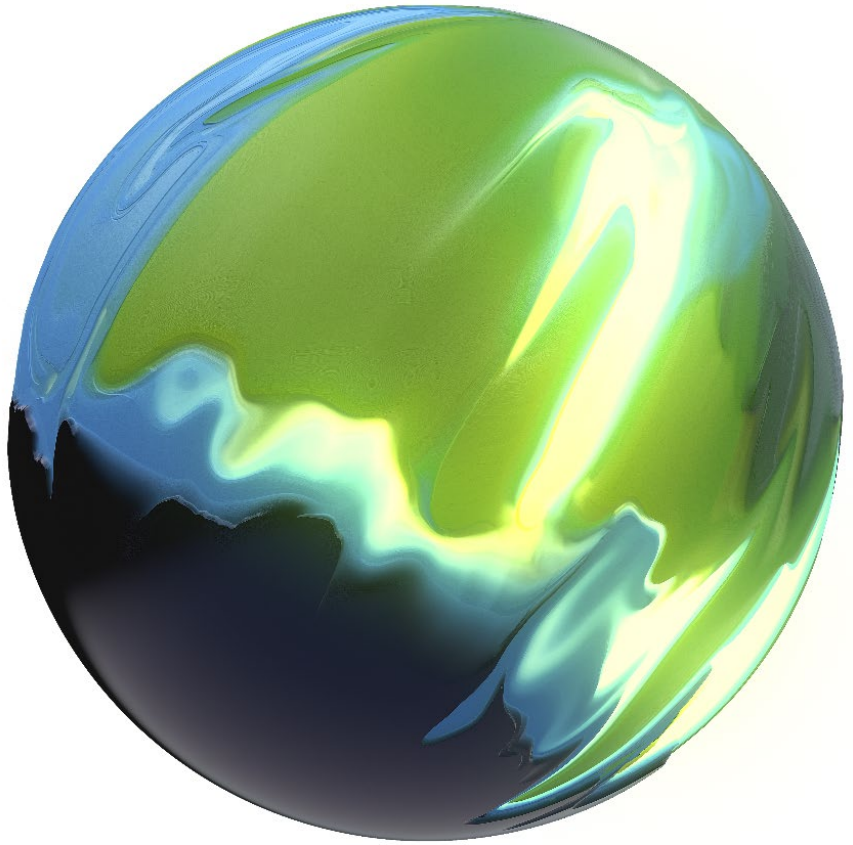
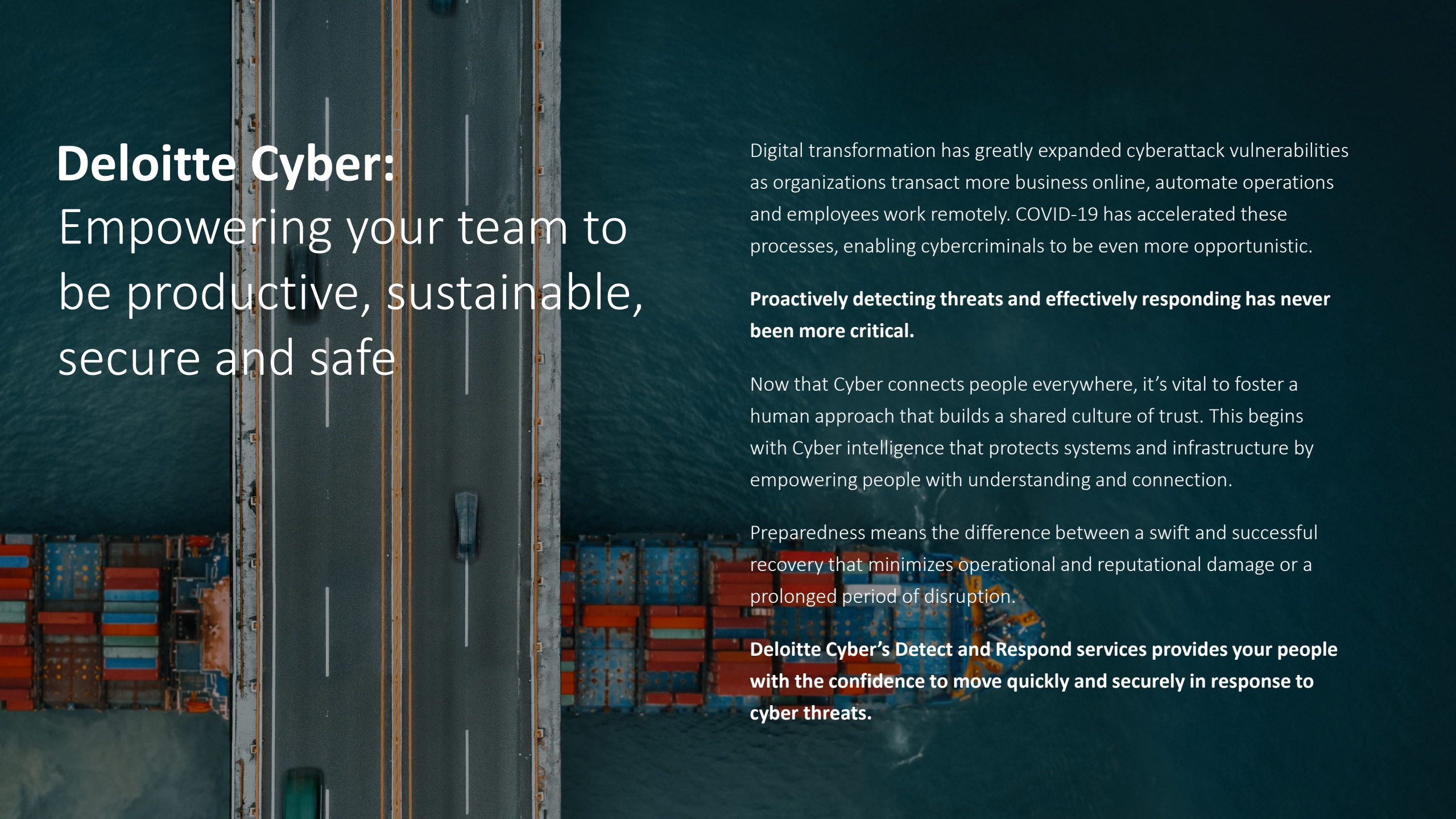
Deloitte.



Detect & Respond:
Staying ahead of cyber threats

Deloitte Cyber | Empowering your people for the future

MAKING AN IMPACT THAT MATTERS since 1845



Deloitte Cyber: Empowering your team to be productive, sustainable, secure and safe

Digital transformation has greatly expanded cyberattack vulnerabilities as organizations transact more business online, automate operations and employees work remotely. COVID-19 has accelerated these processes, enabling cybercriminals to be even more opportunistic.

Proactively detecting threats and effectively responding has never been more critical.

Now that Cyber connects people everywhere, it's vital to foster a human approach that builds a shared culture of trust. This begins with Cyber intelligence that protects systems and infrastructure by empowering people with understanding and connection.

Preparedness means the difference between a swift and successful recovery that minimizes operational and reputational damage or a prolonged period of disruption.

Deloitte Cyber's Detect and Respond services provides your people with the confidence to move quickly and securely in response to cyber threats.

We heard when you asked…

Deloitte Cyber understands the nature of the threats you confront and their potential impacts. We'll work alongside you to help you anticipate, respond and recover.

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

Remote work increases our attack surface with every new device accessing our networks. How can we **track and manage** them all?

What do we need to **integrate threat intelligence** with security event monitoring?

How can we automate processes and operations to **optimize resources and reduce costs** while improving outcomes?

How can we **improve our existing security** operations to match the current threat landscape?

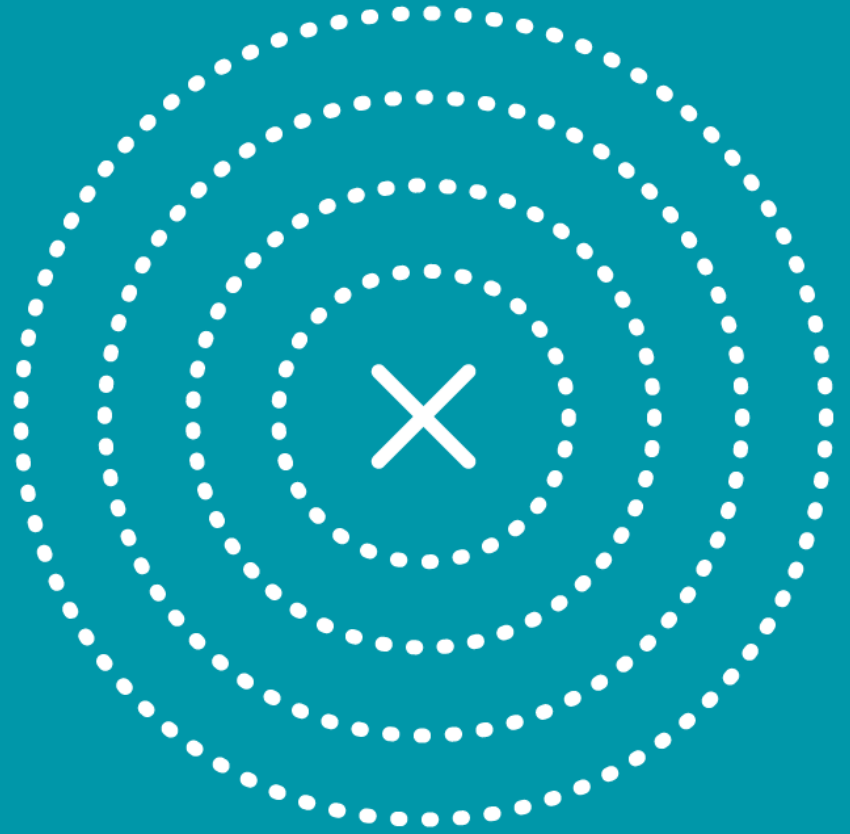
How do we **gain visibility of the entire threat landscape** including internal (HR, users, databases, cloud) and external data (social media, dark web)?

As we move to Industry 4.0, what can we do to **detect and respond to new threats?**

24/7 Cyber detection and response

We can be your eyes and ears, scanning the threat landscape. The intelligence we gather from security technologies, social media, the dark web and beyond enables us to understand potential impacts to your organization. We translate this knowledge into controls to monitor then mitigate specific threats.

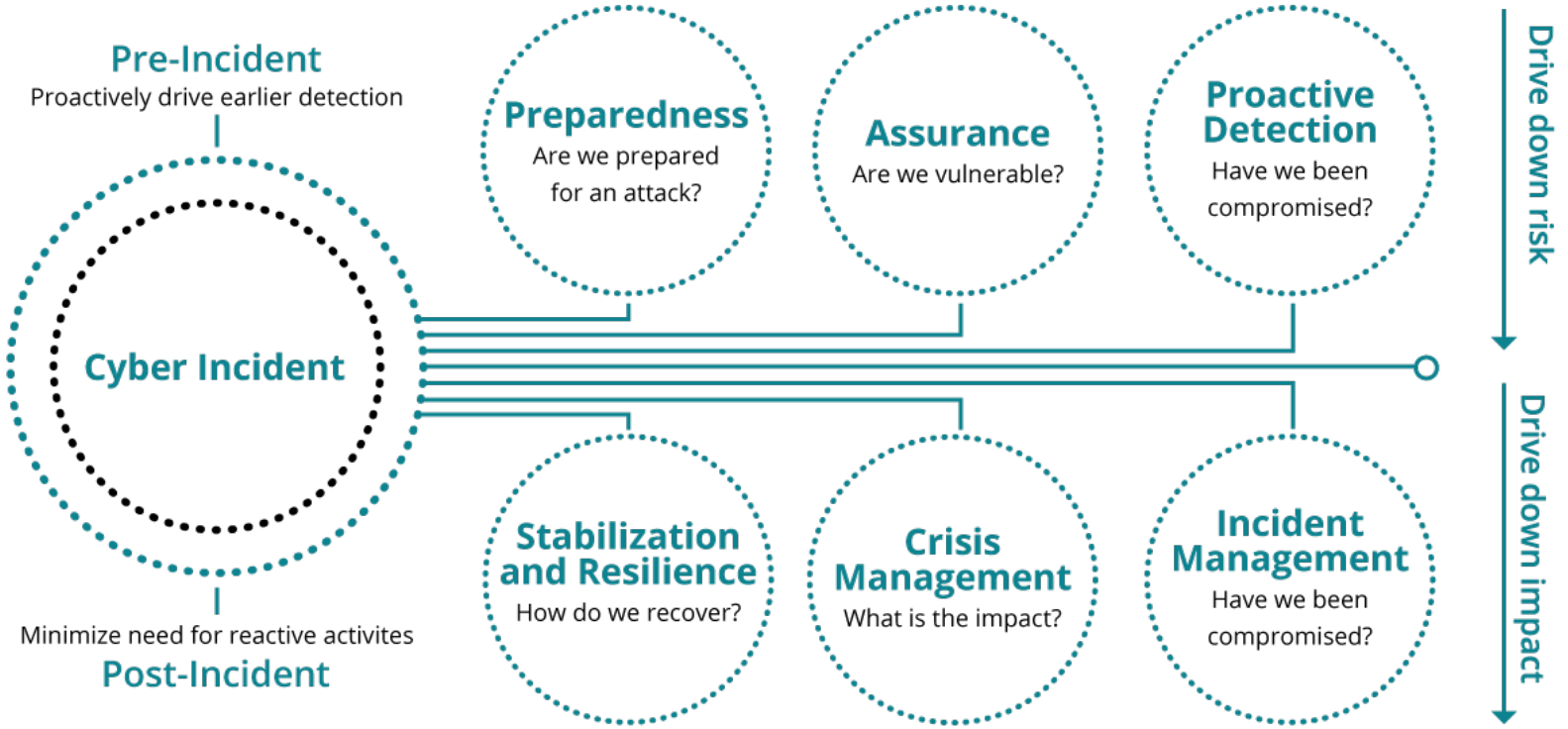
This comprehensive approach enables us to assess, triage and escalate critical incidents so we can effectively respond to threats before they inflict financial, operational and reputational damage.



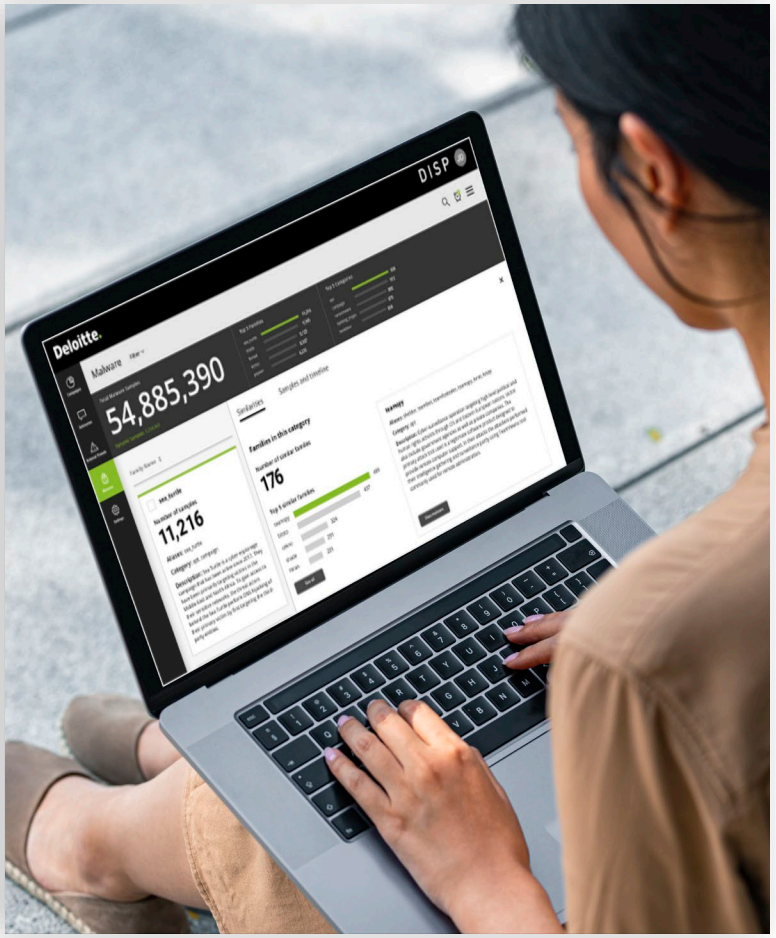
Methodology

Deloitte has created a methodology and service portfolio to drive your security operations in an evolving threat environment.

Together, they deliver more effective and faster detection, the most appropriate response plus the maximum return on investment.

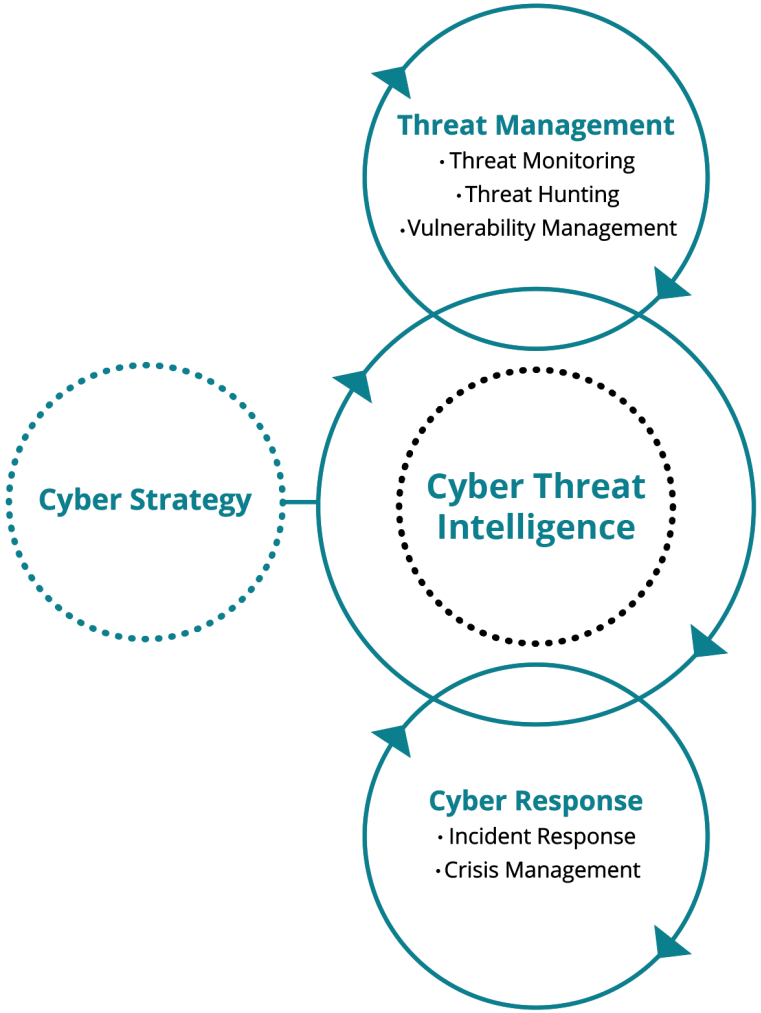


Intelligence-driven



Effectively operationalizing intelligence requires breaking out of a siloed approach to threat management and leveraging intelligence to drive decisions across your organization.

We provide you with evidence-based knowledge about existing or emerging threats in a timely, accurate, relevant and predictive manner. You stay informed and your decisions are enhanced at every level. Our proprietary Deloitte Cyber Threat Intelligence, derived from our global network's analysis, is manually validated prior to being distributed to our clients.



Detect & Respond services and solutions

- THREAT INTELLIGENCE
- THREAT DETECTION AND RESPONSE
- ATTACK SURFACE MANAGEMENT
- INCIDENT RESPONSE
- THREAT HUNTING
- CYBER OPERATE

THREAT INTELLIGENCE

Whether driven by emerging hostile tactics or shifts in your business priorities, Deloitte Cyber gives you greater visibility into the evolving threat landscape, being uniquely protected by our self-produced intelligence.

You'll stay ahead of danger with:

- **Global emerging threats monitoring:** Coming from our internal analysis and manual investigations conducted by our global research team and thanks to our wide network of clients and partners.
- **Brand targeted threats monitoring:** A focused lens on your specific threats and exposure.
- **Advisory services:** We work with you to support your threat intelligence needs at every stage helping your company to identify priorities and properly consume your intelligence sources.

Our manual and tailored analyses are based on your unique environment. Remain informed with up-to-date internal and external threat intelligence reporting complemented with research targeted by industry, company and adversary profiling. You'll receive:

- 24/7 threat notifications of relevant threats
- Mitigation measures such as takedowns
- External threat visibility
- Malware analysis and observables feed
- Risk mitigation recommendations
- IoT/OT device intelligence
- Context for SIEM use cases and threat hunting activities

THREAT DETECTION AND RESPONSE

Get a detailed picture of the cybersecurity environment that allows you to focus on risk management and outcomes tailored to your business.

We develop a customized approach based on your risk tolerance and threats. By enriching your internal data sources, we'll enhance detection of targeted attacks as well as uncover insider threats.

You can choose to engage with us via a flexible range of models from on-premise to private and public cloud services. Plus, adaptable staffing and talent alternatives can mitigate costs and risks.

- 24x7 cyber threat monitoring
- Alert triage and escalations
- Threat modeling and custom use case and playbook development
- Risk-based reporting and reviews
- IT, OT, IoT and cloud threat monitoring
- Cloud native threat monitoring
- Second Arm of Security Operations (SOAR) as a service
- Managed Endpoint Detection and Response (EDR)
- Security Incident and Event Management (SIEM) and User Behavior Analytics (UBA)

ATTACK SURFACE MANAGEMENT

The attack surface is comprised of the components of your environment that are exposed for exploit. Through asset identification, service fingerprinting and vulnerability scanning, we help you define specific risk areas, identify high priority security and compliance issues and orchestrate remediation efforts.

Our careful attention to risk and performance metrics means we can provide decision support to help you fully build out your cybersecurity program.

We incorporate the results of continuous testing through managed services and intelligent automation into threat detection and response activities. You'll benefit from:

- IoT and OT penetration testing
- Prioritizing threats for remediation with risk and performance metrics
- Shortening dwell time through prompt remediation of vulnerabilities
- Network and cloud asset discovery
- Offensive security
- Red and blue team exercises
- Attack surface reduction
- Attack Path Modeling

INCIDENT RESPONSE

Because of our deep experience across industries, we deliver clarity and confidence when it really matters.

We take care of pre- and post-incident support so you can focus on recovery and transformation.

Our incident response services, knowledge of threats and global reach enable us to better minimize impact and help restore trust in your organization. Our end-to-end service offerings include:

- Incident advisory and defensibility
- Response and forensic analysis
- Trust restoration
- Post-incident response
- Communications

THREAT HUNTING

We'll help you uncover attacks that might fall under the radar of traditional security tools.

We develop a customized approach based on your risk tolerance and threats. By enriching your internal data sources, we'll enhance detection of targeted attacks as well as uncover insider threats.

Our skilled teams investigate and triage potential threats and help remediate them in a timely manner. The hunt can be another periodical level on monitoring, threat intelligence-based or post incident. You'll stay ahead of threats with:

- Malware detection—reduce risks of malicious activity
- Internal threat visibility for indicators of compromise
- Detecting and responding to advanced threats
- Detailed and actionable forensic investigation reports
- Integration with threat monitoring and threat intelligence

CYBER OPERATE

You can turn to Deloitte Cyber to provide your security needs as a managed service with Cyber Operate.

Deloitte can offer dedicated, on-premise or leveraged support with its offshore talent models and shared resource pool. You can leverage our service to fully optimize your security budget. Plus you can take advantage of our industry and cross-industry lessons learned to avoid costly customizations, one-off designs and implementations that are difficult to maintain.

Not only does Cyber Operate bring you efficiency gains and reduce costs, our service delivers a host of additional benefits.

Stability and predictability of operations

- Reduce outages through preemptive maintenance and monitoring
- Simplify processes by applying industry knowledge and data-driven feedback on operations
- Alleviate dependence on hard-to-find and retain specialized skill sets

Technology simplification

- Analyze operations data and business outcomes to identify then resolve issues
- Introduce enhancements derived by data analysis to achieve cybersecurity goals
- Provide prioritized recommendations to automate manual, time consuming processes based on service requests and incidents

Sustainable and scalable operating models

You can tailor our globally-managed services support models to your needs.

If you need to scale rapidly, Cyber Operate lets you flex on demand cost effectively with a leveraged offshore model that addresses spikes, enables growth, and onboards new capabilities.

Global service, locally delivered

Cyber connects everyone in your organization, wherever they are located. Around the world, we can help you shape smarter processes and platforms with greater insight, agility and resilience to threats.

Our global network gives us the depth and breadth of experience in dealing with many of the world's toughest cyber issues while tailoring our offering to meet your regional needs.

Deloitte's Operate services support the business need for hosted and managed security solutions across the spectrum of enterprise-wide Cyber capabilities. The strategy is built around a global network of five regional centers in collaboration with more than 30 local Cyber Centers. This network allows us to be a global partner, maintaining a local approach in order to tailor our offering to the needs of the client in each country.

By seeing that cyber works effectively for each person, we help you grow a culture of safety and trust, so your entire business can move forward with confidence.

A recognized leader in Cybersecurity

- Ranked **#1 globally in Security Consulting,**
  10 consecutive years based on revenue by Gartner
  Source: Gartner, Market Share Analysis: Security Consulting Services Worldwide, 2020, Elizabeth Kim, April 2021

- Named a **global leader in Cybersecurity Consulting Services** based on strategy and for the 5th consecutive wave by Forrester
  Source: Forrester's Wave™: Global Cybersecurity Consulting Providers, Q2 2019

- Deloitte named **a global leader in Worldwide Managed Security Services by IDC**
  Source: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment (doc# US46235320, September 2020).

- Named a **global leader in Cybersecurity Consulting** by ALM Intelligence for 6th consecutive year
  Source: ALM Intelligence; Cybersecurity Consulting 2019; ALM Intelligence estimates © 2019 ALM Media Properties, LLC. Reproduced under license

- **Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

Deloitte Cyber Detect and Respond Leaders

Dwayn Lythgo | Asia Pacific
+65 68004778
dlythgo@deloitte.com

Rocco Galletto | Canada
+1 4166438718
rgalletto@deloitte.ca

Murat Yildiz | Central Europe
+49 6211590125
myildiz@deloitte.de

Nicola Esposito| Global
+134 918 232 431
niesposito@deloitte.es

Tim Erridge | North and South Europe
+44 2073033872
terridge@deloitte.co.uk

Isaac Kohn| United States
+41 582797574
ivkohn@deloitte.ch

www.deloitte.com/cyber

Deloitte.

Click Here to learn more about Deloitte Cyber