HORIZON3

Meeting Canada's Bill C-8 Cybersecurity Requirements with NodeZero®

How autonomous security validation helps critical infrastructure operators build evidence-based cyber resilience under the Critical Cyber Systems Protection Act (CCSPA)

WHITEPAPER

Canada's Bill C-8 reflects a broader shift in cybersecurity regulation. Rather than focusing solely on policies, controls, or periodic assessments, regulators increasingly expect organizations operating critical infrastructure to demonstrate that critical cyber systems remain resilient against real-world attacks.

The legislation received Royal Assent on June 15, 2026. It strengthens Canada's telecommunications security framework and establishes the Critical Cyber Systems Protection Act (CCSPA), creating a regulatory framework for designated operators in federally regulated critical infrastructure sectors to protect critical cyber systems, report significant cyber incidents, and manage cyber risk. The CCSPA will be implemented through a phased regulatory process as designated operators and supporting regulations come into force.

For designated operators, cybersecurity is becoming an ongoing operational responsibility rather than a point-in-time compliance exercise.

Phased Implementation

CCSPA obligations will take effect as regulations designate covered operators and establish implementation requirements.

Critical Infrastructure Sectors

Telecommunications, banking, interprovincial and international pipeline and power line systems, nuclear energy systems, federally regulated transportation systems, and clearing and settlement systems.

The challenge

Critical infrastructure operators already maintain cybersecurity programs, conduct vulnerability assessments, deploy security controls, and respond to incidents. Yet those activities do not necessarily prove that critical cyber systems are protected from compromise.

Attack surfaces change continuously. New vulnerabilities emerge, identities and configurations drift, third-party dependencies introduce exposure, and attackers chain individual weaknesses into attacks capable of disrupting essential services.

Bill C-8 raises the operational question organizations must be prepared to answer:

Can we demonstrate that our critical cyber systems remain protected as threats and infrastructure change?

The **NodeZero® Proactive Security Platform** helps organizations answer that question with continuous, production-safe evidence of exploitability, business impact, and remediation effectiveness.

Turning Bill C-8 requirements into operational cyber resilience

The CCSPA establishes core obligations for designated operators. Organizations must establish and maintain cybersecurity programs, identify and manage cyber risk, protect critical cyber systems, detect cybersecurity incidents, reduce their impact, manage supply-chain risk, maintain records, and report significant cybersecurity incidents. While implementation details will be finalized through regulations, the operational direction is already clear.

1. Establish and maintain a cybersecurity program

KEY REQUIREMENT

Establish, implement, maintain, review, and update a cybersecurity program.

WHAT THE ACT REQUIRES

The CCSPA requires designated operators to establish a cybersecurity program that identifies and manages cybersecurity risks, protects critical cyber systems, detects cybersecurity incidents, minimizes their impact, manages supply-chain and third-party risk, and is reviewed and updated as necessary.

OPERATIONAL IMPLICATION

A cybersecurity program cannot exist only as documentation. Organizations need a repeatable way to demonstrate that cyber risks are continuously identified, validated, reduced, and reassessed as infrastructure and threats evolve.

Periodic penetration tests and vulnerability scans provide snapshots. They do not demonstrate whether attackers can exploit current conditions between assessments or whether remediation actually eliminated the attack path.

How NodeZero helps

Continuous Autonomous Pentesting
Safely validates internal, external, cloud, identity, Kubernetes, and web application environments using real attacker techniques.

AI-Powered WebApp Pentesting
Continuously validates custom web applications in production, safely identifying exploitable weaknesses in the applications attackers increasingly target first.

Risk-Based Exposure Management
Prioritizes proven attack paths instead of theoretical vulnerability lists.

NodeZero Insights
Provides executive reporting, remediation trends, and measurable evidence that the cybersecurity program is improving security over time.

2. Protect critical cyber systems

KEY REQUIREMENT

Protect systems that support Canada's vital services and infrastructure.

WHAT THE ACT REQUIRES

The cybersecurity program must include measures that protect critical cyber systems from compromise and support the continuity and security of the vital services those systems enable.

OPERATIONAL IMPLICATION

Knowing where vulnerabilities exist is only the beginning. Organizations must understand which weaknesses are actually exploitable, how attackers can chain them together, and whether existing controls prevent compromise of critical systems.

How NodeZero helps

Continuous Autonomous Pentesting
Validates exploitable weaknesses from both external and internal perspectives.

Cloud and Kubernetes Pentesting
Extends continuous validation across modern infrastructure.

AI-Powered WebApp Pentesting
Extends security validation to custom web applications and APIs, helping identify exploitable weaknesses before they become an entry point into critical systems.

AD Password Audit and Identity Security Validation
Identify credential and privilege weaknesses that attackers can exploit.

Network Segmentation Testing
Proves whether segmentation controls actually prevent lateral movement toward critical systems.

3. Manage supply-chain and third-party cyber risk

KEY REQUIREMENT

Identify and mitigate cybersecurity risks associated with suppliers and third-party products and services.

WHAT THE ACT REQUIRES

The CCSPA requires designated operators to identify and manage cybersecurity risks arising from their supply chains and from the use of third-party products and services, and to mitigate identified risks.

OPERATIONAL IMPLICATION

Questionnaires, certifications, and contractual assurances do not demonstrate whether third-party relationships introduce exploitable attack paths into the organization.

Organizations need continuous visibility into externally exposed assets and objective validation of real-world exposure.

How NodeZero helps

Third-Party Risk Management (TPRM)
Validates supplier security through autonomous pentesting, replacing questionnaires and assumptions with evidence of real-world resilience.

External Asset Discovery
Continuously identifies internet-facing assets across your organization and third-party ecosystem.

External Pentesting
Safely validates exploitable weaknesses across external attack surfaces, proving real exposure rather than theoretical risk.

Rapid Response
Quickly determines whether newly disclosed vulnerabilities affecting third-party technologies are present and exploitable within your environment.

4. Detect cybersecurity incidents

KEY REQUIREMENT

Detect cybersecurity incidents affecting or capable of affecting critical cyber systems.

WHAT THE ACT REQUIRES

Cybersecurity programs must include measures to detect cybersecurity incidents affecting, or having the potential to affect, critical cyber systems.

OPERATIONAL IMPLICATION

Detection capabilities should be validated against real attacker behavior rather than measured solely by deployed tools or alert volume.

Organizations should understand whether controls detect exploitation, credential abuse, privilege escalation, lateral movement, and attempts to access critical systems.

How NodeZero helps

NodeZero Tripwires
Deploys deception artifacts along validated attack paths, generating high-confidence alerts.

Endpoint Security Effectiveness
Demonstrates whether security controls detect or prevent the techniques used during autonomous testing.

Threat Actor Intelligence
Maps validated findings to relevant threat actor techniques.

Rapid Response
Provides production-safe testing for newly disclosed vulnerabilities.

AI-Powered WebApp Pentesting
Continuously identifies exploitable weaknesses in custom applications, reducing the likelihood that attackers gain an initial foothold through internet-facing business applications.

5. Minimize the impact of cybersecurity incidents

KEY REQUIREMENT

Reduce the operational impact of cybersecurity incidents.

WHAT THE ACT REQUIRES

Cybersecurity programs must include measures to minimize the impact of cybersecurity incidents affecting critical cyber systems and support the continuity of Canada's vital services.

OPERATIONAL IMPLICATION

Organizations must understand not only how an attack begins, but how far an attacker could progress after initial compromise.

Evidence of real attack paths provides far greater operational value than assumptions based solely on vulnerabilities or deployed controls.

How NodeZero helps

Full Attack-Path Validation
Demonstrates how attackers could progress from initial access to business-impacting compromise.

AI-Powered WebApp Pentesting
Validates whether exploitable application vulnerabilities can become the first step in a larger attack chain leading to business-impacting compromise.

High-Value Targeting
Prioritizes validation against systems most important to operations.

Advanced Data Pilfering
Demonstrates whether sensitive information is reachable through validated attack paths without exposing customer data.

1-Click Verify
Confirms that remediation eliminated the exploitable condition.

6. Report incidents and maintain security reports

KEY REQUIREMENT

Report significant cybersecurity incidents and maintain records demonstrating implementation of the cybersecurity program.

WHAT THE ACT REQUIRES

The CCSPA requires designated operators to report cybersecurity incidents involving critical cyber systems to the Communications Security Establishment within the period established by regulation, which cannot exceed 72 hours. Operators must also notify the appropriate regulator and maintain records relating to cybersecurity programs, incidents, supply-chain risk mitigation, and actions taken under the Act.

OPERATIONAL IMPLICATION

Organizations need defensible technical evidence before, during, and after an incident. That evidence should demonstrate what was exploitable, what changed, how risk was reduced, and whether remediation was successful.

NodeZero complements incident response by strengthening the technical evidence supporting regulatory reporting and executive decision-making.

How NodeZero helps

NodeZero Insights
Documents validated exposure, remediation progress, and long-term security trends.

Full Attack-Path Visualization
Provides context for understanding potential business impact.

1-Click Verify
Confirms corrective actions eliminated exploitable attack paths.

Continuous Validation
Creates measurable evidence demonstrating how cyber risk is identified, reduced, and verified over time.

Why continuous validation matters

Bill C-8 does not prescribe a specific cybersecurity technology or testing methodology. Instead, it establishes responsibilities for protecting critical cyber systems and creates a framework for demonstrating that cybersecurity programs are effectively managing operational risk.

The practical challenge is proving that those programs work.

A vulnerability scanner identifies potential weaknesses.

A configuration review confirms a control was deployed.

A remediation ticket records that a change was made.

None of those activities, by themselves, demonstrate that an attacker can no longer compromise a critical cyber system.

Visibility answers

- What assets exist?
- Which vulnerabilities have been identified?
- Which controls are deployed?
- Which remediation activities were completed?

Evidence answers

- Which vulnerabilities are actually exploitable?
- How can attackers chain weaknesses together?
- Can they reach critical cyber systems?
- What operational impact could result?
- Did remediation eliminate the attack path?

From periodic assessment to continuous evidence

Bill C-8 establishes cybersecurity as an ongoing operational responsibility. Continuous autonomous security validation supports that responsibility through a repeatable cycle.

Hack. Fix. Verify. Repeat.

Stage	What it does
Hack	Safely identifies exploitable attack paths using real attacker techniques.
Fix	Prioritizes remediation based on validated business risk.
Verify	Retests remediation and confirms exploitable attack paths have been eliminated.
Repeat	Continuously refreshes evidence as infrastructure and threats evolve.

Build compliance on evidence, not assumptions

Bill C-8 establishes new expectations for protecting the critical cyber systems that support Canada's most important services and infrastructure.

Implementation will continue through regulations, designation orders, and sector-specific oversight. However, the operational expectation is already clear: organizations must identify cyber risk, protect critical cyber systems, manage supply-chain exposure, detect incidents, minimize operational impact, maintain records, and report significant cybersecurity incidents.

NodeZero helps organizations continuously generate the technical evidence supporting those responsibilities.

By safely validating real attack paths, demonstrating business impact, and verifying that remediation eliminated exploitable conditions, NodeZero enables critical infrastructure operators to move beyond theoretical risk toward measurable cyber resilience.

PROVEN AT ENTERPRISE SCALE

300,000+
production-safe autonomous penetration tests conducted

7,000+
organizations running NodeZero

4 of the Fortune 10
trust NodeZero

Zero
production downtime across autonomous penetration tests

Key takeaway

Security programs should not be measured only by the number of vulnerabilities identified, controls deployed, or remediation tickets closed.

What ultimately matters is whether an attacker can still compromise critical cyber systems, how far they can progress, and whether security controls withstand real-world attacks.

NodeZero provides the continuous evidence organizations need to answer those questions with confidence while preparing for the operational expectations established by Canada's Critical Cyber Systems Protection Act.

This material is intended to provide general information about Bill C-8 and the Critical Cyber Systems Protection Act. It does not constitute legal advice or a definitive interpretation of obligations that may apply to a particular organization.