# KPMG's Cyber Threat Simulation Challenge

## Will your cyber defences protect you? Are you sure?

CEOs, senior executives, and Cybersecurity and IT leaders face growing challenges in maintaining strong cybersecurity postures – often because their offensive (red team) and defensive (blue team) security functions aren't aligned. That's why "purple team" simulations – that shift the focus of conversation from "can someone break in?" to "if someone broke in, would I even know?" – can be so effective. Not only do purple team exercises help highlight gaps, they also provide valuable insights for how organizations can shore up their cyber defences.

In 2024, KPMG in Canada launched its first Cyber Threat Simulation Challenge, conducting a free cyberattack simulation, modeled after a purple team exercise, in a controlled environment to help organizations assess their cybersecurity capabilities.

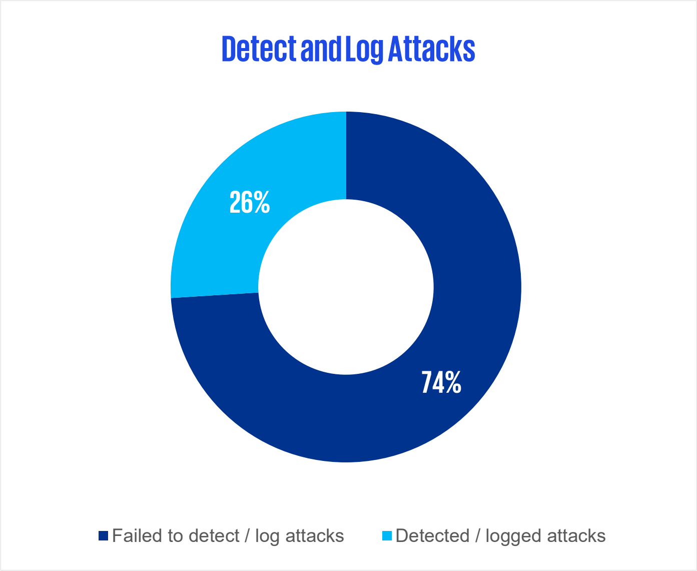
Over 150 companies registered from across Canada, demonstrating how critically important cybersecurity is to today's business leaders and their strong interest in validating their ability to detect and respond to cyber threats effectively.

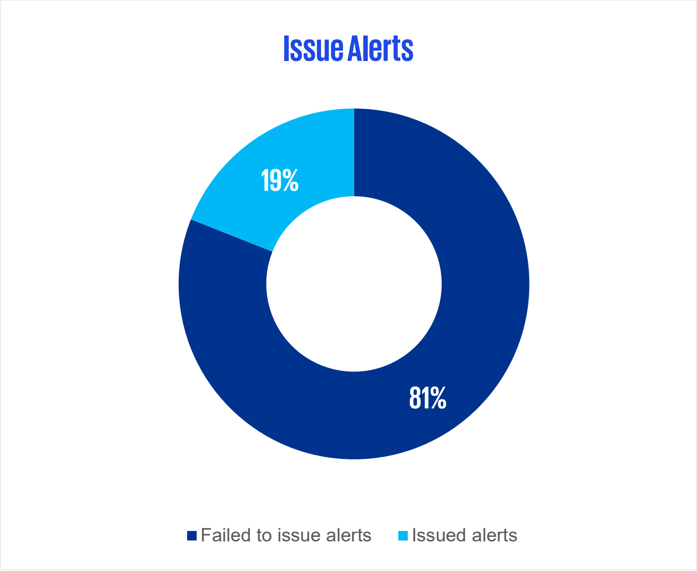
## 2024 Key findings: Few organizations are well prepared

Each hour-long simulation tested 4 to 7 real-world tactics that threat actors frequently use in cyberattacks including: Command & Control, Discovery, Defence Evasion, Credential Access – Kerberoastable, Credential Access - Rubeus, Persistence, and Execution.

The simulation tested organizations' cybersecurity capabilities in detecting and logging attacks, and aising alerts.

The results were remarkable.





If the tests had been real intrusions, it's likely the attacks would have gone unnoticed for most participants. Organizations that performed well during the simulations had strong technology in place to help detect and log cybersecurity incidents, as well as provide alerts to address them as effectively as possible.

Some industries struggled more than others in detecting threats, with Financial Services (primarily small- to medium-sized financial institutions), Healthcare and Wellness, and Food and Beverage topping the list, and small- to medium-sized businesses also tended to have higher detection failure rates.

Almost every participant indicated they hadn't tested their detection capabilities before. And since our research indicates MSSPs frequently don't conduct purple team exercises within their own environments, many organizations may be operating with ineffective detection use cases – and a false sense of security.

## Simulation tests benefit companies of all sizes

One of the biggest misconceptions of purple team exercises is that they're only designed for large organizations. Purple team exercises are beneficial for companies of all sizes, especially when the scope and approach align with your organization's maturity, resources, and risk profile.

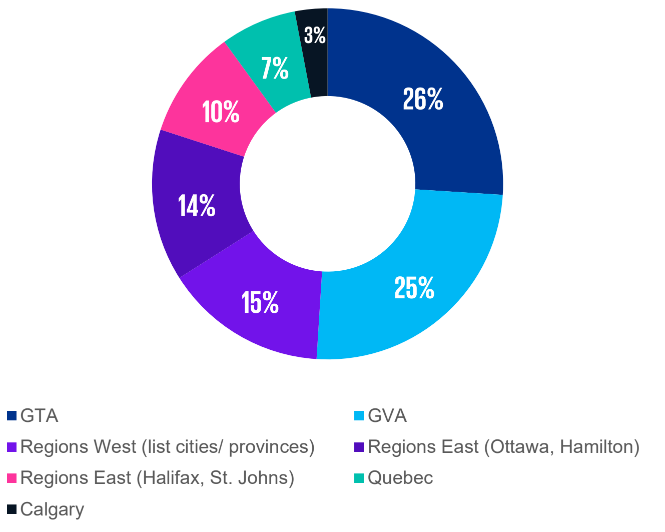
**Small to medium-sized businesses** (SMBs) often lack robust defenses, so cybercriminals increasingly target them. Purple team exercises help SMBs identify vulnerabilities, test defenses, and improve security processes cost-effectively. These exercises raise awareness and strengthen the security culture in organizations with limited resources.

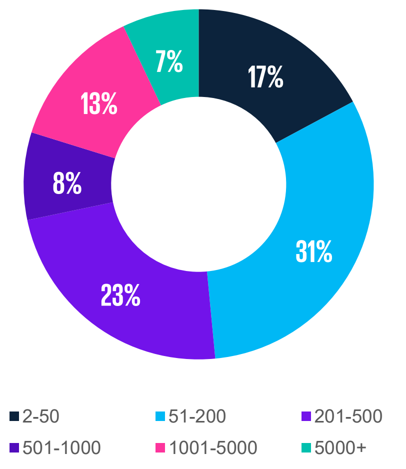
**Mid-market companies** manage growing complexities in IT environments (e.g., cloud, Internet of Things, etc.), but may still face resource constraints. Mid-market companies are often part of larger supply chains, making them attractive targets for attackers aiming at critical infrastructure or enterprise partners.

**Large enterprises** are high-value targets for advanced persistent threats (APTs), ransomware, and nation-state attacks. With complex IT ecosystems and distributed teams, purple team exercises ensure collaboration and coordination between their red and blue teams. They help validate security tools and strategies, refine incident response processes, and align with compliance requirements.

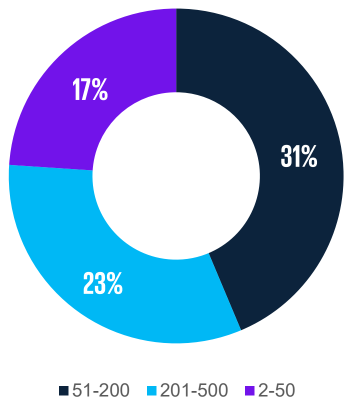
When downtime or breaches can have catastrophic consequences including security risks, financial and reputational losses, and even losses of life, purple team simulations can play a key role in your organization's cybersecurity operations, no matter the size or industry.

## KPMGs Cyber Threat Simulation Challenge: The top results

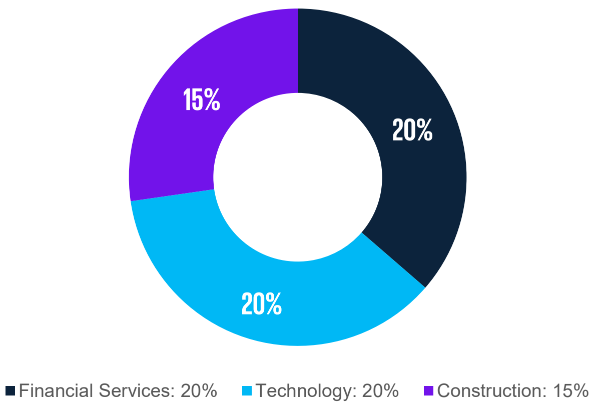

2024 Registrations by province


2024 Registrations by company size

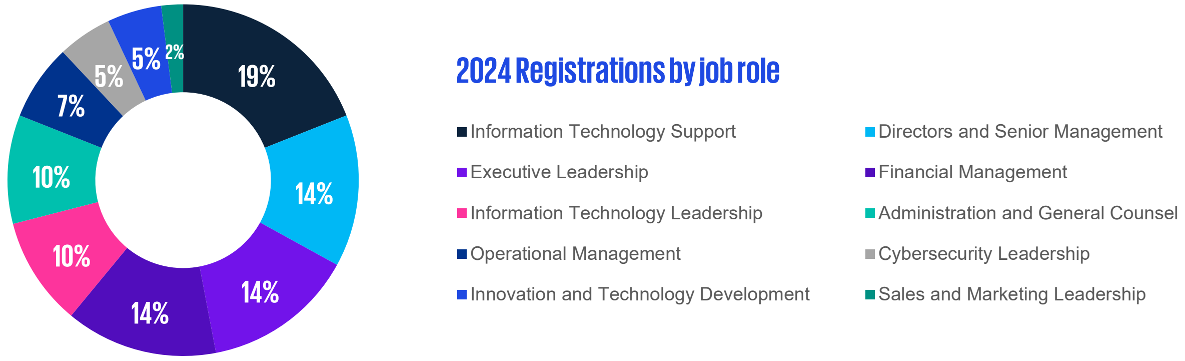
## 2024 Top 3 registrations by company size



## 2024 Top 3 registrations by industry



## 2024 Registrations by job role



## Will your cybersecurity defences protect you? Register now for KPMG's 2025 Cyber Threat Simulation Challenge and find out.

### What are the requirements to participate in the 2025 Challenge?

You'll need a domain joined Windows machine that permits outbound Internet access, preferably a VM that can be deleted afterward to help ensure full cleanup. It should have your regular security stack installed. Local administrator rights are not required. Participation is free of charge.

### How will the 2025 Challenge work?

1. After registering online, you'll receive an introductory email and an initial call from our team.
2. We'll explain the simulation, answer any questions, confirm the timing and the people required for the attack exercise.
3. We'll send you a Zip file that will run our safe malware executable payload, allowing us to perform specific commands within your environment. We'll conduct the simulation and note our observations. Once the simulation is complete, you'll delete the payload.
4. Afterward, we'll provide you with a report of our findings and arrange a follow-up call to discuss them.

kpmg.com/ca