

Deloitte's Cyber Risk capabilities
Cyber Strategy, Secure, Vigilant, and Resilient

Cyber Risk 

Contents

Foreword by Deloitte Cyber Risk Global Leaders 03

Deloitte’s global network of Cyber Intelligence Centers (CICs)	04
Deloitte’s Cyber Risk awards and recognitions	05
Deloitte’s Cyber Risk portfolio	06

Cyber Strategy 07

Cyber Strategy, Transformation, and Assessments	08
Cyber Strategy Framework (CSF)	10
Cyber Risk Management and Compliance	11
Cyber Training, Education, and Awareness	13

Secure 15

Infrastructure Protection	16
Vulnerability Management	18

Application Protection	20
Identity and Access Management	22
Information Privacy and Protection	24

Vigilant 28

Advanced Threat Readiness and Preparation	29
Cyber Risk Analytics	31
Security Operations Center (SOC)	33
Threat Intelligence and Analysis	35

Resilient 37

Cyber Incident Response	38
Cyber Wargaming	40

Contacts 42

Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



Next

Foreword

In an era of rapid digital transformation and the proliferation of ever increasing amounts of data, cyber risk is rising up the priority scale at organizations of all sizes and in all industries.

Deloitte’s experience demonstrates that clients implementing cyber risk 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 cyber risk—Cyber Strategy, Secure, Vigilant, and Resilient.

Deloitte’s alliances with vendors globally provide access to a range of cyber risk technologies.

This enables 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.

Deloitte’s Cyber Risk practice provides the same exceptional quality of service in all 14 capability areas showcased in this document.



Nick Galletto
Global and Americas Cyber Risk Leader



Chris Verdonck
EMEA Cyber Risk Leader



James Nunn-Price
Asia Pacific Cyber Risk Leader

Foreword

Foreword

- Deloitte global network of Cyber Intelligence Centers (CICs)
- Deloitte Cyber awards and recognitions
- Deloitte Cyber Risk portfolio
- End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



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

CYBERINTELLIGENCE
center

Our solutions are supported by
Deloitte's network of CICs

Offers solutions that help its clients protect business assets and mature their security posture, while proactively detecting, responding and recovering from security events. These services are delivered through a global network of CICs, which operate around the clock, 365 days a year to provide fully customizable, industry aligned managed security solutions including advanced security event monitoring, threat analytics, cyber threat management, and incident response for businesses to meet the increasing market demand in cybersecurity services.

Home

Foreword

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



Next

Deloitte's Cyber Risk awards and recognitions

Deloitte ranked #1 globally in security consulting by Gartner (fifth 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, 2016. This is the fifth consecutive year that Deloitte has been ranked #1.

Source: Gartner, Market Share Analysis: Security Consulting Services, Worldwide, 2016.
Elizabeth Kim. 27 June 2017.

Deloitte named a global leader in cybersecurity consulting by ALM Intelligence

ALM Intelligence named Deloitte a leader in Cybersecurity Consulting in its report entitled *Cybersecurity Consulting 2015*. The report notes: "The firm's notable depth across the breadth of the cybersecurity consulting portfolio coupled with its ability to effectively communicate and work with the span of a client organization (boardroom down to IT operations) solidifies its position in the vanguard."

Source: ALM Intelligence, Cybersecurity Consulting 2015; © 2015 ALM Media Properties, LLC. Reproduced under license.

Deloitte named a global leader in security operations consulting by ALM Intelligence (2016)

ALM Intelligence (a research firm, formerly known as Kennedy) notes, "The firm's emphasis on aligning SOC initiatives to what matters to the business—including legal and regulatory requirements and education on threat actors—makes Deloitte an elite firm among its peers when it comes to building a case for investment that resonates with business-side stakeholders."

Source: ALM Intelligence; Security Operations Center Consulting 2015; ALM Intelligence estimates © 2016 ALM Media Properties, LLC. Reproduced under license.

Deloitte qualified professionals

Our consultant of all grades hold key professional and industry certifications, such as CISSP, CISM, ISO27001, COBIT, ITIL, CDP, CEH, and many others. We have won many awards, including the Global Cyberlympics for five years in a row.



Home

Foreword

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



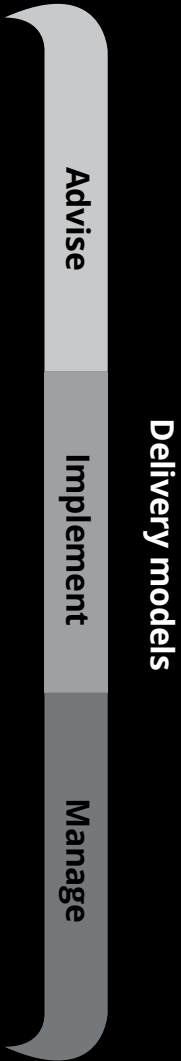
Next

Deloitte's Cyber Risk portfolio

End-to-end cyber risk services

More than 10,000 cyber risk professionals globally

Cyber Strategy	Secure	Vigilant	Resilient
We help executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.	We focus on establishing effective controls around the organization's most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth, and cost optimization objectives.	We integrate threat data, IT data, and business data to equip security teams with context-rich intelligence to proactively detect and manage cyberthreats and respond more effectively to cyber incidents.	We combine proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.
Cyber Strategy, Transformation, and Assessments Cyber Risk Management and Compliance Cyber Training, Education, and Awareness	Infrastructure Protection Vulnerability Management Application Protection Identity and Access Management Information Privacy and Protection	Advanced Threat Readiness and Preparation Cyber Risk Analytics Security Operations Center Threat Intelligence and Analysis	Cyber Incident Response Cyber Wargaming



Home
Foreword
Foreword
Deloitte global network of Cyber Intelligence Centers (CICs)
Deloitte Cyber awards and recognitions
Deloitte Cyber Risk portfolio
End-to-end cyber risk services
Cyber Strategy
Secure
Vigilant
Resilient
Contacts
Next

Cyber Strategy

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

Home

Foreword

Cyber Strategy



Cyber Strategy,
Transformation, and
Assessment

Cyber Risk Management
and Compliance

Cyber Training, Education,
and Awareness

Secure



Vigilant



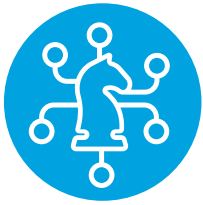
Resilient



Contacts



< > Next



Cyber Strategy, Transformation, and Assessment

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 we can help

Our 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 cyberthreat exposures.

Key solutions

Cyber Strategy, Roadmap, and Architecture

Advise | Implement

Defines cyber strategies, actionable cyber roadmaps, and reference architectures in line with the findings of a maturity assessment. Recommendations are based on a defined target state that is determined by the organization's threat exposure.

Cyber Target Operating Model

Advise | Implement

Constructs an appropriate target state for cyber risk 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 transform to improved cyber governance, security, vigilance, and resilience.

Cyber Maturity Assessments

Advise | Implement | Manage

Enables organizations to identify and understand their key business risks and cyberthreat exposures. This supports measurement of their cyber maturity, either using industry-standard frameworks or Deloitte's proprietary Cyber Strategy Framework.

Cyber Risk Quantification

Advise | Implement

Provides the information needed to make security investment decisions. Deloitte uses unique methods to quantify both the client's risk and the expected risk mitigation offered by Deloitte security investments.

Home

Foreword

Cyber Strategy



Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



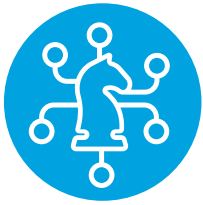
Resilient



Contacts



< > Next



Cyber Strategy, Transformation, and Assessment

Key differentiators

- The Deloitte Cyber Strategy framework measures cyber posture and threat exposure.
- A leading catalog of good practice standards for cyber risk, with proven success across industry sectors.

Deloitte's own Cyber Strategy Framework

(the next page contains details on the framework)



Home

Foreword

Cyber Strategy



Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts

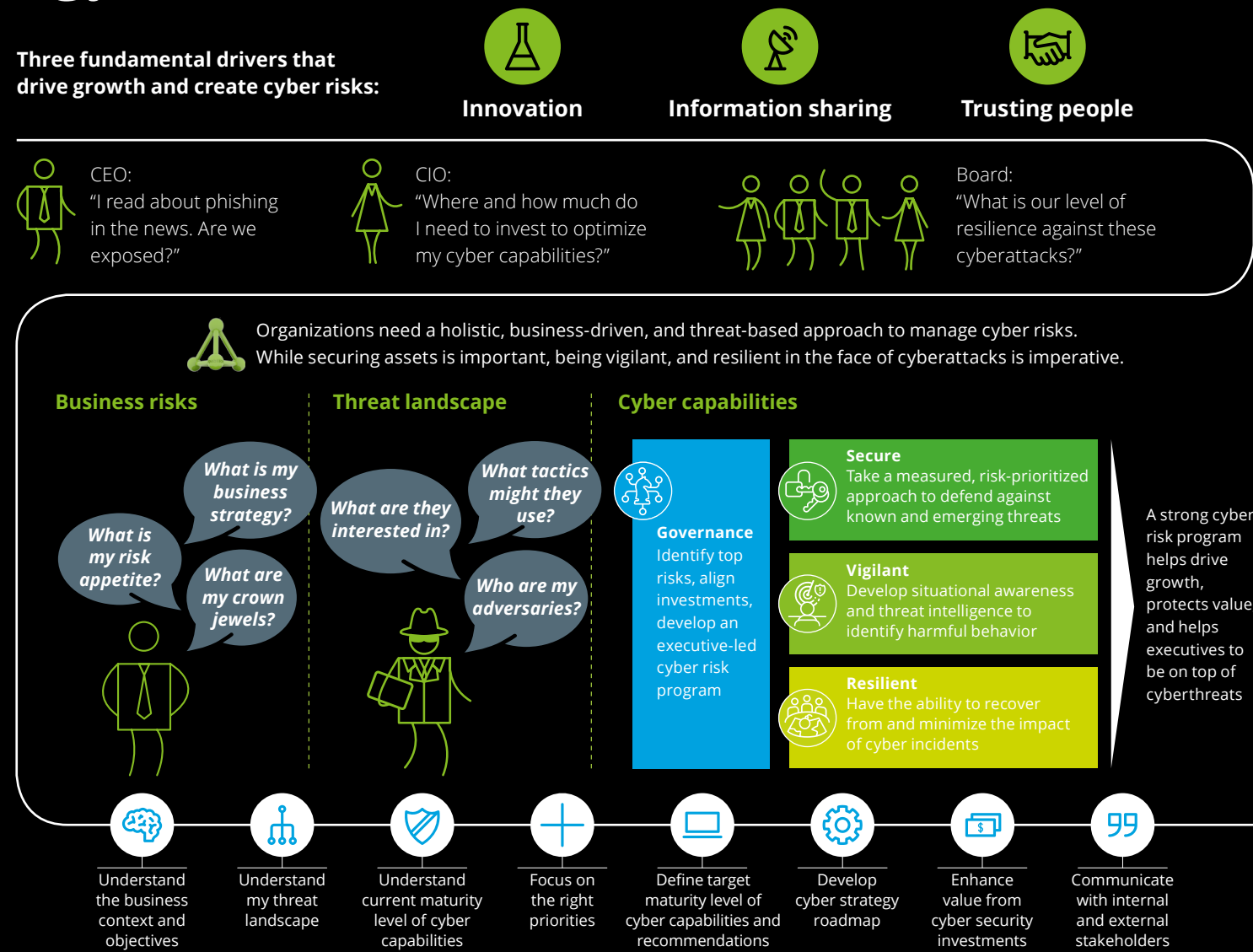









< > Next

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.



Home	
Foreword	
Cyber Strategy	
Cyber Strategy, Transformation, and Assessment	
Cyber Risk Management and Compliance	
Cyber Training, Education, and Awareness	
Secure	
Vigilant	
Resilient	
Contacts	
  Next	



Cyber Risk Management and Compliance

Challenges

Understanding the current status of an organization's security posture requires constant evaluation of evolving risks, security standards, and cyber regulations.

Today's complex and distributed IT landscape and third-party involvement means organizations must take a structured approach to understanding the road ahead.

How we can help

Deloitte's diverse experience in managing cyber risk and compliance can help organizations: define tailored cyber risk management frameworks; support risk transfer via cyber insurance; set and implement cyber-control frameworks; and ensure compliance with cybersecurity regulations.

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.

Home

Foreword

Cyber Strategy



Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts



Next



Cyber Risk Management and Compliance

Key solutions

Cyber Risk Management

Advise | Implement

Defines framework and methodologies to assess cyber risks in order for the organization to understand their magnitude and make informed decisions that align the organization's risk appetite with the risks it faces.

Cyber Risk Dashboarding

Advise | Implement | Manage

Designs and implements risk dashboard constituents, including Key Risk Indicators (KRIs) and dashboards to facilitate effective monitoring of cyber risk from the boardroom to the network.

Cyber Insurance

Advise | Implement

Evaluates coverage of existing insurance policies. Determines areas where residual cyber risk could be transferred to an insurer.

Security Control Framework

Advise | Implement

Defines tailored security-control frameworks based on best practices as guiding principles. Develops policies, procedures, and standards.

Third-Party Risk Management

Advise | Implement

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

Security and Regulatory Compliance

Advise | Implement

Assists and prepares compliance with national and/or sectoral cybersecurity regulations.

Home

Foreword

Cyber Strategy



Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts



Next



Cyber Training, Education, and Awareness

Challenges

Even with excellent people and technology in place, the organization's own employees are the weakest link when it comes to cybersecurity. The so-called insider threat is real. Building secure defenses against outside threats is not enough if data is leaked from within an organization.

How we can help

Deloitte can help to accelerate behavioral change. Organizations that adopt the right behavior make themselves more secure, vigilant, and resilient when faced with cyberthreats.

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

Key solutions

Insider Risk

Advise | Implement

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

Cyber Security Awareness Program

Advise | Implement | Manage

Understands the current state of a company's awareness level, defines a strategy, and develops a recognizable awareness campaign, multimedia content package, and communication tools.

Technical Cyber Training

Advise | Implement

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

Certification Readiness

Implement

Delivers 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).

[Home](#)[Foreword](#)[Cyber Strategy](#)

Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

[Secure](#)[Vigilant](#)[Resilient](#)[Contacts](#)[Next](#)

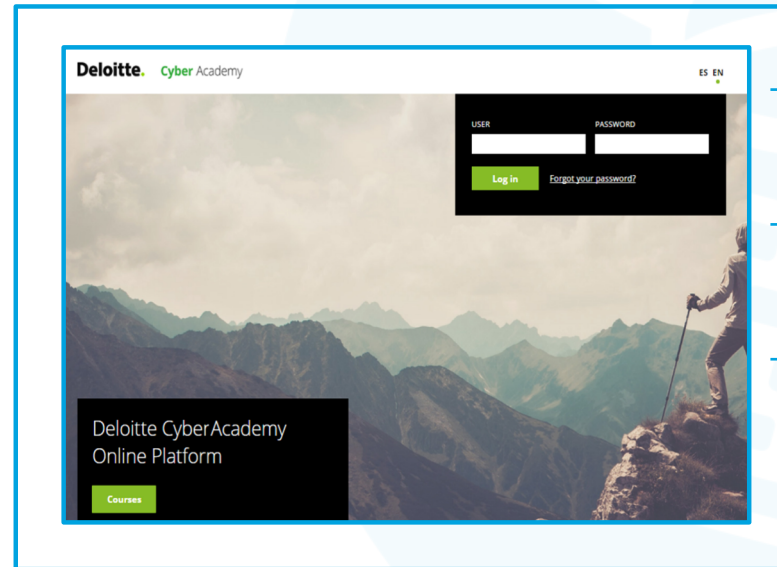


Cyber Training, Education, and Awareness

Key differentiators

- We deliver online and on-site technical training and awareness programs to clients and internal practitioners via a dedicated Cyber Academy Online Platform.
- The Academy collaborates with universities and educational institutions to create expertise and professional performance in the area of Cyber Security, with programs such as a Master's Degree in Cyber Security among our online postgraduate offering.
- We 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.

Deloitte's own Cyber Academy Online Platform



Customizable

Interactive

Measureable

Home

Foreword

Cyber Strategy



Cyber Strategy, Transformation, and Assessment

Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts



< > Next

Secure

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

Home

Foreword

Cyber Strategy



Secure



Infrastructure
Protection

Vulnerability Management

Application Protection

Identity and Access
Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Infrastructure Protection

Challenges

Hyper-connectivity is creating a new era for cyber infrastructure. Ever more connected devices pose new cybersecurity challenges for public and private-sector organizations as the volume of threats to their infrastructure rises.

Devices connected to corporate infrastructures need to continuously acquire, store, and use large amounts of data, a significant proportion of which will be sensitive. Protecting this data against cyberattack is of paramount importance.

Today's smart cybersecurity protects data by using secure data platforms, clear data governance, and smart access protocols such as electronic finger printing.

The development of new technologies will drive exciting innovations in Smart Cities, Smart Factories and the Internet of Things (IoT) as communication and automation control become ubiquitous.

How we can help

Deloitte has developed a set of services that comprehensively address cybersecurity challenges in the architecture, deployment, and maintenance of traditional and new infrastructure and technologies.

Deloitte's security professionals, from diverse architecture, engineering, and operational technology backgrounds, are experts across the evolving infrastructure and product landscape.

[Home](#)[Foreword](#)[Cyber Strategy](#)[Secure](#)[Infrastructure Protection](#)[Vulnerability Management](#)[Application Protection](#)[Identity and Access Management](#)[Information Privacy](#)[Information Protection](#)[Vigilant](#)[Resilient](#)[Contacts](#)[Next](#)



Infrastructure Protection

Key solutions

IoT Strategy, Roadmap, and Architecture

Advise | Implement | Manage

Reviews industrial and consumer product codes and delivers secure development practices to enhance clients' capabilities in implementing next-generation connected products. We help organizations undertake readiness assessments, align their IoT security vision with their overall mission and vision statements, build IoT roadmaps and adapt traditional governance models to new IoT developments.

Cloud Security

Advise | Implement | Manage

Evaluates client requirements, assesses cloud usage, builds the business case and cloud roadmaps, and assists with cloud vendor evaluation.

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.

Anti-DDoS Attacks

Advise | Manage

Analyzes organizations' readiness to defend themselves against Distributed Denial of Service (DDoS) attacks. We provide cloud-based anti-DDoS protection for infrastructures, websites, and DNS servers.

Key differentiators

- We offer secure, end-to-end solution-transformation capabilities, from vision alignment to the design of secure products.

[Home](#)[Foreword](#)[Cyber Strategy](#)[Secure](#)[Infrastructure Protection](#)[Vulnerability Management](#)[Application Protection](#)[Identity and Access Management](#)[Information Privacy](#)[Information Protection](#)[Vigilant](#)[Resilient](#)[Contacts](#)[Next](#)



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 we can help

Deloitte offers the expertise of highly skilled security professionals to help organizations identify vulnerabilities. Deloitte's team works side by side with organizations to remedy and manage these vulnerabilities.

Our 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, we offer a range of managed solutions including vulnerability assessments, remediation support, and vulnerability management advisory.

Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Vulnerability Management

CYBERINTELLIGENCE
center

Our solutions are supported by
Deloitte's network of CICs

Key solutions

Vulnerability Assessments

Implement | Manage

Uses known hacking methods and vulnerabilities, tests the security of applications and IT systems, and achieves increased levels of security. Deloitte can undertake this work fully on behalf of organizations or complement organization's internal vulnerability assessment team.

Hacking and Phishing as a Service

Manage

Provides regular insight into an organization's potential vulnerabilities. Many organizations perform security tests only once while cyber criminals are constantly seeking to find and exploit new vulnerabilities.

Vulnerability Remediation Support

Implement | Manage

Configures and manages vulnerability management solutions providing insight into the business-relevant vulnerabilities that matter.

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.

Key differentiators

- Our professionals include a global pool of award-winning ethical hackers.
- We utilize proven Deloitte methods and cutting-edge vulnerability management tools.
- We offer a range of managed solutions including vulnerability assessments, remediation support, and vulnerability management advisory.

Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Application Protection

CYBERINTELLIGENCE
center

Our solutions are supported by
Deloitte's network of 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 and acquiring and maintaining the required skills and knowledge to be a major challenge.

How we can help

Deloitte software security specialists assist organizations to thoroughly assess the protection level of applications.

With specialized knowledge of a large number of specific applications and secure development methods, Deloitte helps secure the design, development, and configuration of applications.

Key solutions

Enterprise Application Security

Advise | Implement | Manage

Assesses the current state of an organization's applications and the security controls on the application layers for enterprise systems.

Source Code Review

Manage | Implement

Analyzes application source code to test for common mistakes. The analysis can be conducted through one-off application assessments or as an integral part of an organization's software development process.

Secure by Design: Secure SDLC

Advise | Implement

Assesses an organization's software development life cycle (SDLC) to determine if security is properly incorporated. In addition, we help organizations embed Secure by Design principles and controls.

Home

Foreword

Cyber Strategy



Secure



Infrastructure
Protection

Vulnerability Management

Application Protection

Identity and Access
Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Application Protection

Deloitte Application Security Platform

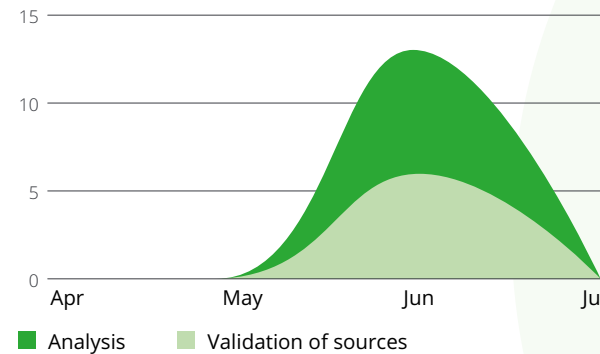
- Source code review activities centralization
- Advanced reporting capacities
- Real-time activities progress feedback
- Vulnerability lifecycle management
- Multi-vendor support
- CWE and CVSS aligned GAST taxonomy

Key differentiators

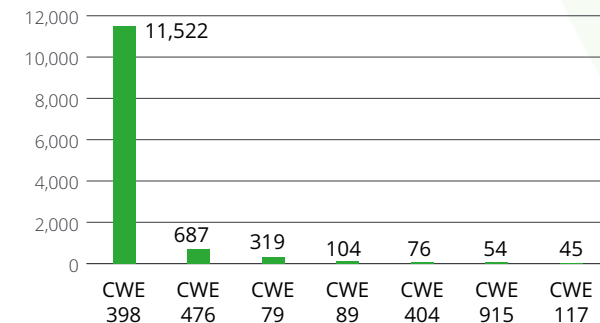
- We leverage static application security testing technology which enables the client to be one step ahead, with 40 percent portfolio coverage versus five percent portfolio coverage using the traditional approach.
- We help organizations raise their situational risk awareness and actionable remediation insights, empowering them to regulate application portfolios effectively.

Source code analysis overview

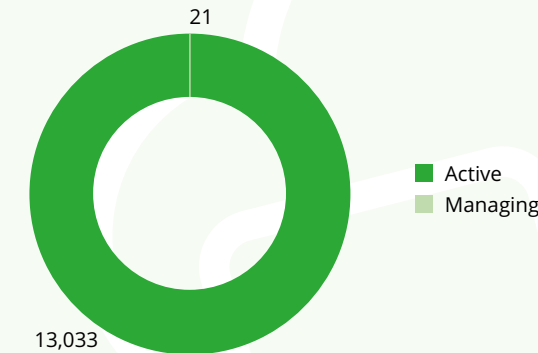
Analysis and validation of sources



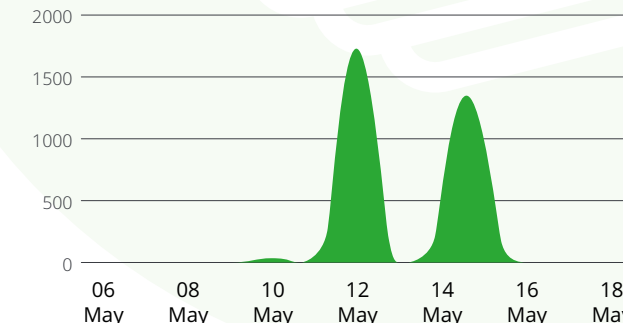
Top CWEs detected



Weaknesses found



Total analyzed lines



Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Identity and Access Management

Challenges

The traditional network perimeter has faded. In response, organizations are increasingly focusing on user identity assurance and information access controls.

Identity and Access Management (IAM) provides 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 we can help

Identity and access are two of the key elements that underpin digital commerce and automated business processes. Deloitte has established 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

IAM Drivers Identification and Selection of IAM Investment Areas

Advise

Defines the objectives for IAM, such as enabling new information exchanges (e.g. low-friction customer registration), more efficient compliance demonstration (e.g. risk-focused access reviews), and enhanced controls (e.g. monitoring of IT administrator actions).

Current State Assessments for IAM Components

Advise

Assesses the current maturity of IAM-related controls and pinpoints key improvement areas.

IAM Functionality Design and Preparation for Implementation

Advise | Implement

Formalizes requirements, designs a fitting solution landscape by selecting the most appropriate solution set, and transforms the organization and its processes to optimize returns on IAM investments.

IAM Platform Deployment

Implement

Makes the IAM vision a reality by implementing IAM solutions to support your IAM processes with Deloitte key technology partners (SailPoint, OKTA, CyberArk, and ForgeRock).

Reach of IAM Platform Extension

Manage

Integrates business applications with the IAM platform to increase the reach of automated controls.

[Home](#)[Foreword](#)[Cyber Strategy](#)[Secure](#)[Infrastructure Protection](#)[Vulnerability Management](#)[Application Protection](#)[Identity and Access Management](#)[Information Privacy](#)[Information Protection](#)[Vigilant](#)[Resilient](#)[Contacts](#)[Next](#)

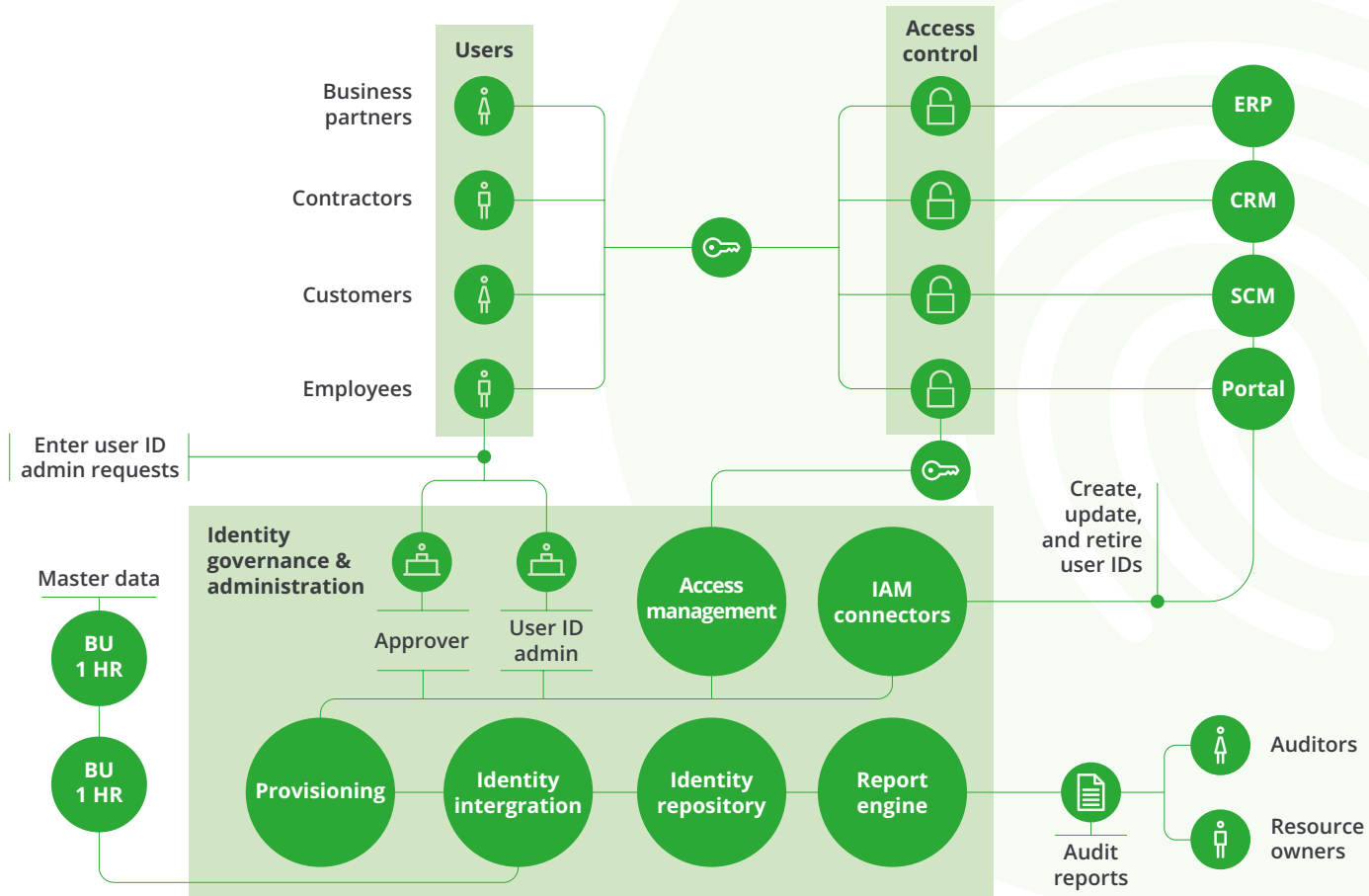


Identity and Access Management

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 and Access Management components



Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Information Privacy

Challenges

Organizations need to be able to use, analyze, and share their data while ensuring compliance with invasive regulatory control and customer/employee privacy expectations.

Greater reliance on effective data use, combined with increased regulation and control requirements, such as General Data Protection Regulation (GDPR), puts significant operational pressure on organizations.

This requires a holistic and integrated data privacy approach to an environment that is often highly segmented.

How we can help

With an excellent track record in turning privacy-related challenges into tested, modular, and pragmatic solutions, Deloitte is dedicated to supporting organizations in navigating privacy risk.

Key solutions

Privacy/GDPR Maturity Assessments and Roadmap

Advise | Implement

Assesses and identifies the current state of an organization's GDPR readiness. This includes a prioritized and risk-based roadmap that clearly identifies actionable mitigating measures and short-term fixes.

Privacy/GDPR Strategy and Transformation Program

Advise | Implement

Builds a holistic and tailored transformation program in close partnership with organizations. We help organizations incorporate fit for purpose privacy solutions in their DNA.

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

Advise | Implement | Manage

Provides hands-on, technology-enabled services and controls, using best practices,

an extensive toolkit including privacy impact assessments, GDPR/Data Protection Officer (DPO) helpdesk, GDPR stress testing, data inventory, and data mapping.

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) applications and implementation, allowing the effective sharing of personal data across borders.

Privacy/GDPR training and Awareness

Implement

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

Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next

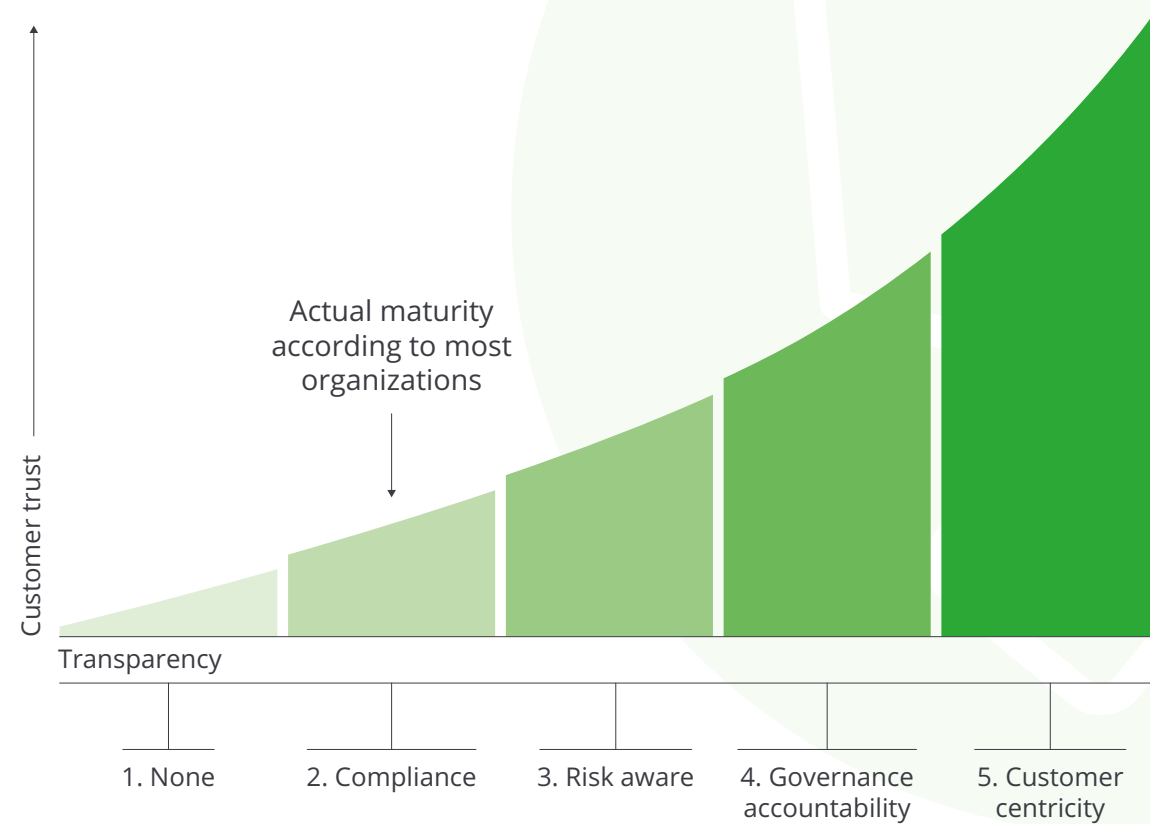


Information Privacy

Key differentiators

- Our highly integrated international team has in-depth and tested GDPR experience and ensures tailored data privacy/GDPR solutions.
- Deloitte methodology is holistic and hands-on, integrating privacy tools and in-depth data protection knowledge.

Information Privacy and Data protection maturity model



Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next



Information Protection

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 reputation damage.

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

How we 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 differentiators

- Team of experts who are technically certified and experienced in complex programs.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

Home

Foreword

Cyber Strategy



Secure



Infrastructure
Protection

Vulnerability Management

Application Protection

Identity and Access
Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



< > Next



Information Protection

Key solutions

Data Loss Prevention (DLP)

Advise | Implement | Manage

Assists in identification, monitoring, and protection of data in motion, at rest, in use, and in the cloud.

People Risk

Advise

Enables improved security awareness and culture, and understanding of insider threats focused on protecting sensitive data.

Cryptography

Advise | Implement

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

Data Governance

Advise | Implement

Enables monitoring of access activity and improved visibility of risks to stored data across the business.

Information Classification

Advise | Implement

Helps with integration and implementation of classification technology and programs.

Data Mapping and Data Inventories

Advise | Implement

Assists in understanding where data exists and how it is handled across the data management lifecycle through data flow diagrams and data inventories.

Privacy by Design

Advise | Implement

Enables the embedding of privacy into the design and day-to-day operation of information technologies and business practices; organizations can obtain Privacy By Design Certification from Ryerson University leveraging Deloitte's certification assessment framework.

Home

Foreword

Cyber Strategy



Secure



Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



Next

Vigilant

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

Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



Next



Advanced Threat Readiness and Preparation

CYBERINTELLIGENCE
center

Advanced Threat Readiness and Preparation services are driven by and fed with the latest Cyberthreat 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 we can help

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

Our 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

Advanced Threat Simulation / Red Teaming

Advise | Implement

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 will perform realistic attack scenarios to achieve predefined objectives, using social engineering, phishing, physical penetration testing, and network exploitation.

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, applying 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.

Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

Resilient



Contacts



Next

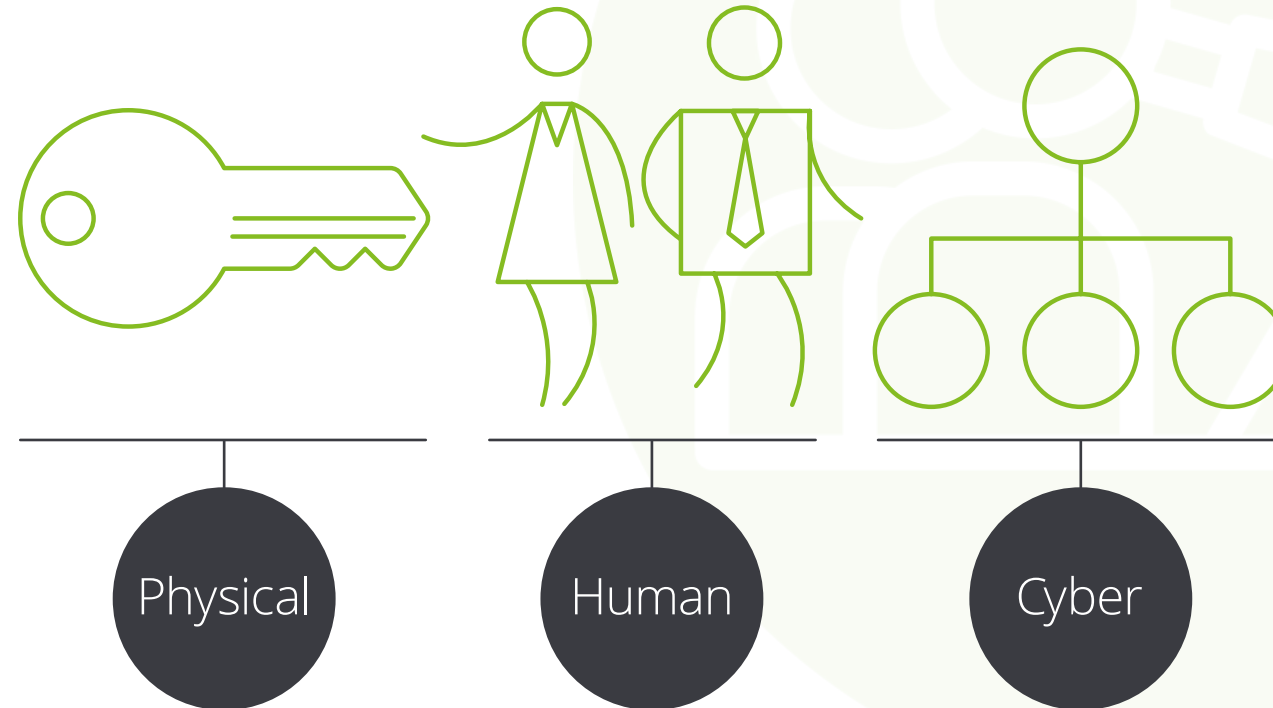


Advanced Threat Readiness and Preparation

Key differentiators

- With the Deloitte service-delivery model, organizations benefit from seamless integration with their vulnerability lifecycle management tasks.
- Our advanced services enable organizations to address emerging threats from new and disruptive technologies.
- We 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



Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

Resilient



Contacts



Next



Cyber Risk Analytics

CYBERINTELLIGENCE
center

Our solutions are supported by
Deloitte's network of 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 we can help

Deloitte's Cyber Risk Analytics services use advanced methods to analyze current cyberthreats and determine which are relevant and have the highest potential impact on strategic business objectives.

Our cyber risk analytics services are built around leading monitoring and correlation tools within the security information and event management (SIEM) and behavioral analytics markets. We employ various concepts, from log collection and correlation to behavioral analysis.

Armed with this information, organizations can focus resources on maintaining their desired security levels at minimum cost.

Key solutions

Social Listening and Analytics

Advise | Implement | Manage

Empowers organizations to do more than merely react to social media. We enable them to protect themselves, leverage opportunities, and learn the risks from these sources.

Monitoring and Correlation

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. We manage all events 24/7, using the Deloitte Security Operations Centers.

SIEM Intelligence

Advise | Implement

Improves SIEM services by assessing an organization's SIEM and analytics maturity and governance. We design a SIEM evolution roadmap, and design and develop use cases, as well as assist in SIEM provisioning.

Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



Next

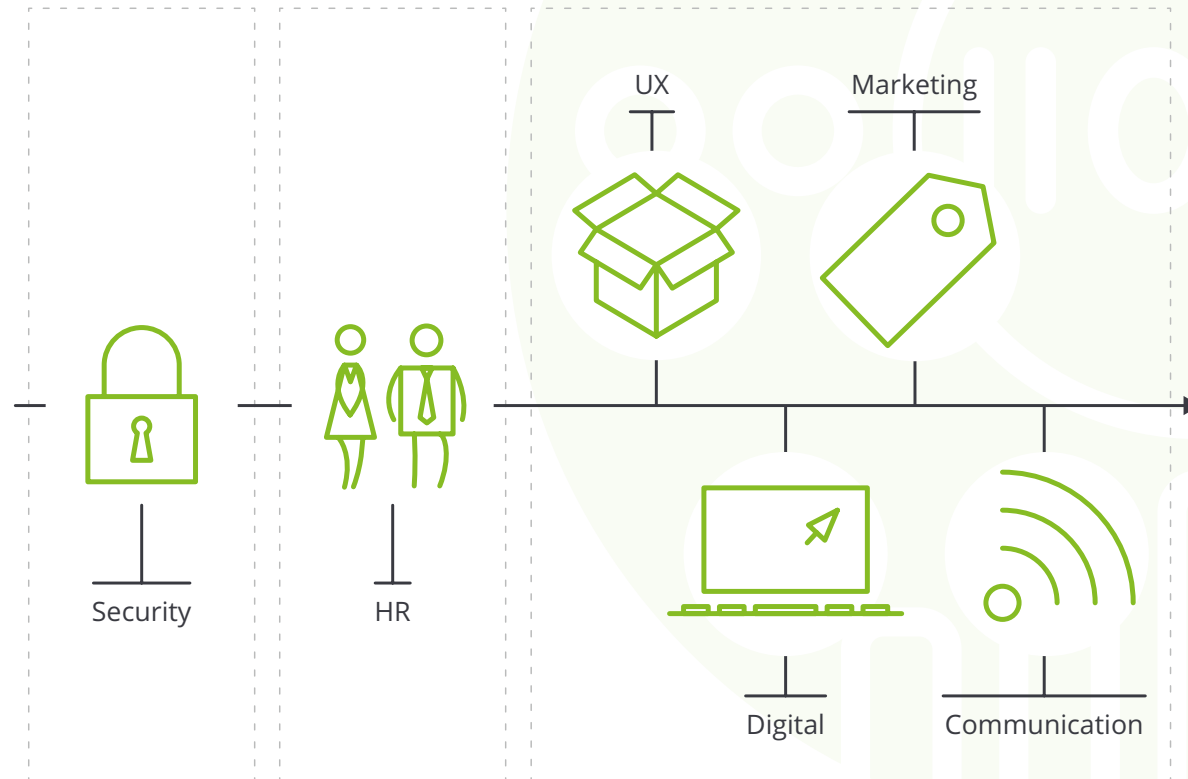


Cyber Risk Analytics

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.

Social Listening and Analytics throughout the organization



Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



< > Next



Security Operations Center (SOC)

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.

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

How we 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 work 24/7 to detect malicious activities. Deloitte professionals operate and manage security information and event management (SIEM) platforms allowing threat-hunting capabilities.

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.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



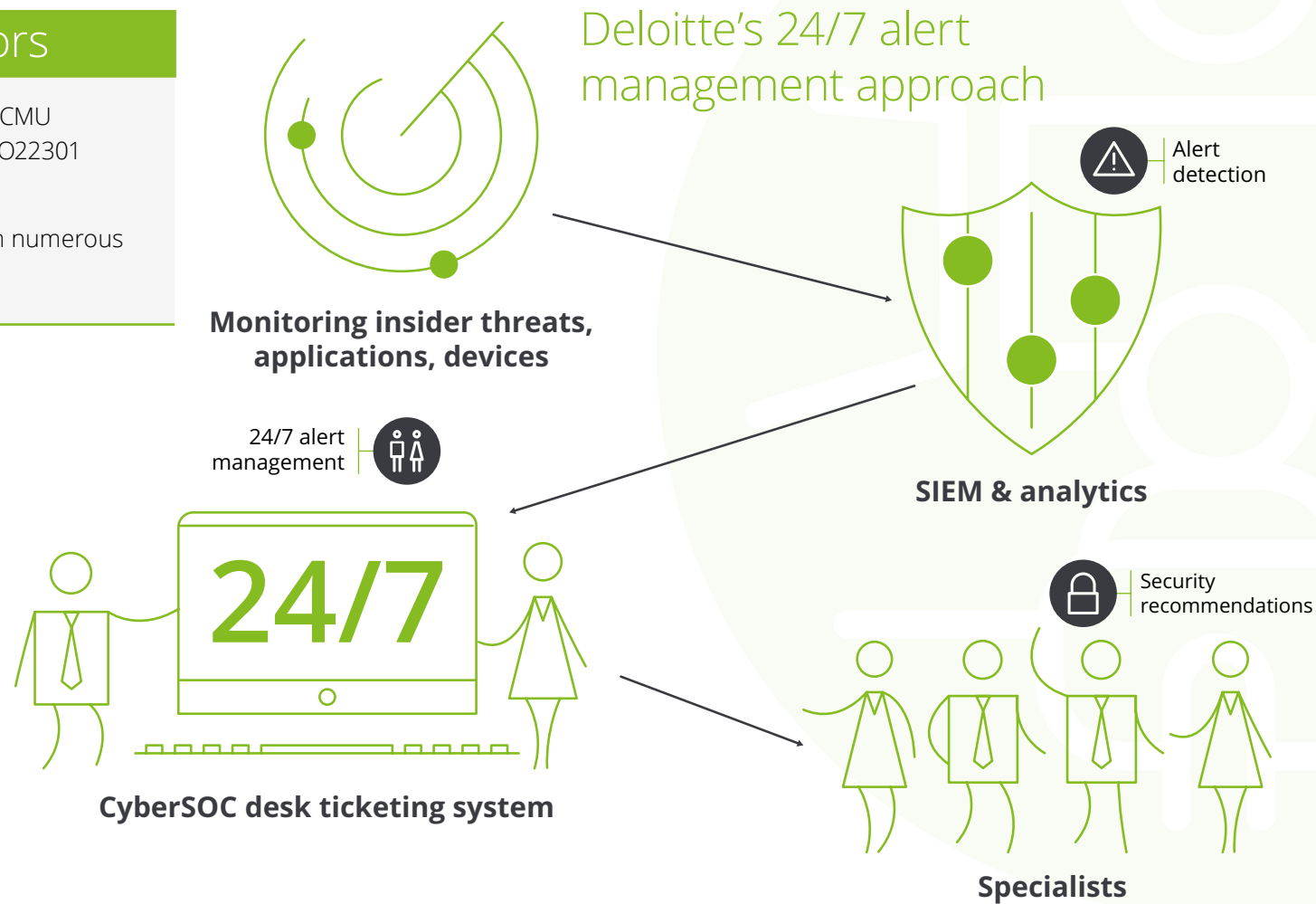
< > Next



Security Operations Center (SOC)

Key differentiators

- Deloitte's SOC is part of the CMU CERTNetwork, certified in ISO22301 and ISO27001.
- Deloitte's CICs benefit from numerous intelligence sources.



Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



< > Next



Threat Intelligence and Analysis

Challenges

Understanding the cyberthreat landscape is difficult as threats are continuously evolving.

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

How we 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

Cyberthreat Intelligence

Advise | Implement | Manage

Looks for potentially threatening events taking place outside the organization's perimeter and provides custom insights in line with the organization's strategic and intelligence requirements.

Forecasting Emerging Threat

Manage

Forecasts emerging threats, enabling organizations to adapt their security methods and policies to future threats.

Intelligence Collection Grid

Manage

Collects and stores intelligence events from multiple sources around the globe and over time prevents, investigates, and forecasts threats.

Threat Modeling

Advise | Implement | Manage

Identifies assets, threat actors, vulnerabilities, targets, methods, and associated countermeasures to prevent or mitigate the effects of potential threats on an organization.

Cyber Trend Report

Advise | Manage

Illustrates how threat actors work through a compilation of relevant threats across a set period of time and provides statistics, trends and a summary of the organization's cyberthreat landscape.

CYBERINTELLIGENCEcenter

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.

Home

Foreword

Cyber Strategy



Secure



Vigilant



Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

Resilient



Contacts



< > Next



Threat Intelligence and Analysis

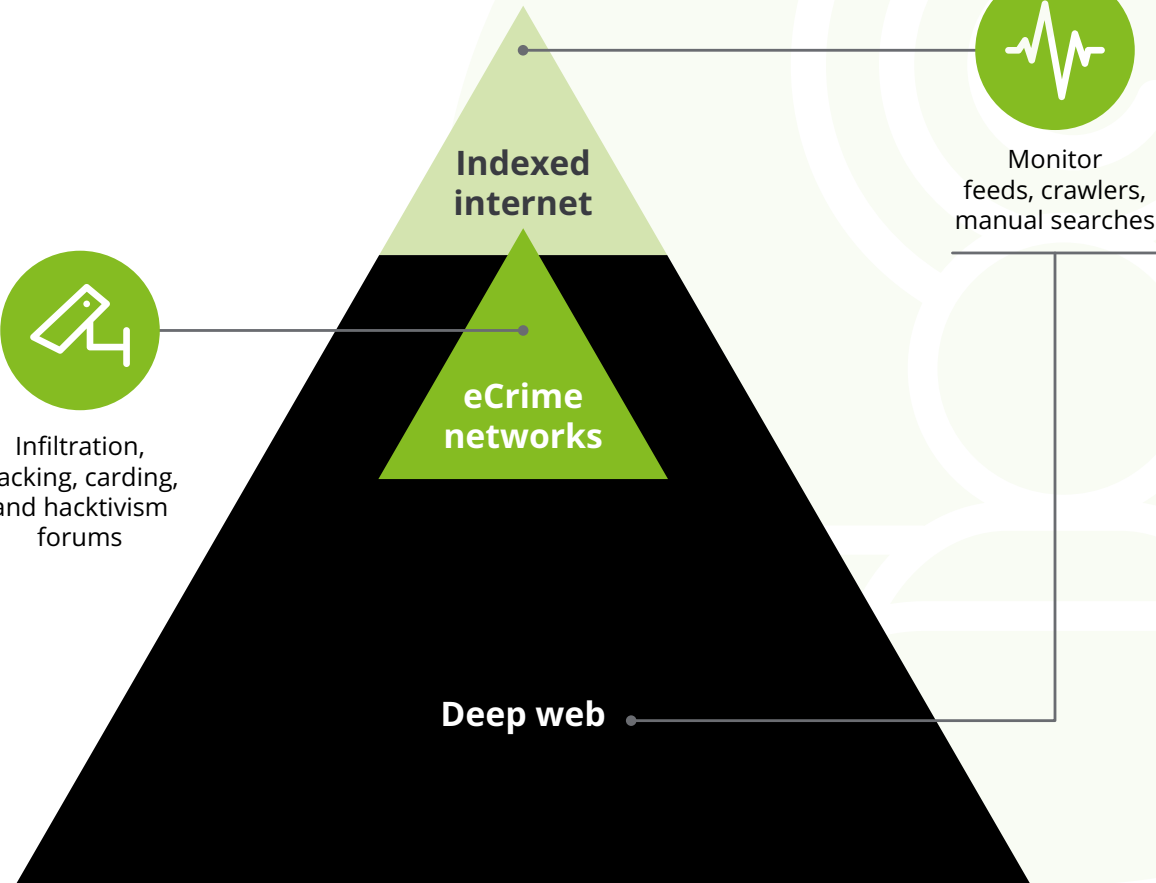
Key differentiators

- We provide 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.
- Our experienced analysts 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.

Cyberthreat Intelligence 24/7



Infiltration,
hacking, carding,
and hacktivism
forums



Home

Foreword

Cyber Strategy



Secure



Cyber Vigilance



Advanced Threat
Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence
and Analysis

Resilient



Contacts



< > Next

Resilient

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

Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient

Cyber Incident
Response

Cyber Wargaming



Contacts



Next



Cyber Incident Response

CYBERINTELLIGENCE
center

Our solutions are supported by
Deloitte's network of CICs

Challenges

Cyberthreats are constantly evolving and increasing in volume, intensity, and complexity. Cyber crisis management has therefore become a major focus of 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 we 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.

We can help organizations to improve their cyber response capabilities, establishing a high level of readiness through effective preparation, training, and simulations. We provide real-time, on-site, and 24/7 support for a cyber incident or crisis that could harm strategic objectives, revenue, reputation, or viability.

Key solutions

Cyber Crisis Management

Advise | Implement | Manage

Assists your executive leadership to improve their strategic crisis management decision-making capabilities, helping them respond effectively to a large-scale crisis event and emerge stronger. We have one of the largest, most respected teams of crisis and continuity management professionals in the world.

Cyber Incident Response

Advise | Implement | Manage

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

IT Resilience and Recovery

Advise

Provides support in enacting your contingency plans and returning technical operations to a normal state after a cyberattack or other disruption.

Breach Notification and Response

Advise | Implement

Provides analysis and guidance for notification and response based on new regulations which require specific responses from organizations following a data breach.

Cyber Forensic Services

Advise | Implement | Manage

Investigates cybercrimes to determine the nature, extent, means, and origin of an incident. This supports organizations in any legal actions they may need to take.

Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient



Cyber Incident
Response

Cyber Wargaming

Contacts



< > Next



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.

Our services are supported by the Deloitte network of CICs, providing 24/7 support 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.



Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient



Cyber Incident Response

Cyber Wargaming

Contacts



< > Next



Cyber Wargaming

Challenges

Organizations are not prepared to counter cyber crime unless they have been tested. An incident and crisis management response framework is not enough.

Organizations must test their defense plans regularly if they are to be confident about their ability to respond effectively to threats.

How we can help

The Deloitte Wargaming portfolio of services creates an environment for client teams to simulate incidents and crises, allowing them to develop coordinated responses and identify areas that need improvement in order to prepare for a real-world threat.

These exercises are particularly relevant for cyberthreats that 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

Increases awareness and supports the development of cyber crisis management plans, procedures, roles, and responsibilities. They focus on detailed discussion of an unfolding pre-prepared scenario, often split into key incident/crisis response phases. We also run more technical 'Breach Readiness Workshops' to help validate, check, and challenge existing response processes and playbooks.

Cyber Table-Top Exercise

Advise

Guides teams in reviewing plans and processes, and practice their roles and responsibilities. The exercises often focus on sharpening specific skills (such as logging, conducting risk assessments, and rehearsing decision-making processes) and identify 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.

[Home](#)[Foreword](#)[Cyber Strategy](#)[Secure](#)[Vigilant](#)[Resilient](#)[Cyber Incident Response](#)[Cyber Wargaming](#)[Contacts](#)[Next](#)

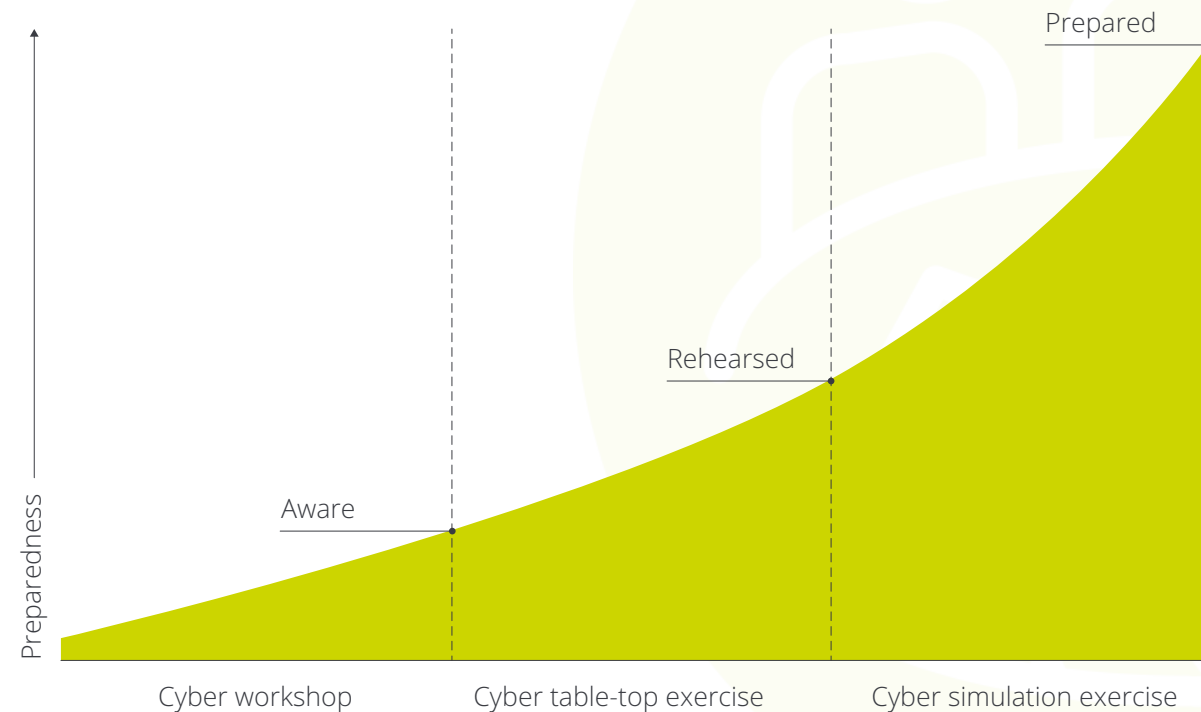


Cyber Wargaming

Key differentiators

- Deloitte's capability has been built through years of practical experience, delivering hundreds of simulations at board, executive, and operational levels.
- We use 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.
- We use 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



Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient



Cyber Incident Response

Cyber Wargaming

Contacts



< > Next



Contacts

Nick Galletto

Global and Americas Cyber Risk Leader
ngalletto@deloitte.ca

Chris Verdonck

EMEA Cyber Risk Leader
cverdonck@deloitte.com

James Nunn-Price

Asia Pacific Cyber Risk Leader
jamesnunnprice@deloitte.com.au

[Home](#)[Foreword](#)[Cyber Strategy](#)[Secure](#)[Vigilant](#)[Resilient](#)[Contacts](#)

Next



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) 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 entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2017. For information, contact Deloitte Touche Tohmatsu Limited.