INFOSEC GLOBAL

Discovery of Quantum Vulnerable Cryptography and Migration to Post-Quantum Cryptography

Dr. Vladimir Soukharev

Principal Cryptographic Technologist

and Chief Post-Quantum Researcher

InfoSec Global, Canada

INFOSEC GLOBAL

Common Cryptographic Pitfalls

Lack of Crypto Visibility

Organizations do not know which cryptographic algorithms are used to protect critical information

Vulnerable Crypto Implementation

Organizations implementing their own specific cryptography with lack of skills

In-Secure Crypto and Key Usage

Incorrect usage of cryptography parameters due to lack of crypto knowledge

Outdated Crypto Algorithms

Previously safe algorithms becoming in-secure without knowing it

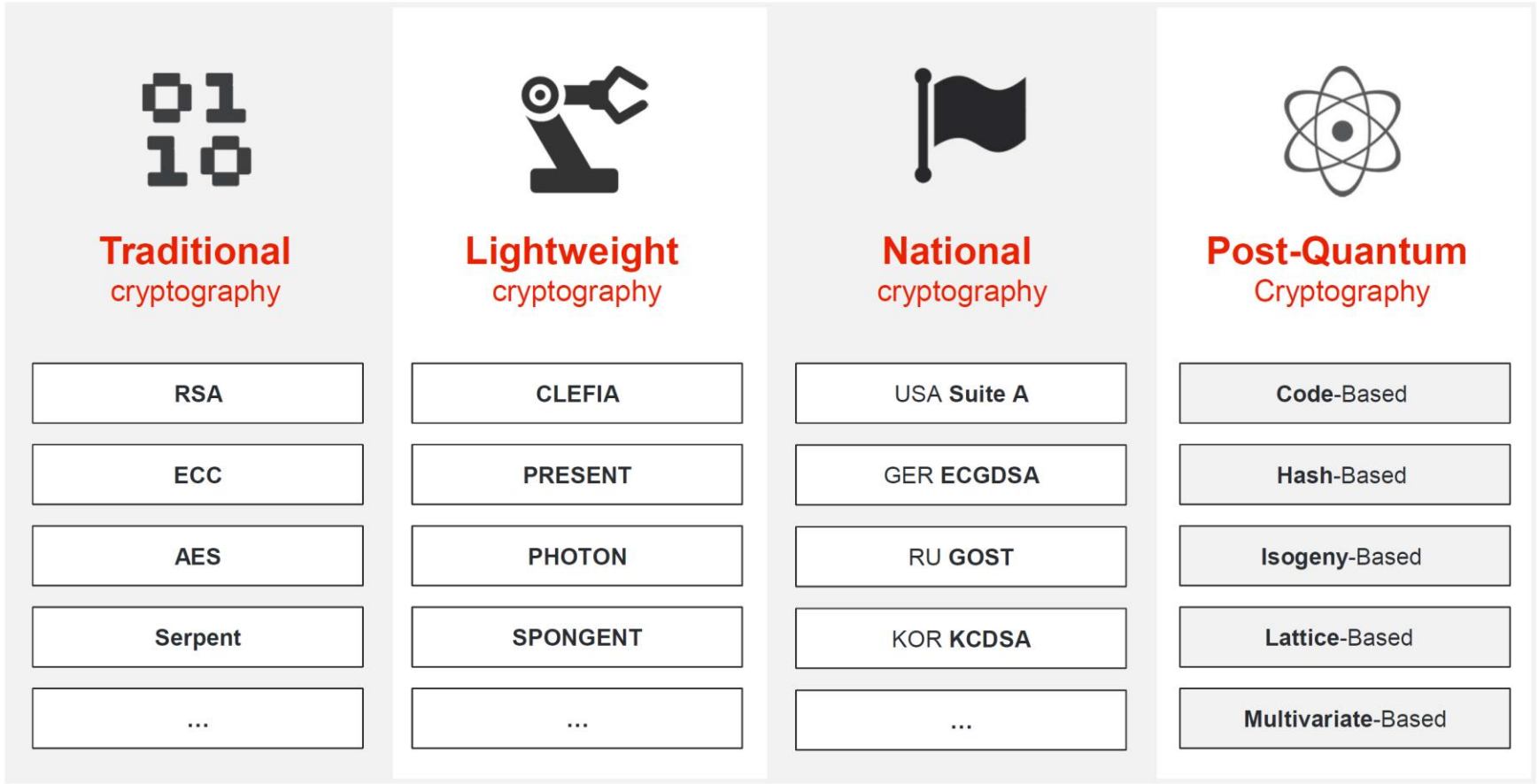
Quantum Computer Vulnerable Crypto

Long-life data protect by crypto scheme not ready for quantum computer era

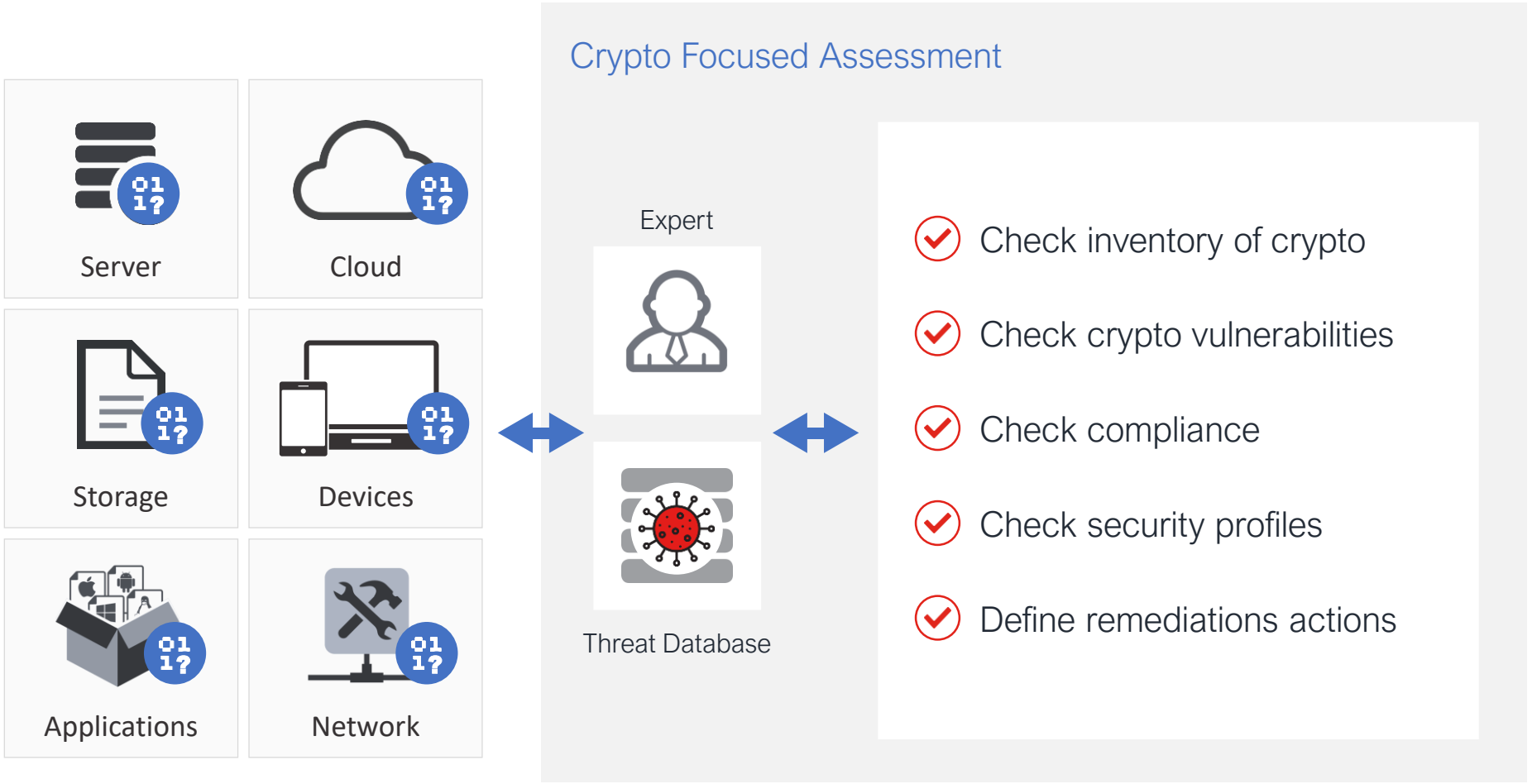
Complex Crypto Update Process

Costs and efforts required to manually update cryptography across several systems and apps

Diversity of Crypto Options



Crypto Threat Management



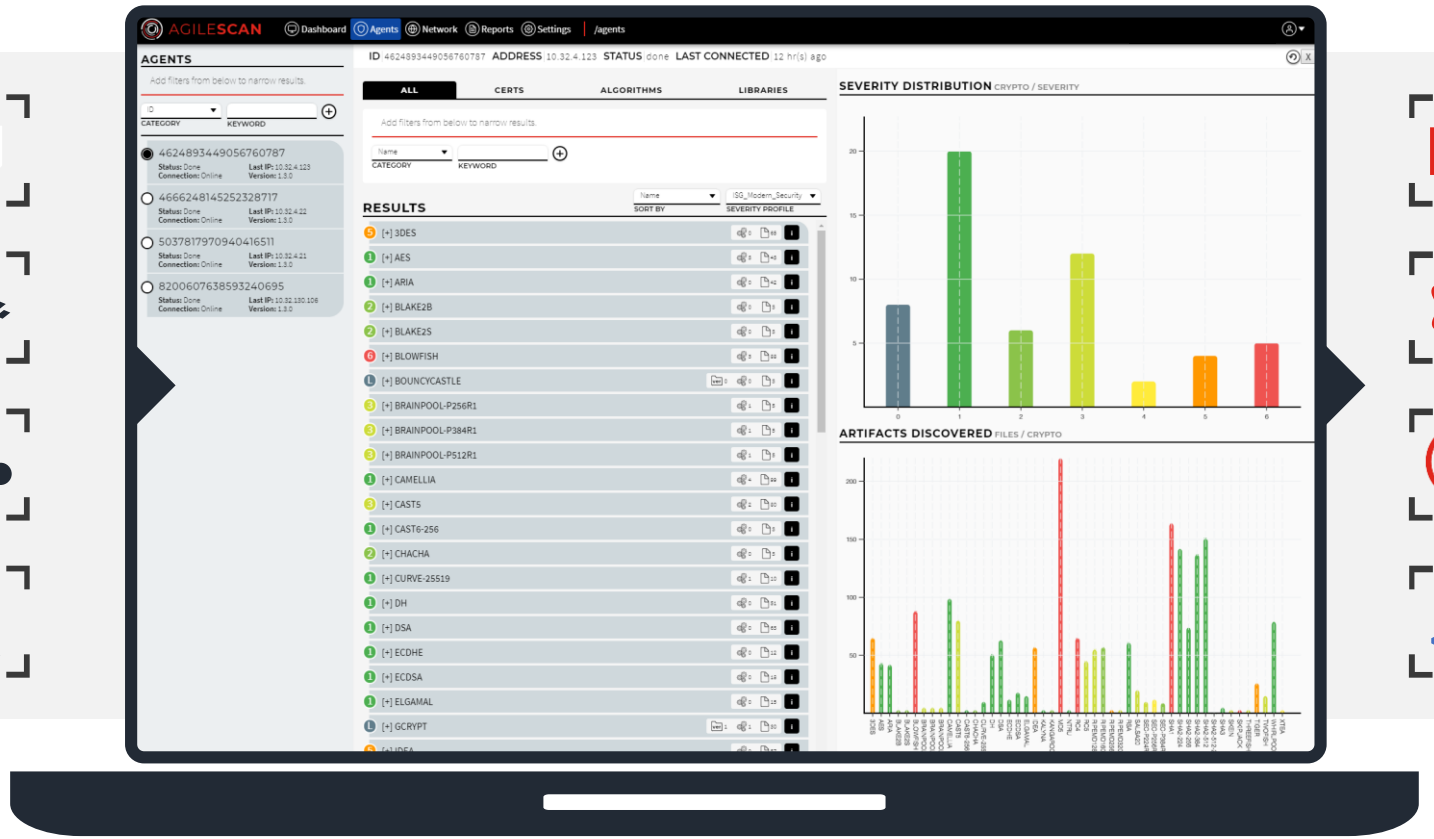
Crypto Analytics
Cryptographic Risk Assessment

Applications

Firmware

Hosts

Network



Inventory, assess and report **Certificates**

Inventory, assess and report **Cryptographic Algorithms**

Inventory, assess and report **Cryptographic Protocols**

Inventory, assess and report **Cryptographic Libraries**

Cryptographic Agility

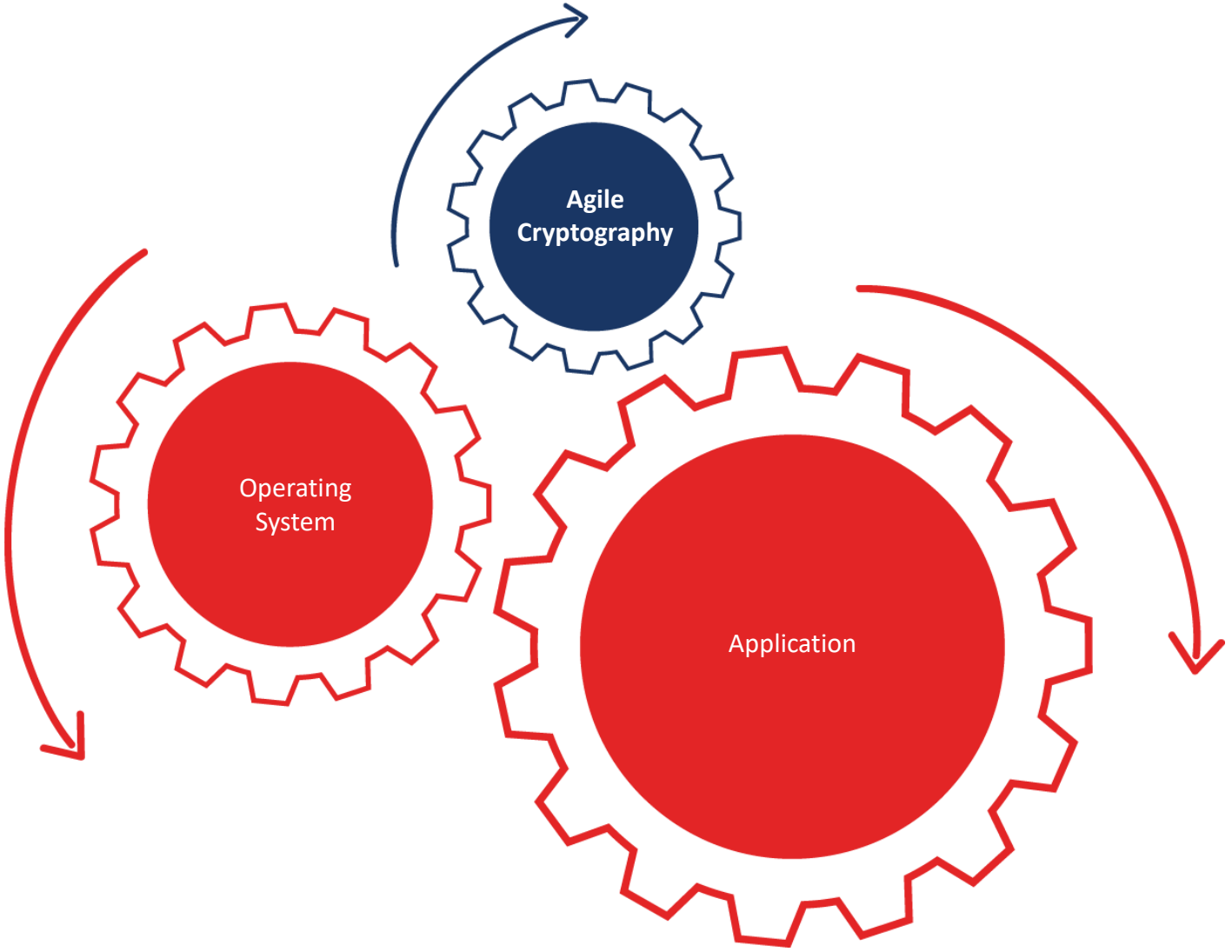
Cryptographic agility is the ability of a system to easily adopt alternatives to the cryptographic primitives it was originally designed to use.

Need for Cryptographic Agility

Modern Cryptography	Platform Optimized Cryptography	FIPS Certified Crypto	Custom Crypto Integration
Use modern, resilient and clean crypto implementation	Implement dedicated algorithms, counter measures or optimizations	Certify specific platform for use in government	Allow end-user to select crypto to use in their systems

Post-Quantum Readiness	In Field Crypto Update	Sovereign Crypto Program	Future Cryptography
Swap to post-quantum crypto standards as soon as available	Update crypto foundation of systems running in the field	Deploy National Crypto Program	Prepare systems for future standards

Agile Cryptography



INFOSEC GLOBAL

Crypto Agile Architecture

Applications

Abstract Crypto API | Protocol API

Dynamic Linking Engine

Cryptographic providers | Application Independent

- **Standard** Crypto Provider
- **FIPS** Crypto Provider
- **Post-Quantum** Crypto Provider
- **Plugin** Architecture

Agile Cryptography

Abstract API
Hide crypto complexity to developers

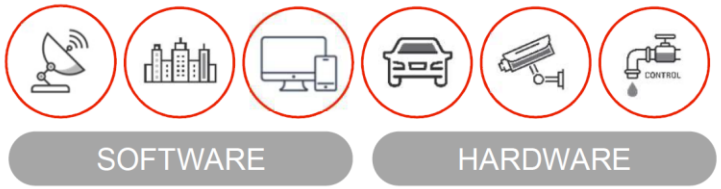
Dynamically Loadable
Change crypto during runtime

Select Implementation Type
Depending on use case

Deploy New Algorithm
Without modifying application code

Let experts decide which crypto to use
Make it manageable by others

Make it run on everything
Support as many platforms as possible



Prepare for the Quantum Computer

Create a Crypto Inventory

Know your vulnerabilities

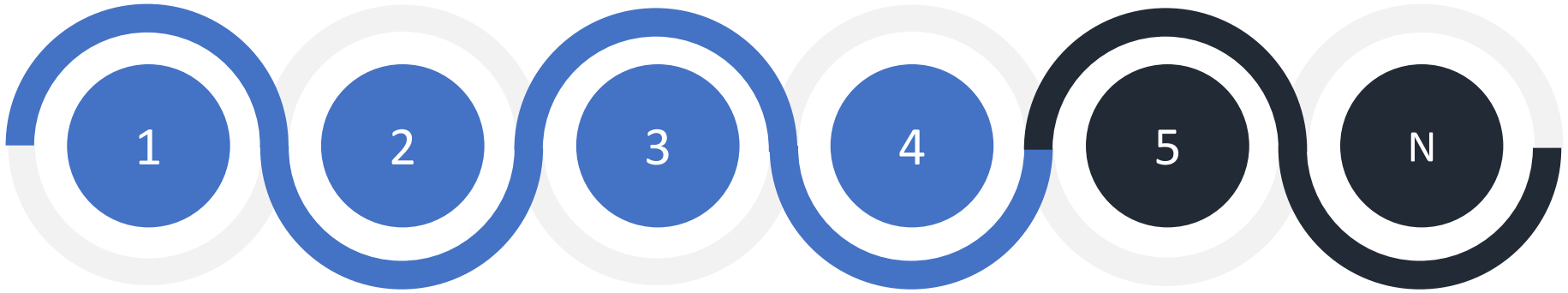
Move to a Crypto Agile System

Do the effort once

Use standard crypto for now

Move to NIST standards

NIST published its standards



Risk Assessment

When do I need to worry?

Move to PQC

Use todays PQC algorithms

Monitor Crypto Threats

Ready for future crypto challenges

Today

Quantum Computer Risk

Dr. Vladimir Soukharev
Principal Cryptographic Technologist
and Chief Post-Quantum Researcher

Vladimir.Soukharev@infosecglobal.com

InfoSec Global, Canada