

Deloitte.



Cyber Risk Services

Secure success

Operate with resilience. Grow with confidence.

Secure success

Organizations today are not closed off, independent entities. They are hyper-connected parts of bigger collaborative ecosystems. While these open ecosystems may feel risky or complex to manage, the greatest risk organizations face is not leveraging the opportunities they present.

Our technology and business specialists put cyber to work for your organization. They use their breadth of knowledge, from finance to customer experience, to amplify cyber's impact and deliver outsized outcomes.

Our powerful solutions simplify complexity, accelerate innovation, and supercharge transformation. That way, you can operate with resilience, grow with confidence, and secure success for your organization.



We understand your challenges & opportunities.

We'll work alongside you with a full range of services to help you foster innovation for secure and sustainable growth.



We are moving quickly on digital transformation, **moving to the cloud and migrating systems.** Can you help us to make sure they are cyber secure?



How do we effectively manage **the convergence of IT and OT** environments?



How do I prepare our organization for and defend against **today's sophisticated cyberattacks?**



What are **the identity access requirements around cloud** or even a hybrid environment?



Our remote workforce means **1,000s of new devices and endpoints on our networks** and systems, how do we track and manage them all?



How do I manage **the complexity of compliance** with the evolving regulatory environment?



What do we need to do to **improve our existing security operations** to match the current threat landscape?



How can we **create a future of trust** across the enterprise and with our customers?

We listen to your needs.

Our focus on personal relationships, the breadth and depth of our experience, and deep technology and product innovation enable us to bring stakeholders together for increased interoperability and impact.

Whatever your organization's strategic business priorities, we'll help you improve threat awareness and visibility and strengthen your ability to thrive in the face of cyber incidents.

No matter how complex your situation, we'll always listen and work with you to address your questions and find the right answers for your unique needs.

We advise, implement, and manage cyber solutions where you need us most, across your entire enterprise.



Cyber services and solutions

Deloitte offers a fully customizable suite of cyber solutions and managed services. With a commitment to technological innovation and broad industry expertise, our Deloitte global network gives us the insight and experience to face any scenario.

-  Cyber Attack Services (Penetration Testing)
-  Cyber Strategy & Governance
-  Application Security & Digital Identity
-  IT Risk & Audit
-  IT Regulatory Compliance
-  Artificial Intelligence & Data
-  Third Party Assurance & Management
-  Detect & Respond

Cyber Attack Services (Penetration Testing)

Penetration testing helps answering the question: “Can someone break-in my system and take advantage of my data?”

We offer wide variety of penetration testing services to our clients, including Red Teaming, application level- (e.g., Web, API, Mobile, Binary), external and internal infrastructure level- (including on-premise and on cloud solutions) penetration testing services.

From our special cybersecurity lab, we help our clients with connected device testing (e.g., Automotive, Healthcare or IoT) for the whole connected ecosystem, including hardware-, firmware- and interface level penetration testing beside the backend, mobile and API testing.

We also provide penetration testing services for SCADA/OT environments. Our team is capable to handle large penetration testing programs with hundreds of penetration testing.

- Circuit level testing a.k.a. hardware hacking
- Firmware level assessment
- Bus and interface testing, including internal and external communication channels
- Application and backend testing

— **Web Penetration Testing**

— **Mobile Penetration Testing**

— **Infrastructure Penetration Testing**

— **Binary Penetration Testing**

— **Automotive Penetration Testing**

— **Hardware Penetration Testing**

— **OT/SCADA Testing**

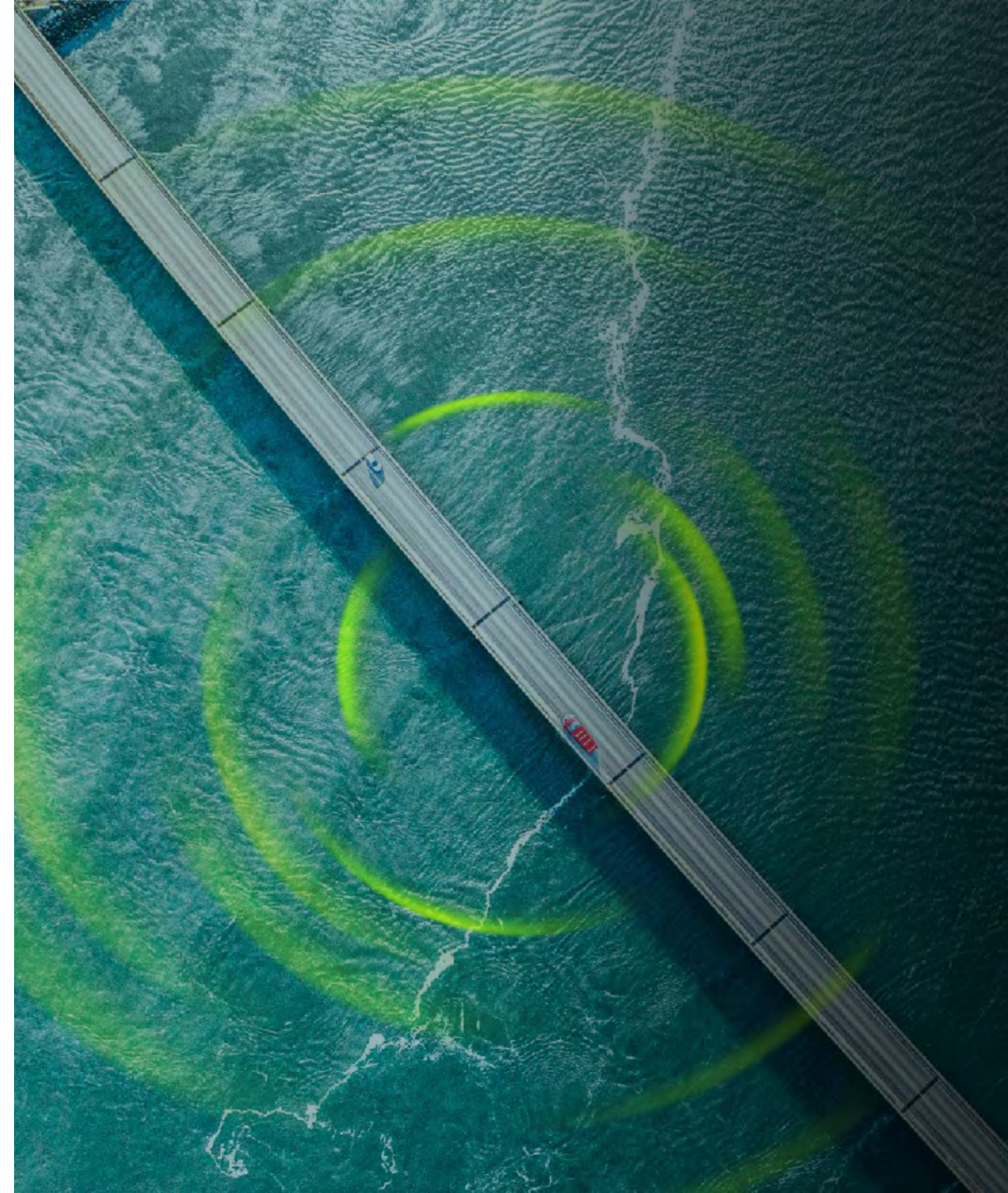
— **Red Teaming**

Cyber Strategy & Governance

Getting a clear picture of your cyber security needs is the first step toward mitigating risk.

We specialize in delivering comprehensive cyber strategy & governance services tailored to safeguard digital assets. From risk assessment to proactive defense planning, our experts craft robust strategies that align with organizational business objectives. With a focus on continuous adaptation, we ensure that companies remain resilient in the ever-evolving landscape of cyber threats. Effective cyber governance is essential for safeguarding confidential information, ensuring business continuity, and maintaining the trust of customers and stakeholders.

- Cyber Strategy Advisory & Benchmarking
- Cyber Risk Assessments
- Cyber Cloud Strategy, Excellence & Architecture
- Business Continuity & Incident Response
- Cyber Security Policy, Cyber Simulations & Awareness Trainings
- Emerging Technologies
- Zero trust



Application Security & Digital Identity

The more applications you run, the more you need a holistic approach to security.

Our teams deploy compliant application security processes, guidelines and mechanisms across all layers and provide comprehensive security baseline across the whole application infrastructure stack and cloud.

We provide comprehensive solutions that empower our clients to control user access, enhance security, and ensure compliance across the whole organization. Our IAM experts design and implement robust frameworks, enabling seamless yet secure user authentication and authorization processes. By centralizing user management and access controls, we help minimize risks, prevent unauthorized access rights, and foster a culture of resilient cyber security.

- **SAP Security & GRC**
- **Identity & Access Management**
- **Business Application Security**

IT Risk & Audit

Technology and the Digital enterprise are the cornerstones for an organization's risk oversight and decision-making processes.

We offer top-tier IT risk assessment & audit services designed to protect the digital landscape. Through detailed evaluations, we identify potential vulnerabilities and threats, providing comprehensive understanding of the risk exposure. Our team delivers actionable insights and recommendations tailored to the unique risk profiles of organizations and advise on leading industry practices based on the results of our security audits.

- ISO 27001 readiness
- ISO 27701 readiness
- Tisax readiness
- IT risk assessments
- Automotive cyber risk assessments
- SOC1 (ISAE 3402) readiness & audit
- SOC2 (ISAE 3000) readiness & audit
- Microsoft SSPA Assessment
- FedRAMP readiness
- NIST 800-53 readiness



IT Regulatory Compliance

Design, assess, transform

We assist our Clients in providing comprehensive IT regulatory compliance audit services to ensure that they meet all the necessary legal and industry-specific requirements. Our expert team conducts thorough assessments of IT infrastructure and practices, identifying potential gaps and vulnerabilities that may lead to compliance issues. We develop tailored solutions and strategies to address these challenges, helping to mitigate risks and avoid costly fines or legal non-compliance. We are able to support organizations to meet requirements including:

PSD2, GDPR, NIS2, DORA, AI ACT.

- DORA
- NIS2
- PSD2
- SWIFT
- AI ACT
- Compliance with the requirements of the Central Bank of Hungary

Artificial Intelligence & Data

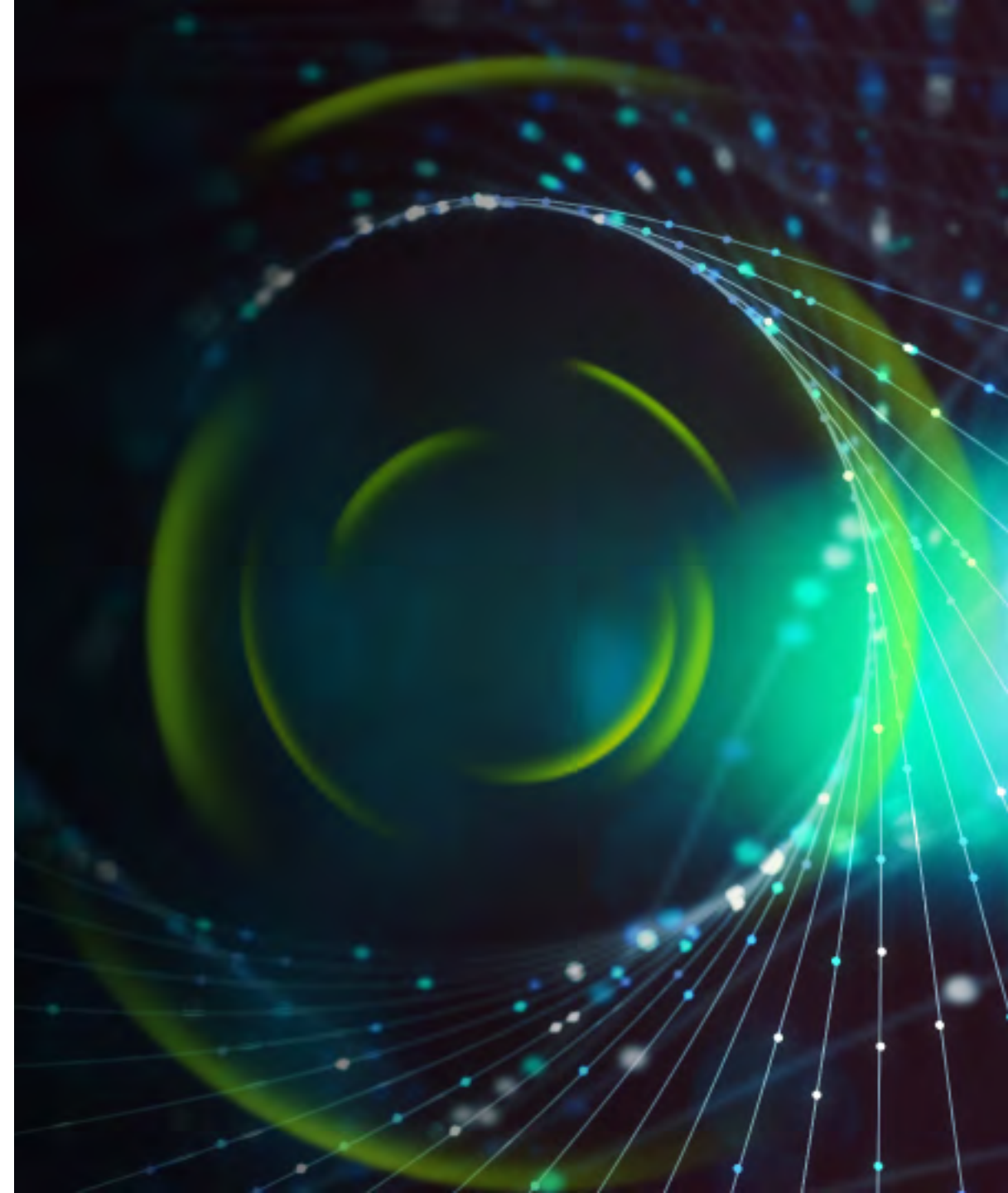
When you harness the power of analytics, automation, and artificial intelligence (AI), you can uncover hidden relationships from vast amounts of data.

Deloitte can assist in performing gap and maturity assessments on processes and controls that guide organizational AI, and identify deficiencies that can lead to potential non-compliance.

Within the AI spectrum, we can perform an ethical risk assessment and gap analysis to identify those solutions that exhibit issues or shortcomings with respect to ethical values and principles.

Deloitte experts also assist their Clients in many aspects of data management, from creating a data management strategy, delivering data deletion solutions to implementing data migration projects.

- AI Strategy
- AI Risk & Governance
- Ethical & Trustworthy AI
- AI ACT & compliance
- Algorithm Assurance
- Data Governance & Management
- Data Protection & Privacy
- OneTrust Technology Platform



Third Party Assurance & Management

A typical Fortune 500 organization may use more than 100,000 external third-parties to meet its business objectives and stay competitive.

Our Third Party Assurance & Management services provide attestation (or advisory) on IT procedures and controls, thus we help Clients to demonstrate their sound internal IT controls. Forms and aim of assurance (or advisory) can vary on a wide range, our experts are ready to help selecting the right one, meeting your needs.

We offer:

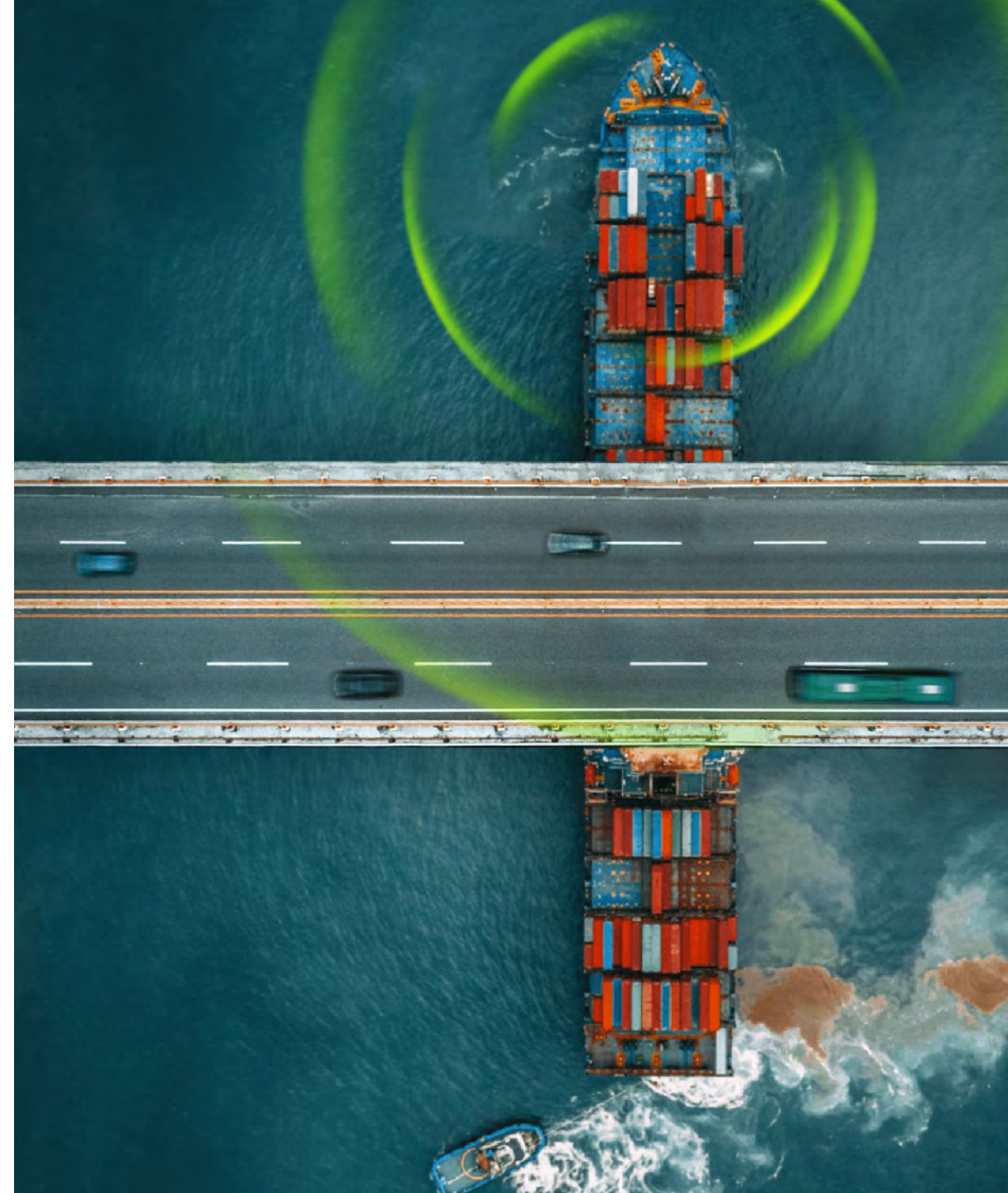
- Service Organization Controls (SOC) 1 reporting (based on ISAE 3402 standard)
- Service Organization Controls (SOC) 2 reporting (based on Trust Service Criteria)
- Vendor risk management
- Algorithm Assurance
- Microsoft SSPA Assessment
- Software Asset Management

Detect & Respond

As cyberattacks grow in frequency and sophistication, you need to outsmart the cybercriminals.

We help organizations detect, contain, and recover from security incidents and breaches. We offer the following regional services to enhance incident management:

- Managed Security Services
- Security Operations Centre
- Detect & Response Governance, Compliance & Architecture



Recognized leader in cybersecurity

Ranked #1 in Market Share for Security Consulting Services based on revenue for 11th consecutive year by Gartner

Source: Gartner, Gartner Market Share Security Consulting Services, Worldwide, 2021

Named a global leader in cybersecurity Incident Response Services by Forrester

Source: Forrester Research, The Forrester Wave™:Cybersecurity Incident Response Services, Q1 2022, By Jess Burn with Joseph Blankenship, Danielle Jessee, Peggy Dostie, Published 28th March 2022

Named a leader in Worldwide Incident Readiness Services by IDC

Source: "IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment", by Craig Robinson and Christina Richmond, November 2021, IDC # US46741420

Named a worldwide leader in Managed Cloud Security Services by IDC

Source: IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment, by Cathy Huang, September 2022, IDC # US48761022

Named a leader in Cloud Security Services in the Asia Pacific region by IDC

Source: IDC MarketScape: Asia/Pacific Cloud Security Services 2021 Vendor Assessment, By Cathy Huang and James Sivalingam, June 2021, IDC #AP47097721e

Named a leader in Canadian Security Services by IDC

Source: IDC MarketScape: Canadian Security Services 2022 Vendor Assessment, by Yogesh Shivhare March 2022, IDC #CA48060922

CONTACTS:



Zoltán Szöllősi | Partner
Risk Advisory
+36209107644
zszollosi@deloittece.com



László Tóth | Partner
Risk Advisory
+36204056501
ltoth@deloittece.com

Visit cyber.deloitte.hu for more information.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.