Cyber Intelligence Centre

Is your business security centred?

Minimize cyber risk with a managed security service solution

Deloitte.

Cyber threats are real ...

In recent years, cyberattacks have become increasingly coordinated and sophisticated, with cyber criminals targeting specific organizations, regions and customer profiles. To prevent potential financial, reputational and operational damage, organizations must go beyond the IT function. Senior management, legal counsel and boards must take proactive steps to strengthen cyber resiliency.

To assess your preparedness, answer a few critical questions, such as:

- What is your cyber security strategy?
- What capabilities do you have right now and how confident are you that it's working?
- What procedures would you follow if you were under attack?

Get the answers you need

Deloitte's Cyber Intelligence Centre (CIC) helps you manage cyber risks with a range of customized, integrated security services that deliver 24x7, business-focused security for your critical systems and data.

Identified as a Kennedy Vanguard Leader for having the most comprehensive competency strengths across the cyber spectrum, Deloitte provides security services to some of the world's largest organizations.

and growing

Global scope. Customized focus.

Globally, we have over 900 Certified Information Systems Security Professionals (CISSP), 1,500 Certified Information Systems Auditors (CISA), 150 Certified Information Security Managers (CISM) and 65 Certified International Privacy Professionals (CIPP). We also have Cyber Intelligence Centres strategically located in Canada and around the world.

Whether you are looking for a fully managed cybersecurity solution or a way to replace or augment your existing solution, the Cyber Intelligence Centre can help you:

Our cyber risk services can help you

Secure

By adopting a risk-based approach to cyber crime prevention, you gain access to timely, actionable threat intelligence, positioning you to improve the effectiveness of your security controls.

Vigilant

With a customized approach to cyber intelligence that takes your specific environment into account, you can more readily predict and prevent security incidents, strengthen your organization's threat profile and reduce your vulnerabilities to criminal attack.

Resilient

Some cyber incidents can cause serious business crises. Enhancing your ability to detect and respond to threats helps you minimize losses and get back to business-as-usual faster.

Cover off cyber risks – from end-to-end

With access to skilled resources, proven processes and effective tools that cross the entire security spectrum, you can keep pace with a constantly evolving threat landscape.

What can we do for you?

Secure

Establish a current security state to ensure that all devices are patched, updated and ready to handle potential attacks.

Vigilant

Establish periodic review of software and technologies in use to detect vulnerabilities and bugs.

Resilient

Establish the ability to handle critical incidents, quickly return to normal operations, and repair damage to the organization.

Are you inviting attackers in?

As global communication systems become more complex and access to technology proliferates, organizations of all sizes, in all sectors,face a growing range of cyber threats. Minimize the impact of breaches and protect against operational, financial and reputation risk with actionable, customized threat intelligence.

Cyber threat intelligence

Actionable threat reporting
Predictive analytics and risk modelling provide round-the-clock system and external threat monitoring based on relevance to your organization and industry. Detect advanced threats and act before they happen.

Cyber profiling
Your organization's cyber profile – the information the Internet makes available about your business, users and technology – will show you what criminals are working with when they target you.

Surveillance and CyberWatch
In-depth threat surveillance, threat indicator analysis and cyber chatter analysis are provided to you in customized reports to keep your organization in-the-know and able to execute impact-reducing threat responses.

Advanced threat analysis
Our next-generation analytical and forensics tools can help your organization address, triage and respond to advanced threats that could do irreparable harm to your networks and systems (e.g., malware, suspicious emails, unauthorized application changes and data access attempts).

Protect and detect

Traditional cyber crime approaches simply cannot handle advanced, evolving cyber threats. With next-generation detection and prevention security controls you can prepare for new threats based on your business's specific threat exposures.

Cyber threat mitigation

CyberSOC
The Deloitte Cyber SOC (Security Operations Centre) builds a central point within your organization to manage your preparation, detection, response and mitigation activities.
Core capabilities include:

- **Advanced, 24-7 security monitoring** for early threat detection
- **Advanced security analytics,** such as predictive analytics and adaptive risk modelling
- **Deloitte Advanced Threat (DAT) management,** where new data continuously improves threat knowledge and mitigation

Advanced cybersecurity vulnerability analysis
Cyberattackers are always searching for new vulnerabilities and weaknesses, from web exposures, to misconfigurations to training gaps that result in unprotected data. Assess and verify vulnerability exposures, identify relevant threats and enhance security using attack diagnostic services and cutting-edge application and network penetration testing.

Data loss prevention and insider threat prevention
Our Cyber Intelligence Centre can help detect insider threats, nested user activity and threats to critical data assets.

Advanced threat technology, combined with our world-class security transformation experience, provides a comprehensive solution to manage internal cyber risk.

An attack is inevitable – losing the battle shouldn't be

In today's rapidly evolving threat landscape, it is a matter of when, not if, an attack will happen. Preparation is critical. When you have a security incident, you need the ability to respond quickly, get the right people engaged, isolate the incident and remediate any damage with minimal business disruption. Then you incorporate that knowledge, learn from your mistakes and come back even stronger.

Cyber incident response

Cyber simulations
Using interactive techniques, this solution immerses participants in a simulated cyberattack scenario to help organizations evaluate their existing cyber response and their true organizational preparedness to effectively respond to cyberattacks.

Advanced threat response and recovery
We provide access to the skills, experience and knowledge your organization needs to effectively manage crisis response, reduce breach severity and accelerate response and recovery times.

Security forensics and root cause analysis
Following the response and recovery process, you want to assess what happened, find out how it happened and make sure it doesn't happen again. Root Cause Analysis (RCA) can involve not only incidents, but the failure of controls designed to *prevent* incidents; it also includes mitigation procedures.

We provide the people, processes, tools and technology to monitor and assess threats specific to your organization 24x7.

Transform your cybersecurity function

The Deloitte Cyber Intelligence Centre can help your organization disrupt attacks as they happen, reduce the timeframe and costs of recovery and contain future threats.

We provide the people, processes, tools and technology to monitor and assess threats specific to your organization 24x7, so you can quickly and effectively mitigate risk and strengthen your cyber resilience. Our professionals can also contextualize relevant threats to determine the risks to your business, customers and stakeholders.

To discuss strategies for enhancing your cyber resiliency, contact:

National

Mark Fernandes
Cyber Security Leader
416-601-6473
markfernandes@deloitte.ca

Nick Galletto
Technology Risk Leader
416-601-6734
ngalletto@deloitte.ca

Regional

Amir Belkhelladi
Partner
Enterprise Risk Services
514-393-7035
abelkhelladi@deloitte.ca

Alain Rocan
Partner
Enterprise Risk Services
613-751-5386
arocan@deloitte.ca

Justin Fong
Partner
Enterprise Risk Services
403-503-1464
jfong@deloitte.ca

Albert Yap
Partner
Enterprise Risk Services
604-640-3279
ayap@deloitte.ca

Dina Kamal
Senior Manager
Enterprise Risk Services
416-775-7414
dkamal@deloitte.ca

www.deloitte.ca/cyber

Designed and produced by the Deloitte Design Studio, Canada. 13-3727T