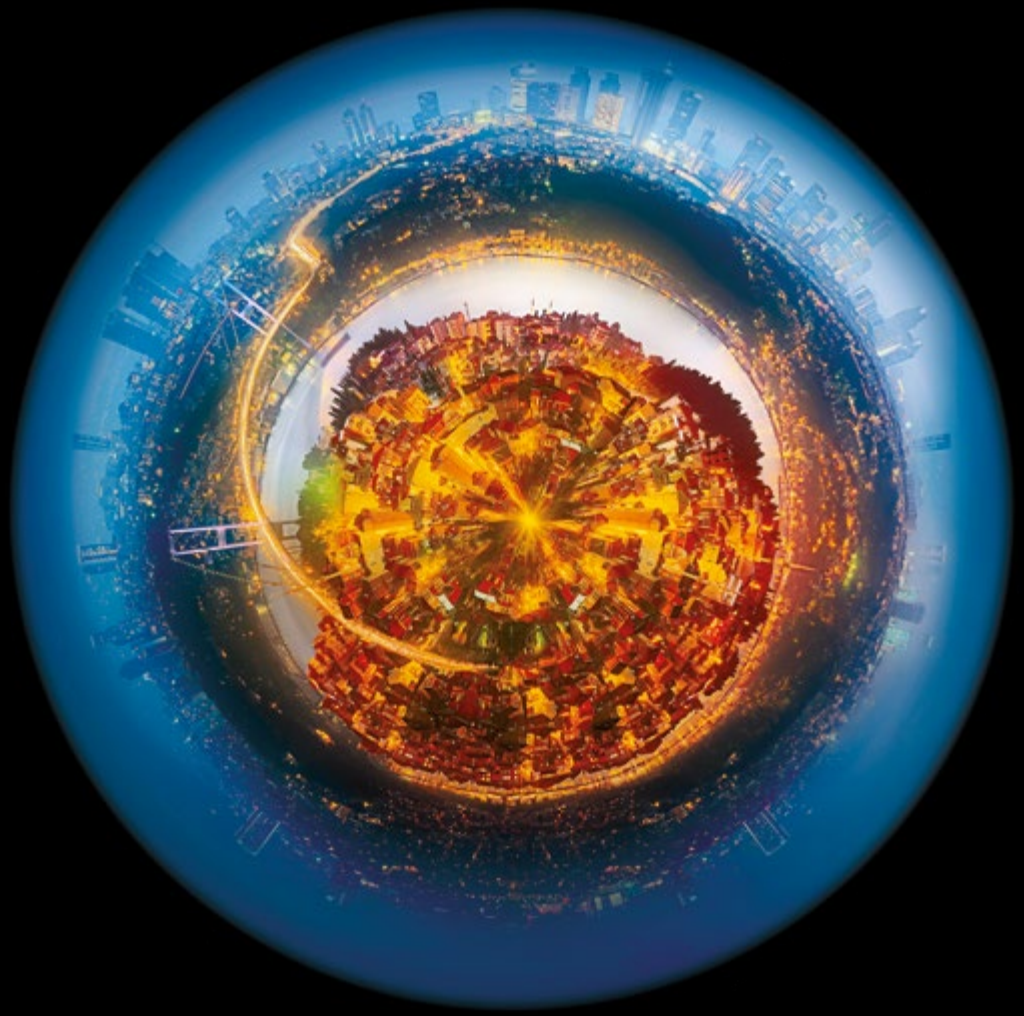
Deloitte.



Deloitte Cyber Risk capabilities in EMEA

Cyber Strategy, Secure, Vigilant and Resilient

Cyber Risk

Contents

Foreword

In an era of rapid digital transformation and proliferation of ever increasing amounts of data, cybersecurity is becoming an ever greater priority for organizations of all sizes and in all industries.

Our strategy aims to increase the impact and success of our cyber business with our most important clients whilst delivering a significant and positive impact to society that matters.

Deloitte's experience demonstrates that clients implementing cybersecurity models that anticipate threats not only deal more effectively with them. They also achieve better business results, reflected in growth in their bottom lines.

Our practitioners provide capabilities across the four main domains of cybersecurity - Cyber Strategy, Secure, Vigilant and Resilient.

Deloitte's alliances with many vendors in the cybersecurity market provide it access to a range of technologies.

These strengths enable us to collectively deliver a large number of projects every year in advisory, implementation and managed services tailored to the precise, individual needs of each client.

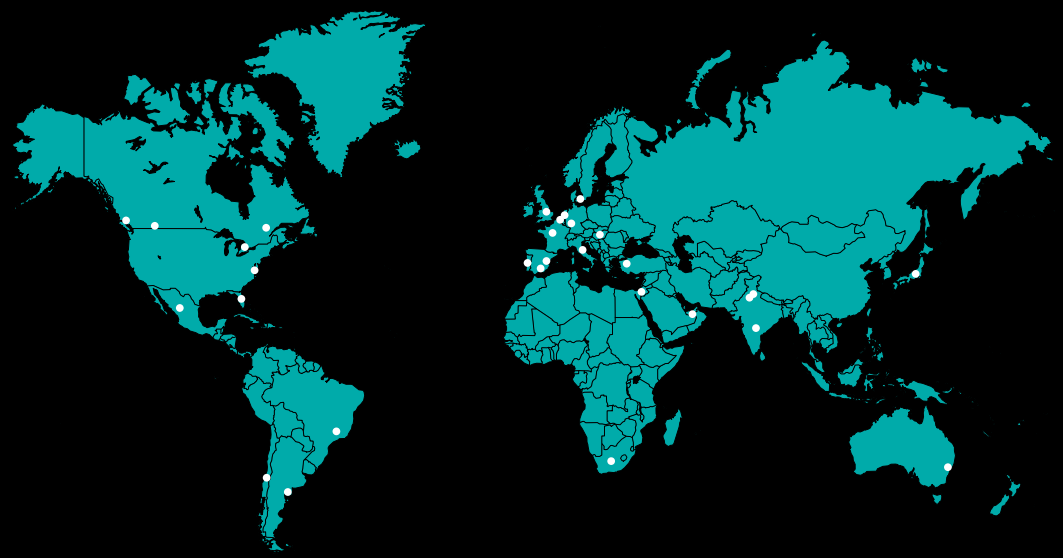
All Deloitte's Cyber Risk practices throughout EMEA provide the same exceptional quality of service in all 14 capability areas showcased in this document.

Chris Verdonck
EMEA Cyber Risk Leader

Next

Deloitte's global network of Cyber Intelligence Centers (CICs)

As cyber threats evolve and become more complex, many business leaders recognize they can't manage the challenge alone. Our CICs provide fully customizable managed security solutions including, **but not limited to,** advanced security event monitoring, threat analytics, cyber threat management and incident response for businesses in the region to meet the increasing market demand in cybersecurity services.



CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's Global network of Cyber Intelligence Centers (CICs).

Next

Deloitte's Cyber Risk awards and recognitions

Deloitte ranked #1 globally in security consulting by Gartner (sixth consecutive year)

Gartner, a technology research company, has once again ranked Deloitte #1 globally in Security Consulting, based on revenue, in its market share analysis entitled Market Share: Security Consulting Services, Worldwide, 2017. This is the sixth consecutive year that Deloitte has been ranked #1.

Source: Gartner, Market Share Analysis: Security Consulting Services, Worldwide, 2017, Elizabeth Kim, 27 June 2018.

Deloitte named a global leader in Cybersecurity Consulting by ALM Intelligence

ALM Intelligence (a research firm, formerly known as Kennedy) named Deloitte a global leader in Cybersecurity Consulting. The report notes: "Deloitte expertly couples both the needs of the business, by understanding the business context and objectives of aligning cyber to business goals; and of the IT security function, with its ability to create in-depth cybersecurity strategies and programs that are in-line with strategic objectives and organization-wide risk appetite."

Source: ALM Intelligence; Cybersecurity Consulting 2017; ALM Intelligence estimates © 2017 ALM Media Properties, LLC. Reproduced under license.

Deloitte named a worldwide leader in Managed Security Services based on capability and strategy by IDC

IDC MarketScape report notes: "Deloitte offers a range of managed cyber services, from basic MSS to some advanced detection capabilities, and tailors its offering from a risk perspective."

Source: IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment by Martha Vazquez, August 2017, IDC #US41320917.

Deloitte qualified professionals

Deloitte consultants hold key professional and industry certifications, such as CISSP, CISM, ISO27001, COBIT, ITIL, CDPP, CEH and many others.

Deloitte Cyber Risk teams have won many awards and competitions, including the Global CyberLympics for six years in a row.

Next

Deloitte's Cyber Risk portfolio

End-to-end cybersecurity

Cyber Strategy

Helps executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.

- Cyber Strategy, Transformation and Assessments
- Cyber Risk Management and Compliance
- Cyber Training Education and Awareness

Secure

Focuses on establishing effective controls around organizations' most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth and cost optimization objectives.

- Infrastructure Protection
- Vulnerability Management
- Application Protection
- Identity Services
- Information Privacy and Protection

Vigilant

Integrates threat data, IT data and business data to equip security teams with context-rich intelligence to proactively detect and manage cyber threats and respond more effectively to cyber incidents.

- Advanced Threat Readiness and Preparation
- Cyber Risk Analytics
- Security Operation Center
- Cyber Threat Intelligence

Resilient

Combines proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.

- Cyber Incident Response
- Cyber Wargaming

Delivery models: Advise, Implement, Manage

Next

Cyber Strategy

Deloitte helps executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.

Next

Cyber Strategy, Transformation and Assessments

Challenges

Organizations increasingly depend on complex technology ecosystems for several key purposes: to interact in new ways with customers and third-parties; to use data to improve decision-making; and to increase reach and profitability.

As cyberattacks become more frequent and severe, Board members and executives are seeing that technology-based initiatives open doors to cyber risks.

How Deloitte can help

Deloitte services help organizations establish their strategic direction and structures, and develop effective cyber-risk reporting. They support the creation of executive-led cyber-risk programs. They take account of the client's risk appetite, helping organizations identify and understand their key business risks and cyber-threat exposures.

Key solutions

Cyber Strategy Framework (CSF)

Advise | Implement | Manage

Enables organizations to identify and understand their key business risks and cyber-threat exposures. Defines cyber strategies, actionable cyber roadmaps and reference architectures in line with the findings of a maturity assessment.

Cyber Target Operating Model

Advise | Implement

Constructs an appropriate target state for cybersecurity roles, responsibilities, related processes and governance functions. These take into account the organization's existing structure, team capabilities, resource availability and third-party ecosystem.

Cyber Transformation

Advise | Implement | Manage

Mobilizes, manages and delivers a structured and prioritized program of work to help organizations enhance their cyber governance, and to become more secure, vigilant, and resilient.

Cyber Benchmarking

Advise

Based on the Cyber Strategy Framework capabilities, enables organizations to compare their cyber maturity with industry peers on a global level. The insights gathered in this exercise complement the maturity assessment by identifying the capabilities with the greatest need for investment and resources.

Next

Cyber Strategy, Transformation and Assessments

Key differentiators

- The Deloitte Cyber Strategy framework measures cyber posture and threat exposure.
- A managed service, which enables Chief Information Security Officers (CISOs) to execute their management activities effectively.
- A leading catalog of good practice standards for cybersecurity, with proven success across industry sectors.

Deloitte's own Cyber Strategy Framework

Methodology

CSF incorporates a proven methodology based on three components: business, threats and capabilities.

Content Packs

CSF features an innovative and comprehensive approach to assessing cyber security, based on the combination of qualitative (closed statement) and quantitative (metric) approaches. CSF includes support for content packs, which enable reporting on alternative standards, in addition to customizing the platform to client's environment, specific needs, and/or control framework.

Platform

CSF includes a versatile online platform.

Deloitte

CSF is underpinned by the expertise and experience of global Deloitte cyber professionals.

Next

Cyber Strategy Framework (CSF)

Managing cyber risk to grow and protect business value

The Deloitte CSF is a business-driven, threat-based approach to conducting cyber assessments based on an organization's specific business, threats and capabilities. CSF incorporates a proven methodology to assess an organization's cyber resilience; content packs which enable us to conduct assessments against specific standards; and an intuitive online platform incorporating a range of dashboards that can be customized for an executive, managerial and operational audience.

Three fundamental drivers that drive growth and create cyber risks:

Innovation | **Information sharing** | **Trusting people**

CEO: "I read about phishing in the news. Are we exposed?"

CIO: "Where and how much do I need to invest to optimize my cyber capabilities?"

Board: "What is our level of resilience against these cyber attacks?"

Organizations need a holistic, business-driven and threat-based approach to manage cyber risks. While securing assets is important, being vigilant and resilient in the face of cyber attacks is imperative

Business risks

What is my business strategy?

What is my risk appetite?

What are my crown jewels?

Threat landscape

What are they interested in?

What tactics might they use?

Who are my adversaries?

Cyber capabilities

Governance
Identify top risks, align investments, develop an executive-led cyber risk program

Secure
Take a measured, risk-prioritized approach to defend against known and emerging threats

Vigilant
Develop situational awareness and threat intelligence to identify harmful behavior

Resilient
Have the ability to recover from and minimize the impact of cyber incidents

A strong cyber risk program helps drive growth, protects value and helps executives to be on top of cyber threats

1. Understand the business context and objectives
2. Understand my threat landscape
3. Understand current maturity level of cyber capabilities
4. Focus on the right priorities
5. Define target maturity level of cyber capabilities and recommendations
6. Develop cyber strategy roadmap
7. Enhance value from cyber security investments
8. Communicate with internal and external stakeholders

Next

Cyber Risk Management and Compliance

Challenges

In today's complex, continuously evolving, and distributed IT landscape and third-party involvement, organizations must take a structured approach to understanding and evaluating evolving risks as well as aligning with cyber regulations.

Thus, while being an essential component in establishing strategic cyber direction, cyber risk management remains an ongoing process of identifying, assessing, and responding to cyber risk.

Furthermore, to provide an integrated view, organizations are under pressure to expand their operational risk management framework to include cyber risks.

How Deloitte can help

Deloitte's diverse experience in managing cyber risk and compliance can help organizations to operationalize by defining tailored frameworks and solutions, and thus determining the best approach to dealing with cyber risks: avoid, transfer, accept, or mitigate.

Key solutions

Cyber Risk Management

Advise | Implement

Defines framework and methodologies to operationalize assessment of cyber risks to understand their magnitude and make informed decisions that align the organization's risk appetite with the risks it faces. Evaluates coverage of existing insurance policies. Determines areas where residual cyber risk could be transferred to an insurer. Leverages leading GRC solutions to unify and automate cyber risk management activities across the organization, including risk governance, risk reporting and metrics.

Cyber Policies Management

Advise | Implement

Defines the cyber security policy management framework/process to manage the entire lifecycle for scoping, designing, authoring, reviewing and publishing cyber policies. Develops cyber policies that define controls required to address cyber risks.

Third-Party Risk Management

Advise | Implement

Customizes services at each step of the third-party cyber-risk management lifecycle. Providing end-to-end oversight of the third-party risk management program.

Cyber Compliance Management

Advise | Implement

Assesses and prepares compliance with international cybersecurity standards (e.g., ISO/IEC 27001:2013), as well as EU, national and/or sector specific cybersecurity regulations.

NIS Directive Compliance

Advise | Implement

Assesses and prepares organizations, such as National Competent Authorities (NCAs), Single Point of Contacts (SPOCs), CSIRTs, Operators of Essential Services (OES), and Digital Service Providers (DSPs), for compliance with requirements enhancing the security of network and information systems. Helps organizations develop cyber risk capabilities that address security requirements and incident notifications.

Cyber Risk Management and Compliance

Key differentiators

- Mature proprietary methodologies and tools, complemented by vendor alliances.
- Strong experience in integrating cyber risk into the broader enterprise risk management framework.
- Deep knowledge and experience with security control frameworks and regulations.
- Deloitte's proprietary tool, Cyber Strategy Framework (CSF) significantly supporting Cyber Compliance Assessment.

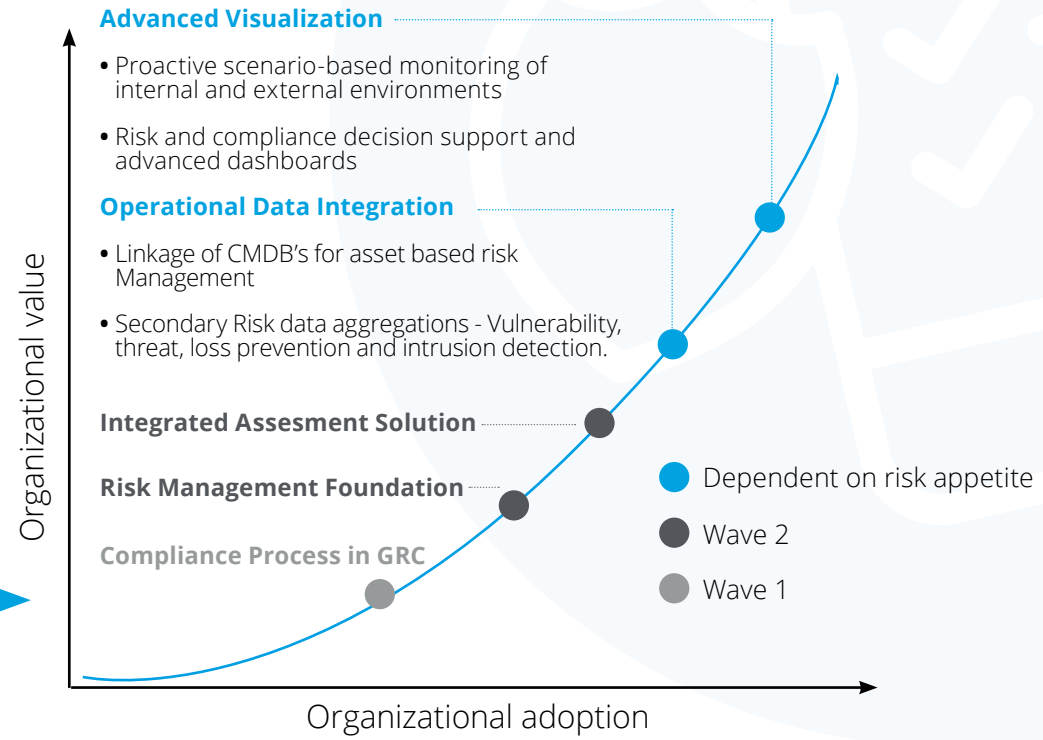
Leading organizations...

- Seek to leverage cost efficiencies from a harmonized control environment.
- Are rapidly evolving to support the information, technology and operations risk and compliance management processes.
- Seek to utilize risk based performance measurement that leverages more granular, transparent risk and compliance management approaches.

Deloitte's Cyber Risk Management and Compliance solutions aim at:

Developing a common and convergent approach when dealing with cyber risk, control, and compliance based activities.

Establishing convergence of the first and the second line of defense within the organization.



Cyber Training, Education and Awareness

Challenges

In a world of ever evolving technology and threats, how confident can an organization be that their employees understand how to help secure their organization? Cyber criminals frequently use employees as their attack vector.

Like any other operating system, this 'human firewall' should be continually updated as well. It is crucial to effectively engage employees, make them the strongest line of defense, and create a cyber risk culture where secure behavior is embedded in the company's DNA.

How Deloitte can help

Deloitte helps to accelerate behavioral change. Organizations that adopt the right behavior make themselves more secure, vigilant, and resilient when faced with cyber threats.

Deloitte helps organizations to develop and embed a cyber risk culture by defining, delivering, and managing programs, both online and onsite, to improve technical skills, foster security awareness, and plan other initiatives needed to effect digital transformation successfully.

Key solutions

Cyber Risk Culture Program

Advise | Implement | Manage

Understands and measures current state of a company's cyber risk culture. Defines a strategy, and develops campaigns that provide immersive learning opportunities, including gamification and engaging communication tools.

In addition, looks into stakeholder and leadership engagement and develops a strong cyber workforce through recruiting, rewarding, and building a cyber risk culture measurement framework reporting ROI.

'Human Firewall' Testing

Advise | Implement | Manage

Through technical simulation exercises (such as Phishing as a Service, Tailgating Exercises, USB Drop, Password Complexity Test) understands the current paradigm phasing an organization in terms of social engineering. Explains how this may affect different departments, and creates a plan to mitigate this type of attacks.

Insider Risk

Advise | Implement

Helps organizations identify, monitor and manage the main sources of insider threat. Enables to establish Potential Risk Indicators (PRIs) and create awareness of the main indicators of maturity in managing insider risk.

Technical Cyber Training

Advise | Implement

Delivers both introductory and highly specialized technical training in cybersecurity, either onsite or through a purpose-built online platform. Deloitte's catalog of courses covers areas such as: Hacking, Secure Development, Forensics, Reversing, Industrial Control System (ICS) security and Incident Response.

Certification Readiness

Implement

Delivers onsite training to prepare employees for qualifications such as Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

Cyber Training, Education and Awareness

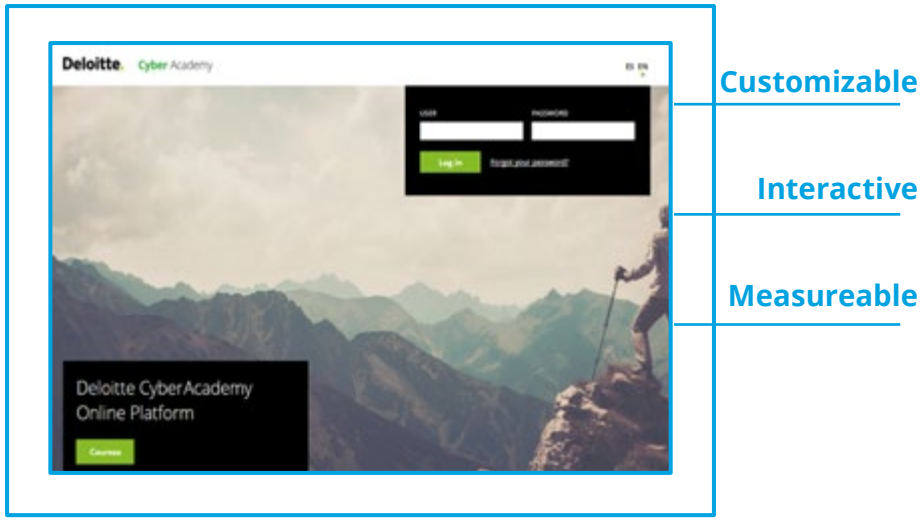
CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Key differentiators

- Deloitte teams work with leadership and learning psychologists, human resources, and cyber specialists to build and deliver the most effective learning and awareness courses tailored to each audience, embedding the desired cyber-risk culture. The focus is on techniques that implement behavioral change to be able to measure the level of effectiveness of all actions that are taken. Deloitte programs respect the corporate culture of every organization.
- We deliver online and onsite technical training and awareness programs to clients and internal practitioners. The online training, both technical and awareness, can be delivered through Deloitte's dedicated EMEA Cyber Academy Online Platform or integrated with an organization's LMS system, thus providing different tailoring options to meet each client's needs.
- The EMEA Cyber Academy collaborates with universities and educational institutions to create expertise and professional performance in the area of Cyber Security, with programs such as specialized online Master's Degree in Cyber Security.

Deloitte's own Cyber Academy Online Platform



Secure

Deloitte focuses on establishing effective controls around the organizations' most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth and cost optimization objectives.

Next

Infrastructure Protection

Challenges

Hyper-connectivity, the move towards cloud based virtual data centers, and the convergence of IT and OT environments are creating a new era for cyber infrastructure where communication and automation control become ubiquitous – posing security challenges for both public and private sector organizations. As the volume of threats to their infrastructure rises, operators are exposed to new types of risks that go beyond data breach: to potential business disruption, plant damage or destruction, or even loss of life.

Digital transformation relies on a massive growth of interconnected systems, increasing the complexity of technical and managerial risks associated with the converged IT-OT environments, which will be managed by an elevated number of diverse stakeholders.

Most operators deploy a large set of cyber security technologies with only a few having evolved to a minimum recommended level. These technologies are often not very effective.

Companies often depend on what vendors offer. Their security measures tend to lack connection with their real business and specific security needs.

How we can help

Deloitte offers clear vision into clients' vulnerabilities (both strategic and technical) and addresses them specifically.

Deloitte's team unites professionals with development, engineering and operations backgrounds, who have also worked in top management and management consulting positions, and have good knowledge of the evolving infrastructure and product landscape.

Deloitte's set of services comprehensively adresses cybersecurity challenges in the architecture, deployment, and maintenance of traditional and new infrastructures and technologies.

Deloitte provides a purpose-built approach focused on providing relevant and actionable insights into organizations, spanning their cyber security domains (on premises and in the cloud) and management processes in order to better protect their critical assets. Drawing on a unique combination of technology, risk, regulatory and industry experience, Deloitte helps clients to raise situational risk awareness, provides actionable remediation plans, and offers managed security services to address today's complex requirements.

Next

Infrastructure Protection

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Key differentiators

- Deloitte supports clients in setting their strategy towards cyber security, developing a Target Operating Model, and engaging top management in addressing cyber risks while enabling them to incorporate new technologies effectively.
- Deloitte assesses risk broadly in converged IT-OT environments, and connected products in an integrated way.
- Deloitte assists clients in the move towards cloud-based virtual data centers; and supports clients by bridging development and operations with security (DevSecOps) to support agile, cost-effective and secure business processes.
- Deloitte helps clients to become secure by reducing the "attack surface" and vigilant by determining whether and how quickly cyber attacks in key areas of the company would be detected.
- Deloitte supports clients in managing and recovering from cyber attacks to limit impacts and maintain critical functions.
- Deloitte offers secure, end-to-end solution-transformation capabilities, from vision alignment to the design of secure product.

Key solutions

IoT Strategy, Roadmap and Architecture

Advise | Implement | Manage

Reviews maturity level of cyber security processes in organizations within the industrial and consumer products sector. Delivers secure development practices to enhance clients' capabilities in implementing next-generation connected products. Helps clients undertake readiness assessments, align their IoT security vision with their overall mission and business objectives, build IoT roadmaps and adapt traditional governance models to new IoT developments.

Network Strategy and Optimization

Advise

Analyzes client infrastructure to identify and remedy the configuration of network components and help clients design their network architecture into secure zones and conduits. Supports clients in the definition of criteria for network segregation according to the most relevant standards and leading practices.

Cloud Security

Advise | Implement | Manage

Supports clients in the move towards secure, cloud-based, virtual data centers. Evaluates clients´ requirements, assesses cloud usage, builds business cases, develops a secure cloud operating model and assists with vendor evaluation. Helps clients implement and manage cloud-based cybersecurity solutions and tests cloud implementations for security weaknesses. Monitors cloud for security and compliance breaches as a managed service.

Monitoring and Protection

Advise | Manage

Analyzes organizations' readiness to defend themselves against cyber attacks in converged IT-OT environments. Support the identification and selection of cyber security technologies, with strong knowledge of the best-of-breed OT passive probing solutions, to identify and manage cyber threats. Provides managed services to support industrial client CSIRT.

Vulnerability Management

Challenges

Businesses rely on a stable and secure IT environment as the foundation for driving new digital innovations and products.

New security vulnerabilities are published on a daily basis and hackers are constantly looking for ways to gain access to systems and data.

Identifying, managing and correcting vulnerabilities in an environment that consists of multiple applications, systems and locations is a significant management challenge.

How Deloitte can help

Deloitte's highly skilled security professionals help organizations identify vulnerabilities. Deloitte's team works shoulder to shoulder with organizations to remedy and manage these vulnerabilities.

These services include fully managed vulnerability assessments from Deloitte's award-winning ethical hackers and support in designing, implementing and operating vulnerability-management systems and processes.

Supported by Deloitte's network of CICs, Deloitte's teams offer a range of managed solutions including vulnerability assessments, remediation support and vulnerability management advisory.

Deloitte's Vulnerability Assessment methodology that helps unburden clients

	Project initiation	Testing and analysis	Reporting
Goals and activities	Kick-off meeting	Application Security Assessment	Completion of report
	Validation of scope, approach, milestones and stakeholders	Source Code Assessment	Management summary and technical details
	Technical preparation: provision of test accounts, documentation, whitelisting, where needed	External/Internal Network Penetration Test	Report discussion and optional management presentation
		Client Security Assessment	Completion of final report
		Mobile Application Security Assessment (optional)	Workshop and training (optional)
Results	**Final project plan**	**List of identified vulnerabilities**	**Final report**

Vulnerability Management

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Key differentiators

- Deloitte professionals include a global pool of award-winning ethical hackers.
- These offerings rely on proven Deloitte methods and cutting-edge vulnerability management tools.
- Deloitte offers a range of managed solutions including vulnerability assessments, remediation support and vulnerability management advisory.
- Deloitte leverages a broad range of subject matter experts on topics such as secure development, incident response, or privacy to remediate the root causes of vulnerabilities.

Key solutions

Security Assessments

Implement | Manage

Uses known ethical hacking methods and proprietary steps to test the security of applications and IT systems. This gives clients insights into their security posture and is a first step in remediating root causes and increasing levels of security. Deloitte can undertake this work fully to "unburden" the client or complement client's internal security assessment team.

Vulnerability Remediation Support

Implement | Manage

Understands remediation of security vulnerabilities as a complex matter.

Supports remediation with tailored vulnerability management tooling, and subject matter expertise so the client can concentrate on their business-relevant vulnerabilities and achieve structural improvements.

Vulnerability Management Capability Design

Advise

Establishes vulnerability management processes, governance, capabilities, tools and expertise for organizations. Deloitte will enable an organization to identify, manage and remedy issues with the various stakeholders involved in a timely way.

Application Protection

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Challenges

Applications form a major part of every IT landscape. Ensuring they are protected requires secure design, implementation and configuration. Testing of the protection requires robust processes, dedicated resources, and a skilled team.

Many organizations find setting up such processes, acquiring and maintaining the required skills and knowledge to be a major challenge.

How Deloitte can help

Deloitte software security specialists assist organizations to thoroughly develop and/or manage their application security processes.

Additionally, Deloitte is well positioned to support and manage the testing for organizations as a market-leading cybersecurity service provider. Deloitte's in-house developed platform, GAST, allows Managed Application Security Services to test large volumes of applications in a multi-vendor environment. This supports Deloitte clients in developing secure applications and it also enables them to save time and cost.

Key solutions

Security and Privacy by Design and Default: SDLC Process Integration

Advise | Implement | Manage

Integrates security and privacy into the Software Development Life Cycle (SDLC) process, ensuring that privacy and security requirements are considered throughout all phases of the application's life cycle. This results in reduced costs, traceability, increased security and compliance with privacy laws.

Assesses efficiency of existing controls in the SDLC process and any development methodology.

Focuses on education, guidance and reviews, including:

- Secure Coding Guidelines
- Training and Awareness
- Threat Modeling
- Security Architecture Reviews
- Software Deployment Security
- Mandatory Privacy and Security Requirements

Application Security Testing

Implement | Manage

Implements processes to regularly test the application's security. Identifies vulnerabilities through security testing methods and remediates these to reduce risk exposure. Tracks the remediation progress and provides insights into the security posture and the most common coding mistakes.

Deloitte. GAST

Next

Application Protection

Deloitte GAST platform
(Global Application Security Testing)

- Centralized operations
- Advanced and customizable reporting
- Real-time progress feedback
- Weaknesses lifecycle management
- Multi-vendor assessments
- Aligned security taxonomies

Key differentiators

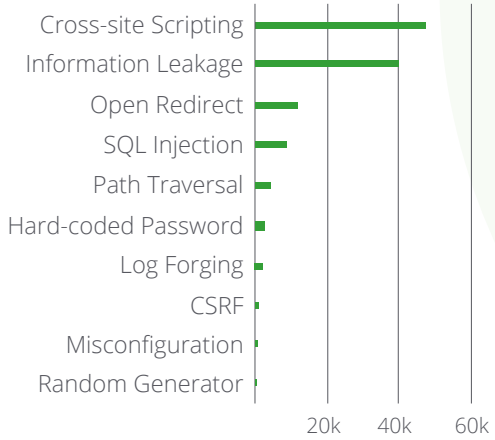
Deloitte's purpose-built service provides clients with relevant and actionable insights, spanning the entire S-SDLC. It helps clients better protect their sensitive data and critical applications.

Drawing on a unique combination of technology, risk, regulatory, and industry experience, Deloitte's service can help clients raise situational risk awareness and actionable remediation insights. Therefore, it empowers them to effectively manage and enhance their application portfolio without undermining their security posture.

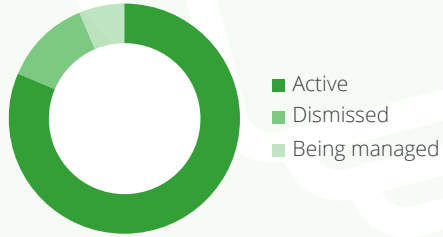
Source code analysis overview

Weaknesses by criticality

Top Common Weakness Enumerations (CWE) detected



Status of detected weaknesses



80+ scans in 2017

17M lines of code scanned

300K identified weaknesses

44K false positives

Identity Services

Challenges

The classical network perimeter has faded. In response, organizations increasingly focus on user identity assurance and information access controls.

Identity Services (Identity and Access Management - IAM) provide tools, processes and methods to enhance the security of online transactions while minimizing friction in the user experience. IAM also provides a trusted environment for omni-channel communication between users (customers, business partners and employees) and IT platforms.

How Deloitte can help

Identity and access are two of the key elements that underpin digital commerce and automated business processes. Deloitte has established a proven methodology to guide clients through the full IAM program lifecycle, from defining a clear vision and strategy for secure access to information assets, to the actual deployment and operation of IAM platforms and integration with IT platforms.

Key solutions

Identity Target Operating Model

Advise | Implement | Manage

Implements the right organizational structure. Prepares the stakeholders for an operational Identity Service.

Identity Governance and Lifecycle Management

Advise | Implement | Manage

Monitors the user lifecycle. Controls user permissions for employees, business partners, and customers.

Access and Digital Rights Management

Advise | Implement | Manage

Secures real-time access to information by verifying authenticity of user request and enabling low-friction information exchange (including Single Sign On and Multi-Factor authentications).

Privileged Account Management

Advise | Implement | Manage

Provides secure access to administrative consoles and administrator password vaulting in order to decrease exposure to internal threat.

Identity Repository and Data Management

Advise | Implement | Manage

Stores trusted information on identities to allow controlled access by applications and business services (e.g., Azure AD and User Master Data Management).

User and Entity Trust Services

Advise | Implement | Manage

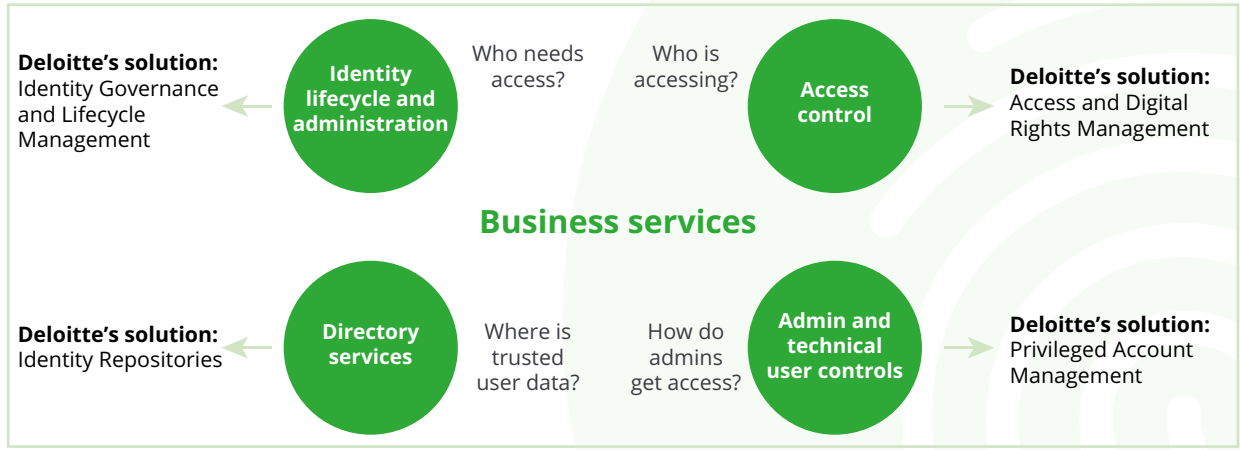
Implements users' trust in digital systems, ranging from customer onboarding to trusted use of IoT devices acting on behalf of a person.

Identity Services

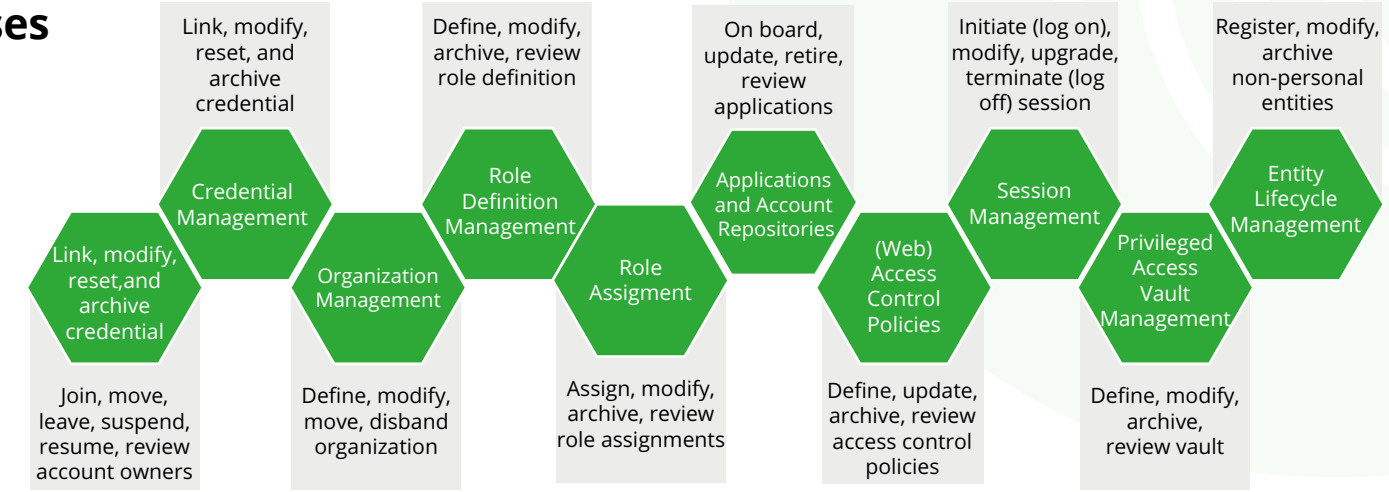
Key differentiators

- Business and user-centric view of IAM as part of Deloitte DNA.
- Experience of global best practices and IAM solution architectures.
- Close solution partner network with major IAM capability providers.

Identity components



Identity processes



Information Privacy

Challenges

Privacy has become a global issue with a heightened sense of regulatory and public awareness. The high bar for privacy compliance is the new normal.

Using, analyzing and sharing your data while ensuring sustainable compliance with invasive regulatory controls (e.g., GDPR), increasing and changing customer/employee privacy expectations, puts significant operational and strategic pressure on organizations. It requires a holistic and pragmatic approach.

How Deloitte can help

Deloitte works with clients to answer questions that matter the most (e.g., how to use personal data more effectively, how to demonstrate effective compliance, how to manage breaches and notifications, how to embed privacy capability). Deloitte offers a tested and comprehensive suite of end-to-end Privacy Services helping you to transform and maintain your management of regulatory and operational challenges, making the most of personal data.

Key solutions

Privacy/GDPR Strategy and Transformation Program

Advise | Implement

Builds a holistic and tailored transformation program in close partnership with clients. Helps clients incorporate fit-for-purpose and sustainable privacy solutions into their DNA.

Privacy by Design/Managed Services (e.g., Data Protection Officer as a Service)

Advise | Implement | Manage

Provides hands-on, technology-enabled services, tools, dashboards and controls. Offers integrated toolkits and advisory services, including privacy impact assessments, breach management and notification GDPR/Data Protection Officer (DPO) helpdesk, GDPR stress testing, third party management, data inventory, and data mapping.

Preference Management and Customer Engagement

Advise | Implement | Manage

Assesses the current state of an organization's readiness and provides solutions to deal with data subject rights management (e.g., right to access, right to deletion). Assist in building a sustainable data subjects' rights management environment. This includes a specific focus on marketing compliance and (as needed) consent management.

International Data Transfer Strategy and Implementation

Advise | Implement

Assesses and builds a contractual, regulatory and operational framework for international data transfers. Includes guidance from start to finish related to, Binding Corporate Rules (BCR) application and implementation.

Privacy/GDPR training, Awareness and Cultural Change

Implement

Offers tailored GDPR awareness and training, on-site or via e-learning/classroom formats, using, for example, the Deloitte EMEA Privacy Academy, and covering both GDPR compliance and its operational/technical implications.

Customer Breach Support and Response

Implement | Manage

Visit page 38.

Information Privacy

Key differentiators

- Dedicated global team with a strong presence across the EMEA region that works seamlessly to solve clients' most complex problems.
- Alliance programs with key vendors enable Deloitte to deliver technology that enhances clients' operational efficiency and minimizes the impact on business.
- Services that are tailored to clients' needs and can be delivered in a variety of flexible ways, including managed service offerings, across a number of key domains.
- Broader scope of service than just compliance management. Support of clients' wider business objectives, unlocking the value of the data they use, and support them in building trust with their customers.

Privacy: Achieving sustainable compliance

Need for combining forces (beyond GDPR, towards data governance)

Processes and organization
Review and implement the correct business processes and privacy operating model

Legal and compliance
Install GDPR/privacy controls as part of unified risk management

GDPR/Data Governance Journey

Cyber security and IT
Implement right technology and cyber governance measures

Data management
Implement integrated and sustainable controls for personal data

Next

Information Protection

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Challenges

Organizations are expected to keep personal and corporate data confidential, yet data breaches still occur. These can result in financial loss, regulatory sanction and reputational damage.

Common challenges are identifying organization's business critical information, localizing it and ensuring it is adequately protected in a world where the quick exchange of information is integral to business success.

How Deloitte can help

We offer organizations access to market-leading technical, business and operational expertise to help them make informed decisions about their data.

Deloitte solutions cover the broad challenge of information protection, including risks arising from people and processes, as well as from technology.

Key solutions

Data Loss Prevention (DLP)

Advise | Implement | Manage | Health check

Assists in the identification, monitoring and protection of sensitive data in motion, at rest, in use and in the cloud. Assists in the integration, implementation and management of data loss prevention programs from a technical, business, and compliance point of view.

People Risk

Advise | Implement

Improves security awareness and incorporates it in organization's culture. Enhances understanding of insider threats. Focuses on protecting sensitive information and preventing risky use of business information.

Information Governance

Advise | Implement

Enables monitoring of access activity and improves visibility of risks to stored information across the business. Assists in the definition of sensitive information governance rules and in target operating model definition.

Information Mapping and Inventories

Advise | Implement

Assists in the information lifecycle protection enforcement from collection to deletion and in the documentation expected by data protection authority (data flows, data mapping).

Information Classification

Advise | Implement

Assists in the sensitive data inventory; in the definition, integration, implementation of sensitive information; in the classification technology and programs.

Privacy by design / by default

Advise | Implement

Advises on Information Protection profiles and programs to embed data protection mechanisms in new solutions and in day-to-day operations. Enables informed business decisions to mitigate residual risk and to adopt pragmatic remediation plans.

Cryptography

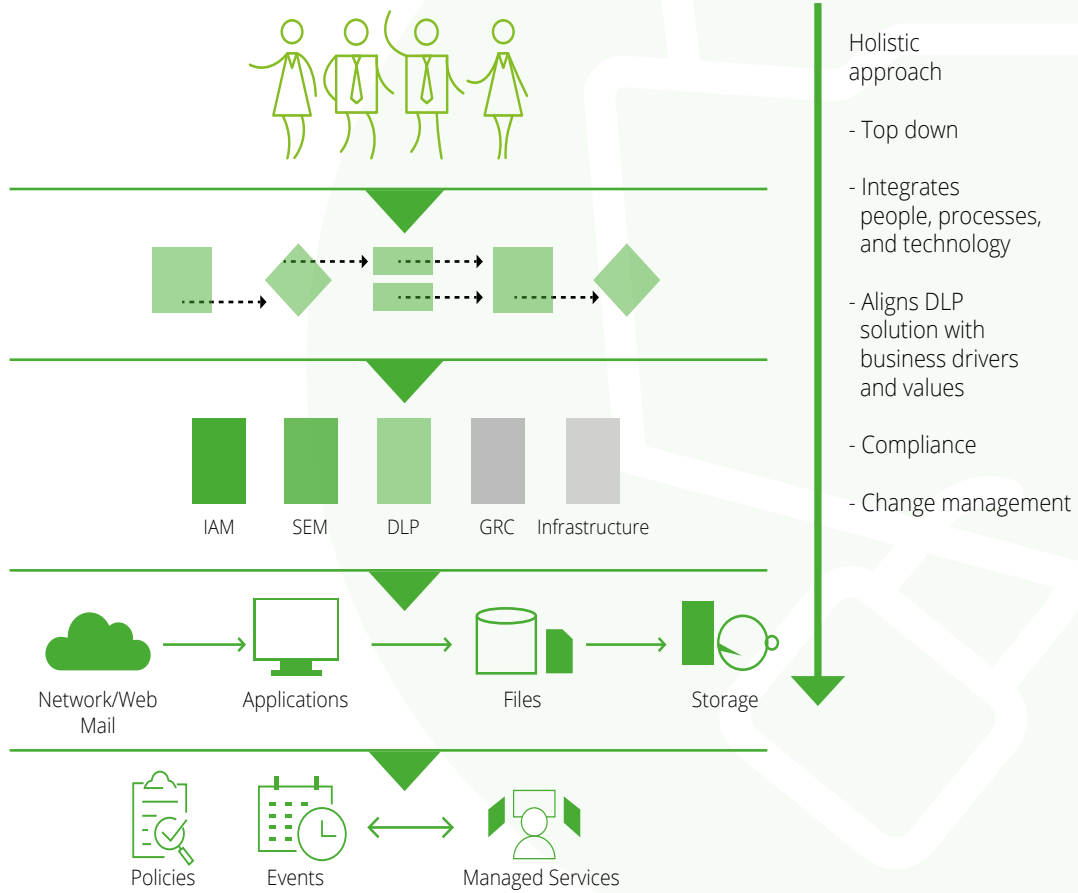
Advise | Implement

Allows business integration and implementation of enterprise key management, rights management and encryption solutions.

Information Protection

Key differentiators

- Global strategic alliances with multiple key vendors on the market.
- Team of senior specialists across EMEA who are technically certified and experienced in complex programs.
- Advanced managed security services capabilities on EMEA level.
- End-to-end solutions combining deep technical expertise with high-end advisory skills of Deloitte professionals.
- Tailored Data Loss Prevention (DLP) approach.
- Experience with large Information Protection projects across industries.



Vigilant

Deloitte integrates threat data, IT data and business data to equip security teams with context-rich intelligence to proactively detect and manage cyber threats and respond more effectively to cyber incidents.

Next

Advanced Threat Readiness and Preparation

CYBER INTELLIGENCE CENTER

Advanced Threat Readiness and Preparation services are driven by and fed with the latest Cyber Threat Intelligence. Based on Deloitte's world-wide network of CICs, we can follow and analyze the latest trends and attacks and use this information to generate realistic and up-to-date view of the organization's threat landscape.

Challenges

Threat techniques evolve daily in volume, intensity and complexity as hackers seek new vulnerabilities in software to compromise key systems across organizations.

Carrying out occasional, intermittent compliance-focused technical security assessments is not enough. Much more is required to understand if organizations can become compromised.

How Deloitte can help

Deloitte helps organizations assess and prepare their IT infrastructure, software and third-parties by combining classical ethical hacking principles and technical security reviews with advanced services in which Deloitte specialists adopt similar approach to that of an attacker.

Deloitte's services allow organizations to leverage any detection or response-mechanisms already in place, augment these where necessary, and most importantly, ensure all systems work together seamlessly so that the whole is greater than the sum of its parts.

Key solutions

Red Teaming / Advanced Threat Simulation

Advance | Implement | Manage

Simulates comprehensive cyberattack that tests the organization's prevention, detection, and response mechanisms and incorporates three core elements of security: physical, cyber and human. The red team creates and executes realistic attack scenarios to achieve predefined objectives, through the use of social engineering, phishing, physical penetration testing and network exploitation.

Regulatory-driven red teaming:

Some industries, such as Financial Services (CBEST/TIBER) or the Government (GBEST) have added Red Teaming to the arsenal of services that aim to enhance organizational security by performing realistic adversarial simulations through red teaming. To meet these project requirements, Deloitte usually incorporates a threat intelligence component, enabling the attack scenarios to be tailored to the client depending on the specific threats and threat actors they face.

Purple Teaming

Advise | Implement

Combines a non-covert red team engagement with a hybrid blue team made up of Deloitte and the organization's security experts. Deloitte runs through realistic scenarios to test and verify detection and response capabilities.

Threat Readiness Advisory and Remediation

Advise | Implement | Manage

Helps most mature organizations deal with advanced threats guiding improvements of ROI on existing detection technologies. By improving interaction between systems, applies realistic use cases and staff training.

Cyber Compromise Assessment

Advise | Manage

Examines an organization's network to identify potential compromised devices by monitoring for malicious network traffic and suspicious network activity.

EDGE: Emerging and Disruptive Technologies Evaluation

Advise

Carries out security evaluations for new technologies and paradigms, helps organizations to anticipate security risks associated with their newly-adopted technologies.

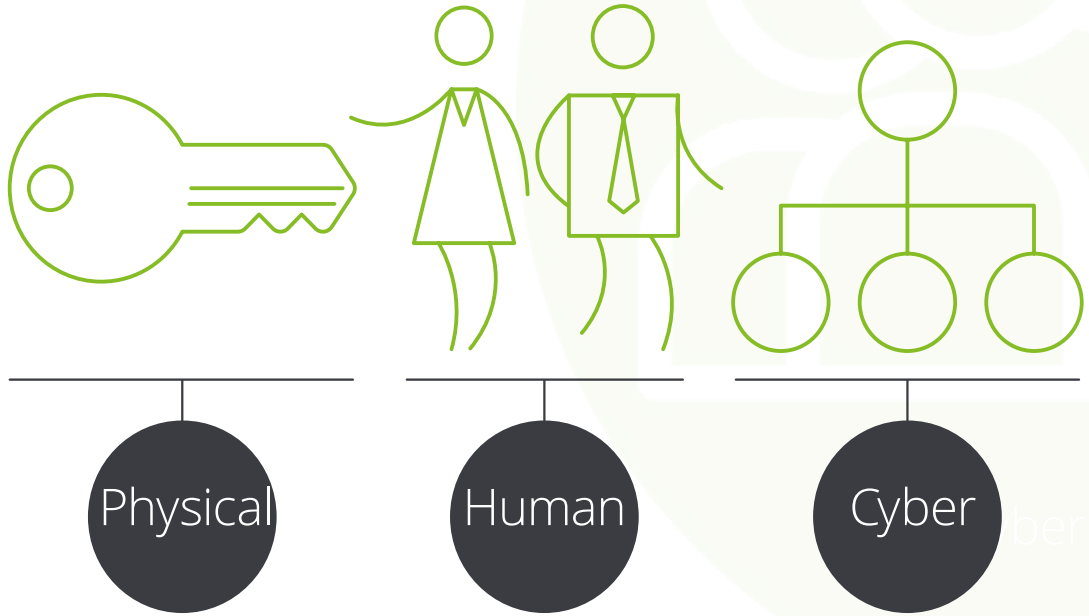
Next

Advanced Threat Readiness and Preparation

Key differentiators

- With the Deloitte service-delivery model, organizations benefit from seamless integration with their vulnerability lifecycle management tasks.
- Deloitte's advanced services enable organizations to address emerging threats from new and disruptive technologies.
- Deloitte teams work with the latest open-source and commercial technologies and can work with any technology an organization might already have deployed.

Identify the weakest link with Deloitte Red, Blue and Purple teaming



Cyber Risk Analytics

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Challenges

The greatest challenge organizations face today is the sheer abundance of threats, which makes it difficult to focus on those that pose the highest immediate risk.

How Deloitte can help

Deloitte's cyber risk analytics services are built to use threat monitoring tools for log collection and monitoring from the traditional rules to the most advanced behavioral analytics techniques and machine learning mechanisms to detect and report about suspicious activity that requires immediate action to mitigate.

Key solutions

Monitoring and Correlation

Advise | Implement | Manage

Enables organizations to view what is happening in cyberspace through advanced analytics. Either through monitoring and correlation of events, log collection with Deloitte Managed Security Services (MSS) platforms or through Cyber Risk Analytics and behavior analytics tools deployed on-site. By covering the whole lifecycle of the tools, Deloitte teams manage all events 24/7, using the Deloitte Security Operations Centers.

SIEM Intelligence

Advise | Implement | Manage

Enhances cyber maturity and governance. A threat monitoring process requires customized approach and continuous adaptation to new threats and new attack vectors. Deloitte has created a methodology to assess clients' necessities, to prioritize threats, and to define and implement tailored use cases that reduce threat exposure and improve the visibility of all kinds of events happening within the client's environment.

Phases of the Monitoring and Correlation process:

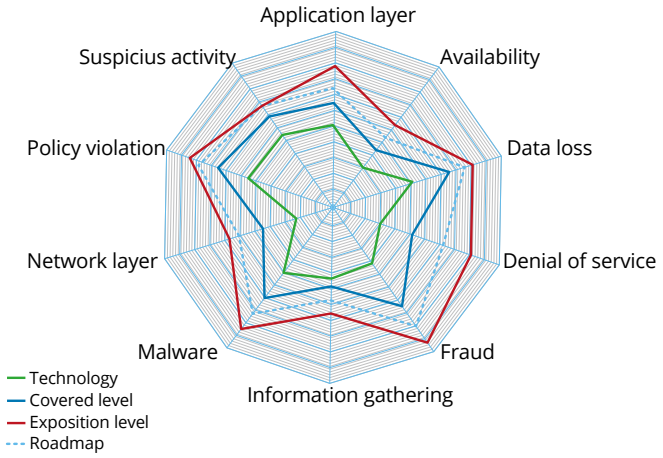
Design — Deploy — Review — Integration — Use cases — Remote Administration — 24/4 Alert management →

Cyber Risk Analytics

Key differentiators

- A flexible, remotely managed service as well as an on-site delivery model.
- Rapid deployment of Managed Security Services (MSS) with no setup costs.
- Broad experience with use cases and specific monitoring tools across a range of industries.

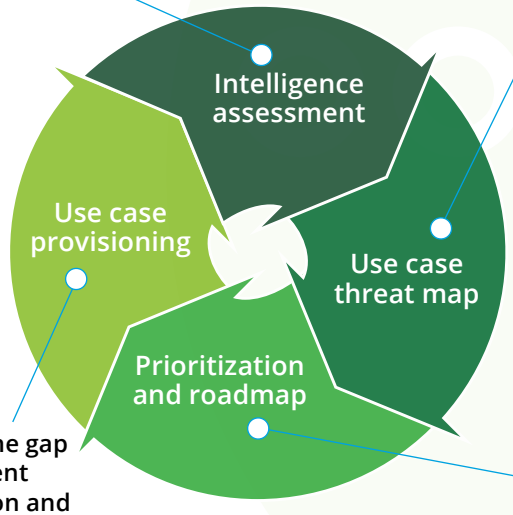
Threat map



The methodology consists of four steps:

Tailored use cases and optimization of rules using Deloitte's intelligence library:

Specifies the changes to help the organization comply with the designed roadmap.



Risk analysis and organization's security goals:

Identifies the current status discovered by an initial questionnaire. Sets meetings with the appropriate stakeholders to enable the client to track progress in a threat map.

Identification of the gap between the current and target situation and roadmap definition:

Once defined, prioritizes the implementation of use cases in order to address the most critical threats or important business services first.

Analysis of existing use cases and provided coverage:

Based on the threat map, defines how the use cases will increase the actual technology coverage and how they will reduce the gap between the threat exposure and the technology coverage.

Next

Security Operations Center (SOC)

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Challenges

Organizations need to develop their information security capabilities, to respond faster, work more efficiently and protect their core business. To achieve this, it is imperative that they have a mature SOC capability.

Special skills and technology platforms are essential. Organizations often find it difficult to build, maintain and resource a SOC.

How Deloitte can help

We provide managed SOC services (on-site and hosted) which integrate event monitoring and correlation with threat intelligence and a business-focused output. We also advise organizations on design and deployment of their own SOC, and can help them establish and develop their capabilities.

Key solutions

24/7 Security Threat Monitoring

Advise | Implement | Manage

Offers a flexible and easily scalable service in which a team of certified analysts works 24/7 to detect malicious activities. Deloitte professionals operate and manage security information and event management (SIEM) platforms.

SOC Capability Design and Deployment

Advise | Implement

Assesses the people, process and technology aspects of an organization's SOC. Uses industry best practices to design and deploy a tailored SOC solution. This enables organizations to identify and respond to the most severe threats they face.

Threat Hunting

Advise | Implement | Manage

Provides a complementary proactive monitoring methodology supported by multiple technologies. Enables organizations to fill detection gaps that cannot be discovered by real-time detection engines.

Security Orchestation and Automation

Advise | Implement | Manage

Enables organizations to collect security threat data and alerts from multiple sources. Uses a combination of human and automated resources to manage incidents according to a standardized workflow.

Security Dashboards

Advise | Implement | Manage

Provides visual reports describing the organization's current security status based on multiple type of indicators, such as operatives, security devices, or SLA compliance.

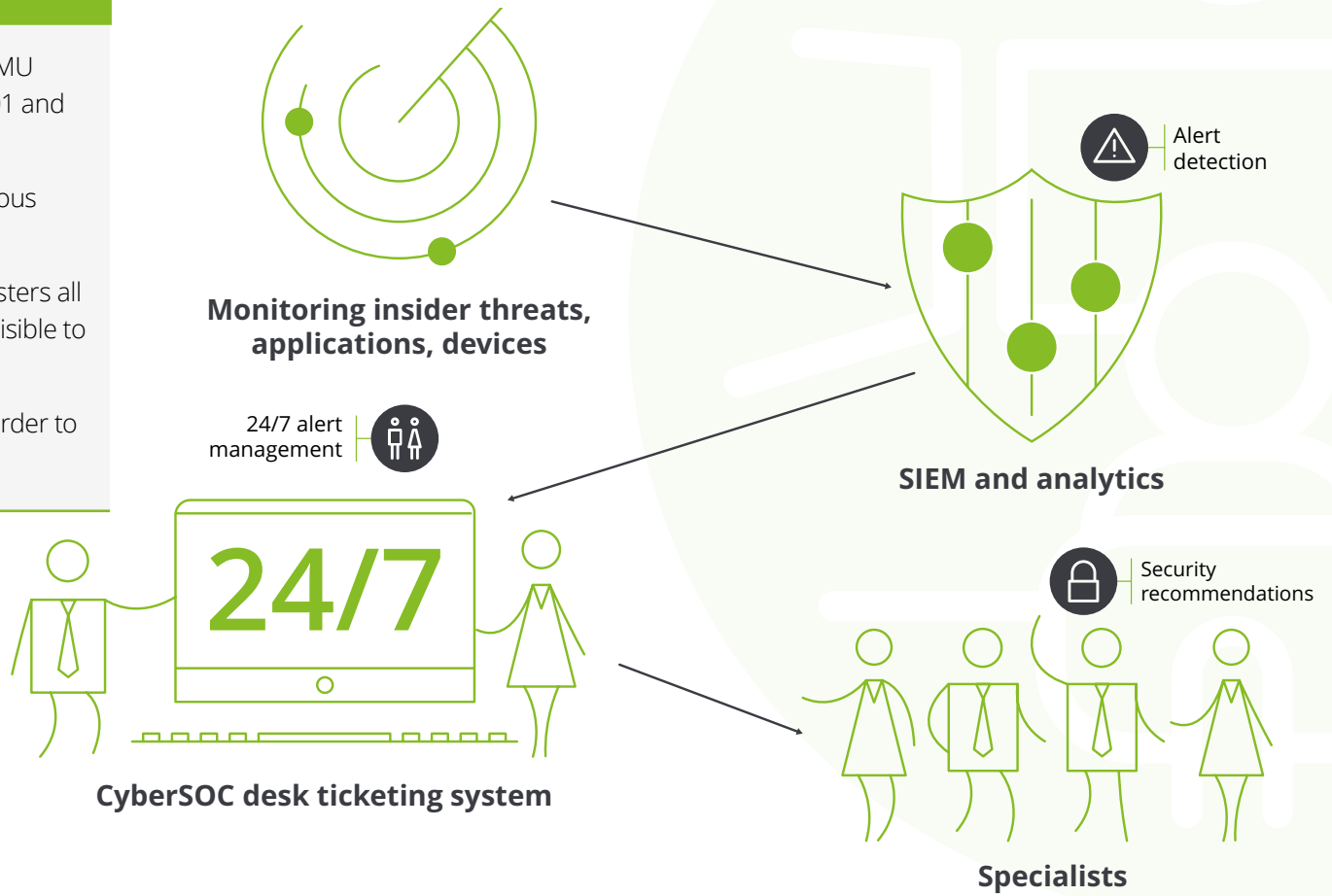
Next

Security Operations Center (SOC)

Key differentiators

- Deloitte EMEA SOC is part of the CMU CERT Network, certified in ISO22301 and ISO27001.
- Deloitte's CICs benefit from numerous intelligence sources.
- Mature process definition that registers all actions taken and makes them all visible to the client.
- Integration of multiple services in order to enable 24/7 capabilities.

Deloitte's 24/7 alert management approach



Cyber Threat Intelligence

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of CICs. Intelligence sharing among CICs allows us to be aware of threats across different regions and businesses so that Deloitte is able to provide unique, valuable and fresh information to clients.

Challenges

Understanding the cyber threat landscape is difficult as threats are continuously evolving.

An integral approach to identifying threats requires significant resources to gather, filter and interpret threat notifications from a wide variety of sources.

How Deloitte can help

Deloitte's Threat Intelligence and Analysis services offer monitoring, collection and analysis of events that may become threats to your organization.

Deloitte's services provide actionable intelligence that supports proactive defense against potential cyberattacks and incidents.

Key solutions

Standard Services – Client generic

Advise | Implement | Manage

Observables Feed
Provides machine-readable curated indicators of compromise feed including context information.

Daily Threat Advisory Digest
Provides a daily digest of threats driven by global priority intelligence requirements.

Urgent Threat Notifications
Provides time-sensitive notifications about emerging threats that require prompt response.

Threat Reports
Provides timely analysis of emerging threats that require greater prioritization.

Deloitte Intelligence Service Platform (DISP)
Gives access to a database of general and industry-specific threat advisories and additional modules.

Monthly Threat Report (per industry)
Shares threat landscape analyses (one industry each month).

Premium Services – Client specific

Advise | Implement | Manage

External Threat Monitoring
Provides client-specific cyber reconnaissance to search for evidence of malicious cyber activity directed against the client, including monitoring of dark web, social media, and underground communities. Includes:

- Confidential data leakage
- Brand abuse
- Fake mobile apps
- Phishing websites
- Vulnerabilities and exploits

Advanced Malware Analysis
Shares static and dynamic analysis to understand malware behaviors, targeted environments, and unique markers.

Take-Down Services
Focuses on removal of fraudulent content on the Internet, which affects the client's brand.

Threat Intelligence Research (via RFIs)
Facilitates requests to provide information and intelligence on specific cyber threats of the client's choosing.

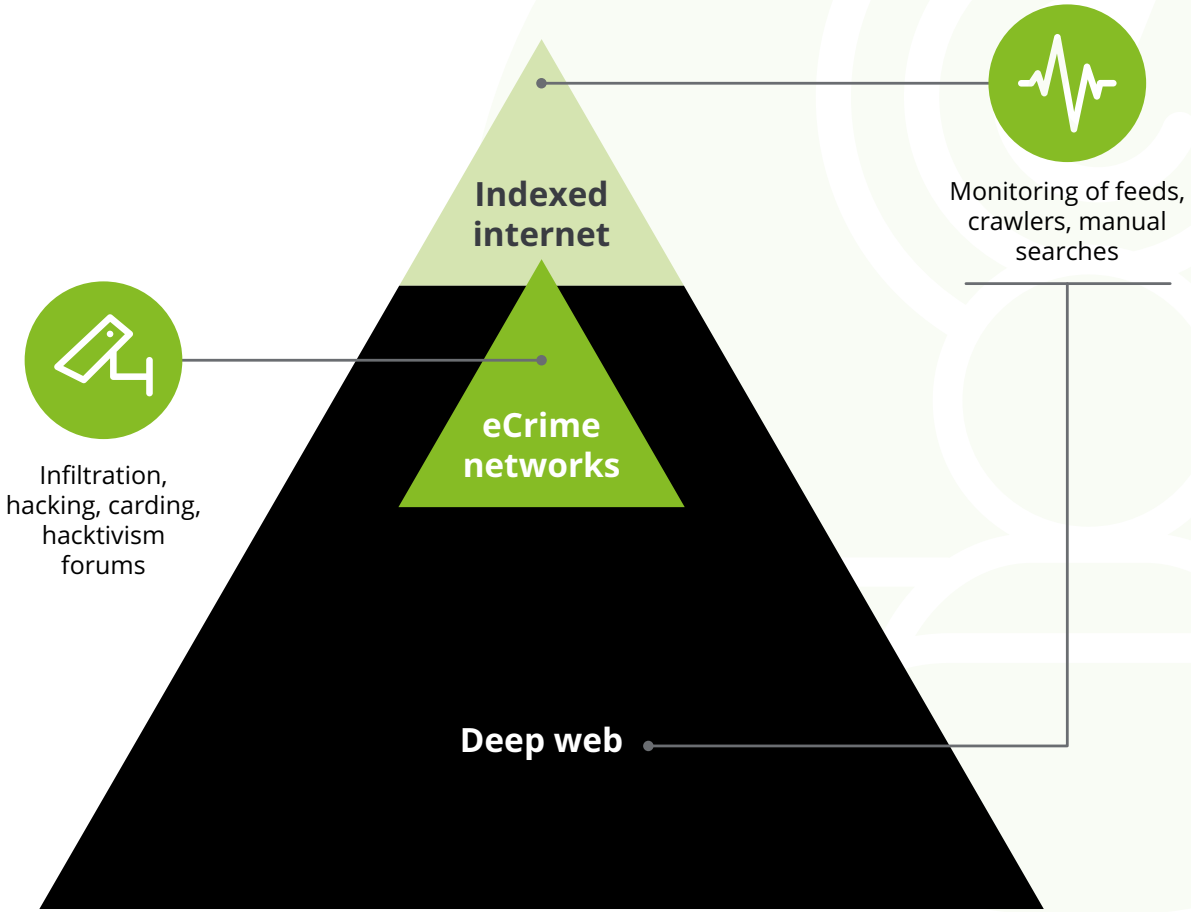
Next

Cyber Threat Intelligence

Key differentiators

- Deloitte provides a tailored Threat Intelligence service, not as a feed or a tool. Actionable intelligence is properly distributed to prevent or mitigate threats that target the client's business.
- Deloitte's experienced professionals undertake research, analysis and validation of threats. They are also at the organizations' disposal to attend to specific intelligence requests that can arise throughout time.

Cyber Threat Intelligence 24/7



Next

Resilient

Deloitte combines proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.

Next

Cyber Incident Response

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte's network of Cyber Intelligence Centers (CICs).

Challenges

Cyber threats are constantly evolving and increasing in volume, intensity and complexity. Cyber crisis management has therefore become a major focus for management and the board.

It has become more likely that an attack can penetrate an organization's defenses and security controls. When this happens organizations must respond fast, thoroughly and decisively.

How Deloitte can help

Deloitte's services provide organizations with a set of operational and strategic cyber-capabilities in a single comprehensive solution, from preparation to 24/7 real-time implementation and response.

Deloitte can help organizations to improve their cyber-response capabilities, establishing a high level of readiness through effective preparation and training. Deloitte provides 24/7 support for a cyber incident or crisis that could harm strategic objectives, revenue, reputation or viability. The support can be provided remotely or on-site as required.

Key solutions

Cyber Incident Response and Forensics

Advise | Implement

Deploys the Deloitte Cyber Incident Response team 24/7, enabling clients to respond effectively and decisively to a cyber-security incident. Deloitte specialists have experience dealing with a vast range of cyber incidents.

Helps the business recover quickly back to normal operations. Deloitte teams are also able to forensically investigate cybercrime to determine the nature, extent, means and origin of an incident. This supports organizations in any legal actions they may need to take.

Provides a proactive set of advisory services that can help organizations improve the ability to respond to incidents.

Technology Resilience

Advise | Implement | Manage

Enhances the technical response team with a team of technology specialists who support clients in enacting their contingency plans and returning technical operations to a normal state after a cyberattack or other disruption. This team can focus on specific systems or applications to support the recovery effort. These specialists are also skilled in the development of recovery plans and preparation activities that need to be developed prior to any incident.

Customer Breach Support and Response

Implement | Manage

Helps clients minimize the impact of a data breach – by putting their customers at the heart of the response and hand holding them through the days and weeks following an incident.

Includes customer breach notification plans and communications, and the scalable infrastructure and trained resource to engage, support and protect clients' customers - and thus their organization - through the crisis.

Information Privacy Capability

Advise | Implement | Manage

Visit solutions on page 24.

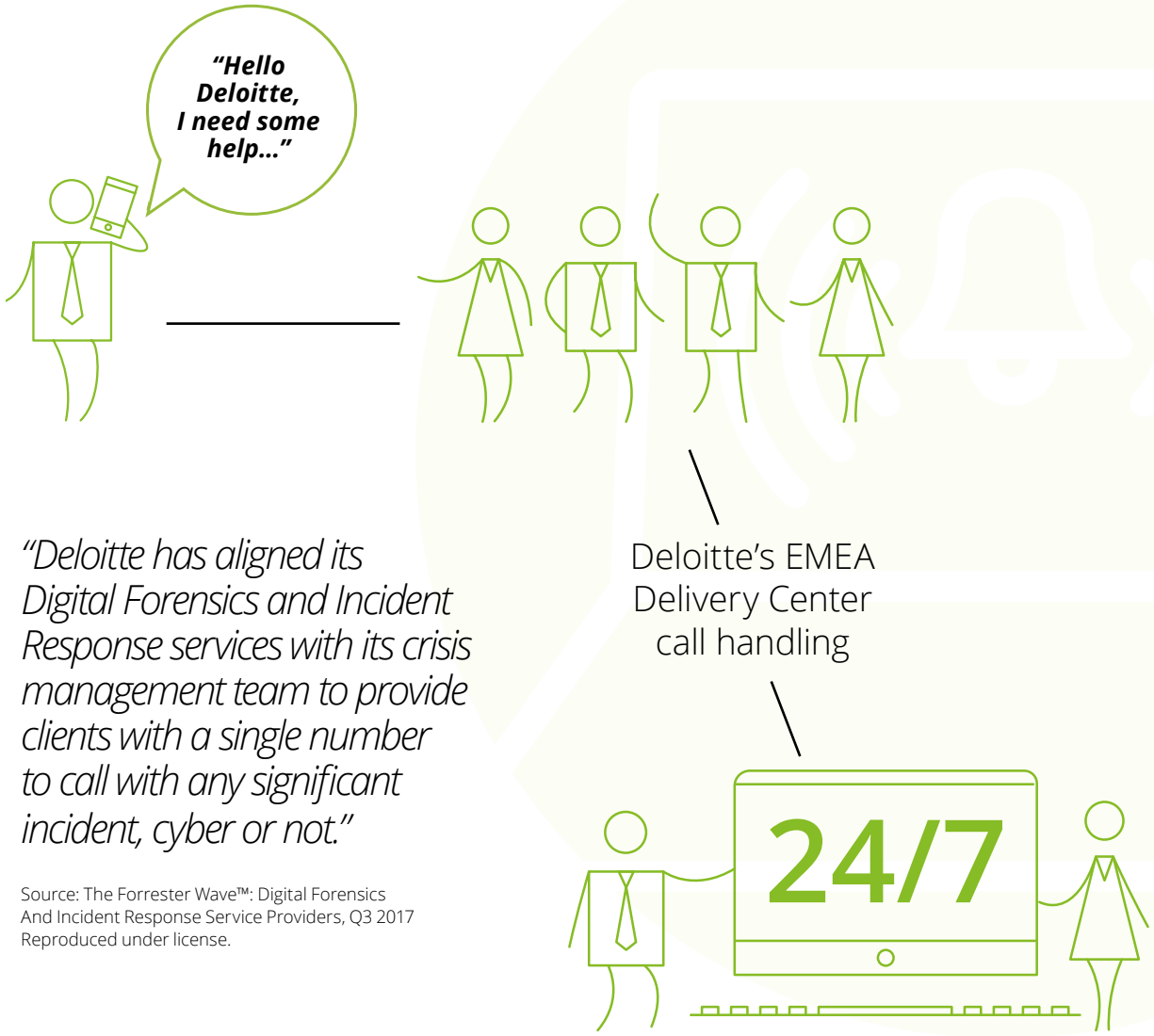
Cyber Incident Response

Key differentiators

- Deloitte's experience in incident and crisis management minimizes the time and resources needed to resolve an emergency.
- Deloitte's understanding of business and risk allows us to respond to incidents from both a technical and a strategic perspective.

These services are supported by the Deloitte EMEA network of CICs, providing support 24/7 with a dedicated Deloitte cyber-response 'front office'. We shorten response times by leveraging Deloitte's geographic breadth and depth.

By dialing a regional Deloitte Response number, a client will immediately be connected to the integrated platform for all cyber-crisis management services within Deloitte EMEA.



"Deloitte has aligned its Digital Forensics and Incident Response services with its crisis management team to provide clients with a single number to call with any significant incident, cyber or not."

Source: The Forrester Wave™: Digital Forensics And Incident Response Service Providers, Q3 2017 Reproduced under license.

Next

Cyber Wargaming

Challenges

Preparing an organization to respond to cyber attacks is critical and can only be done through rehearsing the company's capability to respond to the specific complexities a cyber event presents. These challenges include responding within complex timeframes, making decisions with minimal information, managing information, and knowing who to communicate with and when.

Organizations must test their technical, business and strategic response because cyber threats have the potential to turn into a major corporate crisis, requiring a coordinated response from the communications and corporate affairs functions, the board and non-executive directors.

Key solutions

Cyber Workshop

Advise

Aims to increase awareness and support the development of plans and procedures for the technical, operational and strategic response teams as well as functional teams such as communications.

Focuses on detailed discussion of an unfolding pre-prepared scenario, often split into key incident/crisis response phases.
Includes key areas for discussion: roles, responsibilities, information management, identifying issues and decisions, as well as team working.

Cyber Table-Top Exercise

Advise

Guides teams in reviewing plans and processes, and practicing their roles and responsibilities.

The exercises often focus on sharpening specific skills (such as logging, conducting risk assessments and rehearsing decision-making processes) and identifying opportunities to improve the prevention of, response to, and recovery from a cyber incident or crisis.

Cyber Simulation Exercise

Advise | Implement

Rehearses or stress-tests existing plans and procedures against complex and multi-faceted cyber incidents or crises. Exercises are designed to take place in a realistic, real-time and 'live' controlled environment – often involving multiple levels of an organization operating remotely on a global scale. They unfold through a variety of pre-prepared so-called 'injects' delivered by role players and experienced exercise facilitators. Participants are immersed in the pressure of a real cyber-related crisis.

How Deloitte can help

The Deloitte Wargaming portfolio of services enables organizations to simulate incidents and crises in a realistic environment, allowing them to develop coordinated responses and identify areas that need improvement. These exercises provide a motivating learning experience while validating policies, structures, processes and understanding.

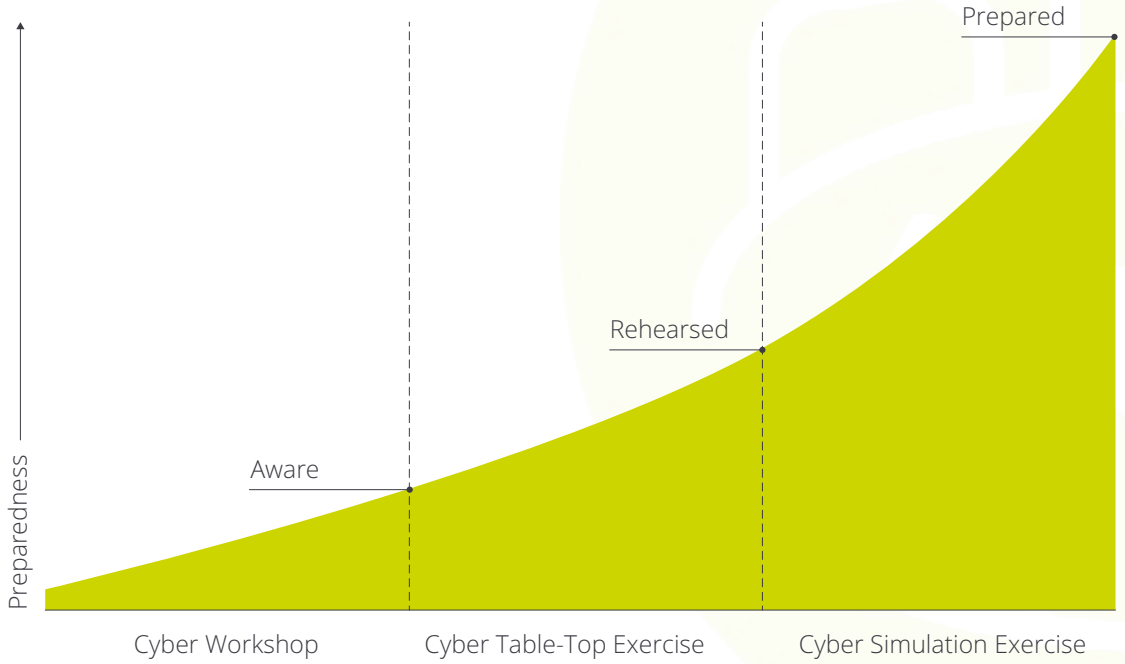
Next

Cyber Wargaming

Key differentiators

- Deloitte's capability has been built through years of practical experience, delivering hundreds of simulations at board, executive, business and technical levels.
- Deloitte uses scenario-specific subject matter experts, from within the organization or Deloitte, in order to tailor highly realistic scenarios in the organization's own operating environment.
- Deloitte uses innovative simulation and wargaming techniques to engage and challenge senior participants and get them thinking about 'what keeps them up at night'. This helps them to answer the questions often asked by key stakeholders, including customers and regulators:
  - Are you and your organization ready to deal with a cyber crisis?
  - Are your people clear of their roles and responsibilities during a cyber crisis?

Cyber Wargaming approach



Contacts

Chris Verdonck
EMEA Cyber Risk Leader
Deloitte Global Risk Advisory
cverdonck@deloitte.com

Africa
Shahil Kanjee
skanjee@deloitte.co.za

Austria
Gilbert Wondracek
gwondracek@deloitte.at

Belgium
Chris Verdonck
cverdonck@deloitte.com

Central Europe
Lajos Antal
lantal@deloittece.com

CIS
Denis Lipov
dlipov@deloitte.ru

Cyprus
Panicos Papamichael
ppapamichael@deloitte.com

Denmark
Thomas Brun
tbrun@deloitte.dk

Finland
Karthi Pillay
Karthi.Pillay@deloitte.fi

France
Michael Bittan
mbittan@deloitte.fr

Germany
Peter Wirnsperger
pwirnsperger@deloitte.de

Greece
Christos Vidakis
cvidakis@deloitte.gr

Iceland
Thorvaldur Henningsson
thenningsson@deloitte.is

Ireland
Jacky Fox
jacfox@deloitte.ie

Israel
Lior Kalev
lkalev@deloitte.co.il

Italy
Stefano Buschi
sbuschi@deloitte.it

Luxembourg
Roland Bastin
rbastin@deloitte.lu

Middle East
Fadi Mutlak
fmutlak@deloitte.com

Netherlands
Niels van de Vorle
nvandevorle@deloitte.nl

Norway
Bjorn Jonassen
bjojonassen@deloitte.no

Portugal
Frederico Mendes Macias
fremacias@deloitte.pt

Spain
Cesar Martin Lara
cmartinlara@deloitte.es

Sweden
Marcus Sorlander
msoerlander@deloitte.se

Switzerland
Klaus Julisch
kjulisch@deloitte.ch

Turkey
Burc Yildirim
buyildirim@deloitte.com

United Kingdom
Phill Everson
peverson@deloitte.co.uk

Next

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J11183