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

OUR VISION

To be the premier, independent, one-stop cyber sresource, connecting any client—from SMB to Enterprise—with the ideal partners required to secure their environment

HILLCYDE

HILLCYDE

Overview

simulated cyberattack authorized by the organization and conducted on its own systems to evaluate their security posture. Unlike a simple vulnerability assessment, pen testing actively attempts to exploit known vulnerabilities, security weaknesses, and misconfigurations to gain access to critical assets and demonstrate real-world impact. By safely testing controls and human response, pen testing helps validate security investments, ensuring that defensive systems, processes, and personnel are effective in an active attack scenario.

Environment Testing

Penetration testing must be tailored to the specific environment being protected to achieve meaningful results, requiring high specialization for critical areas. Operational Technology (OT) Testing involves highly cautious assessments of industrial control systems (ICS) and SCADA environments, focusing on their unique protocols, legacy systems, and safety-critical nature to identify vulnerabilities without disrupting plant operations. Simultaneously, Cloud Testing assesses the security configurations, Identity and Access Management (IAM), and services within public cloud environments like AWS, Azure, or GCP, ensuring cloud-native deployments are secure against both external and internal threats.

Simulating Attacks

Comprehensive penetration testing simulates both External and Internal threat exposure to provide a complete picture of risk. External testing focuses on public-facing assets, applications, and networks accessible from the internet to identify perimeter weaknesses and initial attack vectors. Internal testing simulates an attacker who has already breached the perimeter (or an insider threat), assessing the ability to move laterally, elevate privileges, and access sensitive data. By simulating these realistic scenarios, organizations understand their entire attack surface and can measure the effectiveness of their layered security controls.

Penetration Testing Execution Standard (PTES)

Our partners uphold the highest standards in penetration testing methodology, notably aligning with the Penetration Testing Execution Standard (PTES). LARES is a firm that played a key role in the creation and establishment of the PTES, which provides a globally recognized framework for all penetration testing engagements. This ensures that every test is conducted meticulously, ethically, and results in comprehensive, actionable intelligence regarding real-world attack paths and their impact..

Contact HillCyde

If you have a Penetration Testing requirement—whether it's for a standard network assessment, a critical application, or a sensitive OT environment—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.