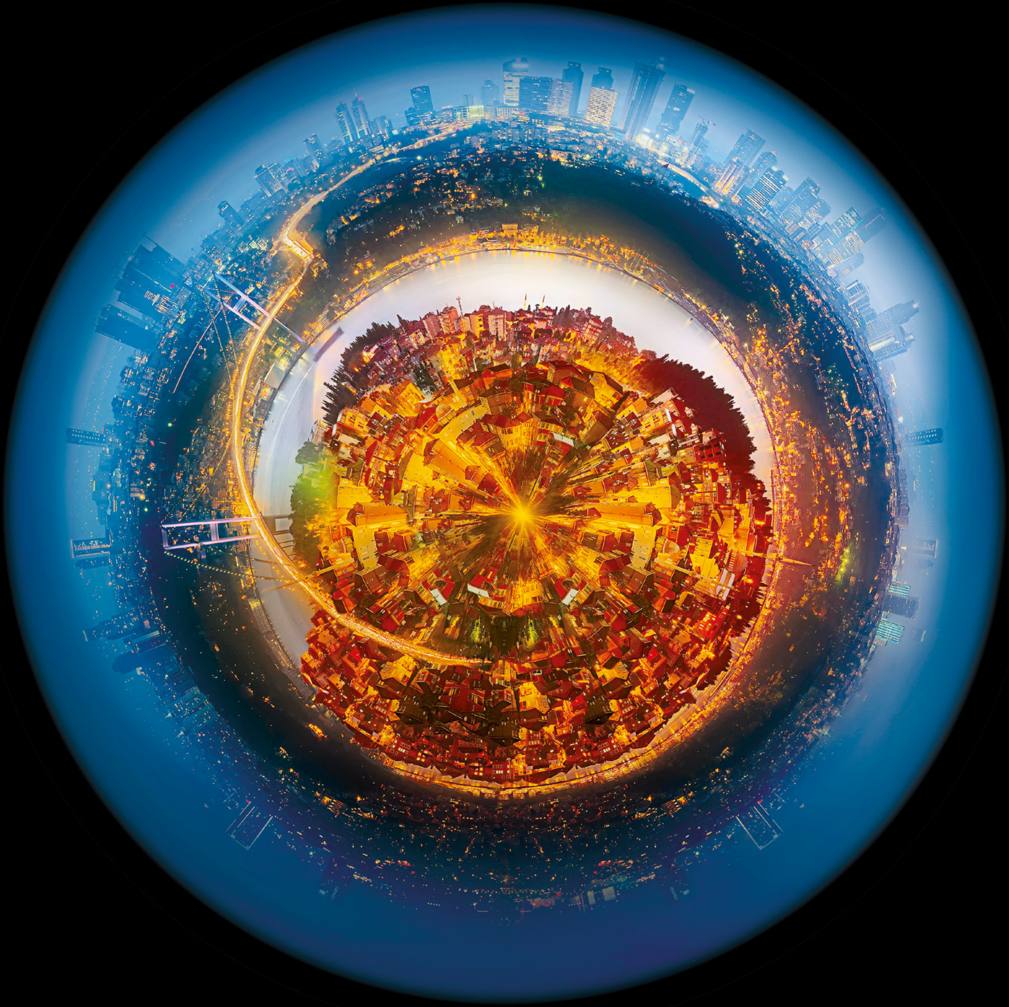
Deloitte.



Deloitte Cyber Risk Capabilities in the Middle East

Cyber Strategy, Secure Vigilant and Resilent

Cyber Risk ●

Contents

Foreword

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

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 Middle East 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.

Deloitte's Cyber Risk Practices throughout the Middle East provide the same exceptional quality of service in all 14 capability areas showcased in this document.

Fadi Mutlak
Middle East Cyber Risk Leader

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

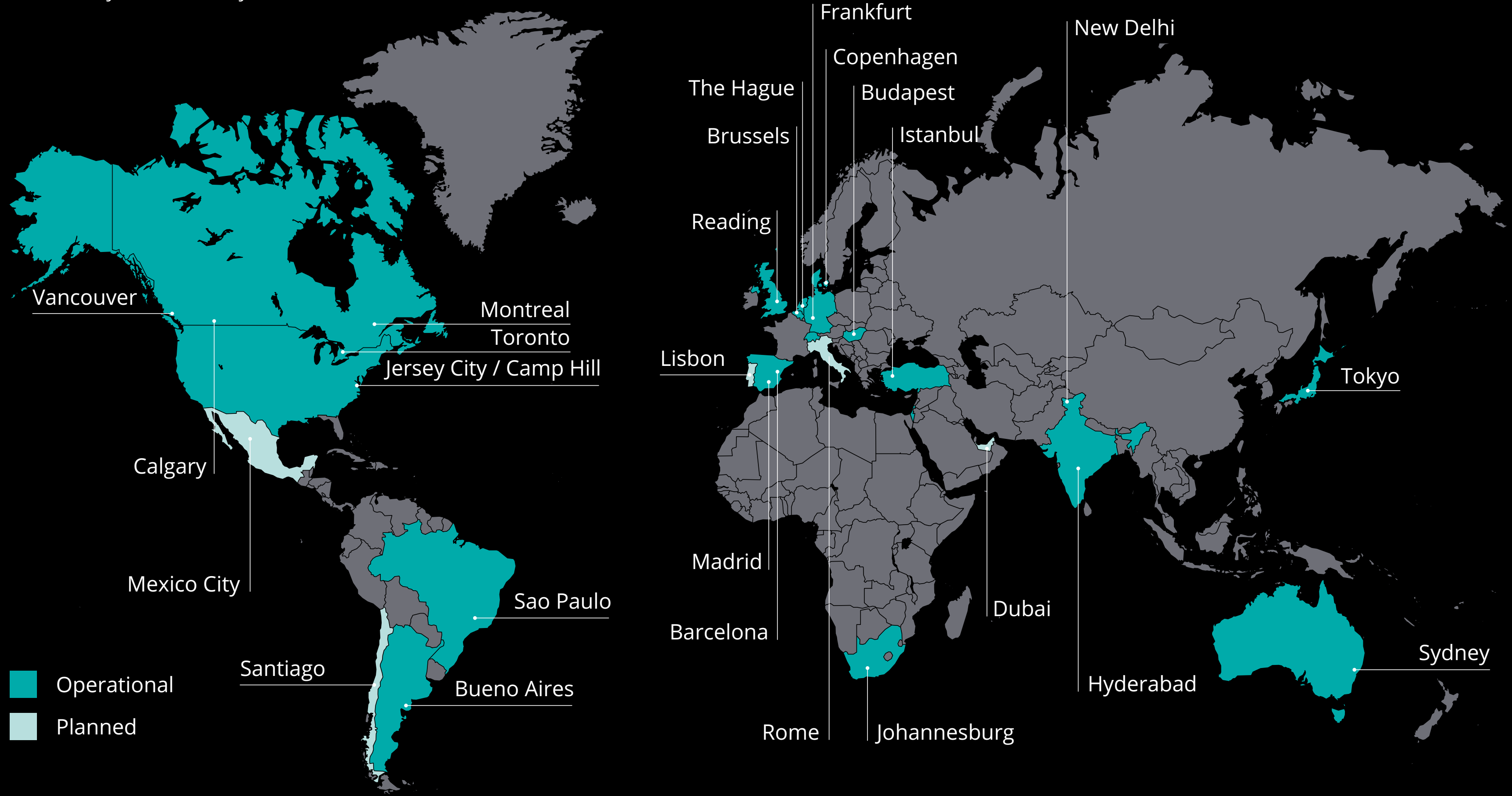
Next

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

CYBER
INTELLIGENCE
CENTER

Our solutions are supported by Deloitte's 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.



🟩 Operational
▢ Planned

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, 2015. This is the fourth consecutive year that Deloitte has been awarded the #1 ranking.

Deloitte named a global leader in cybersecurity consulting by ALM Intelligence

ALM Intelligence (a research firm, formerly known as Kennedy) 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.”

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

ALM Intelligence 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.”

Deloitte qualified professionals

Our consultant of all grades hold key professional and industry certifications, such as CISSP, CISM, ISO27001, COBIT, ITIL, CDPP, 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 cybersecurity

More than 1,500 **Cyber Risk professionals across EMEA**

Cyber Strategy

We help 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

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.

Infrastructure Protection.

Vulnerability Management.

Application Protection.

Identity and Access Management.

Information Privacy and Protection.

Vigilant

We integrate 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 Operations Center.

Threat Intelligence and Analysis.

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.

Cyber Incident Response.

Cyber Wargaming.

Delivery models

Advise

Implement

Manage

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

Cyber Strategy

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

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 cyber-threat 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 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 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 cyber-threat 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

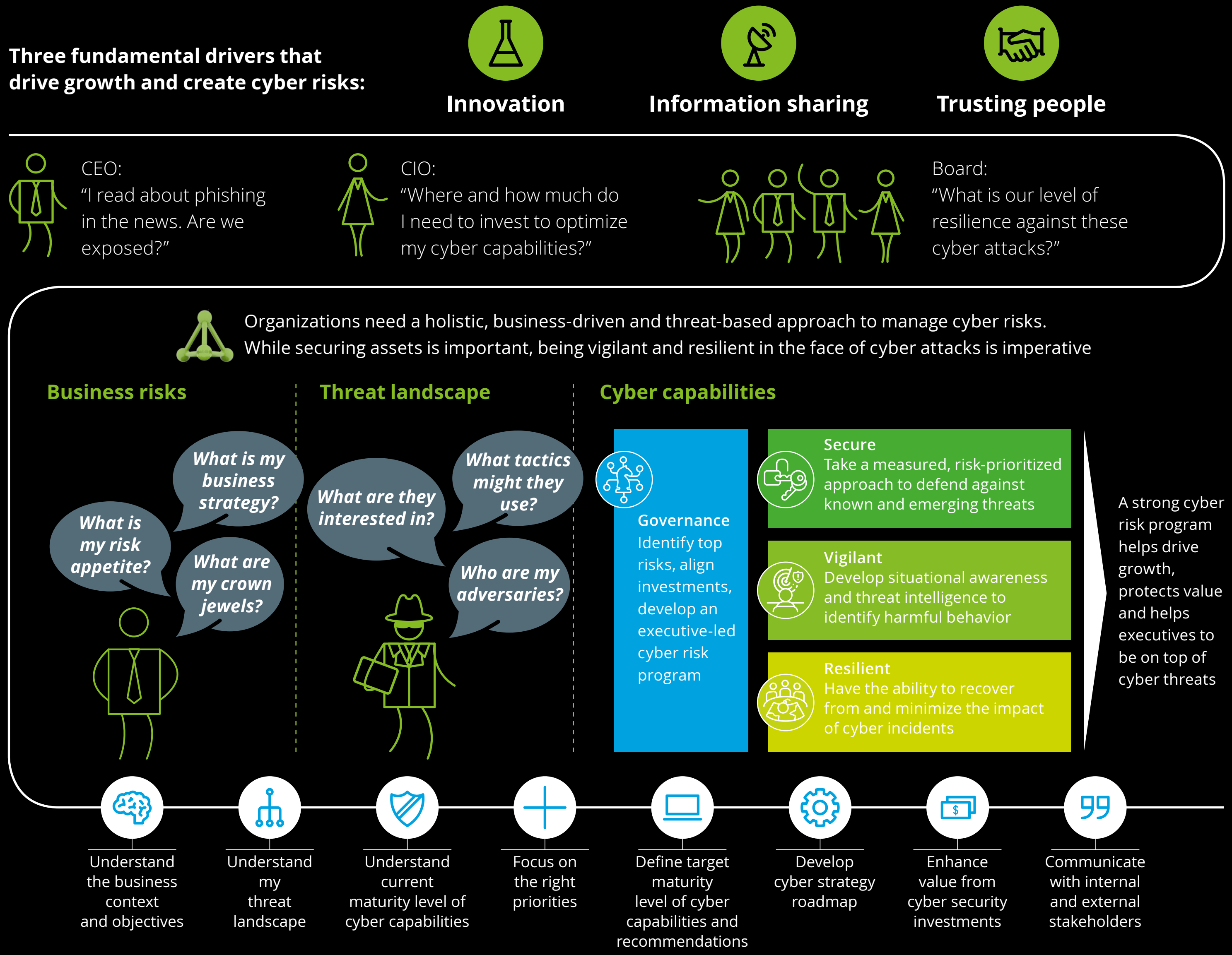
- The Deloitte Cyber Strategy framework measures cyber posture and threat exposure.
- A leading catalog of good practice standards for cybersecurity, with proven success across industry sectors.

Deloitte's own Cyber Strategy Framework

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 risk appetite?
What is my business strategy?
What are my crown jewels?

Threat landscape

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

- Understand the business context and objectives
- Understand my threat landscape
- Understand current maturity level of cyber capabilities
- Focus on the right priorities
- Define target maturity level of cyber capabilities and recommendations
- Develop cyber strategy roadmap
- Enhance value from cyber security investments
- Communicate with internal and external stakeholders

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 to: 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 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 the use of best practices as guiding principles. Developing policies, procedures and standards.

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.

Security and Regulatory Compliance

Advise | Implement

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

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.

Our alliances

servicenow

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 cyber threats.

Deloitte can help organizations to 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 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).

Cyber Training, Education and Awareness

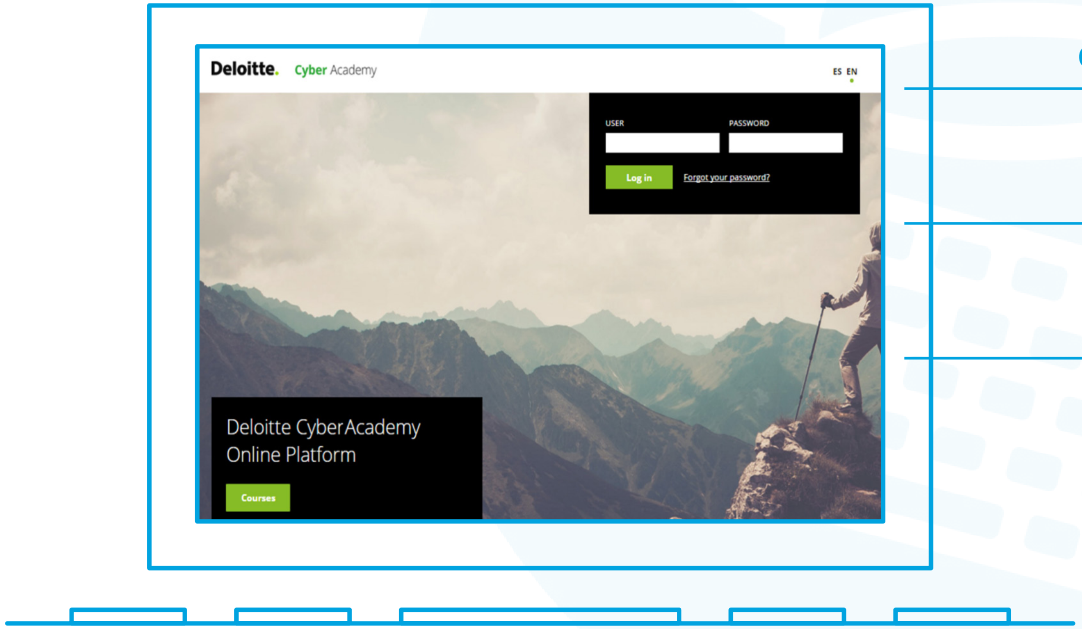
CYBER
INTELLIGENCE
CENTER

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

Key differentiators

- We deliver online and on-site technical training and awareness programs to clients and internal practitioners via a dedicated EMEA 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.

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 continuously to acquire, store and use large amounts of data, a significant proportion of which will be sensitive. Protecting this data against cyber-attack is of paramount importance.

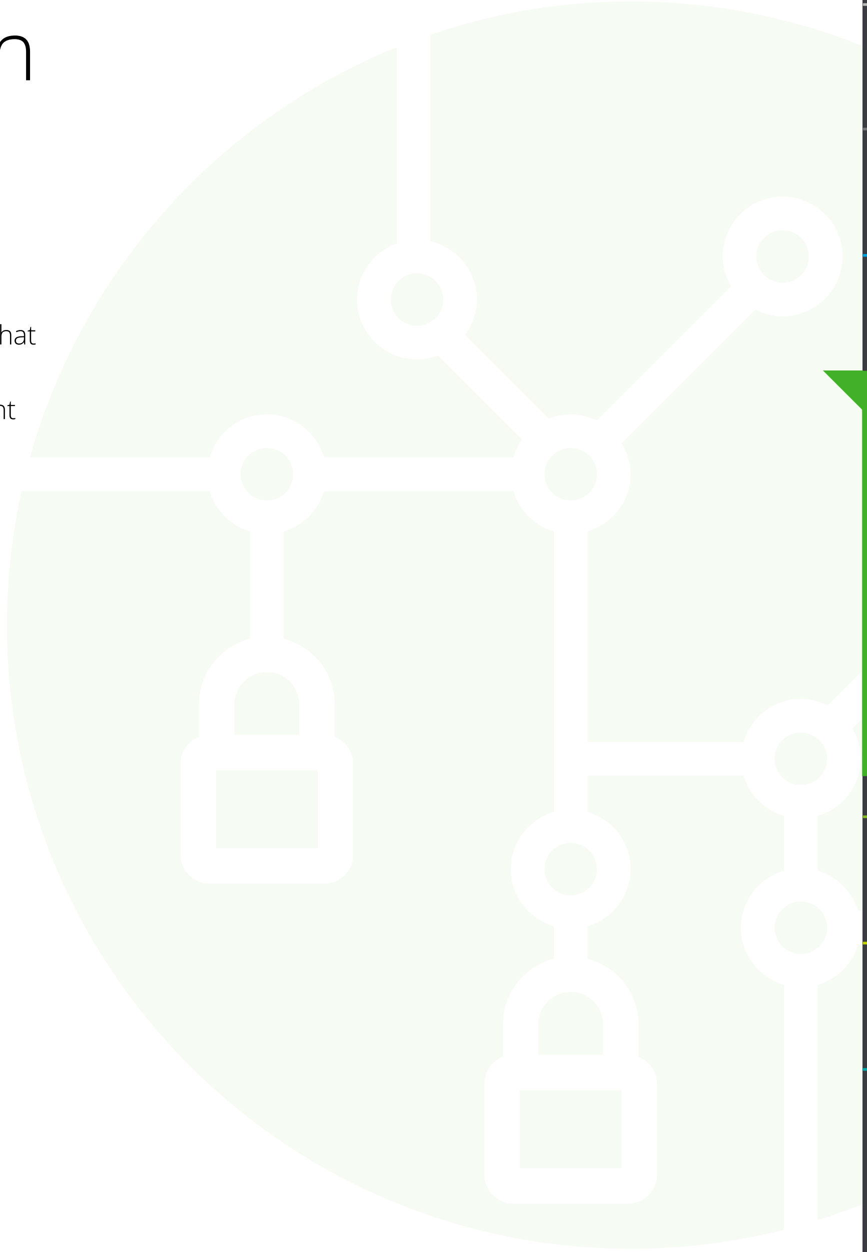
Today's smart cybersecurity protects data by using secure data platforms, clear data governance and smart access protocols such as electronic finger printing.

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

CYBER
INTELLIGENCE
CENTER

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

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 shoulder to shoulder 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.

Vulnerability Management

CYBER
INTELLIGENCE
CENTER

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

Next

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 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 assess thoroughly the protection level of applications.

With specialized knowledge of a large number of specific applications and secure development methods, Deloitte helps with secure 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 establish if security is appropriately incorporated. In addition, we help organizations to embed Secure by Design principles and controls.

Application Protection

Deloitte GAST 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

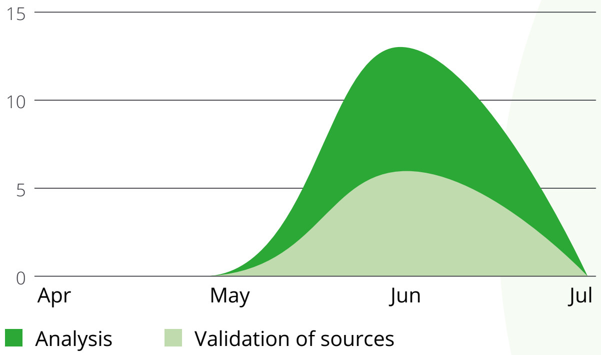
Key differentiators

We leverage static application security testing technology which enables the client to be one step ahead, with forty percent portfolio coverage versus five percent portfolio coverage using the traditional approach.

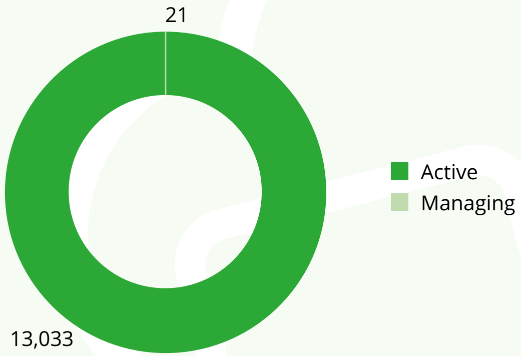
- We help organizations to raise their situational risk awareness and actionable remediation insights, empowering them to regulate application portfolios effectively.

Source code analysis overview

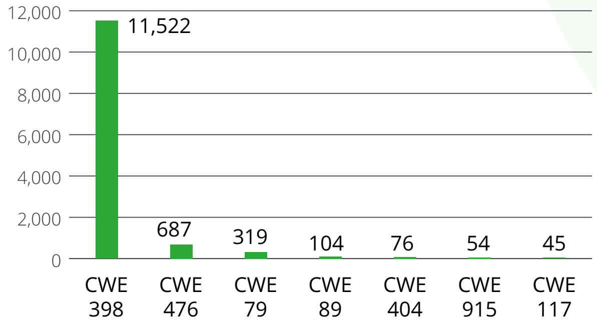
Analysis and validation of sources



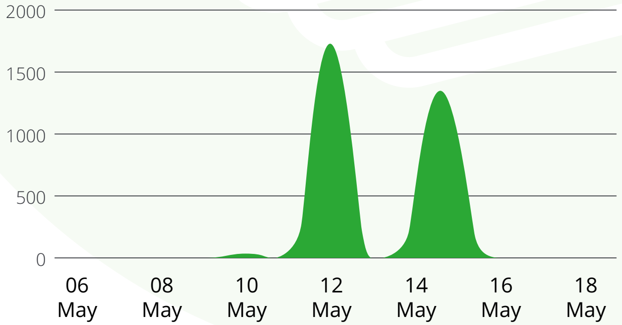
Weaknesses found



Top CWEs detected



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 classical network perimeter has faded. In response, organizations increasingly focus 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 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

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.

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.

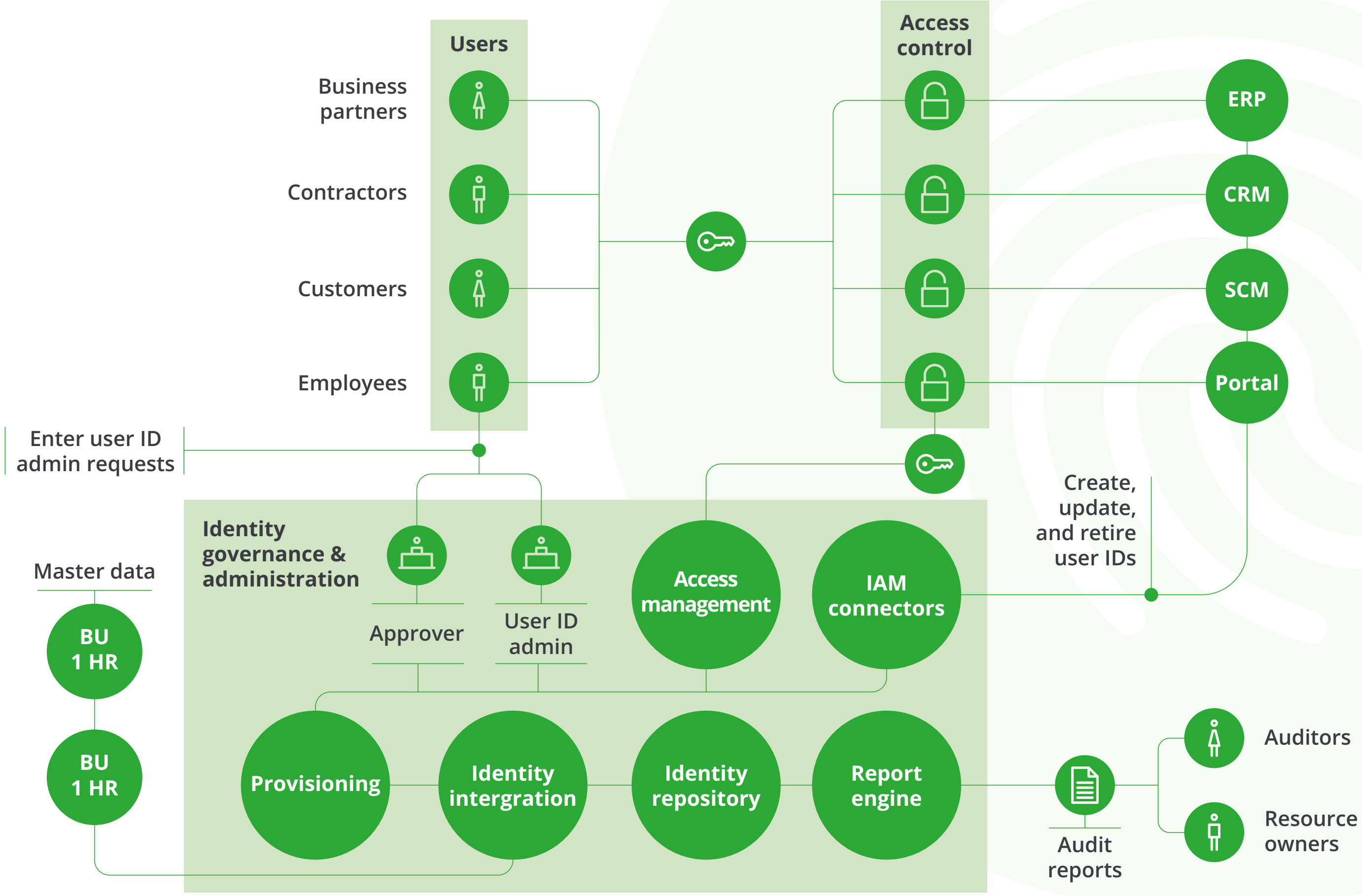
Our alliances

SailPoint

okta

CYBERARK

Identity and Access Management components



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.

Ever-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 bringing 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 to 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

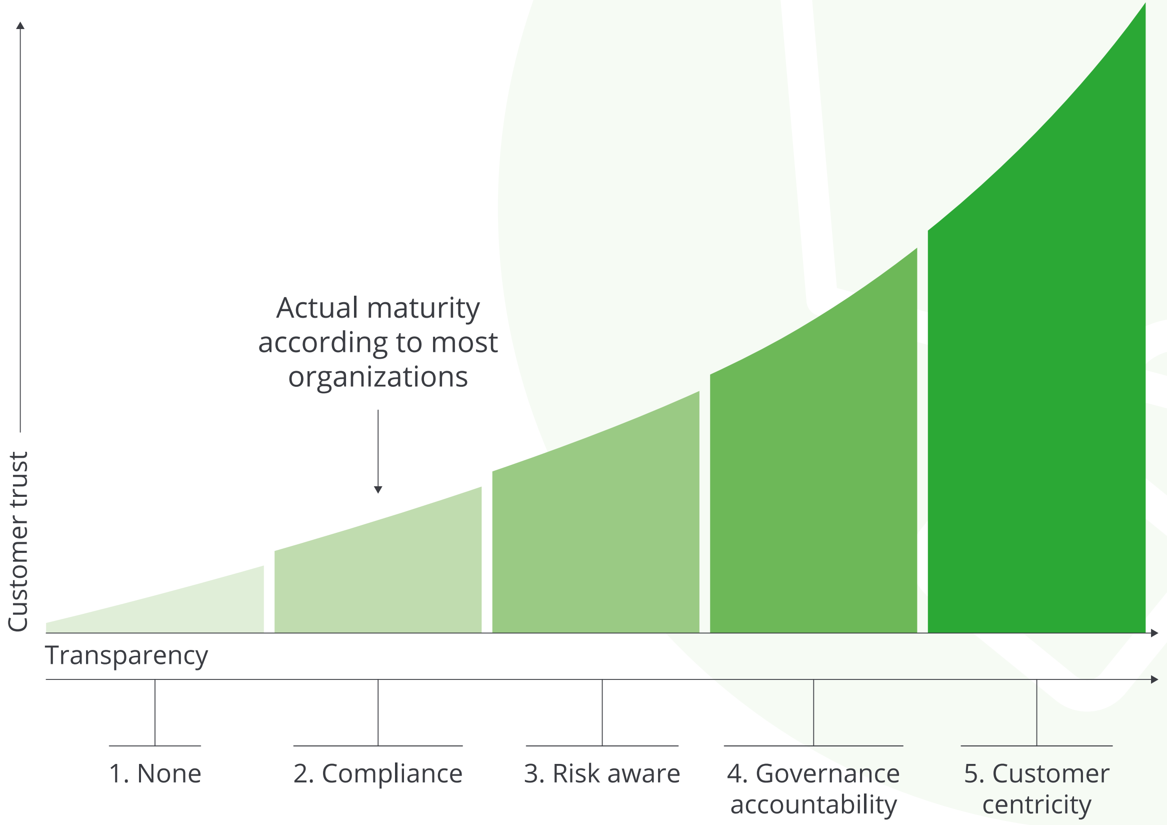
Offers tailored GDPR awareness and training, on-site or via e-learning/classroom formats, using, for example, the Deloitte EMEA Privacy Academy, and covering both GDPR compliance and its operational/technical implications.

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



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 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 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.

Information Protection

Key differentiators

- Global alliances, such as with Symantec and IBM, enable us to offer end-to-end solutions with deep technical expertise.
- Team of experts across EMEA who are technically certified and experienced in complex programs.

Our alliances

Symantec™

IBM® Platinum Business Partner

TITUS

Vigilant

We integrate 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
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 we 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 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,

Malware 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

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

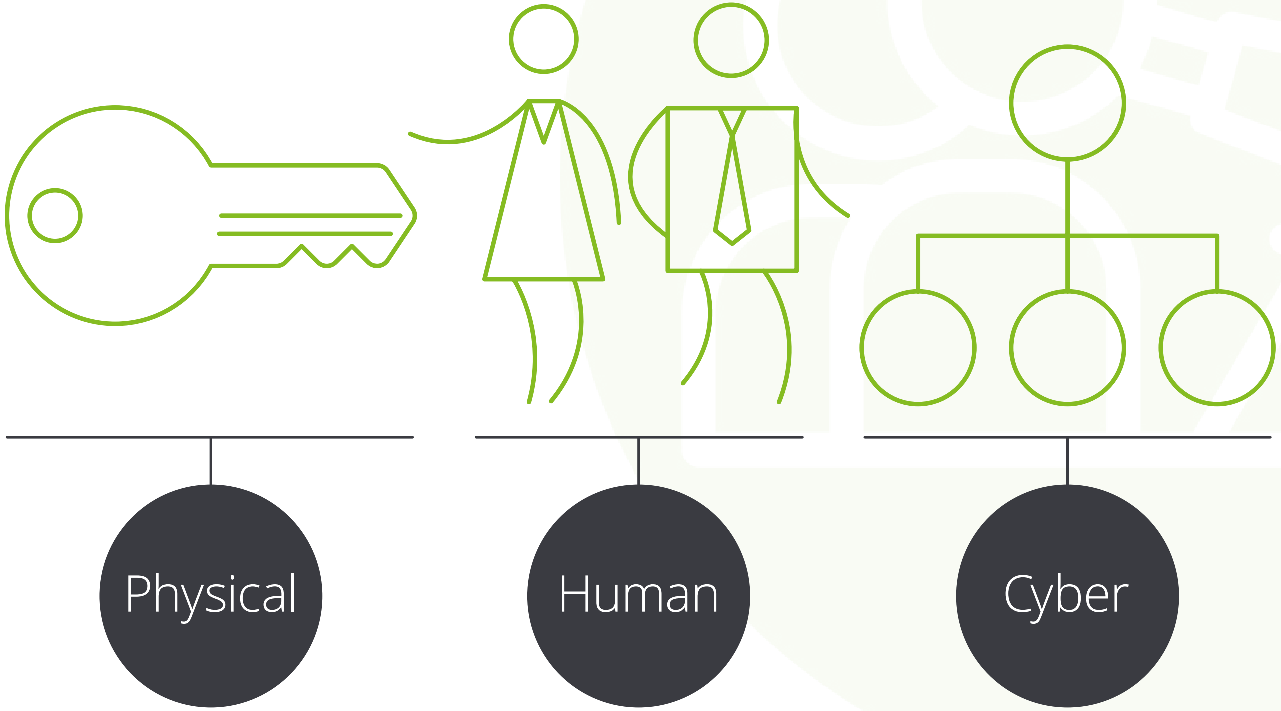
Home
Foreword
Cyber Strategy
Secure
Vigilant
Advanced Threat Readiness and Preparation
Cyber Risk Analytics
Security Operations Center
Threat Intelligence and Analysis
Resilient
Contacts
Next

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



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 we can help

Deloitte's Cyber Risk Analytics services use advanced methods to analyze current cyber threats 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

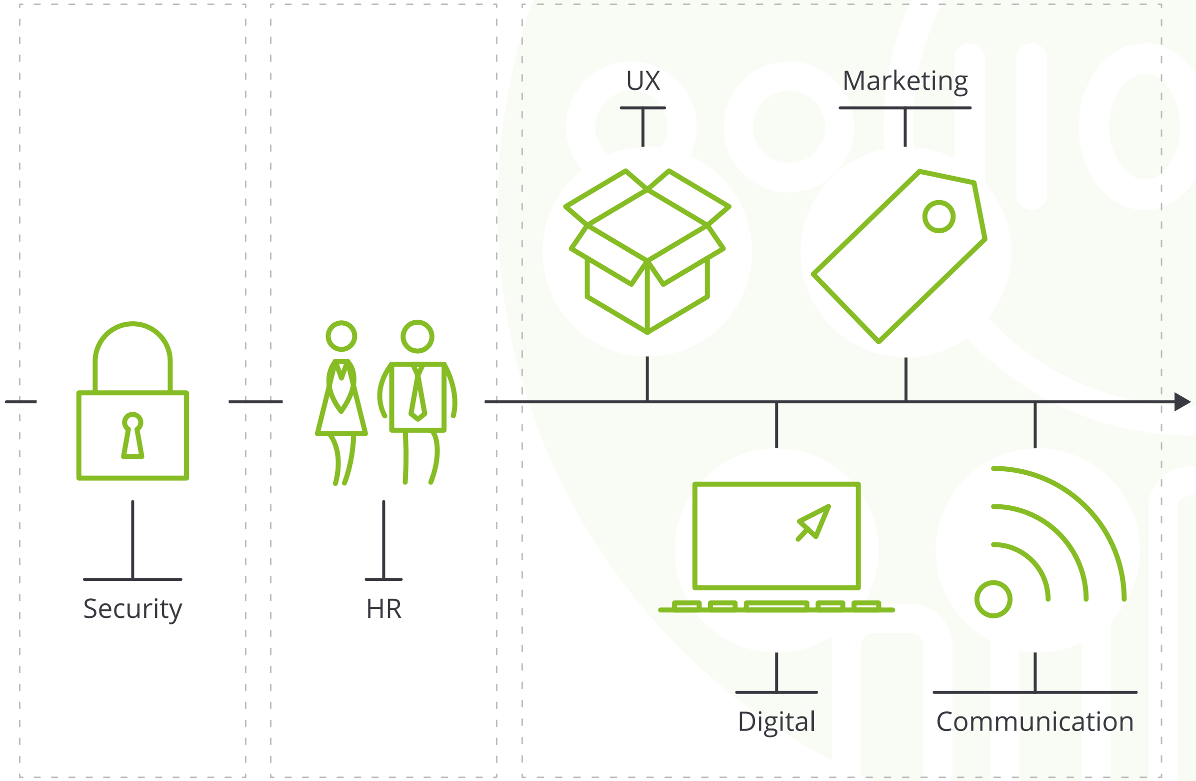
Improves SIEM services by assessing an organization's SIEM and analytics maturity and governance. We design a SIEM evolution roadmap, and design and develop use cases, as well as assist in SIEM provisioning.

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



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.

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. Use 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.

SOC Cyber Security Dashboard

Advise | Implement | Manage

Defines and develops cyber risk metrics, indicators and dashboards to provide insight into the operational effectiveness of the SOC.

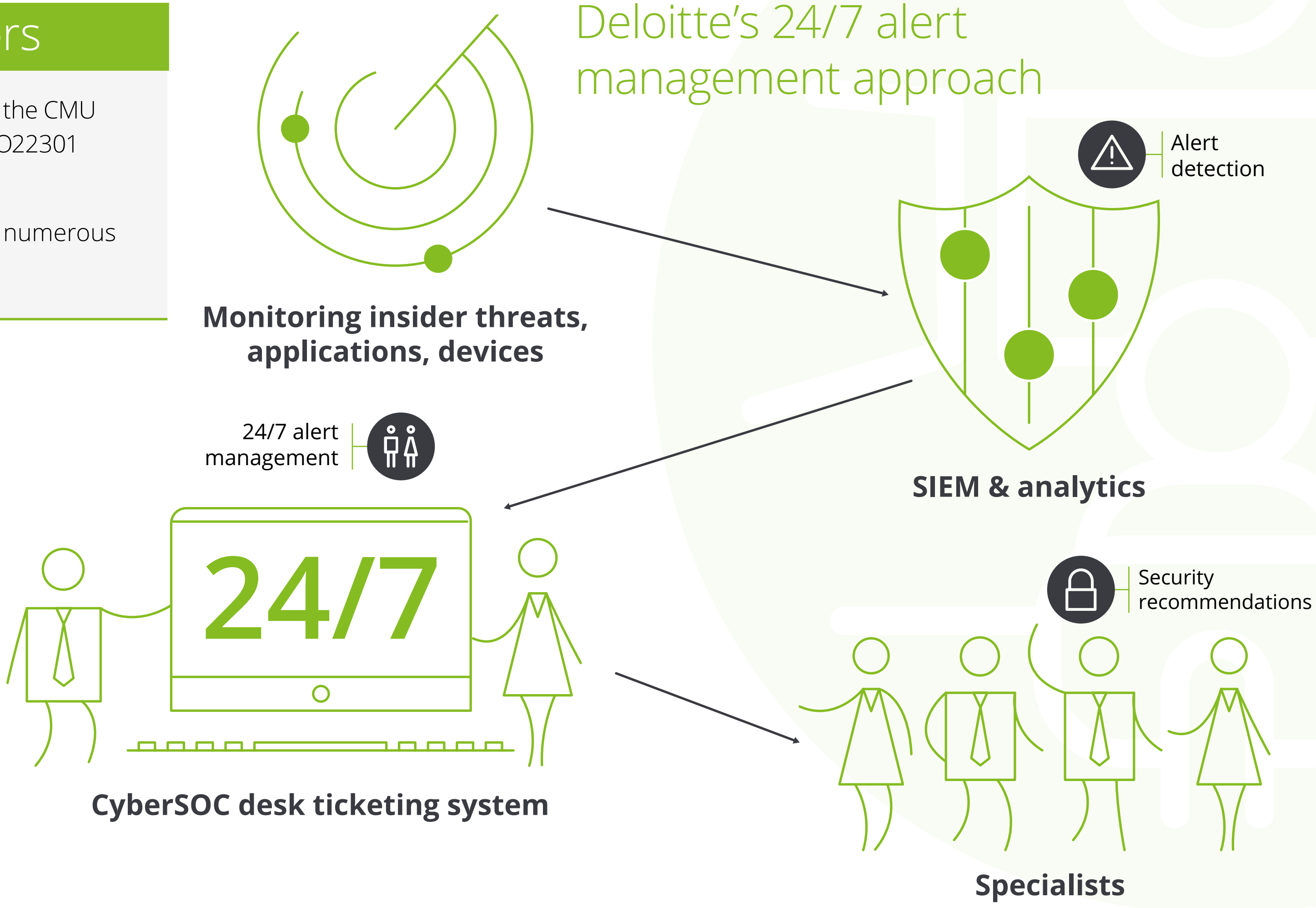
Home
Foreword
Cyber Strategy
Secure
Vigilant
Advanced Threat Readiness and Preparation
Cyber Risk Analytics
Security Operations Center
Threat Intelligence and Analysis
Resilient
Contacts
Next

Security Operations Center (SOC)

Key differentiators

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

Deloitte's 24/7 alert management approach



Threat Intelligence and Analysis

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 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

Cyber Threat Intelligence

Advise | Implement | Manage

Looks out 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 Modelling

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

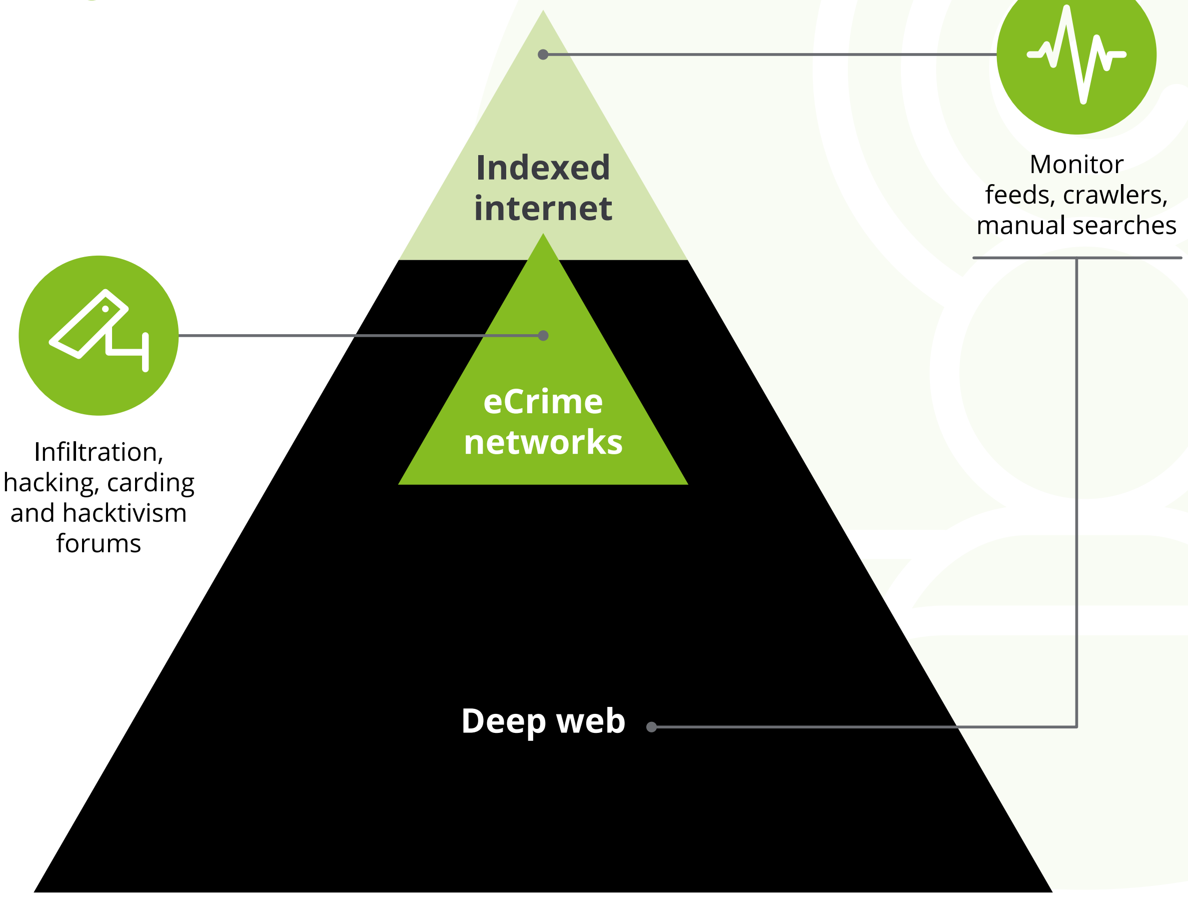
Illustrates how threat actors work through a compilation of relevant threats across a set period of time and provides statistics, trends and a summary of the organization's cybersecurity threat landscape.

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.

Cyber Threat Intelligence 24/7


Indexed internet
eCrime networks
Deep web
Monitor feeds, crawlers, manual searches
Infiltration, hacking, carding and hacktivism forums

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

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 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

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

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 threats.

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 analyzes 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.

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 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 gets special call-out in the Vanguard not only for its impressive capabilities – even within the context of the Big Four – but because it has taken steps to elevate crisis management to a more strategic level."*

2015 Kennedy Report: Event-Driven Consulting in Financial Services: Crisis Advisory in the New Regulatory Framework

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 cyber threats 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

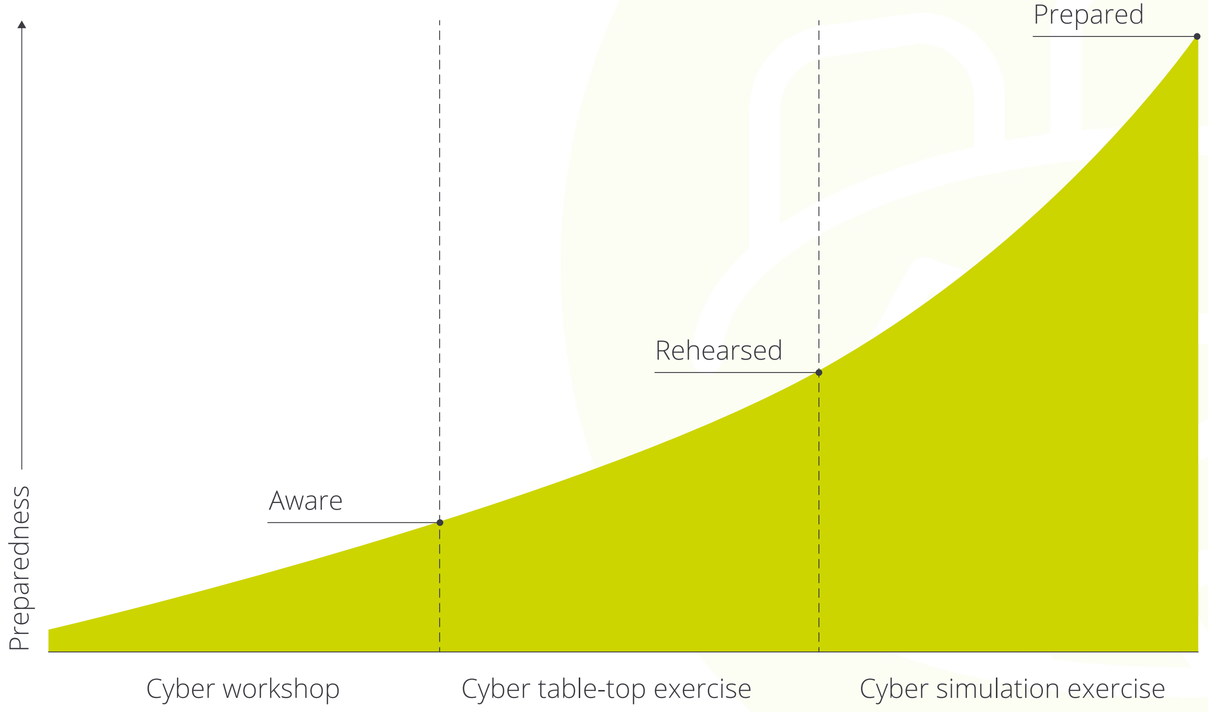
Rehearses or stress-tests existing plans and procedures against complex and multi-faceted cyber incidents or crises. Exercises are designed to take place in a realistic, real-time and 'live' controlled environment – often involving multiple levels of an organization operating remotely on a global scale. 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.

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



Contacts

Fadi Mutlak
ME Cyber Risk Leader
fmutlak@deloitte.com

UAE
Ziad Haddad
zhaddad@deloitte.com

Qatar
Amandeep Arneja
aarneja@deloitte.com

Saudi Arabia
Nader Farid
nfarid@deloitte.com

Kuwait
Tamer Charife
tcharife@deloitte.com

Cyber.Strategy
Trajce Dimkov
trdimkov@deloitte.com

Cyber.Resilient
Maher Yamout
myamout@deloitte.com

Cyber.Secure
Nithin Haridas
niharidas@deloitte.com

Cyber.Vigilant
Nithin Haridas
niharidas@deloitte.com

Home
Foreword
Cyber Strategy
Secure
Vigilant
Resilient
Contacts
Next

Deloitte.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte & Touche (M.E.) would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte & Touche (M.E.) accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

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 and their related entities 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, 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.

Deloitte & Touche (M.E.) is a member firm of Deloitte Touche Tohmatsu Limited (DTTL) and is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DTME’s presence in the Middle East region is established through its affiliated independent legal entities which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DTME’s affiliates and related entities cannot oblige each other and/or DTME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable only for its own acts or omissions and not those of any other affiliate.

Deloitte provides audit, tax, consulting, and financial advisory services through 25 offices in 14 countries with more than 3,300 partners, directors and staff. It is a Tier 1 Tax advisor in the GCC region since 2010 (according to the International Tax Review World Tax Rankings). It has also received numerous awards in the last few years which include best Advisory and Consultancy Firm of the Year 2016 in the CFO Middle East awards, best employer in the Middle East, the Middle East Training & Development Excellence Award by the Institute of Chartered Accountants in England and Wales (ICAEW), as well as the best CSR integrated organization.