WHO
WE ARE

HILLCYDE

ABOUT US

As a female-owned, Indigenous-led company and certified member of the CCIB, our approach is rooted in understanding deep connections—to the land and the businesses we serve. We provide thoughtful, sustainable insight and guidance, cutting through vendor noise to design solutions that genuinely fit your needs and deliver long-term value. We focus on building the right solution for you, starting with your requirements, not a product.

OUR MISSION

To build trust in cybersecurity by serving as the independent consultant,, connecting clients with the right partners and tailored solutions for their business

Incident Response

From IBM 2025 Cost of a Data Breach Report. Organizations with documented IR plans experience 85% faster recovery times than unprepared organizations.

HILLCYDE

Incident Response
IRP & TTX

HILLCYDE

Overview
The coordinated process of preparing for, detecting, containing, mitigating, and recovering from a cybersecurity incident or breach. The core goal is to reduce the damage, time, and costs associated with a security event while restoring normal operations as quickly and securely as possible. Effective IR requires a pre-defined plan, specialized tools, and a trained team to handle events ranging from common malware to complex, targeted attacks.

Incident Response Planning (IRP)
A formal Incident Response Plan (IRP) provides the structured guidance necessary to handle a security event efficiently and consistently. The plan is typically structured around six key phases: Preparation (establishing policies and resources); Identification/Detection (determining if an incident occurred); Containment (limiting scope and damage); Eradication (removing the root cause); Recovery (restoring systems); and Lessons Learned (improving the plan for future events). Adopting an IRP can dramatically reduce the average downtime for critical systems from around 23 days to approximately 2.5 days.

IR Table Top Exercises
Comprehensive penetration testing essential for transforming a static IRP document into a functional, validated capability. These drills simulate a real-world cyberattack scenario, allowing key personnel to walk through their roles, responsibilities, and communication protocols. Companies that conduct regular IR plan testing reduce their average breach costs by $1.49 million, demonstrating the financial necessity of these exercises. Regular TTXs ensure that the response team is familiar with the plan and prepared to respond effectively, reducing panic and minimizing damage when a real event occurs.

Advisory Services
Specialized Advisory Services provide the strategic leadership and guidance necessary to build and sustain a mature IR capability. A Virtual CISO (vCISO) acts as a retained executive resource to manage the security strategy, budget, and risk programs, ensuring the IRP aligns with overall business objectives. Program Development services focus on creating a strategic roadmap and establishing governance frameworks for the entire security function, ensuring IR maturity grows alongside the business. These services transition the organization from a reactive stance to a proactive one by embedding security into operations.

Contact HillCyde
If you have an Incident Response requirement—whether it's for creating a robust IRP, testing your current response capability with table top exercises, or needing 24/7 managed defense—our diverse portfolio of world-class, independent partners can deliver the precise expertise you require.

Contact HillCyde at **sales@hillcyde.com** to find your match.