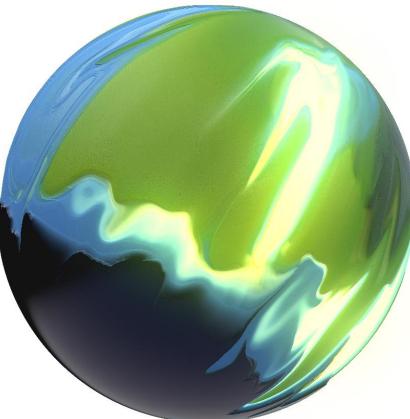
Deloitte.



Detect and Respond:

Staying ahead of cyber threats

Empowering your people for the future

Risk Advisory's Cyber Practice:

Empowering your team to be productive, sustainable, secure, and safe

Digital transformation has greatly expanded cyberattack vulnerabilities as organisations 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.

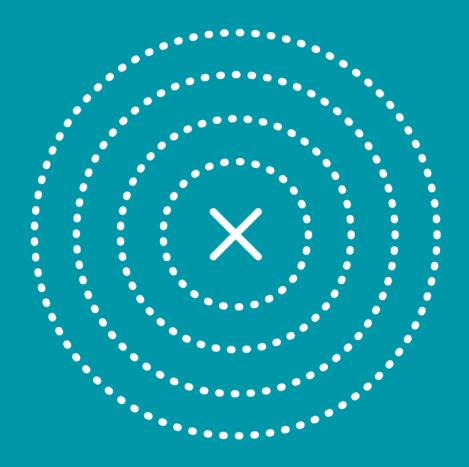
Preparedness means the difference between a swift and successful recovery that minimises operational and reputational damage or a prolonged period of disruption.

Our Detect and Respond services provides your people with the confidence to move quickly and securely in response to cyber 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 organisation. We translate this knowledge into controls to monitor and 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.



We understand your issues and requirements

66	66	66
Remote work increases our attack surface with every new device accessing our networks. How can we track and manage them all?	How do we scale up our threat intelligence capabilities?	How can we automate processes and operations to optimise resources and reduce costs while improving outcomes?
66	66	66
How can we improve our existing security operations to match the	How do we gain visibility of the entire threat landscape including internal	As we move to Industry 4.0, what can we do to detect and respond to new

Based on this understanding, our service offerings help you

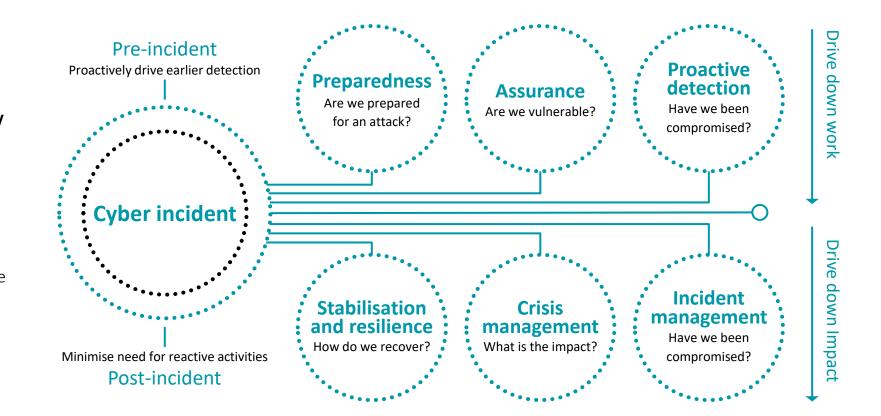
- Identify the critical vulnerabilities *swiftly*
- Manage your attack surface comprehensively

- Detect and respond to threat *ably*
- Prepare your teams to respond to incidents *effectively*

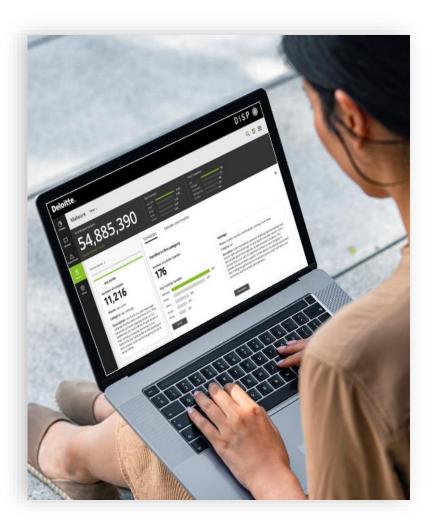
Our methodology

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.

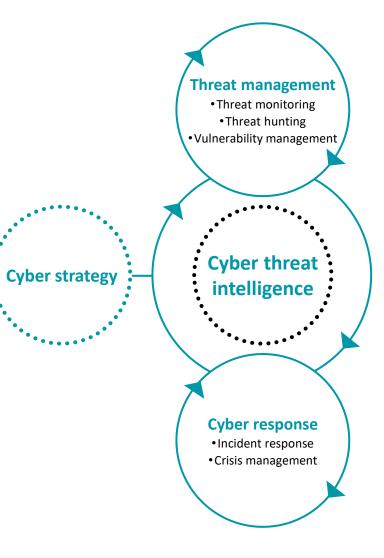


Intelligence-driven capabilities



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

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 Threat Intelligence, derived from our global network's analysis, is manually validated prior to being distributed to our clients.



Detect and respond services and solutions

Threat intelligence

 \bigcirc

- Threat detection and response
- Threat hunting
- Attack surface management
- Cyber simulations
- Incident response



Whether driven by emerging hostile tactics or shifts in your business priorities, cyber gives you greater visibility into the evolving threat landscape, being uniquely protected by our selfproduced 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 wide network of clients and partners.
- **External threat monitoring:** A focused lens on your organisation and brand-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.

Threat intelligence

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
- External threat visibility
- Mitigation measures such as takedowns
- Threat Intelligence feed
- Risk mitigation recommendations
- IoT/OT device intelligence
- Context for Security Incident and Event Management (SIEM) use cases and threat hunting activities

Threat detection and response

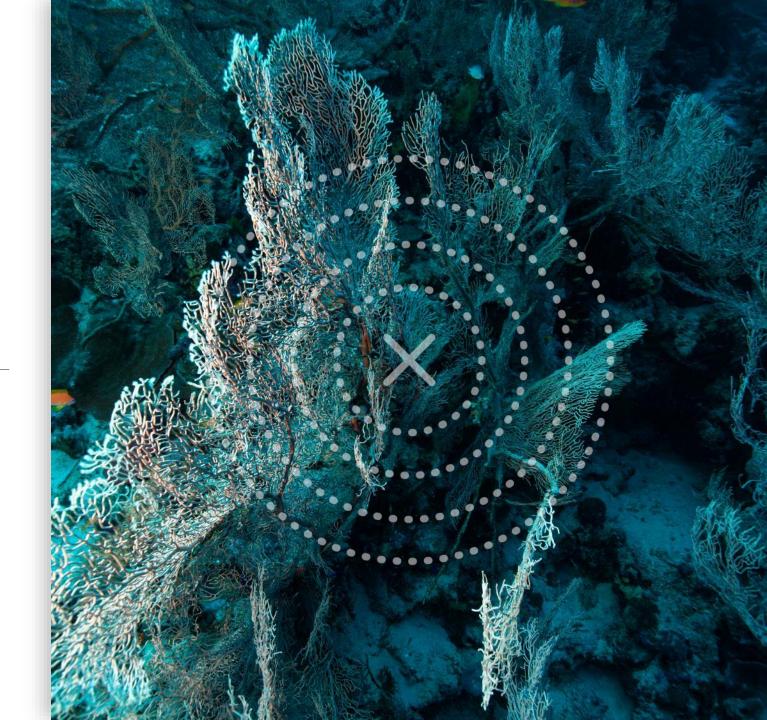
Get a detailed picture of the cybersecurity environment that allows you to focus on risk management and outcomes tailored to your business.

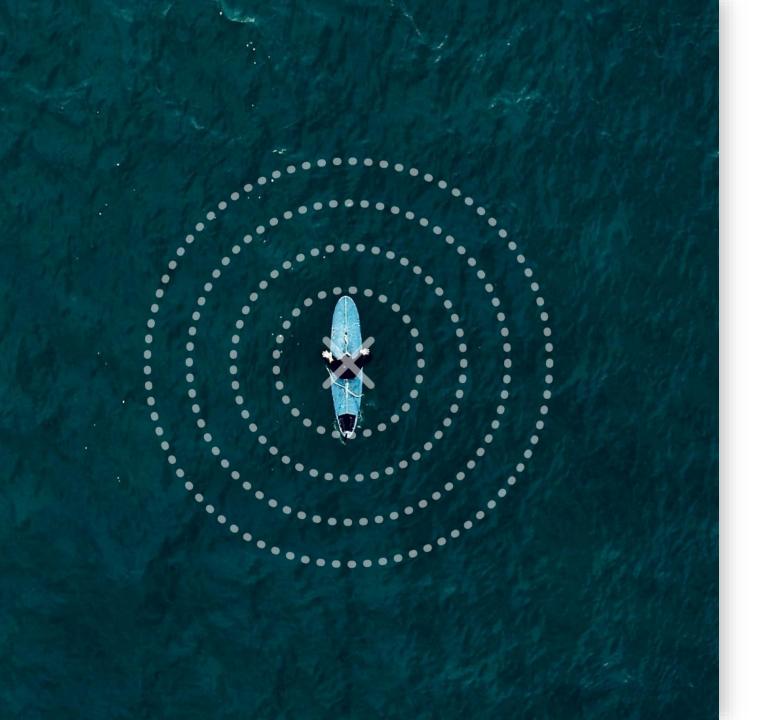
We build on an industry leading approach tuned to your risk tolerance, threats, and encompassing your business context. By providing coverage across your IT and even OT environment, we speed up detection and response to generic and targeted attacks.

You can choose to engage with us via a flexible range of models from fully managed services to hybrid and captive service models. Plus, adaptable staffing and technology optional help control costs and mitigate risks.

- 24x7 cyber threat monitoring
- Alert triage and escalations
- Mature use case and playbook library
- Risk-based reporting and reviews
- Hybrid IT and cloud threat monitoring

- OT/ICS Threat monitoring
- Automated Incident Containment
- Managed Extended Detection and Response services (XDR)
- SIEM and User Behaviour Analytics (UBA)





Threat hunting

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

We develop a customised approach based on your risk tolerance , potential adversaries, and threats. By enriching your internal data sources, we'll hunt for targeted attacks as well as uncover insider threats.

Our skilled teams work with you to identify your key adversaries and threats that matter and then scope hunts. These can be an addon to the monitoring or conducted on a periodic basis separately. Infused with timely threat intelligence, you will stay ahead of threats with:

- Reduction in risks of malicious activity
- Internal threat visibility for indicators of compromise
- Detecting and responding to advanced threats
- Options to choose between onetime or periodic hunts
- Integration with threat monitoring and threat intelligence



Attack surface management

We help you define specific risk areas, identify high priority security and compliance issues, and orchestrate remediation efforts.

Through asset identification, service fingerprinting, and vulnerability scanning, we enumerate the components of your environment that make up the attack surface and may be exposed to exploitation.

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

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

- Intelligent Risk Assistant driven Vulnerability Assessment and penetration testing
- Prioritising threats for remediation with risk and performance metrics
- Shortening dwell time through vulnerability programme management

- IoT and OT Penetration Testing
- Offensive security
- Red and blue team exercises
- Attack surface reduction
- Threat Modellling

Cyber simulations

Our cyber simulations assess your controls and processes during simulated attacks to identify their effectiveness, detect any gaps, and prepare your people for what's coming next.

Our expert-built simulations and war gaming exercises enable you to take advantage of our industry and cross-industry lessons learned, based on our real-world experiences delivering incident response services.

You will benefit from:

- Exposure to real world adversary Tactics, Techniques, and Procedures (TTPs) enabling an active engagement and enhancing the knowledge of your teams
- Evaluation of your incident preparedness
- Improvement of your team's cohesiveness to work during incident investigations via best practice led cyber range simulations and training programmes



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 minimise the impact of an attack and restore trust in your organisation. Our end-to-end service offerings include:

- Incident Response Plan
 Development
- Incident Response Services
- Compromise Assessments

- Crisis Management
- Post Incident Support
- Cyber Forensics



Global service, locally delivered

Cyber connects everyone in your organisation, wherever they are located.

We have built our cyber business around a diverse **global network** of risk advisory professionals with **17,000+** Globally and **3,000 + in India**.

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 our client's regional needs.

Deloitte has built a global network of **33** Cyber Intelligence Centres with **2** CICs in India at Hyderabad and Gurugram. This network allows us to be a global partner, maintaining a local approach in order to tailor our offering to the needs of the Indian clients.

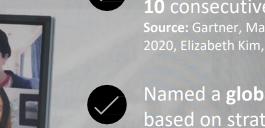
By seeing that cyber works effectively for each person, we help you grow a culture of safety and trust, so your entire business can move forward with confidence.



Panoramic Snapshot of Deloitte CIC in National Capital Region (Gurugram)

- ISO 27001, ISO 9001, ISO 22301 certified facility
- 24x7x365 operations and remote management services
- Highly skilled and expert professionals with industry leading certifications at respective levels
- Standardisation with other global CICs
- Completely segregated environment to ensure data confidentiality and continuous research and development

A recognised 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 organisation 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.



Anthony Crasto

President, Risk Advisory Deloitte India acrasto@deloitte.com

Kamaljit Chawla

Leader – Cyber Operate Risk Advisory, Deloitte India kamaljitc@deloitte.com

Om Ahuja

Partner, Risk Advisory Deloitte India <u>omahuja@deloitte.com</u>

Abhijit Katkar

Partner, Risk Advisory Deloitte India akatkar@deloitte.com

Harjinder Singh Takher Partner, Risk Advisory Deloitte India

harjinders@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities 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.

© 2024 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited