



Cyber Incident Response (IR) Navigator

AI-driven insight. Confident incident response.

Deloitte's Cyber IR Navigator uses advanced artificial intelligence (AI), comprehensive threat intelligence, and real-world incident data to guide organizations through cyber crises with speed and confidence. Providing tailored insights, streamlined incident management, and automated workflows—it enables rapid, informed decisions to stop the attack and accelerate recovery.



The challenge

Today's cyber incidents are more complex, fast-moving, and higher-stakes than ever before.

Expanding digital ecosystems, stakeholder expectations, mounting regulatory demands, and the relentless pace of the threat have rendered traditional incident response approaches ineffective. Organizations must now navigate hundreds of simultaneous critical decisions—often under intense pressure and with incomplete information—to manage cybersecurity incidents, minimize business impact, and restore operations quickly.

AI-powered integration for confident cyber incident response & recovery

The IR Navigator is an AI-powered platform that enables Deloitte teams to respond to cyber incidents rapidly and confidently. Acting as a semi-autonomous platform, it provides real-time, tailored insights by drawing from a vast repository of incident and threat intelligence sources from Deloitte's global network, third-party, public, and proprietary threat data.

Key features include:

Guided Response

Provides adaptive, role-based guidance, AI-driven playbooks, integrated support, and scenario modeling to help stakeholders manage incidents with clarity and compliance.

Integrated Incident Management

Gives incident response teams a unified, automated platform for managing data, workflows, and stakeholders, enabling seamless coordination and informed decision-making across all functions.

Advanced Data Analytics & Benchmarking

Transforms incident data into actionable insights by benchmarking, analyzing metrics, forecasting timelines, and highlighting priorities for faster, more effective responses.

Intelligence Integration

Delivers real-time threat intelligence, uses advanced language models for attacker analysis, and offers recommendations tailored to specific industries, locations, and regulations.

Business Impact Mitigation

Delivers structured, data-driven insights and continuous access to key metrics, empowering smarter decisions and reducing financial and operational impact.

Streamlined Process & Reporting

Streamlines IR with automated response playbooks, real-time dashboards, customizable reports, and post-incident reviews for ongoing improvement and compliance.



The Deloitte difference

EMBEDDED INDUSTRY INTELLIGENCE

The IR Navigator combines decades of incident response expertise with cutting-edge AI. Deloitte's platform uses intelligent algorithms to analyze industry data, real-world scenarios, and active threats—delivering tailored, context-aware guidance for every incident. AI ensures the Navigator automatically aligns response strategies to each organization's regulatory, operational, and risk environment, enabling rapid, informed action shaped by proven intelligence.

INTEGRATED WITH LEADING-EDGE SOLUTIONS

Deloitte brings a comprehensive suite of cybersecurity services, spanning proactive readiness, incident response, and recovery. The IR Navigator seamlessly aligns with Deloitte offerings such as Cyber Incident Readiness, Response, and Recovery (CIR3); Managed Extended Detection & Response (MXDR) by Deloitte; AI-driven cyber analytics; and proprietary tools such as TrustIQ. It also benefits from our deep alliances with technology leaders, through an ecosystem that helps us deliver integrated, scalable cyber solutions.

DELIVERED BY GLOBAL, MULTIDISCIPLINARY TEAMS

With a global reach and local presence, Deloitte provides rapid support wherever a cyber event unfolds. Our multidisciplinary model integrates advanced AI-driven detection and analysis with specialized cybersecurity talent, deep industry knowledge, and seamless access to legal, audit, risk, tax, communications, and advisory professionals. This blend of human expertise and AI delivers holistic support—empowering organizations to respond to incidents, meet regulatory obligations, and protect their reputation with greater speed and precision.

The IR Navigator in action: A treatment plan for a ransomware attack

Unusual network activity at a large North American hospital indicated a cyber incident was unfolding. Within hours, a widescale ransomware “detonation” threatened to leave systems and data inaccessible. Unaddressed, the attack could put patients’ lives and health at risk, and force staff to rely on manual processes such as hand-written notes for recording and sharing critical information.

The solution

Deloitte used the IR Navigator to provide benchmarking and analytics for planning each phase of incident response. Through AI-driven response playbooks, the platform outlined specific steps, including remediation reminders and alerts for engaging stakeholders. Leveraging the platform, Deloitte was able to quickly isolate and investigate the threat—seeking entry points, identifying dropped tools, determining patient data impact, and rebuilding systems.

Impact

Working with Deloitte, the hospital isolated ransomware within days, returning to baseline operations within one week and achieving complete recovery at two weeks. The hospital achieved: streamlined, accelerated incident response; increased confidence addressing threats; an enhanced ability to protect operations and mission; greater resilience for critical systems; and improved cybersecurity posture for future threats.

Delivering impact with the IR Navigator



Streamline and optimize response

Automate and elevate every phase of incident response with real-time intelligence, data-driven methodologies and playbooks, and seamless coordination.



Accelerate response, containment, and recovery

Rapid insights and workflow automation mean faster remediation, reduced disruption, and lower costs.



Strengthen reporting and compliance

Generate tailored, audit-ready reports and streamline responses to regulatory requests.



Enhance strategic decision-making

Enable incident response teams to prioritize high-value actions with AI-powered recommendations and a unified view of incident activity.



Protect reputation and trust

Safeguard brand reputation and build trust with customers, regulators, and stakeholders through proactive communication, transparent reporting, and defensible action plans.



Advance resilience for the future

Build the agility and intelligence required to adapt and thrive in a dynamic cyber risk landscape.

Counter cyber attacks with speed and confidence

To learn more, visit www.deloitte.com/CIRNavigator, or contact our team today.



John Gelinne
Global Cyber Resilience
Deloitte Global
jjgelinne@deloitte.com

Marco Manglaviti
IR Navigator Development Lead
Deloitte Canada
mmanglaviti@deloitte.ca

INDUSTRY RECOGNITION

#1

Ranked No. 1 in Security Services Worldwide by revenue in Gartner® Market Share Report, 2024.¹

Named a **leader in Worldwide Cybersecurity Incident Response Services** by IDC MarketScape²

Named a **leader in Worldwide Data Protection and Governance Services** by IDC MarketScape³

Endnotes

1. Gartner, Market Share: Security Services, Worldwide, 2024, By Rahul Yadav, Shailendra Upadhyay, Akshita Joshi, Tarun Rohilla, Bryan Haley, 25 April 2025. 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 accuracy, completeness, or reliability.

About 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.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member