CASE STUDY

SHADOWHQ

Canadian Utility Goes from Ad Hoc to Incident-Ready

Team Cut Hours from Response Times and Runs 10+ Tabletop Exercises Annually

Customer

Delivering Essential Services with a Proactive Cyber Security Mindset

The water and wastewater sector plays a critical role in public health and safety but is one of the least regulated industries when it comes to cyber security. Without stringent national mandates, utilities often rely on internal leadership and best-practice frameworks to maintain strong defenses.

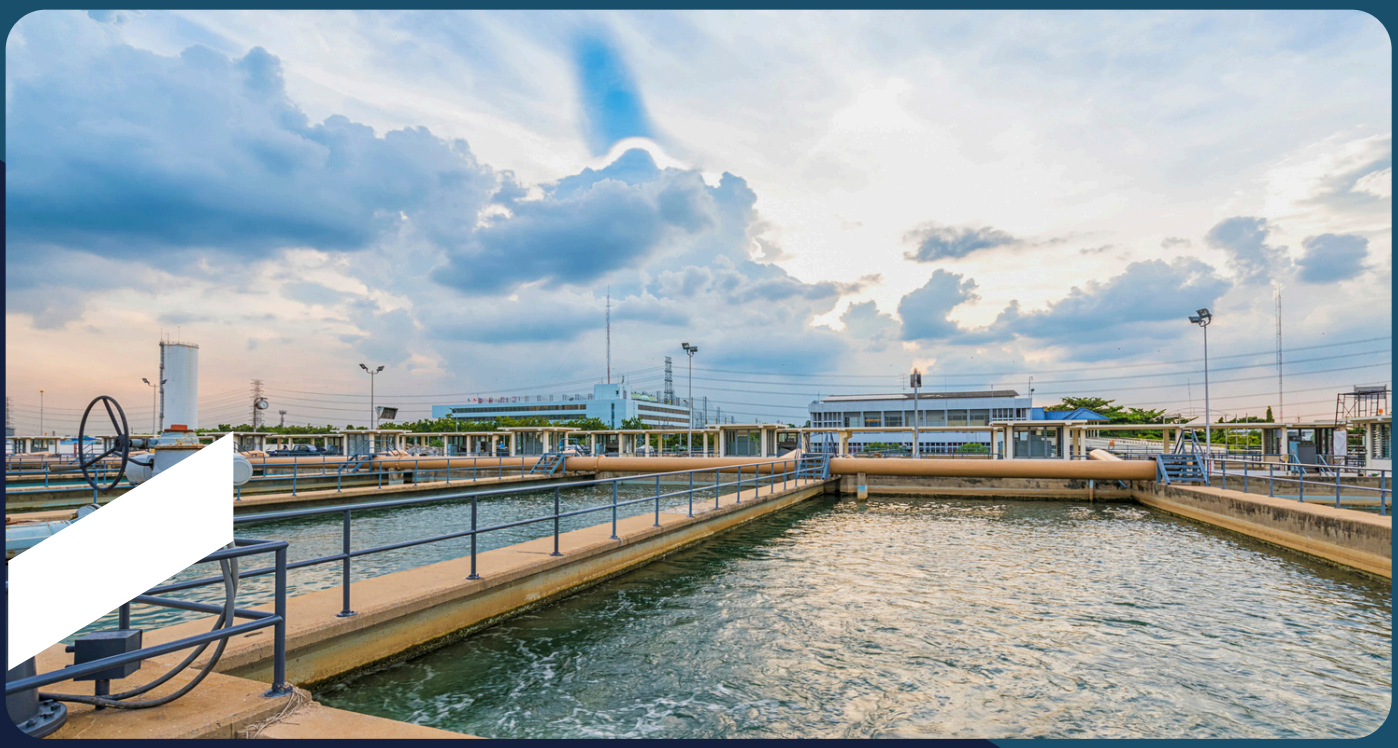
One Canadian water utility—serving approximately 400,000 residents with water, wastewater, and stormwater services—chose to be proactive. Despite the absence of formal regulations, the organization's cyber security leadership team was committed to building and maintaining a hardened, forward-leaning security program, anchored in the NIST-CSF framework.

.

INDUSTRY
Critical Infrastructure

HEADQUARTERS
Canada

COMPANY SIZE
- Serves approximately 400,000 citizens
- Provides water, wastewater and stormwater services across a Canadian city
- More than 600 dedicated staff



The Challenge

From Call Trees to Critical Gaps in Incident Response

During a cyber security audit, the utility identified a key gap: its incident response (IR) communications and coordination processes were ad hoc, siloed, and overly dependent on individuals. The audit recommended implementing a separate, out-of-band communications and ticketing system to maintain operations during an outage or cyberattack.

Prior to adopting ShadowHQ, the utility relied heavily on manual processes like cell phone call trees. If a critical team member was unavailable, incident activities could stall. Communication across IT and OT teams was inconsistent, and incident documentation was scattered across multiple tools, making after-action reporting time-consuming.

10 Minutes

Time to activate entire response team

The team's greatest concerns were:

- Loss of communication during a widespread attack or system outage
- Single points of failure in knowledge and execution of IR tasks
- Lack of centralization for playbooks, artifacts, and real-time updates

The Solution

Centralized Out-of-Band Communications and Rapid Playbook Deployment

ShadowHQ was selected for its ability to deliver secure, out-of-band communication, centralized incident coordination, and integrated ticketing—all within one platform.

Deployment was fast and efficient:

- **One month** to full operation
- **Ten playbooks loaded in under two weeks**
- **Broader Adoption** - The executive saw the tool's potential beyond cybersecurity, particularly for use cases like mass communication and incident coordination across other business units.

ShadowHQ's intuitive interface made it easy to create and refine playbooks, run realistic scenarios, and securely store all incident-related artifacts. It became the utility's central hub for both cyber security crisis management and tabletop exercises.

Results

Tabletop Exercises as a Force Multiplier

The utility dramatically expanded its tabletop exercise program with ShadowHQ:

- Runs monthly tabletop exercises, with up to two per month during initial playbook development
- Plans to complete more than 15 tabletops in one year, covering IT, OT, and operational impact scenarios
- Uses ShadowHQ to simulate realistic incidents, inject updates mid-exercise, and measure communication readiness

One notable exercise revisited a real incident—this time playing it out as if the incident hadn't been resolved as quickly as it was in real life. This deep dive allowed them to take the Incident further and validated the team's original response and strengthened their contingency planning.

In its first real incident using ShadowHQ, the utility:

- Cut response and resolution time to 2–3 hours by quickly adapting an existing playbook
- Saved a full day of post-incident reporting by pulling a complete timeline directly from the platform, eliminating the need to compile emails, chats, and meeting notes
- Streamlined executive reporting with accurate, real-time updates

The platform's centralized coordination eliminated the need for multiple update meetings and ensured everyone—from IR team members to executives—had the same situational awareness.

The cyber security risk manager emphasized that ShadowHQ not only met their original goal of securing out-of-band communications but also became a catalyst for building a proactive, well-structured incident readiness program—setting the utility ahead of potential regulatory changes.

> **"It's been a great partnership. The ShadowHQ team is incredibly responsive to what we need and receptive to our feedback.**
> **Any organization using this would find their incident response program better coordinated, more resilient, and panic-proof."**

SHADOWHQ

About ShadowHQ

ShadowHQ is a secure, out-of-band platform that helps CISOs and disaster recovery teams achieve incident preparedness.
Learn more at www.shadowhq.io.

Schedule a demo at **shadowhq.io/book-a-demo/**