Deloitte.

AIM FOR THE
EXTRAORDINARY

Cyber everywhere.
Go anywhere

EMEA
Cybersphere
Center

2022

EMEA Cybersphere Center
Aim for the extraordinary
2023

MAKING AN
IMPACT THAT
MATTERS
since 1845

EMEA Cybersphere Center
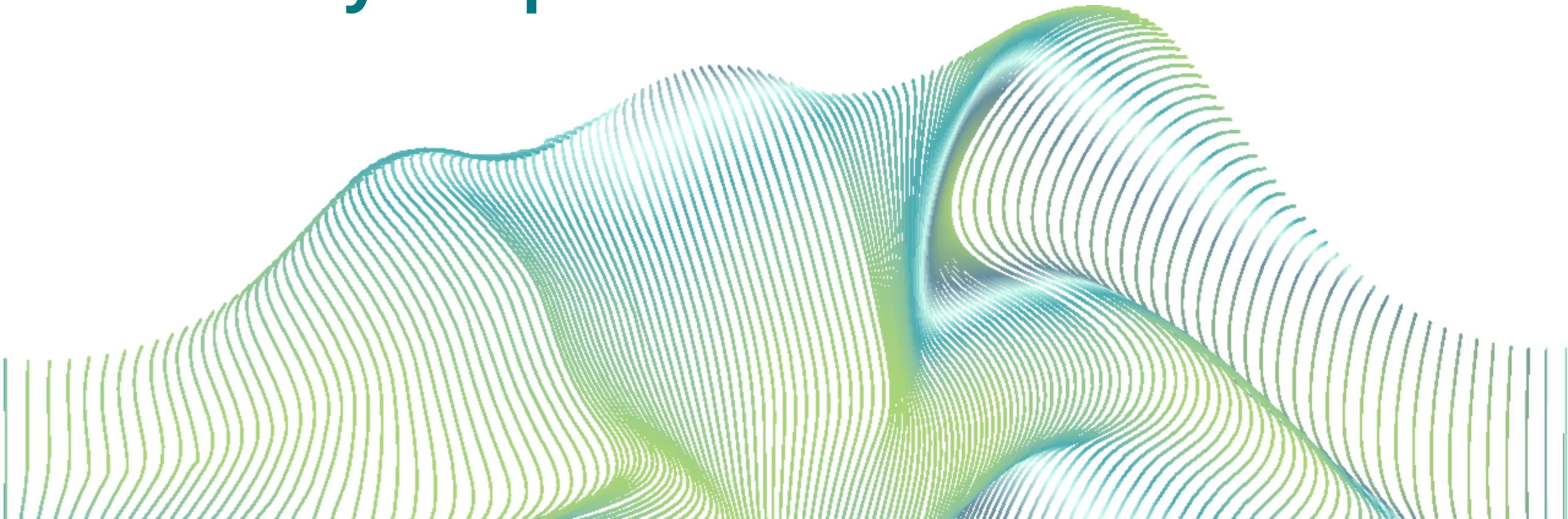
EMEA Cybersphere Center
ECC Client Experience

The **EMEA Cybersphere Center** **it's the cyber operate services partner for clients** that helps them to perform better by solving complex problems in a sustainable and scalable way.

The center boasts spaces that allow us to interact with our clients and enjoy a more personal relationship with them, which helps us to better understand their challenges and create **tailored solutions**

North Tower
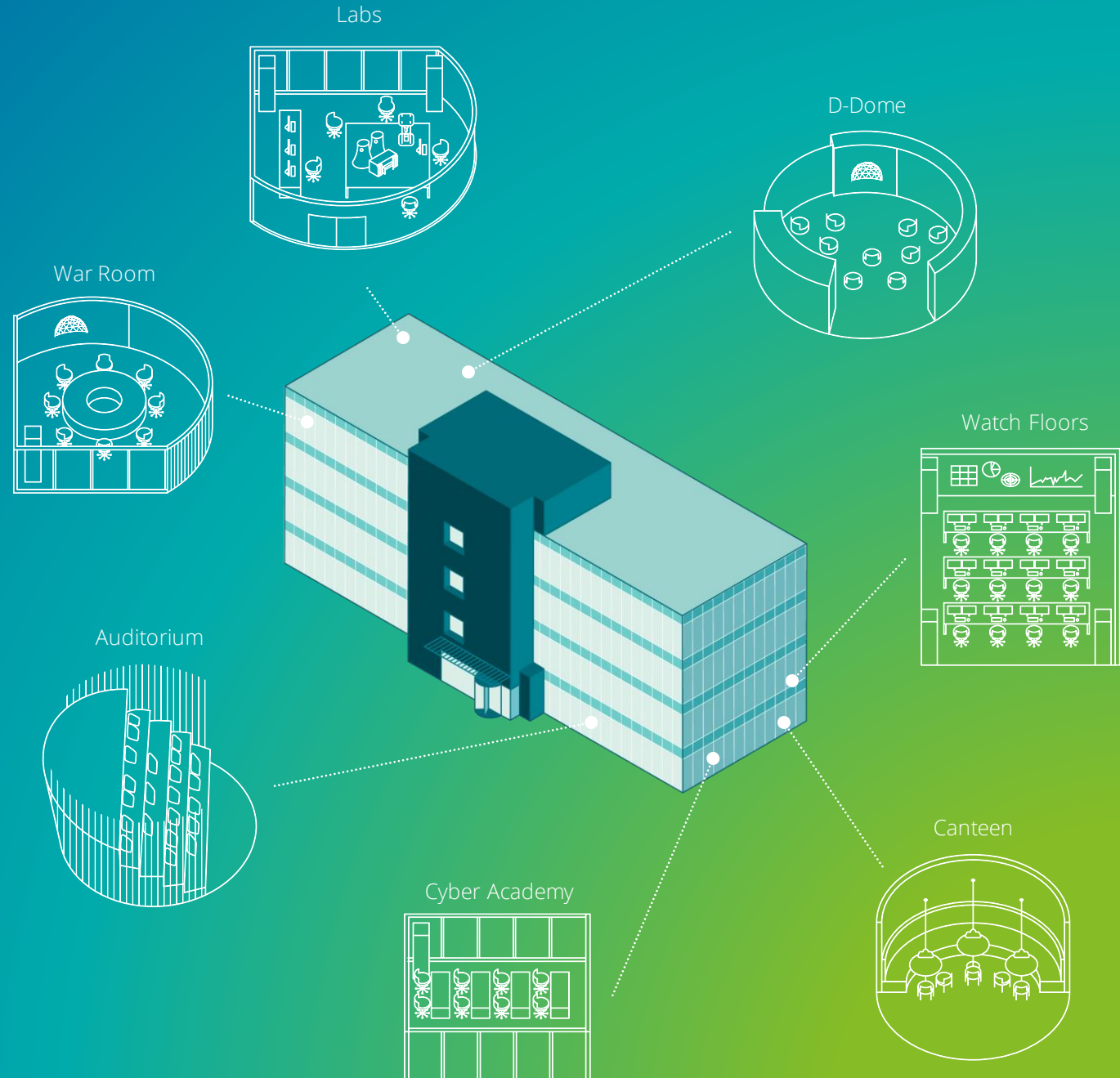
17.800
m²

18
floors

+350
Strategy and
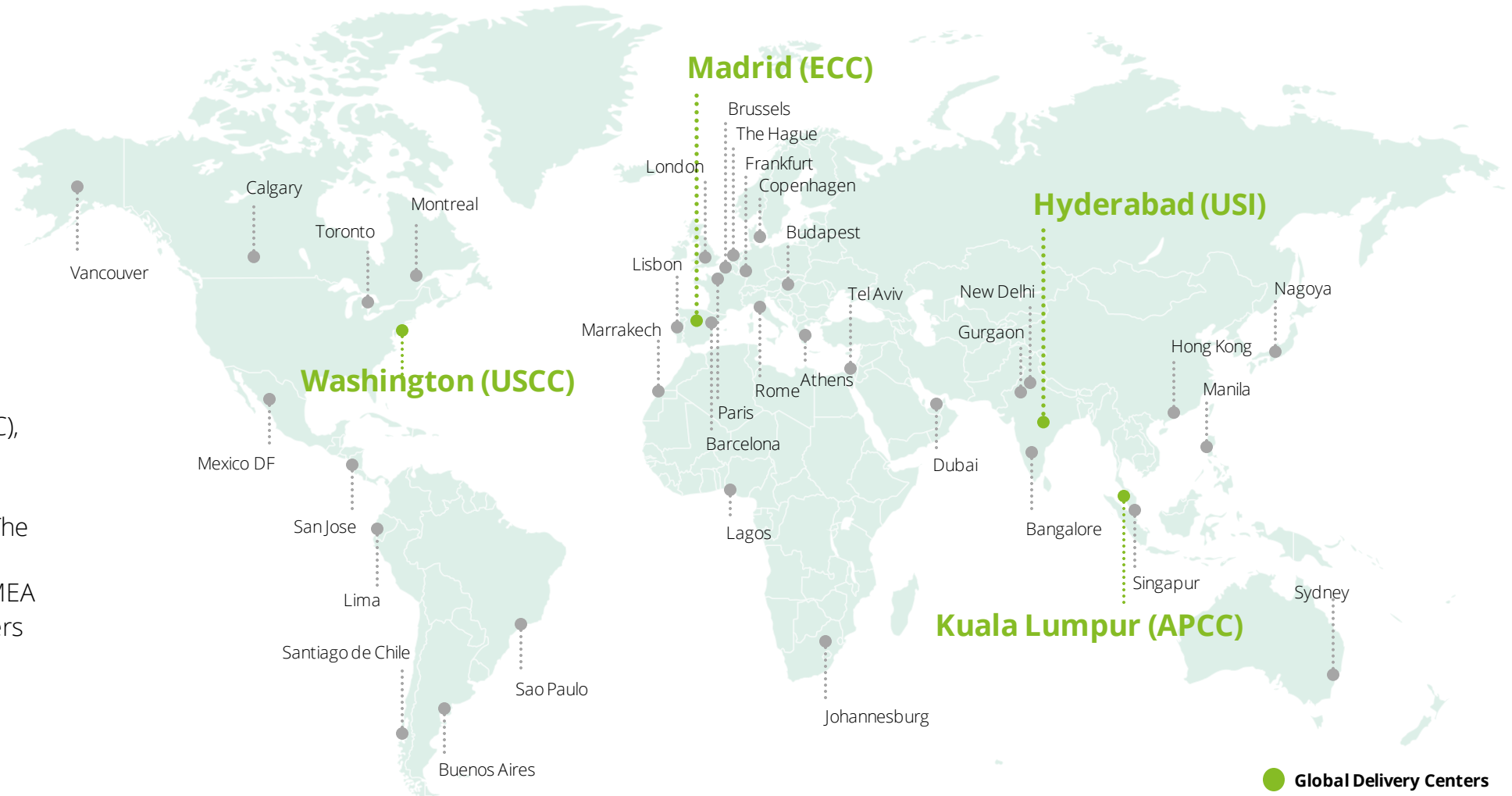Consulting teams

South Tower

3.940
m²

3
floors

+400
Cyber operations
professionals

Labs

D-Dome

War Room

Watch Floors

Auditorium

Cyber Academy

Canteen

EMEA Cybersphere Center
Snapshot

Our delivery strategy is built around a global network of **Global** Delivery Centers (GDC), operating in 24/7, and **local** Cyber Centers (CC) acting as front offices for our clients. The ECC, located in Madrid, is the **Center of Excellence** for EMEA supporting around 30+ centers globally.

Madrid (ECC)

Hyderabad (USI)

Washington (USCC)

Kuala Lumpur (APCC)

Vancouver
Calgary
Montreal
Toronto
Mexico DF
San Jose
Lima
Santiago de Chile
Buenos Aires
Sao Paulo

Brussels
The Hague
Frankfurt
Copenhagen
London
Budapest
Lisbon
Tel Aviv
Marrakech
Rome
Athens
Paris
Barcelona
Lagos
Dubai
Johannesburg

New Delhi
Gurgaon
Bangalore
Singapur

Nagoya
Hong Kong
Manila
Sydney

● Global Delivery Centers
● Cyber Centers

EMEA Cybersphere Center
Snapshot

37
Different **nationalities** of employees working at the ECC

96%
Renewal rate after 5 years of services

+100
RFPs managed in FY22

+15.000
Cyber professionals globally

+400
ECC professionals and 10+ languages

+150
Active MSS **clients**

+1,2M
Analyzed tickets in FY22

+35K
Cybersecurity training hours per user delivered by the Cyber Academy

+30
Cyber Centers supported

Aim for the extraordinary

Certifications / Accolades

We strive to be recognized for our excellence and service to our clients. We understand and determine what our customer wants and deliver the service with a high standard of professionalism and conscientiousness. We pay great attention to the performance and acquisition of the latest certifications that ensure the maintenance of our level of expertise
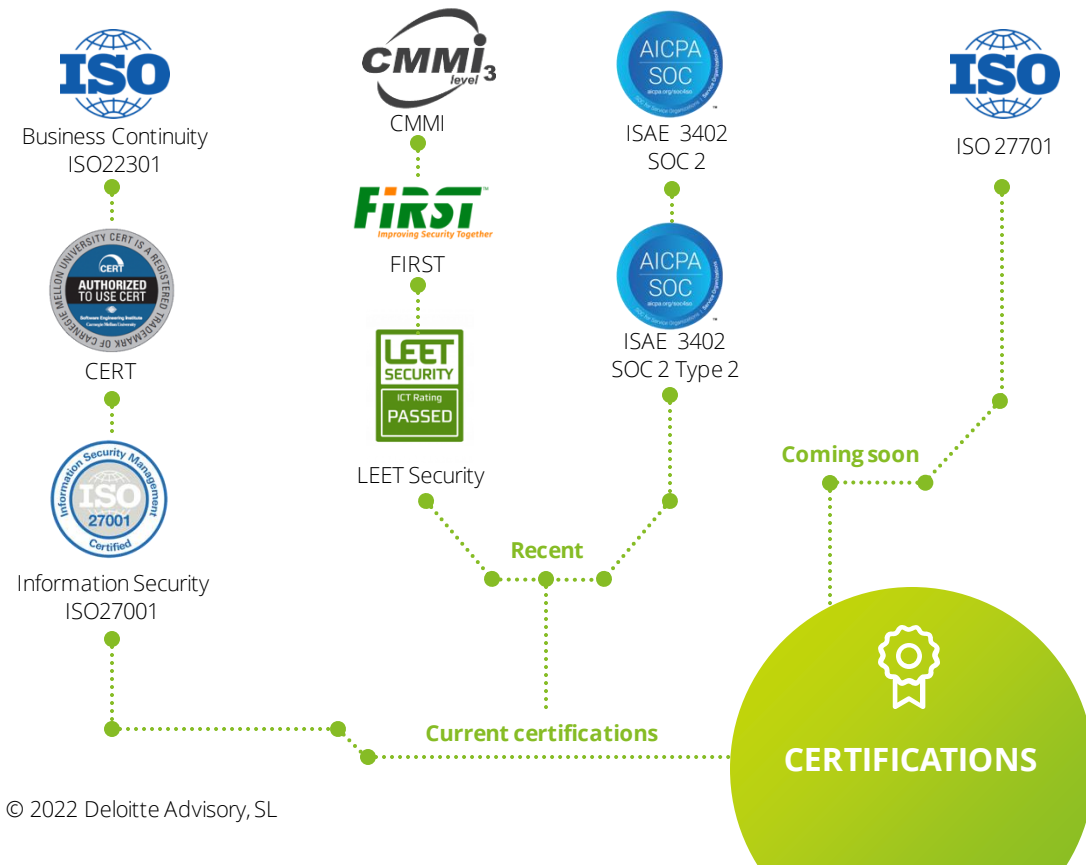
Our leadership is supported by international references:

ISO
Business Continuity
ISO22301

CERT

ISO 27001
Information Security
ISO27001

CMMI

FIRST

LEET Security

ISAE 3402
SOC 2

ISAE 3402
SOC 2 Type 2

ISO 27701

Coming soon

Recent

Current certifications

CERTIFICATIONS

Information Security Consulting

Global leader in Information Security Consulting in line with the existing strategy capabilities.

Forrester, 2019

Incident Readiness Services

Deloitte's leadership and ability to tailor and scale clients' incident readiness needs were called out by IDC

IDC, 2021

Managed Detection and Response

Gartner assessed the capabilities of our ECC and highlighted its leadership role as a Cybersecurity Incident Managed Detection and Response Center

Gartner, 2018

Security Consulting

Deloitte ranked 1st for the ninth consecutive year in Security Consulting in Gartner's magic quadrant

Gartner, 2019

Managed Security Services

Global Leader of Managed Security Service in line with the existing strategy and capabilities

IDC, 2017 & 2020

Cyber Incident Response

Global leader in Cyber Incident Response

Forrester, 2019

ACCOLADES

Aim for the extraordinary

WiC / Talent & Formation

At Cyber, we believe in Corporate Social Responsibility

Cybersecurity has become one of the most relevant and fastest growing areas in the technological field worldwide. We base our practice on managing the impacts we have on clients, employees, stakeholders and communities. As a result, social initiatives are born that represent our sense of resposibilitiy.

#cybereveryone

A prime example is Women in Cyber (WiC)

Mission

Create a culture in which initiatives such as WiC are no longer neccesary

Vision

Enhace diversity and success of profiles from different backgrounds in Deloitte Cyber

Objectives

Increase the number of women that consider and start a career in security

Provide the support required for women to reach leadership roles

Create a strong internal and external network of female talent

WOMEN IN CYBER

With the help of its Cyber Academy, the ECC takes care of the personal and professional development by investing in specific training for technical and soft skills.

Employees have access to over **240 training hours** within the first 2 years as a Level 1 operator, and training plans are also adapted for the specific needs of Level 2 and 3.

Level 1
Operator

Level 2
Security Analyst

Senior Security Analyst

Level 3
Researcher

Service Delivery Manager

Security Architect

Career path

South Korea
Finland
Mexico
Ukraine
UK
Brazil
Moldavia
Cuba
Nigeria
Zambia
India
Argentina
Poland
Equatorial Guinea
Australia
Colombia
China
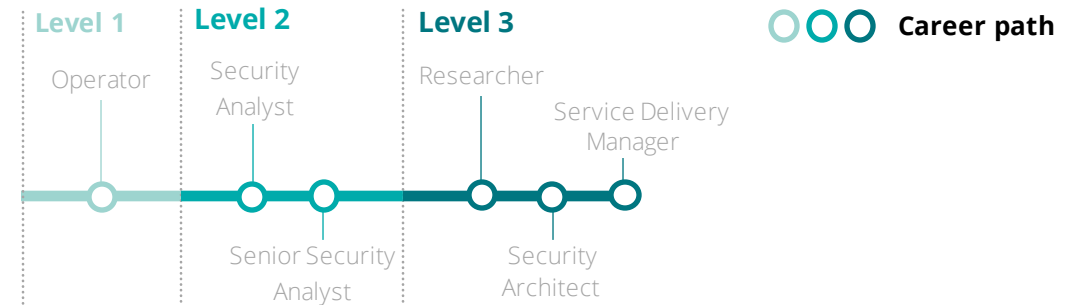
120+ International employees

30+ Different nationalities

TALENT & FORMATION

EMEA Cybersphere Center
Our added value for Deloitte's MFs

How the ECC can help

Service T&C
RFP & pre-sales support
SMEs support to deep-dive technically

Client Success Cases
References
Client Experiences

**Innovation**
Alliances
Certifications

ECC ⌄ MF ⌃ Client

The **ECC** supports local MFs as the **Center of Excellence** for remote delivery

CCs are connected to each other and to the rest of Deloitte's global network. They also receive support from the ECC. The common aim is to **optimize all services and adapt them to local clients' needs.**

- Deloitte's **global network** of **CCs** provides a high added-value to managed security services
- **CCs** act as front offices for local clients, as the last mile of the delivery

ECC Capabilities

Aim for the extraordinary

Our capabilities

ADVICE

D.

IMPLEMENT

OPERATE
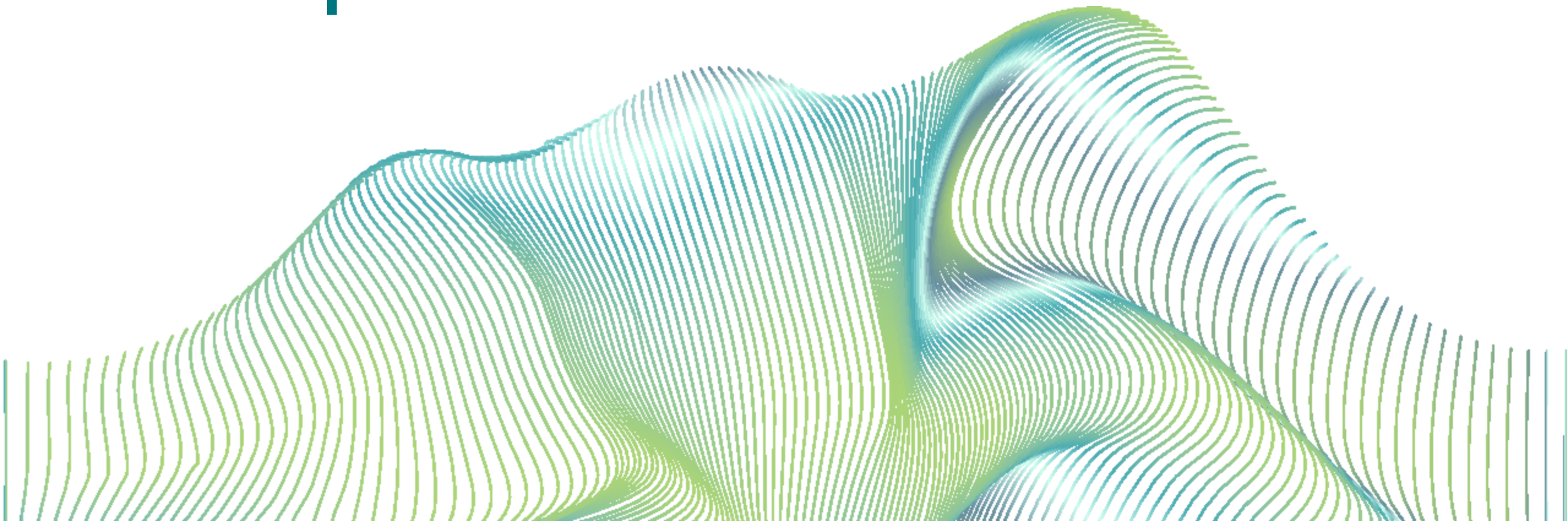
DIGITAL IDENTITY

DETECT & RESPOND

EMERGING TECH (IoT/ OT)

CLOUD & INFRASTRUCTURE
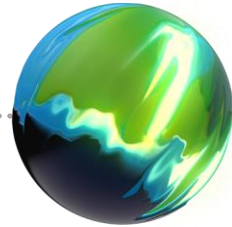
Through this service, Deloitte helps organizations with their cyber capabilities and solutions focused on **cyber defense and incident response** programs and operations.
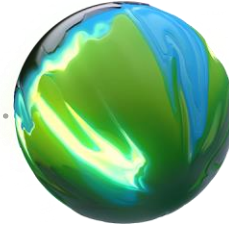
Deloitte boasts cutting-edge cyber capabilities and solutions, with a special focus on next-generation technologies, **including IoT and ICS.**
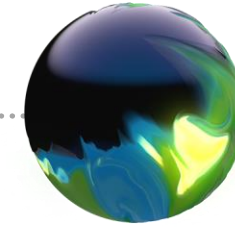
Deloitte accompanies its clients during the digitalization and innovation process, incorporating cybersecurity into their **Cloud infrastructure, whether public, private, or hybrid.** The scope of this offering includes the development, transformation, and resilience of a **secure network architecture**
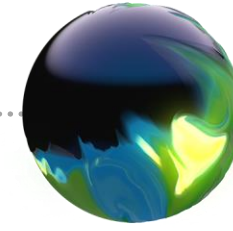
Aim for the extraordinary

Our capabilities

ADVICE

OPERATE   D.   IMPLEMENT

**DETECT &
RESPOND**
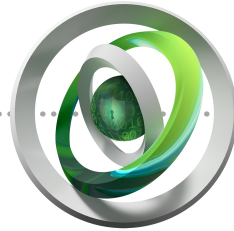
**EMERGING TECH
(IoT/ OT)**
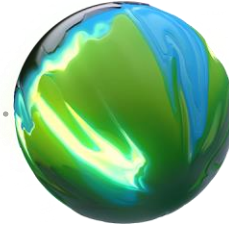
**CLOUD &
INFRASTRUCTURE**

- Identify
- Protect
- Detect & Respond
- Recover
- Lab Innovation Services

- Cyber Cloud Protection
- Managed Security Technologies
- Health check monitoring
- Network Security Transformation
- Infrastructure Design & Rollout

The ECC Detect & Response module includes:

Managed Extended Detection & Response (MXDR)	**MSS (BYOTS)**	**Threat Intelligence**	**Digital Forensic & Incident Response**	**Offensive Security**

ECC capabilities
Detect & Respond

The scope of this market offering includes the detection, response, and resilience program components.

We help our clients to understand and identify their exposure to cyber threats using our industry expertise and know-how, and also by simulating the same behaviors of a potential attacker.

We support them in detecting and responding to threats on their infrastructure, on the Cloud, and in the supply chain, leveraging data analytics and machine learning.

We also monitor cyber space thanks to our Intelligence team, identifying potential threats targeting our clients and providing valuable information to prevent cyberattacks. This deep knowledge of threat actors help us to contextualize every event before it turns into an incident.

Using our network of partners and established ecosystem, we are **experts in implementing and managing the most effective technologies** for cyber analytics, information security, and also workflow management, orchestration and automation, in order to solve the problems faced by clients and evolve their cyber operations.

Deloitte helps organizations to enhance and run their capabilities and solutions focused on cyber defense programs and operations, along with incident response and resilience programs and operations.

ECC capabilities
Detect & Respond

We provide a blend of sophisticated monitoring technology, advanced analytics, and human intelligence to help clients detect, analyze, and respond to threats before they disrupt the business.

Outcome Focused
Focused on security outcomes

Near real-time breadth & depth of visibility into threats
Designed to give clients access to the advanced threat detection and response capabilities their organizations require

Advanced & Industry Leading technological capabilities
Combines industry-leading technology with experienced Deloitte teams

Modular Architecture
Deloitte teams to provide a modular set of threat hunting, detection, response and remediation capabilities to clients

Advanced Analytics
Artificial Intelligence, Central & Edge Analytics, Threat Intelligence production

Global and local approach
Able to combine the excellence of our global delivery network with local support and tailored additional services.

Identify

Learn and adapt

Prevent and protect

Anticipate

Detect

Recover

Respond & Remediate

Deloitte cybersecurity actionable intelligence

Services

Managed Extended Detection and Response (MXDR) by Deloitte

Managed Security Services (MSS)

Threat Intelligence

Digital Forensic & Incident Response

Offensive Security
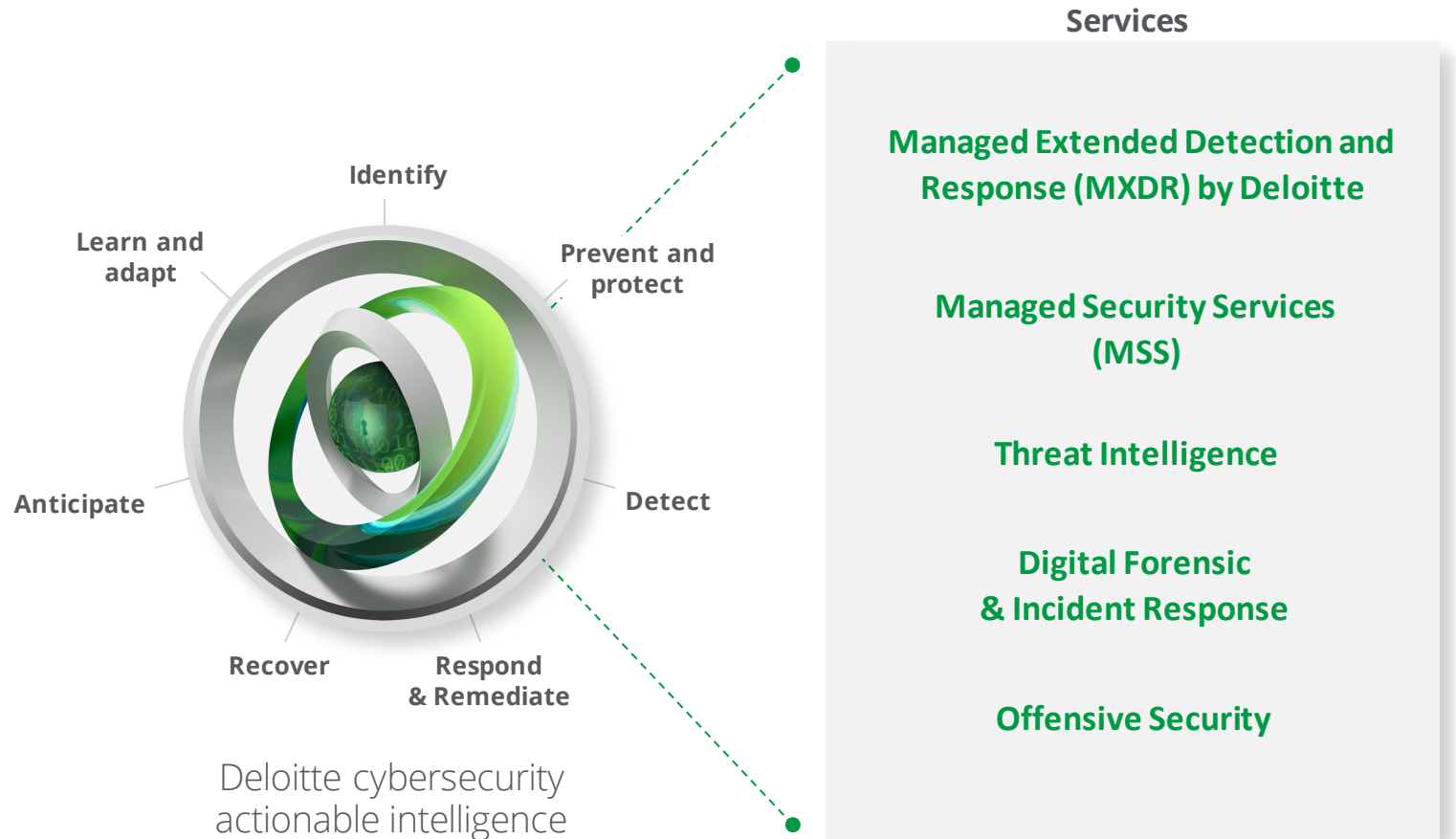
ECC capabilities

Emerging Technologies (IoT/ICS)

We invest in innovative OT and IoT technology, boasting a designated team and extensive capabilities that make it possible to offer our clients cybersecurity solutions in industrial and IoT environments.

We have a team of experts with training plans specifically focused on cybersecurity in OT and IoT environments. These plans include certifications such as GICSP (GIAC), IEC62443 (ISA), NERC Standard, OSCP, OCSEE (Offensive Security), along with various vendor-specific trainings.
.

Each service line has its own development strategy and roadmap in order to be able to provide exceptional services to our clients using the most cutting-edge technology.

Deloitte's labs are available to our clients to test scenarios and solutions, in order to avoid potential impacts to processes and be able to select the technology that best adapts to their needs.

We boast partnerships with the main security vendors in order to offer solutions specifically designed for industrial and IoT environments.

We help our clients to embed innovation in their products and to find solution to their most complex digital challenges, including areas like IoT and ICS.

ECC capabilities
Emerging Technologies (IoT/ICS)

Identification

The first step when defining an IoT/ICS cybersecurity strategy and roadmap is to analyze the existing environment, risks, and capabilities, in order to create a Cybersecurity Master Plan. This strategic analysis, accompanied by tactical and operational tests (such as asset discovery and an understanding of the existing security measures), makes it possible to establish plans for quick wins and medium- and long-term projects

Protect

These capabilities and services focus on protecting systems by defining security architectures in ICS environments or certifying IoT services. In addition, specific security technologies are tested for these environments before being implemented, thus ensuring the processing, availability, and latency of the environments. The technologies and controls include remote access management, physical device protection, data diodes, specific antimalware solutions for operating environments, and more.

Detect & Respond

Thanks to our specific use cases for industrial environments, we help organizations to detect and provide a quick and effective response to security incidents that occur as a result of OT and IoT threats. We have an organizational monitoring model that is specialized for industrial environments with specific playbooks adapted to these cases, along with teams that are specialized and expertly-trained in OT and IoT technologies.

Recover

This service helps organizations to establish incident response capabilities specific to IoT and industrial environments. Moreover, it covers preparation, training of deployed staff, and automation of certain incident response aspects. Realistic and systematic ICS and IoT incident response simulation tests are also performed.

Lab Innovation Services

Realistic threat scenarios are created that are adapted to specific needs, in order to run security technology and service integration tests; define security recommendations and best practices; access vulnerability scan results; and create demos, trainings, and exercises.

AVAILABLE MODELS

Healthcare   Power Supply Chain   Connected Vehicles

Smart Factories   Smart Stadium   Advanced Analytics
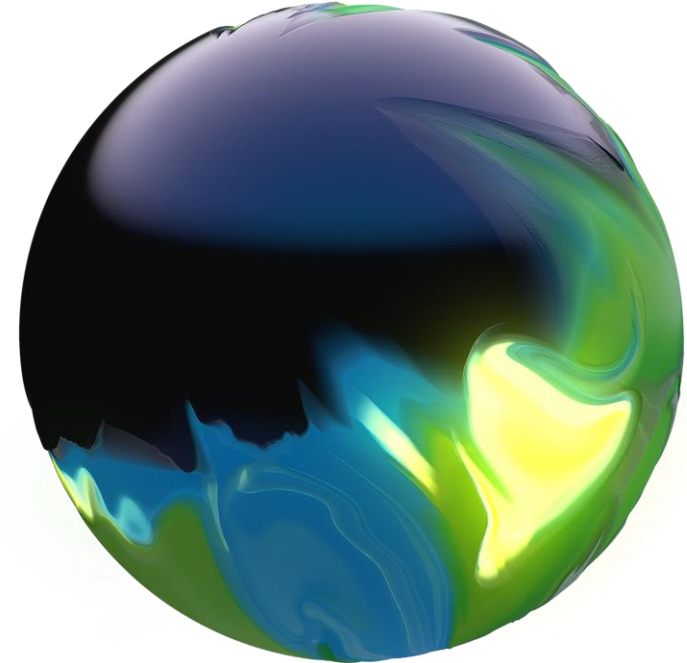
ECC capabilities
Cloud & Infrastructure | Cloud

Security should be present throughout all phases of Cloud strategies, right from kickoff. For this reason, Deloitte has a global project framework for all areas involved in Cloud strategies.

We offer a monitoring service to ensure compliance with security policies in workloads deployed on the Cloud and also to help detect anomalous behavior.

The extensive experience of our team allows us to support our clients in the design of reference architectures for the integration of security controls as part of the agile design of digital products. The result of this is that all elements on the Cloud are secure.

We provide our clients with the support required throughout the digitalization and innovation process, incorporating cybersecurity into their Cloud infrastructure, whether public, private, or hybrid.

ECC capabilities
Cloud & Infrastructure | Cloud

Implementation of Cloud security solutions

- Configuration of native security solutions on all Cloud providers

- Implementation of third-party solutions to improve Cloud security

Managed Cloud security services
(Cyber Cloud Protection)

- Compliance monitoring service that can be integrated with Cloud providers via an API
- Kubernetes microservices can be made more secure

- Anomalous behavior in Cloud management can be analyzed

- Various service levels to suit the needs of our clients

- Azure, AWS, Cloud, and Alibaba support

ECC capabilities
Cloud & Infrastructure | Infrastructure

We focus on establishing effective controls for companies' most sensitive assets and addressing the need to reduce risks, all while maximizing productivity, business growth, and profit.

We tackle cybersecurity challenges related to the design, deployment, and maintenance of control frameworks, infrastructures, and technologies.

We cover end-to-end projects in which we design secure architectures, implement cybersecurity solutions for user workstation protection and navigation, and also offer a remote operation and administration for the majority of industry vendors.

The aim is to make changes with as little impact on as few business processes as possible. We achieve this by ensuring that all authorized changes are performed efficiently and securely, and that they are always verified and documented.

The scope of this market offering includes development, transformation and management of secure network architecture through various mechanisms including network segmentation.

ECC capabilities
Cloud & Infrastructure | Infrastructure

Managed Security Technologies

- Remote administration and operation of security solutions by professionals that are experts on these technologies
- Capabilities: Endpoint and Email Protection, Web Application Firewall and Database Activity Monitoring, Firewalls and Network Access Control, IDS/IPS, Proxies, and OT/IoT
- We also develop added-value capabilities within every service as a result of synergies with other ECC teams, such as second opinion verdicts for email

Health Check Monitoring

Managed service for monitoring the health status of security servers and platforms

Firewall Assurance

- This Deloitte service makes it possible to analyze the security of network communications by automatically reviewing firewall rules. The results are aligned with security best practices and any applicable regulations (e.g. PCI, DSS, GDPR, etc.)
- The service is offered as a "oneshot" (one-off reviews), continued (periodic reviews), or active (analysis of security rule compliance before application)

Deception as a Service *(availanle soon)*

Managed services related to internal and external deception campaigns, with the aim of attracting the attention of attackers and studying them in order to prevent and anticipate attacks

FUTURE OF CYBER
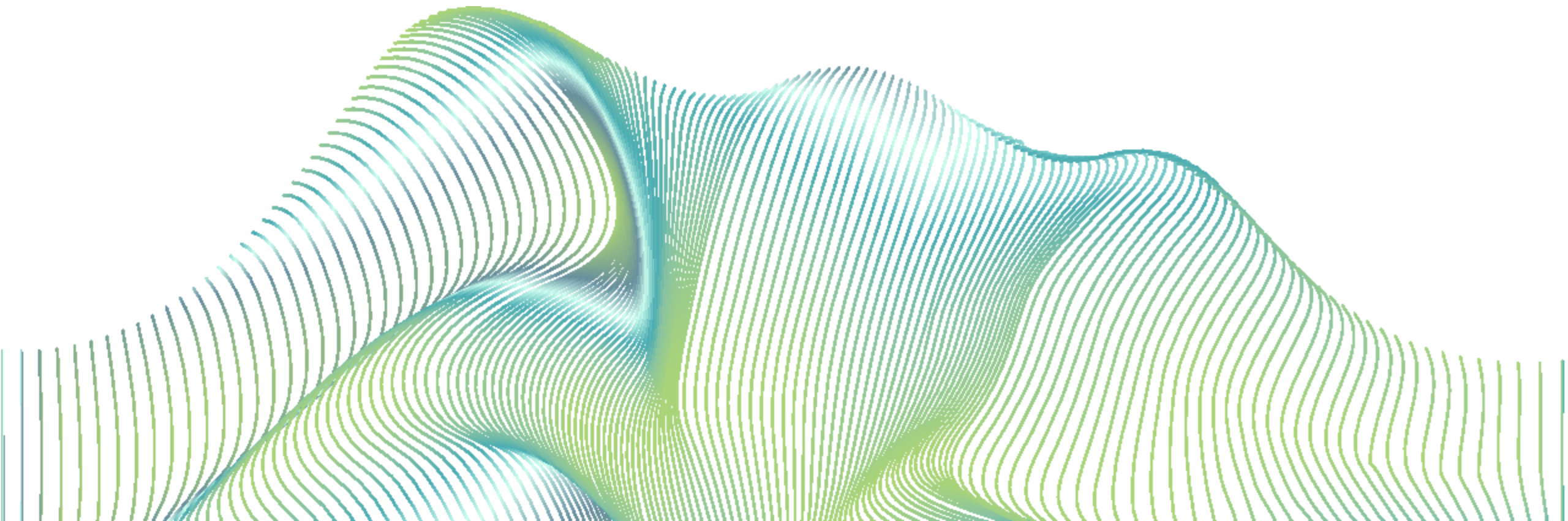
Future of Cyber

Innovation

We innovate at the intersection of our clients, industries, ecosystems and capabilities to anticipate and prepare for the cyber solutions of the future

Co-design use case together with our strategic clients

Evaluation of Technologies, architectures and methodologies through use cases

Alliances with clients and vendors for the analysis, improvement, and training on OT / IoT security technologies

○ Global Intelligence Platform: **DISP**

○ **6 IoT/OT prototypes** of real environments

○ Specialized **I+D+I** Cyber team

○ Global innovation program (Global Operate, MXDR)

As organizations continue to face evolving cyber challenges, we continue to **explore, invest and innovate**

Future of Cyber
IoT Labs
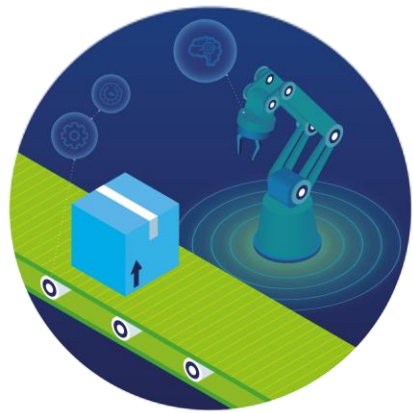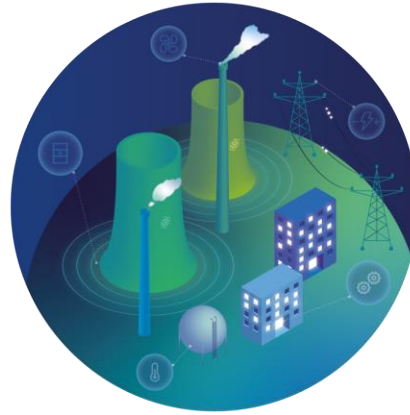
Client area + Labs demos

Area addressed to clients with various meeting points and connected to labs where to perform demos and dynamic activities.
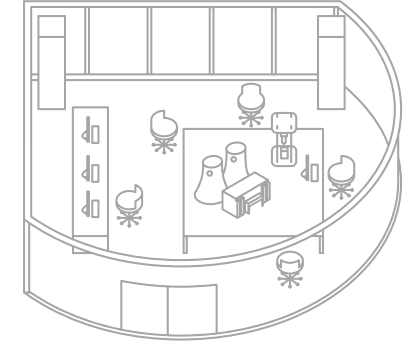
What is Cyber Emerging Tech?

This term refers to advanced capabilities designed to respond to the risks and needs arising from the digitalization and interconnection of operational environments, as well as the deployment and integration of new technology, such as **connected devices, Smart cities, 5G networks, cognitive analytics algorithms**, and more.

At Deloitte, we have built a specific strategy based on the creation of an innovative platform, which allows us to **create digital twins to better understand the abovementioned environments**, put our capabilities to the test, and drive the development of both our teams and the tools used by our SOC.

Future of Cyber

IoT Labs | Prototypes

Power Supply Chain
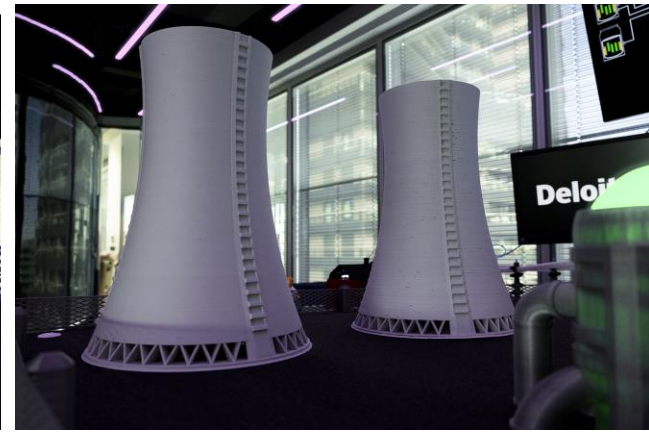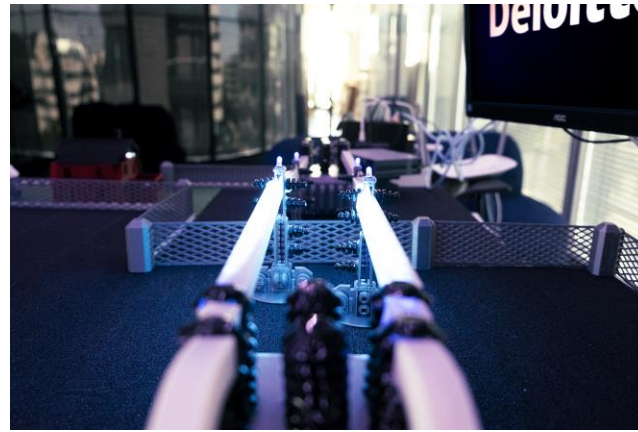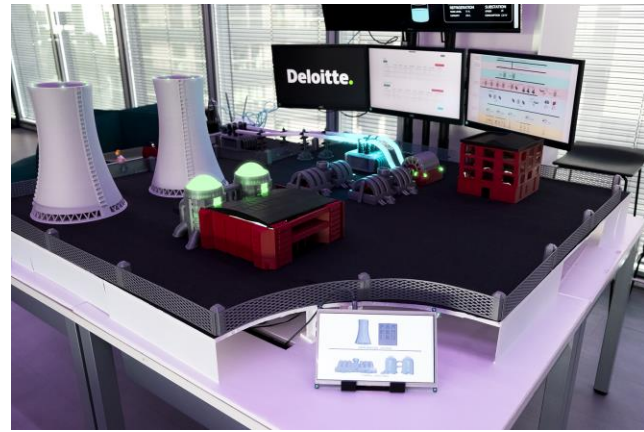
Smart Stadium

CONTACT US
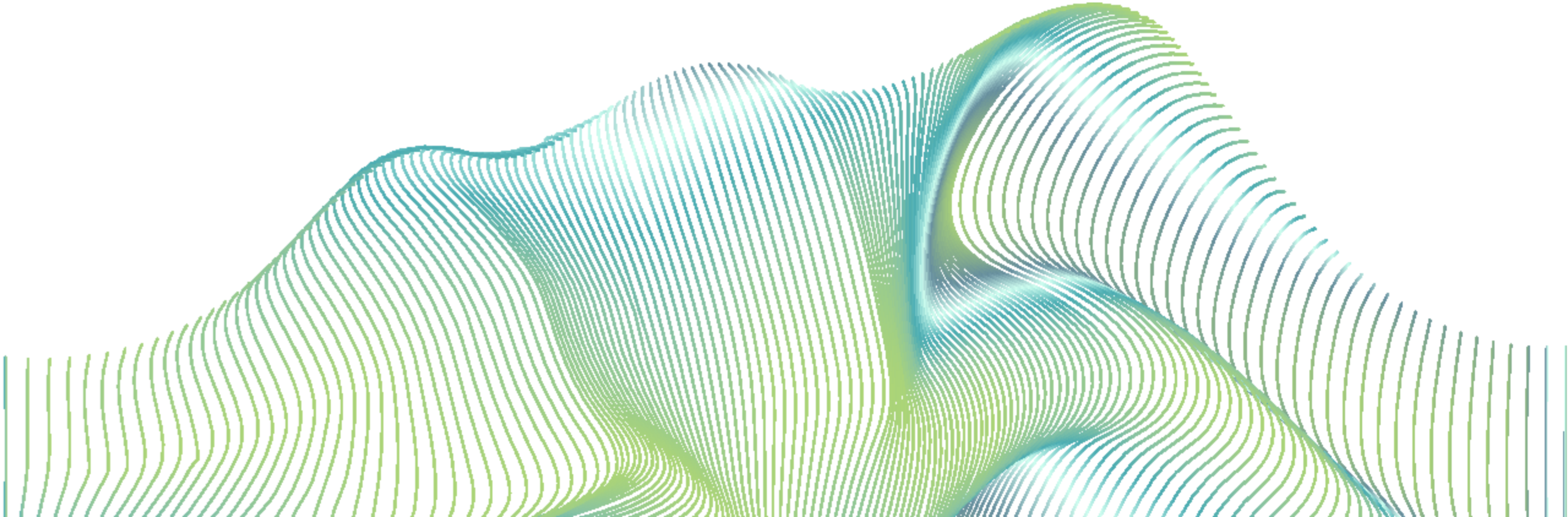
Contact us

César Martín Lara
Managing Partner
Cyber Spain
cmartinlara@deloitte.es
+34 699912931

Edward Moore
Cyber Partner
HUB / CAP
emoore@deloitte.es
+34 686003244

Isaac Núñez
Cyber Partner
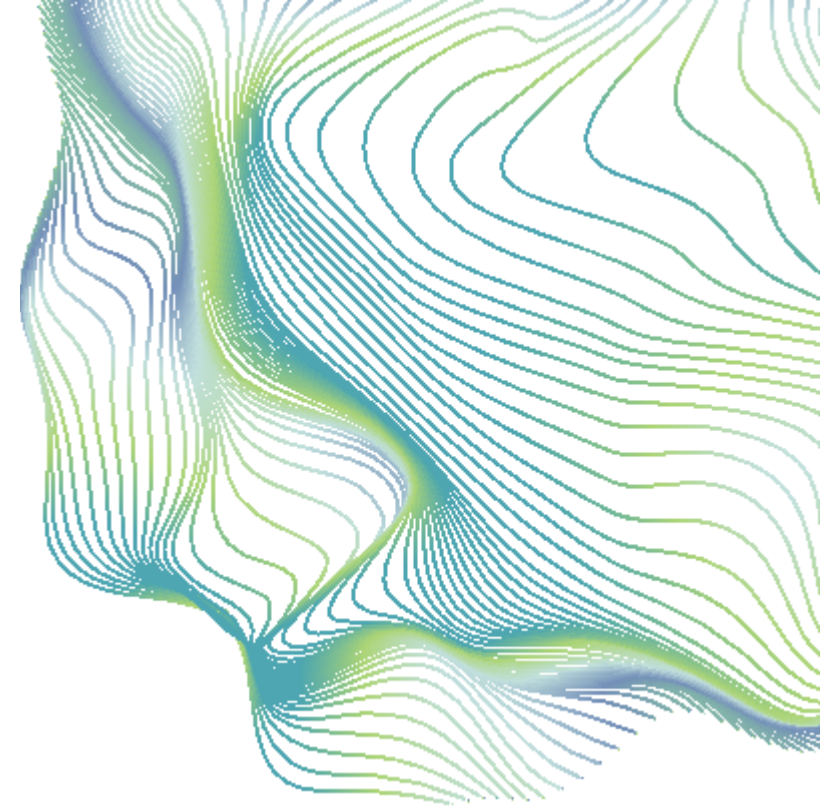Operations
inunez@deloitte.es
+34 667640019

Juan A. Santos
Cyber Partner
EMEA
jsantosgonzalez@deloitte.es
+34 6591498281

Nicola Esposito
Cyber Partner
Non EMEA - Global
niesposito@deloitte.es
+34 6390325860

Deloitte.