the knowledge be transferred though capacity building, awareness campaigns, trainings, courses, cyber camps, drills, hands on exercises, workshops, cybersecurity dialogues, among others.
- The National CIRT can develop technical material, publications, research, develop national tendencies, indicators, deployment agreements with national educational institutions, contribute to the creation of careers on cybersecurity, offer mentorship programs, fellowships. disseminating best practices, offer advice to other functions of the government as the legal sector, the judiciary sector, the banking sector, among others.
- As for the advisory functions, it implies advisory support to the legal system, explain cybersecurity concepts at the court, clarify doubts in case of analysis of digital evidence, support to risk management, support the deployment of business continuity plans, support the deployment of disaster recovery plans, advice in the deployment of cybersecurity policies and procedures, among several other possible functions.

Incident samples

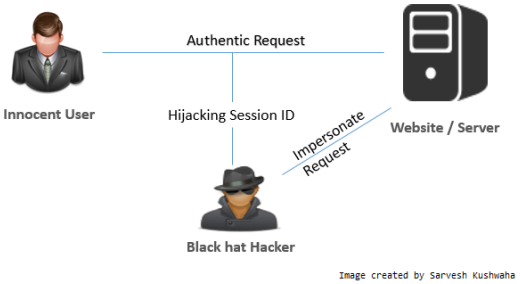
Scan activity to firewall servers	Web defacement
Information leakage	Phishing sites
Compromised server	Espionage
Intrusion	DoS / DDoS attacks
Use of proxy server as open proxy	SMTP relay
Virus infection	SPAM
Laptop Theft	Malware distribution
Botnet and C&C	One-Click Fraud
Identity Theft	Unauthorized Access

CyberAttacks and Hacking

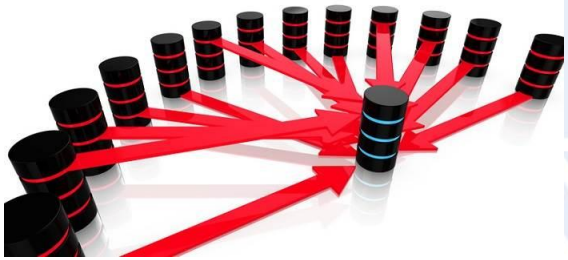


IP Spoofing

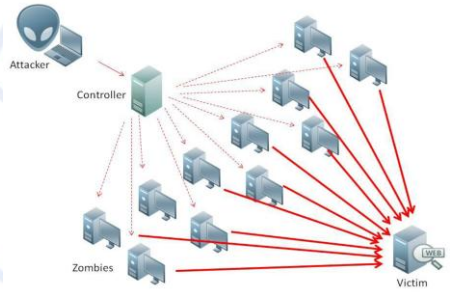
Fishing



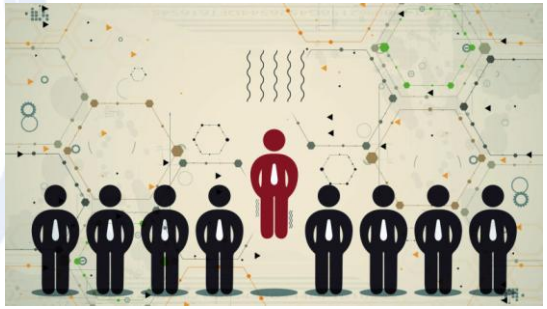
Session Hijacking
Man-in-the-Middle



DoS



DDoS, rDoS



Social Engineering

Ramsomeware
Virus

Exploits
Worms

SQL injection
Spyware

Credential Reuse
Spam

Incident response

Process of addressing computer security incidents

- Observe system for unexpected behaviour or anything suspicious
- Investigate anything considered unusual
- If the investigation finds something that isn't explained by authorized activity, immediately initiate response procedures

Global Cybersecurity Index 2024

5th edition

September 2024

ITU Global Cybersecurity Index is a composite index that measures key aspects of state-level cybersecurity practices

Driven by ITU Plenipotentiary Res 130 (Rev. Bucharest, 2022), and WTDC Res 45 (Rev. Kigali 2022)

The GCI is designed to:

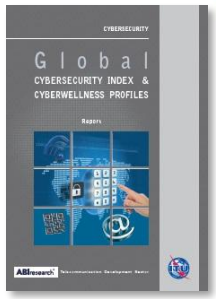
- ✓Drive awareness global cybersecurity
- ✓Share best practices
- ✓Drive continuous cybersecurity improvement
- ✓Build capacity in ITU Members

Key Facts

First released: **2015**

Past editions: 4

Country Participation in 2024: **172 (of 194)**



GCIv5 commitment is measured using the five pillars of the Global Cybersecurity Index Questionnaire

194 countries → 83 questions → 19 indicators → 5 pillars → Overall scores

The Global Cybersecurity Index is unique in measuring countries' cybersecurity commitments over time

- Only composite index that measures 194 countries' actions ("commitments") supporting cybersecurity
- Focuses on inputs of cybersecurity across 5 pillars (Legal, Technical, Organizational, Capacity Development, Cooperation)

Expert Group

- 140 Experts from government, academia, civil society, and private sector, led by Vanessa Copetti Cravo (Brazil) in 2022-2023
- Give input into questions, structure, weightages, and calculations

Questionnaire

- Sent to all ITU Member States, desk research conducted for non respondents
- 152 countries responded for the 5th edition
- Countries asked to provide evidence to substantiate their responses

Country Verification

- Country responses are verified by GCI Team
- Over 30,000 URLs, and over 1,000 pdfs were submitted as part of 5th edition

Report

- Global Report released
- ITU's most downloaded publication in 2021

The GCI has become a touchstone for measuring cybersecurity progress of countries

Governments

172 governments designated GCI focal points

Researchers

> 3 000

research papers published mentioning the GCI

among others

News Media

> 49 000

news articles published mentioning the GCI

among others

Development Organizations

among others

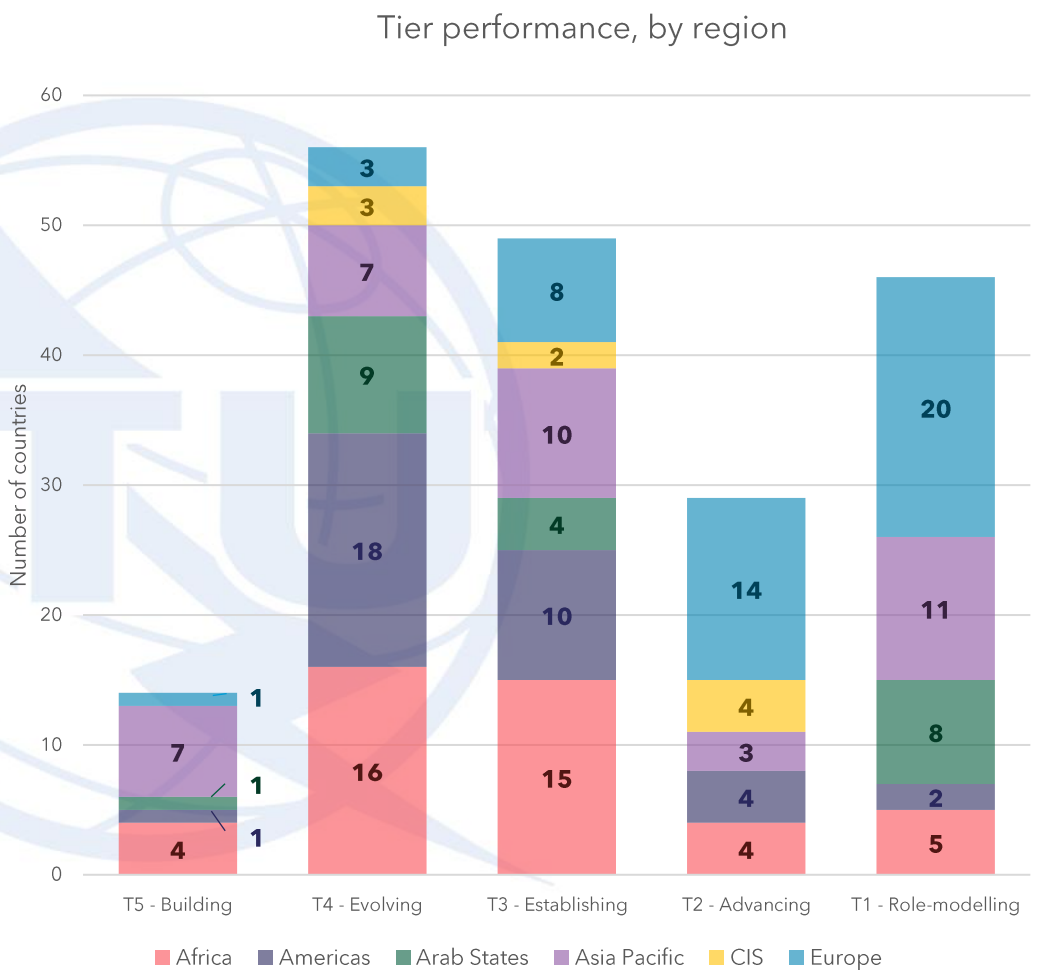
International Organizations

among others

GCI 2024 presents country performance in Tiers

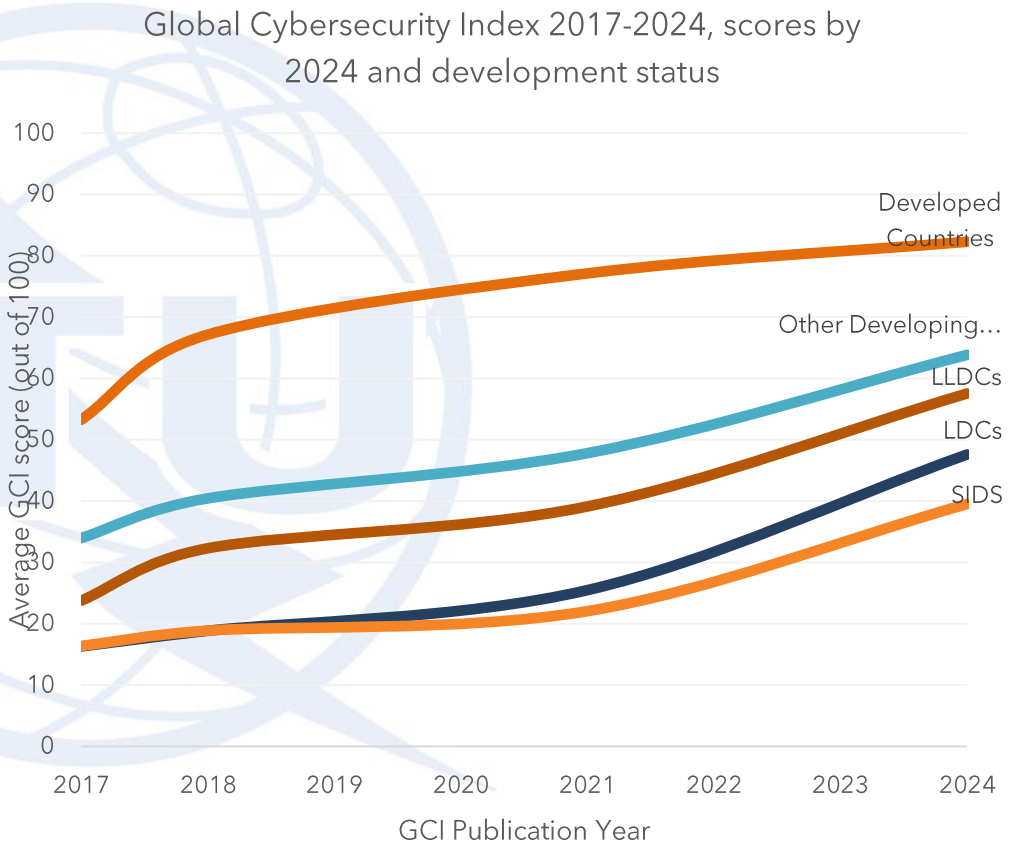
The 5th edition of the GCI introduced *Tiers* – countries are grouped based on their score into bands (as directed by Res 45 (Rev. Kigali, 2022), and Res 130 (Rev. Bucharest, 2022)

- Score ranges for Tiers are based on GCI Expert Group recommendations
- 46 countries are T1 - Role-Modelling (scoring above 95). Had tiers been applied in the previous edition, 30 countries would have been T1

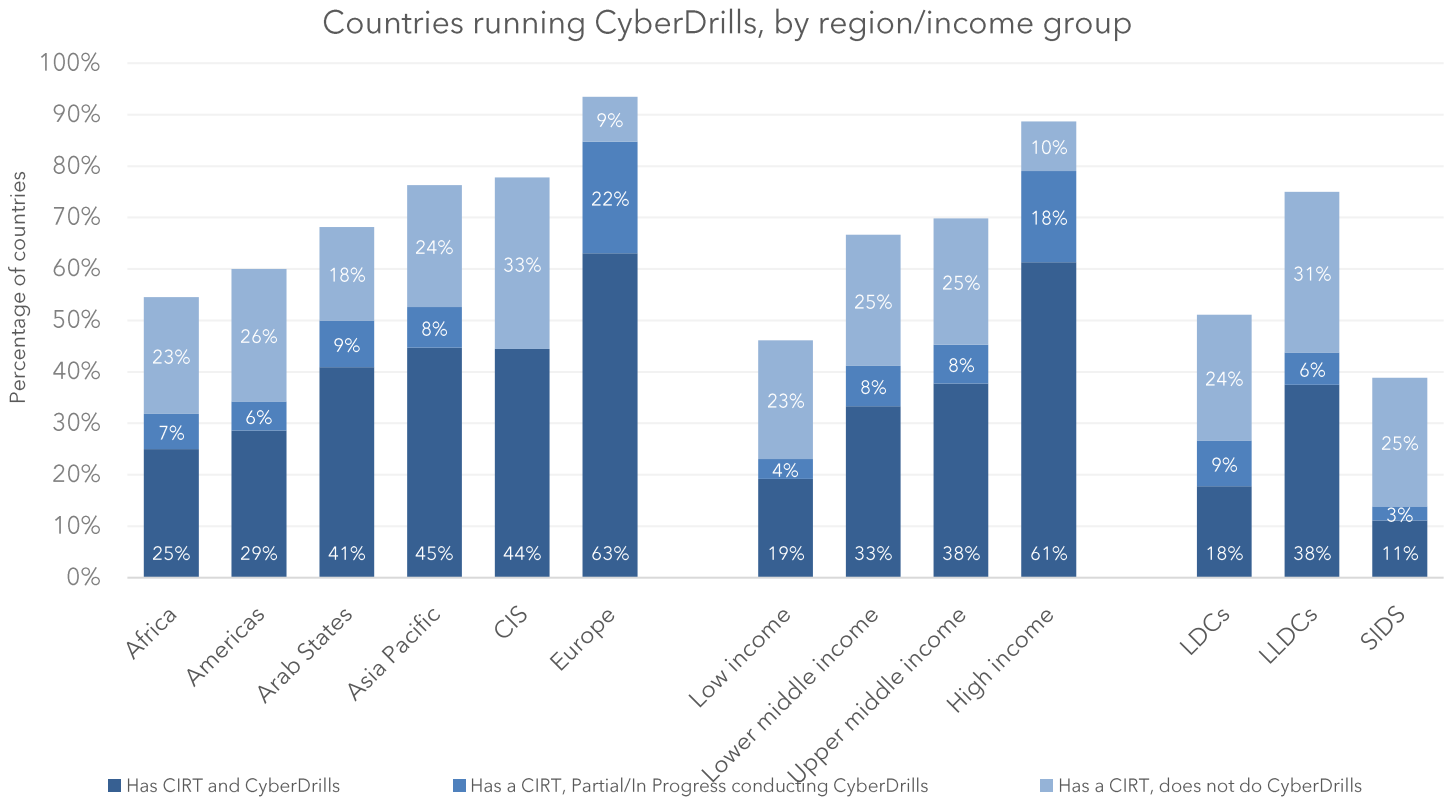


LDCs are starting to accelerate their cybersecurity efforts, but more efforts are needed for LLDCs and SIDS

- Developing countries are starting to close the cybercapacity gap, but progress is uneven. Standout countries are pulling the average higher
- LLDCs and SIDSs continue to face resource and capacity limitations, such connectivity challenges and vulnerabilities to hazards. They lag in implementing Computer Incident Response Teams (CIRTs) and relevant capacity development
- Much progress happening due to countries in Africa beginning to implement Computer Incident Response Teams (CIRTs), National Cybersecurity Strategies (NCSs)
- Overall, most countries are strongest in Legal Measures (existence of legal institutions and effective frameworks dealing with cybersecurity and cybercrime)

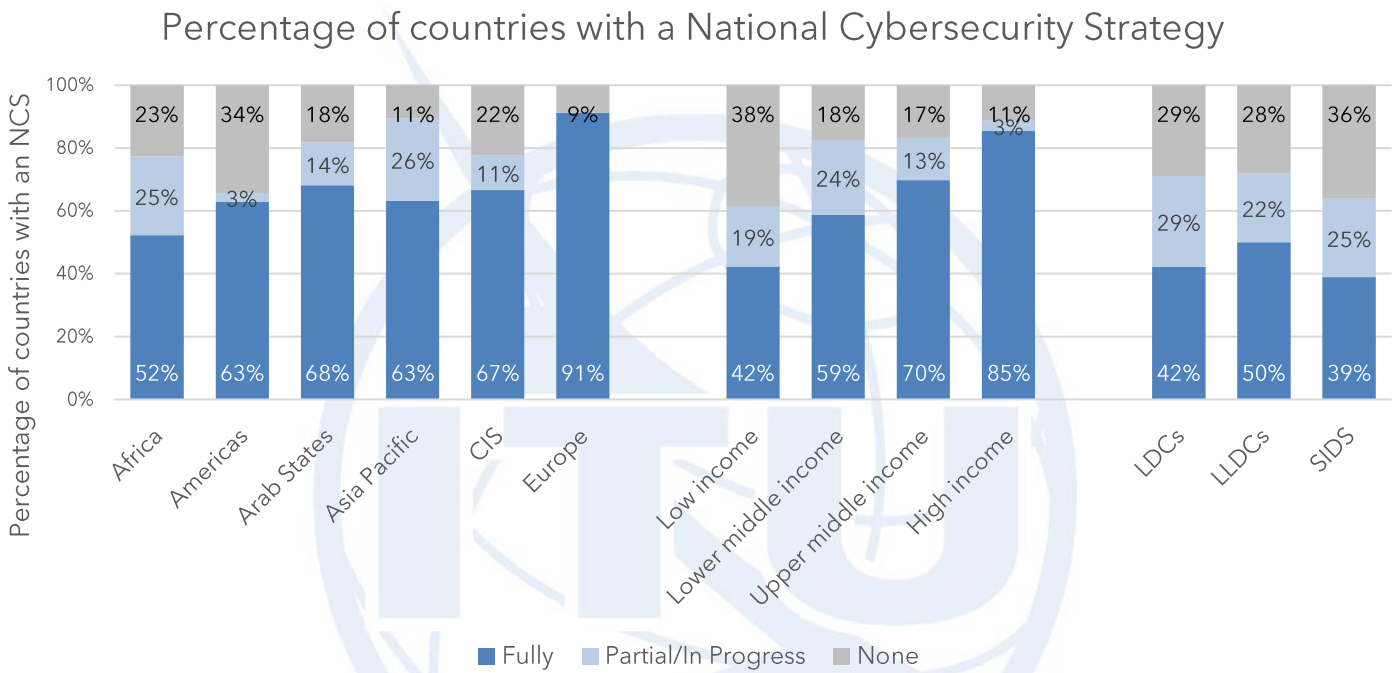


National CyberDrills are used by CIRTs to train, inform, cyber preparedness



- To enhance preparedness and capabilities, CIRTs, as well as Cyber Security Authorities are increasingly running cybersecurity simulation exercises among stakeholders, also known as CyberDrills.
- While **140** countries participated in regional CyberDrills organized by the ITU in 2023, running national CyberDrills remains important to engage domestic stakeholders in hands-on exercises. **41%** (**80**) of CIRTs run their own CyberDrills

More countries have a National Cybersecurity Strategy



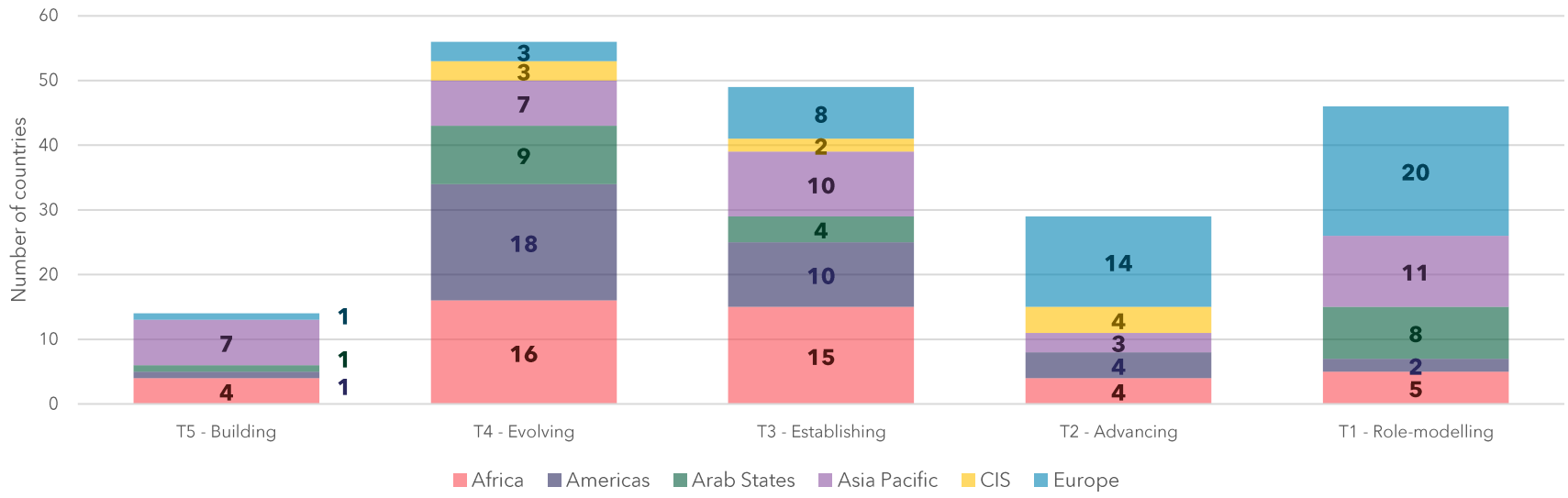
- National Cybersecurity Strategies are increasingly recognized as a tool to help align efforts in cybersecurity across government
- As of 2024, **132** countries have a National Cybersecurity Strategy, up from **107** in 2021.
- Much of progress can be attributed to the African region, which nine countries shepherded in their first National Cybersecurity Strategies. In addition, many countries worked to revise and update their existing strategies.

Regions based on World Bank intermediate regions, or closest proximate area

GCI 2024: Americas Tier Performance

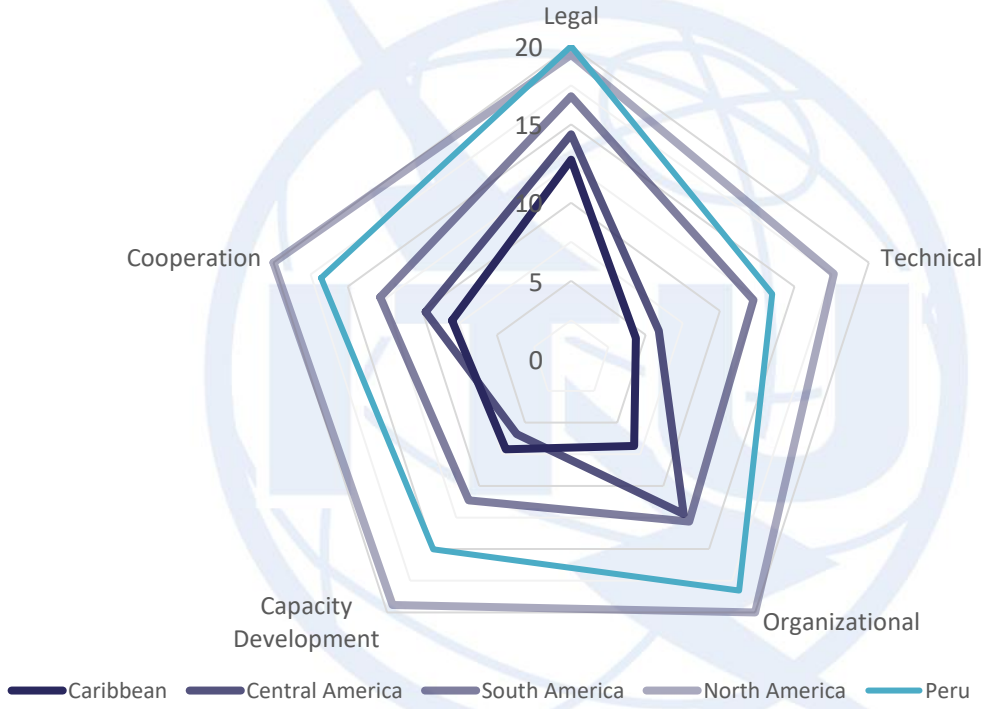
T5 *Building*	T4 *Evolving*	T3 Establishing	T2 Advancing	T1 Role-Modelling
Antigua and Barbuda*	Argentina Bahamas* Barbados* Belize Bolivia (Plurinational State of)*** Dominica* El Salvador Grenada* Guatemala Guyana Haiti* ** Honduras Nicaragua Saint Kitts and Nevis* Saint Lucia* Saint Vincent and the Grenadines* Suriname* Venezuela	Chile Colombia Costa Rica Cuba* Dominican Rep.* Jamaica* Panama Paraguay*** Peru Trinidad and Tobago*	Canada Ecuador Mexico Uruguay	Brazil United States of America

* SIDS ** LDC *** LLDCs



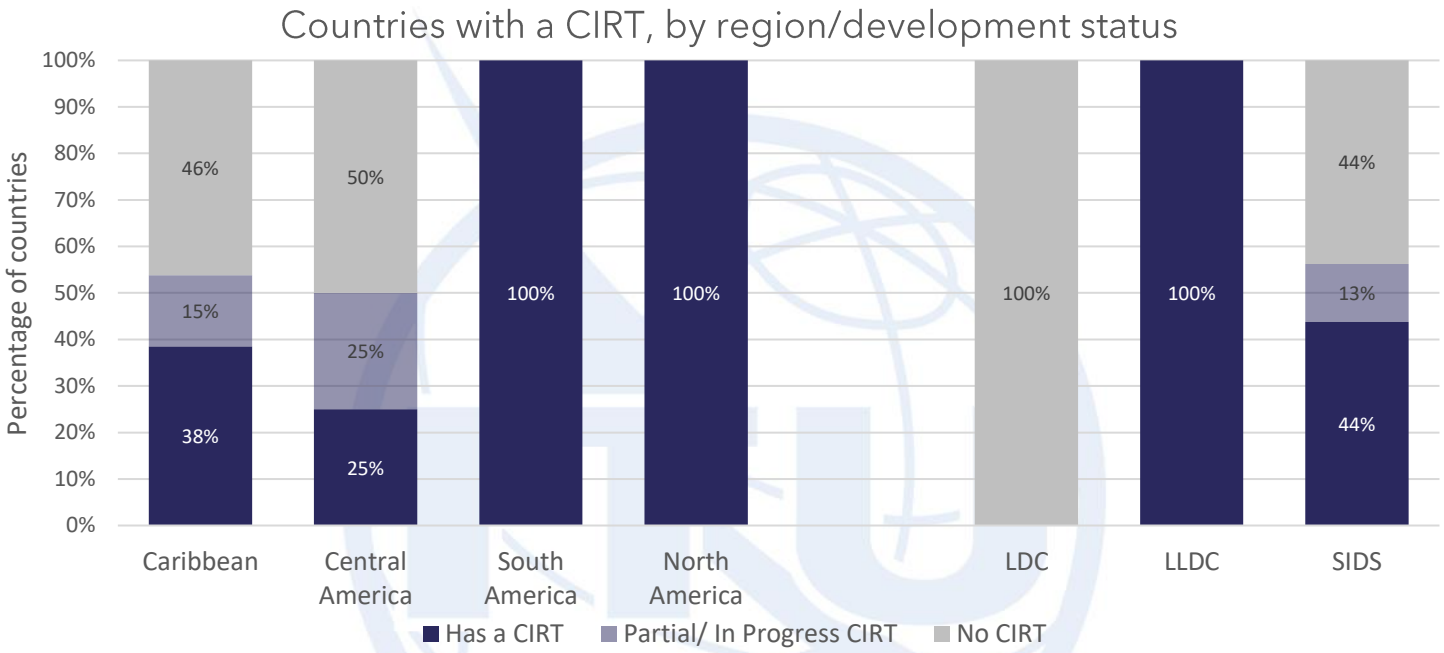
Americas has sharp contrasts inter-regionally, and room for improvement on capacity development and technical measures

Americas average score, by geographic area



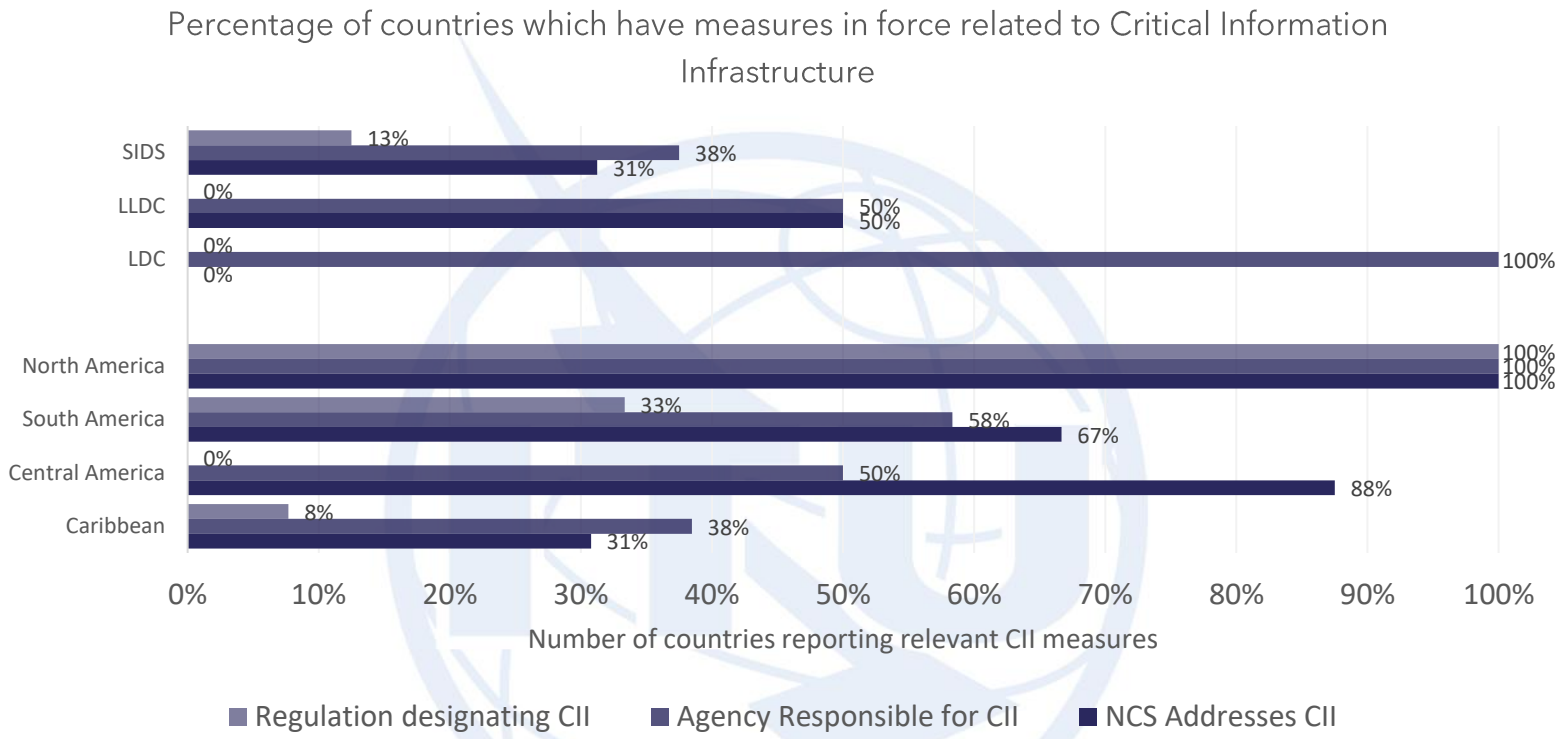
- SIDS score low overall, hampered by resource limitations
- South America has high levels of CIRT development, and are more often conducting cyber exercises
- Regional bodies, such as OAS, have been critical figures in driving cybersecurity development

CIRTs are playing a key role in the cybersecurity ecosystem



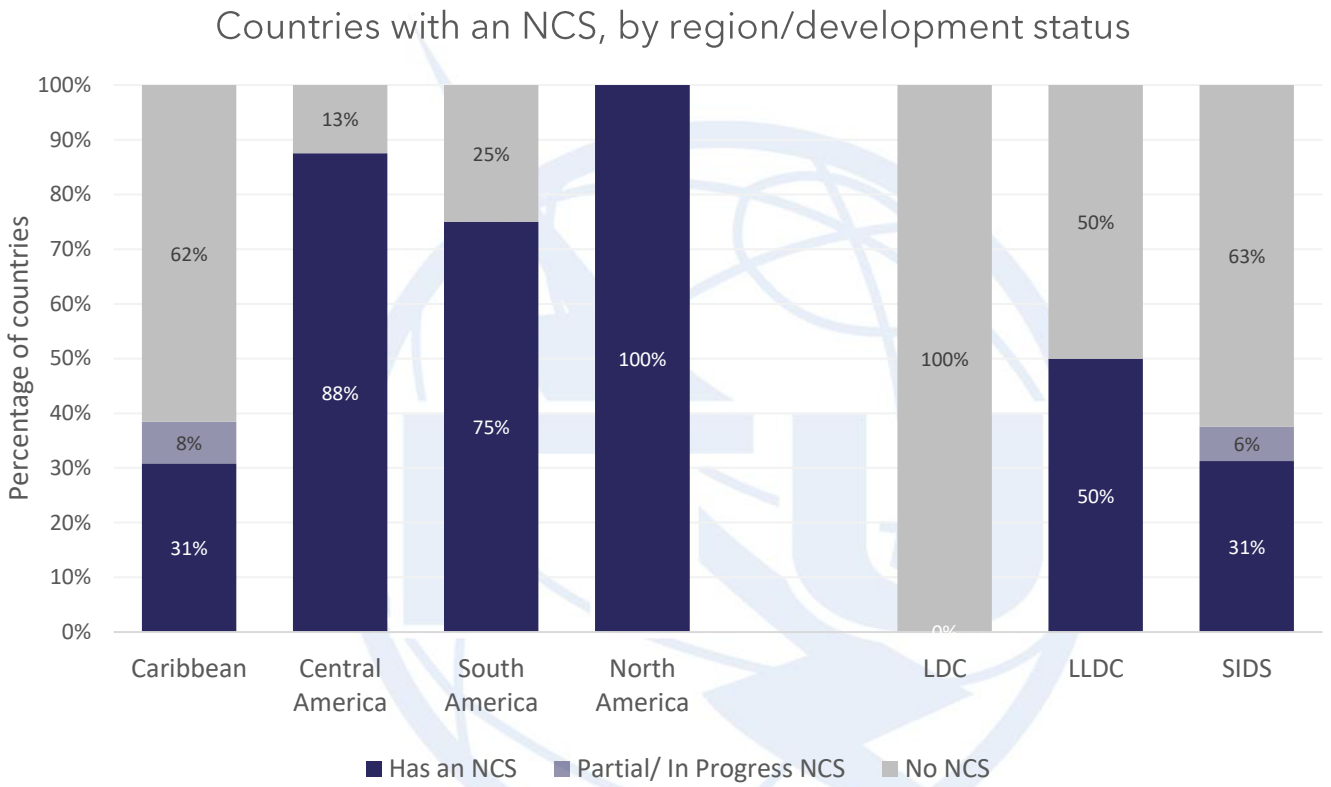
- Computer Incident Response Teams, Computer Security Incident Response Teams, Computer Emergency Response Teams, as well as SOCs, ISACs, and other teams monitor threats and help act in the event of a cybersecurity incident.
- Based on current data, **139** countries globally have a national CIRT, of which **21** countries in the Americas have a CIRT.
- Caribbean and Central America lag behind compared to the rest of AMS countries, with **10** countries not having a National CIRT and **4** countries having it in progress

Critical Information Infrastructure efforts lack supporting legal measures



- Critical Information Infrastructure (CII) is tackled in the GCI through questions in the Legal, Technical, Organizational, and Capacity Development pillars. Developing a synergistic CII ecosystem involves addressing all these pillars in concert and ensuring that these measures reflect current threats and vulnerabilities.
- With **18** countries in the Americas having an agency, ministry, or other group with the responsibility of cybersecurity for CII, only **7** countries have regulation designating CII.
- Many countries have measures in progress. **62.5%** of countries in Central America have CII regulations in progress

More countries in the AMS region have a National Cybersecurity Strategy



- National Cybersecurity Strategies are increasingly recognized as a tool to help align efforts in cybersecurity across government
- As of 2024, globally **127** countries have a National Cybersecurity Strategy, up from **107** in 2020.
- In the AMS region alone, most of the countries have their NCS developed. There are still **8** countries in the Caribbean without having an NCS.

Since 2014, Q8/17 has developed 16 standards about cloud cybersecurity: Series ITU-T X.1600, X.1630 And X.1640, and 3 standars about cybersecurity on big data: ITU-T X.1750.

X.1600	Arquitectura de seguridad de la nube de borde
X.1601	Marco de seguridad para la computación en la nube
X.1602	Requisitos de seguridad para entornos de aplicaciones de software como servicio
X.1603	Requisitos de seguridad de datos para el servicio de monitorización de la computación en la nube
X.1604	Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube
X.1605	Requisitos de seguridad de la Infraestructura como Servicio (IaaS) pública en la computación en la nube
X.1606	Requisitos de seguridad para entornos de aplicaciones de comunicaciones como servicio
X.1631	Tecnologías de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube
X.1641	Directrices para la seguridad de los datos de los clientes de servicios en la nube
X.1642	Directrices para la seguridad operativa de la computación en la nube
X.1643	Requisitos y directrices de seguridad para contenedores de virtualización en entornos de computación en la nube
X.1644	Pautas de seguridad para la nube distribuida
X.1645	Requisitos de la plataforma de conocimiento de la situación de seguridad de red para la computación en la nube
X.1646	Amenazas a la seguridad que deben identificarse en el ámbito de la seguridad como servicio
X.1647	Pautas de seguridad para seleccionar métodos y recursos informáticos de proveedores de servicios en la nube
X.1648	Directriz sobre la seguridad de los datos en la informática de borde
X.1750	Directrices sobre la seguridad del big data como servicio para proveedores de servicios de big data
X.1751	Directrices de seguridad para la gestión del ciclo de vida de big data por parte de los operadores de telecomunicaciones
X.1752	Pautas de seguridad para la infraestructura y la plataforma de big data

Elemento de trabajo	Asunto/Título	Momento
X.1649 (ex X.sgmc)	Pautas de seguridad para múltiples nubes	2025-04
X.1753 (ex X.gdsml)	Directrices para la seguridad de datos mediante el aprendizaje automático en infraestructuras de big data	2025-04
X.1631rev	Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube	2025-09
X.asm-cc	Requisitos de la gestión de la superficie de ataque para la computación en la nube	2025-09
X.ckrp	Marco del fondo de recursos de claves criptográficas para la computación en la nube	2026-06
X.fr-msp	Requisitos funcionales de la plataforma de microsegmentación en un entorno basado en la nube	2027-01
X.gapci	Directrices sobre la protección anti-DDoS para la infraestructura en la nube	2026-06
X.gdso -cs	Directrices de desarrollo, seguridad y operaciones (DevSecOps) para servicios en la nube	2027-09
X.mbaas -cs-sec	Requisitos de seguridad y marco del servicio de colaboración para múltiples plataformas de blockchain como servicio	2025-09
X.scr-cna	Requisitos de seguridad del entorno de ejecución de contenedores en espacio aislado para aplicaciones nativas de la nube	2026-06
X.sfrms	Marco de seguridad y requisitos de microservicios para computación en la nube utilizando tecnología de contenedores	2027-01
X.sgcnp	Pautas de seguridad para la plataforma como servicio para aplicaciones nativas de la nube	2027-01
X.sg-tc	Pautas de seguridad de servicios de nube confiables	2027-01
X.soar-cc	Marco de orquestación, automatización y respuesta de seguridad para la computación en la nube	2025-09
X.srapi-cc	Requisitos de seguridad de la interfaz de programación de aplicaciones (API) para la computación en la nube	2026-06
X.sreai-ec	Requisitos de seguridad para la entrega de IA de borde en la computación de borde	2027-10
TR.fcnsc	Informe técnico: Marco para un mecanismo de colaboración de seguridad basado en la nube entre proveedores de servicios en la nube	2026-06

Thank You!!!