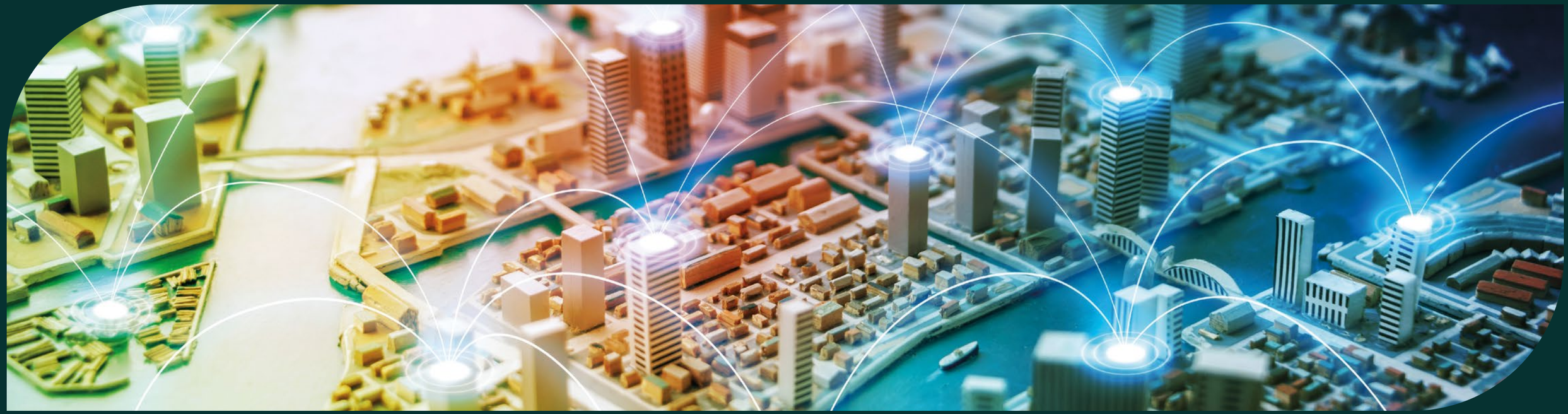
CIMA+ Engineering for **people**

CYBERSECURITY SERVICES



cima.ca

A LEADER IN CONSULTING ENGINEERING

With more than 30 years of industry experience, CIMA+ is the consulting engineering firm of choice across Canada. Our interdisciplinary team works hand-in-hand with clients to deliver exceptional results on projects large and small.

EMPLOYEE-OWNED AND CLIENT FOCUSED

We are proud to be employee-owned and rated one of Canada's best employers. This unique business model supports our strong culture of excellence, entrepreneurial spirit, and accountability. Clients love working with our talented roster of professionals and we take pride in delivering successful projects that set the stage for long-lasting, partnerships.

40+
offices across Canada

30+
years of industry experience

3,600+
employees

> **"We wish to make a difference with our employees, clients, and business partners to shape an inclusive, fair and carbon neutral world. We must work towards this ideal that is not contrary but rather complementary to the sustained growth we are aiming to achieve."**
>
> **Denis Thivierge,** P. Eng.
> President and Chief Executive Officer

CIMA+

KINCENTRIC
Best Employer
CANADA 2023

CYBERSECURITY THREAT AND RISK ASSESSMENT

When designing an architecture, engineering an application, or rolling out new technologies, organizations must ensure that cybersecurity risks are considered early on. This is key to delivering solutions that are secure by-design.

A cybersecurity threat and risk assessment examines potential threats and vulnerabilities in the framework of a project. This is performed by leveraging threat intelligence and modelling to identify risks, while considering regulatory compliance if applicable.

All the threats identified are documented and rated based on the probability they will manifest, and their impact. Our experts also provide recommendations and advice on adequate mitigation measures.

An inherently secure design is the most effective means of protecting your assets against attackers.

WHO IS IT FOR?

- Organizations concerned about their cybersecurity during the execution of strategic projects
- Organization requiring cybersecurity risks to be identified and rated
- Organizations requiring projects to be compliant with existing cybersecurity standards and best practices
- Organizations combining operational technologies (OT) with information technologies (IT)

CYBERSECURITY POSTURE ASSESSMENT

All organizations want to reduce their cybersecurity risks to a minimum, but cybersecurity resources are limited. Where should you start?

Cyberattacks can have critical consequences, particularly in the industrial sector. As these events are more and more frequent, we realize that there is no one-size-fits-all approach and no single product that can eradicate all cyber risks.

We take into consideration the particular threat landscape of each client organization to strategically determine the best course of action. We believe that adopting a strategic approach is key to ensuring a good return-on-investments (ROI) in terms of cybersecurity.

A cybersecurity posture assessment will provide stakeholders with a clear picture of the organization's maturity level regarding its cybersecurity practices. We provide a strategic roadmap to help you achieve your target state and track your progress over time.

Assessment criteria are based on the industry's best practices and recognized frameworks, such as NERC-CIP, NIST, CIS, and the Canadian Cyber Security Audit Program.

WHO IS IT FOR?

- C-Suite and cybersecurity managers concerned about their organization's cybersecurity posture
- Organizations concerned about the prioritization of cybersecurity investments
- Organizations who wish to track their maturity level in terms of cybersecurity

VULNERABILITY ASSESSMENT

Good cybersecurity practices are essential,
but organizations need to make sure they are adequately applied.

A vulnerability assessment is the most effective nd diligent way to test your organization's cybersecurity, ensuring that there are no vulnerabilities or security misconfigurations that can be exploitable by attackers. Such audits can be performed on external networks to determine public exposure to attackers and on internal networks for more comprehensive results.

A vulnerability assessment will reveal which assets pose the greatest risks to the organization and suggest the most effective mitigation measures. We provide technical support to help you navigate the challenges associated with risk remediation.

Vulnerability assessments should be carried out regularly, especially in mission-critical or fast-changing environments.

WHO IS IT FOR?

- Organizations performing due diligence
- Organizations having recently experienced a cybersecurity incident or near miss
- Organizations whose network underwent significant changes

CIMA+

INTRUSION TEST

Mission-critical assets and public-facing infrastructure assets are the preferred targets for attackers. Such intrusions can have a significative impact, especially when it targets operational technologies (OT). This is where in-depth security testing can make a difference.

An intrusion test is the best method to identify hard-to-find vulnerabilities, misconfigurations, and security flaws within applications.

Intrusion tests are performed by specially trained security professionals (ethical hackers) using real-world attacker's tactics and techniques to simulate controlled cyberattacks. Moreover, an intrusion test will concretely demonstrate the real impacts of cyberattacks, thus helping the organization identify and understand the risks to which it is exposed.

All the threats identified are documented and rated according to the probability they will manifest, and the severity of their impact. Our experts provide an action plan to help you mitigate the risks associated with these threats, as well as technical support to help you navigate the challenges associated with risk remediation.

WHO IS IT FOR?

- Organizations performing due diligence on their highly exposed assets or mission-critical systems
- Organizations requiring a high level of confidence in the cybersecurity of specific assets
- Organizations concerned about the security of a third-party solution

Contact:

Marc-André Gagnon
Director
Cybersecurity Services
marc-andre.gagnon@cima.ca

FOR MORE INFORMATION, CONTACT US:

info@cima.ca

CIMA+ HEAD OFFICE

600–3400, boulevard du Souvenir
Laval QC H7V 3Z2 Canada
T 514 337-2462

WE HAVE A LOCAL PRESENCE FROM COAST TO COAST, ALL ACROSS CANADA.

Baie-Comeau Beauce Bécancour Barrie Bowmanville Burlington Calgary – Airport Calgary – Downtown Clarenville Edmonton – Downtown Edmonton – West Gatineau Granby Guelph Halifax Kelowna Kitchener Labrador City Laval Lévis London Longueuil Mississauga Montréal Oakville Ottawa Québec City Red Lake Regina Rimouski Rivière-du-Loup Rouyn-Noranda Saguenay Saint John, NB Saskatoon Sept-Îles Sherbrooke Sorel-Tracy St John's, NL Sudbury Terrace Terrebonne Thunder Bay Toronto Vancouver Victoria West Kootenays

KINCENTRIC
Best Employer
CANADA 2023

CIMA+ Engineering for people

cima.ca

260521_CIMA+_Cybersecurity_Services_2024_v9.indd